ETSI TS 129 512 V17.7.0 (2022-06)

5G;
5G System;
Session Management Policy Control Service;
Stage 3
(3GPP TS 29.512 version 17.7.0 Release 17)

Reference
RTS/TSGC-0329512vh70

Keywords
5G

ETSI

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

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

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

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Legal Notice

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

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

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

Modal verbs terminology

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

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

Contents

Foreword

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

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

Version x.y.z

where:

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

1 Scope

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

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

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

The Policy Control Function with session related policies provides the Session Management Policy Control Service to the NF server consumers (e.g. 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 Specification Version 3.0.0", https://spec.openapis.org/oas/v3.0.0.

[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] Void.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[32] 3GPP TS 29.122: "T8 reference point for Northbound APIs".

[33] 3GPP TS 23.527: "5G System; Restoration Procedures".

[34] 3GPP TS 29.503: "5G System; Unified Data Management Services; Stage 3".

[35] 3GPP TS 32.255: "Charging management; 5G data connectivity domain charging; stage 2".

[36] 3GPP TS 29.518: "5G System; Access and Mobility Management Services; Stage 3".

[37] 3GPP TS 29.274: "3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3".

[38] 3GPP TR 21.900: "Technical Specification Group working methods".

[39] 3GPP TS 29.521: "5G System; Binding Support Management Service; Stage 3".

[40] 3GPP TS 29.524: "Cause codes mapping between 5GC interfaces; Stage 3".

[41] 3GPP TS 24.008: "Mobile radio interface Layer 3 specification".

[42] 3GPP TS 23.316: "Wireless and wireline convergence access support for the 5G System (5GS)".

[43] 3GPP TS 24.193: "Access Traffic Steering, Switching and Splitting (ATSSS); Stage 3".

[44] 3GPP TS 24.519: "Time-Sensitive Networking (TSN) Application Function (AF) to Device-Side TSN Translator (DS-TT) and Network-Side TSN Translator (NW-TT) protocol aspects; Stage 3".

[45] IEEE 802.1Q: "Virtual Bridged Local Area Networks".

[46] 3GPP TS 29.551: "5G System; Packet Flow Description Management Service; Stage 3".

[47] BBF TR-456: "AGF Functional Requirements".

[48] CableLabs WR-TR-5WWC-ARCH: "5G Wireless Wireline Converged Core Architecture".

[49] 3GPP TS 24.539: "5G System (5GS); Network to TSN translator (TT) protocol aspects; Stage 3".

[50] 3GPP TS 29.564: "5G System; User Plane Function Services; Stage 3".

[51] 3GPP TS 29.520: "5G System; Network Data Analytics Services; Stage 3".

[52] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".

[53] 3GPP TS 29.565: "5G System; Time Sensitive Communication and Time Synchronization Function Services; Stage 3".

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].

5G QoS Flow: The finest granularity for QoS forwarding treatment in the 5G System. All traffic mapped to the same 5G QoS Flow receive the same forwarding treatment (e.g. scheduling policy, queue management policy, rate shaping policy, RLC configuration, etc.). Providing different QoS forwarding treatment requires separate 5G QoS Flow.

5G QoS Identifier: A scalar that is used as a reference to a specific QoS forwarding behaviour (e.g. packet loss rate, packet delay budget) to be provided to a 5G QoS Flow. This may be implemented in the access network by the 5QI referencing node specific parameters that control the QoS forwarding treatment (e.g. scheduling weights, admission thresholds, queue management thresholds, link layer protocol configuration, etc.).

Access Traffic Steering: The procedure that selects an access network for a new data flow and transfers the traffic of this data flow over the selected access network. Access traffic steering is applicable between one 3GPP access and one non-3GPP access.

Access Traffic Switching: The procedure that moves all traffic of an ongoing data flow from one access network to another access network in a way that maintains the continuity of the data flow. Access traffic switching is applicable between one 3GPP access and one non-3GPP access.

Access Traffic Splitting: The procedure that splits the traffic of a data flow across multiple access networks. When traffic splitting is applied to a data flow, some traffic of the data flow is transferred via one access and some other traffic of the same data flow is transferred via another access. Access traffic splitting is applicable between one 3GPP access and one non-3GPP access.

Application detection filter: A logic used to detect packets generated by an application based on extended inspection of these packets, e.g., header and/or payload information, as well as dynamics of packet flows. The logic is entirely internal to a UPF, and is out of scope of this specification.

Application identifier: An identifier, referring to a specific application detection filter.

Application service provider: A business entity responsible for the application that is being / will be used by a UE, which may be either an AF operator or has an association with the AF operator.

Binding: The association between a service data flow and the QoS Flow transporting that service data flow.

Binding mechanism: The method for creating, modifying and deleting bindings.

Charging control: The process of associating packets, belonging to a service data flow, to a charging key and applying online charging or offline charging, as appropriate.

Charging key: information used by the CHF for rating purposes.

Detected application traffic: An aggregate set of packet flows that are generated by a given application and detected by an application detection filter.

Dynamic PCC Rule: a PCC rule, for which the definition is provided to the SMF by the PCF.

Gating control: The process of blocking or allowing packets, belonging to a service data flow / detected application's traffic, to pass through to the UPF.

MA PDU Session: A PDU Session that provides a PDU connectivity service, which can use one access network at a time, or simultaneously one 3GPP access network and one non-3GPP access network.

Monitoring key: information used by the SMF and PCF for usage monitoring control purposes as a reference to a given set of service data flows or application (s), that all share a common allowed usage on a per UE and DNN and S-NSSAI basis.

Operating System (OS): Collection of UE software that provides common services for applications.

Operating System Identifier (OSId): An identifier identifying the operating system.

PCC decision: A PCF decision for policy and charging control provided to the SMF (consisting of PCC rules and PDU Session related attributes), a PCF decision for access and mobility related control provided to the AMF, a PCF decision for UE access selection and PDU Session selection related policy provided to the UE or a PCF decision for background data transfer policy provided to the AF.

PCC rule: A set of information enabling the detection of a service data flow and providing parameters for policy control and/or charging control and/or other control or support information. The possible information is described in clause 6.3.1.

PDU Session: Association between the UE and a Data Network that provides a PDU connectivity service.

Policy control: The process whereby the PCF indicates to the SMF how to control the QoS Flow. Policy control includes QoS control and/or gating control.

Policy Control Request trigger report: a notification, possibly containing additional information, of an event which occurs that corresponds with a Policy Control Request trigger.

Policy Control Request trigger: defines a condition when the SMF shall interact again with the PCF.

Predefined PCC Rule: a PCC rule that has been provisioned directly into the SMF by the operator.

Redirection: Redirect the detected service traffic to an application server (e.g. redirect to a top-up / service provisioning page).

Service data flow: An aggregate set of packet flows carried through the UPF that matches a service data flow template.

Service data flow filter: A set of packet flow header parameter values/ranges used to identify one or more of the packet flows in the UPF. The possible service data flow filters are defined in clause 6.2.2.2.

Service data flow filter identifier: A scalar that is unique for a specific service data flow (SDF) filter within a PDU session.

Service data flow template: The set of service data flow filters in a PCC Rule or an application identifier in a PCC rule referring to an application detection filter in the SMF or in the UPF, required for defining a service data flow.

Service identifier: An identifier for a service. The service identifier provides the most detailed identification, specified for flow based charging, of a service data flow. A concrete instance of a service may be identified if additional AF information is available (further details to be found in clause 6.3.1).

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

Onboarding Standalone Non-Public Network

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].

ADC	Application Detection and Control
5G-RG	5G Residential Gateway
AF	Application Function
AMF	Access and Mobility Management Function
API	Application Programming Interface
ATSSS	Access Traffic Steering, Switching, Splitting
ATSSS-LL	ATSSS Low-Layer
BBF	Broadband Forum
CHEM	Coverage and Handoff Enhancements using Multimedia error robustness feature
CHF	Charging Function
DDD	Downlink Data Delivery
DDN	Downlink Data Notification
DN-AAA	Data Network Authentication, Authorization and Accounting
DNN	Data Network Name
DS-TT	Device-side TSN translator
DTS	Data Transport Service
EAS	Edge Application Server
ePDG	evolved Packet Data Gateway
FN-RG	Fixed Network Residential Gateway
GEO	Geosynchronous Orbit
GFBR	Guaranteed Flow Bit Rate
GUAMI	Globally Unique AMF Identifier
HFC	Hybrid Fiber Coax
HTTP	Hypertext Transfer Protocol
I-SMF	Intermediate SMF
LEO	Low Earth Orbit
MA	Multi-Access
MEO	Medium Earth Orbit
MPTCP	Multi-Path TCP Protocol
NAS	Non-Access-Stratum
NEF	Network Exposure Function
NF	Network Function
NID	Network Identifier
NRF	Network Repository Function
NWDAF	Network Data Analytics Function
NW-TT	Network-side TSN translator
ON-SNPN	Onboarding Standalone Non-Public Network
PCC	Policy and Charging Control
PCF	Policy Control Function
PFD	Packet Flow Description
PFDF	Packet Flow Description Function
PMIC	Port Management Information Container
PSA	PDU Session Anchor
PSAP	Public Safety Answering Point
QoS	Quality of Service
RTT	Round-Trip Time
SDF	Service Data Flow
SMF	Session Management Function
SNPN	Stand-alone Non-Public Network
S-NSSAI	Single Network Slice Selection Assistance Information
SUPL	Secure User Plane for Location
TNAN	Trusted Non-3GPP Access Network
TWAN	Trusted WLAN Access Network
TSC	Time Sensitive Communication
TSCAI	Time Sensitive Communication Assistance Information
TSCTSF	Time Sensitive Communication and Time Synchronization Function
TSN	Time Sensitive Networking
TSN GM	TSN Grand Master
UDM	Unified Data Management
UDR	Unified Data Repository
UE	User Equipment
UL CL	UpLink CLassifier

UMIC	User plane node Management Information Container
URLLC	Ultra Reliable Low Latency Communication
W-5GAN	Wireline 5G Access Network
W-5GBAN	Wireline BBF Access Network
W-5GCAN	Wireline 5G Cable Access Network
W-AGF	Wireline Access Gateway Function

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 (e.g. SMF). The Session Management Policy Control Service can be used for charging control, policy control, application detection and control and/or access traffic steering, switching and splitting within a MA PDU Session. Session Management Policy Control Service applies to the cases where the SMF interacts with the PCF in the non-roaming scenario, the 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.

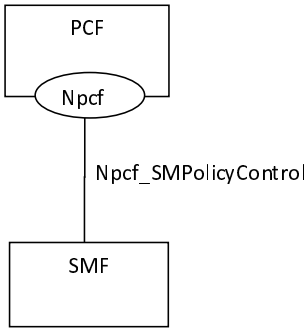

Figure 4.1.2-1: Reference Architecture for the Npcf_SMPolicyControl Service; SBI representation

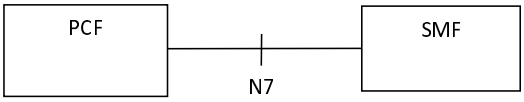

Figure 4.1.2-2: Reference Architecture for the Npcf_SMPolicyControl Service; reference point representation

NOTE: The 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 traffic steering, switching and steering within a MA PDU Session, access network information report, UMIC, PMIC and TSCAI input container 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;

NOTE: For local breakout roaming, session management policy data for the UE as defined in 3GPP TS 29.519 [15] is not available in the VPLMN and V-PCF uses locally configured information according to the roaming agreement with the HPLMN operator. All interactions to the UDR in this document are subject to this restriction.

- 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 from the CHF; and
- PCF pre-configured policy context.

4.1.3.2 NF Service Consumers

The SMF is responsible for the enforcement of session management related policy decisions from the PCF, related to service flow detection, QoS, charging, gating, traffic usage reporting, traffic steering and access traffic steering, switching and splitting within a MA PDU Session.

The SMF shall support:

- sending the PDU session related attributes to the PCF;
- requesting and receiving the PCC rule(s) from the PCF;
- binding of service data flows to QoS flow as defined in 3GPP TS 29.513 [7];
- deriving rule(s) from the PCC rule(s) and then providing those rules to the user plane function or remove the rule(s) from the user plane as defined in 3GPP TS 29.244 [13];
- deriving the QoS rules towards the UE;
- deriving the QoS profile towards the access network;
- deriving the ATSSS rules towards the UE if applicable;
- transferring the DS-TT PMIC transparently towards/from the UE/DS-TT and transferring the B/PMIC transparently towards/from the UPF/NW-TT, if applicable;
- adapting received TSCAI input information (TSC assistance container) to 5GS GM and transferring the TSCAI to the AN-RAN;
- handling the policy control request trigger; and

- handling the PDU session related policy information.

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

4.1.4 Rules

4.1.4.1 General

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

Two types of rules are defined:

- Session rule; and
- PCC rule.

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

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

4.1.4.2 PCC rules

4.1.4.2.1 PCC rules definition

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

- Dynamic PCC rules: PCC rules that are dynamically provisioned by the PCF to the SMF. These PCC rules may be either predefined or dynamically generated in the PCF. Dynamic PCC rules can be installed, modified and removed at any time.
- Predefined PCC rules: PCC rules that are preconfigured in the SMF. Predefined PCC rules can be activated or deactivated by the PCF at any time. Predefined PCC rules within the PCF may be grouped allowing the PCF to dynamically activate a set of PCC rules.

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

NOTE 1: When the SMF interacts with the PCF for a PCC rule base, the PCF has no way of knowing which individual PCC rule of the PCC rule base caused the interaction. If such knowledge is required for specific PCC rules, then these PCC rules need to be implemented either as dynamic PCC rules or as predefined PCC rules that are not grouped in a PCC rule base. The SMF decision logic for interacting (or not) with the PCF about an event related to a PCC rule base is up to implementation and depends on the specific issue that triggered this interaction.

NOTE 2: The operator can define a predefined PCC rule, to be activated by the SMF. Such a predefined rule is not explicitly known in the PCF.

A PCC rule consists of:

Table 4.1.4.2.1-1: PCC rule information elements

Information name	Description	Category
Rule identifier	Uniquely identifies the PCC rule, within a PDU Session. It is used between PCF and SMF for referencing PCC rules.	Mandatory
	Service data flow detection	
Precedence	Determines the order, in which the service data flow templates are applied at service data flow detection, enforcement and charging.	Mandatory
Service Data Flow Template	For IP PDU traffic: Either a list of service data flow filters or an application identifier that references the corresponding application detection filter for the detection of the service data flow. For Ethernet PDU traffic: Combination of traffic patterns of the Ethernet PDU traffic.	Mandatory
Mute for notification	Defines whether application's start or stop notification is to be muted.	Optional
	Charging	
Charging key	The charging system (CHF) uses the charging key to determine the tariff to apply to the service data flow.	Optional
Service identifier	The identity of the service or service component the service data flow in a rule relates to.	Optional
Sponsor Identifier	An identifier, provided from the AF, which identifies the Sponsor, used for sponsored flows to correlate measurements from different users for accounting purposes.	Optional
Application Service Provider Identifier	An identifier, provided from the AF, which identifies the Application Service Provider, used for sponsored flows to correlate measurements from different users for accounting purposes.	Optional
Charging method	Indicates the required charging method for the PCC rule. Values: online or offline or none.	Optional
Service Data flow handling while requesting credit	Indicates whether the service data flow is allowed to start while the SMF is waiting for the response to the credit request. Only applicable for charging method online.	Optional
Measurement method	Indicates whether the service data flow data volume, duration, combined volume/duration or event shall be measured. This is applicable to reporting, if the charging method is online or offline. Note: Event based charging is only applicable to predefined PCC rules and PCC rules used for application detection filter (i.e. with an application identifier).	Optional
Application Function Record Information	An identifier, provided from the AF, correlating the measurement for the Charging key/Service identifier values in this PCC rule with application level reports.	Optional
Service identifier level reporting	Indicates that separate usage reports shall be generated for this Service identifier. Values: mandated or not required.	Optional
	Policy control	
5QI	Identifier of the authorized QoS parameters for the service data flow.	Mandatory
ARP	The Allocation and Retention Priority for the service data flow consisting of the priority level, the pre-emption capability and the pre-emption vulnerability.	Mandatory
Gate status	The gate status indicates whether the service data flow, detected by the service data flow template, may pass (Gate is open) or shall be discarded (Gate is closed).	Optional
QoS Notification Control (QNC)	Indicates whether notifications are requested from 3GPP NG-RAN when the GFBR can no longer (or again) be guaranteed for a QoS Flow during the lifetime of the QoS Flow.	Optional
Reflective QoS Control	Indicates to apply reflective QoS for the SDF.	Optional
MBR (UL/DL)	The uplink/downlink maximum bitrate authorized for the service data flow.	Optional
GBR (UL/DL)	The uplink/downlink guaranteed bitrate authorized for the service data flow.	Optional
UL sharing indication	Indicates resource sharing in uplink direction with service data flows having the same value in their PCC rule.	Optional
DL sharing indication	Indicates resource sharing in downlink direction with service data flows having the same value in their PCC rule.	Optional
Redirect	Redirect state of the service data flow (enabled/disabled).	Optional
Redirect Destination	Controlled Address to which the service data flow is redirected when redirect is enabled.	Optional

Bind to default QoS Flow	Indicates that the dynamic PCC rule shall always have its binding with the default QoS Flow.	Optional
Priority Level	Indicates a priority in scheduling resources among QoS Flows.	Optional
Averaging Window	Represents the duration over which the guaranteed and maximum bitrate shall be calculated.	Optional
Maximum Data Burst Volume	Denotes the largest amount of data that is required to be transferred within a period of 5G-AN PDB.	Optional
Disable UE notifications at changes related to Alternative QoS Profiles	Indicates to disable QoS flow parameters signalling to the UE when the SMF is notified by the NG-RAN of changes in the fulfilled QoS situation. The fulfilled situation is either the QoS profile or an Alternative QoS Profile.	Optional
	Access Network Information Reporting	
User Location Required	The UE location(s) (e.g. the serving cell of the UE) is to be reported. When the corresponding QoS flow is deactivated, and if available, information on when the UE was last known to be in that location is also to be reported.	Optional
UE Timezone Required	The time zone of the UE is to be reported.	Optional
	Usage Monitoring Control	
Monitoring key	The PCF uses the monitoring key to group services that share a common allowed usage.	Optional
	N6-LAN Traffic Steering Enforcement Control	
Traffic steering policy identifier(s)	Reference to a pre-configured traffic steering policy at the SMF.	Optional
	AF influenced Traffic Steering Enforcement Control	
Data Network Access Identifier	Identifier of the target Data Network Access.	Optional
Per DNAI: Traffic steering policy identifier	Reference to a pre-configured traffic steering policy at the SMF.	Optional
Per DNAI: N6 traffic routing information	Describes the information necessary for traffic steering to the DNAI.	Optional
Information on AF subscription to UP path changes events	Indicates whether a notification in case of UP path change is requested, as well as the destination(s) for where to provide the notification.	Optional
Indication of UE IP address preservation	Indicates UE IP address should be preserved.	Optional
Indication of traffic correlation	Indicates that the target PDU Sessions should be correlated via a common DNAI in the user plane.	Optional
Information on User Plane Latency requirements	Indicates the user plane latency requirements.	Optional
EAS IP replacement information	Contains EAS IP replacement information (i.e. IP addresses and port numbers of source and target EAS).	Optional
Indication for simultaneous connectivity at edge relocation	Indicates request from the AF for temporary simultaneous connectivity over source and target PSA at edge relocation. It may provide AF guidance to determine when the connectivity over the source PSA can be removed.	Optional
Indication of EAS rediscovery.	Indicates the rediscovery of EAS.	Optional
	RAN support information	
UL Maximum Packet Loss Rate	The maximum rate for lost packets that can be tolerated in the uplink direction for the service data flow.	Optional
DL Maximum Packet Loss Rate	The maximum rate for lost packets that can be tolerated in the downlink direction for the service data flow.	Optional
	MA PDU Session Control	
Application descriptors	Identifies the application traffic for which MA PDU Session control is required based on the Steering functionality, the Steering mode, the Steering mode indicator and the Threshold values.	Optional
Steering Functionality	Indicates the applicable traffic steering functionality.	Optional
Steering mode (UL/DL)	Indicates the UL and/or DL traffic distribution rules between the 3GPP and Non-3GPP accesses together with associated parameters (when applicable) for the traffic matching the service data flow.	Optional
Steering mode indicator	Indicates either autonomous load-balance operation or UE-assistance operation, if the steering mode is set to "LOAD_BALANCING".	Optional
Threshold values	Indicates the threshold value(s) for maximum RTT and/or maximum Packet Loss Rate.	Optional

Charging for Non-3GPP access	Indicates parameters used for charging packets carried via Non-3GPP access for a MA PDU Session. The same set of parameters as for the Charging information above applies. If a parameter is not included here, the value provided in the Charging information above applies.	Optional
Usage Monitoring for Non-3GPP access	Indicates parameters used to monitor usage of the packets carried via Non-3GPP access for a MA PDU Session. The same set of parameters as for the Usage Monitoring information above applies. If a parameter is not included here, the value provided in the Usage Monitoring information above applies.	Optional
	IPTV (NOTE 1)	
IP Multicast traffic control information	Indicates whether the service data flow, corresponding to the service data flow template, is allowed or not allowed.	Optional
	QoS Monitoring for URLLC	
QoS parameter(s) to be measured	UL packet delay, DL packet delay or round trip packet delay.	Optional
Reporting frequency	Defines the frequency for the reporting, such as event triggered, periodic, or when the PDU Session is released.	Optional
Target of reporting	Defines the target of the QoS Monitoring reports, it can be either the PCF and/or the AF, decided by the PCF.	Optional
Indication of direct event notification	Indicates that the QoS Monitoring event shall be reported by the UPF directly to the AF or Local NEF indicated by the Target of reporting.	Optional
	Alternative QoS Parameter Sets (NOTE 2)	
Packet Delay Budget	Indicates the packet delay budget in this Alternative QoS Parameter Set.	Optional
Packet Error Rate	Indicates the packet error rate in this Alternative QoS Parameter Set.	Optional
GBR (UL/DL)	The uplink/downlink guaranteed bitrate authorized for the service data flow in this Alternative QoS Parameter Set.	Optional
	TSCAI Input container	
Burst Arrival Time	Indicates the burst arrival time in reference to TSN GM for TSN or external GM for non-TSN applications at ingress port.	Optional
Periodicity	The time period (in reference to TSN GM for TSN or external GM for non-TSN applications) between start of two bursts.	Optional
Flow Direction	Direction of the flow.	Optional
Survival Time	It refers to the time period an application can survive without any burst. It is expressed in reference to the TSN GM for TSN and external GM for non-TSN applications.	Optional
Time Domain	Indicate the (g)PTP domain the (TSN)AF is located in.	Optional
NOTE 1: Only applicable to the 5G-RG connecting to the 5GC via NG-RAN as defined in Annex C. NOTE 2: Only applicable for GBR service data flow with QoS Notification Control enabled. NOTE 3: The parameter "Bind to QoS Flow associated with the default QoS rule and apply PCC rule parameters" defined in table 6.3.1 of 3GPP TS 23.503 [6] is implemented as follows: a default QoS with a GBR type or delay critical GBR type 5QI and a PCC rule bound to the default QoS flow are provisioned as defined in clause 4.2.6.2.1. NOTE 4: The parameter "Indication of exclusion from session level monitoring" defined in table 6.3.1 of 3GPP TS 23.503 [6] is implemented as follows: a PCC rule identifier is included within the "exUsagePccRuleIds" attribute of the UsageMonitoringData instance of PDU session level usage monitoring to indicate that the service data flow shall be excluded from PDU Session usage monitoring as defined in clause 4.2.6.5.3.		

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

4.1.4.2.2 PCC rules operation

For dynamic PCC rules, the following applies:

- Installation: to provision the PCC rules.
- Modification: to modify the PCC rules.
- Removal: to remove the PCC rules.

For predefined PCC rules, the following operations are available:

- Activation: to activate the PCC rules.
- Deactivation: to deactivate the PCC rules.

4.1.4.3 Session rule

4.1.4.3.1 Session rules definition

A session rule consists of policy information elements associated with PDU session. A session rule is dynamically provisioned by the PCF to the SMF (i.e., there are only dynamic session rules). The encoding of the SessionRule data type is defined in clause 5.6.2.7.

A session rule shall include:

- Session Rule Identifer.

A session rule may include:

- Authorized Session-AMBR;
- Authorized Default QoS;
- Reference to Usage Monitoring Data;
- Reference to Usage Monitoring Data for Non-3GPP access of MA PDU session; and
- Reference to Condition Data.

4.1.4.3.2 Session rules operation

For Session rules, the following applies:

- Installation: to provision the session rules.
- Modification: to modify the session rules.
- Removal: to remove the session rules.

4.1.4.4 Policy Decision types

4.1.4.4.1 General

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

The following types of policy decision are defined:

- Traffic control data;
- QoS data;
- Charging data;
- Usage Monitoring data; and
- QoS 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 clause 5.6.2.10.

Traffic control data shall include:

- Traffic Control Data ID.

Traffic control data may include:

- Flow status;
- Redirect Information;
- Mute Notification;
- Traffic Steering Policy ID UL;
- Traffic Steering Policy ID DL;
- Routing requirements;
- UP path change event subscription from the AF;
- Information on User Plane Latency requirements;
- EAS IP replacement information;
- Indication of traffic correlation;
- Indication of simultaneous connectivity temporarily maintained for source and target PSA during edge relocation and guidance about when the connectivity over the source PSA can be removed;
- Access Traffic Steering Functionality;
- Access Traffic Steering Mode DL;
  - Access Traffic Steering Mode; and
  - Optionally, Access Traffic Steering Mode Indicator or Access Traffic Steering Mode Threshold;
- Access Traffic Steering Mode UL; and
  - Access Traffic Steering Mode; and
  - Optionally, Access Traffic Steering Mode Indicator or Access Traffic Steering Mode Threshold;
- Multicast Access Control.

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 clause 5.6.2.8.

QoS data shall include:

- QoS Data ID;

QoS data may include:

- 5QI;
- ARP;
- QNC;
- Maximum Packet Loss Rate UL;
- Maximum Packet Loss Rate DL;
- Maximum Bit Rate UL;

- Maximum Bit Rate DL;
- Guaranteed Bit Rate UL;
- Guaranteed Bit Rate DL;
- 5QI Priority Level;
- Averaging window;
- Maximum Data Burst Volume;
- Bound to default QoS flow indication;
- Resource Sharing Key UL;
- Resource Sharing Key DL;
- Reflective QoS attribute;
- Packet Delay Budget; and
- Packet Error Rate.

NOTE: Either 5QI and ARP combination or Bound to default QoS flow indication is provided.

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 clause 5.6.2.11.

Charging data shall include:

- Charging Data ID;
- Rating Group.

Charging data may include:

- Metering Method;
- Charging Method;
- Service Data flow handling while requesting credit;
- Reporting Level;
- Service ID;
- Sponsor ID;
- Application Service Provider ID; and
- AF Charging ID.

4.1.4.4.5 UsageMonitoring data definition

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

Usage Monitoring Data shall include:

- Usage Monitoring ID.

NOTE: A Usage Monitoring ID corresponds to a valid Monitoring Key.

Usage Monitoring Data may include:

- Volume Threshold;
- Volume Threshold UL;
- Volume Threshold DL;
- Time Threshold;
- Monitoring Time;
- Next Volume Threshold;
- Next Volume Threshold UL;
- Next Volume Threshold DL;
- Next Time Threshold;
- Inactivity Time; and
- PCC rule identifier(s) corresponding to the service data flow(s) which need to be excluded from PDU session level usage monitoring.

4.1.4.4.6 QoS Monitoring data definition

QoS Monitoring data defines QoS Monitoring related parameters (e.g. request QoS monitoring parameters to be measured) associated with a rule. The QoS Monitoring data encoding table is defined in clause 5.6.2.40.

QoS Monitoring data shall include:

- QoS Monitoring Data ID;
- requested QoS monitoring parameters to be measured;
- reporting frequency.

QoS monitoring data may include:

- reporting thresholds;
- wait time;
- reporting period;
- target of reporting; and
- indication of direct event notification.

4.1.5 Policy control request trigger

A policy control request trigger is a condition pre-configured in the SMF (i.e. always report) or provisioned by the PCF to the SMF, which defines when the SMF shall interact again with PCF for further policy decision related to a PDU session.

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

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

When the SMF interacts with the PCF when the condition(s) associated with policy control request triggers are met, the SMF shall send the related attributes that have changed together with the corresponding triggers.

4.1.6 Requested rule data

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

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

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

The encoding of the requested rule data is further specified in clause 5.6.2.24.

When the SMF receives the requested rule data, the SMF shall report the corresponding information to the PCF for the associated PCC rule(s).

4.1.7 Requested usage data

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

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

The encoding of the requested usage data is further specified in clause 5.6.2.25.

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

4.1.8 Condition data

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

Condition data shall include:

- Condition Data ID.

Condition data may include:

- Activation Time;
- Deactivation Time;
- Access Type; and
- RAT Type

NOTE: Access type and RAT type are only applicable to the session rule.

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(s) condition is met.	NF consumer (SMF)
Npcf_SMPolicyControl_UpdateNotify	Update and/or delete PCC rule(s), PDU session related policy context at the SMF and Policy Control Request Trigger(s) 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 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 the creation of a corresponding SM Policy Association with the PCF.
- Provisioning of PCC rules.
- Provisioning of policy control request triggers.
- Provisioning of charging related information for a PDU session.
- Provisioning of revalidation time.
- Policy provisioning and enforcement of authorized AMBR per PDU session.
- Policy provisioning and enforcement of authorized default QoS.
- Provisioning of PCC rule for Application Detection and Control.
- 3GPP PS Data Off Support.
- IMS Emergency Session Support.
- Request Usage Monitoring Control.
- Access Network Charging Identifier report.
- Request for the successful resource allocation notification.
- Provisioning of IP Index Information.
- Negotiation of the QoS flow for IMS signalling.
- PCF resource cleanup.
- Access traffic steering, switching and splitting support.
- DNN Selection Mode Support.
- Detection of the SM Policy Association enabling Time Sensitive Communications and Time Synchronization.
- Support of Dual Connectivity end to end redundant User Plane paths.

- SNPN UE Remote Provisioning support via User Plane.
- Network slice related data rate policy control.
- Request of Presence Reporting Area Change Report.

When the EMDBV feature defined in clause 5.8 is supported by both the PCF and the SMF, the PCF shall use the extMaxDataBurstVol attribute instead of the maxDataBurstVol attribute to signal maximum data burst volume values higher than 4095 Bytes.

When the EMDBV feature is supported by the PCF but not supported by the SMF and the PCF needs to signal maximum data burst volume values higher than 4095 Bytes, the PCF shall use the maxDataBurstVol attribute set to 4095 Bytes.

For values lower than or equal to 4095 Bytes, the PCF shall use the maxDataBurstVol attribute.

NOTE: Maximum data burst volume values are sent by the PCF in responses to the SMF or in an SM Policy Association Update request i.e. after feature negotiation, so the PCF knows whether the SMF supports the EMDBV feature.

4.2.2.2 SM Policy Association establishment

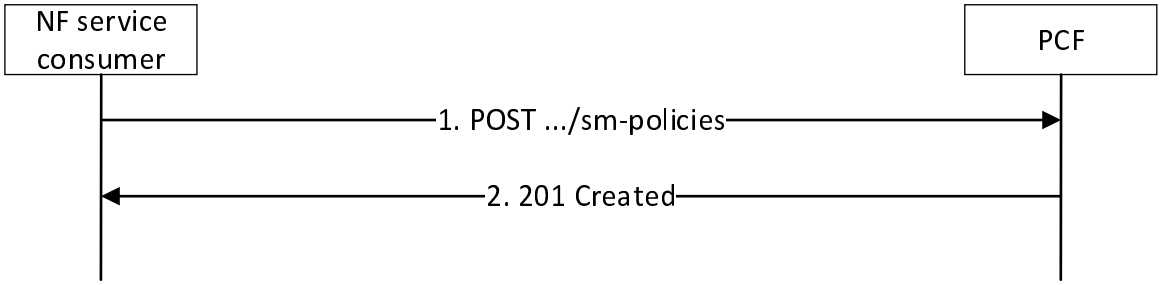

Figure 4.2.2.2-1: SM Policy Association establishment

When the NF service consumer receives the Nsmf_PDUSession_CreateSMContext Request as defined in clause 5.2.2.2 of 3GPP TS 29.502 [22], if the NF service consumer was requested not to interact with the PCF, the NF service consumer shall not interact with the PCF. Otherwise, the NF service consumer shall send an HTTP POST request to the PCF to create an "Individual SM Policy" resource as described in step 1 of figure 4.2.2.2-1.

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

NOTE 2: The indicator to not interact with the PCF is configured in the UDM. It is delivered by the UDM to the NF service consumer within the Charging Characteristics using the Session Management Subscription Data Retrieval service operation as described in 3GPP TS 29.503 [34]. The indicator is operator specific, therefore it can only be used in non-roaming and home routed roaming cases.

The NF service consumer shall include the "SmPolicyContextData" data structure in the payload body of the HTTP POST request in order to request the creation of a representation of the "Individual SM Policy" resource as described below.

The NF service consumer shall include (if available) in the "SmPolicyContextData" data structure:

- SUPI of the user within the "supi" attribute;
- PDU Session Id within the "pduSessionId" attribute;
- DNN within the "dnn" attribute;
- DNN selection mode within the "dnnSelMode" attribute, if the "DNNSelectionMode" feature is supported;
- URL identifying the recipient of SM policies update notifications within the "notificationUri" attribute;

- PDU Session Type within the "pduSessionType" attribute;
- PEI within the "pei" attribute;
- Internal Group Id(s) within the "interGrpIds" attribute;
- type of access within the "accessType" attribute;

NOTE 3: In this Release, for SNPN-enabled UE registered in the SNPN, direct access to the SNPN is specified for 3GPP access only.

- type of the radio access technology within the "ratType" attribute;
- the combination of additional access type and RAT type within the "addAccessInfo" attribute, if the ATSSS feature is supported;
- the UE Ipv4 address within the "ipv4Address" attribute and/or the UE Ipv6 prefix within the "ipv6AddressPrefix" attribute;
- the UE time zone information within the "ueTimeZone" attribute;
- the UDM subscribed Session-AMBR or, if the "DN-Authorization" feature is supported, the DN-AAA authorized Session-AMBR within the "subsSessAmbr" attribute;

NOTE 4: When both, the UDM subscribed Session-AMBR and the DN-AAA authorized Session-AMBR are available in the NF service consumer, the NF service consumer includes the DN-AAA authorized Session-AMBR.

- if the "VPLMN-QoS-Control" feature is supported, the highest Session-AMBR and the default QoS supported in the VPLMN within the "vplmnQos" attribute, if available;

NOTE 5: In home routed roaming, the H-SMF may provide the QoS constraints received from the VPLMN (defined in 3GPP TS 23.502 [3] clause 4.3.2.2.2) to the PCF.

- the DN-AAA authorization profile index within the "authProfIndex" attribute, if the "DN-Authorization" feature is supported;
- subscribed Default QoS Information within the "subsDefQos" attribute;
- the number of supported packet filters for signalled QoS rules within the "numOfPackFilter" attribute;
- the online charging status within the "online" attribute;
- the offline charging status within the "offline" attribute;
- the charging characteristics within the "chargingCharacteristics" attribute;
- the access network charging identifier within the "accNetChId" attribute;
- the address of the network entity performing charging within the "chargEntityAddr" attribute;
- the 3GPP PS data off status within the "3gppPsDataOffStatus" attribute, if the "3GPP-PS-Data-Off" feature is supported;
- indication of UE support of reflective QoS within the "refQosIndication" attribute;
- user location(s) information within the "userLocationInfo" attribute;

NOTE 6: The SMF encodes both 3GPP and non-3GPP access UE location in the "userLocationInfo" attribute when they are both received from the AMF.

- the S-NSSAI corresponding to the network slice to which the PDU session is allocated within the "sliceInfo" attribute;
- the required QoS flow usage for the default QoS flow within the "qosFlowUsage" attribute;
- the MA PDU session indication within the "maPduInd" attribute, if the "ATSSS" feature is supported;

- the ATSSS capability within the "atsssCapab" attribute, if the "ATSSS" feature is supported;

- the identifier of the serving network (the PLMN Identifier or the SNPN Identifier) within the "servingNetwork" attribute;

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

- one or more framed routes within the "ipv4FrameRouteList" attribute for IPv4 and/or one or more framed routes within the "ipv6FrameRouteList" attribute;

NOTE 8: When both, the UDM subscribed framed routes and the DN-AAA authorized framed routes are available in the NF service consumer, the NF service consumer includes the DN-AAA authorized framed routes. If the UDM or DN-AAA updates the framed routes during the lifetime of the PDU Session, the NF service consumer releases the PDU Session as defined in clause 4.2.5.2.

- the serving network function identifier within the "servNfId" attribute;

- when the "PvsSupport" feature is supported, the onboarding indication within the "onboardInd" attribute and the Provisioning Server address(es) within the "pvsInfo" attribute;

- when the "SatBackhaulCategoryChg" feature is supported, the satellite backhaul category within the "satBackhaulCategory" attribute;

NOTE 9: When the "satBackhaulCategory" attribute is not present, non-satellite backhaul applies.

- when the "AMInfluence" feature is supported, the PCF for the UE callback URI and, if received, SBA binding information within the "pcfUeInfo" attribute;

- trace control and configuration parameters information within the "traceReq" attribute; and

- when the "EneNA" feature is supported, the list of NWDAF instance IDs used for the PDU Session within the "nwdafInstanceId" and their associated Analytic ID(s) within "nwdafEvents" consumed by the NF service consumer, included within the "nwdafDatas" attribute.

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

NOTE 10: The "ipDomain" attribute is helpful when within a network slice, there are several separate IP address domains, with SMF/UPF(s) that allocate Ipv4 IP addresses out of the same private address range to UE PDU Sessions. The same IP address can thus be allocated to UE PDU sessions served by SMF/UPFs in different IPv4 address domains. If one PCF controls several SMF/UPFs in different IP address domains, the UE IP address is thus not sufficient for the AF session binding procedure, as described in 3GPP TS 29.514 [17]. The SMF assists the PCF in the session binding supplying an "ipDomain" attribute denoting the IPv4 address domain identity of the allocated UE IPv4 address.

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

- a Location header field containing the URI of the created resource; and

- a response body providing the session management related policies, e.g. provisioning of PCC rules as defined in clause 4.2.6.2, provisioning of policy control request triggers as defined in clause 4.2.6.4.

The NF service consumer shall use the URI received in the Location header in subsequent requests to the PCF to refer to the created "Individual SM Policy" resource.

If the PCF received the list of NWDAF instance IDs used for the PDU Session in "nwdafInstanceId" attribute and their associated Analytic IDs in "nwdafEvents" attribute included within the "nwdafDatas" attribute the PCF may select those NWDAF instances as described in 3GPP TS 29.513 [7].

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

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

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

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

If the NF service consumer receives an HTTP response with the above error codes, the NF service consumer shall reject the PDU session establishment procedure that initiated the HTTP POST Request.

If the PCF, based on local configuration and/or operator policies, denies the creation of the Individual SM Policy resource, the PCF may reject the request with in an HTTP "403 Forbidden" response message including the "cause" attribute of the ProblemDetails data structure set to "POLICY_CONTEXT_DENIED". At reception of this error code and based on configured failure actions, the NF service consumer may reject or allow, by applying local policies, the PDU session establishment.

If the "SamePcf" feature as defined in clause 5.8 is supported, when the PCF determines that the same PCF shall be selected for the SM Policy associations to the same UE ID, S-NSSAI and DNN combination in the non-roaming or home-routed scenario and there is no SM Policy association for the UE ID, S-NSSAI and DNN combination, the PCF, after determining whether the BSF supports the "SamePcf" or the "ExtendedSamePcf" feature as described in 3GPP TS 29.521 [39], shall request the BSF to check if there is an existing PCF binding information for the same UE ID, S-NSSAI and DNN combination registered by other PCF(s) as defined in clause 4.2.2.2 of 3GPP TS 29.521 [39]. If the PCF receives the from the BSF "403 Forbidden" status code with the "cause" attribute of the ProblemDetails data structure set to "EXISTING_BINDING_INFO_FOUND" and the FQDN or description of IP endpoints of the Npcf_SMPolicyControl service of the existing PCF (i.e. that handles SM Policy association(s) to the same UE ID, S-NSSAI and DNN combination) within the "pcfSmFqdn" attribute or the "pcfSmIpEndPoints" attribute of the BindingResp data structure respectively as defined in clause 4.2.2.2 of 3GPP TS 29.521 [39], the PCF shall reply to the SMF with an HTTP "308 Permanent Redirect" error response and the Location header containing a URI as defined in clause 5.3.2.2, with the FQDN or IP endpoint of this PCF's Npcf_SMPolicyControl service as {apiRoot}. Upon reception of the response, the NF service consumer shall initiate a new HTTP POST request based on the returned URI.

The forwarding of the Origination Time Stamp parameter shall apply as described hereafter, if the NF service consumer supports the detection and handling of late arriving requests as specified in clause 5.2.3.3 of 3GPP TS 29.502 [22] and the procedure is enabled by the operator. If the NF service consumer receives a request to create an SM Context or a PDU session context, which includes the 3gpp-Sbi-Origination-Timestamp header as defined in clause 5.2.3.2, the NF service consumer shall forward this header to the PCF as HTTP custom header. See also clause 4.2.7 for the handling at the PCF, when the PCF receives the 3gpp-Sbi-Origination-Timestamp header.

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 SMF with the charging information, i.e. the CHF address(es), and if available, the associated CHF instance ID(s) and CHF set ID(s), during the initial interaction with the SMF defining the charging function respectively based on the operator policy. In this case, the PCF may retrieve the CHF addresses, and if available, the associated CHF instance ID(s) and CHF set ID(s) as follows:

- The PCF receives it from the UDR as part of the Policy Data Subscription information, as defined in clause 5.2.10 of 3GPP TS 29.519 [15].
- It is locally configured in the PCF based on operator policies.
- The PCF discovers it by interacting with the NRF, as described in clause 6.1 of 3GPP TS 32.290 [30].

In order to provision the CHF information to the SMF, the PCF shall include the "chargingInfo" attribute containing the charging information within the SmPolicyDecision data structure.

Within the ChargingInformation data structure, both the primary CHF address, within the "primaryChfAddress" attribute, and secondary CHF address, within the "secondaryChfAddress" attribute, shall be provided simultaneously when the feature "CHFsetSupport" is not supported. When the feature "CHFsetSupport" is supported, the PCF shall include the "secondaryChfAddress" attribute if available (i.e. if previously retrieved from the UDR, locally configured in the PCF or discovered from the NRF).

When the CHF supports redundancy based on NF Set concepts as described in 3GPP TS 29.500 [4], the required charging information consists of CHF address, encoded within the"primaryChfAddress" attribute, CHF instance, encoded within the "primaryChfInstanceId" attribute, and primary CHF set id, encoded within the "primaryChfSetId". The CHF set information may be also complemented by secondary CHF address, encoded within the "secondaryChfAddress", for backwards compatibility purposes with the primary/secondary redundancy mechanism.These shall overwrite any predefined CHF addresses and associated CHF instance ID and CHF set ID at the SMF.

NOTE: When the feature "CHFsetSupport" is supported by the NF service consumer, it indicates the NF service consumer supports CHF redundancy based on NF Set concepts as described in 3GPP TS 29.500 [4], clause 6.5.3.

Provisioning charging information without PCC rules for charged service data flows shall not be considered as an error, since such PCC rules may be provided later. If the PCF has provided the charging information within the SmPolicyDecision data structure during the initial interaction with the SMF, the PCF shall not modify the charging information in subsequent interactions.

If no charging information is provisioned by the PCF, the SMF shall use the charging information obtained via one of the following procedures, with the precedence order highest to lowest (see 3GPP TS 32.255 [35], clause 5.1.8):

1. UDM provided charging characteristics.
2. NRF based discovery.
3. SMF locally configured charging characteristics.

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 within which the charging method is omitted, i.e. either both the "online" and the "offline" attributes are not provided or only one of them is provided and set to "false" within the ChargingData data structure to which the PCC rule refers. The SMF may have a pre-configured default charging method.

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

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

When the "OfflineChOnly" feature is supported, the PCF may include the "PDU Session with offline charging only" indication as specified in clause 4.2.2.3.3.

NOTE: It is possible that there is no default charging method applied to a PDU session.

4.2.2.3.3 Provisioning of the "PDU Session with offline charging only" indication

If the "OfflineChOnly" feature, specified in clause 5.8, is supported, the PCF may provide in the response to the received HTTP POST message from the SMF the "PDU Session with offline charging only" indication, within the "offlineChOnly" attribute, to signal that the online charging method shall never be configured for any of the PCC Rules activated during the lifetime of the PDU Session, nor provided as the Default Charging Method, as specified in clause 6.4 of 3GPP TS 23.503.

If the "OfflineChOnly" feature, specified in clause 5.8, is supported and the PCF includes the "PDU Session with offline charging only" indication set to "true" in the "offlineChOnly" attribute within the SmPolicyDecision data structure, then the default charging method for the PDU session is offline charging, and the "online" attribute and the "offline" attribute shall not be provisioned by the PCF within the SmPolicyDecision data structure.

NOTE: If the PCF includes the "PDU Session with offline charging only" indication set to "true" in the "offlineChOnly" attribute within the SmPolicyDecision data structure, and the "online" attribute and the "offline" attribute are also provisioned by the PCF within the SmPolicyDecision data structure, then the SMF could ignore the values of the "online" attribute and the "offline" attribute.

4.2.2.4 Provisioning of revalidation time

The PCF may provide within the SmPolicyDecision data structure 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 an interaction with the PCF to request PCC rule(s).

The SMF shall start the timer based on the revalidation time and shall trigger a PCC rule request towards the PCF before the indicated revalidation time.

4.2.2.5 Policy provisioning and enforcement of authorized AMBR per PDU session

The SMF shall, if available include either the UDM subscribed Session-AMBR or, if the "DN-Authorization" feature is supported, the DN-AAA authorized Session-AMBR per PDU session within the "subsSessAmbr" attribute in the SmPolicyContextData data structure, as defined in clause 4.2.2.2. When both the UDM subscribed Session-AMBR and the DN-AAA authorized Session-AMBR are available in the SMF, the DN-AAA authorized Session-AMBR shall take precedence over the UDM subscribed Session-AMBR.

In home routed roaming, and if the "VPLMN-QoS-Control" feature is supported, the SMF shall provide the Session-AMBR constraints received from the VPLMN, if available, within the "vplmnQos" attribute.

The PCF shall authorize the Session-AMBR based on the operator's policy and, in the home routed scenario, shall ensure that the authorized Session-AMBR value does not exceed the Session-AMBR value provided by the VPLMN, if available.

NOTE: If the SMF does not provide the Session-AMBR constraints in the VPLMN to the PCF, the PCF considers that no Session-AMBR constrains apply unless operator policies define any.

When network slice data rate policy control applies, the PCF shall authorize the Session-AMBR as described in clause 4.2.6.8.

The PCF shall provision the authorized Session-AMBR to the SMF in the response to the received HTTP POST message, as defined in clauses 4.2.6.3.1 and 4.2.6.3.2.

Upon reception of the authorized Session-AMBR from the PCF, the SMF shall apply the corresponding procedures towards the access network, the UE and the UPF for the enforcement of the Session-AMBR for the concerned PDU session.

4.2.2.6 Policy provisioning and enforcement of authorized default QoS

During PDU session establishment, as defined in clause 4.2.2.2, the SMF shall, if available, include the subscribed default QoS within the "subsDefQos" attribute.

In home routed roaming, and if the "VPLMN-QoS-Control" feature is supported, the SMF shall provide the default QoS constraints received from the VPLMN, if available, within the "vplmnQos" attribute.

The PCF shall authorize the default QoS based on the operator's policy and, in the home routed scenario, shall ensure that the authorized default QoS contains a 5QI and ARP value, and MBR/GBR value, if applicable, supported by the VPLMN, if available.

NOTE 1: If the SMF does not provide the default QoS constraints in the VPLMN to the PCF, the PCF considers that no default QoS constrains apply unless operator policies define any.

The PCF shall provision the authorized default QoS to the SMF in the response to the received HTTP POST message, as defined in clauses 4.2.6.3.1 and 4.2.6.3.2.

Upon reception of 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 this enforcement of the authorized default QoS for the concerned PDU session.

NOTE 2: If dynamic PCC is not deployed, the SMF can have a DNN based configuration to enable the establishment of a GBR resource type default QoS flow. This configuration contains a standardized GBR 5QI as well as GFBR and MFBR for UL and DL.

NOTE 3: GBR resource type is not applicable to the default QoS flow of a PDU session that is interworking with EPS.

4.2.2.7 Provisioning of PCC rule for Application Detection and Control

If the ADC feature is supported, and the user subscription indicates that application detection and control is required, the PCF may provision PCC rule(s) for application detection and control as defined in clause 4.2.6.2.11 in the response message to the received HTTP POST request from the SMF.

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

4.2.2.8 3GPP PS Data Off Support

When the 3GPP-PS-Data-Off feature, as defined in clause 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 establishment of a PDU session over 3GPP access and/or non-3GPP access, it shall include the "3gppPsDataOffStatus" attribute set to true within the SmPolicyContextData data structure in the HTTP POST message that it sends to the PCF, as defined in clause 4.2.2.2.

If the PCF receives that HTTP POST message with a SmPolicyContextData data structure containing a "3gppPsDataOffStatus" attribute set to true as above and the "accessType" attribute indicating "3GPP_ACCESS", the PCF shall configure the SMF to block any downlink and optionally uplink IP flows that are not related to a service contained in the list of 3GPP PS Data Off Exempt Services, e.g. by not installing any related dynamic PCC rule(s) or by not activating the related predefined PCC rule(s) such as PCC rule(s) with wild-carded service data flow filters. The PCF may also, subject to its normal policies, provide the PCC rule(s) for the service(s) included in the list of 3GPP PS Data Off Exempt Services, as defined in clause 4.2.6.2.1.

The PCF shall subscribe to the "AC_TY_CH" policy control request trigger with the SMF, as defined in clause 4.2.6.4, in order to support this feature, if the PCF determines that the UE is allowed to access the network via non-3GPP access.

NOTE 1: The PCF can be configured with a list of 3GPP PS Data Off Exempt Services per DNN and S-NSSAI. The list of 3GPP PS Data Off Exempt Services for an DNN and S-NSSAI can also be empty, or can allow for any service within that DNN and S-NSSAI, 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 in 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 active, e.g. by treating any service within a well-known IMS DNN as part of the 3GPP PS Data Off Exempt Services.

NOTE 3: The packets transferred over non-3GPP access are unaffected by the 3GPP PS Data Off functionality.

If the "ATSSS" feature, as defined in clause 5.8 is supported, and the PCF receives in the SmPolicyContextData data structure the "maPduInd" attribute, the "3gppPsDataOffStatus" attribute set to true and the"accessType" attribute or the "addAccInfo" attribute set to "3GPP_ACCESS", the PCF shall configure the SMF in such a way that:

- packets for services belonging to the 3GPP PS Data Off Exempt services are forwarded over 3GPP access and non-3GPP access as indicated by the policy for ATSSS Control, as specified in clause 4.2.6.2.17; and

- for downlink and optionally uplink flows not related to a service contained in the list of 3GPP PS Data Off Exempt services, the PCF may configure the SMF to handle the associated traffic only via non-3GPP access, if available, by providing the corresponding ATSSS policy within the related PCC rule, as specified in clause 4.2.6.2.17.

4.2.2.9 IMS Emergency Session Support

A SMF that requests PCC Rules at PDU Session Establishment for an IMS emergency session in a PLMN or an SNPN shall send an HTTP POST message to the PCF, as defined in clause 4.2.2.2, including the "dnn" attribute containing the Emergency DNN. The SMF may include the SUPI, within the "supi" attribute, and if the SUPI is not available or unauthenticated, the SMF shall include the PEI, within the "pei" attribute, the "invalidSupi" attribute set to "true" and an implementation specific value within the "supi" attribute. The SMF may include the rest of the attributes described in clause 4.2.2.2. The SMF may also include the GPSI, if available, within the "gpsi" attribute.

NOTE: IMS Emergency services are not supported for SNPN when the UE accesses the SNPN over NWu via a PLMN.

The PCF shall detect that a PDU session is restricted to IMS Emergency services when the "dnn" attribute included in the HTTP POST message received from the SMF includes a data network identifier that matches one of the Emergency DNs from the configurable list. The PCF does not perform in this case subscription check procedures with UDR; it uses instead the locally configured operator policies to make authorization and policy decisions. The PCF:

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

- may provision the authorized QoS that applies to the default QoS flow in the response message to the SMF within the "authDefQos" attribute of a session rule according to the procedures described in clause 4.2.3.6, except for obtaining the authorized QoS upon interaction with the UDR. The value of the "priorityLevel" attribute included within the "arp" 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 set to "3GPP_ACCESS", the values of the "preemptCap" and the "preemptVuln" attributes included within the "arp" attribute shall be assigned as required by local operator policies,

- may provision the authorized Session-AMBR in the response message to the SMF, according to the procedures described in clause 4.2.3.5.

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

4.2.2.10 Request Usage Monitoring Control

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

4.2.2.11 Access Network Charging Identifier report

During the PDU session establishment procedure, if the Access Network Charging Identifier is within the Uint32 value range, the SMF may provide the access network charging identifier information within the "accNetChId" attribute of the SmPolicyContextData data structure if this Access Network Charging Identifier applies to the whole PDU session. In this case, within the associated AccNetChId data structure, the SMF shall include the "accNetChaIdValue" attribute containing the Access Network Charging Identifier for the default QoS flow and the "sessionChScope" attribute set to true. The SMF may provide the address of the network entity performing the charging functionality within the "chargEntityAddr" attribute.

If the "AccNetChargId_String" feature is supported by the SMF, and the Access Network Charging Identifier value is longer than Uint32:

- if the SMF doesn’t know if the PCF supports the "AccNetChargId_String" feature, the SMF shall not provide the access network charging identifier information;

- if the SMF knows the PCF supports the feature "AccNetChargId_String", the SMF shall encode the access network charging identifier within "accNetChargIdString" attribute.

NOTE: During the PDU Session Establishment procedure, the "refPccRuleIds" attribute is not provided within the AccNetChId data structure, regardless of whether the charging identifier applies to the entire PDU session or to the default QoS flow, since the PCC Rules are not yet authorized at this stage.

4.2.2.12 Request for the successful resource allocation notification

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

4.2.2.13 Request of Presence Reporting Area Change Report

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

4.2.2.14 Provisioning of IP Index Information

If the PDU session type received within the "pduSessiontype" attribute is "IPV4" or "IPV6" or "IPV4V6", and no corresponding IP address/prefix is received, the PCF may include within the SmPolicyDecision data structure the IP index information within the "ipv4Index" attribute, for IPv4 address allocation, and/or the "ipv6Index" attribute, for IPv6 address allocation, based on the user's subscription information retrieved from the UDR and operator's policy.

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

4.2.2.15 Negotiation of the QoS flow for IMS signalling

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

If during PDU session establishment procedure, the SMF includes the "IMS_SIG" value within the "qosFlowUsage" attribute and the PCF accepts that default QoS flow is dedicated to IMS signalling, the PCF shall within the SmPolicyDecision data structure include the "IMS_SIG" value within the "qosFlowUsage" attribute. In this case, the PCF shall restrict the QoS flow to only be used for IMS signalling as specified in 3GPP TS 23.228 [16] by applying the applicable 5QI for IMS signalling.

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

4.2.2.16 PCF resource cleanup

In the Npcf_SMPolicyControl_Create service operation, the SMF as NF service consumer may provide SMF Id in "smfId" attribute and recovery timestamp in "recoveryTime" attribute. The PCF may use the "smfId" attribute to supervise the status of the SMF as described in clause 5.2 of 3GPP TS 29.510 [29] and perform necessary cleanup upon status change of the SMF later, and/or both the "smfId" attribute and the "recoveryTime" attribute in cleanup procedure as described in clause 6.4 of 3GPP TS 23.527 [33].

4.2.2.17 Access traffic steering, switching and splitting support

If the SMF supports the "ATSSS" feature defined in clause 5.8, the SMF shall within the SmPolicyContextData data structure include the ATSSS capability within the "atsssCapab" attribute and the MA PDU session Indication within the "maPduInd" attribute as defined in clause 4.2.2.2.

The SMF determines the ATSSS capability supported for the MA PDU Session based on the ATSSS capabilities provided by the UE and per DNN configuration on SMF, as follows:

- If the SMF receives the UE's ATSSS capabilities "MPTCP functionality with any steering mode and ATSSS-LL functionality with only Active-Standby steering mode" and;
  - if the DNN configuration allows both MPTCP and ATSSS-LL with any steering mode, including RTT measurement without using PMF protocol, the SMF shall set the "atsssCapab" attribute to the value "MPTCP_ATSSS_LL_WITH_ASMODE_UL", or;

- if the DNN configuration allows both MPTCP and ATSSS-LL with any steering mode, including RTT measurement without using PMF protocol, but the UPF does not support the RTT measurement without using PMF protocol, the SMF shall set the "atsssCapab" attribute to the value "MPTCP_ATSSS_LL_WITH_EXSDMODE_DL_ASMODE_UL".

- if the DNN configuration allows MPTCP with any steering mode and ATSSS-LL with only Active-Standby steering mode, the SMF shall set the "atsssCapab" attribute to the value "MPTCP_ATSSS_LL_WITH_ASMODE_DLUL".

- If the SMF receives the UE's ATSSS capabilities "ATSSS-LL functionality with any steering mode" and the DNN configuration allows ATSSS-LL with any steering mode, the SMF shall set the "atsssCapab" attribute to the value "ATSSS_LL".

- If the SMF receives the UE's ATSSS capabilities "MPTCP functionality with any steering mode and ATSSS-LL functionality with any steering mode", and the DNN configuration allows both MPTCP and ATSSS-LL with any steering mode, the SMF shall set the "atsssCapab" attribute to the value "MPTCP_ATSSS_LL".

If the SMF receives the MA PDU Request Indication from the UE and the SMF determines that the MA PDU session is allowed based on the Session Management subscription data retrieved from the UDM and the operator policy, the SMF shall include the "MA_PDU_REQUEST" within the "maPduInd" attribute; otherwise if the SMF receives the MA PDU Network-Upgrade Allowed indication from the UE and the SMF determines that the MA PDU session is allowed based on the Session Management subscription data retrieved from the UDM and the operator policy, the SMF shall include the "MA_PDU_NETWORK_UPGRADE_ALLOWED" within the "maPduInd" attribute.

If the PCF supports the "ATSSS" feature, the PCF may provide PCC rules and/or session rules of ATSSS policy for the MA PDU session as defined in clause 4.2.6.2.17 and clause 4.2.6.3.4; otherwise the PCF shall not provide any PCC rules and/or session rules of ATSSS policy.

4.2.2.18 DNN Selection Mode Support

If the SMF supports the "DNNSelectionMode" feature defined in clause 5.8, when the SMF receives from the AMF the DNN selection mode, the SMF shall send an HTTP POST message as defined in clause 4.2.2.2 and shall include the received information in the "dnnSelMode" attribute.

The "dnnSelMode" attribute indicates whether the DNN suplied in the "dnn" attribute is an explicitly subscribed DNN and thus verified by the network against UDM subscription (regardless of whether it was originally provided by the UE or replaced by the network), or if it is a non-subscribed DNN (and provided by the UE, or replaced by the network).

If the PCF supports the "DNNSelectionMode" feature, when the "dnnSelMode" attribute indicates:

- the DNN is not explicitly subscribed, the PCF may provision PCC rules and Session rules according to the PCF local configuration for the UE provided and/or network provided non-subscribed DNN;

- the DNN is explicitly subscribed and verified by the network against UDM subscription, the PCF proceeds according to existing specified procedures.

4.2.2.19 Detection of the SM Policy Association enabling Time Sensitive Communications and Time Synchronization

When the feature "TimeSensitiveNetworking" or "TimeSensitiveCommunication" is supported, the PCF detects if the Npcf_SMPolicyControl_Create request relates to SM Policy Association enabling Time Sensitive Communications and Time Synchronization based on the received DNN and S-NSSAI. The PCF then may provide within the SmPolicyDecision data structure the "TSN_BRIDGE_INFO" policy control request trigger within the "policyCtrlReqTriggers" attribute to instruct the SMF to trigger a PCF interaction when the trigger is met; i.e., new TSC user plane node information is available.

NOTE: Time sensitive communication and time synchronization are not supported in home-routed roaming scenarios.

4.2.2.20 Support of Dual Connectivity end to end redundant User Plane paths

Upon the initial interaction with the PCF, if the "Dual-Connectivity-redundant-UP-paths" feature is supported, the PCF shall determine, based on operator's policy (e.g. when some of the allowed services require redundancy), whether the PDU session is a redundant one.

When the PCF determines that the PDU session is a redundant PDU session, the PCF shall provision the "redSessIndication" attribute set to true within the SmPolicyDecisionData returned in the response to the HTTP POST request.Upon receiving the indication from the PCF that the PDU session is a redundant PDU session, the SMF shall apply the corresponding procedures towards the access network and the UPF for the establishment of the redundant user plane paths as defined in clause 5.33.2.1 of 3GPP TS 23.501 [2].

The PCF shall not modify during the PDU session lifetime the indication of whether the redundant user plane paths are allowed for the PDU session.

4.2.2.21 User Plane Remote Provisioning of UE SNPN Credentials in Onboarding Network

User Plane Remote Provisioning of UEs SNPN Credentials when in Onboarding Network is provided through a DNN and S-NSSAI used for onboarding.

When the "PvsSupport" feature is supported, the PCF may make authorization and policy decisions to restrict the use of the PDU Session established to the DNN and S-NSSAI used for onboarding in a ON-SNPN, e.g., by restricting the traffic to/from Provisioning Server address(es) and DNS server address(es) only.

When the Onboarding Network is a ON-SNPN, during the PDU session establishment procedure related to a PDU session for used for User Plane Remote Provisioning, the SMF shall include the indication that the PDU session is used for onboarding with the "onboardInd" attribute set to true and provide within "pvsInfo" attribute, if available, the information related to the Provisioning Server(s) that provisions the UE with credentials and other data to enable SNPN access.

If the "onboardInd" attribute set to true is received during the SM policy association establishment and the combination of the received DNN within "dnn" attribute and the S-NSSAI within "sliceInfo" attribute corresponds to a PDU session used for User Plane Remote Provisioning, the PCF shall omit the subscription data check with UDR. Instead, the PCF shall use the locally stored Onboarding Configuration Data for this DNN and S-NSSAI combination to make authorization and policy decisions.

If the "pvsInfo" attribute with the Provisioning Server(s) information is received in the request, the PCF shall use the received information to create the service data flow template of the Provisioning Server(s) in the derived PCC Rule(s). If the "pvsInfo" attribute is not received, the PCF shall construct this service data flow template(s) based on the local configuration stored as part of the Onboarding Configuration Data. In addition, the PCF may create service data flow templates for the DNS server address(es) stored as part of the Onboarding Configuration Data. The "pvsInfo" attribute provided by the SMF may include, for each provided Provsioning Server, the Provisioning Server IP address(es) and/or FQDN(s).

NOTE 1: How the PCF resolves a Provisioning Server FQDN to an IP address or IP address range with other mechanism than local configuration in the Onboarding Configuration Data is not specified in this release of the specification

The PCF shall select the QoS information of the PCC rule(s) applicable to the User Plane Remote Provisioning service based on policies locally configured at the PCF as part of the Onboarding Configuration Data.

The PCF shall install the derived PCC Rule(s) in the response. The installed PCC Rule(s) shall take precedence over the locally stored PCC Rule(s) in the SMF.

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

NOTE 2: When the Onboarding Network is a PLMN or a SNPN, the SMF does not provide the "onboardInd" attribute and the "pvsInfo" attribute. The PCF retrieves policy control subscription profile for this SUPI, DNN, S-NSSAI from UDR, that includes the list of allowed services. If the list of allowed services includes both PVS and DNS services, then the PCF, based on local policies, determines the PVS and DNS address(es) to be used in the SDF template of the PCC Rule(s) and allows traffic to/from these destinations as per currently specified procedures.

4.2.2.22 Network slice related data rate policy control

When an Npcf_SMPolicyControl_Create request is received, the PCF may check if the S-NSSAI to which the received request relates is subject to network slice data rate policy control. If it is the case, the PCF shall apply network slice data rate control as described in clause 4.2.6.8.

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 terminate operations.

The following procedures using the Npcf_SMPolicyControl_UpdateNotify service operation are supported:

- PCF initiated update of the policies associated with a PDU session.
- PCF initiated deletion of the SM Policy Association of a PDU session.
- Provisioning of PCC rules.
- Provisioning of policy control request triggers.
- Provisioning of revalidation time.
- Policy provisioning and enforcement of the authorized AMBR per PDU session.
- Policy provisioning and enforcement of the authorized default QoS.
- Provisioning of PCC rules for Application Detection and Control.
- 3GPP PS Data Off Support.
- IMS Emergency Session Support.
- Request Access Network Information.
- Request Usage Monitoring Control.
- Request for the result of PCC rule removal.
- Access Network Charging Identifier request.
- Request successful resource allocation notifications.
- IMS Restoration Support.
- P-CSCF Restoration Enhancement Support.
- Access traffic steering, switching and splitting support.
- Policy provisioning and enforcement of AF session with required QoS.
- Forwarding of TSC user plane node management information and port management information received from the TSN AF or TSCTSF.
- Provisioning of TSCAI input information and TSC QoS related data.
- Policy provisioning of QoS Monitoring to assist URLLC Service.
- Policy decision and condition data error handling.
- Network slice related data rate policy control.
- Request of Presence Reporting Area Change Report.

- PCC Rule Error Report.
- Session Rule Error Report.

4.2.3.2 SM Policy Association Update request

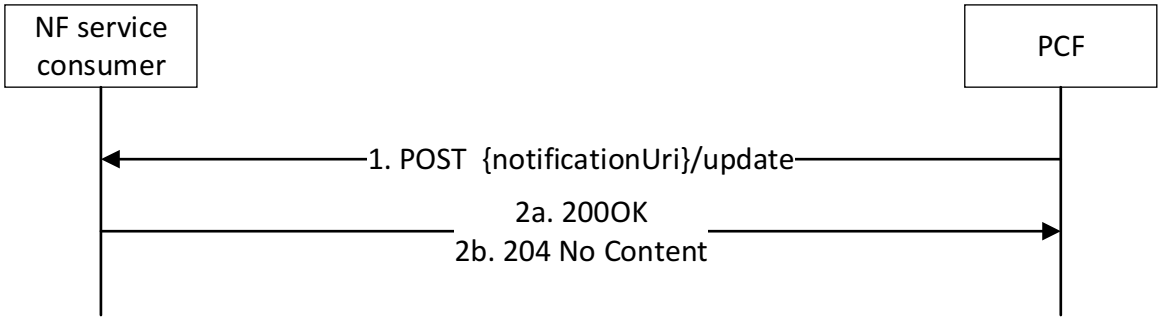

Figure 4.2.3.2-1: SM Policy Association Update request

The PCF may decide to provision policies related to an Individual SM Policy resource without obtaining a request from the NF service consumer, e.g. in response to information provided to the PCF via the Rx or N5 reference points, or in response to an internal trigger within the PCF. The PCF shall send for this purpose a POST request to the NF service consumer (e.g. SMF) using the URI"{notificationUri}/update". The payload body of the message shall contain a SmPolicyNotification data structure that contains:

- the representation of the updated policies within the "smPolicyDecision" attribute; and
- the resource URI of the Individual SM Policy resource related to the notification within the "resourceUri" attribute.

Detailed procedures related to the provisioning and enforcement of the policy decisions contained within the SmPolicyDecision data structure are provided in clause 4.2.6.

In case of a successful update of SM policies:

- if the PCF provisioned the policy control request triggers related to access type change, RAT change or location change, a "200 OK" response code and a response body with the corresponding available information in the "UeCampingRep" data structure shall be returned in the response;
- otherwise, a "204 No Content" response code shall be returned in the response.

NOTE: When there is an ongoing procedure that collisions with the update of SM policies (e.g. during handover from 5GS to EPS) the SMF, based on operator policies, can delay the update of SM policies and return a "204 No Content" response code. In this case the SMF will process the request when the procedure is finished.

If errors occur when processing the HTTP POST request, the NF service consumer shall send an HTTP error response as specified in clause 5.7.

If the feature "ES3XX" is supported, and the NF service consumer determines the received HTTP POST request needs to be redirected, the NF service consumer shall send an HTTP redirect response as specified in clause 6.10.9 of 3GPP TS 29.500 [4].

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

If the "SessionRuleErrorHandling" feature is supported and the NF service consumer received one or more PCC rules and/or session rules from the PCF but the validation of all these PCC Rules and/or session rules was unsuccessful, the NF service consumer shall reject the request and include in an HTTP "400 Bad Request" response message the ErrorReport data structure. Within the ErrorReport data structure, the NF service consumer shall include the "error" attribute containing the "cause" attribute of the ProblemDetails data structure set to "RULE_PERMANENT_ERROR" or "RULE_TEMPORARY_ERROR" and the "ruleReports" attribute to report the PCC rule status of the affected PCC rules as defined in clause 4.2.3.16 and/or the "sessRuleReports" attribute to report the session rule status of the affected session rules as defined in clause 4.2.3.20.

If the NF service consumer received one or more PCC rules from the PCF but the validation of some of them was unsuccessful, the NF service consumer shall include an HTTP "200 OK" status code together with one or more RuleReport data structure(s) to report the PCC rule status of the affected PCC rules as defined in clause 4.2.3.16 in the "PartialSuccessReport" data structure included in the response message. The "failureCause" attribute of the "PartialSuccessReport" shall be set to "PCC_RULE_EVENT" or "PCC_QOS_FLOW_EVENT".

If the "SessionRuleErrorHandling" feature is supported and the NF service consumer received one or more PCC rule and/or session rules from the PCF but the validation of some of them was unsuccessful, the NF service consumer shall include an HTTP "200 OK" status code together with the "ruleReports" attribute to report the PCC rule status of the affected PCC rules as defined in clause 4.2.3.16 and/or the "sessRuleReports" attribute to report the session rule status of the affected session rules as defined in clause 4.2.3.20 in the "PartialSuccessReport" data structure included in the response message. The "failureCause" attribute of the "PartialSuccessReport" shall be set to "RULE_PERMANENT_ERROR" or "RULE_TEMPORARY_ERROR".

If the PCF provisioned policy control request triggers, the NF service consumer may include in the "PartialSuccessReport" data structure the "ueCampingRep" attribute with the corresponding available information. When it is required to report multiple instances of the "PartialSuccessReport" data structure due to different "failureCause" values, the NF service consumer shall use only one instance of the "PartialSuccessReport" data structure to include the "ueCampingRep" attribute with the corresponding available information.

4.2.3.3 SM Policy Association termination request

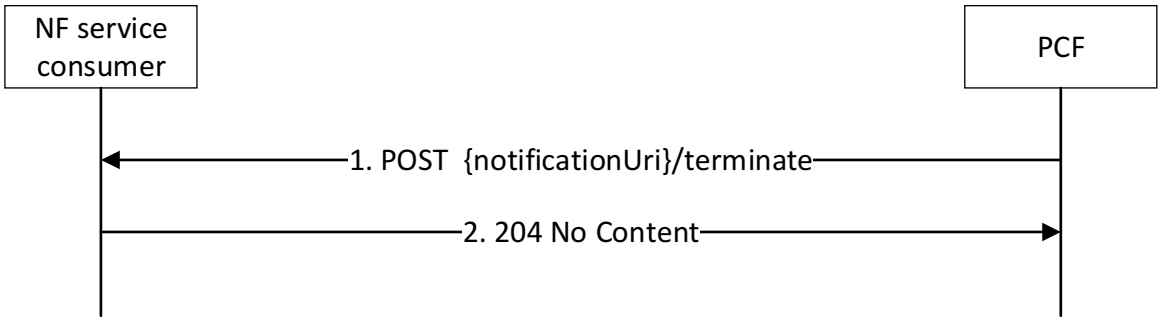

Figure 4.2.3.3-1: SM Policy Association termination request

The PCF may request PDU session termination and the corresponding deletion of the Individual SM policy resource in the following circumstances:

- If the PCF decides to terminate a PDU session due to an internal trigger or a trigger from the UDR.
- The PCF may also decide to terminate a PDU session upon receiving a POST message from the NF service consumer (e.g. when data usage quota is reached).

The PCF shall send a POST request to the NF service consumer (e.g. SMF) using the URI {notificationUri}/terminate and include the TerminationNotification data structure in the body of the HTTP POST request. Within the TerminationNotification data structure, the PCF shall include:

- the resource URI of the Individual SM policy resource related to the termination request within the "resourceUri" attribute; and
- the cause of why the PCF requests the termination of the policy association within the "cause" attribute.

If the NF service consumer accepts the received POST request, the NF service consumer shall send a "204 No Content" response.

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

If errors occur when processing the HTTP POST request, the NF service consumer shall send an HTTP error response as specified in clause 5.7.

If the feature "ES3XX" is supported, and the NF service consumer determines the received HTTP POST request needs to be redirected, the NF service consumer shall send an HTTP redirect response as specified in clause 6.10.9 of 3GPP TS 29.500 [4].

4.2.3.4 Provisioning of revalidation time

During the lifetime of a 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 an interaction with the PCF to request PCC rule(s) 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 the "RE_TIMEOUT" policy control request trigger, if it has been previously provided.

When the SMF receives the revalidation time within the "revalidationTime" attribute, the SMF shall store the received value and start the associated timer based on it. Then, the SMF shall trigger a PCC rule request towards the PCF before the indicated revalidation time.

If the "RE_TIMEOUT" policy control request trigger is removed, the SMF shall stop the associated timer.

NOTE: By disabling the revalidation function, the revalidation time value previously provided to the SMF is not applicable anymore.

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 defined in clause 4.2.3.2.

If the "VPLMN-QoS-Control" feature is supported, the PCF shall ensure that the authorized Session-AMBR value does not exceed the Session-AMBR supported by the VPLMN, if applicable.

The PCF shall provision the new authorized session AMBR to the SMF as defined in clauses 4.2.6.3.1 and 4.2.6.3.2.

Upon reception of the authorized Session-AMBRR, the SMF shall apply the corresponding procedures towards the access network, the UE and the UPF for the enforcement of the AMBR for the concerned PDU session.

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

4.2.3.6 Policy provisioning and enforcement of authorized default QoS

The PCF may modify the authorized default QoS during the lifetime of the PDU session and provision it to the SMF by invoking the procedure defined in clause 4.2.3.2.

If the "VPLMN-QoS-Control" feature is supported, the PCF shall ensure that the authorized default QoS contains a 5QI and ARP value, and MBR/GBR, if applicable, supported by the VPLMN, if applicable.

The PCF shall provision the authorized default QoS to the SMF as defined in clauses 4.2.6.3.1 and 4.2.6.3.2.

Upon reception of 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 for the concerned PDU session.

4.2.3.7 Provisioning of PCC rule for Application Detection and Control

If the ADC feature is supported, the user subscription indicates that application detection and control is enabled, and the PCF determines that application detection is required because of e.g. an internal/external trigger or the PCF has received from an NF service consumer (e.g. another PCF) a subscription to the event for application start/stop traffic detection (see TS 29.514 [17], clause 4.2.6.9), the PCF may provision PCC rule(s) for application detection and control as defined in clause 4.2.6.2.11 in the notification (i.e. HTTP POST) request.

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

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 as described in clause 4.2.2.8 or 4.2.4.8, the PCF shall check:

- for a non-MA PDU session, 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;
- for a MA PDU session:
  a. whether the corresponding service is a 3GPP Data Off Exempt Service and permissible according to the user's subscription and the policies of the PCF; or
  b. whether the corresponding service does not belong to the 3GPP PS Data Off Exempt Services, but:
     - the non-3GPP access is available; and
     - the PCF policies allow all the traffic of the service to be forwarded using the non-3GPP access.

If so, the PCF shall install, modify or delete thecorresponding PCC rules. For a MA PDU session and when theservice does not belong to the 3GPP PS Data Off Exempt Services, the policy for ATSSS Control included in the PCC rule, as specified in clause 4.2.6.2.17, shall enable all the traffic to be forwarded using only the non-3GPP access.

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 make the necessary policy control decisions 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 rules associated to services not contained in the list of 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 of 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 redundant to 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", the "preemptCap" and the "preemptVuln" attributes of the Arp data structure within the QoS data decision to which each PCC Rule refers shall be assigned values (i.e. priority and pre-emption level) as required by local operator policies (e.g. if an IMS Emergency session is prioritized, the "priorityLevel" attribute may contain a value that is reserved for an operator domain use of IMS Emergency session).

The PCF shall immediately initiate the procedures described in clause 4.2.6.2.1 to provision the necessary PCC Rules and the procedures described in clause 4.2.6.2.3 to provision the authorized QoS perPCC rule.

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

Any SMF-initiated request for PCC Rules for an IMS Emergency service with the "repPolicyCtrlReqTriggers" attribute containing the "RES_MO_RE" value (i.e. UE-initiated resource reservation) shall be rejected by the PCF via an HTTP "403 Forbidden" response message including the "cause" attribute of the ProblemDetails data structure set to "ERROR_TRAFFIC_MAPPING_INFO_REJECTED".

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 by the PCF of a request to terminate an AF session for an IMS Emergency service triggers the removal by the PCF of the PCC Rules assigned to the terminated IMS Emergency Service in the SMF, using the procedure defined in clause 4.2.6.2.1.

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

- initiate a QoS flow termination procedure, when all the PCC Rules bound to a QoS flow are removed; or
- initiate a QoS flow modification procedure, when not all the PCC Rules bound to a QoS flow are removed.

In addition, the SMF shall initiate an inactivity timer if all PCC Rules with a 5QI other than the 5QI of the default QoS flow or the 5QI used for IMS signalling were removed from the PDU session restricted to Emergency Services (e.g. to enable PSAP Callback session). When the inactivity timer expires, the SMF shall initiate a PDU session termination procedure as defined in clause 4.2.5.

4.2.3.10 Request of Access Network Information

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

4.2.3.11 Request Usage Monitoring Control

If the UMC feature defined in clause 5.8 is supported, the PCF may provision the usage monitoring control policy to the SMF, as defined in clause 4.2.6.5.3, to request the activation of 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 the SMF. The SMF shall derive the appropriate policies based on the policies provisioned by the PCF and provision them to the appropriate UPF, if applicable, access network, if applicable, and UE, if applicable.

4.2.3.13 Request for the result of PCC rule removal

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

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

4.2.3.14 Access Network Charging Identifier request

The PCF may request the SMF to provide the Access Network Charging Identifier associated to the dynamic PCC rules as defined in clause 4.2.6.5.1.

4.2.3.15 Request for the successful resource allocation notification

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

4.2.3.16 PCC Rule Error Report

If the SMF receives one or more PCC rule(s) as defined in clause 4.2.3.1. but the validation of all the received PCC Rules was unsuccessful, the SMF shall reject the request via an HTTP "400 Bad Request" status code and include in the corresponding response message the "ruleReports" attribute containing RuleReport data structure(s) to report the failure for the affected PCC rule(s) within the ErrorReport data structure; otherwise, if the validation of only some of the received PCC rules was unsuccessful, the SMF shall reply to the PCF with an HTTP "200 OK" status code and include in the corresponding response message one or more RuleReport data structure(s) to report the failure for the affected PCC rule(s) within the PartialSuccessReport data structure.

Within each RuleReport instance, the SMF shall identify the failed PCC rule(s) by including their identifiers within the "pccRuleIds" attribute, identify the failure reason code by including a "failureCode" attribute, and include the PCC rule(s) status within the "ruleStatus" attribute containing a value as follows:

- If the installation/activation of one or more new PCC rules (i.e. rules which were not previously successfully installed) fails, the SMF shall set the "ruleStatus" attribute value to "INACTIVE".
- If the modification of a currently active PCC rule fails, the SMF shall retain the existing PCC rule as active without any modification, unless the reason for the failure has an impact also on the existing PCC rule.

The removal of a PCC rule shall never fail, even if the related PDU session procedures with the UE fail. The SMF shall the retain information on the removal of the PDU session and conduct the necessary PDU session procedures with the UE when it is possible.

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

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

4.2.3.17 IMS Restoration Support

If the ProvAFsignalFlow feature defined in clause 5.8 is supported, and in order to support IMS Restoration procedures (refer to 3GPP TS 23.380 [21]), the PCF needs to convey the AF address to the SMF. In order to do so, in case the AF provisions information about the AF signalling flows between the UE and the AF, as defined in clause 4.4.5a of 3GPP TS 29.214 [18], or in clauses 4.2.2.16 and 4.2.3.17 of 3GPP TS 29.514 [17], the PCF shall install the corresponding dynamic PCC rules (if not installed before) as defined in clause 4.2.6.2.1. The PCF shall include within the associated PccRule instance(s) the signalling flows between the UE and the AF within the "flowInfos" attribute and the "afSigProtocol" attribute set to the value corresponding to the signalling protocol used between the UE and the AF.

The SMF shall respond to the PCF with an HTTP "204 no content" and initiate the corresponding QoS flow procedures, if required. The SMF shall extract the AF address from the provisioned PCC rule(s) and use it for the monitoring procedures as defined for the different access types.

NOTE 1: The SMF can use the extracted AF address from the PCC rule(s) to check if the monitoring procedures have to be started for the corresponding AF.

In case the AF de-provisions information about the AF signalling flows between the UE and the AF, as defined in clause 4.4.5a of 3GPP TS 29.214 [18], or in clauses 4.2.2.16 and 4.2.3.17 of 3GPP TS 29.514 [17], the PCF shall remove the corresponding dynamic PCC rule(s) by triggering a notification (i.e. HTTP POST) message towards the SMF. The PCF shall then apply the procedures defined in clause 4.2.6.2.1.

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

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

4.2.3.18 P-CSCF Restoration Enhancement Support

This clause is applicable when the PCF-based P-CSCF Restoration Enhancement, as defined in 3GPP TS 23.380 [21] and controlled by the feature "PCSCF-Restoration-Enhancement" defined in clause 5.8, is supported by both the PCF and the SMF.

If the PCF receives a request for P-CSCF restoration from the P-CSCF as defined in clause 4.4.7 of 3GPP TS 29.214 [18] or in clause 4.2.2.27 of 3GPP TS 29.514 [17], the PCF shall send a notification (i.e. HTTP POST) message to the SMF including the "pcscfRestIndication" attribute set to true for the corresponding PDU session.

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

4.2.3.19 Request of Presence Reporting Area Change Report

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

4.2.3.20 Session Rule Error Report

If the "SessionRuleErrorHandling" feature is supported and the SMF receives one or more session rule(s) as defined in clause 4.2.6.3.1 but the validation of all the received session rules was unsuccessful, the SMF shall reject the request via an HTTP "400 Bad Request" status code and include in the corresponding response message the "sessRuleReports" attribute containing SessionRuleReport data structure(s) to report the failure for the affected session rule(s) within the ErrorReport data structure; otherwise, if the validation of some of the received session rules was unsuccessful, the SMF shall reply to the PCF with an HTTP "200 OK" status code and include in the corresponding response message the "sessRuleReports" attribute containing one or more SessionRuleReport data structure(s) to report the failure for the affected session rule(s) within the PartialSuccessReport data structure.

Within each SessionRuleReport instance, the SMF shall identify the failed session rule(s) by including their identifier(s) within the "ruleIds" attribute, identify the failure reason code by including a "sessRuleFailureCode" attribute, and include the session rule(s) status within the "ruleStatus" attribute containing a value as follows:

- If the installation of one or more new session rule(s) (i.e. rules which were not previously successfully installed) fails, the SMF shall set the "ruleStatus" attribute value to "INACTIVE".
- If the modification of a currently provisioned session rule fails, the SMF shall retain the existing session rule as provisioned without any modification, unless the reason for the failure has an impact also on the existing session rule. The SMF shall report the modification failure to the PCF.

The removal of a session rule shall never fail, even if the related PDU session procedures with the UE fail. The SMF shall then retain information on the removal of the PDU session and conduct the necessary PDU session procedures with the UE when it is possible.

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

4.2.3.21 Access traffic steering, switching and splitting support

If the PCF supports the "ATSSS" feature, the PCF may provide PCC rules and/or session rules for the MA PDU session as defined in clause 4.2.6.2.17 and clause 4.2.6.3.4.

4.2.3.22 Policy provisioning and enforcement of the AF session with required QoS

If the PCF receives a QoS reference parameter during the initial provisioning of service information as defined in clause 4.2.2.32 of 3GPP TS 29.514 [17] , or if the PCF receives individual QoS parameters during the initial provisioning of service information as defined in clause 4.2.2.24 of 3GPP TS 29.514 [17], the PCF shall authorize the service information from the AF and derive the QoS parameters of the related PCC rule(s) based on the received service information and the indicated QoS reference parameter or the indicated individual QoS parameters (e.g, Requested Maximum Bitrate and Requested Guaranteed Bitrate).

NOTE: A SLA has to be in place between the operator and the ASP defining the possible QoS levels and their charging rates. For each possible pre-defined QoS information set, the PCF needs to be configured with the corresponding QoS parameters and their values as well as the appropriate Charging key (or receive this information from the UDR).

If the PCF receives a different QoS reference parameter or different individual QoS parameters during the modification of service information as defined in clause 4.2.3.30 of 3GPP TS 29.514 [17], the PCF shall update accordingly the related QoS parameters corresponding to the new QoS parameter in the related PCC rule(s).

If the AF subscribes to Service Data Flow QoS notification control, the PCF may additionally receive the Alternative Service Requirements during the initial provisioning of service information as defined in clause 4.2.2.32 of 3GPP TS 29.514 [17].

In this case, when the PCF authorizes service information based on the indicated QoS reference parameter or individual QoS parameters, or individual QoS parameters, and the "AuthorizationWithRequiredQoS" feature is supported, the PCF shall additionally derive alternative QoS parameter sets for the concerned PCC rule(s) based on the QoS reference parameters or individual QoS parameters provided in the Alternative Service Requirements. In order to do so, the PCF shall include one or more references to the QosData data structure within the "refAltQosParams" attribute of the concerned PCC rule(s) and a "qosDecs" attribute containing these QoS data decision(s) within the SmPolicyDecision data structure. In each QoS data decision instance, the PCF shall include the alternative QoS parameter set Id within the "qosId" attribute, the alternative packet delay budget within the "packetDelayBudget" attribute, the alternative packet error rate within the "packetErrorRate" attribute, the alternative guaranteed bandwidth in uplink within the "gbrUl" attribute and the alternative guaranteed bandwidth in downlink within the "gbrDl" attribute. The "refAltQosParams" attribute is an ordered list of alternative QoS parameter sets, where the lower the index of the array for a given entry, the higher the priority.

If the AF changes or newly provides the Alternative Service Requirements during the modification of service information as defined in clause 4.2.3.30 of 3GPP TS 29.514 [17], the PCF shall update accordingly or provide the Alternative QoS parameter sets in the related PCC rule(s).

The PCF shall provision the related PCC rule(s) with alternative QoS parameter set(s) and enable QoS Notification Control, if it has not been enabled yet, as defined in clause 4.2.3.30 of 3GPP TS 29.514 [17].

If the "DisableUENotification" feature is supported and if the AF indicated to the PCF that the UE does not need to be informed about changes related to Alternative QoS Profiles as as defined in clause 4.2.2.32 or 4.2.3.30 of 3GPP TS 29.514 [17] and the PCF decides to disable the notifications to the UE when changes related to the Alternative QoS Profiles occur, the PCF shall include the "disUeNotif" attribute set to true within the corresponding the PCC rule instance.

When the SMF receives PCC rule(s) with alternative QoS parameter sets, the SMF shall enforce these PCC rule(s) and derive in addition the alternative QoS profile(s) towards the access network based on the received alternative QoS parameter set(s).

4.2.3.23 Forwarding of TSC user plane node management information and port management information received from the TSN AF or TSCTSF

During the lifetime of a PDU session enabling Time Sensitive Communications and Time Synchronization the PCF may receive a UMIC and/or one or more PMIC(s) from the TSN AF or TSCTSF within the service information as defined in 3GPP TS 29.514 [17]. A UMIC carries TSC user plane node management information. A PMIC carries port management information for a port located in DS-TT and/or NW-TT.

If the feature "TimeSensitiveNetworking" or "TimeSensitiveCommunication" is supported the PCF initiates the Npcf_SMPolicyControl_UpdateNotify request and sends possibly updated policy information about the PDU Session and/or the UMIC and/or the PMIC(s) to the SMF via the SmPolicyDecision structure, in which the UMIC is encoded in the "tsnBridgeManCont" attribute, the DS-TT PMIC is encoded in the "tsnPortManContDstt" attribute and the one or more NW-TT PMIC(s) are encoded in the "tsnPortManContNwtts" attribute.

The PMIC(s) are encoded in the "PortManagementContainer" data type, that includes the port management information in the "portManCont" attribute and the related port number in the "portNum" attribute. If the port is on DS-TT the SMF forwards the PMIC(s) to the DS-TT port. If the port is on NW-TT the SMF forwards the PMIC(s) to the NW-TT port.

The UMIC is encoded in the "BridgeManagementContainer" data type, that includes the TSC user plane node management information in the "bridgeManCont" attribute. The SMF always forwards the UMIC to the TSC user plane node functionality of the UPF/NW-TT.

4.2.3.24 Provisioning of TSCAI input information and TSC QoS related data

The PCF may receive the TSCAI input information in the TSC assistance container and TSC traffic QoS related information from the TSN AF or TSCTSF.

If the feature "TimeSensitiveNetworking" or "TimeSensitiveCommunication" is supported by both the SMF and PCF as described in clause 5.8, the PCF shall provide for the derived PCC rule(s):

- the 5G QoS parameters and the optional 5G QoS characteristics corresponding to a 5QI for a delay-critical GBR derived from the TSC traffic QoS information received from the TSN AF or TSCTSF encoded within a QosData type referred in the "refQosData" of the PCC rule; and

- the TSCAI input information as received from the TSN AF or TSCTSF, with the periodicity, burst arrival time and survival time encoded in the "tscaiInputUl" attribute and/or "tscaiInputDl" attribute of the PCC rule and, when the feature "TimeSensitiveCommunication" is supported, the (TSN)AF (g)PTP domain encoded in the "tscaiTimeDom" attribute.

The values of MDBV and PDB applied to the derived 5QI shall follow principles defined in clause 5.27.3 of 3GPP TS 23.501 [2].

For IEEE TSN networks, the value of the MBR, if applicable, and the GBR are derived using the Maximum Bit Rate provided by the TSN AF. For other time sensitive communication networks, the value of the GBR may be derived using the input provided by the TSCTSF (e.g. the Minimum Bit Rate) and applying the QoS mapping procedures as specified in clause 7.3.3 of 3GPP TS 29.513 [7].

The ARP is assigned a value preconfigured for TSC services.

As specified in clause 4.2.3.22, when the PCF receives a QoS reference from the TSCTSF, the PCF shall derive the above QoS parameters based on pre-defined QoS parameters referenced by the QoS reference. When the PCF receives individual QoS parameters from the TSCTSF, the PCF shall set derived QoS parameters based on the received individual QoS parameters and applying the QoS mapping procedures as specified in clause 7.3.3 of 3GPP TS 29.513 [7].

If the PCF receives Alternative Service Requirements that contain QoS references from the TSCTSF, the PCF shall derive the alternative QoS parameter set(s) based on the pre-defined QoS parameters referenced by the received Alternative Service Requirements as defined in clause 4.2.3.22. If the PCF receives Alternative Service Requirements that contain Requested Alternative QoS Parameter Set(s) from the TSCTSF, the PCF shall set the alternative QoS parameter set(s) based on the Requested Alternative QoS Parameter Set(s) contained in the received Alternative Service Requirements as defined in clause 4.2.3.22.

The SMF shall convert the received TSCAI input information from the external GM into the 5G GM based on the time offset and cumulative rateRatio (when available) between external time and 5GS time as measured and reported by the UPF and, forward the derived TSCAI parameters per QoS Flow basis to the AN-RAN as follows:

- For the traffic in downlink direction, the SMF shall correct the value of the "burstArrivalTime" attribute of the "tscaiInputDl" attribute based on the latest received time offset measurement from the UPF and set the downlink TSCAI Burst Arrival Time as the sum of the corrected value and the CN PDB as described in clause 5.7.3.4 of 3GPP TS 23.501 [2], representing the latest possible time when the first packet of the data burts arrives at the AN.

- For the traffic in uplink direction, the SMF shall correct the value of "burstArrivalTime" attribute of the "tscaiInputUl" attribute based on the latest received time offset measurement from the UPF and set the uplink TSCAI Burst Arrival Time as the sum of corrected value and the UE-DS-TT Residence Time representing the latest possible time when the first packet of the data burst arrives at the egress of the UE. How the SMF corrects the Burst Arrival Time if the UE-DS-TT residence time has not been provided by the UE is up to SMF implementation.

- The SMF shall correct the value of "periodicity" attribute of the "tscaiInputUl" and/or "tscaiInputDl" using the cumulative rateRatio if the cumulative rateRation measurement was previously received from the UPF and set

the TSCAI Periodicity as the corrected value. Otherwise, the SMF shall set the periodicity in the TSCAI Periodicity without any correction.

- If the "TimeSensitiveCommunication" feature is supported and the TSCAI Survival Time Information is received:
  - when the "surTimeInNumMsg" attribute is received, the SMF shall convert the value of "surTimeInNumMsg" attribute of the "tscaiInputUl" and/or "tscaiInputDl" attributes into time units by multiplying its value by the corrected uplink TSCAI Periodicity and/or downlink TSCAI Periodicity respectively, and set the TSCAI Survival Time to the calculated value; or
  - when the "surTimeInTime" is received, the SMF shall correct the value of "surTimeInTime" attribute of the "tscaiInputUl" and/or "tscaiInputDl" attributes using the cumulative rateRatio if the cumulative rateRatio measurement was previously received from the UPF and set the TSCAI Survival Time to the corrected value. Otherwise, the SMF shall set the TSCAI Survival Time without correction.

If the "TimeSensitiveCommunication" feature is supported, depending on whether the Time Domain information is included in the "tscaiTimeDom" attribute of the PCC rule, SMF may perform the following:

- if the "tscaiTimeDom" attribute is not included in the PCC rule, the SMF provisions the UPF/NW-TT to report the clock drifting between 5G clock and the external GM clock for the (g)PTP time domain number that is configured to the NW-TT.
- If the "tscaiTimeDom" attribute is included in the PCC rule and does not indicate Time Domain = "5GS", the SMF provisions the UPF/NW-TT to report the clock drifting between 5G clock and the external GM clock for the received Time Domain information.

NOTE: The Time Domain value corresponding to "5GS" is locally configured in the SMF and in the TSCTSF and indicates that the AF does not provide a Time Domain, as specified in 3GPP TS 29.565 [53], and it is not needed to adjust the TSCAI input information. The omission of the Time Domain within the "tscaiTimeDom" attribute of the PCC rule indicates it is needed to apply the TSN AF time domain, configured in the NW-TT, to adjust the TSCAI input information.

The SMF shall use the N4 Association Setup or Update procedures as described in 3GPP TS 29.244 [13] to provision the UPF to report the clock drifting.

If the SMF receives the clock drifting from the UPF for a Time Domain, and

- if the received Time Domain matches the Time Domain information within the "tscaiTimeDom" attribute included in the PCC rule; or
- the "tscaiTimeDom" attribute is not included within the PCC rule,

then the SMF may determine the time offset and cumulative rateRatio (when available) based on received Time Domain information and adjust the TSCAI information as described above.

If the received clock drifting from the UPF does not match the Time Domain information within the "tscaiTimeDom" attribute of the PCC rule or the received "tscaiTimeDom" attribute of the PCC rule indicates Time Domain = "5GS" then the SMF will not adjust the TSCAI information.

The provisioning of TSCAI input information and TSC traffic QoS configuration per PCC Rule shall be performed using the PCC rule provisioning procedure as defined in clause 4.2.6.2.1.

4.2.3.25 Policy provisioning of QoS Monitoring to Assist URLLC Service

The QoS Monitoring for URLLC refers to the real time packet delay measurement between the UE and the UPF for a QoS flow corresponding to an URLLC service.

If the "QosMonitoring" feature is supported, the PCF may generate the authorized QoS Monitoring data decision for the service data flow based on the QoS Monitoring request if received from the AF and may determine whether the QoS monitoring report is sent to the AF/NEF by the SMF bypassing the PCF or by the PCF. When the feature "ExposureToEAS" is supported and the AF indication of direct notification is received, the PCF may determine whether duplicate notification is required, i.e., whether the QoS monitoring report is sent to the local AF/NEF by both, the UPF and the PCF.

The PCF shall include within the SmPolicyDecision data structure one or more QosMonitoringData instances within the "qosMonDecs" attribute if not provided yet and, if the PCF determines that the QoS monitoring report shall be sent by the PCF from the SMF, "QOS_MONITORING" within the "PolicyCtrlReqTriggers" attribute, if it has not been provisioned yet.

NOTE 1: The QoS monitoring report can be sent by the SMF to the PCF as described in clause 4.2.4.24 The QoS monitoring report of the PCF to the AF/NEF is described in 3GPP TS 29.514 [17], the QoS monitoring report of the SMF to the AF/NEF bypassing the PCF is described in 3GPP TS 29.508 [12] and the QoS monitoring report to the Local NEF/AF by the UPF is described in 3GPP TS 29.564 [50].

For each QosMonitoringData instance, PCF shall include:

- the requested QoS monitoring parameter(s) to be measured (i.e. DL, UL and/or round trip packet delay) within the "reqQosMonParams" attribute;
- the frequency(s) of reporting (e.g. event triggered, periodic, or when the PDU Session is released, and/or any combination) within the "repFreqs" attribute;
- for the case the "repFreqs" attribute includes the value "EVENT_TRIGGERED":
  - the delay threshold for downlink with the "repThreshDl" attribute if "reqQosMonParams" attribute includes DOWNLINK;
  - the delay threshold for uplink with the "repThreshUl" attribute if "reqQosMonParams" attribute includes UPLINK; and/or
  - the delay threshold for round trip with the "repThreshRp" attribute if "reqQosMonParams" attribute includes ROUND_TRIP;
  - the minimum waiting time between subsequent reports within the "waitTime" attribute;
- for the case the "repFreqs" attribute includes "PERIODIC", the reporting period within the "repPeriod" attribute;
- either the notification URI within the "notifyUri" attribute and the notification correlation id within the "notifyCorreId" attribute if the PCF determines that the notification shall be sent to the AF directly from the SMF or the notification URI within the "notifyUri" attribute, the notification correlation id within the "notifyCorreId" attribute corresponding to the Local NEF or AF and the "directNotifInd" attribute set to true if the feature "ExposureToEAS" is supported and the PCF determines that the direct notification by the UPF to the Local NEF or AF is required based on the indication of direct notification received from the AF.

NOTE 2: If the feature "ExposureToEAS" is supported and if the PCF determines to receive QoS Monitoring report while direct UPF notification is also required, the PCF can provision the "QOS_MONITORING" policy control request trigger to the SMF together with the "directNotifInd" attribute set to true.

The PCF shall include the value of QoS Monitoring Data ID of QosMonitoringData instance within the "refQosMon" attribute of the corresponding PCC rule and provide the QoS monitoring data decision together with the PCC rule if it has not been provisioned to the SMF. When the SMF receives the PCC rule, the SMF shall send a QoS Monitoring request to the PSA UPF via N4 as defined in 3GPP TS 29.244 [13] and NG-RAN via N2 signalling to request the QoS monitoring between PSA UPF and NG-RAN as defined in 3GPP TS 29.502 [22]. If the feature "ExposureToEAS" is supported and if the SMF receives both the "QOS_MONITORING" policy control request trigger and the indication of direct notifcation, the SMF shall request the UPF to perform duplicated notification as defined in 3GPP TS 29.244 [13].

If the PCF receives the request from the local NEF/AF to disable the QoS monitoring from the AF or the Local NEF, the PCF shall update the PCC rule with the "refQosMon" attribute set to NULL. The PCF may also remove the corresponding QoS Monitoring Data if no PCC rule is referring to it.

If the PCF receives the request to disable the direct event notification to the local NEF or AF by the UPF, the PCF shall determine whether the PCF or the SMF bypassing the PCF sends the QoS monitoring reports to the local AF/NEF:

a. if the QoS monitoring reports are sent by the SMF bypassing the PCF:
   - update the PCC rule with the "refQosMon" attribute referring a QosMonitoringData instance which does not include the "directNotifInd" attribute set to true and still includes the "notifyUri", and the "notifyCorreId" attributes; or

- update the corresponding QosMonitoringData instance by including the "directNotifInd" attribute set to false and still keeping the "notifyUri", and the "notifyCorreId" attributes;

b. if the QoS monitoring reports are sent by the PCF:

- update the PCC rule with the "refQosMon" attribute referring a QosMonitoringData instance which does not include the "directNotifInd", the "notifyUri", and the "notifyCorreId" attributes or update the QosMonitoringData instance by removing the "directNotifInd", the "notifyUri", and the "notifyCorreId" attributes ; and

- provision the value "QOS_MONITORING" within the "PolicyCtrlReqTriggers" attribute, if not previously provided.

The SMF shall request to the UPF to disable the notification to the AF/(Local)NEF via N4 as defined in 3GPP TS 29.244 [13] and shall start sending the related notifications to PCF or to the indicated Notification URI and notification correlation Id, as applicable.

The subscription to notification of QoS monitoring events from the SMF bypassing the PCF is disabled by replacing the QosMonitoringData instance with an instance that does not include the "notifyUri" and the "notifyCorrelId" attributes. The subscription to notification of QoS monitoring events from the SMF to PCF is disabled by removing the value "QOS_MONITORING" within the "PolicyCtrlReqTriggers" attribute.

4.2.3.26 Policy decision error handling

4.2.3.26.1 Policy decision types and condition data error handling

If the "PolicyDecisionErrorHandling" feature is supported and the "ExtPolicyDecisionErrorHandling" feature is not supported, and the SMF receives one or more policy decision type(s) (as defined in clause 4.1.4.4) and/or condition data (as defined in clause 4.1.8), which are not referred by any provisioned PCC rule or session rule as defined in clause 4.2.3.2, but the storage of the policy decision types and/or condition data was unsuccessful (e.g. the policy decision could not be successfully stored due to a limitation of resources at the SMF) or there are semantical inconsistencies in the provided data, the SMF shall behave as follows:

- Include an HTTP "200 OK" status code and one or more PolicyDecisionFailureCode data types to indicate the type(s) of the failed policy decisions and/or condition data in the response message, if the SMF does not need to report any other information (e.g. the failure reports of the PCC rule(s) or session rule(s) which are provisioned in the same message, are not needed).

- Include an HTTP "200 OK" status code and one or more PartialSuccessReport data structure(s) including the "policyDecFailureReports" attribute to indicate the type(s) of the failed policy decisions and/or condition data and the "failureCause" attribute set to "POL_DEC_ERROR" in the response message, if the SMF needs to report partial success (e.g. some of the PCC rules and/or session rules provisioned by the PCF in the same message were not installed/activated successfully).

- Include an HTTP "400 Bad Request" status code and the ErrorReport data structure including the "policyDecFailureReports" attribute to indicate the type(s) of the failed policy decisions and/or condition data in the response message, if the SMF needs to reject the request (e.g. all the PCC rules and/or session rules provisioned by the PCF in the same message were not installed/activated successfully).

NOTE: An error within a policy decision type and/or condition data not referred by any PCC rules or session rules is encoded within the "policyDecFailureReports" attribute as specified in the PolicyDecisionFailureCode data structure defined in clause 5.6.3.28.

When the PCF receives the above reports, the PCF shall consider all the instances of the policy decisions and/or condition data which were provisioned in the request message and indicated in the PolicyDecisionFailureCode data type as removed from the SMF. When the PCF receives a response with HTTP "400 Bad Request" status code but the "policyDecFailureReports" attribute is not included in the provided ErrorReport data structure, the PCF shall consider all the provisioned instances of the policy decsions and/or condition data in the request message as removed from the SMF.

The removal of a policy decision type and/or condition data shall not fail.

4.2.3.26.2 Policy decision types, condition data and other policy decisions error handling

If the "ExtPolicyDecisionErrorHandling" feature is supported and the SMF receives one or more policy decision type(s) (as defined in clause 4.1.4.4) and/or condition data (as defined in clause 4.1.8), which are not referred by any provisioned PCC rule or session rule as defined in clause 4.2.3.2, and/or other SM policy decisions (e.g. the SMF receives policy control request triggers and applicable additional information) and the SMF detects that the received policy decision(s) cannot be enforced (e.g, because of semantical inconsistencies in the provided data):

- If the SMF does not need to reject the request (e.g. none, or only some but not all, of the PCC rule(s) and/or session rule(s) provisioned by the PCF in the same message are not installed/activated successfully), the SMF shall include one or more PartialSuccessReport data structure(s) in the response message with an HTTP "200 OK" status code. The SMF shall include in each PartialSuccessReport data structure the "failureCause" attribute set to "POL_DEC_ERROR" and the "policyDecFailureReports" attribute to indicate the failed policy decision type(s) and/or condition data that are not referred by any provisioned PCC rule or session rule and/or in other SM policy decision(s), and may include the "invalidPolicyDecs" attribute to provide more details on these failed policy decision type(s) and/or condition data that are not referred by any provisioned PCC rule or session rule and/or other SM policy decisions.

- If the SMF needs to reject the request (e.g. all the PCC rules and/or session rules provisioned by the PCF in the same message are not installed/activated successfully), the SMF shall include an ErrorReport data structure within a response message with an HTTP "400 Bad Request" status code. The SMF shall include the "policyDecFailureReports" attribute to indicate a failed policy decision type(s) and/or condition data that are not referred by any provisioned PCC rule or session rule and/or in other SM policy decisions, and may include the "invalidPolicyDecs" attribute to provide more details on these failed policy decision types and/or condition data that are not referred by any provisioned PCC rule or session rule and/or other SM policy decisions.

NOTE: An error within a policy decision type and/or condition data not referred by any PCC rules or session rules and/or an error in other policy decisions is encoded within the "policyDecFailureReports" attribute as specified in the PolicyDecisionFailureCode data structure defined in clause 5.6.3.28.

When the PCF receives the above reports, the PCF shall behave as follows:

- For the policy decisions and/or condition data:

  a. The PCF shall consider all the instances of the policy decision(s) and/or condition data which are provisioned in the request message and indicated in the PolicyDecisionFailureCode data type as removed from the SMF.

  b. When the PCF receives a response with HTTP "400 Bad Request" status code but the "policyDecFailureReports" attribute is not included in the provided ErrorReport data structure, the PCF shall consider all the provisioned instance(s) of the policy decision(s) and/or condition data in the request message as removed from the SMF.

  c. The removal of a policy decision type and/or condition data shall not fail.

- For the other policy decisions:

  a. The PCF shall consider all the new failed policy decisions provisioned in the request message and indicated in the PolicyDecisionFailureCode data type as not installed in the SMF.

  b. The PCF shall consider all the modified policy decisions provisioned in the request message and indicated in the PolicyDecisionFailureCode data type as unmodified in the SMF.

  c. The PCF shall consider all the removed policy decisions provided in the request message as deleted in the SMF.

NOTE 2: The removal of a policy decision does not fail. Even if there is an inconsistency e.g. between the deletion of a policy control request trigger and the deletion of the applicable additional information, the whole related policy decision is removed.

4.2.3.27 Network slice related data rate policy control

At the time a PCF-initiated change of the authorized Session-AMBR occurs or PCC Rule(s) for GBR service data flow(s) need to be provisioned at the SMF, the PCF may check if the concerned S-NSSAI is subject to network slice

data rate policy control. If it is the case, the PCF shall apply network slice data rate control as described in clause 4.2.6.8.

4.2.4 Npcf_SMPolicyControl_Update Service Operation

4.2.4.1 General

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

The following procedures using the Npcf_SMPolicyControl_Update service operation are supported:

- Provisioning of PCC rules.
- Provisioning of policy control request triggers.
- Request the policy based on revalidation time.
- Policy provisioning and enforcement of authorized AMBR per PDU session.
- Policy provisioning and enforcement of authorized default QoS.
- Application detection information reporting.
- Indication of QoS Flow Termination Implications.
- 3GPP PS Data Off Support.
- Request and report Access Network Information.
- Request Usage Monitoring Control and report Accumulated Usage.
- Ipv6 Multi-homing support.
- Request and report the result of PCC rule removal.
- Access Network Charging Identifier Request and report.
- Request and report the successful resource allocation notification.
- Negotiation of the QoS flow for IMS signalling.
- Notification about Service Data Flow QoS target enforcement.
- Request the termination of SM Policy association.
- Reporting of TSC user plane node management information and port management information.
- QoS Monitoring Report.
- Policy decision and condition data error handling.
- Request the policy after DDN failure events.
- Network slice related data rate policy control.
- Presence Reporting Area Information Report.
- PCC Rule Error Report.
- Session Rule Error Report.
- UE initiates a resource modification support.
- Trace Control.

4.2.4.2 Requesting the update of the Session Management related policies

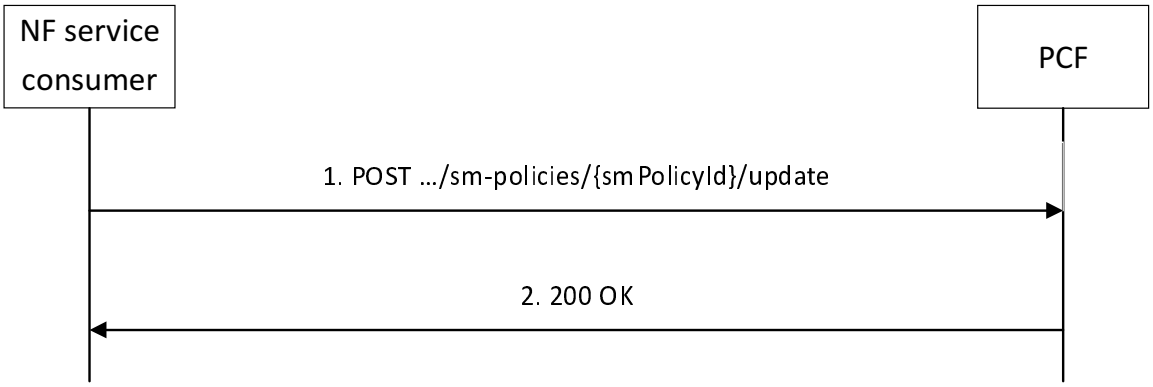

Figure 4.2.4.2-1: Requesting the update of the Session Management related policies

When the NF service consumer detects that one or more policy control request triggers are met, 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. The NF service consumer include SmPolicyUpdateContextData data structure in the payload body of the HTTP POST to request a update of representation of the "Individual SM Policy" resource. The NF service consumer shall include the met policy control request trigger(s) within the "repPolicyCtrlReqTriggers" attribute and applicable updated value(s) in the corresponding attribute(s).

The NF service consumer shall include (if the corresponding policy control request trigger is met and the applicable information is available) in SmPolicyUpdateContextData data structure:

- type of access within the "accessType" attribute;
- type of the radio access technology within the "ratType" attribute;
- the new allocated UE Ipv4 address within the "ipv4Address" attribute and/or the UE Ipv6 prefix within the "ipv6AddressPrefix" attribute;
- multiple new allocated UE Ipv6 prefixes within the "addIpv6AddrPrefixes" attribute, if the "MultiIpv6AddrPrefix" feature is supported;
- the released UE Ipv4 address within the "relIpv4Address" attribute and/or the UE Ipv6 prefix within the "relIpv6AddressPrefix" attribute;
- multiple released UE Ipv6 prefixes within the "addRelIpv6AddrPrefixes" attribute, if the "MultiIpv6AddrPrefix feature" is supported;
- the UE MAC address within the "ueMac" attribute;
- the released UE MAC address within the "relUeMac" attribute;
- the indication of UE supporting reflective QoS within the "refQosIndication" attribute;
- access network charging identifier within the "accNetChIds" attribute;
- the 3GPP PS data off status within the "3gppPsDataOffStatus" attribute, if the "3GPP-PS-Data-Off" feature is supported;
- the UE time zone information within the "ueTimeZone" attribute;
- the UDM subscribed Session-AMBR or, if the "DN-Authorization" feature is supported, the DN-AAA authorized Session-AMBR within the "subsSessAmbr" attribute;

NOTE 1: When both, the UDM subscribed Session-AMBR and the DN-AAA authorized Session-AMBR are available in the NF service consumer, the NF service consumer includes the DN-AAA authorized Session-AMBR.

- if the "VPLMN-QoS-Control" feature is supported, the highest Session-AMBR and the default QoS supported in the VPLMN within the "vplmnQos" attribute, if available;

NOTE 2: In home routed roaming, the H-SMF may provide the QoS constraints received from the VPLMN (defined in 3GPP TS 23.502 [3] clause 4.3.2.2.2) to the PCF.

- if the "DN-Authorization" feature is supported, the DN-AAA authorization profile index within the "authProfIndex" attribute;
- subscribed Default QoS Information within the "subsDefQos" attribute;
- detected application information within the "appDetectionInfos" attribute;
- if the "UMC" feature is supported, the accumulated usage reports within the "accuUsageReports" attribute;
- if the "PRA" feature is supported, the reported presence reporting area information within the "repPraInfos" attribute;
- the QoS flow usage required of the default QoS flow within the "qosFlowUsage" attribute;
- indication whether the QoS targets of one or more SDFs are not guaranteed or guaranteed again within the "qncReports" attribute;
- user location(s) information within the "userLocationInfo" attribute;

NOTE 3: The SMF encodes both 3GPP and non-3GPP access UE location in the "userLocationInfo" attribute when they are both received from the AMF.

- if the "GroupIdListChange" feature is supported, the Internal Group Identifier(s) of the served UE within the "interGrpIds " attribute;
- if the "SatBackhaulCategoryChg" feature is supported, the satellite backhaul category or non-satellite backhaul within the "satBackhaulCategory" attribute;
- if the "AMInfluence" feature is supported, the PCF for the UE callback URI and, if received, SBA binding information within the "pcfUeInfo" attribute;
- serving network function identifier within the "servNfId" attribute;
- identifier of the serving network within the "servingNetwork" attribute; and
- when the "EneNA" feature is supported, the list of NWDAF instance IDs used for the PDU Session within the "nwdafInstanceId" and their associated Analytic ID(s) within "nwdafEvents" updated with the new values included within the "nwdafDatas" attribute.

NOTE 4: The NF service consumer provides the complete updated list of NWDAF instance IDs and associated Analytic ID(s) used for the PDU session. If all NWDAF data is deleted an empty list is included.

The NF service consumer may include in "SmPolicyUpdateContextData" data structure the IPv4 address domain identity within the "ipDomain" attribute.

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

NOTE 5: An empty SmPolicyDecision data structure is included in the "200 OK" response when the PCF decides not to update policies.

If the PCF received a new list of NWDAF instance IDs used for the PDU Session in "nwdafInstanceId" attribute and their associated Analytic IDs in "nwdafEvents" attribute included within the "nwdafDatas" attribute the PCF may select those NWDAF instances based on this new list as described in 3GPP TS 29.513 [7].

If errors occur when processing the HTTP POST request, the PCF shall send an HTTP error response as specified in clause 5.7.

If the feature "ES3XX" is supported, and the PCF determines the received HTTP POST request needs to be redirected, the PCF shall send an HTTP redirect response as specified in clause 6.10.9 of 3GPP TS 29.500 [4].

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

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

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

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

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

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

4.2.4.3 Request the policy based on revalidation time

If the timer for the policy revalidation is started, the SMF shall send the PCC rule request before the indicated revalidation time. The SMF shall within the SmPolicyUpdateContextData data structure include RE_TIMEOUT within the "repPolicyCtrlReqTriggers" attribute. The SMF shall stop the timer once the SMF sends the HTTP POST 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 instruct the SMF to revalidate the provided PCC rules by including the "revalidationTime" attribute within the SmPolicyDecision in the HTTP POST response.

NOTE 2: If the PCF omits the "revalidationTime" attribute the revalidation function remains enabled, but the timer remains stopped till the PCF provides a revalidation time within the "revalidationTime" attribute.

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

The PCF may disable the revalidation function by removing the RE_TIMEOUT policy control request trigger in the HTTP POST response message. If the revalidation function is disabled, the SMF shall ignore any received value of revalidation time and shall not start the timer for revalidation.

NOTE 3: By disabling the revalidation function the revalidation time value previously provided to the SMF is not applicable anymore.

4.2.4.4 Policy provisioning and enforcement of authorized AMBR per PDU session

When the SMF detects that the Session-AMBR changes, the SMF shall notify of the change to the PCF by invoking the procedure defined in clause 4.2.4.2, and shall include the new Session-AMBR within the "subsSessAmbr" attribute and the "SE_AMBR_CH" policy control request trigger within the "repPolicyCtrlReqTriggers" attribute.

If the "DN-Authorization" feature is supported, when both, the UDM subscribed Session-AMBR and the DN-AAA authorized Session-AMBR are available in the SMF, the DN-AAA authorized/re-authorized Session-AMBR shall take precedence over the changes on UDM subscribed Session-AMBR.

If the "VPLMN-QoS-Control" feature is supported,

- in the home routed scenario, when the SMF detects that the Session-AMBR supported in the VPLMN changes (i.e. when the UE moves from the HPLMN to a VPLMN with Session-AMBR constraints or between VPLMNs with different Session-AMBR constraints), the SMF shall notify of the change to the PCF by invoking the procedure defined in clause 4.2.4.2, and shall include the new VPLMN Session-AMBR within the "vplmnQos" attribute and the "VPLMN_QOS_CH" policy control request trigger within the "repPolicyCtrlReqTriggers" attribute.

- when the SMF detects that the UE moves from a VPLMN with Session-AMBR constraints to a VPLMN where the QoS constraints are not applicable in the home routed scenario or the UE moves back to the non-roaming scenario, the SMF shall notify the PCF that the QoS constraints in the VPLMN are not applicable by invoking the procedure defined in clause 4.2.4.2, and shall include the "vplmnQosNotApp" attribute set to true and the "VPLMN_QOS_CH" policy control request trigger within the "repPolicyCtrlReqTriggers" attribute.

Upon receiving the change of Session-AMBR, the PCF shall ensure that the authorized Session-AMBR value does not exceed the Session-AMBR supported by the VPLMN, if applicable, and provision the new authorized Session-AMBR to the SMF in the response as defined in clauses 4.2.6.3.1 and 4.2.6.3.2.

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

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

4.2.4.5 Policy provisioning and enforcement of authorized default QoS

When the SMF detects that the subscribed default QoS change, the SMF shall notify of the PCF by invoking the procedure as defined in clause 4.2.4.2, include the new subscribed default QoS within the "subsDefQos" attribute and "repPolicyCtrlReqTriggers" set to DEF_QOS_CH.

If the "VPLMN-QoS-Control" feature is supported,

- in the home routed scenario, when the SMF detects that the default QoS supported in the VPLMN changes (i.e. when the UE moves from the HPLMN to a VPLMN with default QoS constraints or between VPLMNs with different default QoS constraints), the SMF shall notify of the change to the PCF by invoking the procedure defined in clause 4.2.4.2, and shall include the new default QoS value supported in the VPLMN within the "vplmnQos" attribute and the "VPLMN_QOS_CH" policy control request trigger within the "repPolicyCtrlReqTriggers" attribute;

- when the SMF detects that the UE moves from a VPLMN with default QoS constraints to a VPLMN where the QoS constraints are not applicable in the home routed scenario or the UE moves back to the non-roaming scenario, the SMF shall notify the PCF that the QoS constraints in the VPLMN are not applicable by invoking the procedure defined in clause 4.2.4.2, and shall include the "vplmnQosNotApp" attribute set to true and the "VPLMN_QOS_CH" policy control request trigger within the "repPolicyCtrlReqTriggers" attribute.

Upon receiving the change of default QoS, the PCF shall ensure that the authorized default QoS contains a 5QI and ARP values supported by the VPLMN, if applicable, and shall provision the authorized default QoS to the SMF in the response of the message as defined in clauses 4.2.6.3.1 and 4.2.6.3.2.

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

4.2.4.6 Application detection information reporting

If the ADC feature is supported and if the SMF receives the PCC rule for application detection and control, the SMF shall instruct the UPF as defined in 3GPP TS 29.244 [13] to:

- Detect the application traffic.
- Report the detected application's traffic start/stop events along with the application instance identifier and service data flow descriptions when service data flow descriptions are deducible.

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 clause 4.2.4.2 by including the information regarding the detected application`s traffic within the "appDetectionInfos" 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 each AppDetectionInfo instance, the SMF shall include the corresponding application identifier within the "appId" attribute, and may include the detected service data flow description within the "sdfDescriptions" attribute if deducible and a dynamically allocated application instance identifier for the detected service data flow descriptions within the "instanceId". The "sdfDescriptions" attribute, if present, shall contain the "flowDescription" attribute and "flowDirection" attribute. The application instance identifier allows the 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 clause 4.2.4.2 by including the information regarding the detected application`s traffic within the "appDetectionInfos" attribute and the "APP_STO" within the "repPolicyCtrlReqTriggers" attribute. For each AppDetectionInfo instance, the SMF shall include the corresponding application identifier within the "appId" attribute and the 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.

When a PFD provisioned by the PFDF as specified in 3GPP TS 29.551 [46] is removed/modified and the removed/modified PFD was used to detect application traffic related to an application identifier in a PCC rule installed or activated for a PDU session, if the removed/modified PFD results in that the stop of an application or an application instance is not able to be detected, and if the SMF has reported the application start as described in this clause to the PCF for the application or application instance represented by this PFD, the SMF shall report the application stop to the PCF for the corresponding application or the corresponding application instance, if the stop of the application's traffic, identified by the corresponding application or the corresponding application instance, is received from the UPF.

NOTE: Multiple PFDs can be associated with the application identifier. When the removed/modified PFD is the last one which is used to detect traffic identified by the "appId" attribute, the SMF reports application stop.

4.2.4.7 Indication of QoS Flow Termination Implications

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

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

If the NetLoc feature is supported, and if the identifier of the affected PCC rule was included within the "refPccRuleIds" attribute of the RequestedRuleData data structure when the affected PCC rule was installed or modified, the SMF shall provide the access network information to the PCF by including the user location(s) 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 or the SNPN Identifier

(the PLMN Identifier and the NID) 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).

NOTE 1: The SMF derives the value of the "userLocationInfoTime" attribute from the age of location information received from the AMF at PDU session update as described in 3GPP TS 29.502[22]. Whether the "userLocationInfo" attribute also encodes the age of location is implementation specific.

NOTE 2: The SMF encodes both 3GPP and non-3GPP access UE location in the "userLocationInfo" attribute when they are both received from the AMF.

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

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

4.2.4.8 3GPP PS Data Off Support

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

Upon reception of this HTTP POST message with the "repPolicyCtrlReqTriggers" attribute set to the value "PS_DA_OFF" or "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 PS_DA_OFF 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 3GPP access, i.e.:
  - for a non MA PDU session, the "accessType" attribute is set to "3GPP_ACCESS"; and
  - for a MA PDU session, either the "accessType" attribute or the "addAccessInfo"attribute indicate "3GPP_ACCESS", and the "relAccessInfo" attribute either is not available or does not indicate "3GPP_ACCESS".

If the PCF determines that the 3GPP PS Data Off handling functionality becomes active, the PCF 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 over 3GPP access; and
- all other downlink packets and optionally uplink packets are:
  - for a non-MA PDU session or a MA PDU session where non-3GPP access is not available, discarded by modifying or removing any related dynamic PCC rule(s) or by deactivating any related predefined PCC rule(s);
  - for a MA PDU session where non-3GPP access is available, forwarded only via non-3GPP access, if it is ensured by the policy for ATSSS Control as specified in clause 4.2.6.2.17.

NOTE 2: In order for the UPF to prevent the services that do not belong to the list of 3GPP PS Data Off Exempt Services, if such services are controlled by dynamic PCC rules, the PCF can either close gates for the downlink and optionally the uplink directions via the "flowStatus" attribute in the related dynamic PCC rules or remove those dynamic PCC rules. If the services are controlled by predefined PCC rules, the 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 PS Data Off Exempt Services. The network configuration can ensure that at least one PCC rule is bound to the default QoS flow when PS Data Off is activated in order to avoid the deletion of an existing PDU session or to not fail a PDU session establishment.

If the PCF determines that the 3GPP PS Data Off handling functionality becomes inactive, the PCF shall make the necessary policy control decisions and perform PCC rule operations 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 or not).

NOTE 3: The PCF can then open gates via the "flowStatus" attribute for active PCC rules associated to services not contained in the list of 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 of 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 redundant with this PCC rule.

4.2.4.9 Request and Report of Access Network Information

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

If the AN_INFO policy control request trigger is set, upon receiving the "lastReqRuleData" attribute with the "reqData" attribute with the value(s) MS_TIME_ZONE and/or USER_LOC_INFO and the "refPccRuleIds" attribute containing the PCC rule identifier(s) corresponding to the PCC rule(s) which is being installed, modified or removed together, the SMF shall apply the Namf_EventExposure service for Time-Zone-Report and/or Location-Report event with One-Time Report type as defined in clause 5.3.1 and 5.3.2.2.2 of 3GPP TS 29.518 [36] if the related information is not available to obtain this information. When the SMF then receives access network information from the AMF, the SMF shall provide the required access network information to the PCF by as defined in clause 4.2.4.2 and set the corresponding attributes as follows:

- If the user location(s) 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).

NOTE 1: The SMF derives the value of the "userLocationInfoTime" attribute from the age of location information received in the Location-Report (defined in clause 5.3.1 of 3GPP TS 29.518 [36]) from the AMF. Whether the "userLocationInfo" attribute also encodes the age of location is implementation specific.

NOTE 2: The SMF encodes both 3GPP and non-3GPP access UE location in the "userLocationInfo" attribute when they are both received from the AMF.

- 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 or the SNPN Identifier (the PLMN Identifier and the NID) within the "servingNetwork" attribute.

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

NOTE 3: If the SMF receives the access network information but receives the rejection of the QoS flow creation or modification, the SMF reports the the enforcement error of the PCC rule to the PCF as defined in clause 4.2.4.15.

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

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 requesting the access network information unless the associated QoS flow or PDU session has been released.

4.2.4.10 Request Usage Monitoring Control and Reporting Accumulated Usage

4.2.4.10.1 General

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

The SMF shall report the accumulated usage to the PCF in the following conditions:

- when a usage threshold is reached, as described in this clause;
- when all PCC rules for which usage monitoring is enabled for a particular usage monitoring key are removed or deactivated, as specified in clause 4.2.4.10.2;
- when usage monitoring is explicitly disabled by the PCF, as specified in clause 4.2.6.5.3.2;
- when a PDU session is terminated, as specified in clause 4.2.5.3;
- when requested by the PCF, as specified in clause 4.2.6.5.3.3.

The UPF measures the volume and/or the time of usage of all traffic of a PDU session or the corresponding service data flows. When the SMF receives the accumulated usage report from the UPF as defined in clauses 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 clause 4.2.4.2, including one or more accumulated usage reports within the "accuUsageReports" attribute and the "US_RE" value within the "repPolicyCtrlReqTriggers" attribute. Each AccuUsageReport data structure shall contain the accumulated usage report within one or two Usage Report information element, i.e. the accumulated usage before the monitoring time or the accumulated usage both before and after the monitoring time, corresponding to one usage monitoring control instance as requested by the PCF.

If the monitoring time is provided by the PCF for a usage monitoring control instance and:

- if the SMF receives only one Usage Report information elements corresponding to the usage monitoring control instance from the UPF, within the AccuUsageReport data structure, the SMF shall include the accumulated usage before the monitoring time within the "timeUsage" attribute, "volUsage" attribute, "volUsageUplink" attribute and/or "volUsageDownlink" attribute, if applicable; otherwise,
- if the SMF receives two Usage Report information elements corresponding to the usage monitoring control instance from the UPF, within the AccuUsageReport data structure, the SMF includes the accumulated usage before the monitoring time within the "timeUsage" attribute, "volUsage" attribute, "volUsageUplink" attribute and/or "volUsageDownlink" attribute, if applicable, and the accumulated usage after the monitoring time within the "nextTimeUsage" attribute, "nextVolUsage" attribute, "nextVolUsageUplink" attribute and/or "nextVolUsageDownlink" attribute, if applicable.

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

- if the PCF wishes to continue monitoring for the usage monitoring control instance and:
  - if monitoring shall continue for specific level(s), the PCF shall provide in the response to the received HTTP POST message the new threshold(s) corresponding to these level(s) using the same attributes as before (i.e. "volumeThreshold", "volumeThresholdUplink", "volumeThresholdDownlink" and/or "timeThreshold"; "nextVolThreshold", "nextVolThresholdUplink", "nextVolThresholdDownlink", and/or "nextTimeThreshold" if the "monitoringTime" attribute is provided within an entry of the "umDecs" attribute); or
  - if the PCF wishes to stop monitoring for specific level(s) the PCF shall not include in the response to the received HTTP POST message updated threshold(s) for these specific level(s), i.e. the corresponding "volumeThreshold" attribute, "volumeThresholdUplink" attribute, "volumeThresholdDownlink" attribute, "timeThreshold" attribute, "nextVolThreshold" attribute, "nextVolThresholdUplink" attribute, "nextVolThresholdDownlink" attribute, and/or "nextTimeThreshold" attribute shall not be included within an entry of the "umDecs" attribute.
- otherwise, if the PCF wishes to stop monitoring for the usage monitoring control instance, the PCF shall not include any thresholds of this usage monitoring control instance in the response to the HTTP POST message or

remove the reference to the usage monitoring control instance from the concerned dynamic PCC rule or session rule.

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

Upon reception of the reported usage from the SMF, the PCF shall deduct the value of the usage report from the total allowed usage for that PDU session, usage monitoring key, or both as applicable, and the PCF may also derive and update the PCC rules based on the remaining allowed usage or reported usage and provision them to the SMF. If the remaining allowed usage reaches a value zero (or below zero), the PCF may apply other policy decisions and interact with the SMF accordingly.

NOTE: The PCF can also update the related usage monitoring information in the UDR as defined in 3GPP TS 29.519 [15] according to the received usage report(s).

4.2.4.10.2 PCC Rule Removal

When the PCF removes or deactivates the last PCC rule associated with a usage monitoring key in an Npcf_SMPolicyControl_UpdateNotify request as described in clause 4.2.3.2 or in an Npcf_SMPolicyControl_Update response as described in clause 4.2.3.4 whose request was not related to reporting usage for the same monitoring key, the SMF shall send a new Npcf_SMPolicyControl_Update request including the "US_RE" value within the "repPolicyCtrlReqTriggers" attribute and one or more accumulated usage reports within the "accuUsageReports" attribute within the SmPolicyUpdateContextData data type of the HTTP POST request using the procedures to report accumulated usage defined in clause 4.2.4.10.

When the SMF reports that the last PCC rule associated with a usage monitoring key is inactive, the SMF shall report the accumulated usage for that monitoring key within the same HTTP POST request if the "ruleReports" attribute was included in the SmPolicyUpdateContextData data type; otherwise, if the "ruleReports" attribute was included in the HTTP POST response of an Npcf_SMPolicyControl_UpdateNotify request, the SMF shall invoke the Npcf_SMPolicyControl_Update service operation by sending a new HTTP POST request to report accumulated usage for the usage monitoring key.

4.2.4.11 Ipv6 Multi-homing support

The SMF may insert an additional PDU Session Anchor to an existing PDU session by using Ipv6 multi-homing mechanism. In this case, the SMF shall inform the PCF when one or more new Ipv6 prefix is allocated to the new PDU Session Anchor as defined in clause 4.2.4.2. The SMF shall, within the SmPolicyUpdateContextData data structure, include the "UE_IP_CH" within the "repPolicyCtrlReqTriggers" attribute and include the new Ipv6 prefix within the "ipv6AddressPrefix" attribute or multiple new Ipv6 prefixes within the "addIpv6AddrPrefixes" attribute, if the "MultiIpv6AddrPrefix" feature is supported.

When the PCF receives the request from the SMF indicating the addition of one or more new Ipv6 prefixes, the PCF shall determine the impacted PCC rules and/or session rules associated with each new Ipv6 prefix and provision them to the SMF as defined in clauses 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. The PCF shall additionally consider the new Ipv6 prefix, or the multiple new Ipv6 prefixes if the "MultiIpv6AddrPrefix" feature is supported, during subsequent PCC rules and/or session rules updates.

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 clause 4.2.5.2. The SMF shall, within the SmPolicyUpdateContextData data structure, include the "UE_IP_CH" within the "repPolicyCtrlReqTriggers" attribute and include the released Ipv6 prefix within the "relIpv6AddressPrefix" attribute or multiple released UE Ipv6 prefixes within the "addRelIpv6AddrPrefixes" attribute, if the "MultiIpv6AddrPrefix feature" is supported.

When the PCF receives the request from the SMF indicating the release of one or more Ipv6 prefixes, the PCF shall determine the previously provisioned PCC rules and/or session rules associated with each released Ipv6 prefix and shall remove and/or update them from the SMF as applicable. The PCF shall remove the released Ipv6 prefix, or the multiple released Ipv6 prefixes if the "MultiIpv6AddrPrefix" is supported.

4.2.4.12 Request and report for the result of PCC rule removal

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

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

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

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

4.2.4.13 Access Network Charging Identifier request and report

If the "PolicyCtrlReqTriggers" attribute with the value "AN_CH_COR" has been provided to the SMF, the SMF shall notify of the PCF the Access Network Charging Identifier(s) that the SMF has assigned for the dynamic PCC Rules which referred from the RequestedRuleData data structure containing the CH_ID within the "reqData" attribute by including an "accNetChIds" attribute within the SmPolicyUpdateContextData data structure in the HTTP POST message.

If the SMF assigns an Access Network Charging Identifier to the whole PDU session, and the Access Network Charging Identifier is within the Uint32 value range; the SMF shall include one AccNetChId instance within the "accNetChIds" attribute and include the Access Network Charging Identifier within the "accNetChaIdValue" attribute and the "sessionChScope" attribute set to true; otherwise, within each AccNetChId instance, the SMF shall include Access Network Charging Identifier within the "accNetChaIdValue" attribute and all the PCC rule identifier(s) associated to the provided Access Network Charging Identifier within the "refPccRuleIds" attribute; otherwise, if the "AccNetChargId_String" feature is supported by the SMF and the PCF, and the Access Network Charging Identifier value is longer than Uint32, the SMF shall include one AccNetChId instance within the "accNetChIds" attribute and the Access Network Charging Identifier within the "accNetChargIdString" attribute and the "sessionChScope" attribute set to true.

The PCF may request the SMF to provide the Access Network Charging Identifier associated to the new dynamic PCC rules as defined in clause 4.2.6.5.1 in the response message.

4.2.4.14 Request and report for the successful resource allocation notification

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

If the "PolicyCtrlReqTriggers" attribute with the value "SUCC_RES_ALLO" has been provided to the SMF, the SMF shall notify of the PCF the resources associated to the PCC rules which referred from the RequestedRuleData data structure containing the "SUCC_RES_ALLO" within the "reqData" attribute are successfully allocated. When the SMF received successful resource allocation response from the access network, the SMF shall within the SmPolicyUpdateContextData data structure include the "SUCC_RES_ALLO" within the "repPolicyCtrlReqTriggers" attribute and "ruleReports" attribute. Within the RuleReport instance, the SMF shall include the corresponding PCC rule identifier(s) within the "pccRuleIds" attribute and the "ruleStatus" attribute set to value "ACTIVE". If the "AuthorizationWithRequiredQoS" feature as defined in clause 5.8 is supported and if the SMF additionally receives the reference to the matching Alternative QoS Profile which the NG-RAN can guarantee, the SMF shall also include the reference to the QosData data structure for the Alternative QoS parameter set corresponding to the reference to the matching alternative QoS profile within the "altQosParamId" attribute.

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

4.2.4.15 PCC Rule Error Report

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

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

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

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

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

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

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

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

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

4.2.4.16 Presence Reporting Area Information Report

If the PRA or ePRA feature as defined in clause 5.8 is supported and when the SMF receives the presence reporting area information from the serving node as defined in 3GPP TS 29.518 [36] indicating that the UE is inside or outside of one or more presence reporting areas or any of the presence reporting areas is set to inactive, the SMF shall check if the reported presence reporting area identifier corresponds to a presence reporting area that is relevant for the PCF. In that case, the SMF shall within the SmPolicyUpdateContextData data structure include the "PRA_CH" within the "repPolicyCtrlReqTriggers" attribute and one or more Presence Reporting Area Information Report within the "repPraInfos" attribute. For each PresenceInfo data structure, the SMF shall also include the presence reporting area status within the "presenceState" attribute and the presence reporting area identifier within the "praId" attribute for each of the presence reporting areas reported by the serving node.

If the SMF receives presence reporting area information for a Set of Core Network predefined Presence Reporting Area encoded within the "praId" attribute together with the individual PRA Identifier encoded within the "additionalPraId" attribute as described in 3GPP TS 29.518 [36], the SMF shall only provide the PCF with the presence reporting area information corresponding to the additional PRA information (i.e. the individual PRA identifier) encoded within the "praId" attribute.

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

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

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

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

4.2.4.17 UE initiates a resource modification support

In the case that the UE initiates a resource modification procedure as defined in clause 6.4.2.2 of 3GPP 3GPP TS 24.501 [20], the SMF shall within the SmPolicyUpdateContextData data structure include the "RES_MO_RE" within the "repPolicyCtrlReqTriggers" attribute and shall include the UE request of specific QoS handling for selected SDF within the "ueInitResReq" attribute. Within the UeInitiatedResourceRequest data structure, the SMF shall include the "ruleOp" attribute, "packFiltInfo" attribute and "reqQos" attribute if applicable as follows:

- When the UE requests to "Create new QoS rule", the SMF shall include the "ruleOp" attribute set to "CREATE_PCC_RULE", the "packFiltInfo" attribute and "reqQos" attribute containing the requested QoS for the new PCC rule. Each PacketFilterInfo instance shall contain one packet filters requested for creating the new QoS rule. If the PCF authorizes the request, the PCF shall create a new PCC rule by including the new packet filters within the service data flow template of the PCC rule. When the SMF received the PCC rule, the SMF shall derive the QoS rule based on the PCC rule, assign a new QoS rule identifier within the PDU session for the QoS rule. The SMF shall keep the mapping between the PCC rule identifier and the QoS rule identifier.

- When the UE requests to "Modify existing QoS rule and add packet filters" for the QoS rule created as a result of the UE-initiated resource modification, SMF shall include the "ruleOp" attribute set to "MODIFY_PCC_RULE_AND_ADD_PACKET_FILTERS", the "pccRuleId" attribute including the PCC rule identifier corresponding the QoS rule identifier and the "packFiltInfo" attribute. Each PacketFilterInfo instance shall contain one packet filters requested for addition to this QoS Rule. If the UE request includes the modified QoS information the SMF shall also include the "reqQos" attribute to indicate the updated QoS for the affected PCC rule(s). If the PCF authorizes the request, the PCF shall update the PCC rule by adding the new packet filters to the service data flow template of the PCC rule.

- When the UE requests to "Modify existing QoS rule and replace all packet filters" for the QoS rule created as a result of the UE-initiated resource modification, SMF shall include the "ruleOp" attribute set to "MODIFY_PCC_RULE_AND_REPLACE_PACKET_FILTERS", the "pccRuleId" attribute including the PCC rule identifier corresponding the QoS rule identifier and the "packFiltInfo" attribute. Each PacketFilterInfo instance shall contain one packet filters requested for addition to this QoS Rule. If the UE request includes the modified QoS information the SMF shall also include the "reqQos" attribute to indicate the updated QoS for the affected PCC rule. If the PCF authorizes the request, the PCF shall update PCC rule by replacing the all existing packet filters within the service data flow template of the PCC rule with the new packet filter(s).

- When the UE requests to "Modify existing QoS rule and delete packet filters" for the QoS rule created as a result of the UE-initiated resource modification, SMF shall include the "ruleOp" attribute set to "MODIFY_PCC_RULE_AND_DELETE_PACKET_FILTERS", the "pccRuleId" attribute including the PCC rule identifier corresponding the QoS rule identifier and the "packFiltInfo" attribute. Each PacketFilterInfo instance shall within the "packFiltId" attribute include the removed packet filter identifier assigned by the PCF corresponding to the packet filter identifier received from the UE. If the UE request includes modified QoS information the SMF shall also include the "reqQos" attribute to indicate the updated QoS for the affected PCC rule(s). If the PCF authorizes the request, the PCF shall update PCC rule by removing the corresponding packet filters from the service data flow template of the PCC rule.

- When the UE requests to "Modify existing QoS rule without modifying packet filters" for the QoS rule created as a result of the UE-initiated resource modification, SMF shall include the "ruleOp" attribute set to "MODIFY_PCC_RULE_WITHOUT_MODIFY_PACKET_FILTERS", the "pccRuleId" attribute including the PCC rule identifier corresponding the QoS rule identifier, the "packFiltInfo" attribute and the modified QoS information within the "reqQos" attribute. The "packFiltInfo" attribute shall include one PacketFilterInfo instance which includes any packet filter identifier assigned by the PCF for the PCC rule within the "packFiltId" attribute.

- When the UE requests to "Delete existing QoS rule" the SMF shall include the "ruleOp" attribute set to "DELETE_PCC_RULE" for the QoS rule created as a result of the UE-initiated resource modification, the "pccRuleId" attribute including the PCC rule identifier corresponding the QoS rule identifier and the "packFiltInfo" attribute. The "packFiltInfo" attribute shall include one PacketFilterInfo instance which includes any packet filter identifier assigned by the PCF for the PCC rule within the "packFiltId" attribute. The PCF shall remove the PCC rule when the PCF receives the request according to the PCC rule identifier.

NOTE 1: The UE can only modify or delete the packet filters that the UE has introduced and associated resources. The packet filter identifiers contained in the FlowInformation data structure are only used for packet filters created by the UE.

The SMF shall calculate the requested GBR, for a GBR 5QI, as the sum of the previously authorized GBR for the affected PCC rule, corresponding to the QoS rule, adjusted with the difference between the requested GBR for the QoS flow and previously negotiated GBR for the QoS flow. For the UE request to create a new QoS Rule, the GBR as requested by the UE for the QoS rule shall be used.

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

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

NOTE 2: The UE signalling with the network is governed by the applicable NAS signalling TS. The NAS 3GPP TS for a specific access may restrict the UE possibilities to make requests compared to what is stated above.

Upon receipt of the request from the SMF, the PCF shall check the set of services the user is allowed to access. If the user is not allowed to access AF session based services, the PCF shall check whether the user is allowed to request resources for services not known to the PCF and whether the requested QoS and/or packet filters can be authorized. If the user is not allowed to request resources for services not known to the PCF, the PCF shall reject the request with in an HTTP "403 Forbidden" response message including the "cause" attribute of the ProblemDetails data structure set to "POLICY_CONTEXT_DENIED".

If the PCF authorizes the request from the UE, the PCF shall construct a PCC rule(s) based on the UeInitiatedResourceRequest data structure. For the request to add the filter(s), the PCF shall within the FlowInformation data structure include the assigned packet filter identifier within the "packFiltId" attribute. When the SMF derives the QoS based on the PCC rule, the SMF shall assign a new packet filter identifier for each added packet filter within the QoS rule and keep the mapping between the packet filter identifier for the packet filter within the PCC rule and QoS rule.

The PCF shall perform the QoS authorization for the new created or modified PCC rules if requested by the UE as defined in clause 4.2.6.6.2.

If the PCF detects that the packet filters in the request for new PCC rules received from the SMF is covered by the packet filters of outstanding PCC rules that the PCF is provisioning to the SMF, the PCF may reject the request and indicate the cause for the rejection including the "cause" attribute of the ProblemDetails data structure set to "ERROR_CONFLICTING_REQUEST" in an HTTP "403 Forbidden" response message. If the SMF receives a response message with this code, the SMF shall ignore the PDU session modification that initiated the HTTP request as specified in 3GPP TS 24.501[20] clause 6.3.2.5.

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

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

4.2.4.18 Trace Control

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

4.2.4.19 Negotiation of the QoS flow for IMS signalling

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

4.2.4.20 Notification about Service Data Flow QoS target enforcement

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

- the GBR QoS targets cannot be guaranteed; or
- the GBR QoS targets can be guaranteed again;

the SMF shall inform the PCF that the GBR QoS targets cannot be guaranteed or can be guaranteed again for the PCC rules bound to the QoS flows.

The SMF gets the knowledge that the GBR QoS targets cannot be guaranteed or can be guaranteed again for the QoS flow(s) as follows:

- upon receiving a notification from the NG-RAN that the GFBR can no longer be guaranteed or can be guaranteed again as defined clause 5.2.2.3.1 of 3GPP TS 29.502 [22]; or
- during a handover, a QoS Flow which is listed as transferred QoS Flow received from the AMF as defined clause 5.2.2.3.1 of 3GPP TS 29.502 [22] can be interpreted as a notification that GFBR can be guaranteed again if the SMF has received a notification from the source NG-RAN that the GFBR can no longer be guaranteed but does not receive an explicit notification that the GFBR can no longer be guaranteed for that QoS Flow from the Target NG-RAN within a configured time as previous bullet.

The SMF shall send an HTTP POST request to the PCF with an SmPolicyUpdateContextData data structure, including the "QOS_NOTIF" within "repPolicyCtrlReqTriggers" attribute and the "qncReports" attribute. In each QosNotificationControlInfo data structure, the SMF shall include the indication that the GBR QoS targets cannot be guaranteed or the GBR QoS targets can be guaranteed again within the "notifType" attribute and affected PCC rule identifiers within the "refPccRuleIds" attribute. If the "AuthorizationWithRequiredQoS" feature as defined in clause 5.8 is supported, the SMF shall also include the reference to the QosData data structure for the Alternative QoS parameter set corresponding to the reference to the matching alternative QoS profile within the "altQosParamId" attribute if the SMF additionally receives the reference to the matching Alternative QoS Profile which the NG-RAN can guarantee when the NG-RAN indicates the GBR QoS targets cannot be guaranteed. When the SMF additionally receives an indication that lowest priority Alternative QoS Profile cannot be fulfilled from the NG-RAN the SMF shall omit the "altQosParamId" attribute to indicate that that the lowest priority alternative QoS profile could not be fulfilled either. When the "DisableUENotification" feature is supported, if the corresponding PCC rule does not include the "disUeNotif" attribute set to true, the SMF shall also send the fulfilled QoS profile or Alternative QoS Profile to the UE as defined in clause 5.2.2.3.1.1 of 3GPP TS 29.518 [36], if applicable.

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

When the PCF receives the HTTP POST request, it shall acknowledge the request by sending a "200 OK" response to the SMF and then notify the AF as defined in 3GPP TS 29.514 [17], clause 4.2.5.4.

4.2.4.21 Session Rule Error Report

If the "SessionRuleErrorHandling" feature is supported and if the installation of one or more session rules fails using the procedure as defined in clauses 4.2.2.1 or 4.2.4.1 or the PCF provisioned one or more session rules as defined in clause 4.2.3.1 but enforcement of the session Rule was unsuccessful (e.g. session-AMBR is rejected by the AMF in the roaming scenario, and the SMF determines that the PDU session is kept, the SMF shall include the "sessRuleReports" attribute for the affected session rules to report the failure within the SmPolicyUpdateContextData data structure. Within each SessionRuleReport instance, the SMF shall identify the failed session rule(s) by including the affected

session rules within the "ruleIds" attribute, identify the failed reason code by including a "sessRuleFailureCode" attribute, and shall include rule status within the "ruleStatus" attribute with the value as described below.

If the installation of one or more new session rules fails, the SMF shall set the "ruleStatus" to INACTIVE.

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

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

If a session rule was successfully installed, but can no longer be enforced by the SMF:

- If the "ImmediateTermination" feature is supported, and based on operator's policy, the SMF shall evaluate whether the PDU session can be kept. If the SMF determines to terminate the PDU session immediately, the SMF shall trigger the deletion of the SM Policy Association as described in clauses 4.2.5, otherwise the SMF shall set the "ruleStatus" attribute to INACTIVE.

- If the the "ImmediateTermination" feature is not supported, the SMF shall set the "ruleStatus" attribute to INACTIVE.

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

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

4.2.4.22 Request the termination of SM Policy association

If "RespBasedSessionRel" feature is supported, PCF may request the PDU session termination upon receiving a POST message from the SMF (e.g. when usage quota reached). In this case, the PCF shall include the "relCause" attribute within the SmPolicyDecision data structure of the response to the POST message.

After the receipt of a successful HTTP POST response from the PCF containing the "relCause" attribute within the SmPolicyDecision data structure, the SMF shall invoke the Npcf_SMPolicyControl_Delete Service Operation defined in clause 4.2.5 to terminate the policy association and initiate the procedure to terminate the PDU session as defined in 3GPP TS 29.502 [22].

4.2.4.23 Reporting of TSC user plane node management information and port management information

If the feature "TimeSensitiveNetworking" or "TimeSensitiveCommunication" is supported and the "TSN_BRIDGE_INFO" policy control request trigger is provisioned in the SMF, when new TSC user plane node information is available the SMF requests to update the SM Policy Association and provides to the PCF information on the conditions that have been met.

The Policy Control Request Trigger condition "TSN_BRIDGE_INFO" is met when:

a. the SMF detects new TSC user plane node ports which supports exchange of Port Management Information Containers. The SMF shall send to the PCF, if available:

   - the DS-TT port number encoded in the "dsttPortNum" attribute allocated by the UPF;

   - the TSC user plane node Id received from the UPF encoded in the "bridgeId" attribute;

   - the MAC address of the DS-TT port received from the UE encoded in the "dsttAddr" attribute; and

   - the UE-DS-TT residence time if received from the UE encoded in the "dsttResidTime" attribute,

   within the SmPolicyUpdateContextData structure encoded in the "tsnBridgeInfo" attribute of the TsnBridgeInfo data type; and/or

b. when the SMF receives a UMIC from the TSC user plane node functionality of the UPF/NW-TT and/or a PMIC from the DS-TT port and/or one or more PMIC(s) in the corresponding one or more NW-TT ports. The SMF

shall transparently forward to the PCF the UMIC encoded within the "tsnBridgeManCont" attribute and/or the DS-TT PMIC encoded within the "tsnPortManContDstt" attribute and/or the one or more NW-TT PMIC(s) encoded within the "tsnPortManContNwtts" attribute within the SmPolicyUpdateContextData structure.

For IP type of PDU sessions, the UE IP address of the PDU session received within the "ipv4Address" or "ipv6AddressPrefix" attribute, as described in clause 4.2.2.2 and 4.2.4.2 (reported with trigger "UE_IP_CH") is used as identifier of the PDU session related to the reported TSC user plane node information.

For Ethernet type of PDU sessions (IEEE TSN and other time sensitive communications than TSN) the MAC address of the DS-TT port received within the "dsttAddr" attribute is used as identifier of the PDU session related to the reported TSC user plane node information.

4.2.4.24 Notification about Service Data Flow QoS Monitoring

When the SMF gets the information about any one of the following items for one or more SDFs from the UPF:

- uplink packet delay(s); or
- downlink packet delay(s); or
- round trip delay(s);

then SMF shall inform the PCF for the impacted PCC rules.

The SMF shall send an HTTP POST request to the PCF with an SmPolicyUpdateContextData data structure, including the "QOS_MONITORING" within "repPolicyCtrlReqTriggers" attribute and the "qosMonReports" attribute. In each QosMonitoringReport data structure, the PCF shall include:

- one or two uplink packet delays within the "ulDelays" attribute; or
- one or two downlink packet delays within the "dlDelays" attribute; or
- one or two round trip packet delays within the "rtDelays" attribute; and
- affected PCC rule identifiers within the "refPccRuleIds" attribute.

4.2.4.25 Access traffic steering, switching and splitting support

If "ATSSS" feature defined in clause 5.8 is supported and the PCF has previously provisioned the AC_TY_CH policy control request trigger, when the UE requests to:

- add an access to an already established MA PDU session (i.e. registers to another acess), the SMF shall, within the SmPolicyUpdateContextData data structure, include the "AC_TY_CH" within the "repPolicyCtrlReqTriggers" attribute and include the additional Access type and the additional RAT type if available within the "addAccessInfo" attribute.
- release an access from an already established MA PDU session (i.e. deregisters from one access but remains registered on the other access), the SMF shall, within the SmPolicyUpdateContextData data structure, include the "AC_TY_CH" within the "repPolicyCtrlReqTriggers" attribute and include the released access type and the released RAT type if available within the "relAccessInfo" attribute.

When the PCF receives the request from the SMF indicating the addition of Access Type or removal of Access Type, the PCF may provide PCC rules and/or session rules for the MA PDU session as defined in clause 4.2.6.2.17 and clause 4.2.6.3.4.

4.2.4.26 Policy decision error handling

4.2.4.26.1 Policy decision types and condition data error handling

If the "PolicyDecisionErrorHandling" feature is supported and the "ExtPolicyDecisionErrorHandling" feature is not supported, and one or more policy decision types (as defined in clause 4.1.4.4) and/or condition data (as defined in clause 4.1.8) which are not referred by any PCC rules or session rule is provisioned using the procedure as defined in clauses 4.2.2.1, 4.2.3.1 or 4.2.4.1 but the storage was unsuccessful (e.g. the policy decision could not be successfully

stored due to a limitation of resources at the SMF), or because there are semantical inconsistencies in the provided data, the SMF shall include the "policyDecFailureReports" attribute to indicate the type(s) of the failed policy decisions and/or condition data within the SmPolicyUpdateContextData data structure.When the PCF receives the above reports, the PCF shall consider all the instances of the policy decsions and/or condition data which are not referred by any PCC rule and/or session stored at the SMF and indicated by the PolicyDecisionFailureCode data type are removed from the SMF.

The removal of a policy decision type and/or condition data shall not fail.

4.2.4.26.2 Policy decision types, condition data and other policy decisions error handling

If the "ExtPolicyDecisionErrorHandling" feature is supported and one or more policy decision types (as defined in clause 4.1.4.4) and/or condition data (as defined in clause 4.1.8) which are not referred by any PCC rules or session rules is provisioned using the procedure as defined in clauses 4.2.2.1, 4.2.3.1 or 4.2.4.1, and/or other SM policy decisions (e.g. the SMF receives policy control request triggers and applicable additional information) but the SMF detects the received policy decision cannot be enforced (e.g. because semantical inconsistencies in the provided data), and the SMF determines that the PDU session can be kept, the SMF shall within the SmPolicyUpdateContextData data structure include the "policyDecFailureReports" attribute to indicate a failure in the provided policy decision types and/or condition data not referred by any PCC rules or session rules and/or in other SM policy decisions, and may include the "invalidPolicyDecs" attribute to indicate the failed policy decision types and/or condition data not referred by any PCC rules or session rules and/or other SM policy decisions.

When the PCF receives the above report, the PCF shall consider:

- all the instances of the policy decsions and/or condition data which are not referred by any PCC rule and/or session stored at the SMF and indicated by the PolicyDecisionFailureCode data type are removed from the SMF; and
- for the other policy decisions:
  a. All the new failed policy decisions provisioned are not installed in the SMF.
  b. All the modified policy decisions shall remain unmodified in the SMF.
  c. All the removed policy decisions provided in the request message are deleted in the SMF.

NOTE: The removal of a policy decision does not fail. Even if there is an inconsistency e.g. between the deletion of a policy control request trigger and the deletion of the applicable additional information, the whole related policy decision is removed.

4.2.4.27 Policy Control for DDN Events

If the feature "DDNEventPolicyControl" or "DDNEventPolicyControl2" is supported, and if the PCF has previously provisioned "DDN_FAILURE" policy control request trigger, the SMF shall send the PCC rule request when it receives an event subscription for DDN Failure event including the traffic descriptors. The SMF shall send an HTTP POST request to the PCF with an SmPolicyUpdateContextData data structure, including the "DDN_FAILURE" within "repPolicyCtrlReqTriggers" attribute and include one or more traffic descriptor(s) in the "trafficDescriptors" attribute within the SmPolicyUpdateContextData structure for policy evaluation. Upon reception of the HTTP POST message:

- if the PCF determines that there is an existing PCC rule for the traffic detection of DDD Status event which has the same traffic descriptor(s) as the new request one, the PCF shall update the existing PCC rule for traffic detection of DDD Status event by including both the "DDN_FAILURE" and "DDD_STATUS" values within the "notifCtrlInds" attribute of the "ddNotifCtrl" attribute if the "DDNEventPolicyControl" feature is supported or of the "ddNotifCtrl2" attribute if the "DDNEventPolicyControl2" feature is supported to indicate both the DDN Failure and DDD Status event detection;
- if the PCF determines that there is an existing PCC rule for the policy and charging control which has the same traffic descriptor(s) as the new request one, the PCF shall update the existing PCC rule by including the downlink data notification control information within the "ddNotifCtrl" attribute if the "DDNEventPolicyControl" feature is supported or within the "ddNotifCtrl2" attribute if the "DDNEventPolicyControl2" feature is supported to indicate the DDN Failure event detection. Within the DownlinkDataNotificationControl or DownlinkDataNotificationControlRm data type, the PCF shall include the "DDN_FAILURE" value within the "notifCtrlInds" attribute;

- otherwise the PCF shall make a new PCC rule by including the reported traffic descriptors within the "flowInfos" attribute, setting a lower value to the "precedence" attribute and including the downlink data notification control information within the "ddNotifCtrl" attribute if the "DDNEventPolicyControl" feature is supported or within the "ddNotifCtrl2" attribute if the "DDNEventPolicyControl2" feature is supported and setting the other PCC rule information to the same values as in an existing PCC rule that previously matched the traffic. Within the DownlinkDataNotificationControl or DownlinkDataNotificationControlRm data type, the PCF shall include the "DDN_FAILURE" value within the "notifCtrlInds" attribute to indicate the DDN Failure event detection. When the new PCC rule has to be bound to the default QoS flow, the PCF shall include the "defQosFlowIndication" attribute set to true within the QosData data structure to which the PCC rule refers. From now on, the PCF needs to keep new PCC rule for event detection fully synchronized with the existing PCC rule that previously matched the traffic for all other policy and charging control settings to ensure the same user experience and traffic treatment according to the operator policy.

If the feature "DDNEventPolicyControl" or the "DDNEventPolicyControl2" is supported, and if the PCF has previously provisioned "DDN_DELIVERY_STATUS" policy control request trigger, the SMF shall send the PCC rule request when it receives an event subscription for DDD Status event including the traffic descriptors. The SMF shall send an HTTP POST request to the PCF with an SmPolicyUpdateContextData data structure, including the "DDN_DELIVERY_STATUS" within "repPolicyCtrlReqTriggers" attribute, include one or more traffic descriptor(s) in the "trafficDescriptors" attribute and the type(s) of notification in the "typesOfNotif" attribute within the SmPolicyUpdateContextData structure for policy evaluation. Upon reception of the HTTP POST message:

- if the PCF determines that there is an existing PCC rule for traffic detection of DDN Failure event which has the same traffic descriptor(s) as the new request one, the PCF shall update the existing PCC rule for traffic detection of DDN Failure event by including both the "DDN_FAILURE" and "DDD_STATUS" values within the "notifCtrlInds" attribute and the type(s) of notifications within the "typesOfNotif" attribute of the "ddNotifCtrl" attribute if the "DDNEventPolicyControl" feature is supported or of the "ddNotifCtrl2" attribute if the "DDNEventPolicyControl2" feature is supported to indicate both the DDN Failure and DDD Status event detection;

- if the PCF determines that there is an existing PCC rule for the policy and charging control which has the same traffic descriptor(s) as the new request one, the PCF shall update the existing PCC rule by including the downlink data notification control information within the "ddNotifCtrl" attribute if the "DDNEventPolicyControl" feature is supported or within the "ddNotifCtrl2" attribute if the "DDNEventPolicyControl2" feature is supported to indicate the DDD Status event detection. Within the DownlinkDataNotificationControl or DownlinkDataNotificationControlRm data type, the PCF shall include the "DDD_STATUS" value within the "notifCtrlInds" attribute and the type(s) of notifications within the "typesOfNotif" attribute;otherwise the PCF shall make a PCC rule by including the reported traffic descriptors within the "flowInfos" attribute, setting a lower value to the "precedence" attribute and including the downlink data notification control information within the "ddNotifCtrl" attribute if the "DDNEventPolicyControl" feature is supported or within the "ddNotifCtrl2" attribute if the "DDNEventPolicyControl2" feature is supported to indicate the DDD Status event detection and setting the other PCC rule information to the same values as in an existing PCC rule that previously matched the traffic. Within the DownlinkDataNotificationControl or DownlinkDataNotificationControlRm data type, the PCF shall include the "DDD_STATUS" value within the "notifCtrlInds" attribute and the type(s) of notifications within the "typesOfNotif" attribute to indicate that DDN Status event detection is required. When the new PCC rule has to be bound to the default QoS flow, the PCF shall include the "defQosFlowIndication" attribute set to true within the QosData data structure to which the PCC rule refers. From now on, the PCF needs to keep new PCC rule for event detection fully synchronized with the existing PCC rule that previously matched the traffic for all other policy and charging control settings to ensure the same user experience and traffic treatment according to the operator policy.

If the feature "DDNEventPolicyControl2" is supported, when the SMF receives a request to cancel a subscription of the DDN Failure or DDD status event and if the PCF has previously provisioned "DDN_FAILURE_CANCELLATION" and "DDN_DELIVERY_STATUS_CANCELLATION policy control request trigger, the SMF shall send an HTTP POST request to the PCF with an SmPolicyUpdateContextData data structure, including the "DDN_FAILURE_CANCELLATION" or "DDN_DELIVERY_STATUS_CANCELLATION" within "repPolicyCtrlReqTriggers" attribute respectively and include the rule identifier of the PCC rule which is used for traffic detection of event within the "pccRuleId" attribute. Upon reception of the HTTP POST message:

- If the PCC rule corresponding to the received PCC rule identifier is only used for the traffic detection of DDN failure or DDD Status respectively, the PCF shall remove the PCC rule locally and request the SMF to remove it too.

- If the PCC rule corresponding to the received PCC identifier is used for the traffic detection of both DDN failure and DDD status events, the PCF shall update the PCC rule by removing the downlink data notification control information for DDN failure or DDD status respectively from the PCC rule. In order to do that, within the DownlinkDataNotificationControlRm data type of the "ddNotifCtrl2" attribute, the PCF shall omit the "DDN_FAILURE" or "DDD_STATUS" within the "notifCtrlInds" attribute respectively. If the data notification control information for the DDD status is omitted, the PCF shall aslo include the "typesOfNotif" attribute set to NULL.

- If the PCC rule corresponding to the receied PCC rule identifier is also used for the policy and charging control to the service data flow besides the traffic detection of the DDN failure or DDD status event, the PCF shall update the PCC rule by removing the downlink data notification control information from the PCC rule. In order to do that, the PCF shall include the "ddNotifCtrl2" attribute set to NULL.

NOTE: The "ddNotifCtrl" attribute is used to contain the downlink data notification control information if the "DDNEventPolicyControl" feature is supported; while the "ddNotifCtrl2" attribute is used to contain the downlink data notification control information if the "DDNEventPolicyControl2" feature is supported.

When the SMF receives the new or updated PCC rule within the response message from the PCF, SMF shall perform the DDD Status and/or DDN Failure event based on the downlink data notification control information within the PCC rue as follows:

- If the downlink data notification control information indicates that the detection of DDD Status event and buffered notification type is required, the SMF shall derive a PDR and a related FAR as defined in clause 5.28 of 3GPP TS 29.244 [13] to request the UPF to report an event of the first buffered downlink data packet identified by the PDR. When the SMF receives the corresponding report, the SMF shall send the notification to the NEF as defined in clause 4.2.2.2 of 3GPP TS 29.508 [12].

- If the downlink data notification control information indicates that the detection of DDD Status event and transmitted notification type is required, the SMF shall detect event and send the notification as defined in clause 4.2.2.2 of 3GPP TS 29.508 [12].

- If the downlink data notification control information indicates that the detection of DDN Failure event and/or DDD Status event and discarded notification type is required, the SMF shall derive a PDR and a related FAR as defined in clause 5.28 of 3GPP TS 29.244 [13] to request the UPF to report an event of the first discarded downlink data packet identified by the PDR. When the SMF receives the corresponding report, the SMF shall send the notification to the AMF as defined in clause 5.2.2.5.1 of 3GPP TS 29.502 [22] and/or send the notification to the NEF as defined in clause 4.2.2.2 of 3GPP TS 29.508 [12] respectively.

4.2.4.28 Network slice related data rate policy control

When an Npcf_SMPolicyControl_Update request that requires a change of the authorized Session-AMBR and/or MBR update(s) for PCC Rule(s) corresponding to GBR service data flow(s) is received, the PCF may check if the S-NSSAI to which the received request relates is subject to network slice data rate policy control. If it is the case, the PCF shall apply network slice data rate control as described in clause 4.2.6.8.

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 policy context associated with a PDU Session.

The following procedures using the Npcf_SMPolicyControl_Delete service operation are supported:

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

- Report Accumulated Usage.

- Report Access Network Information.

- Report Service Data Flow QoS Monitoring.

- Network slice related data rate policy control.

4.2.5.2 SM Policy Association termination

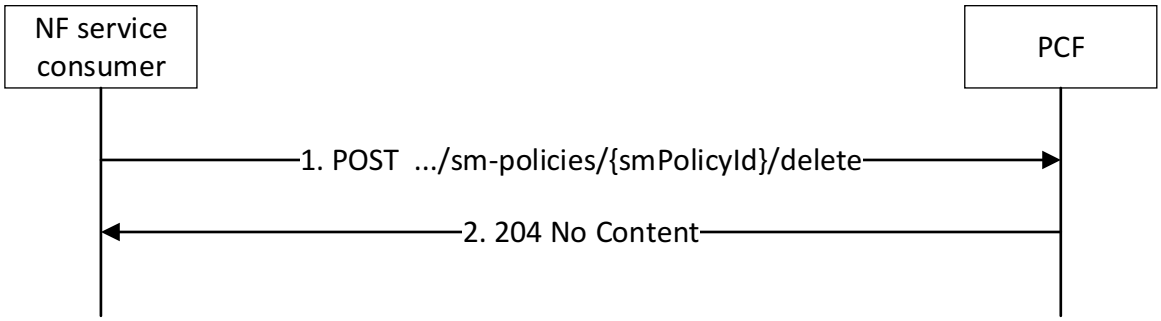

Figure 4.2.5.2-1: SM Policy Association termination

When an individual resource of the SM Policy Association collection shall be deleted, the NF service consumer shall invoke the Npcf_SMPolicyControl_Delete service operation towards the PCF using an HTTP POST request, as shown in figure 4.2.5.2-1, step 1.

The NF service consumer 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 HTTP POST request sent by the NF service consumer (e.g. SMF) shall contain (if available) the SM Policy Association related information within the SmPolicyDeleteData data structure in the request body:

- accumulated usage within the "accuUsageReports" attribute as defined in clause 4.2.5.3;
- the user location(s) information within the "userLocationInfo" attribute, the information on when the UE was last known to be in that location within the "userLocationInfoTime" attribute, the PLMN Identifier or the SNPN Identifier (the PLMN Identifier and the NID) within the "servingNetwork" attribute, the timezone information within the "ueTimeZone" attribute and the RAN and/or NAS release cause(s) within the "ranNasRelCauses" attribute as defined in clause 4.2.5.4;

NOTE 1: The SMF derives the value of the "userLocationInfoTime" attribute from the age of location information received from the AMF at PDU session termination as described in 3GPP TS 29.502[22]. Whether the "userLocationInfo" attribute also encodes the age of location is implementation specific.

NOTE 2: The SMF encodes both 3GPP and non-3GPP access UE location in the "userLocationInfo" attribute when they are both received from the AMF.

- the "PS_TO_CS_HO" value within the "pduSessRelCause" attribute, if the PDU session is released due to PS to CS handover and the "PDUSessionRelCause" feature defined in clause 5.8 is supported;
- one or more QoS Monitoring report(s) within the "qosMonReports" attribute, as defined in clause 4.2.5.5;
- the "RULE_ERROR" value within the "pduSessRelCause" attribute, if the PDU session is released due to a failed enforcement of the applied session rule as described in clause 4.2.4.21 and the "ImmediateTermination" feature defined in clause 5.8 is supported.

When the PCF receives the HTTP POST request from the NF service consumer and if the PCF successfully processed and accepted the received HTTP POST request from the NF service consumer, the PCF shall acknowledges the request by sending an HTTP response message with the corresponding status code. The PCF acknowledges the delete request by sending a "204 No Content" response to the NF service consumer, as shown in figure 4.2.5.2-1, step 2. Further, the PCF shall remove the individual resource linked to the delete request.

If errors occur when processing the HTTP POST request, the PCF shall send an HTTP error response as specified in clause 5.7.

If the feature "ES3XX" is supported, and the PCF determines the received HTTP POST request needs to be redirected, the PCF shall send an HTTP redirect response as specified in clause 6.10.9 of 3GPP TS 29.500 [4].

4.2.5.3 Report Accumulated Usage

If the UMC feature is supported, at PDU session termination, the SMF shall send the accumulated usage information for all the monitoring keys for which usage monitoring was previously enabled. When the SMF receives the accumulated usage report from the UPF as defined in clause 7.5.7.2 of 3GPP TS 29.244 [13], the SMF shall include one or more received accumulated usage reports in the "accuUsageReports" attribute of the SmPolicyDeleteData data structure.

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

4.2.5.4 Report Access Network Information

If the RAN-NAS-Cause feature is supported or the NetLoc feature is supported, within the SmPolicyDeleteData data structure, the SMF shall provide the available access network information within the "userLocationInfo" attribute (if available), the information on when the UE was last known to be in that location within the "userLocationInfoTime" attribute (if available), the "ueTimezone" attribute (if available). Additionally, for the NetLoc feature, if the user location information is not available, the SMF shall include the PLMN Identifier or the SNPN Identifier (the PLMN Identifier and the NID) within the "servingNetwork" attribute; for RAN-NAS-Cause feature, if the SMF received from the access network the RAN cause and/or the NAS cause due to PDU session termination, the SMF shall provide the received cause(s) in the "ranNasRelCauses" attribute.

NOTE 1: The SMF derives the value of the "userLocationInfoTime" attribute from the age of location information received in the Location-Report (defined in clause 5.3.1 of 3GPP TS 29.518 [36]) from the AMF. Whether the "userLocationInfo" attribute also encodes the age of location is implementation specific.

NOTE 2: The SMF encodes both 3GPP and non-3GPP access UE location in the "userLocationInfo" attribute when they are both received from the AMF.

4.2.5.5 Report Service Data Flow QoS Monitoring

If the QosMonitoring feature is supported, when the SMF receives from the UPF the information about any one of the following items for one or more SDF(s) as defined in clause 5.24.4.3 of 3GPP TS 29.244 [13]:

- uplink packet delay(s);
- downlink packet delay(s); or
- round trip delay(s);

then within the SmPolicyDeleteData data structure, the SMF shall include one or more Qos Monitoring report(s) within the "qosMonReports" attribute. In each QosMonitoringReport data structure, the PCF shall include:

- one or two uplink packet delay(s) within the "ulDelays" attribute; or
- one or two downlink packet delay(s) within the "dlDelays" attribute; or
- one or two round trip packet delay(s) within the "rtDelays" attribute; and
- the affected PCC rule identifiers within the "refPccRuleIds" attribute.

4.2.5.6 Network slice related data rate policy control

When an Npcf_SMPolicyControl_Delete request is received, the PCF may check if the S-NSSAI to which the received request relates is subject to network slice data rate policy control. If it is the case, the PCF shall apply network slice data rate control as described in clause 4.2.6.8.

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 clause 4.2.2;
- the SM Policy Association Notification request as part of the Npcf_SMPolicyControl_UpdateNotify Service Operation as described in clause 4.2.3.2; and
- the Npcf_SMPolicyControl_Update service operation as described in clause 4.2.4

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

Policy decisions may include:

- Session Rule(s), as described in clause 4.1.4.3, encoded within the "sessRules" attribute;
- PCC Rule(s), as described in clause 4.1.4.2, encoded within the "pccRules" attribute;
- QoS decision(s), as described in clause 4.1.4.4.3, which can be referenced from PCC rule(s), encoded within the "qosDecs" attribute;
- Charging decision(s), as described in clause 4.1.4.4.4, which can be referenced from PCC rule(s), encoded within the "chgDecs" attribute;
- Traffic control decision(s), as described in clause 4.1.4.4.2, which can be referenced from PCC rule(s), encoded within the "traffContDecs" attribute;
- Usage monitoring control decision(s), as described in clause 4.1.4.4.5, which can be referenced from PCC rule(s) and session rule(s), encoded within the "umDecs" attribute;
- QoS monitoring decision, as described in clause 4.1.4.4.6, which can be referenced from PCC rule(s), encoded within the "qosMonDecs" attribute;
- Condition(s) that can be referenced from PCC rule(s) and session rule(s), encoded within the "conds" attribute;
- QoS characteristics for non-standard 5QIs and non-preconfigured 5QIs provided within the "qosChars" attribute;
- A reflective QoS timer;
- Policy control request triggers and applicable additional information, e.g. Revalidation Time, PRA information;
- Last requested rule data;
- Last requested usage data;
- Default charging method of the PDU session;
- "PDU Session with offline charging only" indication;
- Charging information;
- P-CSCF Restoration Indication;
- IP index information;
- Presence Reporting Area information;
- TSC user plane node management information;
- port management information for the DS-TT port;
- port management information for the NW-TT port;

- The request of the PDU session termination;
- Usage of QoS flow;
- Redundant PDU session indication.

For the Npcf_SMPolicyControl_Create Service Operation, the SmPolicyDecision data structure shall contain a full description of all policy decision(s) provided by the PCF for the policy association.

For the Npcf_SMPolicyControl_UpdateNotify service operation for the SM Policy Association Notification request and for the Npcf_SMPolicyControl_Update service operation, the SmPolicyDecision data structure shall contain a description of the changes to the policy decision(s) with respect to the last provided policy decision(s) for the corresponding policy association. The redundant PDU session indication, the default charging method of the PDU session, the "PDU Session with offline charging only" indication, the charging information, the Reflective QoS Timer and the IP index information shall not be updated by the PCF.

If no other rule is defined for specific data types within the SmPolicyDecision data structure, the encoding of changes of the policy decision(s) 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 "qosDecs" attribute, the "traffContDecs" attribute, the "umDecs" attribute, the "conds" attribute, etc.), this attribute shall be provided with a value containing a map with entries according to the following principles:
   - A new entry of the map shall be added by supplying a new identifier (e.g. rule / decision identifier) as the key and the corresponding structured data type instance (e.g. PCC rule) with the complete content as the value.
   - An existing entry of the map shall be modified by supplying the existing identifier as the key and the corresponding structured data type instance as the value, with the same existing identifier (e.g. set the "qosId" to the same existing QoS data decision identifier), which shall describe the modifications following bullets 1 to 6.
   - An existing entry of the map shall be deleted by supplying the existing identifier as the key and "NULL" as the value.
   - For an unmodified entry of the map, no entry needs to be provided within the map.
2) To modify an attribute with a structured data type instance as the 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 the value, the attribute shall be provided with a complete representation of its value, which 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 the 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 the related data structures, no attribute can be marked as mandatory except the attribute containing the identifier (e.g. rule / decision identifier).

The PCF shall not remove a provisioned policy decision data or condition data from the SMF when the associated reference(s) from the PCC rule(s) or session rule(s) are still valid except the usage montoring data referred by the pre-defined PCC rule(s) (see clause 4.2.6.5.3.2 for further information). If the PCF determines that the policy decision or condition data shall be used for future PCC or session rule(s), the PCF may keep a policy decision data or condition data valid when the PCF removes all the PCC rule or session rule(s) referring to that policy decision data or condition data; otherwise the PCF shall remove the provisioned policy decision data or condition data when the PCF removes all the PCC or session rule(s) referring to the policy decision data or condition data.

When the NF service consumer (SMF) accepts the notification of policy updates, and/or when after receiving the response to the request of policies the SM Policy association is retained in the NF service consumer (SMF), if the installation/activation of one or more new PCC rule(s) or the installation of one or more session rule(s) (i.e. rules which were not previously successfully installed) fails, although the failed PCC rule(s) or session rule(s) are removed, the

policy decision and/or condition data which are referred by the failed PCC rule(s) or session rule(s) may remain applicable in the SMF until the PCF removes them. If the PCF determines that the policy decision or condition data that remain applicable shall be used for future PCC or session rule(s) (e.g. because the PCF reattempts to install the failed PCC rule) the PCF may keep these policy decision data or condition data valid; otherwise the PCF shall immediately remove these policy data or condition data from the SMF.

NOTE 3: Due to internal policies, the SMF could decide to remove the policy decision and/or condition data not referred by any PCC and/or session rule(s) before the PCF decides to remove them. When the PCF decides to remove the policy decision and/or condition data that were silently removed by the SMF, the SMF accepts the removal indication, as specified in clauses 4.2.3.26 and 4.2.4.26. When the PCF decides to reuse the policy decision and/or condition data that were silently removed by the SMF, the SMF reports PCC and/or session rule error as specified in clauses 4.2.3.16, 4.2.4.15, 4.2.3.20 and 4.2.4.21.

NOTE 4: When the PCF notification of policy updates is rejected as specified in clauses 4.2.3.16 and 4.2.3.20 with a HTTP "400 Bad Request" status code, the whole update is rejected, including the provided policy decision and/or condition data. When the SMF reports PCC and/or session rule(s) error as specified in clauses 4.2.4.15 and 4.2.4.21 for all the provisioned PCC rule and/or session rule(s), the valid policy decision and/or condition data provided in the corresponding update response can remain valid in the SMF until the PCF removes them.

The error handling for the policy decision and/or condition data which are not referred by any PCC rule and/or session rule stored at the SMF is defined in clause 4.2.3.26 and 4.2.4.26.

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 PCC rule(s) shall be included in the "pccRules" map attribute within the SmPolicyDecision data structure with the associated "pccRuleId" as the key of the map. For activating a pre-defined PCC rule or installing or modifying a dynamic PCF-provisioned PCC rule, the corresponding PccRule data structure 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, this predefined PCC rule is deactivated simultaneously in all the QoS flows where it was previously activated.

In order to activate a pre-defined PCC rule, the PCF shall include within the PccRule data structure the pre-defined PCC rule identifier within the "pccRuleId" attribute and the "refCondData" attribute, if applicable, i.e. the PccRule data structure is empty, except for the "pccRuleId" attribute and the "refCondData" attribute, if applicable. If the "refCondData" attribute is applicable, a "conds" attribute containing the corresponding ConditionData data structure referred by this PCC rule shall be included in the SmPolicyDecision data structure, if it has not been previously provided.

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

- It may include the precedence of a PCC rule among the other PCC rules of the PDU session, within the "precedence" attribute. Within a PDU session, the PCF shall authorize different precedence values for the PCC rules whose packet filters contained within the "flowDescription" attribute or the "ethFlowDescription" attribute include the "packetFilterUsage" attribute set to "true".

NOTE 2: The SMF sets the precedence value of a QoS rule to the precedence value of the PCC rule for which the QoS rule is generated. The UE considers as an error when two or more QoS rules associated with a PDU session have identical precedence values.

- It shall include either the flow information within the "flowInfos" attribute or the application identifier within the "appId" attribute.

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

- It may include one or more reference(s) to the QosData structure within the "refAltQosParams" attribute to refer to the Alternative QoS parameter set(s) of the service data flow. In this case, a "qosDecs" attribute containing the corresponding alternative QoS data policy decision(s) shall be included in the SmPolicyDecision data structure, if it has not been previously provided,

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

- 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 decision shall be included in the SmPolicyDecision data structure, if it has not been previously provided.

- It may include one reference to the QosMonitoringData data structure within the "refQosMon" attribute. In this case, a "qosMonDecs" attribute containing the corresponding QoS Monitoring data policy decision shall be included in the SmPolicyDecision data structure, if it has not been previously provided.

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

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

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

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

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

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

The SMF shall ensure that at least one PCC Rule bound to the default QoS flow is activated for the PDU Session. If the PCF does not provision any PCC rule, the SMF shall activate at least one pre-defined PCC rule which is not known by the PCF and bind it to the default QoS flow.

If the authorized default QoS is GBR type or delay critical GBR type as defined in clause 4.2.6.3.3, to ensure that one and only one of the authorized PCC rules is bound to the default QoS flow the PCF shall indicate that one and only one PCC rule is bound to the default QoS flow as defined in clause 4.2.6.2.10. The SMF shall not bind any other PCC rule to the default QoS flow with a GBR or delay critical GBR 5QI.

4.2.6.2.2 Gate Function

The Gate Function is a user plane function that permits to control, i.e. enabling or disabling, the forwarding of data packets belonging to a service data flow. A gate is provisioned by the PCF within a PCC rule, enforced by the SMF and ultimately applied by the UPF.

If a PCC rule contains the "flowInfos" attribute applicable for uplink service data flow(s), it shall describe a gate for the corresponding uplink service data flow(s). If a PCC rule contains the "flowInfos" attribute(s) applicable for downlink service data flow(s), it shall describe a gate for the corresponding downlink service data flow(s). If the PCC rule contains an "appId" attribute, it shall describe a gate for the corresponding detected application traffic. In order to do so, the "flowStatus" attribute within the TrafficControlData data structure to which the PCC rule refers shall describe if uplink and/or downlink gate(s) is/are open or closed.

The commands to open or close a gate shall lead to enabling or disabling the passage of the corresponding data packets. If a gate is closed, all data packets of the related service data flow(s) are dropped by the UPF. If a gate is open, the data packets of the related service data flow(s) are allowed to be forwarded by the UPF.

4.2.6.2.3 Policy enforcement for authorized QoS per PCC Rule

The PCF may provide the authorized QoS for a PCC rule to the SMF. The Provisioning of the authorized QoS per PCC Rule shall be performed using the PCC rule provisioning procedure defined in clause 4.2.6.2.1. For a PCF-provided PCC rule, the authorized QoS shall be encoded using the QosData data structure. The PCF shall include for this purpose a reference to this 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 associated QoS profile towards the access network, if applicable, the associated QoS rule towards the UE, if applicable, and the associated QoS information with the PDR(s) towards the UPF.

4.2.6.2.4 Redirect Function

When the ADC feature is supported, the PCF may provide the redirect instructions for one or several dynamic PCC rule(s) to the SMF. This Provisioning shall be performed using the policy provisioning procedure defined in clause 4.2.6.1.

The "traffContDecs" attribute within the SmPolicyDecision is used to provide traffic control decision(s). The redirect instructions shall be encoded using the "redirectInfo" attribute within the corresponding TrafficControlData data structure, and used to provide a RedirectInformation data structure with the following components:

- The "redirectEnabled" attribute to indicate whether redirect is enabled or not. It shall be included and set to true when the redirect instruction is initially provisioned and may be included in subsequent updates of the RedirectInformation to enable or disable the redirect instruction.

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

NOTE 1: The SMF/UPF uses the preconfigured redirection address only if it can be applied to the application traffic being detected, e.g. the redirection destination address could be preconfigured on a per application identifier basis.

If redirect action(s) need to be applied to a dynamic PCC rule, this PCC rule shall reference a traffic control decision with the relevant redirect instructions. If a dynamic PCC rule includes flow information for UE IPv4 address and IPv6 prefix address(es) related to the same application identifier and the ADCmultiRedirection feature is supported, the "addRedirectInfo" attribute including more than one RedirectInformation data structure may be provided simultaneously to the redirect instruction.

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

If the "redirectServerAddress" attribute is not provided in the dynamic PCC rule and the redirection address is not preconfigured in the SMF/UPF for this PCC rule, the SMF shall perform PCC Rule Error Report, as specified in clauses 4.2.3.16 and 4.2.4.15, and set the "failureCode" attribute to "MISS_REDI_SER_ADDR".

NOTE 2: When the redirect server address is not provided by the PCC rule, the SMF determines the "MISS_REDI_SER_ADDR" error, e.g. when the SMF determines the redirect destination is not pre-configured at both the SMF and the UPF.

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

- update the PCC rule to modify the reference to Traffic Control Data decision to point to another (existing or new) Traffic Control Data decision that does not have "redirectInfo" instructions; or

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

For a predefined PCC rule, the redirect information shall be included in the rule definition at the SMF/UPF. Redirect information shall be activated for predefined PCC rules while those rules are active.

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 clause 4.2.6.2.1. For a dynamic PCC rule, 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). For a predefined PCC rule, the reference to a usage monitoring control instance shall be included in the rule definition at the SMF. 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 an appropriate operator or 3rd party service functions (e.g. NAT, antimalware, parental control, DdoS protection) in the N6-LAN or 5G-LAN type of services, or enabling the routing of the user traffic to a local Data Network identified by a DNAI per AF request.

4.2.6.2.6.1 Steering the traffic in the N6-LAN or steering the 5G-LAN type of services

This procedure is only applicable in non-roaming and home-routed scenarios.

For the purpose of steering the subscriber's traffic to an appropriate operator or 3rd party service functions in the N6-LAN or steering the 5G-LAN type of services, the PCF shall include within the PccRule data structure a reference to the relevant Traffic Control Data decision and:

- include within the PccRule data structure either the application to be detected identified by the "appId" attribute or the service data flow to be detected identified by the "flowInfos" attribute; and
- include a "traffContDecs" attribute containing the corresponding Traffic Control Data decision within the SmPolicyDecision, if it has not been previously provided. In this case, the PCF shall include directly within this Traffic Control Data decision a traffic steering policy identifier for downlink within the "trafficSteeringPolIdDl" attribute and/or a traffic steering policy identifier for uplink within the "trafficSteeringPolIdUl" attribute.

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

If traffic steering policy provided in the "trafficSteeringPolIdUl" and/or "trafficSteeringPolIdDl" attribute are invalid or unknown, or the enforcement of the steering of the traffic failed, the SMF shall return a PCC Rule Error Report, as specified in clauses 4.2.3.16 and 4.2.4.15, and set the "failureCode" attribute to "TRAFFIC_STEERING_ERROR".

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

This procedure is only applicable in non-roaming and visited access (i.e. LBO) scenarios.

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 the individual IP address/ prefix allocated to a UE or the UE MAC address, the PCF shall store the received traffic routing information and perform session binding as defined in clause 6.2 of 3GPP TS 29.513 [7] to determine the impacted PDU session.
- Otherwise, the PCF fetches from the UDR, as defined in 3GPP TS 29.519 [15], the traffic routing data information applicable for a UE, any UE or an Internal Group Id (if received in the SMF request).

Then the PCF authorizes the request for influencing SMF routing decisions. For the impacted PDU Session that corresponds to the AF request, the PCF shall take into account, if available, the local routing indication stored in the policy data subscription information in the UDR, as defined in 3GPP TS 29.519 [15], to determine whether it is allowed to generate PCC rules with traffic routing information. When allowed, the PCC rules are generated based on the AF request as follows:

- When the request is for influencing SMF routing decisions, based on traffic routing information, operator's policy, etc., the PCF determines the traffic steering policy. The traffic steering policy indicates, for each DNAI, a traffic steering policy identifier configured in the SMF and/or if the N6 routing information associated to the application is explicitly provided by the AF, the N6 routing information (as provided by the AF). The traffic steering policy identifier is derived by the PCF from the routing profile Id provided by the AF and is related to the mechanism enabling traffic steering to the DN. Then:

  - The PCF shall include within each PccRule data structure the necessary information to identify the concerned traffic within either the "flowInfos" attribute or the "appId" attribute, and include within the TrafficControlData data type that the PCC rule refers to a list of locations that the traffic shall be routed to in the "routeToLocs" attribute, and, if the "AF_latency" feature is supported, the PCF shall include the maximum allowed user plane latency within the "maxAllowedUpLat" attribute if available. If "EASIPreplacement" feature is supported, the PCF shall include the EAS IP replacement information within the "easIpReplaceInfos" attribute if available.

  - Within each RouteToLocation instance, the PCF shall include a DNAI in the "dnai" attribute to indicate the location of the application towards which the traffic routing is applied, and a traffic steering policy identifier in the "routeProfId" attribute, to indicate the traffic steering policy that applies to the indicated DNAI, and/ or the explicit N6 traffic routing information in the "routeInfo" attribute.

  - If the AF provides both a routing profile Id and N6 routing information for a DNAI, the PCF may include a RouteToLocation instance with the required information or may include two RouteToLocation instances with the same DNAI within the "dnai" attribute and a traffic steering policy identifier within the "routeProfId" attribute in one instance and explicit routing information within the "routeInfo" attribute in the other instance.

NOTE 1: The N6 traffic routing requirements are related to the mechanism enabling traffic steering in the local access to the DN. The routing profile ID refers to a pre-agreed policy between the AF and the 5GC. This policy may refer to different steering policy identifier(s) sent to the SMF and e.g. based on time of the day, etc.

NOTE 2: When per DNAI both, the "routeProfId" and the "routeInfo"attributes are provided, if the pre-configured traffic steering policy referenced by the "routeProfId" attribute contains information that is overlapping with the N6 traffic routing information provided in the "routeInfo" attribute, the N6 traffic routing information takes precedence.

NOTE 3: In this release of the specification, either a traffic steering policy identifier for UL or a traffic steering policy identifier for DL can be defined per DNAI.

- When the request is for subscribing to UP path change events of the PDU session, the PCF shall include the information on AF subscription to UP path change events within the PCC rule(s) to request the SMF to create a subscription to such notifications for the AF. In order to do so, the PCF shall include within each PccRule data structure the necessary information to identify the concerned traffic within either the "flowInfos" attribute or the "appId" attribute, and include within the Traffic Control Data decision that the PCC rule refers to the information on AF subscription to events within the "upPathChgEvent" attribute. Within this "upPathChgEvent" attribute, the PCF shall include the "dnaiChgType" attribute to indicate the type of notification (i.e. early notification, late notification or both), the notification URI within the "notificationUri" attribute, the notification correlation Id within the "notifCorreId" attribute, and if the URLLC feature is supported, an indication of AF acknowledgement to be expected within the "afAckInd" attribute. In order to enable the AF to identify the AF request to which the notification corresponds when the AF receives a UP path change notification from the SMF, as defined in clause 4.2.2.2 of 3GPP TS 29.508 [12], the PCF shall set the values of the "notificationUri" attribute and "notifCorreId" attribute respectively as follows:

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

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

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

for the traffic related with the concerned application, no DNAI change takes place once selected initially for this application.

- If the "EASDiscovery" feature is supported and the AF request includes an indication that EAS rediscovery is required, the PCF shall include within the PccRule data instance(s) the necessary information to identify the traffic within the "appId" attribute and the "easRedisInd" attribute set to true.

- If the URLLC feature is supported and the AF request includes an indication that the UE IP address preservation should be considered, the PCF shall include within the concerned PccRule data instance(s) the "addrPreserInd" attribute set to true.

- If the AF request includes an indication that the PDU session should be correlated via a common DNAI for a given traffic, the PCF shall include within the TrafficControlData data instance provisioned for one or more PCC rule(s), the "traffCorreInd" attribute set to true.

- If the feature "SimultConnectivity" is supported and the AF request includes an indication that the simultaneous connectivity may be temporarily maintained for the target and the source PSA during the edge re-location procedure, the PCF may include within the TrafficControlData data instance provisioned for one or more PCC rule(s) the "simConnInd" attribute set to true, as indicated by the AF. If the feature "SimultConnectivity" is supported and the AF request includes the time interval to be considered for inactivity of the traffic routed through the source PSA after which the simultaneous connectivity can be terminated, the PCF may also include the received duration within the "simConnTerm" attribute.

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

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

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

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

- if the PDU Session is of IP type and the "addrPreserInd" attribute is included and set to true in the PCC rule(s), the SMF should preserve the UE IP address and, if necessary, not reselect the related PSA UPF for the traffic identified in the PCC rule once the PSA UPF is selected; otherwise, the SMF (re)selects UPF(s) as it might be required 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).

- determine the target DNAI(s) for the current UE location, which may imply I-SMF selection or removal to be requested to the AMF as defined in 3GPP TS 29.502 [22].

- if the "traffCorreInd" attribute set to true is included in the TrafficControlData data type referenced by a set of PCC rules, based on SMF implementation and local configuration, the SMF should select a common DNAI from the list of DNAI included in the "routeToLocs" attribute for the identified traffic of the PDU session.

- if the "simConnInd" attribute set to true is included in the TrafficControlData data type referenced by a set of PCC rules, the SMF may temporarily maintain simultaneous connectivity for the source and target PSA at edge relocation procedure, and may influence the establishment of a temporary N9 forwarding tunnel between the source UL CL and target UL CL. If the "simConnTerm" attribute is also included, the SMF may consider the indicated time interval as the minimum one to be considered for inactivity for the described traffic before the connectivity over the source PSA may be removed.

- if the "maxAllowedUpLat" attribute is received, SMF may use this value to decide whether edge relocation is needed to ensure that the user plane latency does not exceed the value and whether to relocate the PSA UPF to satisfy the user plane latency.

- if the "easIpReplaceInfos" attribute is received, the SMF may instruct the local PSA UPF with the EAS IP replacement information using "Outer Header Creation" as defined in 3GPP TS 29.244 [13] clause 8.2.56 and "Outer Header Removal" as defined in 3GPP TS 29.244 [13] clause 8.2.64. The PSA UPF shall be configured by the SMF to perform one creation and one removal of the appropriate outer header(s) both in the uplink and in the downlink direction in a way that the address information indicated by the "source" attribute (within "easIpReplaceInfos") is used in the headers of the packets towards the UE and the address information indicated by the "target" attribute (within "easIpReplaceInfos") is used in the headers of the packets towards the DN.

- if the "easRedisInd" attribute set to true is included, the SMF may indicate the UE to refresh the cached EAS information as defined in clause 6.3.2 of 3GPP TS 24.501 [20].

If routing of traffic to a local access to a data network policy provided in the "routeToLocs" attribute is invalid, unknown or not applicable, or the enforcement of the steering of the traffic to the indicated DNAI failed, the SMF shall return a PCC Rule Error Report, as specified in clauses 4.2.3.16 and 4.2.4.15, and set the "failureCode" attribute to "DNAI_STEERING_ERROR".

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 clause 4.2.6.2.1and include within its "refCondData" attribute the value of the "condId" attribute of the targeted ConditionData instance. The PCF shall also ensure that this referenced ConditionData instance is included in the "conds" map attribute within the SmPolicyDecision data structure, following the procedures defined in clause 4.2.6.1.

Within the ConditionData instance, the PCF shall include the activation time within the "activationTime" attribute and/or the deactivation time within the "deactivationTime" attribute.

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

1) If only the "activationTime" attribute is provided by the PCF and the time specified in it is in the future, then the SMF shall set the PCC rule to inactive state and only change it to active state at the specified time. If this time specified in the "activationTime" attribute is in the past, then the SMF shall immediately set the PCC rule to active state.

2) If only the "deactivationTime" attribute is provided by the PCF and the time specified in it is in the future, then the SMF shall set the PCC rule to active state and only change it to inactive state at the specified time. If this time specified in the "deactivationTime" is in the past, then the SMF shall immediately set the PCC rule to inactive state.

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

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

5) If both the "activationTime" attribute and the "deactivationTime" attribute are provided by the PCF and are both in the past, and the value specified in the "activationTime" occurs before the value specified in the "deactivationTime" attribute, then the SMF shall immediately set the PCC rule to inactive state.

6) If both the "activationTime" attribute and the "deactivationTime" attribute are provided by the PCF and are both in the past, and the value specified in the "deactivationTime" attribute occurs before the value specified in the "activationTime" attribute, then the SMF shall immediately set the PCC rule to active state.

7) If both "activationTime" attribute and "deactivationTime" attribute are specified with the same time, the SMF shall report a PCC rule error for the concerned PCC rule(s), as specified in clauses 4.2.3.16 and 4.2.4.15, and set the "failureCode" attribute to "INCORRECT_COND_DATA".

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

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

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

   - the PCF may update the PCC rule by replacing the existing ConditionData instance's "condId" attribute value within the "refCondData" attribute with a another one pointing to another ConditionData instance and including within the SmPolicyDecision data structure this new ConditionData instance within the "conds" attribute, if not previously provisioned; or

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

3) When modifying a PCC rule by deleting the previously provisioned deferred activation time and/or deactivation time:

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

   - the PCF may also delete this condition data decision to which the PCC rule refers as defined in clause 4.2.6.1 (i.e. delete the corresponding ConditionData instance within the SmPolicyDecision data structure), if no other PCC rule is referring to this condition data decision.

To delete a conditioned PCC rule, the PCF shall run the procedures as defined in clause 4.2.6.2.1.

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

The PCC rule(s) including a reference to a Condition Data decision which includes an "activationTime" attribute and/or a "deactivationTime" attribute shall be bound to a QoS flow associated with a default QoS rule that allows all UL packets. If such PCC rule(s) are not bound to a QoS flow associated with a default QoS rule, the SMF shall report a failure to the PCF by including the "ruleReports" attribute with the "failureCode" attribute set to the value "NO_QOS_FLOW_BOUND" for the affected PCC rule(s). Changes of the QoS profile or QoS rule which will initiate signalling towards the access network and/or UE in such PCC rule(s) shall also not be applied.

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

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

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

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

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

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

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

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

4.2.6.2.9 Resource reservation for services sharing priority

When the PCF derives PCC Rules corresponding to a service related to an AF that has indicated that priority sharing is allowed for that service over Rx interface or within the Npcf_PolicyAuthorization service, it derives the corresponding PCC Rules according to current procedures as described in 3GPP TS 29.513 [7], clause 7.3. The PCF may additionally take the suggested pre-emption capability and vulnerability values into account if the AF provided them when the PCF determines the ARP pre-emption capability and vulnerability. The ARP derived at this point and the priority sharing indicator provided over Rx reference point (see 3GPP TS 29.214 [18] for further information) or over the Npcf_PolicyAuthorization service (see 3GPP TS 29.514 [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 [18], clause 4.4.8, or 3GPP TS 29.514 [17], clauses 4.2.2.21, 4.2.3.21 and 4.2.4.9), 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 QoS flow. Furthermore, a combined modification of the ARP parameter in the PCC rules ensures that a QoS flow 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 clause.

The PCF shall provision the PCC Rules according to the rederived ARP information as described in clause 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 clauses 4.2.3.1.6 and 4.2.4.15 (PCC Rule Error Report) and if the PCF supports the MCPTT-Preemption feature as defined in clause 5.4.1 of 3GPP TS 29.214 [18] or in clause 5.8 of 3GPP TS 29.514 [17], the PCF shall check if pre-emption control based on the pre-emption control information provided by the AF as defined in clauses 4.4.1 or 4.4.2 of 3GPP TS 29.214 [18] or in clauses 4.2.2.21, 4.2.3.21 or 4.2.4.9 of 3GPP TS 29.514 [17] applies.

NOTE 2: The PCF determines that pre-emption control applies based on the presence of the Pre-emption-Control-Info AVP received over Rx reference point as defined in 3GPP TS 29.214 [18] or "preemptControlInfo" attribute received over N5 reference point as defined in 3GPP TS 29.514 [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 clauses 4.4.1 or 4.4.2 of 3GPP TS 29.214 [18] or in clauses 4.2.2.21, 4.2.3.21 or 4.2.4.9 of 3GPP TS 29.514 [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 [18], or the "preemptControlInfo" attribute received over N5 interface as defined in 3GPP TS 29.514 [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 [18] or the "preemptControlInfo" attribute received over N5 interface as defined in 3GPP TS 29.514 [17] 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 clauses 4.4.1 or 4.4.2 of 3GPP TS 29.214 [18] or in clauses 4.2.2.21 or 4.2.3.21 of 3GPP TS 29.514 [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 clauses 4.4.1 or 4.4.2 of 3GPP TS 29.214 [18].

NOTE 3: If the PCF receives a report that a PCC rule provisioning or modification failed due to the resource reservation failure and the PCF does not support the MCPTT-Preemption feature as defined in clause 5.4.1 of 3GPP TS 29.214 [18] or clause 5.8 of 3GPP TS 29.514 [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 clauses 4.4.1 or 4.4.2 of 3GPP TS 29.214 [18] or in clauses 4.2.2.21 or 4.2.3.21 of 3GPP TS 29.514 [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 remain on the default QoS flow. The SMF shall then, for the indicated PCC rule, bind it to the default QoS flow until this PCC rule is removed or until the PCF modifies this PCC rule to set the "defQosFlowIndication" attribute to false. For this second case, Tthe SMF case shall evaluate the full QoS information within the QosData data structure to which the PCC rule refers and follow normal policy enforcement procedures for authorized QoS per service data flow as described in clause 4.2.6.2.3.

NOTE: 5QI, ARP, QNC (if available), Priority Level (if available), Averaging Window (if available) and Maximum Data Burst Volume (if available) within the 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 the QoS Data decision or it is included and 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 is provided and set to true within the QosData data structure to which the PCC rule refers, the SMF shall bind the related PCC rule to the default QoS flow. This binding remains valid until the related PCC rule is removed or if the PCF indicates to the SMF that the binding to the default QoS flow for this PCC rule no longer applies.

The SMF shall ignore the values of the other attributes, including 5QI, ARP, QNC (if available), Priority Level (if available), Averaging Window (if available) and Maximum Data Burst Volume (if available), provided within the QosData data structure if the "defQosFlowIndication" attribute is provided by the PCF and set to true. If the PCF has previously indicated to the SMF that a PCC rule shall be bound to the default QoS flow, and desires to indicate that this binding no longer applies the PCF shall update this PCC rule by including the "defQosFlowIndication" attribute set to false. The SMF shall in this case evaluate the full QoS information within the QosData data structure to which the PCC rule refers and follow normal policy enforcement procedures for authorized QoS per service data flow as described in clause 4.2.6.2.3.

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 shall now apply for this

PCC rule, the PCF shall update the PCC rule by including (or updating) the "defQosFlowIndication" attribute and set it to true. The SMF shall in this case follow the procedures described in this clause.

4.2.6.2.11 PCC rule for Application Detection and Control

If the ADC feature is supported, the user subscription indicates that application detection and control is enabled, and the PCF determines that application detection is required because of e.g. an internal/external trigger or the PCF has received from an NF service consumer (e.g. another PCF) a subscription to the event for application start/stop traffic detection (see TS 29.514 [17], clause 4.2.6.9), the PCF may instruct the SMF to detect application(s) by installing or activating PCC rule(s).

An application to be detected is identified by an application identifier, which shall be provided within the "appId" attribute for dynamic PCC rules or pre-provisioned for predefined PCC rules. If the PCF requires to be notified when application start/stop is detected, it shall also provide the APP_STA and APP_STO policy control request triggers to the SMF as defined in clause 4.2.6.4. For dynamic PCC rules, the PCF may also mute such notifications for a specific detected application by including a "traffContDecs" attribute to contain a Traffic Control Data decision which contains the "muteNotif" attribute set to true and including a "refTcData" attribute referring to this Traffic Control Data decision within the concerned PCC rule.

If the application identifier provided in the "appId" attribute is invalid, unknown or not applicable, the SMF shall return a PCC Rule Error Report, as specified in clauses 4.2.3.16 and 4.2.4.15, and set the "failureCode" attribute to "APP_ID_ERR".

In this release of the specification Application Detection and Control applies only to the IP PDU session type.

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 clause 4.2.6.2.1 "Provisioning of PCC rules".

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

When the PCF derives PCC Rules corresponding to non-MPS service, the PCF shall generate the PCC Rules as per normal procedures. At the time the Priority PDU connectivity services is invoked based on the subscription profile stored in the UDR (i.e. Indication for support of Priority PDU connectivity service and MPS Priority Level are set in the UDR) or by the AF (e.g., MPS for DTS is invoked as described in 3GPP TS 29.214 [18] and 3GPP TS 29.514 [17]), the PCF shall upgrade the ARP and/or change 5QI for the PCC Rules to appropriate values as needed for MPS. The PCF shall change the ARP and/or 5QI (also associated QoS characteristics if applicable) modified for the Priority PDU connectivity service to an appropriate value according to PCF decision.

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

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

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

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

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

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

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

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

4.2.6.2.12.2 Invocation/Revocation of Priority PDU connectivity services

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

- Derive the corresponding PCC Rules with the ARP and 5QI (also associated QoS characteristics if applicable) set as appropriate for a prioritized service.
- Set the ARP of the default QoS flow as appropriate for a Priority PDU connectivity services under consideration of the requirement described in clause 4.2.6.2.12.1.
- Set the 5QI (also associated QoS characteristics if applicable) of the default QoS flow as appropriate for the Priority PDU connectivity services.
- Set the ARP of PCC Rules installed before the activation of the Priority PDU connectivity services to the ARP as appropriate for the Priority PDU connectivity services under the consideration of the requirements described in clause 4.2.6.2.12.1.
- Set the 5QI of the PCC Rules installed before the activation of the Priority PDU connectivity services to the 5QI (also associated QoS characteristics if applicable) as appropriate for the Priority PDU connectivity services if modification of the 5QI of the PCC Rules is required.

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

- Delete the PCC Rules corresponding to the Priority PDU connectivity services if they were previously provided.
- Set the ARP of the default QoS flow to the normal ARP under the consideration of the requirements described in clause 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 clause 4.2.6.2.12.1.
- Set the 5QI to an appropriate value according to PCF decision if modification of the 5QI of PCC Rules is required.

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

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

4.2.6.2.12.3 Invocation/Revocation of IMS Multimedia Priority Services

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

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

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

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

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

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

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

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

4.2.6.2.12.4 Invocation/Revocation of MPS for DTS

When the PCF receives from the AF an indication of invocation/revocation of MPS for DTS as specified in 3GPP TS 29.514 [17] or 3GPP TS 29.214[10], and if the "MPSforDTS" feature is supported, the PCF shall make the corresponding policy decisions (i.e. ARP and/or 5QI change for the default QoS) and, if applicable, shall initiate an Npcf_SMPolicyControl_UpdateNotify to provision the modified data.

For the invocation of MPS for DTS, the PCF shall:

- Set the ARP of the default QoS flow as appropriate for MPS for DTS.

- Set the 5QI (also associated QoS characteristics if applicable) of the default QoS flow as appropriate for MPS for DTS.

NOTE 1: For PCC Rules that had the same ARP and 5QI as the original default QoS flow: the PCF indicates to the SMF that the PCC rule is to be bound to the default QoS flow by setting the "defQosFlowIndication" attribute within the QosData data structure to true; or sets the ARP as appropriate for MPS for DTS and the 5QI (also associated QoS characteristics if applicable) as appropriate for MPS for DTS.

For the revocation of MPS for DTS, to revert the MPS for DTS values of the default QoS flow and the PCC rules bound to the default QoS flow, the PCF shall set the ARP and the 5QI of the default QoS flow as appropriate for PCF decision.

NOTE 2: For PCC Rules that had the same ARP and 5QI as the default QoS flow, or had the "defQosFlowIndication" attribute set to true: the PCF sets the ARP; and the 5QI (also associated QoS characteristics if applicable) as appropriate for PCF decision. The provision of the QoS information applicable for the PCC Rules is performed as described in clause 4.2.6.6.

NOTE 3: Revocation may require more complex logic on the part of the PCF beyond simply restoring the prior ARP and 5QI values as set prior to invocation of MPS for DTS, if these values and/or the defQosFlowIndication were modified by another service during the time that MPS for DTS was enabled. The corresponding logic is dependent on the identification of particular services that may be deployed and the desired interactions between MPS for DTS and any such services. These aspects are not considered in the present specification.

The PCF shall provision the SMF upon MPS for DTS invocation and revocation as described above for the default QoS flow as described in clause 4.2.3.6.

On receipt from an AF of a request to report the successful outcome of the MPS for DTS invocation/revocation of priority handling for the default QoS flow (see 3GPP TS 29.214 [18] and 3GPP TS 29.514 [17]), the PCF shall request the SMF to confirm that the resources associated to the MPS for DTS invocation/revocation are successfully allocated. The PCF does this by setting the "policyCtrlReqTriggers" attribute in the "SmPolicyDecision" data structure to the value "SUCC_QOS_UPDATE". On receipt of the "repPolicyCtrlReqTriggers" attribute in the SmPolicyUpdateContextData data structure set to the value "SUCC_QOS_UPDATE" from the SMF, the PCF shall inform the AF that it successfully acted upon the "mpsAction" attribute as defined in 3GPP TS 29.514 [17] or the MPS-Action AVP as defined in 3GPP TS 29.214 [18].

The SMF shall report MPS for DTS invocation/revocation failure to the PCF according to clause 4.2.4.21 if requested to do so by the AF as described in 3GPP TS 29.214 [18], clause 4.4.11 or as described in 3GPP TS 29.514 [17], clause 4.2.2.12.2.

4.2.6.2.13 Sponsored Data Connectivity

Sponsored data connectivity may be performed for service data flows associated with one or more PCC rules if the information about the sponsor, the application service provider and optionally the threshold values are provided by the AF and if the AF has not indicated to disable/not enable sponsored data connectivity as described in 3GPP TS 29.214 [18] clauses 4.4.1 and 4.4.2 or 3GPP TS 29.514 [17] clauses 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 clause 4.2.6.2.1. The sponsor identity shall be set using the "sponsorId" attribute within the ChargingData data type which the PCC rule refers to. The application service provider identity shall be set using the "appSvcProvId" attribute within the ChargingData data type which the PCC rule refers to. The "sponsorId" attribute and "appSvcProvId" shall be set if the "reportingLevel" attribute within the ChargingData data type which the PCC rule refers to is set to the value "SPON_CON_LEVEL".

When receiving the usage thresholds from the AF, the PCF shall use the sponsor identity to generate a value of "umId" attribute of the UsageMonitoringData data type which the PCC rule refers to and request usage monitoring control for the sponsored data connectivity by following the procedures specified in clauses 4.2.6.2.5.

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

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

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

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

- shall disable the usage monitoring for the sponsored data connectivity according to clause 4.2.6.2.5 if it was enabled previously. As a result, PCF gets the accumulated usage of the sponsored data connectivity.

4.2.6.2.14 Support for PCC rule versioning

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

If required by operator policies, the PCF shall assign a content version for each generated PCC rule and shall include the assigned version in the "contVer" attribute included within the PccRule data structure. Upon each PCC rule modification, if the content version was previously assigned to a PCC rule, the PCF shall assign a new content version. In this case, all the content related to that PCC rule shall be included. If the PCF needs to modify the attribute(s) within the PCC rule, the PCF shall include the new content version within the "contVer" attribute together with all modified and unmodified applicable attribute(s) within the PccRule data structure. If the PCF only needs to modify the content of referenced policy decision data and/or condition data for one or more PCC rules, the PCF shall additionally provide the PCC rule(s) which is referring to the modified policy decision data and/or condition data. Within each PCC rule instance, the PCF shall include all unmodified applicable attribute(s) and the new assigned version in the "contVer" attribute. The content version is unique for the lifetime of the PCC rule.

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

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

Whenever the SMF provides a PCC rule report for rules that were provisioned with a content version, the SMF shall include the "contVers" attribute defined in the RuleReport data structure for those corresponding PCC rules. In case it is required to report the content version of multiple PCC rules, the SMF shall use one instance of RuleReport data

structure per PCC rule, and shall include in the "pccRuleIds" attribute only the identifier of the corresponding PCC rule. The SMF may include more than one content version in the "contVers" attribute for the same PCC rule within the corresponding RuleReport instance included in the "ruleReports" attribute (e.g. the SMF has combined multiple PCC rule versions enforcement into one QoS flow operation). In this case, the "ruleStatus" attribute shall indicate the final status of the PCC rule.

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

4.2.6.2.15 Background data transfer support

If the PCF receives Reference Id within the service information from the AF as defined in 3GPP TS 29.514 [17] or 3GPP TS 29.214 [18] or if "EnhancedBackgroundDataTransfer" feature as defined in clause 5.8 is supported and the PCF receives the Reference Id(s) within the PDU session related subscription information from the UDR as defined in 3GPP TS 29.519 [15], the PCF shall retrieve the corresponding transfer policy from the UDR based on the Reference Id(s) as defined in 3GPP TS 29.519 [15]. The PCF shall use the retrieved transfer policy as input for policy decisions (e.g. setting the charging key equal to the charging key of the transfer policy, rule activation/deactivation time according to the time window).

During PDU session establishment, if "EnhancedBackgroundDataTransfer" feature as defined in clause 5.8 is supported and if validation conditions (i.e. Time Window and/or Location Criteria) of the transfer policy are not satisfied then the PCF may reject corresponding SM Policy Association as defined in clause 4.2.2.2 and include in an HTTP "403 Forbidden" response message the "cause" attribute of the ProblemDetails data structure set to "VALIDATION_CONDITION_NOT_MET". And based on this feedback, the SMF shall reject the PDU session setup.

After successful PDU session establishment, if "EnhancedBackgroundDataTransfer" feature as defined in clause 5.8 is supported, PCF may request the PDU session termination if the validation conditions become not satisfied as defined in clause 4.2.3.3. Within the TerminationNotification, the PCF shall include the "cause" attribute set to "VALIDATION_CONDITION_NOT_MET".

If "BDTPolicyRenegotiation" feature as defined in clause 5.8 is supported and if the PCF retrieves the BDT policy and corresponding related information (e.g. network area information, the volume of data to be transferred per UE, etc.) within the BdtData data type, and with the "bdtpStatus" attribute within the BdtData data type set to value "INVALID", the PCF may reject the SM Policy Association establishment or defer to make the policy decisions until the PCF is informed of the result of BDT policy re-negotiation finally. If the PCF determines to reject the SM Policy Association establishment based on the invalid BDT policy, the PCF shall include in an HTTP "403 Forbidden" response message the "cause" attribute of the ProblemDetails data structure set to "INVALID_BDT_POLICY". If the PCF defers to make the policy decisions, then based on the result of the BDT policy renegotiation, the PCF may make the policy decisions or terminate the SM Policy Association as defined in this clause.

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

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

NOTE: The maximum number of packet filters sent to the UE per QoS rule is additionally limited by the access type. When the UE is camping in 5GS the number of packet filters is limited as specified in 3GPP TS 24.501[20].

4.2.6.2.17 Access traffic steering, switching and splitting support

If both the SMF and the PCF support the "ATSSS" feature as defined in clause 5.8, the PCF may enable the control of traffic steering, switching and splitting for a detected service data flow by including MA PDU Session control information within the PCC rule. In order to do so, within the PccRule data structure the PCF:

- may include one reference to the ChargingData data structure within the "refChgN3gData" attribute if the PCF determines that the specific charging parameters used for packets carried via Non-3GPP access. In this case, a "chgDecs" attribute containing the corresponding Charging Data policy decisions shall be included in the SmPolicyDecision data structure if it has not been provided;

- may include one reference to the UsageMonitoringData data structure within the "refUmN3gData" attribute if the PCF determines that the specific usage monitoring parameters used for packets carried via Non-3GPP access. In this case, a "umDecs" attribute containing the corresponding Usage Monitoring Data policy decisions shall be included in the SmPolicyDecision data structure if it has not been provided;

- may include the ATSSS rule application descriptor within "appDescriptor" attribute if the SDF template included in the PCC rule contains an Application Identifier in the "appId" attribute (see clause 4.2.6.2.1). The PCF may retrieve the OS Id(s) from the "UEPolicySet" resource in the UDR as described in 3GPP TS 29.519 [15] to determine, by internal configuration, the OS Application Identifier supported by the OS Id that corresponds to the application identifier included in the SDF template. If no OS Id is available in the UDR, the PCF may use the PEI to determine the OS Id supported by the UE;

NOTE 1: If the PCF does not take into account the received PEI and/or the retrieved OSid(s) to derive the application descriptor, then the PCF can include in the PCC rule multiple application descriptors associated to multiple operating systems.

NOTE 2: If only one UE OSid is stored in the UDR and the PCF takes it into account to derive the application descriptor, then the PCF can omit the OS Id in the application descriptor included in the PCC rule.

- may include the ATSSS policies within the Traffic Control Data decision which the PCC rule refers to. Within the TrafficControlData data structure, based on the ATSSS capability supported for the MA PDU Session, the PCF shall include:

  - the applicable access traffic steering method, "ATSSS_LL" or "MPTCP", for the UL and DL traffic, encoded in the "steerFun" attribute; and

  - the steering rule for access traffic distribution across the 3GPP and Non-3GPP accesses encoded in a "SteeringMode" data structure within the "steerModeDl" attribute for the DL traffic and within the "steerModeUl" attribute for the UL traffic.

The "SteeringMode" data structure shall include:

- the steering mode value determined by the PCF within the "steerModeValue" attribute as follows:

  a. "ACTIVE_STANDBY" indicates the traffic of a SDF is steered on one access (the Active access), when this access is available, and switched to the other access (the Standby access), when Active access becomes unavailable. When the Active access becomes available again, the SDF is switched back to this access. If the Standby access is not defined, then the SDF is only allowed on the Active access and cannot be transferred on another access.

  b. "LOAD_BALANCING" indicates that the traffic of an SDF is split percentually between the 3GPP and Non-3GPP accesses.

  c. "SMALLEST_DELAY" indicates that the traffic of an SDF is steered and/or switched to the access that has the smallest delay (e.g. smallest RTT).

  d. "PRIORITY_BASED" indicates that the traffic of an SDF is steered to the high priority access until the access is determined to be congested. In this case, the traffic of the SDF is also sent to the low priority access, i.e. the SDF traffic is split over the two accesses. When the high priority access becomes unavailable, all SDF traffic is switched to the low priority access. How UE and UPF determine when a congestion occurs on an access is implementation dependent.

- When the access traffic steering mode in the "steerModeValue" attribute is "ACTIVE_STANDBY", the active access encoded within the "active" attribute, and the standby access, if defined, in the "standby" attribute; or

- When the access traffic steering mode in the "steerModeValue" attribute is "LOAD_BALANCING", the traffic load distributed across 3GPP and Non-3GPP accesses encoded within the "3gLoad" attribute as the 3GPP access traffic weight percentage. The sum of the Non-3GPP access traffic weight percentage and the 3GPP access traffic weight percentage must be 100; or

- When the access traffic steering mode in the "steerModeValue" attribute is "PRIORITY_BASED", the high priority access type encoded within the "prioAcc" attribute.

If the EnATSSS feature is supported, the PCF may provide either the steering mode indicator or the authorized threshold values for RTT and/or Packet Loss Rate within the "SteeringMode" data structure as follows:

a. when the access traffic steering mode within the "steerModeValue" attribute is "LOAD_BALANCING" with fixed split percentages or "PRIORITY_BASED", the PCF may provide, within the "thresValue" attribute, the authorized threshold value of RTT encoded in the "rttThres" attribute and/or the authorized threshold value of Packet Loss Rate encoded in the "plrThres" attribute.

   - For "LOAD_BALANCING" steering mode with fixed split percentages (i.e., without the "AUTO_LOAD_BALANCE" or "UE_ASSISTANCE" steering mode indicator), the traffic load distributed across accesses indicated in"3gLoad" attribute shall only apply when the measurement of RTT and/or Packet Loss Rate on both accesses do not exceed the values for RTT and/or Packet Loss Rate provided respectively in the "rttThres" and/or "plrThres" attributes. When at least one measured parameter on one access exceeds the provided threshold value, the UE and UPF may stop sending traffic on this access, or may continue sending traffic on this access, but should reduce the traffic on this access and shall send the amount of reduced traffic on the other access. How UE and UPF adjust the traffic load distributed across accesses is implementation dependent.

   - For "PRIORITY_BASED" steering mode, when the measurement of RTT and/or Packet Loss Rate on the high priority access type exceeds the values for RTT and/or Packet Loss Rate provided respectively in the "rttThres" and/or "plrThres" attributes, this access may be considered as congested by the UE and the UPF. In this case, the traffic of the SDF is also sent to the low priority access.

b. when the access traffic steering mode in the "steerModeValue" attribute is "LOAD_BALANCING", the PCF may provide within the "steerModeInd" attribute:

   - "AUTO_LOAD_BALANCE", when the UE and UPF are allowed to autonomously determine the traffic load of an SDF distributed across accesses; or

   - "UE_ASSISTANCE", when the UE is allowed to decide how to distribute the UL traffic of an SDF and the UE may inform the UPF how it decided to distribute the UL traffic. In the normal cases, although with this indicator provided, the UE shall apply the Steering Mode provided by the network.

When the "steerModeInd" attribute is provided, the traffic load distributed across accesses indicated in "3gLoad" attribute may be ignored by the UE and UPF.

If the value of "atsssCapab" attribute received from the SMF is "MPTCP_ATSSS_LL_WITH_EXSDMODE_DL_ASMODE_UL", the PCF shall provide a PCC Rule for non-MPTCP traffic. To enable non-MPTCP traffic, the PCF shall include a "match all" packet filter within the "flowInfos" attribute, the highest value within the "precedence" attribute of the PCC rule, and within the TrafficControlData data structure referred by the PCC rule, set the "steerFun" attribute to the "ATSSS_LL", the "steerModeValue"attribute of the "steerModeUl" attribute to "ACTIVE_STANDBY", and the "steerModeValue"attribute of the "steerModeDl" attribute to any supported steering mode except the "SMALLEST_DELAY" steering mode.

If the value of "atsssCapab" received from the SMF is "MPTCP_ATSSS_LL_WITH_ASMODE_UL", the PCF shall provide a PCC rule for non-MPTCP traffic. To enable non-MPTCP traffic, the PCF shall include a "match all" packet filter within the "flowInfos" attribute, the highest value within the "precedence" attribute of the PCC rule, and within the TrafficControlData data structure referred by the PCC rule, set the "steerFun" attribute to the "ATSSS_LL", the "steerModeValue"attribute of the "steerModeUl" attribute to "ACTIVE_STANDBY", and the "steerModeValue"attribute of the "steerModeDl" attribute to any supported steering mode.

If the value of "atsssCapab" received from the SMF is "MPTCP_ATSSS_LL_WITH_ASMODE_DLUL", the PCF shall provide a PCC rule for non-MPTCP traffic. To enable non-MPTCP traffic, the PCF shall include a "match all" packet filter within the "flowInfos" attribute, the highest value within the "precedence" attribute of the PCC rule, and within the TrafficControlData data structure referred by the PCC rule, set the "steerFun" attribute to the "ATSSS_LL", the "steerModeValue"attribute of the "steerModeUl" attribute and the "steerModeDl" attribute to "ACTIVE_STANDBY.

If the value of "atsssCapab" received from the SMF is "MPTCP_ATSSS_LL", the PCF shall provide a PCC rule for non-MPTCP traffic. To enable non-MPTCP traffic, the PCF may include a "match all" packet filter within the "flowInfos" attribute, the highest value within the "precedence" attribute of the PCC rule, and within the TrafficControlData data structure referred by the PCC rule, set the "steerFun" attribute to the "ATSSS_LL", the

"steerModeValue"attribute of the "steerModeUl" attribute and the "steerModeDl" attribute to any supported steering mode.

Upon receipt of the PCC rule with the MA PDU Session control information, the SMF shall:

- derive the ATSSS rules to deliver to the UE for UL traffic steering as defined in 3GPP TS 29.502 [22]. When the EnATSSS feature is supported and the SMF received for UL traffic steering either the steering mode indicator within the "steerModeInd" attribute or the threshold value(s) within the "thresValue" attribute, the SMF includes the received steering mode indication or the received threshold value(s) in the derived ATSSS Rule sent to the UE as defined in 3GPP TS 29.502 [22];;

NOTE 3: The Traffic Descriptor in the ATSSS rule is genereated by the SMF from the SDF template of the PCC rule. If the PccRule data structure contains the "flowInfos" attribute, the SMF uses the UL SDF filters for the generation of the IP descriptors or Non-IP descriptors. If the PccRule data structure contains the "appId" attribute, the SMF includes the application descriptors received from the PCF in the "appDescriptor" attribute of the PCC rule.

- derive the QoS profile and provide it to the access network(s) as follows:
  - for a Non-GBR QoS flow,
    a) the SMF shall provide the QoS profile to both access networks if the UE is registered over both accesses during MA PDU Session Establishment procedure;
    b) the SMF shall provide the QoS profile to the access networks over which the user plane resources are activated during MA PDU Session Modification procedure.
  - for a GBR QoS flow,
    a) if the Multi Access policies of the PCC rule indicate the GBR SDF is handled only in one access (i.e. , the SMF shall provide the QoS profile to the access network indicated by the PCC rule;
    b) if the Multi Access policies of the PCC rule indicate the GBR SDF is handled in both accesses, the SMF shall decide to which access network to provide the QoS profile for the GBR SDF based on its local policy (e.g. the local policy is configured the access where the traffic is ongoing according to the Multi Access policies of the PCC rule).
    c) for a GBR QoS flow, traffic splitting is not supported because the QoS profile is provided to a single access network at a given time, and the traffic can be steered or switched as indicated by the "ACTIVE_STANDBY" steering mode. If the SMF receives the report that the current active access is not available from the UPF, the SMF shall perform as follows:
      - if the corresponding PCC rule allows the GBR QoS flow only on this access or if the corresponding PCC rule allows the GBR QoS flow on both accesses but the other access is not available, the SMF shall release the resources for the GBR QoS flow and report to the PCF about the removal of the PCC rule as defined in clause 4.2.4.15.
      - if the corresponding PCC rule allows the GBR QoS flow on both accesses and the other access is available, the SMF shall try to move the GBR QoS flow to the other access. The SMF may trigger a PDU session modification procedure to provide the QoS profile to the other access and release the resources for the GBR QoS flow in the current access.
        - if the QoS notification control is not enabled for the corresponding PCC rule and the other access does not accept the QoS profile, the SMF shall release the resources for the GBR QoS flow and report to the PCF about the removal of the PCC rule as defined in clause 4.2.4.15.
        - if the QoS notification control is enabled for the corresponding PCC rule, the SMF shall notify the PCF within the "qncReports" attribute that the QoS targets of the SDFs are not guaranteed. After the other access accepts the QoS profile, the SMF shall notify the PCF within the "qncReports" attribute that the QoS targets of the SDFs are guaranteed again. If the other access does not accept the QoS profile, the SMF shall delete the GBR QoS flow and report to the PCF about the removal of the PCC rule as defined in clause 4.2.4.15.
- instruct the UPF for DL access traffic steering as defined in 3GPP TS 29.244 [13]. When the EnATSSS feature is supported and the SMF received for DL traffic steering either the steering mode indicator within the

"steerModeInd" attribute or the threshold value(s) within the "thresValue" attribute, the SMF includes the received steering mode indication or the received threshold value(s) in the derived the multi-access rule sent to the UPF as defined in 3GPP TS 29.244 [13];

- apply charging information depending on the used access type if indicated in the PCC rule; and
- apply usage monitoring control depending on the used access type if indicated in the PCC rule.

The PCF may update the steering rule for access traffic distribution across the 3GPP and Non-3GPP accesses for a PCC rule. In order to do so, the PCF may:

- within the corresponding PccRule data structure, include a new reference of a Traffic Control Data decision and provide the Traffic Control Data decision if not provided yet.
- update the Traffic Control Data decision by including the appropriate attribute value(s) within the "steerFun" attribute, "steerModeDl" attribute and/or "steerModeUl" attribute.

4.2.6.2.18 Void

4.2.6.2.19 Provisioning of PCC Rules for Mission Critical Services

4.2.6.2.19.1 General

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

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

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

When the PCF receives an HTTP POST message as defined in clause 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, indication for support of MCS Priority Level. 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 MCS 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 MCS is provided to the PCF through the Nudr service.

Once the PCF receives a notification of a change in Priority PDU connectivity services support, MCS Priority Level and/or IMS priority service support from the UDR, the PCF shall make the corresponding policy decisions (i.e. ARP and/or 5QI (also associated QoS characteristics if applicable) change) and, if applicable, shall initiate an HTTP POST message as defined in clause 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 MCS 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 MCS 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 MCS service. If the ARP pre-emption capability is enabled for any of the authorized PCC rules belonging to an MCS 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 MCS services.

4.2.6.2.19.2 Invocation/Revocation of Priority PDU connectivity services

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

- Derive the corresponding PCC Rules with the ARP and 5QI (also associated QoS characteristics if applicable) set as appropriate for a prioritized service.
- Set the ARP of the default QoS flow as appropriate for a Priority PDU connectivity services under consideration of the requirement described in clause 4.2.6.2.19.1.
- Set the 5QI (also associated QoS characteristics if applicable) of the default QoS flow as appropriate for the Priority PDU connectivity services.
- Set the ARP of PCC Rules installed before the activation of the Priority PDU connectivity services to the ARP as appropriate for the Priority PDU connectivity services under the consideration of the requirements described in clause 4.2.6.2.19.1.
- Set the 5QI of the PCC Rules installed before the activation of the Priority PDU connectivity services to the 5QI (also associated QoS characteristics if applicable) as appropriate for the Priority PDU connectivity services if modification of the 5QI of the PCC Rules is required.

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

- Delete the PCC Rules corresponding to the Priority PDU connectivity services if they were previously provided.
- Set the ARP of the default QoS flow to the normal ARP under the consideration of the requirements described in clause 4.2.6.2.19.1.
- 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 clause 4.2.6.2.19.1.
- Set the 5QI to an appropriate value according to PCF decision if modification of the 5QI of PCC Rules is required.

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

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

4.2.6.2.19.3 Invocation/Revocation of IMS Mission Critical Services

If the PCF receives service information including an MCS 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 clause 4.2.6.2.19.1:

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

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

If the PCF detects that the P-CSCF released all the MCS session and the IMS priority service has been deactivated for the PDU session the PCF shall under consideration of the requirements described in clause 4.2.6.2.19.1:

- delete the PCC Rules corresponding to the IMS Mission Critical Service;
- if required, set the ARP and 5QI of the default QoS flow as appropriate for the IMS Mission Critical set to inactive;
- replace the ARP and 5QI of all PCC Rules assigned to the IMS signalling QoS flow as appropriate when the IMS Mission Critical Service is inactive.

4.2.6.2.20 PCC rules authorization with preliminary service information

If the PCF receives a request for PCC rules for a PDU session from the SMF, while no suitable authorized PCC rules are configured in the PCF or can be derived from service information provisioned by an AF, but the user is allowed to access AF session based services, the PCF may, depending e.g. on the user's subscription details or operator policy, authorise the requested QoS for a timer supervised grace period (the timer started by the PCF by the request from the SMF) to wait for AF service information. If an AF session bound to the same PDU session is ongoing and only preliminary service information was received within this AF session, the PCF shall base the authorization of the requested QoS on the preliminary service information.

NOTE 1: This scenario can for instance be encountered for a UE terminated IMS session establishment or modification with UE initiated resource reservation, refer to 3GPP TS 29.214 [18] or 3GPP TS 29.514 [17]. If the PCF does not authorize a request for PCC rules in this scenario, the IMS session setup can fail.

NOTE 2: During the grace period, the QoS and packet filters requested by the UE need to be authorized even if the user is not allowed to request for resources for services not known to the PCF or if the requested 5QI is not allowed for services not known to the PCF as it is not clear at this point in time whether the UE resource request belongs to an AF session or to a service not known to the PCF.

If the preliminary service information is insufficient to construct appropriate PCC rules or no preliminary service information is available, the PCF shall provide preliminary PCC rules to authorize the UE requested QoS and packet filters. Therefore, the preliminary PCC rules shall contain wildcarded flow description or flow description derived from possible packet filters received as part of the request for PCC rules. The PCF may apply a dedicated charging key value to indicate to the charging subsystem that the charging key is preliminary and may be corrected later on.

NOTE 3: With the dedicated charging key, the PCF instructs the charging subsystem to recalculate the applicable charge for the time when the dedicated charging key value was applied once the dedicated charging key value is replaced with some other value in a new provisioning of PCC rules. For example, if online charging applies, Session Charging with Unit Reservation (SCUR) can be used .When the charging key changes, the SMF will return initially reserved credit units and the CHF then can recalculate the consumed credit units applying the rate derived from the new other charging key value and update the user's credit accordingly.

NOTE 4: A preliminary PCC rule is a normal PCC rule containing preliminary information.

If the PCF receives AF service information while the timer-supervised grace period is running, the PCF shall stop the timer and may derive authorized PCC rules from this service information and update or replace the preliminary PCC rules that were previously provided for the UE requested QoS and packet filters, for instance by choosing service specific QoS parameters and charging keys.

NOTE 5: The dedicated preliminary charging key value that was previously provided by the PCF instructs the charging subsystem to recalculate the applicable charge when the new service specific charging key is provided. The recalculation covers the time when the previous dedicated charging key value was active. The new service specific charging key is applied from that time onwards.

If the timer expires and the PCF has not received any AF service information, the PCF should apply the policy for services not known to the PCF and may downgrade or revoke the authorization for the preliminary PCC rules (previously provided for the UE requested QoS and packet filters) in accordance with the policy for services not known

to the PCF. The PCF should adjust the charging keys within the PCC rules and should downgrade the authorized QoS to the allowed value for the services not known to the PCF, if required.

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 shall include the authorized Session-AMBR within the "authSessAmbr" attribute;
- it shall include the authorized default QoS within the "authDefQos" attribute using the procedure as defined in clause 4.2.6.3.3;
- it may include one reference to the UsageMonitoringData data structure within the "refUmData" attribute. In this case, a "umDecs" attribute containing the corresponding Usage Monitoring data policy decisions shall be included in SmPolicyDecision data structure if it has not been previously provided;
- if the "ATSSS" feature is supported, it may include one reference to the UsageMonitoringData data structure to apply for the Non-3GPP access within the "refUmN3gData" 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 not been previously 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 not been previously 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 attribute(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 ensure that one and only one session rule is enforced in the SMF at a certain point in time.

NOTE: Either there is always an unconditional session rule provisioned in the NF service consumer (SMF), or there is always a conditioned session rule applicable in the NF service consumer (SMF).

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 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 clause 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 clause 4.2.6.1 and that the referenced usage monitoring data is the same for all the provisioned conditioned and non-conditioned session rule(s).

Within the ConditionData instance, the PCF shall include the activation time within the "activationTime" attribute for the time conditioned authorized Session-AMBR and authorized default QoS (deactivation time does not apply for a session rule). If the "AccessTypeCondition" feature as defined in clause 5.8 is supported, the PCF may include for the access type conditioned session rule the access type within the "accessType" attribute and RAT type within the "ratType" attribute if applicable for the access type conditioned authorized Session-AMBR.

NOTE 1: The SMF retains remaining time conditioned session rules that have an execution time in the future.

NOTE 2: Time condition and access type condition can both apply to authorize the Session-AMBR within a session rule.

The PCF shall ensure that a time conditioned session rule and a session rule without time condition for the same session differ only in the authorized session-AMBR and authorized default QoS properties.

When the SMF detects that the referenced usage monitoring data of the enforced session rule is not the same for all the provisioned session rule(s) the SMF shall report the session rule error for the not enforced session rule(s) as defined in clauses 4.2.3.20 and 4.2.4.21, and shall set the "failureCode" attribute to "INCORRECT_UM".

If the SMF receives the conditioned session rule, when the condition indicated in the related attribute(s) within the Condition Data decision (e.g. at the time indicated in the "activationTime" attribute) is met, the SMF shall perform the conditional policy without interaction with the PCF. If the Condition Data decision includes more than one type of conditions and all the types of conditions are met, the SMF shall perform the conditional policy.

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

The PCF may modify a currently installed session rule, including setting, modifying or deleting its condition(s) as follows:

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

2) When modifying a session rule by modifying the condition(s):

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

   - the PCF may update the condition data decision which the session rule refers to by updating the corresponding ConditionData instance as defined in clause 4.2.6.1. The PCF may update the value of the condition within the related attribute (e.g. the value of the existing deferred activation time within the "activationTime" attribute).

3) When modifying a session rule by deleting the condition(s):

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

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

To delete a conditioned session rule, the PCF shall perform the deletion of session rule as defined in clause 4.2.6.3.1. The "ueTimeZone" attribute, if available, may be used by the PCF to derive the value for the "activationTime" attribute.

NOTE 3: Conditioned Session-AMBR and default QoS change helps reducing the signalling 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 signalling storm in the 5GC (e.g. over N1/N2/N4/N11). The PCF can avoid this simultaneous change of the Session-AMBRSession-AMBR and default QoS (e.g. spread the time conditioned change over time for many UEs).

NOTE 4: For services that depend on specific Session-AMBR and/or default QoS change (e.g. an MPS session), the PCF is responsible to ensure that no conditioned session rules interfere with the service (e.g., ensure proper MPS operation by removing time conditioned settings that would later impact MPS).

4.2.6.3.2.2 Time conditioned authorized Session-AMBR

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

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

If the "VPLMN-QoS-Control" feature is supported and the PCF receives the session AMBR constraints from the SMF, the PCF shall ensure that the authorized session AMBR value within each instance of the session rule does not exceed the session AMBR supported by the VPLMN, if applicable.

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 clause 4.2.6.3.2.1 apply with clarifications in the present clause.

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

If the "VPLMN-QoS-Control" feature is supported and the PCF receives the default QoS constraints from the SMF, the PCF shall ensure that the authorized default QoS containing a 5QI and ARP value within each instance of the session rule is supported by the VPLMN, if applicable.

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

4.2.6.3.2.4 Access type conditioned authorized Session-AMBR

The SMF shall enforce the Session-AMBR values corresponding to the session rule whose referred ConditionData instance contains the "accessType" attribute and "ratType" attribute matching the current access type and RAT type of the UE for the given PDU session. If the "VPLMN-QoS-Control" feature is supported and the PCF receives the session AMBR constraints from the SMF, the PCF shall ensure that the authorized session AMBR value within each instance of the session rule does not exceed the session AMBR supported by the VPLMN, if applicable.

The PCF shall ensure that an access type conditioned session rule and a session rule without any access type condition for the same session differ only in the authorized session-AMBR property. If more than one access type conditioned session rules are provisioned, and if there is no session rule without any access type condition provisioned in the SMF, the PCF shall ensure that any two access type conditioned session rules for the same session differ only in the authorized session-AMBR property.

NOTE: Access type conditions are only applicable to the authorized session-AMBR.

If there is a session rule whose authorized Session-AMBR does not depend on any access type condition provided and there is also a session rule with an access type conditioned authorized Session-AMBR provided, then the access type conditioned session rule where the conditions specified within the Condition Data decision are met shall be enforced. Otherwise, the session rule with the authorized Session-AMBR without any access type condition shall be enforced.

If conditions from multiple access type conditioned the session rule with authorized Session-AMBR are met at the same time then the session rule related to the most strict matching condition is enforced, e.g. Policy1 specifies access type only and Policy2 specifies access type (with the value same as in Policy1) and an RAT Type, both, then the Policy2 shall be enforced when the UE's current access type and RAT type matches with the condition specified by Policy2.

If conditions from multiple access type conditioned the session rule with authorized Session-AMBR are met at the same time and all of these policies are equally applicable, e.g. Policy1 specifies access type only and Policy2 specifies RAT type only and if the UE's current access type matches with Policy1 and the UE's current RAT type matches with Policy2, then the SMF should apply the Session-AMBR with Policy2.

An access type conditioned session rule does not apply to a MA PDU session. When the "ATSSS" feature is supported, and the PDU session is a MA PDU session, the PCF shall not provide to the SMF access type conditioned session rules. If access type conditioned session rules are provisioned in the SMF for a MA PDU session (e.g. because of error in the PCF or EPS to 5GS handover) they shall be ignored.

4.2.6.3.3 Provisioning of authorized default QoS

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

In order to provision authorized default QoS for a new session rule, the PCF shall include the assigned 5QI value within the "5qi" attribute and the assigned ARP value within the "arp" attribute in the AuthorizedDefaultQos data structure. The PCF may include the "priorityLevel" attribute in the AuthorizedDefaultQos data structure to authorize the particular 5QI priority level to override the default value for a standardized or pre-configured 5QI. The PCF may include a "QosCharacteristics" entry in the "qosChars" attribute map to provide explicitly signalled QoS characteristics associated with a 5QI that is neither standardized nor pre-configured. When the authorized default QoS applies to explicitly signalled QoS Characteristics, it shall be provisioned as defined in clause 4.2.6.6.3. For 5QI of GBR type or delay critical GBR type, the PCF shall additionally include max bandwidth in uplink within the "maxbrUl" attribute and/or max bandwidth in downlink within the "maxbrDl" attribute, the guaranteed bandwidth in uplink within the "gbrUl" attribute and/or the guaranteed bandwidth in downlink within the "gbrDl" attribute and may include the particular averaging window within the "averWindow" attribute and/or particular maximum data burst volume within the "maxDataBurstVol" or "extMaxDataBurstVol" (if supported, see clause 4.2.2.1) attribute to override the default values for a standardized or pre-configured 5QI.

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

4.2.6.3.4 Access traffic steering, switching and splitting support

If both the SMF and the PCF support the "ATSSS" feature, the PCF may enable the control of the PDU session level Usage Monitoring information depending on what access type is used to carry service data flows.

When the PCF determines that at PDU session level different usage monitoring data shall be defined for the 3GPP and the Non-3GPP access, the PCF shall include within the SessionRule data structure one reference to the UsageMonitoringData policy decision to apply for the Non-3GPP access within the "refUmN3gData" attribute, and a "umDecs" attribute containing the corresponding Usage Monitoring Data policy decisions if it has not been previously provided. When the "refUmN3gData" is omitted, the attribute "refUmData" contains the reference to the UsageMonitoringData policy decision to apply for both, 3GPP and Non-3GPP, accesses.

NOTE: To ensure that the traffic of a set of service data flows is excluded for both, the 3GPP access and Non-3GPP access, from the PDU session level usage monitoring, the "exUsagePccRuleIds" attribute is set to the same value within the Usage Monitoring Control decision referred by the "refUmN3gData" attribute and within the Usage Monitoring Control decision referred by the "refUmData" attribute.

4.2.6.3.5 Usage Monitoring Control

Usage monitoring may be performed for all the traffic of a PDU session in the SMF or for all the traffic of a PDU session excluding the traffic of a service data flow or a group of service data flows.

The provisioning of usage monitoring control for the traffic of a PDU session shall be performed using the session rule provisioning procedure as defined in clause 4.2.6.3.1. When the traffic of a service data flow or a group of service data flows is excluded from the traffic of the PDU session, the UsageMonitoringData policy decision referred within the "refUmData" attribute, and/or the UsageMonitoringData policy decision referred within the "refUmN3gData" attribute when the "ATSSS" feature is supported, shall include the "exUsagePccRuleIds" attribute as defined in clause 4.2.6.5.3.1.

Usage monitoring for all the session rules (conditioned and non-conditioned) shall refer to the same UsageMonitoringData policy decision(s), i.e., the monitoring key that applies to all the traffic of a PDU session, or to all the traffic of a PDU session except certain service data flow(s), shall not change because of the activation of a conditioned session rule.

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 within the SmPolicyDecision data structure.

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

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

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

4.2.6.5 Encoding of the request of information reporting

4.2.6.5.1 Request of Access Network Charging Identifier

When the Access Network Charging Identifier is unknown for an AF session to the PCF, the PCF may request the SMF to provide the Access Network Charging Identifier associated to the dynamic PCC rules. To do so, the PCF shall within SmPolicyDecision data structure provide the "policyCtrlReqTriggers" attribute with the value "AN_CH_COR" if the policy control request trigger is not previously set and the "lastReqRuleData" attribute. For the RequestedRuleData instance, the PCF shall include the CH_ID within the "reqData" attribute and reference of the PCC rule within 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 as defined in clause 4.2.2.11 and 4.2.4.13.

4.2.6.5.2 RAN NAS Cause Support

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

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

4.2.6.5.3 Provisioning of the Usage Monitoring Control Policy

4.2.6.5.3.1 General

The PCF may indicate the need to apply monitoring control of the accumulated usage of network resources on a per 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 to a single service data flow, a set of service data flows or all the traffic in a PDU session. If usage monitoring at 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 usage monitoring at PDU session level.

During PDU session establishment, the PCF may receive information from the UDR about total the allowed usage per DNN / S-NSSAI combination and UE, i.e. the overall amount of allowed traffic volume and/or time of usage that are to

be monitored per DNN / S-NSSAI combination and UE and/or the total allowed usage for Monitoring key(s) per DNN / S-NSSAI combination and UE.

NOTE 1: It depends on the implementation of UDR whether to provide the total allowed usage per DNN / S-NSSAI combination and UE to different PCFs if these different PCFs are serving PDU sessions with the same value of DNN / S-NSSAI combination and UE.

If the SMF supports the UMC feature, the PCF may request usage monitoring control for a PDU session. If at that time the PCF has not provided "US_RE" policy control request trigger to the SMF, the PCF shall include the "policyCtrlReqTriggers" attribute with the value "US_RE" and provide it to the SMF as defined in clause 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 to the SMF, for each usage monitoring control instance, the applicable threshold(s), i.e. volume threshold, time threshold or both volume threshold and time threshold. To provide the initial threshold(s) for each usage monitoring control instance, the PCF shall include these threshold(s) within the "umDecs" attribute within the SmPolicyDecision data structure.

The PCF may provide a monitoring time to the SMF for the usage monitoring control instance(s) and optionally specify a subsequent threshold value for the usage after the monitoring time.

Threshold levels may be defined for:

- the total volume only; or
- the uplink volume only; or
- the downlink volume only; or
- the uplink and downlink volume; and/or
- the time.

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

- the total volume threshold, if applicable, within the "volumeThreshold" attribute;
- the uplink volume threshold, if applicable, within the "volumeThresholdUplink" attribute;
- the downlink volume threshold, if applicable, within the "volumeThresholdDownlink" attribute;
- the time threshold, if applicable, within the "timeThreshold" attribute;
- . the total volume threshold after the monitoring time, if applicable, within the "nextVolThreshold" attribute;
- the uplink volume threshold after the monitoring time, if applicable, within the "nextVolThresholdUplink" attribute;
- the downlink volume threshold after the monitoring time, if applicable, within the "nextVolThresholdDownlink" attribute;
- the time threshold after the monitoring time, if applicable, within the "nextTimeThreshold" attribute;
- the monitoring time, if applicable, within the "monitoringTime" attribute;
- the inactive time, if applicable, within the "inactivityTime" attribute.

If the SMF reports usage before the monitoring time is reached, the monitoring time is not retained by the SMF. Therefore, the PCF may again provide in the response a monitoring time and optionally the subsequent threshold value(s) for the usage after the monitoring time.

The "inactivityTime" attribute represents the time interval after which the time measurement shall stop for the Monitoring Key, if no packets belonging to the corresponding Monitoring Key are received. Time measurement shall resume again on receipt of a further packet belonging to the Monitoring Key. Time measurement for a Monitoring key shall also be stopped when time based usage monitoring is disabled, if this happens before the Inactivity Detection Time is reached. If an "inactivityTime" attribute with value of zero is provided, or if no "inactivityTime" attribute is present within the usage monitoring control instance provided by the PCF, the time measurement shall be performed

continuously from the point the first packet is received matching the applicable Monitoring Key is received and until time based usage monitoring is disabled.

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 the related 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 the related PCC rule(s).

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

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

The PCF may provide new volume threshold(s) and/or a new time threshold to the SMF. The new threshold value(s) override the existing value(s) in the SMF.

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

If the reset time of the usage monitoring related information (see clause 5.4.2.7 of 3GPP TS 29.519 [15]) is reached, the PCF shall reset the remaining allowed usage to the value(s) indicated in the usage monitoring related information and shall then interact with the SMF to undo any previously applied policy decisions related to remaining allowed usage of zero (or below zero).

NOTE 2: The PCF can also update the related usage monitoring information in the UDR as defined in 3GPP TS 29.519 [15] according to the performed reset action.

4.2.6.5.3.2 Disabling Usage Monitoring

After usage monitoring is enabled, the PCF may explicitly disable usage monitoring as a result of receiving an SM Policy association update from the SMF which is not related to reporting usage, but to other external triggers (e.g., receiving an AF request, subscriber profile update), or a PCF internal trigger. When the PCF disables usage monitoring, the SMF shall report the accumulated usage which has occurred while usage monitoring was enabled since the last report.

To disable usage monitoring for a monitoring key, the PCF shall provide either the SMF with the corresponding applicable attributes of the usage monitoring control instance containing a NULL value (e.g. the previous provided "volumeThreshold" is set to NULL"), or:

- for dynamic PCC rule(s) or session rule(s), remove the reference to the corresponding usage monitoring control instance from all the dynamic PCC rule(s) or session rule(s) referencing it;

NOTE: The PCF could keep the UsageMonitoringData policy decision valid in the SMF.

- for predefined PCC rule(s), remove the UsageMonitoringData policy decision referred from all the activated predefined PCC rule(s).

When the PCF disables usage monitoring for usage monitoring key(s) via a Npcf_SMPolicyControl_UpdateNotify or a Npcf_SMPolicyControl_Update service operation, the SMF shall trigger a new Npcf_SMPolicyControl_Update service operation using the procedures specified in clause 4.2.4.10 to report accumulated usage for the disabled usage monitoring key(s).

4.2.6.5.3.3 PCF Requested Usage Report

When usage monitoring is enabled, the PCF may request the SMF to report the accumulated usage for one or more enabled usage monitoring control instance(s) regardless of whether associated usage threshold(s) have been reached or not. In order do so, the PCF shall include the "lastReqUsageData" attribute containing one or more reference(s) to usage

monitoring data decision(s) within the "refUmIds" attribute or the "allUmIds" attribute set to true in an HTTP POST request or in the response of an HTTP POST request from the SMF. The PCF shall require the SMF to report accumulated usage for one or more enabled usage monitoring control instance(s) only in a response to received HTTP POST request from the SMF when the SMF has not provided accumulated usage in this HTTP POST request for the same usage monitoring control instance(s).

4.2.6.5.4 Request for Access Network Information

When the NetLoc feature is supported, if the AF requests the PCF to report the access network information as described in clauses 4.2.2, 4.2.3 or 4.2.4 of 3GPP TS 29.514 [17] or in clauses 4.1 and 4.2 of 3GPP TS 29.214 [18], the PCF shall perform the PCC rule provisioning procedure as defined in clause 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 29.214 [18], 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.

For those PCC Rule(s) based on AF signalling as described in 3GPP TS 29.514 [17] or in 3GPP TS 29.214 [18], the PCF may use 5QI and ARP for AF signalling to avoid signalling to the UE. These PCC Rules shall not include the "packetFilterUsage" attribute set to true within the "flowInfos" attribute.

NOTE: Similarly, for predefined PCC rules based on AF signalling, these PCC Rule(s) could be defined with the 5QI and ARP for AF signalling, and cannot include packet filter usage information.

4.2.6.5.5 Request for the successful resource allocation notification

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

4.2.6.5.6 Provisioning of Presence Reporting Area Information

When the PRA or ePRA feature is supported, the PCF may determine during the lifetime of the PDU session whether reports on the change of UE presence in Presence Reporting Area(s) are desired for this PDU session based on the subscriber's profile configuration. If such reporting is desired for a PDU session, the PCF shall provide the "praInfos" attribute within the SmPolicyDecision data structure. Within each associated PresenceInfoRm data structure, the PCF shall include the Presence Reporting Area Identifier within the "praId" attribute, and, for a UE-dedicated Presence Reporting Area, the list of elements composing the presence reporting area within the "trackingAreaList" attribute, the "ecgiList" attribute, the "ncgiList" attribute, the "globaleNbIdList" attribute and/or the "globalRanNodeIdList" attribute. The PCF shall also activate the reporting of the changes of UE presence in the provided Presence Reporting Area(s) by provisioning the "PRA_CH" policy control request trigger to the SMF, within the "policyCtrlReqTriggers" attribute.

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

If the PCF is configured with a Presence Reporting Area identifier referring to a list of Presence Reporting Area Identifier(s) within a Set of Core Network predefined Presence Reporting Areas as defined in 3GPP TS 23.501 [2], the PCF shall include only the identifier of the Presence Reporting Area Set within the "praId" attribute.

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

The PCF may modify the list of PRA Identifier(s) by providing new Presence Reporting Area(s) or removing existing Presence Reporting Area(s), or modify the list of Presence Reporting Area element(s) by providing the updated Presence Reporting Area(s). In order to do that,

- when the PRA feature is supported, the PCF shall follow the general procedure defined in clause 4.2.6.1 and supply the Presence Reporting Area identifier(s) as key(s) of "praInfos" the map attribute; or

- when the ePRA feature is supported, the PCF shall follow the general procedure defined in clause 4.2.6.1 and supply the Presence Reporting Area identifier(s) as key(s) of "praInfos" map, with the exception that for the modification of the list of the Presence Reporting Area element(s) the PCF shall fully replace the Presence Reporting Areas(s) previously provided with the new complete list of Presence Reporting Area element(s).

NOTE 3: When the PRA feature is supported, the PCF cannot indicate the SMF to remove an existing Presence Reporting Area element(s) from a Presence Reporting Area by providing the updated Presence Reporting Area as defined in clause 4.2.6.1. How to support it depends on implementation.

When PRA or ePRA feature is supported, the PCF may remove the associated policy control request trigger (i.e. "PRA_CH") as defined in clause 4.2.6.4, if previously activated.

If the NF service consumer and the PCF support both PRA and ePRA features, the NF service consumer and PCF shall perform the behaviours as the ePRA feature defined.

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

NOTE 4: For all the Presence Reporting Area(s) provided by the PCF, the SMF can store the Presence Reporting Area Identifier(s) together with an indication that states that it relates to PCF requested PRA status changes.

NOTE 5: This information is needed so that if both the PCF and the CHF request the reporting of PRA status changes, the SMF is able to differentiate whether the reported PRA changes are relevant to the PCF or the CHF.

The SMF shall invoke the Namf_EventExposure service in the AMF to handle the subscription to the presence state of a UE in an area of interest as specified in 3GPP TS 29.518 [36].

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

The SMF shall remove the Namf_EventExposure service subscription with the AMF for the reporting of Changes of UE presence in Presence Reporting Area(s), when the PCF and CHF remove the associated request triggers.

4.2.6.5.7 Policy provisioning and enforcement of reflective QoS

If the PCF receives the "refQosIndication" attribute set to true as defined in clauses 4.2.2.2 or 4.2.4.2, and if the PCF determines that Reflective QoS Control will be enabled for the PDU session based on the operator's policy and user subscriptions, the PCF may provision the Reflective QoS Timer by including the "reflectiveQoSTimer" attribute within the SmPolicyDecision data structure in the response message.

The provisioning of reflective QoS may be performed for service data flows associated with one or more PCC rules, and shall be performed using the PCC rule provisioning procedure. The PCF may within a QoS data decision which a PCC rule refer to include the "reflectiveQos" attribute set to true to enable the Reflective QoS control to a non-GBR downlink service data flow when the PCF authorizes the QoS for the service data flow as defined in clause 4.2.6.6.2.

The PCF shall ensure that both, uplink and downlink traffic for such non-GBR service data flow are allowed.

NOTE 1: The PCF can allow both uplink and downlink traffic for the non-GBR service data flow in several ways, e.g. by installing a PCC rule with uplink and downlink flow information, or by installing separate PCC rules for the uplink flows and downlink flows, or by installing a PCC rule with only the application identifier.

The PCF shall activate the reporting changes of reflective QoS indication by provisioning the "REF_QOS_IND_CH" policy control request trigger to the SMF.

NOTE 2: While the UE applies a standardized value for the precedence of all UE derived QoS rules, PCC rules precedence values can vary and PCF configuration has to ensure that there is a large enough value range for the precedence of PCC rules corresponding to UE derived QoS rules. To avoid that the precedence of network provided QoS rules need to be changed when Reflective QoS is activated and filters are overlapping, the PCF will take the standardized value for the precedence of UE derived QoS rules into account and will setting the precedence value of PCC rules subject to Reflective QoS to a value in the range from 70 to 99 (decimal), as specified in 3GPP TS 24.501 [20], clause 6.2.5.1.1.3.

The SMF shall apply reflective QoS control for the downlink traffic of the service data flows of the PCC rules that reference a QosData decision that includes "reflectiveQos" attribute set to true.

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

If the PCF receives the "refQosIndication" attribute set to false as defined in clause 4.2.4.2, the PCF shall disable the reflective QoS Control for the PDU session. In order to do so, the PCF shall within the QoS data decision which affected PCC rule refer to include the "reflectiveQos" attribute set to false and may update other QoS parameters within the QoS data decision and/or update the flow information of PCC rule by including the "packetFilterUsage" attribute set to true.

4.2.6.6 Authorized QoS

4.2.6.6.1 General

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

- When the authorized QoS applies to a PCC rule, it shall be provisioned within the corresponding PCC rule as defined in clause 4.2.6.6.2.
- When the authorized QoS for a PCC rule with a GBR QCI is candidate for resource sharing an instruction on the allowed sharing may be provisioned as defined in clause 4.2.6.2.8.
- When the authorized QoS applies to a PDU session, it shall be provisioned as defined in clause 4.2.6.3.1.
- When the authorized QoS applies to the default QoS flow, it shall be provisioned as defined in clause 4.2.6.3.1.
- When the authorized QoS applies to an explicitly signalled QoS Characteristics, it shall be provisioned as defined in clause 4.2.6.6.3.
- When the authorized QoS applies to the Reflective QoS, it shall be provisioned as defined in clause 4.2.6.5.7.

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

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

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

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

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

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

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

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

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

The authorized QoS per service data flow shall be provisioned within a QosData data structure. The PCF shall include a "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.

When network slice data rate policy control applies and the authorized QoS per service data flow refers to a 5QI of GBR type, the PCF shall derive the authorized QoS per service data flow as described in clause 4.2.6.8.

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

Within the QoS data decision, for 5QI of non-GBR type, the PCF shall include the authorized non-GBR 5QI within the "5qi" attribute and the ARP within the "arp" attribute. The PCF may authorize the max bandwidth in uplink within the "maxbrUl" attribute and/or max bandwidth in downlink within the "maxbrDl" attribute.

When the PCF authorizes a standardized 5QI but a Priority Level, an Averaging Window and/or a Maximum Data Burst Volume which are different from the standardized value in the table 5.7.4-1 of 3GPP TS 23.501 [2] are required, the PCF shall include the Priority Level within the "priorityLevel" attribute, the Averaging Window within the "averWindow" attribute and/or the Maximum Data Burst Volume within the "maxDataBurstVol" attribute or the "extMaxDataBurstVol" attribute (if supported, see clause 4.2.2.1).

NOTE 1: For the non-standardized or non-configured 5QI, the PCF needs to authorize explicitly signalled QoS Characteristics associated with the 5QI if the PCF has not provisioned it.

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

NOTE 2: If CHEM feature is supported, then PCF as described in clause 7.2.3 of 3GPP TS 29.513 [7] or based on local configuration, the PCF sets the downlink and uplink maximum packet loss rates corresponding to either the most robust codec mode or the least robust codec mode of the negotiated set in each direction.

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

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

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

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

4.2.6.6.3 Policy provisioning and enforcement of authorized explicitly signalled QoS Characteristics

The PCF may provision a dynamically assigned 5QI value (from the non-standardized and non-preconfigured value range) and the associated 5G QoS characteristics to the SMF. In order to do so, the PCF shall include within the SmPolicyDecision data structure the "qosChars" attribute to contain one or more authorized signalled QosCharacteristics instance(s). For each QosCharacteristics instance, the PCF shall include the assigned 5QI value within the "5qi" attribute, the resource type value within the "resourceType" attribute, the 5QI Priority Level value within the "priorityLevel" attribute, the Packet Delay Budget value within the "packetDelayBudget" attribute, the Packet Error Rate value within the "packetErrorRate" attribute, the Averaging Window value within the "averagingWindow" attribute, if applicable, and the Maximum Data Burst Volume value within the "maxDataBurstVol" attribute or the "extMaxDataBurstVol" attribute (if supported, see clause 4.2.2.1), if applicable. If the PCF has provisioned an authorized signalled QosCharacteristics instance to the SMF, the PCF shall not update nor remove it during the lifetime of the policy association.

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

NOTE: Operator configuration is assumed to ensure that the assigned dynamic 5QI value is unique and references the same set of QoS characteristics within the whole PLMN at a given time.

4.2.6.7 Monitoring the data rate per network slice for a UE

The PCF can support monitoring of data rate per S-NSSAI for a UE.

During PDU session establishment, if the PCF supports monitoring of the data rate per S-NSSAI for a UE, the PCF may retrieve for the UE and S-NSSAI to which the PDU session is allocated the UE-Slice-MBR (i.e. the aggregate data rate that can be expected to be provided across all GBR and Non-GBR QoS Flows of a UE for a network slice identified by an S-NSSAI) from the UDR as defined in clause 5.4.2.14 of 3GPP TS 29.519 [15]. The PCF shall monitor the data rate for this S-NSSAI and UE by deriving the utilized data rate based on the authorized Session-AMBR and/or the authorized QoS per service data flow in all PDU session(s) established for the UE in the concerned S-NSSAI and checking the derived value against the UE-Slice-MBR set by the PCF based on the UE-Slice-MBR value retrieved from the UDR and operator policies available at the PCF.

As part of the PDU session modification procedure(s) targeting the PDU session(s) established for the UE in the concerned S-NSSAI, whenever the PCF needs to provide the associated authorized Session-AMBR(s), install new or updated PCC Rule(s) and/or delete PCC Rule(s) related to GBR service data flow(s), the PCF shall calculate the utilized data rate as described in clause 4.2.6.8.2.

At the termination of a PDU session established for the UE in the concerned S-NSSAI, the PCF shall adjust the utilized data rate for the UE based on the release of the Session-AMBR and the removal of all the PCC Rule(s) related to GBR service data flow(s) associated to that PDU session.

To enable this monitoring, the SMF shall select the same PCF instance for all PDU sessions of the UE to the S-NSSAI that is subject to this monitoring as defined in clause 8.3 of 3GPP TS 29.513 [7].

When the calculated utilized data rate for the S-NSSAI and UE reaches a certain percentage of the UE-Slice-MBR value, the PCF may apply a policy decision to strengthen the traffic restrictions for individual PDU session(s) or PCC rule(s) (e.g. change the authorized Session-AMBR as defined in clause 4.2.6.3.1, change the authorized QoS per service data flow as defined in clause 4.2.6.6.2, or change the charging keys) within individual PDU session(s) established for the UE in the concerned S-NSSAI. When the calculated utilized data rate per S-NSSAI for a UE falls below that percentage of the UE-Slice-MBR value, the PCF may relax the traffic restrictions for individual PDU session(s) or PCC rule(s) within individual PDU session(s) established for the UE in the concerned S-NSSAI.

As part of the policy decision to strengthen the traffic restrictions for individual PDU session(s), the PCF may reject the establishment or SMF-initiated modification of the associated SM Policy Association(s) with an HTTP "403 Forbidden" response message including the "cause" attribute of the ProblemDetails data structure set to "EXCEEDED_UE_SLICE_DATA_RATE".

NOTE: It is recommended to avoid frequent policy decisions which trigger a signalling with the UE (like change of the authorized Session-AMBR or change of the authorized QoS per service data flow).

4.2.6.8 Network slice related data rate policy control

4.2.6.8.1 General

A PCF that supports network slice related data rate policy control shall be able to control and manage the network slice data rate.

A Maximum Slice Data Rate may be configured by the operator (e.g. based on an SLA related to the associated network slice identified by an S-NSSAI).

NOTE 1: The Maximum Slice Data Rate defines the maximum allowed aggregate data rate across all GBR and Non-GBR QoS Flows within the network slice identified by an S-NSSAI as defined in 3GPP TS 29.519 [15].

NOTE 2: The maximum data rate of Non-GBR QoS Flow(s) is controlled via the authorized Session-AMBR, while the maximum data rate of a GBR QoS Flow is controlled via the authorized MBR value of the associated PCC rule.

The PCF shall determine, based on local configuration, if the network slice data rate is controlled via PCF-based monitoring by using QoS parameters or with assistance of the NWDAF.

The PCF shall monitor the data rate of the network slice and ensure that it does not exceed the Maximum Slice Data Rate for that network slice by e.g. rejecting new SM Policy Associations, changing the authorized Session-AMBR values (if allowed by the HPLMN), changing the MBR values in PCC rules belonging to GBR service data flows or other actions depending on operator's policies.

NOTE 3: Based on operator's policies, it is also possible for the PCF to accept that new PDU session(s) or PCC rule(s) belonging to GBR service data flow(s) lead to exceeding the Maximum Slice Data Rate and apply a different charging for them. Once the Maximum Slice Data Rate is no longer exceeded, the PCF can decide to go back to applying the previous charging.

NOTE 4: Subject to operator policy and national/regional regulations, prioritised services and emergency services may be exempted from network slice data rate policy control.

NOTE 5: A single PCF can be used for the monitoring and limitation of the network slice related data rate. To enable this, the SMF has to select the same PCF instance for all PDU Sessions of the UE to the S-NSSAI.

4.2.6.8.2 PCF-based network slice data rate policy control by using QoS parameters

If the NWDAF is not deployed or not used for network slice data rate policy control and PCF-based monitoring of network slice data rate by using QoS parameters applies, the UDR shall maintain the Remaining Maximum Slice Data Rate per S-NSSAI as part of the network slice specific policy control data as defined in 3GPP TS 29.519 [15].

Whenever the PCF needs to calculate the data rate related to authorized Session-AMBR and/or the MBR(s) of the GBR Service Data Flow(s), the PCF shall obtain the Remaining Maximum Slice Data Rate by interacting with the UDR as defined in 3GPP TS 29.519 [15]. When the PCF interacts with the UDR may be based on operator policies.

When the PCF needs to provide the authorized Session-AMBR and/or install new or updated PCC Rule(s) and/or delete PCC Rule(s) related to GBR service data flow(s), the PCF shall:

- calculate the difference between the previously authorized Session-AMBR, if applicable, and the new authorized Session-AMBR; and/or

- calculate the difference between the previously authorized MBR and the new authorized MBR(s) for the authorized PCC Rule(s) related to GBR service data flow(s);

And then:

- Calculate the utilized data rate, i.e. the sum of the previously calculated differences, which is to be substracted from the Remaining Maximum Slice Data rate.

NOTE 1: For example, when the PCF modifies as part of the same operation the MBR of PCC Rule A from 100 to 150 and the MBR of PCC Rule B from 30 to 20, deletes PCC Rule C with an MBR of 50 and adds a PCC Rule D of MBR 75, the final calculated value will be +50-10-50+75, i.e. 65. If the authorized Session-AMBR is also updated from 1000 to 2000, the final derived value will be 1065.

NOTE 2: The utilized data rate can be a negative value. In this case, the final Remaining Maximum Slice Data Rate is increased.

Therefore, the PCF shall behave as follows:

- At PDU session establishment, the PCF shall check whether the Remaining Maximum Slice Data Rate is higher than the calculated utilized data rate (e.g. based on the authorized Session-AMBR). If it is the case, the PCF shall deduct the value of the utilized data rate from the Remaining Maximum Slice Data Rate for the concerned S-NSSAI in the UDR. If however the Remaining Maximum Slice Data Rate is not sufficient, the PCF may reject the establishment of the SM Policy Association with an HTTP "403 Forbidden" response message including the "cause" attribute of the ProblemDetails data structure set to "EXCEEDED_SLICE_DATA_RATE".

- At PDU session modification initiated by the SMF, the PCF shall check whether the Remaining Maximum Slice Data Rate is higher than the calculated utilized data rate (e.g. based on the authorized Session-AMBR). If it is the case, the PCF shall deduct the value of the utilized data rate from the Remaining Maximum Slice Data Rate for the concerned S-NSSAI in the UDR. If however the Remaining Maximum Slice Data Rate is not sufficient, the PCF may reject the modification of the SM Policy Association with an HTTP "403 Forbidden" response message including the "cause" attribute of the ProblemDetails data structure set to "EXCEEDED_SLICE_DATA_RATE".

- When a PCC rule of a GBR service data flow is installed, modified, removed, activated or deactivated in the SMF,

  - the PCF shall derive the authorized QoS for the service data flow and the associated utilized data rate and update the Remaining Maximum Slice Data Rate for the concerned S-NSSAI in the UDR accordingly;

  - the PCF may request the SMF to confirm that the resources associated to that PCC rule are successfully allocated as defined in clause 4.2.6.5.5 or released as defined in clauses 4.2.3.13 and 4.2.4.12;

  - if the SMF reports that some of or all the resources cannot be successfully allocated, the PCF shall recalculate the authorized QoS for the service data flow and the associated utilized data rate and update the Remaining Maximum Slice Data Rate for the concerned S-NSSAI in the UDR accordingly.

- When the authorized Session-AMBR changes and/or one or several PCC Rule(s) of a GBR service data flow(s) are installed, removed or modified, the PCF shall calculate the new utilized data rate and update the Remaining Maximum Slice Data Rate for that S-NSSAI in the UDR accordingly.

- At PDU session termination, the PCF shall add the value of the related previously utilized data rate (i.e. based on the authorized Session-AMBR allocated to the PDU session and the previously utilized data rate by the removed PCC Rule(s) related to GBR service data flow(s)) to the Remaining Maximum Slice Data Rate for the concerned S-NSSAI in the UDR.

- If the Remaining Maximum Slice Data Rate for that S-NSSAI reaches a (operator defined) threshold that indicates that it is closer or equal to zero, the PCF may apply policy decision(s) to strengthen the traffic restrictions for the concerned PDU Session(s).

- If the Remaining Maximum Slice Data Rate for that S-NSSAI returns to a value below the (operator defined) threshold, the PCF may apply policy decision(s) to recover the initially derived value(s) for the concerned PDU Session(s).

NOTE 3: While the Remaining Maximum Slice Data Rate is relatively high, the PCF can be configured to maintain a local Remaining Maximum Slice Data Rate and to only interact with the UDR to update the Remaining Maximum Slice Data Rate when a certain threshold is reached, or a certain time window has passed. The higher the configured values are the lower the chances for an accurate limitation of the slice data rate becomes. When multiple PCFs for the same S-NSSAI are deployed, each PCF can also subscribe to the change of the Network slice specific policy control data in the UDR. The UDR will then send a notification to each subscribed PCF when the Remaining Maximum Slice Data Rate per S-NSSAI changes.

NOTE 4: Multiple PCFs responsible for PDU Sessions of UEs to the same S-NSSAI can read and update the Remaining Maximum Slice Data Rate for the S-NSSAI in the UDR using the conditional requests with preconditions for the update of the Remaining Maximum Slice Data Rate, this mechanism using Etags is defined in Table 5.2.2.2-2 of 3GPP TS 29.500 [4] to ensure a proper update of the UDR data in case of simultaneous access from different PCFs.

4.2.6.8.3 Network slice data rate policy control with assistance of the NWDAF

If the NWDAF is used for network slice data rate policy control, the PCF uses the Data Volume Dispersion Analytics provided by the NWDAF. For this purpose, the PCF subscribes to the NWDAF for periodic reporting of the Data Volume Dispersion Analytics statistics for all the UEs using the concerned network slice. The PCF subscribes to the NWDAF for Data Volume Dispersion Analytics reporting at the establishment of the first PDU session within the concerned S-NSSAI (subject to network slice data rate limitation) and cancels this subscription at the termination of the last PDU session within the concerned S-NSSAI as described in 3GPP TS 29.520 [51].

The PCF calculates the utilized data rate of the S-NSSAI by using the Data Volume Dispersion Analytics statistics reported by the NWDAF. When the utilized data rate of the S-NSSAI in UL and/or DL is getting close to or exceeding respectively the value of the "mbrUl" attribute and/or the value of the "mbrDl" attribute of the SlicePolicyData data structure as defined in 3GPP TS 29.519 [15], based on operator policy, the PCF may apply policy decision(s) to strengthen the traffic restrictions for individual PDU sessions and/or PCC rules. For example:

- The PCF may reject the creation or modification of SM Policy Associations that require the increase of the utilized data rate for the S-NSSAI with an HTTP "403 Forbidden" response message including the "cause" attribute of the ProblemDetails data structure set to "EXCEEDED_SLICE_DATA_RATE".

- The PCF may refrain from sending new and/or updated PCC Rules that require the increase of the utilized data rate.

When the utilized data rate of the S-NSSAI in UL and/or DL falls below respectively the value of the "mbrUl" attribute and/or the value of the "mbrDl" attribute of the SlicePolicyData data structure, the PCF may relax the traffic restrictions for individual PDU sessions and/or PCC rules.

When multiple PCFs for the same S-NSSAI are deployed, each PCF subscribes to the analytics from the NWDAF separately.

NOTE: When multiple PCFs are used for the concerned S-NSSAI, the NWDAF triggers Data Volume Dispersion Analytics notifications towards all these PCFs, but their policy decisions can be different.4.2.7 Detection and handling of late arriving requests

4.2.7.1 Handling of requests which collide with an existing SM Policy Association

The PCF may receive an Originating Time Stamp parameter within the 3gpp-Sbi-Origination-Timestamp header, which is set by the AMF, by the Npcf_SMPolicyControl_Create service request.

NOTE 1: The SMF forwards the Origination Time Stamp to the PCF, when received from the AMF to allow the handling of colliding requests at the PCF based on network conditions.

Upon receipt of a Npcf_SMPolicyControl_Create service request which collides with an existing SM Policy Association for the same UE (i.e. same values of "supi" attribute) and the same PDU session Id (i.e. same values of "pduSessionId" attribute), the PCF shall accept the new request only if it contains a more recent timestamp within the 3gpp-Sbi-Origination-Timestamp header than the origination timestamp stored for the existing SM Policy Association. An incoming Npcf_SMPolicyControl_Create service request shall be considered as more recent than an existing SM Policy Association and be accepted if no 3gpp-Sbi-Origination-Timestamp header was provided for at least one of the two SM Policy Associations. The PCF shall reject an incoming request whose timestamp is less recent than the timestamp of the existing SM Policy Association with the HTTP status code "403 Forbidden" and the application error "LATE_OVERLAPPING_REQUEST".

NOTE 2: When the PCF accepts the new request that contains a more recent timestamp within the 3gpp-Sbi-Origination-Timestamp header than the timestamp stored for the SM Policy Association, the PCF performs implementation specific, e.g. locally deletes the existing Individual SM Policy Association.

5 Npcf_SMPolicyControl Service API

5.1 Introduction

The Npcf_SMPolicyControl Service shall use the Npcf_SMPolicyControl API.

The API URI of the Npcf_SMPolicyControl API shall be:

{apiRoot}/<apiName>/<apiVersion>

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

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

with the following components:

- The {apiRoot} shall be set as described in 3GPP TS 29.501 [5].
- The <apiName> shall be "npcf-smpolicycontrol".
- The <apiVersion> shall be "v1".
- The <apiSpecificResourceUriPart> shall be set as described in clause 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 clause 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 clause 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 clause 5.4 of 3GPP TS 29.500 [4]. The use of the JSON format shall be signalled by the content type "application/json".

"Problem Details" JSON object shall be used to indicate additional details of the error in a HTTP response body and shall be signalled by the content type "application/problem+json", as defined in IETF RFC 7807 [31].

5.2.3 HTTP custom headers

5.2.3.1 General

The Npcf_SMPolicyControl API shall support HTTP custom header fields specified in clause 5.2.3.2 of 3GPP TS 29.500 [4] and may support HTTP custom header fields specified in clause 5.2.3.3 of 3GPP TS 29.500 [4].

5.2.3.2 3gpp-Sbi-Origination-Timestamp

The header contains the date and time (with a millisecond granularity) when the originating entity initiated the request as specified in clause 6.1.2.3.2 of 3GPP TS 29.502 [22].

5.3 Resources

5.3.1 Resource Structure

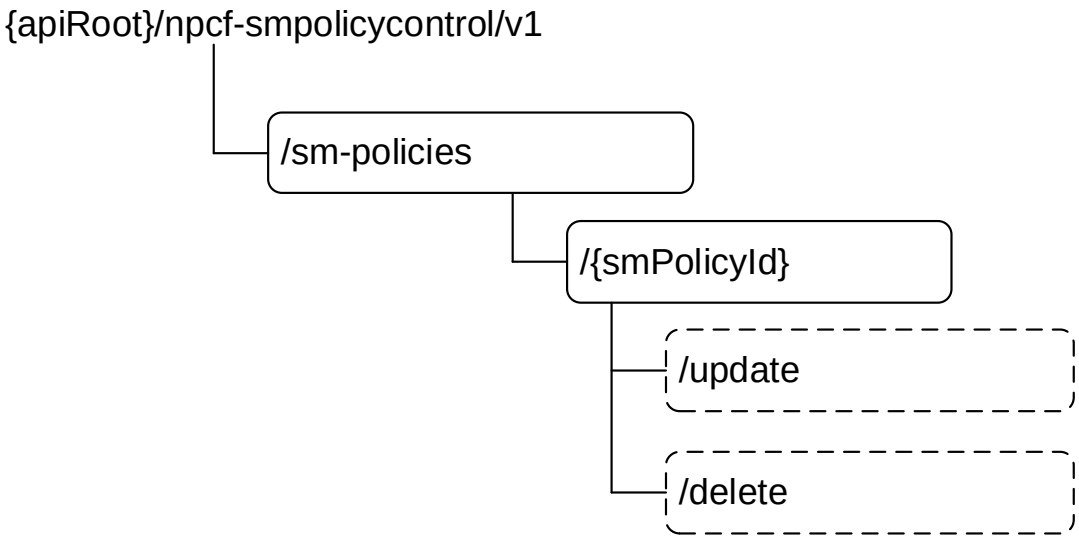

Figure 5.3.1-1: Resource URI structure of the Npcf_SMPolicyControl API

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

5.3.2 Resource: SM Policies

5.3.2.1 Description

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

5.3.2.2 Resource definition

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

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

Table 5.3.2.2-1: Resource URI variables for this resource

Name	Data type	Definition
apiRoot	string	See clause 5.1

5.3.2.3 Resource Standard Methods

5.3.2.3.1 POST

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

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

Name	Data type	P	Cardinality	Description
n/a				

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

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

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

Table 5.3.2.3.1-3: Data structures supported by the POST Response Body on this resource

Data type	P	Cardinality	Response codes	Description
SmPolicyDecision	M	1	201 Created	An individual SM Policy resources for the SUPI and PDU session id are created successfully.
ProblemDetails	O	0..1	400 Bad Request	(NOTE 2)
ProblemDetails	O	0..1	403 Forbidden	(NOTE 2)
n/a			308 Permanent Redirect	The URI of the PCF within the existing PCF binding information stored in the BSF for the indicated combination is returned in the non-roaming or home-routed scenario. (NOTE 3)
NOTE 1: The mandatory HTTP error status codes for the POST method listed in table 5.2.7.1-1 of 3GPP TS 29.500 [4] shall also apply. NOTE 2: Failure cases are described in clause 5.7. NOTE 3: Only applicable to the "SamePcf" feature as defined in clause 5.8.				

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

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

Table 5.3.2.3.1-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains the URI of the PCF within the existing PCF binding information stored in the BSF for the indicated combination.

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	Data type	Definition
apiRoot	string	See clause 5.1
smPolicyId	string	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.
RedirectResponse	O	0..1	307 Temporary Redirect	Temporary redirection, during Individual SM policy retrieval. The response shall include a Location header field containing an alternative URI of the resource located in an alternative PCF (service) instance. Applicable if the feature "ES3XX" is supported.
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection, during Individual SM policy retrieval. The response shall include a Location header field containing an alternative URI of the resource located in an alternative PCF (service) instance. Applicable if the feature "ES3XX" is supported.
NOTE: The mandatory HTTP error status codes for the GET method listed in table 5.2.7.1-1 of 3GPP TS 29.500 [4] shall also apply.				

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

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative PCF (service) instance.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance towards which the request is redirected

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

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative PCF (service) instance.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance towards which the request is redirected

5.3.3.4 Resource Custom Operations

5.3.3.4.1 Overview

Table 5.3.3.4.1-1: Custom operations

Operation Name	Custom operation URI	Mapped HTTP method	Description
delete	/sm-policies/{smPolicyId}/delete	delete (POST)	Delete an individual SM Policy resource.
update	/sm-policies/{smPolicyId}/update	update (POST)	Update an individual SM Policy resource.

5.3.3.4.2 Operation: delete

5.3.3.4.2.1 Description

5.3.3.4.2.2 Operation Definition

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

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

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

Data type	P	Cardinality	Description
SmPolicyDeleteData	O	0..1	Parameters to be sent by the NF service consumer 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.
RedirectResponse	O	0..1	307 Temporary Redirect	Temporary redirection, during Individual SM policy deletion. The response shall include a Location header field containing an alternative URI of the resource located in an alternative PCF (service) instance. Applicable if the feature "ES3XX" is supported.
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection, during Individual SM policy deletion. The response shall include a Location header field containing an alternative URI of the resource located in an alternative PCF (service) instance. Applicable if the feature "ES3XX" is supported.
NOTE: The mandatory HTTP error status codes for the POST method listed in table 5.2.7.1-1 of 3GPP TS 29.500 [4] shall also apply.				

Table 5.3.3.4.2.2-3: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative PCF (service) instance.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance towards which the request is redirected

Table 5.3.3.4.2.2-4: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative PCF (service) instance.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance towards which the request is redirected

5.3.3.4.3 Operation: update

5.3.3.4.3.1 Description

5.3.3.4.3.2 Operation Definition

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

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

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

Data type	P	Cardinality	Description
SmPolicyUpdateContextData	M	1	Parameters to be sent by the NF service consumer 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.
RedirectResponse	O	0..1	307 Temporary Redirect	Temporary redirection, during Individual SM policy modification. The response shall include a Location header field containing an alternative URI of the resource located in an alternative PCF (service) instance. Applicable if the feature "ES3XX" is supported.
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection, during Individual SM policy modification. The response shall include a Location header field containing an alternative URI of the resource located in an alternative PCF (service) instance. Applicable if the feature "ES3XX" is supported.
ProblemDetails	O	0..1	400 Bad Request	(NOTE 2)
ProblemDetails	O	0..1	403 Forbidden	(NOTE 2)
ProblemDetails	O	0..1	404 Not Found	(NOTE 2)
NOTE 1: The mandatory HTTP error status codes for the POST method listed in table 5.2.7.1-1 of 3GPP TS 29.500 [4] shall also apply. NOTE 2: Failure cases are described in clause 5.7.				

Table 5.3.3.4.3.2-3: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative PCF (service) instance.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance towards which the request is redirected

Table 5.3.3.4.3.2-4: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative PCF (service) instance.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance towards which the request is redirected

5.4 Custom Operations without associated resources

None.

5.5 Notifications

5.5.1 General

Table 5.5.1-1: Notifications

Notification	Callback URI	HTTP method or custom operation	Description (service operation)
Policy Update Notification	{notificationUri}/update	update (POST)	Policy Update Notification.
Request for termination of the policy association	{notificationUri}/terminate	terminate (POST)	Request for termination of the policy association.

5.5.2 Policy Update Notification

5.5.2.1 Description

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

5.5.2.2 Operation Definition

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

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

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

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

Data type	P	Cardinality	Response codes	Description
n/a			204 No Content	The SM policies are updated successfully.
UeCampingRep	O	0..1	200 OK	The current applicable values corresponding to the policy control request trigger is reported.
array(PartialSuccessReport)	O	1..N	200 OK	Some of the PCC rules and/or session rule provisioned by the PCF are not installed/activated successfully.
RedirectResponse	O	0..1	307 Temporary Redirect	Temporary redirection, during SM policy notification. The response shall include a Location header field containing an alternative URI representing the end point of an alternative NF service consumer (service) instance where the notification should be sent. Applicable if the feature "ES3XX" is supported.
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection, during SM policy notification. The response shall include a Location header field containing an alternative URI representing the end point of an alternative NF service consumer (service) instance where the notification should be sent. Applicable if the feature "ES3XX" is supported.
ErrorReport	M	1	400 Bad Request	The SM policies including all the PCC rules and session rules provisioned by the PCF are not installed/activated successfully.
array(PolicyDecisionFailureCode)	O	1..N	200 OK	Provisioning of some of the policy decision and/ condition data which are not referred by any PCC rules or session rule are failure.
NOTE 1: The mandatory HTTP error status codes for the POST method listed in table 5.2.7.1-1 of 3GPP TS 29.500 [4] shall also apply. NOTE 2: Failure cases are described in clause 5.7.				

Table 5.5.2.2-3: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI representing the end point of an alternative NF consumer (service) instance towards which the notification should be redirected.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance towards which the notification request is redirected

Table 5.5.2.2-4: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI representing the end point of an alternative NF consumer (service) instance towards which the notification should be redirected.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance towards which the notification request is redirected

5.5.3 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.
RedirectResponse	O	0..1	307 Temporary Redirect	Temporary redirection, during SM policy termination notification. The response shall include a Location header field containing an alternative URI representing the end point of an alternative NF service consumer (service) instance where the notification should be sent. Applicable if the feature "ES3XX" is supported.
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection, during SM policy termination notification. The response shall include a Location header field containing an alternative URI representing the end point of an alternative NF service consumer (service) instance where the notification should be sent. Applicable if the feature "ES3XX" is supported.
NOTE: The mandatory HTTP error status codes for the POST method listed in table 5.2.7.1-1 of 3GPP TS 29.500 [4] shall also apply.				

Table 5.5.3.2-3: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI representing the end point of an alternative NF consumer (service) instance towards which the notification should be redirected.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance towards which the notification request is redirected

Table 5.5.3.2-4: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI representing the end point of an alternative NF consumer (service) instance towards which the notification should be redirected.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance towards which the notification request is redirected

5.6 Data Model

5.6.1 General

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

The Npcf_SMPolicyControl API allows the NF service consumer 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
5GSmCause	5.6.3.2	Indicates the 5GSM cause code value.	RAN-NAS-Cause
AdditionalAccessInfo	5.6.2.43	Indicates the combination of additional Access Type and RAT Type for MA PDU session	ATSSS
AccNetChargingAddress	5.6.2.35	Identifies the address of the network node performing charging and used for charging applications.	
AccNetChId	5.6.2.23	Contains the access network charging identifier for the PCC rule(s) or whole PDU session.	
AccuUsageReport	5.6.2.18	Contains the accumulated usage report information.	UMC
AfSigProtocol	5.6.3.10	Indicates the protocol used for signalling between the UE and the AF.	ProvAFsignalFlow
AppDetectionInfo	5.6.2.22	Contains the detected application's traffic information.	ADC
ApplicationDescriptor	5.6.3.2	Defines the Application Descriptor for an ATSSS rule.	ATSSS
AtsssCapability	5.6.3.26	Contains the ATSSS capability supported for the MA PDU Session.	ATSSS
AuthorizedDefaultQos	5.6.2.34	Authorized Default QoS.	
BridgeManagementContainer	5.6.2.47	Contains the UMIC.	TimeSensitiveNetworking
ChargingData	5.6.2.11	Contains charging related parameters.	
ChargingInformation	5.6.2.17	Contains the addresses, and if available, the instance ID and set ID, of the charging functions.	
ConditionData	5.6.2.9	Contains conditions for applicability of a rule.	
CreditManagementStatus	5.6.3.16	Indicates the reason of the credit management session failure.	
DownlinkDataNotificationControl	5.6.2.48	Contains the downlink data notification control information.	DDNEventPolicyControl
DownlinkDataNotificationControlRm	5.6.2.49	This data type is defined in the same way as the "DownlinkDataNotificationControl" data type, but with the OpenAPI "nullable: true" property.	DDNEventPolicyControl2
EpsRanNasRelCause	5.6.3.2	Indicates the RAN or NAS release cause code information in 3GPP-EPS access type or indicates the TWAN or untrusted WLAN release cause code information in Non-3GPP-EPS access type.	RAN-NAS-Cause
ErrorReport	5.6.2.36	Contains the rule reports.	
FailureCause	5.6.3.14	Indicates the cause of the failure in a Partial Success Report.	
FailureCode	5.6.3.9	Indicates the reason of the PCC rule failure.	
FlowDescription	5.6.3.2	Defines a packet filter for an IP flow.	
FlowDirection	5.6.3.3	Indicates the direction of the service data flow.	
FlowDirectionRm	5.6.3.15	This data type is defined in the same way as the "FlowDirection" data type, but allows null value.	
FlowInformation	5.6.2.14	Contains the flow information.	
IpMulticastAddressInfo	5.6.2.46	Contains the IP multicast addressing information	WWC
MaPduIndication	5.6.3.25	Contains the MA PDU session indication, i.e., MA PDU Request or MA PDU Network-Upgrade Allowed.	ATSSS
MeteringMethod	5.6.3.5	Indicates the metering method.	
MulticastAccessControl	5.6.3.20	Indicates whether the service data flow, corresponding to the service data flow template, is allowed or not allowed.	WWC
NetLocAccessSupport	5.6.3.27	Indicates the access network support of the report of the requested access network information.	NetLoc
NotificationControlIndication	5.6.3.29	Indicates the notification of DDD Status is requested and/or notification of DDN Failure is requested.	DDNEventPolicyControl
NwdafData	5.6.2.53	Indicates the list of NWDAF instance IDs used for the PDU Session and their associated Analytics ID(s) consumed by the NF service consumer.	EneNA
PacketFilterContent	5.6.3.2	Defines a packet filter for an IP flow.	
PacketFilterInfo	5.6.2.30	Contains the information from a single packet filter sent from the NF service consumer to the PCF.	

PartialSuccessReport	5.6.2.33	Includes the information reported by the NF service consumer when some of the PCC rules and/or session rules are not successfully installed/activated.	
PccRule	5.6.2.6	Contains the PCC rule information.	
PduSessionRelCause	5.6.3.24	Contains the NF service consumer PDU Session release cause.	PDUSessionRelCause, ImmediateTermination
PolicyControlRequestTrigger	5.6.3.6	Contains the policy control request trigger(s).	
PolicyDecisionFailureCode	5.6.3.28	Indicates the type of the failed policy decision and/or condition data.	PolicyDecisionErrorHandling
PortManagementContainer	5.6.2.45	Contains the port management information container for a port.	TimeSensitiveNetworking
QosCharacteristics	5.6.2.16	Contains QoS characteristics for a non-standardized or non-configured 5QI.	
QosData	5.6.2.8	Contains the QoS parameters.	
QosFlowUsage	5.6.3.13	Indicates a QoS flow usage information.	
QosMonitoringData	5.6.2.40	Contains QoS monitoring related control information.	QosMonitoring
QosMonitoringReport	5.6.2.42	Contains QoS monitoring reporting information.	QosMonitoring
QosNotificationControlInfo	5.6.2.32	Contains the QoS Notification Control Information.	
RanNasRelCause	5.6.2.28	Contains the RAN/NAS release cause.	RAN-NAS-Cause
RedirectAddressType	5.6.3.12	Indicates the redirect address type.	ADC
RedirectInformation	5.6.2.13	Contains the redirect information.	ADC
ReportingFrequency	5.6.3.22	Indicates the frequency for the reporting	QosMonitoring
ReportingLevel	5.6.3.4	Indicates the reporting level.	
RequestedQos	5.6.2.31	Contains the QoS information requested by the UE.	
RequestedQosMonitoringParameter	5.6.3.21	Indicates the requested QoS monitoring parameters to be measured.	QosMonitoring
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.	UMC
RuleOperation	5.6.3.11	Indicates a UE initiated resource operation that causes a request for PCC rules.	
RuleReport	5.6.2.27	Reports the status of PCC.	
RuleStatus	5.6.3.8	Indicates the status of PCC or session rule.	
ServingNfIdenty	5.6.2.38	Contains the serving Network Function identity.	
SessionRule	5.6.2.7	Contains session level policy information.	
SessionRuleFailureCode	5.6.3.17	Indicates the reason of the session rule failure.	SessionRuleErrorHandling
SessionRuleReport	5.6.2.37	Reports the status of session rule.	SessionRuleErrorHandling
SgsnAddress	5.6.2.50	Contains the serving SGSN address.	2G3GIWK
SmPolicyAssociationReleaseCause	5.6.3.23	Represents the cause why the PCF requests the termination of the SM policy association.	
SmPolicyControl	5.6.2.2	Contains the parameters to request the SM policies and the SM policies authorized by the PCF.	
SmPolicyContextData	5.6.2.3	Contains the parameters to create individual SM policy resource.	
SmPolicyDecision	5.6.2.4	Contains the SM policies authorized by the PCF.	
SmPolicyNotification	5.6.2.5	Contains the update of the SM policies.	
SmPolicyDeleteData	5.6.2.15	Contains the parameters to be sent to the PCF when the individual SM policy is deleted.	
SmPolicyUpdateContextData	5.6.2.19	Contains the met policy control request trigger(s) and corresponding new value(s) or the error report of the policy enforcement.	
SteeringFunctionality	5.6.3.18	Indicates functionality to support traffic steering, switching and splitting determined by the PCF.	ATSSS

SteeringMode	5.6.2.39	Contains the steering mode value and parameters determined by the PCF.	ATSSS
SteerModeIndicator	5.6.3.31	Contains Autonomous load-balance indicator or UE-assistance indicator.	EnATSSS
SteerModeValue	5.6.3.19	Indicates the steering mode value determined by the PCF.	ATSSS
TerminationNotification	5.6.2.21	Termination Notification.	
ThresholdValue	5.6.2.52	Contains the threshold value(s) for RTT and/or Packet Loss Rate.	EnATSSS
TrafficControlData	5.6.2.10	Contains parameters determining how flows associated with a PCCRule are treated (blocked, redirected, etc).	
TsnBridgeInfo	5.6.2.41	Contains parameters that describe and identify the TSC user plane node.	TimeSensitive Networking
TsnPortNumber	5.6.3.2	Contains a port number.	TimeSensitive Networking
UeCampingRep	5.6.2.26	Contains the current applicable values corresponding to the policy control request triggers.	
UeInitiatedResourceRequest	5.6.2.29	Indicates a UE requests specific QoS handling for selected SDF.	
UpPathChgEvent	5.6.2.20	Contains the UP path change event subscription from the AF.	TSC
UsageMonitoringData	5.6.2.12	Contains usage monitoring related control information.	UMC

Table 5.6.1-2 specifies data types re-used by the Npcf_SMPolicyControl service based interface protocol from other specifications, including a reference to their respective specifications and when needed, a short description of their use within the Npcf_SMPolicyControl service based interface.

Table 5.6.1-2: Npcf_SMPolicyControl re-used Data Types

Data type	Reference	Comments	Applicability
5GMmCause	3GPP TS 29.571 [11]	Contains the cause value of 5GMM protocol.	RAN-NAS-Cause
5Qi	3GPP TS 29.571 [11]	Unsigned integer representing a 5G QoS Identifier (see clause 5.7.2.1 of 3GPP TS 23.501 [2]), within the range 0 to 255.	
5QiPriorityLevel	3GPP TS 29.571 [11]	Unsigned integer indicating the 5QI Priority Level (see clauses 5.7.3.3 and 5.7.4 of 3GPP TS 23.501 [2]), within the range 1 to 127. Values are ordered in decreasing order of priority, i.e. with 1 as the highest priority and 127 as the lowest priority.	
5QiPriorityLevelRm	3GPP TS 29.571 [11]	This data type is defined in the same way as the "5QiPriorityLevel" data type, but with the OpenAPI "nullable: true" property.	
AccessType	3GPP TS 29.571 [11]	The identification of the type of access network.	
AccessTypeRm	3GPP TS 29.571 [11]	This data type is defined in the same way as the "AccessType" data type, but with the OpenAPI "nullable: true" property.	ATSSS
Ambr	3GPP TS 29.571 [11]	Session-AMBR.	
AnGwAddress	3GPP TS 29.514 [17]	Carries the control plane address of the access network gateway. (NOTE 1)	
ApplicationChargingId	3GPP TS 29.571 [11]	Application provided charging identifier allowing correlation of charging information.	AF_Charging_Identifier
Arp	3GPP TS 29.571 [11]	ARP.	
AverWindow	3GPP TS 29.571 [11]	Averaging Window.	
AverWindowRm	3GPP TS 29.571 [11]	This data type is defined in the same way as the "AverWindow" data type, but with the OpenAPI "nullable: true" property.	
BitRate	3GPP TS 29.571 [11]	String representing a bit rate that shall be formatted as follows: pattern: "^\d+(\.\d+)? (bps|Kbps|Mbps|Gbps|Tbps)$" Examples: "125 Mbps", "0.125 Gbps", "125000 Kbps".	
BitRateRm	3GPP TS 29.571 [11]	This data type is defined in the same way as the "BitRate" data type, but with the OpenAPI "nullable: true" property.	
Bytes	3GPP TS 29.571 [11]	String with format "byte".	TimeSensitiveNetworking
ChargingId	3GPP TS 29.571 [11]	Charging identifier allowing correlation of charging information.	
ContentVersion	3GPP TS 29.514 [17]	Indicates the content version of a PCC rule. It uniquely identifies a version of the PCC rule as defined in clause 4.2.6.2.14.	RuleVersioning
DateTime	3GPP TS 29.571 [11]	String with format "date-time" as defined in OpenAPI Specification [10].	
DateTimeRm	3GPP TS 29.571 [11]	This data type is defined in the same way as the "DateTime" data type, but with the OpenAPI "nullable: true" property.	
DddTrafficDescriptor	3GPP TS 29.571 [11]	Traffic Descriptor	DDNEventPolicyControl
DlDataDeliveryStatus	3GPP TS 29.571 [11]	Downlink data delivery status.	DDNEventPolicyControl
DnaiChangeType	3GPP TS 29.571 [11]	Describes the types of DNAI change.	
Dnn	3GPP TS 29.571 [11]	The DNN the user is connected to.	
DnnSelectionMode	3GPP TS 29.502 [22]	DNN selection mode.	DNNSelectionMode
DurationSec	3GPP TS 29.571 [11]	Identifies a period of time in units of seconds.	
DurationSecRm	3GPP TS 29.571 [11]	This data type is defined in the same way as the "DurationSec" data type, but with the OpenAPI "nullable: true" property.	
EasIpReplacementInfo	3GPP TS 29.571 [11]	Contains EAS IP replacement information for a Source and a Target EAS.	EASIPreplacement

EthFlowDescription	3GPP TS 29.514 [17]	Defines a packet filter for an Ethernet flow. (NOTE 2)	
ExtMaxDataBurstVol	3GPP TS 29.571 [11]	Maximum Data Burst Volume.	EMDBV
ExtMaxDataBurstVolRm	3GPP TS 29.571 [11]	This data type is defined in the same way as the "ExtMaxDataBurstVol" data type, but with the OpenAPI "nullable: true" property.	EMDBV
FinalUnitAction	3GPP TS 32.291 [19]	Indicates the action to be taken when the user's account cannot cover the service cost.	
FlowStatus	3GPP TS 29.514 [17]	Describes whether the IP flow(s) are enabled or disabled. The value "REMOVED" is not applicable to Npcf_SMPolicyControl service.	
Gpsi	3GPP TS 29.571 [11]	Identifies a GPSI.	
GroupId	3GPP TS 29.571 [11]	Identifies a group of internal globally unique ID.	
Guami	3GPP TS 29.571 [11]	Globally Unique AMF Identifier.	
InvalidParam	3GPP TS 29.571 [11]	Invalid Parameters for the reported failed policy decisions	ExtPolicyDecisionErrorHandling
IpIndex	3GPP TS 29.519 [15]	Information that identifies which IP pool or external server is used to allocate the IP address.	
Ipv4Addr	3GPP TS 29.571 [11]	Identifies an Ipv4 address.	
Ipv4AddrMask	3GPP TS 29.571 [11]	String identifying an IPv4 address mask.	
Ipv6Addr	3GPP TS 29.571 [11]	Identifies an IPv6 address.	
Ipv6Prefix	3GPP TS 29.571 [11]	The Ipv6 prefix allocated for the user.	
MacAddr48	3GPP TS 29.571 [11]	MAC Address.	
MaxDataBurstVol	3GPP TS 29.571 [11]	Maximum Data Burst Volume.	
MaxDataBurstVolRm	3GPP TS 29.571 [11]	This data type is defined in the same way as the "MaxDataBurstVol" data type, but with the OpenAPI "nullable: true" property.	
NfInstanceId	3GPP TS 29.571 [11]	The NF instance identifier.	
NfSetId	3GPP TS 29.571 [11]	The NF set identifier.	
NgApCause	3GPP TS 29.571 [11]	Contains the cause value of NgAP protocol.	RAN-NAS-Cause
NullValue	3GPP TS 29.571 [11]	JSON's null value, used as an explicit value of an enumeration.	
NwdafEvent	3GPP TS 29.520 [51]	Analytics ID consumed by the NF service consumer.	EneNA
PacketDelBudget	3GPP TS 29.571 [11]	Packet Delay Budget.	
PacketErrRate	3GPP TS 29.571 [11]	Packet Error Rate.	
PacketLossRateRm	3GPP TS 29.571 [11]	This data type is defined in the same way as the "PacketLossRate" data type, but with the OpenAPI "nullable: true" property.	
PcfUeCallbackInfo	3GPP TS 29.571 [11]	Contains the PCF for the UE callback URI and SBA binding information, if available	AMInfluence
PduSessionId	3GPP TS 29.571 [11]	The identification of the PDU session.	
PduSessionType	3GPP TS 29.571 [11]	Indicate the type of a PDU session.	
Pei	3GPP TS 29.571 [11]	The Identification of a Permanent Equipment.	
PlmnIdNid	3GPP TS 29.571 [11]	The identification of the Network: The PLMN Identifier (the mobile country code and the mobile network code) or the SNPN Identifier (the PLMN Identifier and the NID).	
PresenceInfo	3GPP TS 29.571 [11]	Contains the information which describes a Presence Reporting Area.	PRA
PresenceInfoRm	3GPP TS 29.571 [11]	This data type is defined in the same way as the "PresenceInfo" data type, but with the OpenAPI "nullable: true" property.	PRA
ProblemDetails	3GPP TS 29.571 [11]	Contains a detailed information about an error.	
QosNotifType	3GPP TS 29.514 [17]	Indicates whether the GBR targets for the indicated SDFs are "NOT_GUARANTEED" or "GUARANTEED" again.	
QosResourceType	3GPP TS 29.571 [11]	Indicates whether the resource type is GBR, delay critical GBR, or non-GBR.	
RatingGroup	3GPP TS 29.571 [11]	Identifier of a rating group.	
RatType	3GPP TS 29.571 [11]	The identification of the RAT type.	
RedirectResponse	3GPP TS 29.571 [11]	Contains redirection related information.	ES3XX

RouteToLocation	3GPP TS 29.571 [11]	A traffic routes to applications location.	TSC
SatelliteBackhaulCategory	3GPP TS 29.571 [11]	Indicates the satellite backhaul category or non-satellite backhaul.	SatBackhaulCategoryChg
ServerAddressingInfo	3GPP TS 29.571 [11]	Contains the Provisioning Server information that provisions the UE with credentials and other data to enable SNPN access.	PvsSupport
ServiceId	3GPP TS 29.571 [11]	Identifier of a service.	
Snssai	3GPP TS 29.571 [11]	Identifies the S-NSSAI.	
SubscribedDefaultQos	3GPP TS 29.571 [11]	Subscribed Default QoS.	
Supi	3GPP TS 29.571 [11]	The identification of the user (i.e. IMSI, NAI).	
SupportedFeatures	3GPP TS 29.571 [11]	Used to negotiate the applicability of the optional features defined in table 5.8-1.	
TraceData	3GPP TS 29.571 [11]		
TimeZone	3GPP TS 29.571 [11]	Contains the user time zone information.	
TscaiInputContainer	3GPP TS 29.514 [17]	TSCAI Input information.	TimeSensitive Networking
Uinteger	3GPP TS 29.571 [11]	Unsigned Integer.	
UintegerRm	3GPP TS 29.571 [11]	This data type is defined in the same way as the "Uinteger" data type, but with the OpenAPI "nullable: true" property.	EnATSSS, AF_latency
Uint64	3GPP TS 29.571 [11]	Unsigned 64-bit integers.	TimeSensitive Networking
Uri	3GPP TS 29.571 [11]	URI.	
UserLocation	3GPP TS 29.571 [11]	Contains the user location(s).	
Volume	3GPP TS 29.122 [32]	Unsigned integer identifying a volume in units of bytes.	
VolumeRm	3GPP TS 29.122 [32]	This data type is defined in the same way as the "Volume" data type, but with the OpenAPI "nullable: true" property.	
VplmnQos	3GPP TS 29.502 [22]	QoS constraints in the VPLMN.	VPLMN-QoS-Control
NOTE 1: "AnGwAddr" data structure is only applicable to the 5GS and EPC/E-UTRAN interworking scenario as defined in Annex B. NOTE 2: In order to support a set of MAC addresses with a specific range in the traffic filter, feature MacAddressRange as specified in clause 5.8 shall be supported.			

5.6.2 Structured data types

5.6.2.1 Introduction

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

5.6.2.2 Type 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 NF service consumer.	
policy	SmPolicyDecision	M	1	Includes the SM policies authorized by the PCF.	

5.6.2.3 Type SmPolicyContextData

Table 5.6.2.3-1: Definition of type SmPolicyContextData

Attribute name	Data type	P	Cardinality	Description	Applicability
accNetChId	AccNetChId	O	0..1	Indicates the access network charging identifier for default QoS flow or whole PDU session.	
chargEntityAddr	AccNetChargingAddress	O	0..1	Address of the network entity performing charging.	
gpsi	Gpsi	O	0..1	Gpsi shall contain either an External Id or an MSISDN.	
supi	Supi	M	1	Subscription Permanent Identifier. (NOTE 2)	
invalidSupi	boolean	C	0..1	When this attribute is included and set to true, it indicates that the "supi" attribute contains an invalid value. This attribute shall be present if the SUPI is not available in the NF service consumer, or the SUPI is unauthenticated. When present it shall be set as follows: - true: invalid SUPI. - false (default): valid SUPI.	
pduSessionId	PduSessionId	M	1	PDU session Id.	
dnn	Dnn	M	1	The DNN of the PDU session, a full DNN with both the Network Identifier and Operator Identifier, or a DNN with the Network Identifier only.	
dnnSelMode	DnnSelectionMode	O	0..1	Indicates whether the requested DNN corresponds to an explicitly subscribed DNN.	DNNSelection Mode
interGrpIds	array(GroupId)	O	1..N	The internal Group Id(s).	
notificationUri	Uri	M	1	Identifies the recipient of SM policies update notifications sent by the PCF.	
pduSessionType	PduSessionType	M	1	Indicates the type of a PDU session.	
accessType	AccessType	O	0..1	The Access Type where the served UE is camping.	
ratType	RatType	O	0..1	The RAT Type where the served UE is camping.	
addAccessInfo	AdditionalAccessInfo	O	0..1	Indicates the combination of additional Access Type and RAT Type for MA PDU session.	ATSSS
servingNetwork	PlmnIdNid	O	0..1	The serving network (a PLMN or an SNPN) where the served UE is camping. For the SNPN the NID together with the PLMN ID identifies the SNPN.	
userLocationInfo	UserLocation	O	0..1	The location where the served UE is camping. (NOTE 3)	
ueTimeZone	TimeZone	O	0..1	The time zone where the served UE is camping.	
pei	Pei	O	0..1	The Permanent Equipment Identifier of the served UE.	
ipv4Address	Ipv4Addr	O	0..1	The IPv4 Address of the served UE.	
ipv6AddressPrefix	Ipv6Prefix	O	0..1	The Ipv6 Address Prefix of the served UE.	
ipDomain	string	O	0..1	IPv4 address domain identifier. (NOTE 1)	
subsSessAmbr	Ambr	O	0..1	UDM subscribed or DN-AAA authorized Session-AMBR.	
authProfIndex	string	O	0..1	DN-AAA authorization profile index.	DN-Authorization
subsDefQos	SubscribedDefaultQos	O	0..1	Subscribed Default QoS Information.	
vplmnQos	VplmnQos	O	0..1	QoS constraints in a VPLMN.	VPLMN-QoS-Control
numOfPackFilter	integer	O	0..1	Contains the number of supported packet filter for signalled QoS rules.	

online	boolean	O	0..1	If it is included and set to true, the online charging is applied to the PDU session.	
offline	boolean	O	0..1	If it is included and set to true, the offline charging is applied to the PDU session.	
chargingCharacteristics	string	O	0..1	Contains the Charging Characteristics applied to the PDU session. Functional requirements for the Charging Characteristics are defined in 3GPP TS 32.255 [35] Annex A. The charging characteristics are encoded as specified in 3GPP TS 29.503 [34].	
3gppPsDataOffStatus	boolean	O	0..1	If it is included and set to true, the 3GPP PS Data Off is activated by the UE.	3GPP-PS-Data-Off
refQosIndication	boolean	O	0..1	If it is included and set to true, the reflective QoS is supported by the UE.	
sliceInfo	Snssai	M	1	Identifies the S-NSSAI.	
qosFlowUsage	QosFlowUsage	O	0..1	Indicates the required usage for default QoS flow.	
servNfId	ServingNfIdentity	O	0..1	Contains the serving network function identity.	
suppFeat	SupportedFeatures	C	0..1	Indicates the list of Supported features used as described in clause 5.8. This parameter shall be supplied by the NF service consumer in the POST request that requested the creation of an individual SM policy resource.	
traceReq	TraceData	O	0..1	Trace control and configuration parameters information defined in 3GPP TS 32.422 [24].	
smfId	NfInstanceId	O	0..1	SMF instance identifier.	
recoveryTime	DateTime	O	0..1	It includes the recovery time of the NF service consumer.	
maPduInd	MaPduIndication	O	0..1	Contains the MA PDU session indication, i.e., MA PDU Request or MA PDU Network-Upgrade Allowed.	ATSSS
atsssCapab	AtsssCapability	O	0..1	Contains the ATSSS capability supported for the MA PDU Session.	ATSSS
ipv4FrameRouteList	array(Ipv4AddrMask)	O	1..N	List of Framed Route information of IPv4.	
ipv6FrameRouteList	array(Ipv6Prefix)	O	1..N	List of Framed Route information of IPv6.	
satBackhaulCategory	SatelliteBackhaulCategory	O	0..1	Satellite backhaul category or non-satellite backhaul used for the PDU session. When this attribute is not present, non-satellite backhaul applies.	SatBackhaulCategoryChg
pcfUeInfo	PcfUeCallbackInfo	O	0..1	PCF for the UE callback URI and SBA binding information.	AMInfluence
pvsInfo	array(ServerAddressingInfo)	O	1..N	Provisioning Server(s) information that provision the UE with credentials and other data to enable SNPN access.	PvsSupport
onboardInd	boolean	O	0..1	If it is included and set to true, it indicates that the PDU session is used for UE Onboarding.	PvsSupport
nwdafDatas	array(NwdafData)	O	1..N	List of NWDAF Instance IDs and their associated Analytics IDs consumed by the NF service consumer.	EneNA

NOTE 1: The value provided in this attribute is implementation specific. The only constraint is that the NF service consumer shall supply a different identifier for each overlapping address domain (e.g. the SMF NF instance identifier).
NOTE 2: For an emergency session, when the SUPI is not available in the NF service consumer, or if available, the SUPI is unauthenticated, the value provided in the "supi" attribute is implementation specific.
NOTE 3: The SMF may encode both 3GPP and non-3GPP access UE location in the "userLocationInfo" attribute.

5.6.2.4 Type SmPolicyDecision

Table 5.6.2.4-1: Definition of type SmPolicyDecision

Attribute name	Data type	P	Cardinality	Description	Applicability
sessRules	map(SessionRule)	O	1..N	A map of Sessionrules with the content being the SessionRule as described in clause 5.6.2.7. The key used in this map for each entry is the sessRuleId attribute of the corresponding SessionRule. (NOTE 2)	
pccRules	map(PccRule)	O	1..N	A map of PCC rules with the content being the PCCRule as described in clause 5.6.2.6. The key used in this map for each entry is the pccRuleId attribute of the corresponding PccRule.	
qosDecs	map(QosData)	O	1..N	Map of QoS data policy decisions. The key used in this map for each entry is the qosId attribute of the corresponding QosData. (NOTE 2)	
chgDecs	map(ChargingData)	O	1..N	Map of Charging data policy decisions. The key used in this map for each entry is the chgId attribute of the corresponding ChargingData.	
chargingInfo	ChargingInformation	C	1	Contains the CHF addresses, and if available, the associated CHF instance ID(s) and CHF set ID(s) of the PDU session. (NOTE 3)	
traffContDecs	map(TrafficControlData)	O	1..N	Map of Traffic Control data policy decisions. The key used in this map for each entry is the tcId attribute of the corresponding TrafficControlData. (NOTE 2)	
umDecs	map(UsageMonitoringData)	O	1..N	Map of Usage Monitoring data policy decisions. The key used in this map for each entry is the umId attribute of the corresponding UsageMonitoringData.	UMC
qosChars	map(QosCharacteristics)	O	1..N	Map of QoS characteristics for non-standard 5QIs and non-preconfigured 5QIs. This map uses the 5QI values as keys. (NOTE 2)	
qosMonDecs	map(QosMonitoringData)	O	1..N	Map of QoS Monitoring data policy decision. The key used in this map for each entry is the qmId attribute of the corresponding QosMonitoringData.	QosMonitoring
reflectiveQoSTimer	DurationSec	O	0..1	Defines the lifetime of a UE derived QoS rule belonging to the PDU Session for reflective QoS. (NOTE 2)	
offline	boolean	O	0..1	Indicates the offline charging is applicable to the PDU session when it is included and set to true. (NOTE 3) (NOTE 4) (NOTE 6)	
online	boolean	O	0..1	Indicates the online charging is applicable to the PDU session when it is included and set to true. (NOTE 3) (NOTE 4) (NOTE 6)	
offlineChOnly	boolean	O	0..1	Indicates that the online charging method shall never be used for any PCC rule activated during the lifetime of the PDU session, when this attribute is present and set to "true". The default value is "false", e.g. if this attribute is omitted. (NOTE 3) (NOTE 4) (NOTE 6)	OfflineChOnly

conds	map(ConditionData)	O	1..N	A map of condition data with the content being as described in clause 5.6.2.9. The key used in this map for each entry is the condId attribute of the corresponding ConditionData.	
revalidationTime	DateTime	O	0..1	Defines the time before which the NF service consumer shall have to re-request PCC rules.	
pcscfRestIndication	boolean	O	0..1	If this attribute is included and set to true, it indicates that P-CSCF Restoration is requested. The default value "FALSE" applies if the attribute is not present and has not been supplied previously.	PCSCF-Restoration-Enhancement
policyCtrlReqTriggers	array(PolicyControlRequestTrigger)	O	1..N	Defines the policy control request triggers subscribed by the PCF.	
lastReqRuleData	array(RequestedRuleData)	O	1..N	Defines the last list of rule control data requested by the PCF.	
lastReqUsageData	RequestedUsageData	O	0..1	Indicates whether the last accumulated usage report is requested by the PCF or not, and includes references to the targeted usage monitoring data instances.	UMC
praInfos	map(PresenceInfoRm)	O	1..N	Defines the PRA information provisioned by the PCF. The "praId" attribute within the PresenceInfo data type shall also be the key of the map. The "presenceState" attribute within the PresenceInfo data type shall not be supplied.	PRA
ipv4Index	IpIndex	C	0..1	Information that identifies the IP address allocation method for IPv4 address allocation. (NOTE 3)	
ipv6Index	IpIndex	C	0..1	Information that identifies the IP address allocation method for IPv6 address allocation. (NOTE 3)	
qosFlowUsage	QosFlowUsage	O	0..1	Indicates the required usage for default QoS flow.	
relCause	SmPolicyAssociationReleaseCause	O	0..1	The cause for which the PCF requests the termination of the policy association.	RespBasedSessionRel
suppFeat	SupportedFeatures	C	0..1	Indicates the list of negotiated supported features. This parameter shall be supplied by the PCF in the response to the POST request that requested the creation of an individual SM policy resource.	
tsnBridgeManCont	BridgeManagementContainer	O	0..1	Transports TSC user plane node management information	TimeSensitiveNetworking
tsnPortManContDstt	PortManagementContainer	O	0..1	Transports port management information for the DS-TT port.	TimeSensitiveNetworking
tsnPortManContNwtts	array(PortManagementContainer)	O	1..N	Transports port management information for one or more NW-TT ports.	TimeSensitiveNetworking
redSessIndication	boolean	O	0..1	Indicates whether the PDU Session is a redundant PDU session: true: end to end redundant PDU session; false: Not end to end redundant PDU session; If this attribute is absent it means the PDU session is not an end to end redundant PDU session. (NOTE 2) (NOTE 3)	Dual-Connectivity-redundant-UP-paths

NOTE 1: For IPv4v6 PDU session, both the "ipv4Index" attribute and "ipv6Index" attribute may be provisioned by the PCF.
NOTE 2: This attribute shall not be removed if it was provisioned.
NOTE 3: This attribute may only be supplied by the PCF in the response to the initial POST request that requested the creation of an individual SM policy resource.
NOTE 4: If both the "offline" attribute and the "online" attribute are omitted by the PCF, and when the "OfflineChOnly" feature is supported, if the "offlineChOnly" attribute is set to "false" or omitted by the PCF, the default charging method pre-configured at the SMF, if available, shall be applied to the PDU session. If both offline and online charging methods are pre-configured at the SMF, the SMF shall determine which one of them to be applied to the PDU session based on local policy. The "offline" attribute and the "online" attribute shall not be simultaneously present with the same value, i.e., both set to true or both set to false.
NOTE 5: If the "chargingInfo" attribute is not supplied by the PCF, the charging information configured at the SMF shall be applied to the PDU session.
NOTE 6: When the "OfflineChOnly" feature is supported and the "offlineChOnly" attribute is present and set to "true", the "online" attribute and the "offline" attribute shall not be present.

5.6.2.5 Type SmPolicyNotification

Table 5.6.2.5-1: Definition of type SmPolicyNotification

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

NOTE: Either the complete resource URI included in the "resourceUri" attribute or the "apiSpecificResourceUriPart" component (see clause 5.1) of the resource URI included in the "resourceUri" attribute can be used by the SMF for the identification of the individual SM policy resource related to the notification.

5.6.2.6 Type PccRule

Table 5.6.2.6-1: Definition of type PccRule

Attribute name	Data type	P	Cardinality	Description
flowInfos	array(FlowInformation)	C	1..N	An array of Ethernet or IP filter information. (NOTE 3
appId	string	C	0..1	A reference to the applicat detection filter configured (NOTE 3)
appDescriptor	ApplicationDescriptor	C	0..1	ATSSS rule application de shall be present when the session is a MA PDU sess SDF template contains an Identifier (i.e. when the "ap attribute is present).
contVer	ContentVersion	O	0..1	Indicates the content versi PCC rule.
pccRuleId	string	M	1	Univocally identifies the P within a PDU session.
precedence	Uinteger	O	0..1	Determines the order in wi PCC rule is applied relativ PCC rules within the same session. It shall be include "flowInfos" attribute is inclu may be included if the "ap attribute is included when initially provisions the PCC (NOTE 2) (NOTE 4)
afSigProtocol	AfSigProtocol	O	0..1	Indicates the protocol used signalling between the UE AF. The default value "NO_INFORMATION" sha the attribute is not present not been supplied previou
appReloc	boolean	O	0..1	It indicates that the applica cannot be relocated once of the application is select 5GC when it is included an "true". Indication of applica relocation possibility. The value "false" shall apply, if attribute is not present and been supplied previously.
easRedisInd	boolean	O	0..1	Indicates the EAS redisco required for the application included and set to "true". value is "false" if omitted. The indication shall be inv was applied unless it is pr again.
addrPreserInd	boolean	O	0..1	Indicates whether UE IP a should be preserved. This attribute shall set to " preserved, otherwise, set The default value "false" s if the attribute is not prese not been supplied previou
refQosData	array(string)	O	1..N	A reference to the QosDat type decision type. It is the described in clause 5.6.2.8 (NOTE 1)

refAltQosParams	array(string)	O	1..N	A Reference to the QoS D decisions for the Alternativ parameter sets of the serv flow. Only the "qosId" attri "gbrUl" attribute, the "gbrD the "packetDelayBudget" a and the "packetErrorRate" are applicable within the a QosData data types. This represents an ordered list, lower the index of the arra given entry, the higher the
refTcData	array(string)	O	1..N	A reference to the TrafficC policy decision type. It is tl described in clause 5.6.2.: (NOTE 1)
refChgData	array(string)	O	1..N	A reference to the Chargir policy decision type. It is tl described in clause 5.6.2.: (NOTE 1) (NOTE 7)
refChgN3gData	array(string)	O	1..N	A reference to the Chargir policy decision type only a Non-3GPP access. It is th described in clause 5.6.2.: (NOTE 1) (NOTE 5) (NOT
refUmData	array(string)	O	1..N	A reference to UsageMoni policy decision type. It is tl described in clause 5.6.2.: (NOTE 1)
refUmN3gData	array(string)	O	1..N	A reference to UsageMoni policy decision type only a Non-3GPP access. It is th described in clause 5.6.2.: (NOTE 1) (NOTE 6)
refCondData	string	O	0..1	A reference to the conditic the condId described in clause 5.6.2.9.
refQosMon	array(string)	O	1..N	A reference to QosMonitor policy decision type. It is tl described in clause 5.6.2.4 (NOTE 1)
tscaiInputUl	TscaiInputContainer	O	0..1	Transports TSCAI input pa for TSC traffic at the ingre of the DS-TT/UE (uplink fl direction).
tscaiInputDl	TscaiInputContainer	O	0..1	Transports TSCAI input pa for TSC traffic at the ingre NW-TT (downlink flow dire
tscaiTimeDom	Uinteger	O	0..1	Indicates the (g)PTP doma (TSN)AF is located in.
ddNotifCtrl	DownlinkDataNotificationControl	O	0.1	The Downlink Data Notific Control applying to the cor DDD Status event notifica DDN Failure event notifica attribute shall not be prese the DDNEventPolicyContr is supported.
ddNotifCtrl2	DownlinkDataNotificationControlRm	O	0..1	The Downlink Data Notific Control applying to the cor DDD Status event notifica DDN Failure event notifica including the removal of pr the downlink data notificat information.

	disUeNotif	boolean	O	0..1	Indicates to disable QoS fl parameters signalling to th the SMF is notified by the changes in the fulfilled Qo when it is included and se The fulfilled situation is eit QoS profile or an Alternati Profile. The default value ' apply, if the attribute is not and has not been supplied previously.

troduced for future compatibility. In this release of the specification the maximum number
array is 1.
th the "appId" attribute, the precedence can be preconfigured in SMF or provided in the
F. The precedence provided by the PCF shall take precedence.
os" attribute or "appId" attribute shall be supplied by the PCF when the PCC rule is initially
"appId" attribute is supplied, the PCF shall not modify the application identifier supplied
attribute later.
attribute is used to specify the precedence of the PCC rule among all PCC rules
e PDU session. It includes an integer value in the range from 0 to 255 (decimal). The
f the "precedence" attribute, the lower the precedence of that PCC rule is. The precedence
70 to 99 (decimal) shall be used for the PCC rules subject to Reflective QoS.
ssion, Charging Data decision referred by the "refChgData" attribute applies to both
s no "refChgN3gData" attribute included. If there is a "refChgN3gData" attribute included,
decision referred by the "refChgN3gData" attribute applies to non-3GPP access and the
cision referred by the "refChgData" attribute applies to 3GPP access. The value(s) of
the Charging Data decision except the "chgId" attribute referred by the "refChgN3gData"
he same as the one(s) within the Charging Data decision referred by the "refChgData"

ssion, Usage Monitoring Data decision referred by the "refUmData" attribute applies to
here is no "refUmN3gData" attribute included. If there is a "refUmN3gData" attribute
ge Monitoring Data decision referred by the "refUmN3gData" attribute applies to non-3GPP
sage Monitoring Data decision referred by the "refUmData" attribute applies to 3GPP

attribute and/or "refChgN3gData" attribute is/are provisioned for a PCC rule, then this
be subject to charging.

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	C	0..1	Authorized Session-AMBR. (NOTE 1)	
authDefQos	AuthorizedDefaultQos	C	0..1	Authorized default QoS information. (NOTE 1)	
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 clause 5.6.2.12. (NOTE 2)	UMC
refCondData	string	O	0..1	A reference to the condition data. It is the condId described in clause 5.6.2.9.	
refUmN3gData	string	O	0..1	A reference to UsageMonitoringData policy decision type to apply for Non-3GPP access. It is the umId described in clause 5.6.2.12. (NOTE 2)	UMC, ATSSS

NOTE 1: The PCF shall provide both "authSessAmbr" and the "authDefQos" attributes the first time the session rule is provisioned. The PCF shall ensure that a session rule enforced in the SMF contains the "authSessAmbr" and the "authDefQos" attributes.
NOTE 2: For a MA PDU session, if the "refUmN3gData" is omitted, the attribute "refUmData" contains the reference to the UsageMonitoringData policy decision to apply for both, 3GPP and Non-3GPP, accesses.

5.6.2.8 Type QosData

Table 5.6.2.8-1: Definition of type QosData

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

extMaxDataBurstVol	ExtMaxDataBurstVolRm	O	0..1	Denotes the largest amount of data that is required to be transferred within a period of 5G-AN PDB. (NOTE 1, NOTE 2)	EMDBV
packetDelayBudget	PacketDelBudget	O	0..1	Unsigned integer. It indicates the Packet Delay Budget expressed in milliseconds.	Authorization WithRequired QoS
packetErrorRate	PacketErrRate	O	0..1	String indicating the packet error rate. Examples: Packet Error Rate $4x10^{-6}$ shall be encoded as "4E-6". Packet Error Rate 10^{-2} shall be encoded as"1E-2".	Authorization WithRequired QoS
NOTE 1: Applicable only when a value different from the standardized value for this 5QI, provided in table 5.7.4-1 3GPP TS 23.501 [2], is required. NOTE 2: Either the maxDataBurstVol attribute or the extMaxDataBurstVol attribute may be present for a Delay Critical GBR QoS flow. If the maximum data burst volume value to be transmitted is lower than or equal to 4095 Bytes, the maxDataBurst Vol attribute is used. If the EMDBV feature is supported by both the PCF and the SMF, the extMaxDataBurstVol attribute is used to transmit the maximum data burst volume values higher than 4095 Bytes (see clause 4.2.2.1). NOTE 3: This attribute is only applicable to GBR type or delay critical GBR type 5QIs.					

5.6.2.9 Type ConditionData

Table 5.6.2.9-1: Definition of type ConditionData

Attribute name	Data type	P	Cardinality	Description	Applicability
condId	string	M	1	Uniquely identifies the condition data within a PDU session.	
activationTime	DateTimeRm	O	0..1	The time when the decision data shall be activated.	
deactivationTime	DateTimeRm	O	0..1	The time when the decision data shall be deactivated. (NOTE 1)	
accessType	AccessType	O	0..1	The condition of access type of the UE when the session AMBR shall be enforced. (NOTE 2)	AccessTypeCondition
ratType	RatType	O	0..1	The condition of RAT type of the UE when the session AMBR shall be enforced. (NOTE 2)	AccessTypeCondition
NOTE 1: It is only included in the ConditionData instance for conditioned PCC rule. NOTE 2: At least one of the "accessType" or "ratType" attributes shall be present in an access type conditioned session rule.					

5.6.2.10 Type TrafficControlData

Table 5.6.2.10-1: Definition of type TrafficControlData

Attribute name	Data type	P	Cardinality	Description	Applicability
tcId	string	M	1	Univocally identifies the traffic control policy data within a PDU session.	
flowStatus	FlowStatus	O	0..1	Enum determining what action to perform on traffic. Possible values are: [enable, disable, enable_uplink, enable_downlink]. The default value "ENABLED" shall apply, if the attribute is not present and has not been supplied previously.	
redirectInfo	RedirectInformation	O	0..1	It indicates whether the detected application traffic should be redirected to another controlled address.	ADC
addRedirectInfo	array(RedirectInformation)	O	1..N	Additional redirection information. Each element indicates whether the detected application traffic should be redirected to another controlled address.	ADCmultiRedirection
muteNotif	boolean	O	0..1	Indicates whether application's start or stop notifications are to be muted. The default value "FALSE" shall apply, if the attribute is not present and has not been supplied previously.	ADC
trafficSteeringPolIdDl (NOTE 1)	string	O	0..1	Reference to a pre-configured traffic steering policy for downlink traffic at the SMF.	TSC
trafficSteeringPolIdUl (NOTE 1)	string	O	0..1	Reference to a pre-configured traffic steering policy for uplink traffic at the SMF.	TSC
routeToLocs (NOTE 1)	array(RouteToLocation)	O	1..N	A list of location(s) to which the traffic shall be routed for the AF request.	TSC
maxAllowedUpLat	UintegerRm	O	0..1	Indicates the target user plane latency in units of milliseconds. The SMF may use this value to decide whether edge relocation is needed to ensure that the user plane latency does not exceed the value.	AF_latency
easIpReplaceInfos	array(EasIpReplacementInfo)	O	1..N	Contains EAS IP replacement information.	EASIPreplacement
traffCorreInd	boolean	O	0..1	Indication of traffic correlation. If it is included and set to "true", traffic should be correlated; The default value "false" applies, if the attribute is not present and has not been supplied previously. (NOTE 2)	
simConnInd	boolean	O	0..1	Indication of simultaneous connectivity temporarily maintained for the source and target PSA. If it is included and set to "true", temporary simultaneous connectivity should be kept. The default value "false" applies, if the attribute is not present and has not been supplied previously.	SimultConnectivity
simConnTerm	DurationSec	C	0..1	Indication of the minimum time interval to be considered for inactivity of the traffic routed via the source PSA during the edge re-location procedure. It may be included when the "simConnInd" attribute is set to true.	SimultConnectivity
upPathChgEvent	UpPathChgEvent	O	0..1	Contains the information about the AF subscription to UP path change events.	TSC
steerFun	SteeringFunctionality	O	0..1	Indicates the applicable traffic steering functionality.	ATSSS

steerModeDl	SteeringMode	O	0..1	Determines the traffic distribution rule across 3GPP and Non-3GPP accesses to apply for downlink traffic.	ATSSS
steerModeUl	SteeringMode	O	0..1	Determines the traffic distribution rule across 3GPP and Non-3GPP accesses to apply for uplink traffic.	ATSSS
mulAccCtrl	MulticastAccessControl	O	0..1	Indicates whether the service data flow, corresponding to the service data flow template, is allowed or not allowed. The default value "NOT_ALLOWED" applies, if the attribute is not present and has not been supplied previously.	WWC
NOTE 1: Traffic steering policy identifier(s) (i.e. "trafficSteeringPolIdDl" attribute and/or "trafficSteeringPolIdUl" attribute) and N6 traffic routing requirements (i.e. "routeToLocs" attribute) are mutually exclusive. NOTE 2: The TSC feature shall be supported in order to support this attribute.					

5.6.2.11 Type ChargingData

Table 5.6.2.11-1: Definition of type ChargingData

Attribute name	Data type	P	Cardinality	Description	Applicability
chgId	string	M	1	Univocally identifies the charging control policy data within a PDU session.	
meteringMethod	MeteringMethod	O	0..1	Defines what parameters shall be metered for offline charging. If the attribute is not present but it has been supplied previously, the previous information remains valid. If the attribute is not present and it has not been supplied previously or the attribute has been supplied previously but the attribute is set to NULL, the metering method pre-configured at the SMF is applicable as default metering method.	
offline	boolean	O	0..1	Indicates the offline charging is applicable to the PCC rule when it is included and set ot true. (NOTE 1)	
online	boolean	O	0..1	Indicates the online charging is applicable to the PCC rule when it is included and set ot true. (NOTE 1, NOTE 5)	
sdfHandl	boolean	O	0..1	Indicates whether the service data flow is allowed to start while the SMF is waiting for the response to the credit request. The default value "FALSE" (blocking) shall apply, if the attribute is not present. (NOTE 2)	
ratingGroup	RatingGroup	O	0..1	The charging key for the PCC rule used for rating purposes.	
reportingLevel	ReportingLevel	O	0..1	Defines on what level the SMF reports the usage for the related PCC rule. If the attribute is not present but it has been supplied previously, the previous information remains valid. If the attribute is not present and it has not been supplied previously or the attribute has been supplied previously but it is set to NULL, the reporting level pre-configured at the SMF is applicable as default reporting level.	
serviceId	ServiceId	O	0..1	Indicates the identifier of the service or service component the service data flow in a PCC rule relates to.	
sponsorId	string	O	0..1	Indicates the sponsor identity.	SponsoredConnectivity
appSvcProvId	string	O	0..1	Indicates the application service provider identity.	SponsoredConnectivity
afChargingIdentifier	ChargingId	C	0..1	An identifier, provided from the AF, correlating the measurement for the Charging key/Service identifier values in this PCC rule with application level reports. (NOTE 4)	
afChargId	ApplicationChargingId	O	0..1	A character string identifier, provided from the AF, correlating the measurement for the Charging key/Service identifier values in this PCC rule with application level reports. (NOTE 3)	AF_Charging_Identifier

NOTE 1: The absence of both the "offline" attribute and "online" attribute or only one attribute is present and set to false within a Charging Data decision instance indicates that the default charging method of the PDU session is applicable to the PCC rule referring to the Charging Data decision. Either "offline" attribute or "online" attribute set to true shall be provisioned initially if there is no default charging method applied to the PDU session. The "offline" attribute and the "online" attribute shall not be simultaneously present with the same value, i.e. both set to "true" or both set to "false".
NOTE 2: The "sdfHandl" attribute shall not be present when the online charging method does not apply for the PCC rule referring to the Charging Data decision (i.e., when the "online" attribute is present and set to false, or is absent and the online default charging method does not apply for the PDU session, or is absent and there is no online default charging method defined).
NOTE 3: The "afChargId" attribute shall be used instead of the "afChargingIdentifier" attribute when the "AF_Charging_Identifier" feature is supported.
NOTE 4: The "afChargingIdentifier" attribute shall not be present when the "AF_Charging_Identifier" feature is supported. When the "AF_Charging_Identifier" feature is not supported it is out of the scope of the specification what the behaviour of the PCF is when the AF provides charging identifier values that are out of ChargingId data type value range.
NOTE 5: When the "OfflineChOnly" feature is supported and the "offlineChOnly" attribute is present and set to "true" within the SmPolicyDecision data structure, then the "online" attribute shall not be present.

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

5.6.2.13 Type RedirectInformation

Table 5.6.2.13-1: Definition of type RedirectInformation

Attribute name	Data type	P	Cardinality	Description	Applicability
redirectEnabled	boolean	C	0..1	This attribute indicates whether the redirect instruction is enabled. It shall be included and set to true when the redirect instruction is provisioned initially within a PCC rule. Subsequently: - It may be included to disable or re-enable the redirect instruction. - Otherwise, if the attribute is omitted, the previous value shall apply.	
redirectAddressType	RedirectAddressType	O	0..1	Indicates the type of redirect address contained within the "redirectServerAddress" attribute.	
redirectServerAddress	string	O	0..1	Indicates the address of the redirect server. - If the "redirectAddressType" attribute indicates "IPV4_ADDR", the encoding is the same as the Ipv4Addr data type defined in 3GPP TS 29.571 [11]. - If the "redirectAddressType" attribute indicates "IPV6_ADDR", the encoding is the same as the Ipv6Addr data type defined in 3GPP TS 29.571 [11]. - If the "redirectAddressType" attribute indicates "URL" or "SIP_URI", the encoding is the same as the Uri data type defined in 3GPP TS 29.571 [11].	

5.6.2.14 Type FlowInformation

Table 5.6.2.14-1: Definition of type FlowInformation

Attribute name	Data type	P	Cardinality	Description	Applicability
flowDescription	FlowDescription	O	0..1	Contains the packet filters of the IP flow(s).	
ethFlowDescription	EthFlowDescription	O	0..1	Defines a packet filter for an Ethernet flow. If the "fDir" attribute is included, it shall be set to "DOWNLINK". If the "fDir" attribute is never provided, the address information within the "ethFlowDescription" attribute shall be encoded in downlink direction.	
packFiltId	string	O	0..1	An identifier of packet filter. (NOTE)	
packetFilterUsage	boolean	O	0..1	The packet shall be sent to the UE. The default value "FALSE" shall apply, if the attribute is not present and has not been supplied previously.	
tosTrafficClass	string	O	0..1	2-octet string. The first octet contains the Ipv4 Type-of-Service or the Ipv6 Traffic-Class field and the second octet contains the ToS/Traffic mask field in hexadecimal representation. Each character in the string shall take a value of "0" to "9" or "A" to "F" and shall represent 4 bits. One example is that of a TFT packet filter as defined in 3GPP TS 24.008 [41].	
spi	string	O	0..1	4 octet string, representing the security parameter index of the IPSec packet in hexadecimal representation. Each character in the string shall take a value of "0" to "9" or "A" to "F" and shall represent 4 bits. One example is that of a TFT packet filter as defined in 3GPP TS 24.008 [41].	
flowLabel	string	O	0..1	3-octet string, representing the Ipv6 flow label header field in hexadecimal representation. Each character in the string shall take a value of "0" to "9" or "A" to "F" and shall represent 4 bits. One example is that of a TFT packet filter as defined in 3GPP TS 24.008 [41].	
flowDirection	FlowDirectionRm	O	0..1	Indicates the direction/directions that a filter is applicable, downlink only, uplink only or both down- and uplink (bidirectional).	
NOTE: The PCF shall only assign the "packFiltId" attribute for PCC rules created as a result of UE-initiated resource allocation.					

5.6.2.15 Type SmPolicyDeleteData

Table 5.6.2.15-1: Definition of type SmPolicyDeleteData

Attribute name	Data type	P	Cardinality	Description	Applicability
userLocationInfo	UserLocation	O	0..1	The location(s) where the served UE is camping. (NOTE 2)	RAN-NAS-Cause, NetLoc
ueTimeZone	TimeZone	O	0..1	The time zone where the served UE is camping.	RAN-NAS-Cause, NetLoc
userLocationInfoTime	DateTime	O	0..1	Contains the NTP time at which the UE was last known to be in the location contained in the "userLocationInfo" attribute. (NOTE 1)	RAN-NAS-Cause, NetLoc
servingNetwork	PlmnIdNid	O	0..1	The serving network (a PLMN or an SNPN) where the served UE is camping. For the SNPN, the NID together with the PLMN ID identifies the SNPN.	NetLoc
ranNasRelCauses	array(RanNasRelCause)	O	1..N	Indicates the RAN and/or NAS release cause(s) code information.	RAN-NAS-Cause
accuUsageReports	array(AccuUsageReport)	O	1..N	Contains the accumulated usage reporting information.	UMC
pduSessRelCause	PduSessionRelCause	O	0..1	Indicates PDU session release cause.	PDUSessionRelCause, ImmediateTermination
qosMonReports	array(QosMonitoringReport)	O	1..N	QoS Monitoring reporting information.	QosMonitoring

NOTE 1: The age of UE location included within the "userLocationInfoTime" attribute is the age of the 3GPP access UE location received from the AMF and shall be included only when the reported "userLocationInfo" attribute includes the UE location in the 3GPP access.
NOTE 2: The SMF may encode both 3GPP and non-3GPP access UE location in the "userLocationInfo" attribute.

5.6.2.16 Type QosCharacteristics

Table 5.6.2.16-1: Definition of type QosCharacteristics

Attribute name	Data type	P	Cardinality	Description	Applicability
5qi	5Qi	M	1	Identifier for the authorized QoS parameters for the service data flow. Applies to PCC rule and PDU session level.	
resourceType	QosResourceType	M	1	Indicates whether the resource type is GBR, delay critical GBR, or non-GBR.	
priorityLevel	5QiPriorityLevel	M	1	Unsigned integer indicating the 5QI Priority Level, within a range of 1 to 127.	
packetDelayBudget	PacketDelBudget	M	1	Unsigned integer indicates the packet delay budget. Packet Delay Budget expressed in milliseconds.	
packetErrorRate	PacketErrRate	M	1	String indicating the packet error rate. Examples: Packer Error Rate $4x10^{-6}$ shall be encoded as "4E-6". Packer Error Rate 10^{-2} shall be encoded as"1E-2".	
averagingWindow	AverWindow	C	0..1	Indicates the averaging window. This IE shall be present only for a GBR QoS flow or a Delay Critical GBR QoS flow.	
maxDataBurstVol	MaxDataBurstVol	C	0..1	Unsigned Integer. Indicates the maximum data burst volume. (NOTE)	
extMaxDataBurstVol	ExtMaxDataBurstVol	C	0..1	Unsigned Integer. Indicates the maximum data burst volume. (NOTE)	EMDBV
NOTE: Either the maxDataBurstVol IE or the extMaxDataBurstVol IE may be present for a Delay Critical GBR QoS flow. If the maximum data burst volume value to be transmitted is lower than or equal to 4095 Bytes, the maxDataBurst Vol IE is used. If the EMDBV feature is supported by both the PCF and the SMF, the extMaxDataBurstVol IE is used to transmit maximum data burst volume values higher than 4095 Bytes (see clause 4.2.2.1).					

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 {apiRoot} part, either in the form of an FQDN or IPAddress/Port Number, of the URI, of the primary CHF instance. (NOTE 1) (NOTE 2)	
secondaryChfAddress	Uri	C	0..1	Contains the {apiRoot} part, either in the form of an FQDN or IPAddress/Port Number, of the URI, of the secondary CHF instance. It shall be present if the feature "CHFsetSupport" is not supported. It may be omitted if the feature "CHFsetSupport" is supported (NOTE 1) (NOTE 2)	
primaryChfSetId	NfSetId	C	0..1	The CHF set ID that the primary CHF instance belongs to may complement the primary CHF address and shall be present, if available. (NOTE 2)	
primaryChfInstanceId	NfInstanceId	C	0..1	The CHF instance ID of the primary CHF instance may complement the primary CHF address and shall be present, if available. (NOTE 2)	
secondaryChfSetId	NfSetId	C	0..1	The CHF set ID that the secondary CHF instance belongs to may complement the secondary CHF address and shall be present, if available, and the feature "CHFsetSupport" is not supported. It may be omitted if available and the feature "CHFsetSupport" is supported.	
secondaryChfInstanceId	NfInstanceId	C	0..1	The CHF instance ID of the secondary CHF instance may complement the secondary CHF address and shall be present, if available, and the feature "CHFsetSupport" is not supported. It may be omitted if available and the feature "CHFsetSupport" is supported.	

NOTE 1: Based on the {apiRoot} of the CHF instance in the form of an FQDN, the consumer can derive the Nfinstance via NRF lookup. It is up to the consumer to determine which service to invoke from the CHF. The {apiRoot} shall apply to all CHF services.

NOTE 2: The NF Service Consumer of the CHF may use the "primaryChfAddress"/"secondaryChfAddress" attributes as primary/secondary redundancy mechanism, or alternatively, when CHF instance and CHF set are available, it may also rely on the availability of a CHF instance within the CHF Set for the same purpose.

5.6.2.18 Type AccuUsageReport

Table 5.6.2.18-1: Definition of type AccuUsageReport

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

5.6.2.19 Type SmPolicyUpdateContextData

Table 5.6.2.19-1: Definition of type SmPolicyUpdateContextData

Attribute name	Data type	P	Cardinality	Description	Applicability
repPolicyCtrlReqTriggers	array(PolicyControlRequestTrigger)	C	1..N	The policy control request triggers which are met. It is omitted if no triggers are met such as in clauses 4.2.4.7 and 4.2.4.15.	
accNetChIds	array(AccNetChId)	O	1..N	Indicates the access network charging identifier for the PCC rule(s) or whole PDU session.	
accessType	AccessType	O	0..1	The Access Type where the served UE is camping.	
ratType	RatType	O	0..1	The RAT Type where the served UE is camping.	
addAccessInfo	AdditionalAccessInfo	O	0..1	Indicates the combination of added Access Type and RAT Type for MA PDU session.	ATSSS
relAccessInfo	AdditionalAccessInfo	O	0..1	Indicates the combination of released Access Type and RAT Type for MA PDU session.	ATSSS
servingNetwork	PlmnIdNid	O	0..1	The serving network (a PLMN or an SNPN) where the served UE is camping. For the SNPN the NID together with the PLMN ID identifies the SNPN.	
userLocationInfo	UserLocation	O	0..1	The location(s) where the served UE is camping. (NOTE 4)	
ueTimeZone	TimeZone	O	0..1	The time zone where the served UE is camping.	
ipv4Address	Ipv4Addr	O	0..1	The IPv4 Address of the served UE.	
ipDomain	string	O	0..1	IPv4 address domain identifier. (NOTE 2)	
relIpv4Address	Ipv4Addr	O	0..1	Indicates the released IPv4 Address of the served UE.	
ipv6AddressPrefix	Ipv6Prefix	O	0..1	The Ipv6 Address Prefix of the served UE.	
relIpv6AddressPrefix	Ipv6Prefix	O	0..1	Indicates the released IPv6 Address Prefix of the served UE in multi-homing case.	
relUeMac	MacAddr48	O	0..1	Indicates the released MAC Address of the served UE.	
ueMac	MacAddr48	O	0..1	The MAC Address of the served UE.	
subsSessAmbr	Ambr	O	0..1	UDM subscribed or DN-AAA authorized Session-AMBR.	
authProfIndex	string	O	0..1	DN-AAA authorization profile index.	DN-Authorization
subsDefQos	SubscribedDefaultQos	O	0..1	Subscribed Default QoS Information.	
vplmnQos	VplmnQos	O	0..1	QoS constraints in a VPLMN (NOTE 5)	VPLMN-QoS-Control
vplmnQosNotApp	boolean	O	0..1	If it is included and set to true, indicates that the QoS constraints in the VPLMN are not applicable. (NOTE 5)	VPLMN-QoS-Control
numOfPackFilter	integer	O	0..1	Contains the number of supported packet filter for signalled QoS rules. (NOTE 1)	
accuUsageReports	array(AccuUsageReport)	O	1..N	Contains the accumulated usage report(s).	UMC
3gppPsDataOffStatus	boolean	O	0..1	If it is included and set to true, the 3GPP PS Data Off is activated by the UE.	3GPP-PS-Data-Off
appDetectionInfos	array(AppDetectionInfo)	O	1..N	Reports the start/stop of the application traffic and detected SDF descriptions if applicable.	ADC
ruleReports	array(RuleReport)	O	1..N	Used to report the PCC rule failure.	
sessRuleReports	array(SessionRuleReport)	O	1..N	Used to report the session rule failure.	SessionRuleErrorHandling

qncReports	array(QosNotificationControlInfo)	O	1..N	QoS Notification Control information.	
qosMonReports	array(QosMonitoringReport)	O	1..N	QoS Monitoring reporting information.	QosMonitoring
userLocationInfoTime	DateTime	O	0..1	Contains the NTP time at which the UE was last known to be in the location. (NOTE 3)	
repPraInfos	map(PresenceInfo)	O	1..N	Reports the changes of presence reporting area. The "praId" attribute within the PresenceInfo data type shall also be the key of the map. The "presenceState" attribute within the PresenceInfo data type shall be supplied. The "additionalPraId" attribute within the PresenceInfo data type shall not be supplied.	PRA
ueInitResReq	UeInitiatedResourceRequest	O	0..1	Indicates a UE requests specific QoS handling for selected SDF.	
refQosIndication	boolean	O	0..1	If it is included and set to true, the reflective QoS is supported by the UE. If it is included and set to false, the reflective QoS is revoked by the UE.	
qosFlowUsage	QosFlowUsage	O	0..1	Indicates the required usage for default QoS flow.	
creditManageStatus	CreditManagementStatus	O	0..1	Indicates the reason of the credit management session failure.	
servNfId	ServingNfIdentity	O	0..1	Contains the serving network function identity.	
traceReq	TraceData	C	0..1	It shall be included if trace is required to be activated, modified or deactivated (see 3GPP TS 32.422 [24]). For trace modification, it shall contain a complete replacement of trace data. For trace deactivation, it shall contain the Null value.	
addIpv6AddrPrefixes	array(Ipv6Prefix)	O	1..N	The Ipv6 Address Prefixes of the served UE. (NOTE 6)	MultiIpv6AddrPrefix
addRelIpv6AddrPrefixes	array(Ipv6Prefix)	O	1..N	Indicates the released IPv6 Address Prefixes of the served UE in multi-homing case. (NOTE 6)	MultiIpv6AddrPrefix
tsnBridgeInfo	TsnBridgeInfo	O	0..1	Transports TSN bridge information.	TimeSensitiveNetworking
tsnBridgeManCont	BridgeManagementContainer	O	0..1	Transports TSN bridge management information.	TimeSensitiveNetworking
tsnPortManContDstt	PortManagementContainer	O	0..1	Transports TSN port management information for the DS-TT port.	TimeSensitiveNetworking
tsnPortManContNwtts	array(PortManagementContainer)	O	1..N	Transports TSN port management information for one or more NW-TT ports.	TimeSensitiveNetworking
maPduInd	MaPduIndication	O	0..1	Contains the MA PDU session indication, i.e., MA PDU Request or MA PDU Network-Upgrade Allowed. (NOTE 1)	ATSSS
atsssCapab	AtsssCapability	O	0..1	Contains the ATSSS capability supported for the MA PDU session. (NOTE 1)	ATSSS
mulAddrInfos	array(IpMulticastAddressInfo)	O	1..N	Contains the IP multicast address information.	WWC
policyDecFailureReports	array(PolicyDecisionFailureCode)	O	1..N	Indicates the type(s) of the failed policy decision and/or condition data.	PolicyDecisionErrorHandling
invalidPolicyDecs	array(InvalidParam)	O	1..N	Indicates the invalid parameters for the reported type(s) of the failed policy decision and/or condition data.	ExtPolicyDecisionErrorHandling
trafficDescriptors	array(DddTrafficDescriptor)	O	1..N	Contains the traffic descriptor(s)	DDNEventPolicyControl

typesOfNotif	array(DlDataDeliveryStatus)	O	1..N	Contains the type of notification of DDD Status.	DDNEventPolicyControl
pccRuleId	string	O	0..1	Contains the identifier of the PCC rule which is used for traffic detection of event (e.g. DDN failure).	DDNEventPolicyControl2
interGrpIds	array(GroupId)	O	1..N	Internal Group Identifier(s) of the served UE.	GroupIdListChange
satBackhaulCategory	SatelliteBackhaulCategory	O	0..1	Satellite backhaul category or non-satellite backhaul used for the PDU session.	SatBackhaulCategoryChg
pcfUeInfo	PcfUeCallbackInfo	O	0..1	PCF for the UE callback URI and SBA binding information.	AMInfluence
nwdafDatas	array(NwdafData)	O	1..N	List of NWDAF Instance IDs and their associated Analytics IDs consumed by the NF service consumer.	EneNA
anGwStatus	boolean	O	1..N	When it is included and set to true, it indicates that the AN-Gateway has failed and that the PCF should refrain from sending policy decisions to the SMF until it is informed that the AN-Gateway has been recovered. (NOTE 1)	SGWRest

NOTE 1: This attribute is only applicable to the 5GS and EPC/E-UTRAN interworking scenario as defined in Annex B.
NOTE 2: The value provided in this attribute is implementation specific. The only constraint is that the NF service consumer shall supply a different identifier for each overlapping address domain (e.g. the SMF NF instance identifier).
NOTE 3: The age of UE location included within the "userLocationInfoTime" attribute is the age of the 3GPP access UE location received from the AMF and shall be included only when the reported "userLocationInfo" attribute includes the UE location in the 3GPP access.
NOTE 4: The SMF may encode both 3GPP and non-3GPP access UE location in the "userLocationInfo" attribute.
NOTE 5: Only one of "vplmnQos" or "vplmnQosNotApp" attributes may be present.
NOTE 6: When the "WWC" feature is supported, IPv6 prefix(es) shorter than /64 or full IPv6 address(es) with a /128 prefix may be encoded as the "addIpv6Prefixes" and the "addRelIpv6Prefixes" attributes, according to 3GPP TS 23.316 [42], clause 8.3.1 and 4.6.2.

5.6.2.20 Type UpPathChgEvent

Table 5.6.2.20-1: Definition of type UpPathChgEvent

Attribute name	Data type	P	Cardinality	Description	Applicability
notificationUri	Uri	M	1	Notification address of AF receiving the event notification.	TSC
notifCorreId	string	M	1	It is used to set the value of Notification Correlation ID in the notification sent by the NF service consumer.	TSC
dnaiChgType	DnaiChangeType	M	1	Indicates the type of DNAI change.	TSC
afAckInd	boolean	O	0..1	Identifies whether the AF acknowledgement of UP path event notification is expected. Set to "true" if the AF acknowledge is expected; otherwise set to "false". Default value is "false" if omitted.	URLLC

5.6.2.21 Type TerminationNotification

Table 5.6.2.21-1: Definition of type TerminationNotification

Attribute name	Data type	P	Cardinality	Description	Applicability
resourceUri	Uri	M	1	The resource URI of the individual SM policy resource related to the notification. (NOTE)	
cause	SmPolicyAssociationReleaseCause	M	1	The cause why the PCF requests the termination of the policy association.	
NOTE: Either the complete resource URI included in the "resourceUri" attribute or the "apiSpecificResourceUriPart" component (see clause 5.1) of the resource URI included in the "resourceUri" attribute can be used by the SMF for the identification of the individual SM policy resource related to the notification.					

5.6.2.22 Type AppDetectionInfo

Table 5.6.2.22-1: Definition of type AppDetectionInfo

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	0..1	Identifier dynamically assigned by the NF service consumer in order to allow correlation of application Start and Stop events to the specific service data flow description, if service data flow descriptions are deducible.	
sdfDescriptions	array(FlowInformation)	O	1..N	Contains the detected service data flow descriptions if they are deducible. When present, it shall only include the "flowDescription" and the "flowDirection" attributes of the FlowInformation data type.	

5.6.2.23 Type AccNetChId

Table 5.6.2.23-1: Definition of type AccNetChId

Attribute name	Data type	P	Cardinality	Description	Applicability
accNetChaIdValue	ChargingId	C	0..1	Contains a charging identifier. (NOTE 1)	
accNetChargIdString	string	C	0..1	A character string containing the charging identifier (see clause 5.1.9.1 of 3GPP TS 32.255 [35]). (NOTE 1)	AccNetChargId_String
refPccRuleIds	array(string)	O	1..N	Contains the identifier of the PCC rule(s) that are associated to the provided Access Network Charging Identifier.	
sessionChScope	boolean	O	0..1	When included and set to true, it indicates that the provided Access Network Charging Identifier applies to the whole PDU Session. Default value is false if omitted.	
NOTE 1: The "accNetChaIdValue" shall be used to encode the charging identifier when the charging identifier is within the Uint32 value range. The "accNetChargIdString" attribute shall be used to encode the charging identifier when the "AccNetChargId_String" feature is supported by the SMF and the PCF and the charging identifier is out of the Uint32 range. NOTE 2: When the "AccNetChargId_String" feature is not supported and the value of the charging identifier is out of the ChargingId data type value range (Uint32) it is not possible to ensure a proper charging correlation using value of the "accNetChaIdValue" attribute.					

5.6.2.24 Type RequestedRuleData

Table 5.6.2.24-1: Definition of type RequestedRuleData

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

5.6.2.25 Type RequestedUsageData

Table 5.6.2.25-1: Definition of type RequestedUsageData

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

5.6.2.26 Type UeCampingRep

Table 5.6.2.26-1: Definition of type UeCampingRep

Attribute name	Data type	P	Cardinality	Description	Applicability
accessType	AccessType	O	0..1	The Access Type where the served UE is camping.	
ratType	RatType	O	0..1	The RAT Type where the served UE is camping.	
servNfId	ServingNfIdentity	O	0..1	Contains the serving network function identity.	
servingNetwork	PlmnIdNid	O	0..1	The serving network (a PLMN or an SNPN) where the served UE is camping. For an SNPN the NID together with the PLMN ID identifies the SNPN.	
userLocationInfo	UserLocation	O	0..1	The location(s) of the served UE. (NOTE)	
ueTimeZone	TimeZone	O	0..1	The time zone where the served UE is camping.	
netLocAccSupp	NetLocAccessSupport	O	0..1	Indicates that the access network does not support the reporting of the requested access network information.	NetLoc
NOTE: The SMF may encode both 3GPP and non-3GPP access UE location in the "userLocationInfo" attribute.					

5.6.2.27 Type RuleReport

Table 5.6.2.27-1: Definition of type RuleReport

Attribute name	Data type	P	Cardinality	Description	Applicability
pccRuleIds	array(string)	M	1..N	Contains the identifier(s) of the affected PCC rule(s).	
ruleStatus	RuleStatus	M	1	Indicates the status of the PCC rule(s).	
contVers	array(ContentVersion)	C	1..N	Indicates the version(s) of the PCC rule(s). If the RuleVersioning feature is supported, the content version shall be included in this attribute if it was included when the corresponding PCC rule was installed or modified.	RuleVersioning
failureCode	FailureCode	C	0..1	Indicates the reason why the PCC Rule(s) are being reported. It shall be included when the NF service consumer reports the failure of the enforcement of the PCC rule(s).	
finUnitAct	FinalUnitAction	O	0..1	Contains the related filter parameters and redirect address parameters (if available), when the user's account cannot cover the service cost.	
ranNasRelCauses	array(RanNasRelCause)	O	1..N	Indicates the RAN or NAS release cause code information.	RAN-NAS-Cause
altQosParamId	string	O	0..1	Indicates the alternative QoS parameter set that the NG-RAN can guarantee. It is included during the report of success resource allocation and indicates that NG-RAN used an alternative QoS profile because the requested QoS could not be allocated.	AuthorizationWithRequiredQoS

5.6.2.28 Type RanNasRelCause

Table 5.6.2.28-1: Definition of type RanNasRelCause

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

5.6.2.29 Type UeInitiatedResourceRequest

Table 5.6.2.29-1: Definition of type UeInitiatedResourceRequest

Attribute name	Data type	P	Cardinality	Description	Applicability
pccRuleId	string	C	1	Indicates a PCC rule corresponding to a QoS rule which is requested to be modified or deleted by the UE.	
ruleOp	RuleOperation	M	1	Indicates an operation for the PCC rule.	
packFiltInfo	array(PacketFilterInfo)	M	1..N	Contains the information from a single packet filter sent from the NF service consumer to the PCF.	
precedence	integer	O	0..1	The requested order for the PCC rule generated from the QoS rule requested by the UE.	
reqQos	RequestedQos	O	0..1	Contains the QoS information requested by the UE.	

5.6.2.30 Type PacketFilterInfo

Table 5.6.2.30-1: Definition of type PacketFilterInfo

Attribute name	Data type	P	Cardinality	Description	Applicability
packFiltId	string	O	0..1	An identifier of packet filter. For PCC rules created as a result of UE-initiated resource modification, the packet filter identifier is assigned by the PCF and is unique per UE and PCF instance.	
packFiltCont	PacketFilterContent	O	0..1	Contains the content of the packet filter as requested by the UE and required by the PCF to create the PCC rules.	
tosTrafficClass	string	O	0..1	2-octet string. The first octet contains the Ipv4 Type-of-Service or the Ipv6 Traffic-Class field and the second octet contains the ToS/Traffic mask field in hexadecimal representation. Each character in the string shall take a value of "0" to "9" or "A" to "F" and shall represent 4 bits. One example is that of a TFT packet filter as defined in 3GPP TS 24.008 [41].	
spi	string	O	0..1	4 octet string, representing the security parameter index of the IPSec packet in hexadecimal representation. Each character in the string shall take a value of "0" to "9" or "A" to "F" and shall represent 4 bits. One example is that of a TFT packet filter as defined in 3GPP TS 24.008 [41].	
flowLabel	string	O	0..1	3-octet string, representing the Ipv6 flow label header field in hexadecimal representation. Each character in the string shall take a value of "0" to "9" or "A" to "F" and shall represent 4 bits. One example is that of a TFT packet filter as defined in 3GPP TS 24.008 [41].	
flowDirection	FlowDirection	O	0..1	Indicates the direction/directions that a filter is applicable, downlink only, uplink only or both down- and uplink (bidirectional).	

5.6.2.31 Type RequestedQos

Table 5.6.2.31-1: Definition of type RequestedQos

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

5.6.2.32 Type QosNotificationControlInfo

Table 5.6.2.32-1: Definition of type QosNotificationControlInfo

Attribute name	Data type	P	Cardinality	Description	Applicability
refPccRuleIds	array(string)	M	1..N	An array of PCC rule id references to the PCC rules associated with the QosNotificationControlInfo.	
notifType	QosNotifType	M	1	Indicates whether the GBR targets for the indicated SDFs are "NOT_GUARANTEED" or "GUARANTEED" again.	
contVers	array(ContentVersion)	C	1..N	Indicates the version of the PCC rule. If rule versioning feature is supported, the content version shall be included if it was included when the corresponding PCC rule was installed or modified.	RuleVersioning
altQosParamId	string	O	0..1	Indicates the alternative QoS parameter set the NG-RAN can guarantee. When it is omitted and "notifType" attribute is NOT_GUARANTEED, it indicates that the lowest priority alternative QoS profile could not be fulfilled.	AuthorizationWithRequiredQoS

5.6.2.33 Type PartialSuccessReport

Table 5.6.2.33-1: Definition of type PartialSuccessReport

Attribute name	Data type	P	Cardinality	Description	Applicability
failureCause	FailureCause	M	1	Application error cause specific to this report.	
ruleReports	array(RuleReport)	C	1..N	Information about the PCC rules provisioned by the PCF not successfully installed/activated.	
sessRuleReports	array(SessionRuleReport)	O	1..N	Information about the session rules provisioned by the PCF not successfully installed.	SessionRuleErrorHandling
ueCampingRep	UeCampingRep	O	0..1	Includes the current applicable values corresponding to the provisioned policy control request triggers.	
policyDecFailureReports	array(PolicyDecisionFailureCode)	O	1..N	Used to report the failure of the policy decision and/or condition data.	PolicyDecisionErrorHandling
invalidPolicyDecs	array(InvalidParam)	O	1..N	Indicates the invalid parameters for the reported type(s) of the failed policy decision and/or condition data.	ExtPolicyDecisionErrorHandling
NOTE: The "ruleReports" shall be included if the SessionRuleErrorHandling feature or the PolicyDecisionErrorHandling feature is not supported.					

5.6.2.34 Type AuthorizedDefaultQos

Table 5.6.2.34-1: Definition of type AuthorizedDefaultQos

Attribute name	Data type	P	Cardinality	Description	Applicability
5qi	5Qi	C	0..1	5G QoS Identifier. It shall be included when the Authorized Default QoS is initially provisioned.	
arp	Arp	C	0..1	Indicates the allocation and retention priority. It shall be included when the Authorized Default QoS is initially provisioned.	
priorityLevel	5QiPriorityLevelRm	O	0..1	Unsigned integer indicating the 5QI Priority Level, within a range of 1 to 127.	
averWindow	AverWindowRm	O	0..1	Indicates the averaging window. (NOTE 1)	
maxDataBurstVol	MaxDataBurstVolRm	O	0..1	Unsigned integer indicating the maximum data burst volume. (NOTE 2)	
gbrUl	BitRateRm	O	0..1	Indicates the guaranteed bandwidth in uplink. (NOTE 1)	
gbrDl	BitRateRm	O	0..1	Indicates the guaranteed bandwidth in downlink. (NOTE 1)	
maxbrUl	BitRateRm	O	0..1	Indicates the max bandwidth in uplink. (NOTE 1)	
maxbrDl	BitRateRm	O	0..1	Indicates the max bandwidth in downlink. (NOTE 1)	
extMaxDataBurstVol	ExtMaxDataBurstVolRm	O	0..1	Unsigned integer indicating the maximum data burst volume. (NOTE 2)	EMDBV
NOTE 1: This attribute is only applicable to GBR type or delay critical GBR type 5QI. NOTE 2: Either the maxDataBurstVol IE or the extMaxDataBurstVol IE may be present for a Delay Critical GBR QoS flow. If the maximum data burst volume value to be transmitted is lower than or equal to 4095 Bytes, the maxDataBurst Vol IE is used. If the EMDBV feature is supported by both the PCF and the SMF, the extMaxDataBurstVol IE is used to transmit maximum data burst volume values higher than 4095 Bytes (see clause 4.2.2.1).					

5.6.2.35 Type AccNetChargingAddress

Table 5.6.2.35-1: Definition of type AccNetChargingAddress

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

5.6.2.36 Type ErrorReport

Table 5.6.2.36-1: Definition of type ErrorReport

Attribute name	Data type	P	Cardinality	Description	Applicability
error	ProblemDetails	M	1	More information on the error shall be provided in the "cause" attribute of the "ProblemDetails" structure.	
ruleReports	array(RuleReport)	O	1..N	Used to report the PCC rule failure.	
sessRuleReports	array(SessionRuleReport)	O	1..N	Used to report the session rule failure.	SessionRuleErrorHandling
policyDecFailureReports	array(PolicyDecisionFailureCode)	O	1..N	Used to report the failure of the policy decision and/or condition data.	PolicyDecisionErrorHandling
invalidPolicyDecs	array(InvalidParam)	O	1..N	Indicates the invalid parameters for the reported type(s) of the failed policy decision and/or condition data.	ExtPolicyDecisionErrorHandling

5.6.2.37 Type SessionRuleReport

Table 5.6.2.37-1: Definition of type SessionRuleReport

Attribute name	Data type	P	Cardinality	Description	Applicability
ruleIds	array(string)	M	1..N	Contains the identifier of the affected session rule(s).	
ruleStatus	RuleStatus	M	1	Indicates the status of the session rule(s).	
sessRuleFailureCode	SessionRuleFailureCode	C	0..1	Indicates the reason that the session rule(s) is being reported. It shall be included when the NF service consumer reports the enforcement failure of the session rule(s).	

5.6.2.38 Type ServingNfIdentity

Table 5.6.2.38-1: Definition of type ServingNfIdentity

Attribute name	Data type	P	Cardinality	Description	Applicability
servNfInstId	NfInstanceId	O	0..1	Network Function Instance Identifier of the 5G serving CN node. It represents the AMF.	
guami	Guami	O	0..1	Globally Unique AMF Identifier.	
anGwAddr	AnGwAddress	O	0..1	Contains the access network control gateway address. It represents the S-GW or ePDG address. (NOTE 2)	
sgsnAddr	SgsnAddress	O	0..1	Contains the serving SGSN address. (NOTE 3)	2G3GIWK
NOTE 1: At least one of the "servNfInstId", "guami", "anGwAddr", or "sgsnAddr" attributes shall be present. NOTE 2: "anGwAddr" attribute is only applicable to the 5GS and EPC (E-UTRAN and non-3GPP access) interworking scenario as defined in Annex B. NOTE 3: "sgsnAddr" attribute is only applicable to the 5GS and EPC (GERAN and UTRAN access) interworking scenario as defined in Annex B.					

5.6.2.39 Type SteeringMode

Table 5.6.2.39-1: Definition of type SteeringMode

Attribute name	Data type	P	Cardinality	Description	Applicability
steerModeValue	SteerModeValue	M	1	Indicates the value of the steering mode.	
active	AccessType	C	0..1	Indicates the Active access. It shall be included when the "steerModeValue" attribute is set to "ACTIVE_STANDBY".	
standby	AccessTypeRm	O	0..1	Indicates the Standby access. It may be included when the "steerModeValue" attribute is set to "ACTIVE_STANDBY".	
3gLoad	Uinteger	C	0..1	Indicates the traffic load to steer to the 3GPP Access expressed in one percent. It shall be set to 0, 10, 20, 30, 40, 50, 60, 70, 80, 90 or 100. It shall be included when the "steerModeValue" attribute is set to "LOAD_BALANCING".	
prioAcc	AccessType	C	0..1	Indicates the high priority access. It shall be included when the "steerModeValue" attribute is set to "PRIORITY_BASED".	
thresValue	ThresholdValue	O	0..1	Indicates the threshold value(s) for RTT and/or Packet Loss Rate. If the EnATSSS feature is supported, it may be included when the "steerModeValue" attribute is set to "LOAD_BALANCING" with fixed split percentages or "PRIORITY_BASED". (NOTE)	EnATSSS
steerModeInd	SteerModeIndicator	O	0..1	Contains Autonomous load-balance indicator or UE-assistance indicator. If the EnATSSS feature is supported, it may be included when the "steerModeValue" attribute is set to "LOAD_BALANCING". (NOTE)	EnATSSS
NOTE: The "thresValue" attribute and "steerModeInd" attribute are mutually exclusive.					

5.6.2.40 Type QosMonitoringData

Table 5.6.2.40-1: Definition of type QosMonitoringData

Attribute name	Data type	P	Cardinality	Description	Applicability
qmId	string	M	1	Univocally identifies the QoS monitoring policy data within a PDU session.	
reqQosMonParams	array(RequestedQosMonitoringParameter)	M	1..N	Indicates the UL packet delay, DL packet delay and/or round trip packet delay between the UE and the UPF is to be monitored when the QoS Monitoring for URLLC is enabled for the service data flow. (NOTE 1)	
repFreqs	array(ReportingFrequency)	M	1..N	Indicates the frequency for the reporting, such as event triggered, periodic, when the PDU Session is released, and/or any combination.	
repThreshDl	integer	O	0..1	Indicates the threshold in units of milliseconds for DL packet delay. Only applicable when the "reqQosMonParams" attribute includes the "DOWNLINK" value and the "repFreqs" attribute includes the value "EVENT_TRIGGERED". Minimum = 0.	
repThreshUl	integer	O	0..1	Indicates the threshold in units of milliseconds for UL packet delay. Only applicable when the "reqQosMonParams" attribute includes the "UPLINK" value and the "repFreqs" attribute includes the value "EVENT_TRIGGERED". Minimum = 0.	
repThreshRp	integer	O	0..1	Indicates the threshold in units of milliseconds for round trip packet delay. Only applicable when the "reqQosMonParams" attribute includes the "ROUND_TRIP" value and the "repFreqs" attribute includes the value "EVENT_TRIGGERED". Minimum = 0.	
waitTime	DurationSecRm	O	0..1	Indicates the minimum waiting time between subsequent reports. Only applicable when the "repFreqs" attribute includes the value "EVENT_TRIGGERED".	
repPeriod	DurationSecRm	O	0..1	Indicates the reporting period. Only applicable when the "repFreqs" attribute includes the value "PERIODIC".	
notifyUri	UriRm	O	0..1	Notification address of the AF or if the "ExposureToEAS" feature is supported, of the Local NEF or AF receiving the event notification. It shall be included if the PCF determines that the notification shall be sent to the AF directly from the NF service consumer or the PCF determines that the notification shall be sent to the Local NEF or AF directly from the UPF. (NOTE 2).	
notifyCorreId	string	O	0..1	It is used to set the value of Notification Correlation ID in the notification sent by the NF service consumer or, if the "ExposureToEAS" feature is supported, the UPF. It may be included if the PCF determines that the notification shall be sent to the AF directly from the NF service consumer or the PCF determines that the notification shall be sent to the Local NEF or AF directly from the UPF. (NOTE 2).	
directNotifInd	boolean	O	0..1	Indicates that the direct event notification sent to the Local NEF or AF by the UPF is requested if it is included and set to true.	ExposureToEAS

NOTE 1: In this release of the specification the maximum number of elements in the array is 3.
NOTE 2: The attributes "notifyUri" and "notifyCorreId' shall not be set to NULL if the "EnEDGE" feature is not supported.

5.6.2.41 Type TsnBridgeInfo

Table 5.6.2.41-1: Definition of type TsnBridgeInfo

Attribute name	Data type	P	Cardinality	Description	Applicability
bridgeId	Uint64	O	0..1	Contains a TSC user plane node Id. It may contain the unique TSN Bridge MAC address for IEEE TSN networks (as defined in IEEE 802.1Q [45] clause 14.2.5) or may contain a unique identifier assigned within 5GS.	
dsttAddr	MacAddr48	O	0..1	Contain the MAC address of DS-TT.	
dsttPortNum	TsnPortNumber	O	0..1	DS-TT port allocated to a PDU session.	
dsttResidTime	Uinteger	O	0..1	The time taken within the UE and DS-TT to forward a packet between the UE/DS-TT port encoded as specified in clause 9.11.4.26 of 3GPP TS 24.501 [20] starting with octet 3 and ending with octet 10.	

5.6.2.42 Type QosMonitoringReport

Table 5.6.2.42-1: Definition of type QosMonitoringReport

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 QoS Monitoring report.	
ulDelays	array(integer)	O	1..N	Uplink packet delay in units of milliseconds. (NOTE)	
dlDelays	array(integer)	O	1..N	Downlink packet delay in units of milliseconds. (NOTE)	
rtDelays	array(integer)	O	1..N	Round trip delay in units of milliseconds. (NOTE)	
NOTE: In this release of the specification the maximum number of elements in the array is 2. If more than one value is received at one given point of time for UL packet delay, DL packet delay or round trip packet delay respectively, the NF service consumer reports the minimum and maximum packet delays to the PCF.					

5.6.2.43 Type AdditionalAccessInfo

Table 5.6.2.43-1: Definition of type AdditionalAccessInfo

Attribute name	Data type	P	Cardinality	Description	Applicability
accessType	AccessType	M	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.	

5.6.2.44 Void

5.6.2.45 Type PortManagementContainer

Table 5.6.2.45-1: Definition of type PortManagementContainer

Attribute name	Data type	P	Cardinality	Description	Applicability
portManCont	Bytes	M	1	Transports port management information for a DS-TT port or a NW-TT port encoded as specified in clause 9.11.4.27 of 3GPP TS 24.501 [20] starting with octet 4.	
portNum	TsnPortNumber	M	1	Provides port number for a DS-TT port or a NW-TT port.	

5.6.2.46 Type IpMulticastAddressInfo

Table 5.6.2.46-1: IpMulticastAddressInfo

Attribute name	Data type	P	Cardinality	Description	Applicability
srcIpv4Addr	Ipv4Addr	C	0..1	Indicates the source IPv4 address of the DL multicast flow. Maybe included if the "ipv4MulAddr" attribute is included.	
ipv4MulAddr	Ipv4Addr	O	0..1	Indicates the destination IPv4 multicast address of the DL multicast flow.	
srcIpv6Addr	Ipv6Addr	C	0..1	Indicates the source IPv6 address of the DL multicast flow. Maybe included if the "ipv6MulAddr" attribute is included.	
ipv6MulAddr	Ipv6Addr	O	0..1	Indicates the destination IPv6 multicast address of the DL multicast flow.	
NOTE: Either "ipv4MulAddr" attribute or "ipv6MulAddr" attribute shall be included.					

5.6.2.47 Type BridgeManagementContainer

Table 5.6.2.47-1: Definition of type BridgeManagementContainer

Attribute name	Data type	P	Cardinality	Description	Applicability
bridgeManCont	Bytes	M	1	Transports a Bridge management service message encoded as specified in clause 8.7 of 3GPP TS 24.539 [49].	

5.6.2.48 Type DownlinkDataNotificationControl

Table 5.6.2.48-1: Definition of type DownlinkDataNotificationControl

Attribute name	Data type	P	Cardinality	Description	Applicability
notifCtrlInds	array(NotificationControlIndication)	M	1..N	Indicates the event notification(s) is requested.	DDNEventPolicyControl
typesOfNotif	array(DlDataDeliveryStatus)	O	1..N	Contains the type of notification of DDD Status.	DDNEventPolicyControl
NOTE: In this release of the specification the maximum number of elements in the array is 2.					

5.6.2.49 Type DownlinkDataNotificationControlRm

This data type is defined in the same way as the "DownlinkDataNotificationControl" data type, but:

- with the OpenAPI "nullable: true" property;
- the removable attributes "notifCtrlInds", and " typesOfNotif " attribute are defined as nullable in the OpenAPI.

5.6.2.50 Type SgsnAddress

Table 5.6.2.50-1: Definition of type SgsnAddress

Attribute name	Data type	P	Cardinality	Description	Applicability
sgsnIpv4Addr	Ipv4Addr	O	0..1	Includes the IPv4 address of the access network gateway control node.	
sgsnIpv6Addr	Ipv6Addr	O	0..1	Includes the IPv6 address of the access network gateway control node.	
NOTE: At least one address of the SGSN (the IPv4 address or the IPv6 address or both if both addresses are available) shall be included.					

5.6.2.51 Void

5.6.2.52 Type ThresholdValue

Table 5.6.2.52 -1: Definition of type ThresholdValue

Attribute name	Data type	P	Cardinality	Description	Applicability
rttThres	UintegerRm	O	0..1	Unsigned integer identifying a threshold value of Maximum RTT in units of milliseconds.	
plrThres	PacketLossRate Rm	O	0..1	Indicates a threshold value of Maximum Packet Loss Rate.	
NOTE: At least one of the attributes shall be included.					

5.6.2.53 Type NwdafData

Table 5.6.2.53-1: Definition of type NwdafData

Attribute name	Data type	P	Cardinality	Description	Applicability
nwdafInstanceId	NfInstanceId	M	1	Uniquely identifies the NWDAF Instance ID consumed by the NF service consumer.	
nwdafEvents	array(NwdafEvent)	O	1..N	List of Analytics IDs consumed by the NF service consumer.	

5.6.3 Simple data types and enumerations

5.6.3.1 Introduction

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

5.6.3.2 Simple data types

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

Table 5.6.3.2-1: Simple data types

Type Name	Type Definition	Description	Applicability
5GSmCause	Uinteger	Indicates the 5GSM cause code value as defined in clause 9.11.4.2 of 3GPP TS 24.501 [20].	RAN-NAS-Cause
EpsRanNasRelCause	string	Indicates the RAN or NAS release cause code information in 3GPP-EPS access type or indicates the TWAN or untrusted WLAN release cause code information in Non-3GPP-EPS access type. It shall be coded as per the RAN/NAS Cause in clause 8.103 of 3GPP TS 29.274 [37], starting with Octet 5.	RAN-NAS-Cause
FlowDescription	string	Defines a packet filter for an IP flow. Refer to clause 5.4.2 of 3GPP TS 29.212 [23] for encoding.	
PacketFilterContent	string	Defines a packet filter for an IP flow. Refer to clause 5.3.54 of 3GPP TS 29.212 [23] for encoding.	
TsnPortNumber	Uinteger	Port number of a DS-TT or NW-TT port.	TimeSensitiveNetworking
ApplicationDescriptor	Bytes	Defines the OS Id and the OS application identifier for an ATSSS rule, where the OS Id is optional. It is a sequence of octets representing the traffic descriptor(s) of the ATSSS rule as Os Id, if applicable, and Os App Id as defined in table 6.1.3.2-1 of 3GPP TS 24.193 [43].	ATSSS

5.6.3.3 Enumeration: FlowDirection

Table 5.6.3.3-1: Enumeration FlowDirection

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

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 NF service consumer. (NOTE)	
AC_TY_CH	Access Type Change. It also indicates the addition or removal of Access Type for MA PDU session.	
UE_IP_CH	UE IP address change. (NOTE)	
UE_MAC_CH	A new UE MAC address is detected or a used UE MAC address is inactive for a specific period.	
AN_CH_COR	Access Network Charging Correlation Information.	
US_RE	The PDU Session or the Monitoring key specific resources consumed by a UE either reached the threshold or needs to be reported for other reasons.	UMC
APP_STA	The start of application traffic has been detected.	ADC
APP_STO	The stop of application traffic has been detected.	ADC
AN_INFO	Access Network Information report.	NetLoc
CM_SES_FAIL	Credit management session failure.	
PS_DA_OFF	The NF service consumer reports when the 3GPP PS Data Off status changes. (NOTE)	3GPP-PS-Data-Off
DEF_QOS_CH	Default QoS Change. (NOTE)	
SE_AMBR_CH	Session-AMBR Change. (NOTE)	
QOS_NOTIF	The NF service consumer notify the PCF when receiving notification from RAN that QoS targets of the QoS Flow cannot be guaranteed or can be guaranteed.	
NO_CREDIT	Out of credit.	
REALLO_OF_CREDIT	Reallocation of credit	ReallocationOfCredit
PRA_CH	Change of UE presence in Presence Reporting Area.	PRA
SAREA_CH	Location Change with respect to the Serving Area.	
SCNN_CH	Location Change with respect to the Serving CN node.	
RE_TIMEOUT	Indicates the NF service consumer generated the request because there has been a PCC revalidation timeout (i.e. Enforced PCC rule request defined in table 6.1.3.5.-1 of 3GPP TS 23.503 [6]).	
RES_RELEASE	Indicates that the NF service consumer can inform the PCF of the outcome of the release of resources for those rules that require so.	RAN-NAS-Cause
SUCC_RES_ALLO	Indicates that the NF service consumer shall inform the PCF of the successful resource allocation for those rules that requires so.	
RAT_TY_CH	RAT type change.	
REF_QOS_IND_CH	Reflective QoS indication Change.	
NUM_OF_PACKET_FILTER	Indicates that the NF service consumer shall report the number of supported packet filter for signalled QoS rules. (NOTE) Only applicable to the interworking scenario as defined in Annex B.	
UE_STATUS_RESUME	Indicates that the UE's status is resumed. Only applicable to the interworking scenario as defined in Annex B.	PolicyUpdateWhenUESuspends
UE_TZ_CH	UE Time Zone Change.	
AUTH_PROF_CH	Indicates that the DN-AAA authorization profile index has changed. (NOTE)	DN-Authorization
TSN_BRIDGE_INFO	Indicates the NF service consumer has detected information about new TSC user plane node port(s), and/or new/updated UMIC and/or PMIC(s).	TimeSensitiveNetworking
QOS_MONITORING	Indicate that the NF service consumer notifies the PCF of the QoS Monitoring information.	QosMonitoring
SCELL_CH	Location Change with respect to the Serving Cell.	
USER_LOCATION_CH	Indicates that user location has changed, applicable to serving area change and serving cell change.	AggregatedUELocChanges
EPS_FALLBACK	EPS Fallback report is enabled in the NF service consumer. Only applicable to the interworking scenario as defined is Annex B.	EPSFallbackReport
MA_PDU	Indicates that the NF service consumer notifies the PCF of the MA PDU session request. Only applicable to the interworking scenario as defined in Annex B. (NOTE)	ATSSS
5G_RG_JOIN	The 5G-RG has joined to an IP Multicast Group.	WWC
5G_RG_LEAVE	The 5G-RG has left an IP Multicast Group.	WWC

DDN_FAILURE	Indicates that the NF service consumer requests policies from PCF if it received an event subscription for DDN Failure event.	DDNEventPolicyControl
DDN_DELIVERY_STATUS	Indicates that the NF service consumer requests policies from PCF if it received an event subscription for DDN Delievery Status event.	DDNEventPolicyControl
GROUP_ID_LIST_CHG	UE Internal Group Identifier(s) has changed: the NF service consumer reports that UDM provided list of group Ids has changed. (NOTE)	GroupIdListChange
DDN_FAILURE_CANCELLATION	Indicates that the event subscription for DDN Failure event is cancelled.	DDNEventPolicyControl2
DDN_DELIVERY_STATUS_CANCELLATION	Indicates that the event subscription for DDD STATUS is cancelled.	DDNEventPolicyControl2
VPLMN_QOS_CH	Indicates that the NF service consumer has detected the change of the QoS supported in the VPLMN, the change from the case where the QoS constraints are applicable to the case where the QoS constraints are not applicable (e.g. the UE moves back from the home routed to the non-roaming scenario) or vice versa. (NOTE)	VPLMN-QoS-Control
SUCC_QOS_UPDATE	Indicates that the NF service consumer notifies the PCF of the successful update of the QoS for MPS.	MPSforDTS
SAT_CATEGORY_CHG	Indicates that the SMF has detected a change between different satellite category, or non-satellite backhaul.	SatBackhaulCategoryChg
PCF_UE_NOTIF_IND	Indicates the SMF has detected the AMF forwarded the PCF for the UE indication to receive/stop receiving notifications of SM Policy association established/terminated events.	AMInfluence
NWDAF_DATA_CHG	Indicates that the NWDAF instance IDs used for the PDU session and/or associated Analytics IDs have changed. (NOTE)	EneNA
NOTE: The NF service consumer always reports to the PCF.		

The PCF may provision the values of policy control request trigger which are not always reported by the NF service consumer as defined in clause 4.2.6.4.

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

If the "PLMN_CH" is provisioned, when the NF service consumer detects a change of the serving network (a PLMN or an SNPN), the NF service consumer shall include the "PLMN_CH" within the "repPolicyCtrlReqTriggers" attribute and the current identifier of the serving network within the "servingNetwork" attribute.

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

If the "AC_TY_CH" is provisioned, when the NF service consumer detects a change of access type, the NF service consumer shall include the "AC_TY_CH" within the "repPolicyCtrlReqTriggers" attribute and the current access type within the "accessType" attribute. The RAT type encoded in the "ratType" attribute shall also be provided when applicable to the specific access type. Specific attributes for the EPC interworking case are described in Annex B. If the ATSSS feature is supported, when the NF service consumer detects an access is added or released for MA PDU session, the NF service consumer shall include the added Access Type or released Access type encoded as "accessType" attribute within the AdditionalAccessInfo data structure. The RAT type encoded in the "ratType" attribute shall also be provided within the AdditionalAccessInfo data structure when applicable to the added access type or released access type.

When the NF service consumer detects an IPv4 address and/or an IPv6 prefix is allocated or released, the NF service consumer shall include the "UE_IP_CH" within the "repPolicyCtrlReqTriggers" attribute and new allocated UE Ipv4 address within the "ipv4Address" attribute and/or the UE Ipv6 prefix within the "ipv6AddressPrefix" attribute or the released UE Ipv4 address within the "relIpv4Address" attribute and/or the UE Ipv6 prefix within the "relIpv6AddressPrefix" attribute. If the "MultiIpv6AddrPrefix" feature is supported ,and if multiple allocated or released IPv6 prefixes are detected, the NF service consumer shall include the new allocated UE Ipv6 prefixes within the "addIpv6AddrPrefixes" attribute and the released UE Ipv6 prefixes within the "addRelIpv6AddrPrefixes" attribute.

When the NF service consumer detects a new UE MAC address or a used UE MAC address is not used any more, the NF service consumer shall include the "UE_MAC_CH" within the "repPolicyCtrlReqTriggers" attribute and new

detected UE MAC address within the "ueMac" attribute or the not used UE MAC address within the "relUeMac" attribute.

If the "AN_CH_COR" is provisioned, when the NF service consumer is provisioned with the PCC rule as defined in clause 4.2.6.5.1, the NF service consumer shall notify the PCF of access network charging identifier associated with the PCC rules as defined in clause 4.2.4.13.

If the "US_RE" is provisioned, when the NF service consumer receives the usage report from the UPF, the NF service consumer shall notify the PCF of the accumulated usage as defined in clause 4.2.4.10. Applicable to functionality introduced with the UMC feature as described in clause 5.8.

If the "APP_STA" is provisioned, when the NF service consumer receives the application start report from the UPF, the NF service consumer shall notify the PCF of the application start report as defined in clause 4.2.4.6. Applicable to functionality introduced with the ADC feature as described in clause 5.8.

If the "APP_STO" is provisioned, when the NF service consumer receives the application stop report from the UPF, the NF service consumer shall notify the PCF of the application stop report as defined in clause 4.2.4.6. Applicable to functionality introduced with the ADC feature as described in clause 5.8.

If the "AN_INFO" is provisioned, when the NF service consumer receives the reported access network information from the access network, the NF service consumer shall notify the PCF of the access network information as defined in clause 4.2.4.9. Applicable to functionality introduced with the NetLoc feature as described in clause 5.8.

If the "CM_SES_FAIL" is provisioned, when the NF service consumer receives a detected transient/permanent failure from the CHF, the NF service consumer shall include the "CM_SES_FAIL" within the "repPolicyCtrlReqTriggers" attribute. If the failure does not apply to all PCC Rules, the affected PCC Rules are indicated within the "ruleReports" attribute, with the "ruleStatus" attribute set to value ACTIVE and the "failureCode" attribute set to the corresponding value as reported by the CHF; otherwise if the failure applies to the session, the "creditManageStatus" shall be set to the corresponding value as reported by the CHF.

If the "PS_DA_OFF" is provisioned, when the NF service consumer receives a change of 3GPP PS Data Off status from the UE, the NF service consumer shall notify the PCF as defined in clause 4.2.4.8. Applicable to functionality introduced with the 3GPP-PS-Data-Off feature as described in clause 5.8.

When the NF service consumer detects a change of subscribed default QoS, the NF service consumer shall include the "DEF_QOS_CH" within the "repPolicyCtrlReqTriggers" attribute and the new subscribed default QoS within the "subsDefQos" attribute.

When the NF service consumer detects a change of Session-AMBR, the NF service consumer shall include the "SE_AMBR_CH" within the "repPolicyCtrlReqTriggers" attribute and the new Session-AMBR within the "subsSessAmbr" attribute.

If the "QOS_NOTIF" is provisioned, when the NF service consumer receives a notification from access network that QoS targets of the QoS Flow cannot be guaranteed or can be guaranteed again, the NF service consumer shall send the notification as defined in clause 4.2.4.20.

If the "NO_CREDIT" is provisioned, when the NF service consumer detects the credit for the PCC rule(s) is no longer available, the NF service consumer shall include the "NO_CREDIT" within the "repPolicyCtrlReqTriggers" attribute, the termination action the NF service consumer applies to the PCC rules as instructed by the CHF within the "finUnitAct" attribute and the affected PCC rules within the "ruleReports" attribute.

When the "ReallocationOfCredit" feature is supported, if the "REALLO_OF_CREDIT" is provisioned, when the NF service consumer detects the credit for the PCC rule(s) is reallocated, the NF service consumer shall include the "REALLO_OF_CREDIT" within the "repPolicyCtrlReqTriggers" attribute and include the affected PCC rules for which credit has been reallocated after credit was no longer available and the "ruleStatus" attribute set to value ACTIVE within the "ruleReports" attribute.

If the "PRA_CH" is provisioned, to detect when the UE enters/leaves certain presence reporting areas, the NF service consumer is provisioned the presence reporting area information as defined in clause 4.2.6.5.6. When the NF service consumer receives the presence reporting area information from the serving node, the NF service consumer shall notify the PCF of the reported presence area information as defined in clause 4.2.4.16. This report includes reporting the initial status at the time the request for reports is initiated. Applicable to the functionality introduced by the PRA or ePRA feature as described in clause 5.8.

If the "SAREA_CH" is provisioned, when the NF service consumer detects a change of serving area (i.e. tracking area, or if the feature "2G3GIWK" is supported routing area), the NF service consumer shall include the "SAREA_CH" within the "repPolicyCtrlReqTriggers" attribute and the current TAI within the "userLocationInfo" attribute in either the "eutraLocation" or "nrLocation", or the current Routing Area within the "userLocationInfo" attribute in the "utraLocation" attribute when UTRAN access, or in the "geraLocation" attribute when GERAN access, as applicable. Non-3GPP access user location is reported in the "n3gaLocation" attribute when applicable. The attributes used in case of EPC interworking are described in Annex B.

If the "SCNN_CH" is provisioned, when the NF service consumer detects a change of serving Network Function (i.e. the AMF, ePDG, S-GW or if the feature "2G3GIWK" is supported SGSN), the NF service consumer shall include the "SCNN_CH" within the "repPolicyCtrlReqTriggers" attribute and the current serving Network Function in the "servNfId" attribute if available. When the serving Network Function is an AMF, the NF service consumer shall include the AMF Network Function Instance Identifier within the "servNfInstId" attribute and the Globally Unique AMF Identifier within the "guami" attribute. The attributes included in case of EPC interworking are described in Annex B.

NOTE 1: In the home-routed roaming case, if the AMF change is unknown to the H-SMF, then the AMF change is not reported.

If the "RE_TIMEOUT" is provisioned, when the NF service consumer is provisioned with the revalidation time by the PCF, the NF service consumer shall request the policy before the indicated revalidation time is reached as defined in clause 4.2.4.3.

If the "RES_RELEASE" is provisioned, when the NF service consumer receives the request of PCC rule removal as defined in clause 4.2.6.5.2, the NF service consumer shall report the outcome of resource release as defined in clause 4.2.4.12. Applicable to functionality introduced with the RAN-NAS-Cause feature as described in clause 5.8.

When "SUCC_RES_ALLO" is provisioned and PCC rules are provisioned according to clause 4.2.6.5.5, the NF service consumer shall inform the PCF of the successful resource allocation as defined in clause 4.2.4.14.

If the feature "2G3GIWK" is supported, and if the "RAI_CH" is provisioned, when the NF service consumer detects a change of routing area, the NF service consumer shall include the "RAI_CH" within the "repPolicyCtrlReqTriggers" attribute and the current RAI within the "userLocationInfo" attribute as described in Annex B.

If the "RAT_TY_CH" is provisioned, when the NF service consumer detects a change of the RAT type, the NF service consumer shall include the "RAT_TY_CH" within the "repPolicyCtrlReqTriggers" attribute and the current RAT type within the "ratType" attribute. For MA PDU session, the NF service consumer shall include the current RAT type at the SmPolicyUpdateContextData data type level or AdditionalAccessInfo data type level. If the RAT type is provided at the SmPolicyUpdateContextData data type level, the NF service consumer shall also provide the associated access type within the SmPolicyUpdateContextData data structure.

If the "REF_QOS_IND_CH" is provisioned, when the NF service consumer receives a change of reflective QoS indication from the UE, the NF service consumer shall include the "REF_QOS_IND_CH" within the "repPolicyCtrlReqTriggers" attribute and the indication within the "refQosIndication" attribute.

When the NF service consumer receives the number of supported packet filter for signalled QoS rules for the PDU session from the UE during the PDU Session Modification procedure after the first inter-system change from EPS to 5GS for a PDU Session established in EPS and transferred from EPS with N26 interface, the NF service consumer shall include the "NUM_OF_PACKET_FILTER" within the "repPolicyCtrlReqTriggers" attribute and the number of supported packet filter for signalled QoS rules within the "numOfPackFilter" attribute. Only applicable to the interworking scenario as defined in Annex B.

If the "UE_STATUS_RESUME" is provisioned, when the NF service consumer detected the UE's status is resumed from suspend state, the NF service consumer shall inform the PCF of the UE status including the "UE_STATUS_RESUME" within "repPolicyCtrlReqTriggers" attribute. The PCF shall after this update the NF service consumer with PCC Rules or session rules if necessary. Applicable to functionality introduced with the PolicyUpdateWhenUESuspends feature as described in clause 5.8.

If the "UE_TZ_CH" is provisioned, when the NF service consumer detects a change of the UE Time Zone, the NF service consumer shall include the "UE_TZ_CH" within the "repPolicyCtrlReqTriggers" attribute and the current UE Time Zone within the "ueTimeZone" attribute.

If the "DN-Authorization" feature is supported, when the NF service consumer detects a change of DN-AAA authorization profile index, the NF service consumer shall include the "AUTH_PROF_CH" within the

"repPolicyCtrlReqTriggers" attribute and the new DN-AAA authorization profile index within the "authProfIndex" attribute.

If the "TimeSensitiveNetworking" or "TimeSensitiveCommunication" feature is supported and "TSN_BRIDGE_INFO" is provisioned, when the NF service consumer detects:

- there is information about new TSC user plane node port(s), e.g. a new manageable Ethernet port, the NF service consumer shall include the "TSN_BRIDGE_INFO" within the "repPolicyCtrlReqTriggers" attribute and the updated TSC user plane node information within the "tsnBridgeInfo" attribute; and/or

- the NF service consumer detects a UMIC or PMIC, the NF service consumer shall include the "TSN_BRIDGE_INFO" within the "repPolicyCtrlReqTriggers" attribute and the UMIC, if available, within the "tsnBridgeManCont" attribute, and/or the PMIC(s), if available, within the "tsnPortManContDstt" and the "tsnPortManContNwtts" attributes.

NOTE 2: When the NF service consumer detects updated Port Management Information of the NW-TT ports, the NF service consumer includes the PMIC within the "tsnPortManContNwtts" attribute of SmPolicyUpdateContextData data type.

If the "QOS_MONITORING" is provisioned, upon receiving the QoS Monitoring report from the UPF, the NF service consumer shall send the QoS monitoring report to the PCF as defined in clause 4.2.4.24.

If the "SCELL_CH" is provisioned, when the NF service consumer detects a change of serving cell, the NF service consumer shall include the "SCELL_CH" within the "repPolicyCtrlReqTriggers" attribute and the current cell Id within the "userLocationInfo" attribute either in the "eutraLocation" attribute when EPC/E-UTRAN access or "nrLocation" attribute when NR access or "geraLocation" attribute when GERAN access or "utraLocation" attribute when UTRAN access, as applicable.

NOTE 3: Location change of serving cell can increase signalling load on multiple interfaces. Hence, it is recommended that any such serving cell changes event trigger subscription is only applied for a limited number of subscribers.

If the "AggregatedUELocChanges" feature is supported and the "USER_LOCATION_CH" is provisioned, when the NF service consumer detects a change of serving cell and/or a change of serving area (i.e. tracking area), the NF service consumer shall include the "USER_LOCATION_CH" within the "repPolicyCtrlReqTriggers" attribute and the current serving area and/or cell Id within the "userLocationInfo" attribute in the "eutraLocation" attribute or "nrLocation" attribute or "geraLocation" attribute or "utraLocation" attribute, as applicable.

NOTE 4: The access network can be configured to report location changes only when transmission resources are established in the radio access network.

If the "EPSFallbackReport" feature is supported and the "EPS_FALLBACK" is provisioned and there is a PCC rule installed that required the reporting, when the NF service consumer receives a PDU session modification response indicating the rejection of the establishment of the QoS flow with 5QI=1, the NF service consumer shall notify the PCF of EPS fallback as defined in clause B.3.4.6.

When the NF service consumer receives the MA PDU Request Indication or MA PDU Network-Upgrade Allowed Indication and ATSSS Capability from the UE during the PDU Session Modification procedure after the first inter-system change from EPS to 5GS for a PDU Session established in EPS and transferred from EPS with N26 interface, the NF service consumer shall include the "MA_PDU" within the "repPolicyCtrlReqTriggers" attribute, the MA PDU session Indication in the "maPduInd" attribute, the ATSSS capability of the MA PDU session within the "atsssCapab" attribute. Only applicable to the interworking scenario as defined in Annex B.

If the "WWC" feature is supported and "5G_RG_JOIN" is provisioned and when the NF service consumer detects a 5G-RG has joined to an IP Multicast Group, the NF service consumer shall include the "5G_RG_JOIN" within the "repPolicyCtrlReqTriggers" attribute and the IP multicast addressing information within the "mulAddrInfos" attribute.

If the "WWC" feature is supported and "5G_RG_LEAVE" is provisioned and when the NF service consumer detects a 5G-RG has left an IP Multicast Group, the NF service consumer shall include the "5G_RG_LEAVE" within the "repPolicyCtrlReqTriggers" attribute and the IP multicast addressing information within the "mulAddrInfos" attribute.

If "DDNEventPolicyControl" feature is supported, and if "DDN_FAILURE" is provisioned, when the NF service consumer receives an event subscription for DDN Failure event including the traffic descriptors, the NF service consumer shall include the "DDN_FAILURE" within the "repPolicyCtrlReqTriggers" attribute and traffic descriptor(s) within the "trafficDescriptors" attribute.

If "DDNEventPolicyControl" feature is supported, and if "DDN_DELIVERY_STATUS" is provisioned, when the NF service consumer receives an event subscription for DDD Status event including the traffic descriptors, the NF service consumer shall include the "DDN_DELIVERY_STATUS" within the "repPolicyCtrlReqTriggers" attribute and traffic descriptor(s) within the "trafficDescriptors" attribute and the requested type(s) of notifications (notifications about downlink packets being buffered, and/or discarded).

If "GroupIdListChange" feature is supported, when the SMF receives the updated Internal Group Identifier(s) from the UDM, the SMF shall include the "GROUP_ID_LIST_CHG" within the "repPolicyCtrlReqTriggers" attribute and the Internal Group Identifier(s) of the served UE within the "interGrpIds" attribute.

If "DDNEventPolicyControl2" feature is supported, and if "DDN_FAILURE_CANCELLATION" is provisioned, when the SMF receives a cancellation of event subscription for DDN Failure event, the SMF shall include the "DDN_FAILURE_CANCELLATION" within the "repPolicyCtrlReqTriggers" attribute and the PCC rule identifier of the PCC rule which is used for traffic detection of DDN failure event within the "pccRuleId" attribute.

If "DDNEventPolicyControl2" feature is supported, and if "DDN_DELIVERY_STATUS_CANCELLATION" is provisioned, when the SMF receives a cancellation of event subscription for DDD Status event, the SMF shall include the "DDN_DELIVERY_STATUS_CANCELLATION" within the "repPolicyCtrlReqTriggers" attribute and the PCC rule identifier of the PCC rule which is used for traffic detection of DDD status event within the "pccRuleId" attribute.

When the "VPLMN-QoS-Control" feature is supported and if the NF service consumer receives a new QoS value supported in the VPLMN, the NF service consumer shall include the "VPLMN_QOS_CH" within the "repPolicyCtrlReqTriggers" attribute and the received QoS constraints within the "vplmnQos" attribute; if the NF service consumer detects that the UE moves from a VPLMN with QoS constraints to the HPLMN or to a VPLMN without QoS constraints, the NF service consumer shall include the "VPLMN_QOS_CH" within the "repPolicyCtrlReqTriggers" attribute and the "vplmnQosNotApp" attribute set to true.

If the "MPSforDTS" feature is supported, and if "SUCC_QOS_UPDATE" is provisioned, when the resources for the MPS for DTS invocation/revocation are successfully allocated for MPS for DTS, the NF service consumer shall include the "SUCC_QOS_UPDATE" within the "policyCtrlReqTriggers" attribute.

If "SatBackhaulCategoryChg" feature is supported, and if "SAT_CATEGORY_CHG" is provisioned, the NF service consumer notifies the PCF when there is a change of the backhaul which is used for the PDU session between different satellite backhaul categories (i.e., GEO, MEO, LEO, or other satellite) or between a satellite backhaul and a non-satellite backhaul. The NF service consumer shall include the satellite backhaul category or non-satellite backhaul within the "satBackhaulCategory" attribute together with the "SAT_CATEGORY_CHG" policy control request trigger within the "repPolicyCtrlReqTriggers" attribute.

NOTE 5: The type (i.e. GEO, MEO, LEO or other satellite) of the satellite involved in the backhaul is referred as the satellite backhaul category. Only a single backhaul category can be indicated.

If the "AMInfluence" feature is supported, and if "PCF_UE_NOTIF_IND" is provisioned, the NF service consumer notifies the PCF about the PCF for the UE request to be notified of PDU session established/terminated events by forwarding within the "pcfUeInfo" attribute, the received PCF for the UE callback URI within the "callbackUri" attribute and, if received, SBA binding information within the "bindingInfo" attribute, together with the "PCF_UE_NOTIF_IND" policy control request trigger within the "repPolicyCtrlReqTriggers" attribute. The NF service consumer notifies the PCF about the PCF for the UE request to stop being notified about the PDU session established/terminated events by sending the "pcfUeInfo" attribute set to NULL together with the "PCF_UE_NOTIF_IND" policy control request trigger within the "repPolicyCtrlReqTriggers" attribute.

If "EneNA" feature is supported, and if "NWDAF_DATA_CHG" is provisioned, the NF service consumer notifies the PCF when there is a change in the list of NWDAF Instance IDs used for the PDU Session and/or associated Analytics IDs. The NF service consumer shall include within the "nwdafDatas" attribute the list of NWDAF instance IDs used for the PDU Session within the "nwdafInstanceId" attribute and their associated Analytic ID(s) within the "nwdafEvents" attribute, and the "NWDAF_DATA_CHG" within the "repPolicyCtrlReqTriggers" attribute.

5.6.3.7 Enumeration: RequestedRuleDataType

Table 5.6.3.7-1: Enumeration RequestedRuleDataType

Enumeration value	Description	Applicability
CH_ID	Indicates that the requested rule data is the charging identifier.	
MS_TIME_ZONE	Indicates that the requested access network info type is the UE's timezone. (NOTE)	
USER_LOC_INFO	Indicates that the requested access network info type is the UE's location. (NOTE)	
RES_RELEASE	Indicates that the requested rule data is the result of the release of resource.	
SUCC_RES_ALLO	Indicates that the requested rule data is the successful resource allocation.	
EPS_FALLBACK	Indicates that the requested rule data is the report of QoS flow rejection due to EPS fallback.	EPSFallbackReport
NOTE: The requested rule data shall also be reported at QoS flow termination and PDU session termination.		

5.6.3.8 Enumeration: RuleStatus

Table 5.6.3.8-1: Enumeration RuleStatus

Enumeration value	Description	Applicability
ACTIVE	Indicates that the PCC rule(s) are successfully installed (for those provisioned from the PCF) or activated (for those pre-defined in the SMF), or that the session rule(s) are successfully installed.	
INACTIVE	Indicates that the PCC rule(s) are removed (for those provisioned from the PCF) or inactive (for those pre-defined in the SMF) or that the session rule(s) are removed.	

5.6.3.9 Enumeration: FailureCode

Table 5.6.3.9-1: Enumeration FailureCode

Enumeration value	Description	Applicability
UNK_RULE_ID	Indicates that the pre-provisioned PCC rule could not be successfully activated because the provided PCC rule identifier is unknown to the NF service consumer.	
RA_GR_ERR	Indicates that the PCC rule could not be successfully installed or enforced because the Rating Group specified within the Charging Data policy decision to which the PCC rule refers is unknown or invalid.	
SER_ID_ERR	Indicates that the PCC rule could not be successfully installed or enforced because the Service Identifier specified within the Charging Data policy decision to which the PCC rule refers is invalid, unknown or not applicable to the service being charged.	
NF_MAL	Indicates that the PCC rule could not be successfully installed (for those provisioned from the PCF), activated (for those pre-defined in the SMF) or enforced (for those already successfully installed) due to SMF/UPF malfunction.	
RES_LIM	Indicates that the PCC rule could not be successfully installed (for those provisioned from the PCF), activated (for those pre-defined in the SMF) or enforced (for those already successfully installed) due to a limitation of resources at the SMF/UPF.	
MAX_NR_QoS_FLOW	Indicates that the PCC rule could not be successfully installed (for those provisioned from the PCF), activated (for those pre-defined in the SMF) or enforced (for those already successfully installed) due to the fact that the maximum number of QoS flows has been reached for the associated PDU session.	
MISS_FLOW_INFO	Indicates that the PCC rule could not be successfully installed (for those provisioned from the PCF) or enforced (for those already successfully installed) because neither the "flowInfos" attribute nor the "appId" attribute is specified by the PCF within the PCC rule entry of the "pccRules" attribute during the first PCC rule installation request.	
RES_ALLO_FAIL	Indicates that the PCC rule could not be successfully installed or maintained since the associated QoS flow establishment/modification failed or the associated QoS flow was released.	
UNSUCC_QOS_VAL	This value is used to: - indicate that QoS validation has failed; or - indicate when Guaranteed Bandwidth > Max-Requested-Bandwidth.	
INCOR_FLOW_INFO	Indicates that the PCC rule could not be successfully installed or modified at the NF service consumer because the provided flow information is not supported by the network (e.g. the provided IP address(es) or Ipv6 prefix(es) do not correspond to an IP version applicable for the PDU session).	
PS_TO_CS_HAN	Indicates that the PCC rule could not be maintained because of PS to CS handover.	
APP_ID_ERR	Indicates that the PCC rule could not be successfully installed or enforced because the Application Identifier is invalid, unknown, or not applicable to the application required for detection.	ADC
NO_QOS_FLOW_BOUND	Indicates that there is no QoS flow to which the SMF can bind the PCC rule.	
FILTER_RES	Indicates that the Flow Information within the "flowinfos" attribute cannot be handled by the NF service consumer because at least one of the restrictions defined in clause 5.4.2 of 3GPP TS 29.212 [23] was not respected.	
MISS_REDI_SER_ADDR	Indicates that the PCC rule could not be successfully installed or enforced at the NF service consumer because there is no valid Redirect Server Address within the provided Traffic Control Data policy decision to which the PCC rule refers, and no preconfigured redirection address for this PCC rule at the SMF/UPF.	ADC
CM_END_USER_SER_DENIED	Indicates that the charging system denied the service request due to service restrictions (e.g. terminate rating group) or limitations related to the end-user, e.g. the end-user's account could not cover the requested service.	

CM_CREDIT_CON_NOT_APP	Indicates that the charging system determined that the service can be granted to the end user but no further credit control is needed for the service (e.g. service is free of charge or is treated via offline charging).	
CM_AUTH_REJ	Indicates that the charging system denied the service request in order to terminate the service for which credit is requested.	
CM_USER_UNK	Indicates that the specified end user could not be found in the charging system.	
CM_RAT_FAILED	Indicates that the charging system cannot rate the service request due to insufficient rating inputs, incorrect combination of inputs or due to an attribute or an attribute value that is not recognized or supported in the rating.	
UE_STA_SUSP	Indicates that the UE is in suspend state. Only applicable to the interworking scenario, as defined in Annex B.	PolicyUpdateWhenUESuspends
UNKNOWN_REF_ID	Indicates that the PCC rule could not be successfully installed/modified because the referenced identifier to a Policy Decision Data or to a Condition Data is unknown to the NF service consumer.	
INCORRECT_COND_DATA	Indicates that the PCC rule could not be successfully installed/modified because the referenced Condition data are incorrect (e.g. the "deactivationTime" and the "activationTime" included in the referenced ConditionData contain the same time value).	
REF_ID_COLLISION	Indicates that the PCC rule could not be successfully installed/modified because a Policy Decision referenced within the PCC rule is also referenced by a session rule (e.g. a session rule and this PCC rule refer to the same Usage Monitoring decision data).	
TRAFFIC_STEERING_ERROR	This value is used to indicate that: - the enforcement of the steering of traffic to the N6-LAN or 5G-LAN failed; or - the dynamic PCC rule could not be successfully installed/modified at the NF service consumer because e.g. there are invalid traffic steering policy identifier(s) within the provided Traffic Control Data policy decision to which the PCC rule refers. Applicable when the functionality introduced with the TSC feature described in clause 5.8 applies.	
DNAI_STEERING_ERROR	This value is used to indicate that: - the enforcement of the steering of traffic to the indicated DNAI failed; or - the dynamic PCC rule could not be successfully installed/modified at the NF service consumer because there is invalid route information for a DNAI(s) (e.g. routing profile id is not configured) within the provided Traffic Control Data policy decision to which the PCC rule refers. Applicable when the functionality introduced with the TSC feature described in clause 5.8 applies.	
AN_GW_FAILED	Indicates that the AN-Gateway has failed and that the PCF should refrain from sending policy decisions to the SMF until it is informed that the S-GW has been recovered. This value shall not be used if the SM Policy association modification procedure is initiated for session rule removal only.	SGWRest
MAX_NR_PACKET_FILTERS_EXCEEDED	This value is used to indicate that the PCC rule could not be successfully installed, modified or enforced at the NF service consumer because the number of supported packet filters for signalled QoS rules for the PDU session has been reached.	

5.6.3.10 Enumeration: AfSigProtocol

Table 5.6.3.10-1: Enumeration AfSigProtocol

Enumeration value	Description	Applicability
NO_INFORMATION	Indicate that no information about the AF signalling protocol is being provided. This is the default value.	ProvAFsignalFlow
SIP	Indicate that the signalling protocol is Session Initiation Protocol.	ProvAFsignalFlow

5.6.3.11 Enumeration: RuleOperation

Table 5.6.3.11-1: Enumeration RuleOperation

Enumeration value	Description	Applicability
CREATE_PCC_RULE	Indicates to create a new PCC rule to reserve the resource requested by the UE.	
DELETE_PCC_RULE	Indicates to delete a PCC rule corresponding to reserve the resource requested by the UE.	
MODIFY_PCC_RULE_AND_ADD_PACKET_FILTERS	Indicates to modify the PCC rule by adding new packet filter(s).	
MODIFY_PCC_RULE_AND_REPLACE_PACKET_FILTERS	Indicates to modify the PCC rule by replacing the existing packet filter(s).	
MODIFY_PCC_RULE_AND_DELETE_PACKET_FILTERS	Indicates to modify the PCC rule by deleting the existing packet filter(s).	
MODIFY_PCC_RULE_WITHOUT_MODIFY_PACKET_FILTERS	Indicates to modify the PCC rule by modifying the QoS of the PCC rule.	

5.6.3.12 Enumeration: RedirectAddressType

Table 5.6.3.12-1: Enumeration RedirectAddressType

Enumeration value	Description	Applicability
IPV4_ADDR	Indicates that the address type is in the form of "dotted-decimal" IPv4 address.	
IPV6_ADDR	Indicates that the address type is in the form of IPv6 address.	
URL	Indicates that the address type is in the form of Uniform Resource Locator.	
SIP_URI	Indicates that the address type is in the form of SIP Uniform Resource Identifier.	

5.6.3.13 Enumeration: QosFlowUsage

Table 5.6.3.13-1: Enumeration QosFlowUsage

Enumeration value	Description	Applicability
GENERAL	Indicates no specific QoS flow usage information is available.	
IMS_SIG	Indicates that the QoS flow is used for IMS signalling only.	

5.6.3.14 Enumeration: FailureCause

Table 5.6.3.14-1: Enumeration FailureCause

Enumeration value	Description	Applicability
PCC_RULE_EVENT	Some of the PCC rules provisioned by the PCF in the request cannot be installed/activated. It is used to inform the PCF that the request failed and should not be attempted again.	
PCC_QOS_FLOW_EVENT	For some reason some of the PCC rules provisioned by the PCF in the request cannot be enforced or modified successfully in a network initiated procedure. It is used to inform the PCF that the request could not be satisfied at the time it was received, but may be able to satisfy the request in the future.	
RULE_PERMANENT_ERROR	The HTTP request is rejected because some of the PCC and/or session rules provisioned by the PCF in the request cannot be installed/activated. It is used to inform the PCF that the request failed, and should not be attempted again.	SessionRuleErrorHandling
RULE_TEMPORARY_ERROR	The HTTP request is rejected because for some reason some of the PCC and/or session rules provisioned by the PCF in the request cannot be enforced or modified successfully in a network initiated procedure. It is used to inform the PCF that the request could not be satisfied at the time it was received, but may be able to satisfy the request in the future.	SessionRuleErrorHandling
POL_DEC_ERROR	Some of the policy decisions (including data that is different than PCC/session rule related data) provided by the PCF in the request cannot be provisioned in the NF service consumer.	PolicyDecisionErrorHandling

5.6.3.15 Enumeration: FlowDirectionRm

This data type is defined in the same way as the "FlowDirection" data type, but also allows null value (specified as "NullValue" data type).

5.6.3.16 Enumeration: CreditManagementStatus

Table 5.6.3.16-1: Enumeration CreditManagementStatus

Enumeration value	Description	Applicability
END_USER_SER_DENIED	Indicates that the charging system denied the service request due to service restrictions (e.g. terminate rating group) or limitations related to the end-user, for example the end-user's account could not cover the requested service.	
CREDIT_CTRL_NOT_APP	Indicates that the charging system determined that the service can be granted to the end user but no further credit control is needed for the service (e.g. service is free of charge or is treated for offline charging).	
AUTH_REJECTED	Indicates that the charging system denied the service request in order to terminate the service for which credit is requested.	
USER_UNKNOWN	Indicates that the specified end user could not be found in the charging system.	
RATING_FAILED	Indicates that the charging system cannot rate the service request due to insufficient rating input, incorrect attribute combination or an attribute value that is not recognized or supported in rating.	

5.6.3.17 Enumeration: SessionRuleFailureCode

Table 5.6.3.17-1: Enumeration SessionRuleFailureCode

Enumeration value	Description	Applicability
NF_MAL	Indicates that the session rule could not be successfully installed) or enforced (for those already successfully installed) due to SMF/UPF malfunction.	
RES_LIM	Indicates that the session rule could not be successfully installed or enforced (for those already successfully installed) due to a limitation of resources at the SMF/UPF.	
SESSION_RESOURCE_ALLOCATION_FAILURE	Indicates the session rule could not be successfully enforced due to failure during the allocation of resources for the PDU session in the UE, RAN or AMF.	
UNSUCC_QOS_VAL	Indicates that the QoS validation has failed.	
INCORRECT_UM	The usage monitoring data of the enforced session rule is not the same for all the provisioned session rule(s), i.e., the reference identifier to a UsageMonitoringData policy decision is not homogeneously provisioned in all session rules (e.g., some, but not all, session rules contain usage monitoring data, or all session rules contain usage monitoring data, but with different monitoring key).	(NOTE)
UE_STA_SUSP	Indicates that the UE is in suspend state. Only applicable to the interworking scenario as defined in Annex B.	PolicyUpdateWhenUESuspends
UNKNOWN_REF_ID	Indicates that the session rule could not be successfully installed/modified because the reference identifier to a Policy Decision Data or to a Condition Data is unknown to the NF service consumer.	
INCORRECT_COND_DATA	Indicates that the session rule could not be successfully installed/modified because the referenced Condition data are incorrect (e.g. the ConditionData instance contains a "deactivationTime" attribute, or the "ratType" attribute value in a ConditionData instance indicates a RAT type (e.g. "NR") that is not specified for the the "accessType" attribute indicated value (e.g. "NON_3GPP_ACCESS").	
REF_ID_COLLISION	Indicates that the session rule could not be successfully installed/modified because the same Policy Decision is referenced by a PCC rule (e.g. the session rule and the PCC rule refer to the same Usage Monitoring decision data).	
NOTE: The "INCORRECT_UM" value shall only be used when the feature "UMC" is supported.		

5.6.3.18 Enumeration: SteeringFunctionality

Table 5.6.3.18-1: Enumeration SteeringFunctionality

Enumeration value	Description	Applicability
MPTCP	Indicates that PCF authorizes the MPTCP functionality to support traffic steering, switching and splitting.	ATSSS
ATSSS_LL	Indicates that PCF authorizes the ATSSS-LL functionality to support traffic steering, switching and splitting.	ATSSS

5.6.3.19 Enumeration: SteerModeValue

Table 5.6.3.19-1: Enumeration SteerModeValue

Enumeration value	Description	Applicability
ACTIVE_STANDBY	Indicates the steering mode is Active-Standy. It is used to steer a SDF on one access (the Active access), when this access is available, and to switch the SDF to the other access (the Standby access), when Active access becomes unavailable.	ATSSS
LOAD_BALANCING	Indicates the traffic of an SDF is split percentually across accesses.	ATSSS
SMALLEST_DELAY	Indicates the traffic of a SDF is steered and/or switch to the access with the smallest delay.	ATSSS
PRIORITY_BASED	Indicates all the traffic of an SDF is steered to the high priority access, until this access is determined to be congested.	ATSSS

5.6.3.20 Enumeration: MulticastAccessControl

Table 5.6.3.20-1: Enumeration MulticastAccessControl

Enumeration value	Description	Applicability
ALLOWED	Indicates the service data flow, corresponding to the service data flow template, is allowed.	WWC
NOT_ALLOWED	Indicates the service data flow, corresponding to the service data flow template, is not allowed. This is default value.	WWC

5.6.3.21 Enumeration RequestedQosMonitoringParameter

Table 5.6.3.21-1: Enumeration RequestedQosMonitoringParameter

Enumeration value	Description	Applicability
DOWNLINK	Indicates the DL packet delay between the UE and the UPF is to be monitored.	
UPLINK	Indicates the UL packet delay between the UE and the UPF is to be monitored.	
ROUND_TRIP	Indicates the round trip packet delay between the UE and the UPF is to be monitored.	

5.6.3.22 Enumeration: ReportingFrequency

Table 5.6.3.22-1: Enumeration ReportingFrequency

Enumeration value	Description	Applicability
EVENT_TRIGGERED	Indicates the delay is reported when the delay exceeds the threshold.	
PERIODIC	Indicates the delay is reported periodically.	
SESSION_RELEASE	Indicates the delay is reported when the PDU session is released.	

5.6.3.23 Enumeration: SmPolicyAssociationReleaseCause

The enumeration SmPolicyAssociationReleaseCause represents the cause why the PCF requests the termination of the policy association. It shall comply with the provisions defined in table 5.6.3.23-1.

Table 5.6.3.23-1: Enumeration SmPolicyAssociationReleaseCause

Enumeration value	Description	Applicability
UNSPECIFIED	This value is used for unspecified reasons.	
UE_SUBSCRIPTION	This value is used to indicate that the policy association needs to be terminated because the subscription of UE has changed (e.g. was removed).	
INSUFFICIENT_RES	This value is used to indicate that the server is overloaded and needs to abort the policy association.	
VALIDATION_CONDITION_NOT_MET	This value is used to indicate that the policy association needs to be terminated because the validation condition of background data transfer policy is not met.	EnhancedBackgroundDataTransfer
REACTIVATION_REQUESTED	This value is used to indicate that policy association needs to be terminated because the PCF is not able to maintain the existing PDU session and requests that the PDU session is reactivated.	ReleaseToReactivate

5.6.3.24 Enumeration: PduSessionRelCause

Table 5.6.3.24-1: Enumeration PduSessionRelCause

Enumeration value	Description	Applicability
PS_TO_CS_HO	Indicates that the PDU session is terminated due to PS to CS handover.	PDUSessionRelCause
RULE_ERROR	Indicates that the PDU session is terminated due to a session rule modification error.	ImmediateTermination

5.6.3.25 Enumeration: MaPduIndication

Table 5.6.3.25-1: Enumeration MaPduIndication

Enumeration value	Description	Applicability
MA_PDU_REQUEST	UE requested MA PDU session and the request is authorized by subscription.	
MA_PDU_NETWORK_UPGRADE_ALLOWED	UE requested single access PDU session with indication of network upgrade to MA PDU session supported and the upgrade is authorized by subscription.	

5.6.3.26 Enumeration: AtsssCapability

Table 5.6.3.26-1: Enumeration AtsssCapability

Enumeration value	Description	Applicability
ATSSS_LL	Indicates that the MA PDU Session supports the ATSSS-LL capability with any steering mode in the uplink and in the downlink.	
MPTCP_ATSSS_LL	Indicates that the MA PDU Session supports both the MPTCP and ATSSS-LL capability with any steering mode in the uplink and in the downlink.	
MPTCP_ATSSS_LL_WITH_ASMODE_UL	Indicates that the MA PDU Session supports the MPTCP capability with any steering mode in uplink and downlink, and ATSSS-LL capability with any steering mode in the downlink and Active-Standby mode in the uplink.	
MPTCP_ATSSS_LL_WITH_EXSDMODE_DL_ASMODE_UL	Indicates that the MA PDU Session supports the MPTCP capability with any steering mode in uplink and downlink, and ATSSS-LL capability with any steering mode except Smallest Delay mode in the downlink and Active-Standby mode in the uplink.	
MPTCP_ATSSS_LL_WITH_ASMODE_DLUL	Indicates that the MA PDU Session supports the MPTCP capability with any steering mode and ATSSS-LL capability with Active-Standby mode in uplink and downlink.	

5.6.3.27 Enumeration: NetLocAccessSupport

Table 5.6.3.27-1: Enumeration NetLocAccessSupport

Enumeration value	Description	Applicability
ANR_NOT_SUPPORTED	Indicates that the access network does not support the report of access network information.	
TZR_NOT_SUPPORTED	Indicates that the access network does not support the report of UE time zone. (NOTE 1)	
LOC_NOT_SUPPORTED	Indicates that the access network does not support the report of UE Location. (NOTE 2)	
NOTE 1: The UE time zone is not available in EPC untrusted WLAN. NOTE 2: The SMF+PGW determines the UE Location is not available as described in clause B.3.6.3.		

5.6.3.28 Enumeration: PolicyDecisionFailureCode

Table 5.6.3.28-1: PolicyDecisionFailureCode

Enumeration value	Description	Applicability
TRA_CTRL_DECS_ERR	Indicates failure in the provisioning of traffic control decision data.	
QOS_DECS_ERR	Indicates failure in the provisioning of QoS decision data.	
CHG_DECS_ERR	Indicates failure in the provisioning of charging decision data.	
USA_MON_DECS_ERR	Indicates failure in the provisioning of usage monitoring decision data.	UMC
QOS_MON_DECS_ERR	Indicates failure in the provisioning of QoS monitoring decision data.	
CON_DATA_ERR	Indicates failure in the provisioning of condition data.	
POLICY_PARAM_ERR	Indicates the information related to the provisioned policy parameter(s) is incorrect, incomplete or inconsistent.	ExtPolicyDecisionErrorHandling

5.6.3.29 Enumeration: NotificationControlIndication

Table 5.6.3.29-1: Enumeration NotificationControlIndication

Enumeration value	Description	Applicability
DDN_FAILURE	Indicates that the notification of DDN Failure is requested.	DDNEventPolicyControl
DDD_STATUS	Indicates that the notification of DDD stauts is requested.	DDNEventPolicyControl

5.6.3.30 Void

5.6.3.31 Enumeration: SteerModeIndicator

Table 5.6.3.31-1: Enumeration SteerModeIndicator

Enumeration value	Description	Applicability
AUTO_LOAD_BALANCE	Allows the UE and UPF to autonomously determine the traffic load of an SDF distributed across accesses.	
UE_ASSISTANCE	Allows the UE to decide how to distribute the UL traffic of an SDF and the UE may inform the UPF how it decided to distribute the UL traffic.	

5.7 Error handling

5.7.1 General

HTTP error handling shall be supported as specified in clause 5.2.4 of 3GPP TS 29.500 [4].

For the Npcf_SMPolicyControl API, HTTP error responses shall be supported as specified in clause 4.8 of 3GPP TS 29.501 [5].

Protocol errors and application errors specified in table 5.2.7.2-1 of 3GPP TS 29.500 [4] shall be supported for an HTTP method if the corresponding HTTP status codes are specified as mandatory for that HTTP method in table 5.2.7.1-1 of 3GPP TS 29.500 [4].

In addition, the requirements in the following clauses shall apply.

5.7.2 Protocol Errors

In this Release of the specification, there are no additional protocol errors applicable for the Npcf_SMPolicyControl API.

5.7.3 Application Errors

The application errors defined for the Npcf_SMPolicyControl API are listed in table 5.7.3-1 and 5.7.3-2.

Table 5.7.3-1: Application errors when PCF acts as a server

Application Error	HTTP status code	Description
USER_UNKNOWN	400 Bad Request	The HTTP request is rejected because the end user specified in the request is unknown to the PCF. (NOTE 1) (NOTE 3)
ERROR_INITIAL_PARAMETERS	400 Bad Request	The HTTP request is rejected because the set of session or subscriber information needed by the PCF for rule selection is incomplete or erroneous or not available for the decision to be made. (E.g. QoS, RAT type, subscriber information) (NOTE 1) (NOTE 2) (NOTE 3)
ERROR_TRIGGER_EVENT	400 Bad Request	The HTTP request is rejected because the set of session information sent the message originated due to a trigger been met is incoherent with the previous set of session information for the same session. (E.g. trigger met was RAT changed, and the RAT notified is the same as before) (NOTE 2) (NOTE 3)
ERROR_TRAFFIC_MAPPING_INFO_REJECTED	403 Forbidden	The HTTP request is rejected because the PCF does not accept one or more of the traffic mapping filters provided by the NF service consumer in a PCC Request. (NOTE 2) (NOTE 3)
ERROR_CONFLICTING_REQUEST	403 Forbidden	The HTTP request is rejected because the PCF cannot accept the UE-initiated resource request as a network-initiated resource allocation is already in progress that has packet filters that cover the packet filters in the received UE-initiated resource request. The NF service consumer shall reject the attempt for UE-initiated resource request. (NOTE 2) (NOTE 3)
LATE_OVERLAPPING_REQUEST	403 Forbidden	The request is rejected because it collides with and exiting Policy Association with a more recent originating timestamp. (NOTE 1)
POLICY_CONTEXT_DENIED	403 Forbidden	The HTTP request is rejected because the PCF does not accept the NF service consumer request due to operator policies and/or local configuration. (NOTE 1) (NOTE 2) (NOTE 3)
VALIDATION_CONDITION_NOT_MET	403 Forbidden	The HTTP request is rejected because the PCF does not accept the NF service consumer request because the validation condition of background data transfer policy is not met. (NOTE 1) (NOTE 3)
PENDING_TRANSACTION	400 Bad Request	This error shall be used when the PendingTransaction feature is supported and the PCF receives an incoming request on a policy association while it has an ongoing transaction on the same policy association and cannot handle the request as described in clause 9.2 of 3GPP TS 29.513 [7]. (NOTE 2)
INVALID_BDT_POLICY	403 Forbidden	The HTTP request is rejected because the PCF does not accept the NF service consumer request because the background data transfer policy is invalid. (NOTE 1)
EXCEEDED_UE_SLICE_DATA_RATE	403 Forbidden	The HTTP request is rejected because the PCF does not accept the NF service consumer request because the authorized data rate exceeds the consumed data rate for that UE and network slice. (NOTE 1) (NOTE 2)
EXCEEDED_SLICE_DATA_RATE	403 Forbidden	The HTTP request is rejected because the PCF does not accept the NF service consumer request because the authorized data rate exceeds the consumed data rate for that slice. (NOTE 1) (NOTE 2)
POLICY_ASSOCIATION_NOT_FOUND	404 Not Found	The HTTP request is rejected because no policy association corresponding to the request exists in the PCF. (NOTE 2)

NOTE 1: These application errors are used by the create service operation (see clause 4.2.2.2) and included in the responses to the POST request.
NOTE 2: These application errors are used by the update service operation (see clause 4.2.4.2) and included in the responses to the POST request.
NOTE 3: The Cause codes mapping performed by NF service consumer between this Application Error and the 5GSM related value is specified in clause 5.2.2.2 of 3GPP TS 29.524 [40].
NOTE 4: Including a "ProblemDetails" data structure with the "cause" attribute in the HTTP response is optional unless explicitly mandated in the service operation clauses.

Table 5.7.3-2: Application errors when NF service consumer acts as a server to receive a notification

Application Error	HTTP status code	Description
PCC_RULE_EVENT	400 Bad Request	The HTTP request is rejected because all the PCC rules provisioned by the PCF in the request cannot be installed/activated. It is used to inform the PCF that the request failed, and should not be attempted again. (NOTE 1)
PCC_QOS_FLOW_EVENT	400 Bad Request	The HTTP request is rejected because for some reason all the PCC rules provisioned by the PCF in the request cannot be enforced or modified successfully in a network initiated procedure. It is used to inform the PCF that the request could not be satisfied at the time it was received, but may be able to satisfy the request in the future. (NOTE 1)
UE_STATUS_SUSPEND	400 Bad Request	The HTTP request is rejected because the UE's status is suspended and the policy decisions received from the PCF cannot be enforced by the NF service consumer. Applicable only to functionality introduced with the PolicyUpdateWhenUESuspends feature as described in clause 5.8. (NOTE 1)
RULE_PERMANENT_ERROR	400 Bad Request	The HTTP request is rejected because all the PCC rules and/or session rules provisioned by the PCF in the request cannot be installed/activated. It is used to inform the PCF that the request failed, and should not be attempted again. Applicable only to functionality introduced with the SessionRuleErrorHandling feature as described in clause 5.8. (NOTE 1)
RULE_TEMPORARY_ERROR	400 Bad Request	The HTTP request is rejected because for some reason all the PCC rules and/or session rules provisioned by the PCF in the request cannot be enforced or modified successfully in a network initiated procedure. It is used to inform the PCF that the request could not be satisfied at the time it was received, but may be able to satisfy the request in the future. Applicable only to functionality introduced with the SessionRuleErrorHandling feature as described in clause 5.8. (NOTE 1)
PENDING_TRANSACTION	400 Bad Request	This error shall be used when the PendingTransaction feature is supported and the NF service consumer receives an incoming request on a policy association while it has an ongoing transaction on the same policy association and cannot handle the request as described in clause 9.2 of 3GPP TS 29.513 [7]. (NOTE 1)
AN_GW_FAILED	400 Bad Request	This error shall be used when SGWRest feature is supported and the received policy decisions (i.e. installation/modification of PCC rules or session rules) cannot be enforced by the SMF because the AN-Gateway has failed. (NOTE 1)
NOTE 1: These application errors are used by the UpdateNotify service operation (see clause 4.2.3.2) and included in the responses to the POST request. NOTE 2: Including a "ProblemDetails" data structure with the "cause" attribute in the HTTP response is optional unless explicitly mandated in the service operation clauses.		

5.8 Feature negotiation

The optional features in table 5.8-1 are defined for the Npcf_SMPolicyControl API. They shall be negotiated using the extensibility mechanism defined in clause 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, steering the 5G-LAN type of services or routing of the user traffic to a local Data Network identified by the DNAI per AF request. If the NF service consumer supports this feature, the PCF shall behave as described in clause 4.2.6.2.6.
2	ResShare	This feature indicates the support of service data flows that share resources. If the NF service consumer supports this feature, the PCF shall behave as described in clause 4.2.6.2.8.
3	3GPP-PS-Data-Off	This feature indicates the support of 3GPP PS Data off status change reporting.
4	ADC	This feature indicates the support of application detection and control.
5	UMC	Indicates that the usage monitoring control is supported.
6	NetLoc	This feature indicates the support of the Access Network Information Reporting for 5GS.
7	RAN-NAS-Cause	This feature indicates the support for the detailed release cause code information from the access network. (NOTE)
8	ProvAFsignalFlow	This feature indicates support for the feature of IMS Restoration as described in clause 4.2.3.17. If NF service consumer supports this feature the PCF may provision AF signalling IP flow information.
9	PCSCF-Restoration-Enhancement	This feature indicates support of P-CSCF Restoration Enhancement. It is used for the NF service consumer to indicate if it supports P-CSCF Restoration Enhancement.
10	PRA	This feature indicates the support of presence reporting area change reporting. The support of the update of a UE Dedicated Presence Reporting Area is unspecified.
11	RuleVersioning	This feature indicates the support of PCC rule versioning as defined in clause 4.2.6.7.
12	SponsoredConnectivity	This feature indicates support for sponsored data connectivity feature. If the NF service consumer supports this feature, the PCF may authorize sponsored data connectivity to the subscriber.
13	RAN-Support-Info	This feature indicates the support of maximum packet loss rate value(s) for uplink and/or downlink voice service data flow(s).
14	PolicyUpdateWhenUESuspends	This feature indicates the support of report when the UE is suspended and then resumed from suspend state. Only applicable to the interworking scenario as defined in Annex B.
15	AccessTypeCondition	This feature indicates the support of access type conditioned authorized Session-AMBR as defined in clause 4.2.6.3.2.4.
16	MultiIpv6AddrPrefix	This feature indicates the support of multiple Ipv6 address prefixes reporting.
17	SessionRuleErrorHandling	This feature indicates the support of session rule error handling.
18	AF_Charging_Identifier	This feature indicates the support of long character strings as charging identifiers.
19	ATSSS	This feature indicates the support of the access traffic switching, steering and splitting functionality as defined in clauses 4.2.6.2.17 and 4.2.6.3.4.
20	PendingTransaction	This feature indicates support for the race condition handling as defined in 3GPP TS 29.513 [7].
21	URLLC	This feature indicates support of Ultra-Reliable Low-Latency Communication (URLLC) requirements, i.e. AF application relocation acknowledgement requirement and UE address(es) preservation. The TSC feature shall be supported in order to support this feature.
22	MacAddressRange	Indicates the support of a set of MAC addresses with a specific range in the traffic filter.
23	WWC	Indicates support of wireless and wireline convergence access as defined in annex C.

24	QosMonitoring	Indicates support of QoS monitoring as defined in clause 4.2.3.25 and 4.2.4.24.
25	AuthorizationWithRequiredQoS	Indicates support of policy authorization for the AF session with required QoS as defined in clause 4.2.3.22.
26	EnhancedBackgroundDataTransfer	Indicates the support of applying the Background Data Transfer Policy to a future PDU session.
27	DN-Authorization	This feature indicates the support of DN-AAA authorization data for policy control.
28	PDUSessionRelCause	Indicates the support of "PS_TO_CS_HO" PDU session release cause.
29	SamePcf	This feature indicates the support of same PCF selection for the parameter's combination.
30	ADCmultiRedirection	This feature indicates support for multiple redirection information in application detection and control. It requires the support of ADC feature.
31	RespBasedSessionRel	Indicates support of handling PDU session termination functionality as defined in clause 4.2.4.22.
32	TimeSensitiveNetworking	Indicates that the 5G System is integrated within the external network as a TSN bridge.
33	EMDBV	This feature indicates the support of the ExtMaxDataBurstVol data type defined in 3GPP TS 29.571 [11]. The use of this data type is specified in clause 4.2.2.1.
34	DNNSelectionMode	This feature indicates the support of DNN selection mode.
35	EPSFallbackReport	This feature indicates the support of the report of EPS Fallback as defined in clauses B.3.3.2 and B.3.4.6.
36	PolicyDecisionErrorHandling	This feature indicates the support of the error report of the policy decision and/or condition data which is not referred by any PCC rule or session rule as defined in clause 4.2.3.26 and 4.2.4.26.
37	DDNEventPolicyControl	This feature indicates the support for policy control in the case of DDN Failure and Delivery Status events as defined in clause 4.2.4.27.
38	ReallocationOfCredit	This feature indicates the support of notifications of reallocation of credit.
39	BDTPolicyRenegotiation	This feature indicates the support of the BDT policy re-negotiation.
40	ExtPolicyDecisionErrorHandling	This feature indicates the support of the error report of a faulty SM policy decision parameter as defined in clause 4.2.3.26 and 4.2.4.26. It requires the support of PolicyDecisionErrorHandling feature.
41	ImmediateTermination	This feature indicates the support of the termination the PDU session when the NF service consumer cannot ensure the UE, RAN, AMF, or UPF can revert to the status before the PDU session modification occurred, as defined in clause 4.2.4.21.
42	AggregatedUELocChanges	This feature indicates the support of notifications of serving area (i.e. tracking area) and/or serving cell changes.
43	ES3XX	Extended Support for 3xx redirections. This feature indicates the support of redirection for any service operation, according to Stateless NF procedures as specified in clauses 6.5.3.2 and 6.5.3.3 of 3GPP TS 29.500 [4] and according to HTTP redirection principles for indirect communication, as specified in clause 6.10.9 of 3GPP TS 29.500 [4].
44	GroupIdListChange	This feature indicates the support for the notification of changes in the list of internal group identifiers.
45	DisableUENotification	Indicates the support of disabling QoS flow parameters signalling to the UE when the SMF is notified by the NG-RAN of changes in the fulfilled QoS situation. This feature requires that the AuthorizationWithRequiredQoS featute is also supported.
46	OfflineChOnly	This feature enables the PCF to signal the "PDU Session with offline charging only" indication as defined in clause 4.2.2.3.3.

47	Dual-Connectivity-redundant-UP-paths	Indicates the support of policy authorization of end to end redundant user plane path using dual connectivity as described in clause 4.2.2.20.
48	DDNEventPolicyControl2	This feature indicates the support for the policy control removal in the case of DDN Failure and/or Delivery Status event(s) is cancelled as defined in clause 4.2.4.27. The DDNEventPolicyControl feature shall be supported in order to support this feature.
49	VPLMN-QoS-Control	Indicates the support of QoS constraints from the VPLMN for the derivation of the authorized Session-AMBR and authorized default QoS.
50	2G3GIWK	This feature indicates the support of GERAN and UTRAN access over N7 interface.
51	TimeSensitiveCommunication	Indicates that the 5G System is integrated within the external network as a TSC user plane node to enable the Time Sensitive Communications and Time Synchronization. This feature requires that the TimeSensitiveNetworking feature is also supported.
52	AF_latency	This feature indicates the support of Edge relocation considering user plane latency. This feature requires that the TSC feature is also supported.
53	SatBackhaulCategoryChg	This feature indicates the support of notification of a change between different satellite backhaul categories, or between satellite backhaul and non-satellite backhaul.
54	CHFsetSupport	Indicates the support of CHF redundancy and failover mechanisms based on CHF instance availability within a CHF Set, as described in clause 4.2.2.3.1.
55	EnATSSS	Indicates the support of ATSSS enhancement. It requires the support of ATSSS feature.
56	MPSforDTS	Indicates support of the MPSfor DTS feature as described in clause 4.2.6.2.12.4.
57	RoutingInfoRemoval	Indicates the support of the removal of the "routeToLocs" attribute from the TrafficControlData instance.
58	ePRA	This feature indicates the support of presence reporting area change reporting. It additionally supports the update of the elements of a UE Dedicated Presence Reporting Area by the full replacement of the previously provided one comparing with the PRA feature.
59	AMInfluence	Indicates the support of the delivery of the PCF for the UE request to be notified by the PCF for the PDU session about PDU session established/terminated events.
60	PvsSupport	This feature indicates the support of SNPN UE Remote Provisioning via User Plane as described in clause 4.2.2.21.
61	EneNA	This feature indicates the support of NWDAF data reporting.
62	BIUMR	This feature bit indicates whether the NF Service Consumer (e.g. SMF) and PCF supports Binding Indication Update for multiple resource contexts specified in clauses 6.12.1 and 5.2.3.2.6 of 3GPP TS 29.500 [4].
63	EASIPreplacement	This feature indicates the support of EAS IP replacement. This feature requires that the TSC feature is also supported.
64	ExposureToEAS	This feature indicates the support of exposure of QoS monitoring results to local AF. This feature requires that QosMonitoring feature is also supported.
65	SimultConnectivity	This feature indicates the support of temporary simultaneously connectivity at edge relocation. This feature requires that the TSC feature is also supported.
66	SGWRest	This feature indicates the support of SGW Restoration procedures. Only applicable to the interworking scenario as defined in Annex B.
67	ReleaseToReactivate	This feature indicates that the PCF can request the SMF for reactivation of a PDU session based on an SM Policy Association release cause.
68	EASDiscovery	This feature indicates the support of EAS (re)discovery.
69	AccNetChargId_String	This feature indicates the support of long character strings as access network charging identifier.
NOTE: 5GS and EPS release cause code information is supported. The EPS release cause code information from the access network is only applicable to EPS interworking scenarios as specified in Annex B.		

5.9 Security

As indicated in 3GPP TS 33.501 [27], the access to the Npcf_SMPolicyControl API shall be authorized by means of the OAuth2 protocol (see IETF RFC 6749 [28]), using the "Client Credentials" authorization grant, where the NRF (see 3GPP TS 29.510 [29]) plays the role of the authorization server.

An NF service consumer, prior to consuming services offered by the Npcf_SMPolicyControl API, shall obtain a "token" from the authorization server, by invoking the Access Token Request service, as described in 3GPP TS 29.510 [29], clause 5.4.2.2.

NOTE: When multiple NRFs are deployed in a network, the NRF used as authorization server is the same NRF that the NF service consumer used for discovering the Npcf_SMPolicyControl service.

The Npcf_SMPolicyControl API defines a single scope "npcf-smpolicycontrol" for OAuth2 authorization (as specified in 3GPP TS 33.501 [27]) for the entire API, and it does not define any additional scopes at resource or operation level.

Annex A (normative): OpenAPI specification

A.1 General

The present Annex contains an OpenAPI [10] specification of HTTP messages and content bodies used by the Npcf_SMPolicyControl API.

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

NOTE 1: The semantics and procedures, as well as conditions, e.g. for the applicability and allowed combinations of attributes or values, not expressed in the OpenAPI definitions but defined in other parts of the specification also apply.

Informative copies of the OpenAPI specification file contained in this 3GPP Technical Specification are available on a Git-based repository, that uses the GitLab software version control system (see clause 5B of the 3GPP TR 21.900 [38] and clause 5.3.1 of the 3GPP TS 29.501 [5] for further information).

A.2 Npcf_SMPolicyControl API

```
openapi: 3.0.0
info:
  title: Npcf_SMPolicyControl API
  version: 1.2.0
  description: |
    Session Management Policy Control Service
    © 2022, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.
externalDocs:
  description: 3GPP TS 29.512 V17.7.0; 5G System; Session Management Policy Control Service.
  url: 'https://www.3gpp.org/ftp/Specs/archive/29_series/29.512/'
security:
  - {}
  - oAuth2ClientCredentials:
    - npcf-smpolicycontrol
servers:
  - url: '{apiRoot}/npcf-smpolicycontrol/v1'
    variables:
      apiRoot:
        default: https://example.com
        description: apiRoot as defined in clause 4.4 of 3GPP TS 29.501
paths:
  /sm-policies:
    post:
      summary: Create a new Individual SM Policy
      operationId: CreateSMPolicy
      tags:
        - SM Policies (Collection)
      requestBody:
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/SmPolicyContextData'
      responses:
        '201':
          description: Created
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/SmPolicyDecision'
          headers:
            Location:
              description: Contains the URI of the newly created resource
              required: true
              schema:
```

```
              type: string
        '308':
          description: Permanent Redirect
          headers:
            Location:
              description: >
                Contains the URI of the PCF within the existing PCF binding information stored in
                the BSF for the same UE ID, S-NSSAI and DNN combination
              required: true
              schema:
                type: string
        '400':
          $ref: 'TS29571_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29571_CommonData.yaml#/components/responses/401'
        '403':
          $ref: 'TS29571_CommonData.yaml#/components/responses/403'
        '404':
          $ref: 'TS29571_CommonData.yaml#/components/responses/404'
        '411':
          $ref: 'TS29571_CommonData.yaml#/components/responses/411'
        '413':
          $ref: 'TS29571_CommonData.yaml#/components/responses/413'
        '415':
          $ref: 'TS29571_CommonData.yaml#/components/responses/415'
        '429':
          $ref: 'TS29571_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29571_CommonData.yaml#/components/responses/500'
        '503':
          $ref: 'TS29571_CommonData.yaml#/components/responses/503'
        default:
          $ref: 'TS29571_CommonData.yaml#/components/responses/default'
      callbacks:
        SmPolicyUpdateNotification:
          '{$request.body#/notificationUri}/update':
            post:
              requestBody:
                required: true
                content:
                  application/json:
                    schema:
                      $ref: '#/components/schemas/SmPolicyNotification'
              responses:
                '200':
                  description: OK. The current applicable values corresponding to the policy control
request trigger is reported
                  content:
                    application/json:
                      schema:
                        oneOf:
                          - $ref: '#/components/schemas/UeCampingRep'
                          - type: array
                            items:
                              $ref: '#/components/schemas/PartialSuccessReport'
                            minItems: 1
                          - type: array
                            items:
                              $ref: '#/components/schemas/PolicyDecisionFailureCode'
                            minItems: 1
                '204':
                  description: No Content, Notification was succesfull
                '307':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/307'
                '308':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/308'
                '400':
                  description: Bad Request.
                  content:
                    application/json:
                      schema:
                        $ref: '#/components/schemas/ErrorReport'
                '401':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/401'
                '403':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/403'
                '404':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/404'
```

```
              '411':
                $ref: 'TS29571_CommonData.yaml#/components/responses/411'
              '413':
                $ref: 'TS29571_CommonData.yaml#/components/responses/413'
              '415':
                $ref: 'TS29571_CommonData.yaml#/components/responses/415'
              '429':
                $ref: 'TS29571_CommonData.yaml#/components/responses/429'
              '500':
                $ref: 'TS29571_CommonData.yaml#/components/responses/500'
              '503':
                $ref: 'TS29571_CommonData.yaml#/components/responses/503'
              default:
                $ref: 'TS29571_CommonData.yaml#/components/responses/default'
      SmPolicyControlTerminationRequestNotification:
        '{$request.body#/notificationUri}/terminate':
          post:
            requestBody:
              required: true
              content:
                application/json:
                  schema:
                    $ref: '#/components/schemas/TerminationNotification'
            responses:
              '204':
                description: No Content, Notification was successful
              '307':
                $ref: 'TS29571_CommonData.yaml#/components/responses/307'
              '308':
                $ref: 'TS29571_CommonData.yaml#/components/responses/308'
              '400':
                $ref: 'TS29571_CommonData.yaml#/components/responses/400'
              '401':
                $ref: 'TS29571_CommonData.yaml#/components/responses/401'
              '403':
                $ref: 'TS29571_CommonData.yaml#/components/responses/403'
              '404':
                $ref: 'TS29571_CommonData.yaml#/components/responses/404'
              '411':
                $ref: 'TS29571_CommonData.yaml#/components/responses/411'
              '413':
                $ref: 'TS29571_CommonData.yaml#/components/responses/413'
              '415':
                $ref: 'TS29571_CommonData.yaml#/components/responses/415'
              '429':
                $ref: 'TS29571_CommonData.yaml#/components/responses/429'
              '500':
                $ref: 'TS29571_CommonData.yaml#/components/responses/500'
              '503':
                $ref: 'TS29571_CommonData.yaml#/components/responses/503'
              default:
                $ref: 'TS29571_CommonData.yaml#/components/responses/default'
  /sm-policies/{smPolicyId}:
    get:
      summary: Read an Individual SM Policy
      operationId: GetSMPolicy
      tags:
        - Individual SM Policy (Document)
      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'
        '307':
          $ref: 'TS29571_CommonData.yaml#/components/responses/307'
        '308':
          $ref: 'TS29571_CommonData.yaml#/components/responses/308'
        '400':
          $ref: 'TS29571_CommonData.yaml#/components/responses/400'
```

```
      '401':
        $ref: 'TS29571_CommonData.yaml#/components/responses/401'
      '403':
        $ref: 'TS29571_CommonData.yaml#/components/responses/403'
      '404':
        $ref: 'TS29571_CommonData.yaml#/components/responses/404'
      '406':
        $ref: 'TS29571_CommonData.yaml#/components/responses/406'
      '429':
        $ref: 'TS29571_CommonData.yaml#/components/responses/429'
      '500':
        $ref: 'TS29571_CommonData.yaml#/components/responses/500'
      '503':
        $ref: 'TS29571_CommonData.yaml#/components/responses/503'
      default:
        $ref: 'TS29571_CommonData.yaml#/components/responses/default'
/sm-policies/{smPolicyId}/update:
  post:
    summary: Update an existing Individual SM Policy
    operationId: UpdateSMPolicy
    tags:
      - Individual SM Policy (Document)
    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'
      '307':
        $ref: 'TS29571_CommonData.yaml#/components/responses/307'
      '308':
        $ref: 'TS29571_CommonData.yaml#/components/responses/308'
      '400':
        $ref: 'TS29571_CommonData.yaml#/components/responses/400'
      '401':
        $ref: 'TS29571_CommonData.yaml#/components/responses/401'
      '403':
        $ref: 'TS29571_CommonData.yaml#/components/responses/403'
      '404':
        $ref: 'TS29571_CommonData.yaml#/components/responses/404'
      '411':
        $ref: 'TS29571_CommonData.yaml#/components/responses/411'
      '413':
        $ref: 'TS29571_CommonData.yaml#/components/responses/413'
      '415':
        $ref: 'TS29571_CommonData.yaml#/components/responses/415'
      '429':
        $ref: 'TS29571_CommonData.yaml#/components/responses/429'
      '500':
        $ref: 'TS29571_CommonData.yaml#/components/responses/500'
      '503':
        $ref: 'TS29571_CommonData.yaml#/components/responses/503'
      default:
        $ref: 'TS29571_CommonData.yaml#/components/responses/default'
/sm-policies/{smPolicyId}/delete:
  post:
    summary: Delete an existing Individual SM Policy
    operationId: DeleteSMPolicy
    tags:
      - Individual SM Policy (Document)
    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
        '307':
          $ref: 'TS29571_CommonData.yaml#/components/responses/307'
        '308':
          $ref: 'TS29571_CommonData.yaml#/components/responses/308'
        '400':
          $ref: 'TS29571_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29571_CommonData.yaml#/components/responses/401'
        '403':
          $ref: 'TS29571_CommonData.yaml#/components/responses/403'
        '404':
          $ref: 'TS29571_CommonData.yaml#/components/responses/404'
        '411':
          $ref: 'TS29571_CommonData.yaml#/components/responses/411'
        '413':
          $ref: 'TS29571_CommonData.yaml#/components/responses/413'
        '415':
          $ref: 'TS29571_CommonData.yaml#/components/responses/415'
        '429':
          $ref: 'TS29571_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29571_CommonData.yaml#/components/responses/500'
        '503':
          $ref: 'TS29571_CommonData.yaml#/components/responses/503'
        default:
          $ref: 'TS29571_CommonData.yaml#/components/responses/default'
components:
  securitySchemes:
    oAuth2ClientCredentials:
      type: oauth2
      flows:
        clientCredentials:
          tokenUrl: '{nrfApiRoot}/oauth2/token'
          scopes:
            npcf-smpolicycontrol: Access to the Npcf_SMPolicyControl API
  schemas:
    SmPolicyControl:
      description: Contains the parameters used to request the SM policies and the SM policies
authorized by the PCF.
      type: object
      properties:
        context:
          $ref: '#/components/schemas/SmPolicyContextData'
        policy:
          $ref: '#/components/schemas/SmPolicyDecision'
      required:
        - context
        - policy
    SmPolicyContextData:
      description: Contains the parameters used to create an Individual SM policy resource.
      type: object
      properties:
        accNetChId:
          $ref: '#/components/schemas/AccNetChId'
        chargEntityAddr:
          $ref: '#/components/schemas/AccNetChargingAddress'
        gpsi:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Gpsi'
        supi:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Supi'
        invalidSupi:
          type: boolean
          description: >
            When this attribute is included and set to true, it indicates that the supi attribute
            contains an invalid value.This attribute shall be present if the SUPI is not available
            in the SMF or the SUPI is unauthenticated. When present it shall be set to true for an
```

```
          invalid SUPI and false (default) for a valid SUPI.
        interGrpIds:
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/GroupId'
          minItems: 1
        pduSessionId:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/PduSessionId'
        pduSessionType:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/PduSessionType'
        chargingcharacteristics:
          type: string
        dnn:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Dnn'
        dnnSelMode:
          $ref: 'TS29502_Nsmf_PDUSession.yaml#/components/schemas/DnnSelectionMode'
        notificationUri:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
        accessType:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/AccessType'
        ratType:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/RatType'
        addAccessInfo:
          $ref: '#/components/schemas/AdditionalAccessInfo'
        servingNetwork:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/PlmnIdNid'
        userLocationInfo:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/UserLocation'
        ueTimeZone:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/TimeZone'
        pei:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Pei'
        ipv4Address:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv4Addr'
        ipv6AddressPrefix:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv6Prefix'
        ipDomain:
          type: string
          description: Indicates the IPv4 address domain
        subsSessAmbr:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ambr'
        authProfIndex:
          type: string
          description: Indicates the DN-AAA authorization profile index
        subsDefQos:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/SubscribedDefaultQos'
        vplmnQos:
          $ref: 'TS29502_Nsmf_PDUSession.yaml#/components/schemas/VplmnQos'
        numOfPackFilter:
          type: integer
          description: Contains the number of supported packet filter for signalled QoS rules.
        online:
          type: boolean
          description: If it is included and set to true, the online charging is applied to the PDU
session.
        offline:
          type: boolean
          description: If it is included and set to true, the offline charging is applied to the PDU
session.
        3gppPsDataOffStatus:
          type: boolean
          description: If it is included and set to true, the 3GPP PS Data Off is activated by the
UE.
        refQosIndication:
          type: boolean
          description: If it is included and set to true, the reflective QoS is supported by the UE.
        traceReq:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/TraceData'
        sliceInfo:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Snssai'
        qosFlowUsage:
          $ref: '#/components/schemas/QosFlowUsage'
        servNfId:
          $ref: '#/components/schemas/ServingNfIdentity'
        suppFeat:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'
        smfId:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/NfInstanceId'
```

```
        recoveryTime:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DateTime'
        maPduInd:
          $ref: '#/components/schemas/MaPduIndication'
        atsssCapab:
          $ref: '#/components/schemas/AtsssCapability'
        ipv4FrameRouteList:
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv4AddrMask'
          minItems: 1
        ipv6FrameRouteList:
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv6Prefix'
          minItems: 1
        satBackhaulCategory:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/SatelliteBackhaulCategory'
        pcfUeInfo:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/PcfUeCallbackInfo'
        pvsInfo:
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/ServerAddressingInfo'
          minItems: 1
        onboardInd:
          type: boolean
          description: If it is included and set to true, it indicates that the PDU session is used
for UE Onboarding.
        nwdafDatas:
          type: array
          items:
            $ref: '#/components/schemas/NwdafData'
          minItems: 1
      required:
        - supi
        - pduSessionId
        - pduSessionType
        - dnn
        - notificationUri
        - sliceInfo
    SmPolicyDecision:
      description: Contains the SM policies authorized by the PCF.
      type: object
      properties:
        sessRules:
          type: object
          additionalProperties:
            $ref: '#/components/schemas/SessionRule'
          minProperties: 1
          description: >
            A map of Sessionrules with the content being the SessionRule as described in
            clause 5.6.2.7. The key used in this map for each entry is the sessRuleId
            attribute of the corresponding SessionRule.
        pccRules:
          type: object
          additionalProperties:
            $ref: '#/components/schemas/PccRule'
          minProperties: 1
          description: >
            A map of PCC rules with the content being the PCCRule as described in
            clause 5.6.2.6. The key used in this map for each entry is the pccRuleId
            attribute of the corresponding PccRule.
          nullable: true
        pcscfRestIndication:
          type: boolean
          description: If it is included and set to true, it indicates the P-CSCF Restoration is
requested.
        qosDecs:
          type: object
          additionalProperties:
            $ref: '#/components/schemas/QosData'
          minProperties: 1
          description: >
            Map of QoS data policy decisions. The key used in this map for each entry is the qosId
            attribute of the corresponding QosData.
        chgDecs:
          type: object
```

```
          additionalProperties:
            $ref: '#/components/schemas/ChargingData'
          minProperties: 1
          description: >
            Map of Charging data policy decisions. The key used in this map for each entry
            is the chgId attribute of the corresponding ChargingData.
          nullable: true
        chargingInfo:
          $ref: '#/components/schemas/ChargingInformation'
        traffContDecs:
          type: object
          additionalProperties:
            $ref: '#/components/schemas/TrafficControlData'
          minProperties: 1
          description: >
            Map of Traffic Control data policy decisions. The key used in this map for each entry
            is the tcId attribute of the corresponding TrafficControlData.
        umDecs:
          type: object
          additionalProperties:
            $ref: '#/components/schemas/UsageMonitoringData'
          minProperties: 1
          description: >
            Map of Usage Monitoring data policy decisions. The key used in this map for each entry
            is the umId attribute of the corresponding UsageMonitoringData.
          nullable: true
        qosChars:
          type: object
          additionalProperties:
            $ref: '#/components/schemas/QosCharacteristics'
          minProperties: 1
          description: Map of QoS characteristics for non standard 5QIs. This map uses the 5QI
values as keys.
        qosMonDecs:
          type: object
          additionalProperties:
            $ref: '#/components/schemas/QosMonitoringData'
          minProperties: 1
          description: >
            Map of QoS Monitoring data policy decisions. The key used in this map for each entry
            is the qmId attribute of the corresponding QosMonitoringData.
          nullable: true
        reflectiveQoSTimer:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DurationSec'
        conds:
          type: object
          additionalProperties:
            $ref: '#/components/schemas/ConditionData'
          minProperties: 1
          description: >
            A map of condition data with the content being as described in clause 5.6.2.9. The key
            used in this map for each entry is the condId attribute of the corresponding
ConditionData.
          nullable: true
        revalidationTime:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DateTime'
        offline:
          type: boolean
          description: Indicates the offline charging is applicable to the PDU session when it is
included and set to true.
        online:
          type: boolean
          description: Indicates the online charging is applicable to the PDU session when it is
included and set to true.
        offlineChOnly:
          type: boolean
          default: false
          description: >
            Indicates that the online charging method shall never be used for any PCC rule activated
            during the lifetime of the PDU session.
        policyCtrlReqTriggers:
          type: array
          items:
            $ref: '#/components/schemas/PolicyControlRequestTrigger'
          minItems: 1
          description: Defines the policy control request triggers subscribed by the PCF.
          nullable: true
        lastReqRuleData:
```

```
          type: array
          items:
            $ref: '#/components/schemas/RequestedRuleData'
          minItems: 1
          description: Defines the last list of rule control data requested by the PCF.
        lastReqUsageData:
          $ref: '#/components/schemas/RequestedUsageData'
        praInfos:
          type: object
          additionalProperties:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/PresenceInfoRm'
          minProperties: 1
          description: Map of PRA information. The praId attribute within the PresenceInfo data type
is the key of the map.
          nullable: true
        ipv4Index:
          $ref: 'TS29519_Policy_Data.yaml#/components/schemas/IpIndex'
        ipv6Index:
          $ref: 'TS29519_Policy_Data.yaml#/components/schemas/IpIndex'
        qosFlowUsage:
          $ref: '#/components/schemas/QosFlowUsage'
        relCause:
          $ref: '#/components/schemas/SmPolicyAssociationReleaseCause'
        suppFeat:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'
        tsnBridgeManCont:
          $ref: '#/components/schemas/BridgeManagementContainer'
        tsnPortManContDstt:
          $ref: '#/components/schemas/PortManagementContainer'
        tsnPortManContNwtts:
          type: array
          items:
            $ref: '#/components/schemas/PortManagementContainer'
          minItems: 1
        redSessIndication:
          type: boolean
          description: >
            Indicates whether the PDU session is a redundant PDU session. If absent it means the PDU
            session is not a redundant PDU session.
    SmPolicyNotification:
      description: Represents a notification on the update of the SM policies.
      type: object
      properties:
        resourceUri:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
        smPolicyDecision:
          $ref: '#/components/schemas/SmPolicyDecision'
    PccRule:
      description: Contains a PCC rule information.
      type: object
      properties:
        flowInfos:
          type: array
          items:
            $ref: '#/components/schemas/FlowInformation'
          minItems: 1
          description: An array of IP flow packet filter information.
        appId:
          type: string
          description: A reference to the application detection filter configured at the UPF.
        appDescriptor:
          $ref: '#/components/schemas/ApplicationDescriptor'
        contVer:
          $ref: 'TS29514_Npcf_PolicyAuthorization.yaml#/components/schemas/ContentVersion'
        pccRuleId:
          type: string
          description: Univocally identifies the PCC rule within a PDU session.
        precedence:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uinteger'
        afSigProtocol:
          $ref: '#/components/schemas/AfSigProtocol'
        appReloc:
          type: boolean
          description: Indication of application relocation possibility.
        easRedisInd:
          type: boolean
          description: Indicates the EAS rediscovery is required.
        refQosData:
```

```
          type: array
          items:
            type: string
          minItems: 1
          maxItems: 1
          description: A reference to the QosData policy decision type. It is the qosId described in
clause 5.6.2.8.
        refAltQosParams:
          type: array
          items:
            type: string
          minItems: 1
          description: A Reference to the QosData policy decision type for the Alternative QoS
parameter sets of the service data flow.
        refTcData:
          type: array
          items:
            type: string
          minItems: 1
          maxItems: 1
          description: A reference to the TrafficControlData policy decision type. It is the tcId
described in clause 5.6.2.10.
        refChgData:
          type: array
          items:
            type: string
          minItems: 1
          maxItems: 1
          description: A reference to the ChargingData policy decision type. It is the chgId
described in clause 5.6.2.11.
          nullable: true
        refChgN3gData:
          type: array
          items:
            type: string
          minItems: 1
          maxItems: 1
          description: >
            A reference to the ChargingData policy decision type only applicable to Non-3GPP access
            if "ATSSS" feature is supported. It is the chgId described in clause 5.6.2.11.
          nullable: true
        refUmData:
          type: array
          items:
            type: string
          minItems: 1
          maxItems: 1
          description: A reference to UsageMonitoringData policy decision type. It is the umId
described in clause 5.6.2.12.
          nullable: true
        refUmN3gData:
          type: array
          items:
            type: string
          minItems: 1
          maxItems: 1
          description: >
            A reference to UsageMonitoringData policy decision type only applicable to Non-3GPP
            access if "ATSSS" feature is supported. It is the umId described in clause 5.6.2.12.
          nullable: true
        refCondData:
          type: string
          description: A reference to the condition data. It is the condId described in clause
5.6.2.9.
          nullable: true
        refQosMon:
          type: array
          items:
            type: string
          minItems: 1
          maxItems: 1
          description: A reference to the QosMonitoringData policy decision type. It is the qmId
described in clause 5.6.2.40.
          nullable: true
        addrPreserInd:
          type: boolean
          nullable: true
        tscaiInputDl:
```

```
          $ref: 'TS29514_Npcf_PolicyAuthorization.yaml#/components/schemas/TscaiInputContainer'
        tscaiInputUl:
          $ref: 'TS29514_Npcf_PolicyAuthorization.yaml#/components/schemas/TscaiInputContainer'
        tscaiTimeDom:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uinteger'
        ddNotifCtrl:
          $ref: '#/components/schemas/DownlinkDataNotificationControl'
        ddNotifCtrl2:
          $ref: '#/components/schemas/DownlinkDataNotificationControlRm'
        disUeNotif:
          type: boolean
          nullable: true
      required:
        - pccRuleId
      nullable: true
    SessionRule:
      description: Contains session level policy information.
      type: object
      properties:
        authSessAmbr:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ambr'
        authDefQos:
          $ref: '#/components/schemas/AuthorizedDefaultQos'
        sessRuleId:
          type: string
          description: Univocally identifies the session rule within a PDU session.
        refUmData:
          type: string
          description: A reference to UsageMonitoringData policy decision type. It is the umId
described in clause 5.6.2.12.
          nullable: true
        refUmN3gData:
          type: string
          description: A reference to UsageMonitoringData policy decision type to apply for Non-3GPP
access. It is the umId described in clause 5.6.2.12.
          nullable: true
        refCondData:
          type: string
          description: A reference to the condition data. It is the condId described in clause
5.6.2.9.
          nullable: true
      required:
        - sessRuleId
      nullable: true
    QosData:
      description: Contains the QoS parameters.
      type: object
      properties:
        qosId:
          type: string
          description: Univocally identifies the QoS control policy data within a PDU session.
        5qi:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/5Qi'
        maxbrUl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRateRm'
        maxbrDl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRateRm'
        gbrUl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRateRm'
        gbrDl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRateRm'
        arp:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Arp'
        qnc:
          type: boolean
          description: >
            Indicates whether notifications are requested from 3GPP NG-RAN when the GFBR can no
longer
            (or again) be guaranteed for a QoS Flow during the lifetime of the QoS Flow.
        priorityLevel:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/5QiPriorityLevelRm'
        averWindow:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/AverWindowRm'
        maxDataBurstVol:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/MaxDataBurstVolRm'
        reflectiveQos:
          type: boolean
```

```
          description: Indicates whether the QoS information is reflective for the corresponding
service data flow.
        sharingKeyDl:
          type: string
          description: Indicates, by containing the same value, what PCC rules may share resource in
downlink direction.
        sharingKeyUl:
          type: string
          description: Indicates, by containing the same value, what PCC rules may share resource in
uplink direction.
        maxPacketLossRateDl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/PacketLossRateRm'
        maxPacketLossRateUl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/PacketLossRateRm'
        defQosFlowIndication:
          type: boolean
          description: Indicates that the dynamic PCC rule shall always have its binding with the
QoS Flow associated with the default QoS rule
        extMaxDataBurstVol:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/ExtMaxDataBurstVolRm'
        packetDelayBudget:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/PacketDelBudget'
        packetErrorRate:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/PacketErrRate'
      required:
        - qosId
      nullable: true
    ConditionData:
      description: Contains conditions of applicability for a rule.
      type: object
      properties:
        condId:
          type: string
          description: Uniquely identifies the condition data within a PDU session.
        activationTime:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DateTimeRm'
        deactivationTime:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DateTimeRm'
        accessType:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/AccessType'
        ratType:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/RatType'
      required:
        - condId
      nullable: true
    TrafficControlData:
      description: Contains parameters determining how flows associated with a PCC Rule are treated
(e.g. blocked, redirected, etc).
      type: object
      properties:
        tcId:
          type: string
          description: Univocally identifies the traffic control policy data within a PDU session.
        flowStatus:
          $ref: 'TS29514_Npcf_PolicyAuthorization.yaml#/components/schemas/FlowStatus'
        redirectInfo:
          $ref: '#/components/schemas/RedirectInformation'
        addRedirectInfo:
          type: array
          items:
            $ref: '#/components/schemas/RedirectInformation'
          minItems: 1
        muteNotif:
          type: boolean
          description: Indicates whether applicat'on's start or stop notification is to be muted.
        trafficSteeringPolIdDl:
          type: string
          description: Reference to a pre-configured traffic steering policy for downlink traffic at
the SMF.
          nullable: true
        trafficSteeringPolIdUl:
          type: string
          description: Reference to a pre-configured traffic steering policy for uplink traffic at
the SMF.
          nullable: true
        routeToLocs:
          type: array
          items:
```

```
            $ref: 'TS29571_CommonData.yaml#/components/schemas/RouteToLocation'
          minItems: 1
          description: A list of location which the traffic shall be routed to for the AF request
          nullable: true
        maxAllowedUpLat:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/UintegerRm'
        easIpReplaceInfos:
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/EasIpReplacementInfo'
          minItems: 1
          description: Contains EAS IP replacement information.
          nullable: true
        traffCorreInd:
          type: boolean
        simConnInd:
          type: boolean
          description: Indicates whether simultaneous connectivity should be temporarily maintained
for the source and target PSA.
        simConnTerm:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DurationSec'
        upPathChgEvent:
          $ref: '#/components/schemas/UpPathChgEvent'
        steerFun:
          $ref: '#/components/schemas/SteeringFunctionality'
        steerModeDl:
          $ref: '#/components/schemas/SteeringMode'
        steerModeUl:
          $ref: '#/components/schemas/SteeringMode'
        mulAccCtrl:
          $ref: '#/components/schemas/MulticastAccessControl'
      required:
        - tcId
      nullable: true
    ChargingData:
      description: Contains charging related parameters.
      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 offline charging is applicable to the PCC rule when it is
included and set to true.
        online:
          type: boolean
          description: Indicates the online charging is applicable to the PCC rule when it is
included and set to true.
        sdfHandl:
          type: boolean
          description: Indicates whether the service data flow is allowed to start while the SMF is
waiting for the response to the credit request.
        ratingGroup:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/RatingGroup'
        reportingLevel:
          $ref: '#/components/schemas/ReportingLevel'
        serviceId:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/ServiceId'
        sponsorId:
          type: string
          description: Indicates the sponsor identity.
        appSvcProvId:
          type: string
          description: Indicates the application service provider identity.
        afChargingIdentifier:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/ChargingId'
        afChargId:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/ApplicationChargingId'
      required:
        - chgId
      nullable: true
    UsageMonitoringData:
      description: Contains usage monitoring related control information.
      type: object
      properties:
```

```
        umId:
          type: string
          description: Univocally identifies the usage monitoring policy data within a PDU session.
        volumeThreshold:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/VolumeRm'
        volumeThresholdUplink:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/VolumeRm'
        volumeThresholdDownlink:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/VolumeRm'
        timeThreshold:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DurationSecRm'
        monitoringTime:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DateTimeRm'
        nextVolThreshold:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/VolumeRm'
        nextVolThresholdUplink:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/VolumeRm'
        nextVolThresholdDownlink:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/VolumeRm'
        nextTimeThreshold:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DurationSecRm'
        inactivityTime:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DurationSecRm'
        exUsagePccRuleIds:
          type: array
          items:
            type: string
          minItems: 1
          description: >
            Contains the PCC rule identifier(s) which corresponding service data flow(s) shall be
            excluded from PDU Session usage monitoring. It is only included in the
            UsageMonitoringData instance for session level usage monitoring.
          nullable: true
      required:
        - umId
      nullable: true
    RedirectInformation:
      description: Contains the redirect information.
      type: object
      properties:
        redirectEnabled:
          type: boolean
          description: Indicates the redirect is enable.
        redirectAddressType:
          $ref: '#/components/schemas/RedirectAddressType'
        redirectServerAddress:
          type: string
          description: >
            Indicates the address of the redirect server. If "redirectAddressType" attribute
            indicates the IPV4_ADDR, the encoding is the same as the Ipv4Addr data type defined in
            3GPP TS 29.571.If "redirectAddressType" attribute indicates the IPV6_ADDR, the encoding
            is the same as the Ipv6Addr data type defined in 3GPP TS 29.571.If "redirectAddressType"
            attribute indicates the URL or SIP_URI, the encoding is the same as the Uri data type
            defined in 3GPP TS 29.571.
    FlowInformation:
      description: Contains the flow information.
      type: object
      properties:
        flowDescription:
          $ref: '#/components/schemas/FlowDescription'
        ethFlowDescription:
          $ref: 'TS29514_Npcf_PolicyAuthorization.yaml#/components/schemas/EthFlowDescription'
        packFiltId:
          type: string
          description: An identifier of packet filter.
        packetFilterUsage:
          type: boolean
          description: The packet shall be sent to the UE.
        tosTrafficClass:
          type: string
          description: Contains the Ipv4 Type-of-Service and mask field or the Ipv6 Traffic-Class
field and mask field.
          nullable: true
        spi:
          type: string
          description: the security parameter index of the IPSec packet.
          nullable: true
        flowLabel:
```

```
          type: string
          description: the Ipv6 flow label header field.
          nullable: true
        flowDirection:
          $ref: '#/components/schemas/FlowDirectionRm'
    SmPolicyDeleteData:
      description: Contains the parameters to be sent to the PCF when an individual SM policy is
deleted.
      type: object
      properties:
        userLocationInfo:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/UserLocation'
        ueTimeZone:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/TimeZone'
        servingNetwork:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/PlmnIdNid'
        userLocationInfoTime:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DateTime'
        ranNasRelCauses:
          type: array
          items:
            $ref: '#/components/schemas/RanNasRelCause'
          minItems: 1
          description: Contains the RAN and/or NAS release cause.
        accuUsageReports:
          type: array
          items:
            $ref: '#/components/schemas/AccuUsageReport'
          minItems: 1
          description: Contains the usage report
        pduSessRelCause:
          $ref: '#/components/schemas/PduSessionRelCause'
        qosMonReports:
          type: array
          items:
            $ref: '#/components/schemas/QosMonitoringReport'
          minItems: 1
    QosCharacteristics:
      description: Contains QoS characteristics for a non-standardized or a non-configured 5QI.
      type: object
      properties:
        5qi:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/5Qi'
        resourceType:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/QosResourceType'
        priorityLevel:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/5QiPriorityLevel'
        packetDelayBudget:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/PacketDelBudget'
        packetErrorRate:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/PacketErrRate'
        averagingWindow:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/AverWindow'
        maxDataBurstVol:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/MaxDataBurstVol'
        extMaxDataBurstVol:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/ExtMaxDataBurstVol'
      required:
        - 5qi
        - resourceType
        - priorityLevel
        - packetDelayBudget
        - packetErrorRate
    ChargingInformation:
      description: Contains the addresses of the charging functions.
      type: object
      properties:
        primaryChfAddress:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
        secondaryChfAddress:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
        primaryChfSetId:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/NfSetId'
        primaryChfInstanceId:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/NfInstanceId'
        secondaryChfSetId:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/NfSetId'
        secondaryChfInstanceId:
```

```
          $ref: 'TS29571_CommonData.yaml#/components/schemas/NfInstanceId'
      required:
        - primaryChfAddress
    AccuUsageReport:
      description: Contains the accumulated usage report information.
      type: object
      properties:
        refUmIds:
          type: string
          description: An id referencing UsageMonitoringData objects associated with this usage
report.
        volUsage:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/Volume'
        volUsageUplink:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/Volume'
        volUsageDownlink:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/Volume'
        timeUsage:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DurationSec'
        nextVolUsage:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/Volume'
        nextVolUsageUplink:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/Volume'
        nextVolUsageDownlink:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/Volume'
        nextTimeUsage:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DurationSec'
      required:
        - refUmIds
    SmPolicyUpdateContextData:
      description: Contains the policy control request trigger(s) that were met and the
corresponding new value(s) or the error report of the policy enforcement.
      type: object
      properties:
        repPolicyCtrlReqTriggers:
          type: array
          items:
            $ref: '#/components/schemas/PolicyControlRequestTrigger'
          minItems: 1
          description: The policy control reqeust trigges which are met.
        accNetChIds:
          type: array
          items:
            $ref: '#/components/schemas/AccNetChId'
          minItems: 1
          description: Indicates the access network charging identifier for the PCC rule(s) or whole
PDU session.
        accessType:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/AccessType'
        ratType:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/RatType'
        addAccessInfo:
          $ref: '#/components/schemas/AdditionalAccessInfo'
        relAccessInfo:
          $ref: '#/components/schemas/AdditionalAccessInfo'
        servingNetwork:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/PlmnIdNid'
        userLocationInfo:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/UserLocation'
        ueTimeZone:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/TimeZone'
        relIpv4Address:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv4Addr'
        ipv4Address:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv4Addr'
        ipDomain:
          type: string
          description: Indicates the IPv4 address domain
        ipv6AddressPrefix:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv6Prefix'
        relIpv6AddressPrefix:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv6Prefix'
        addIpv6AddrPrefixes:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv6Prefix'
        addRelIpv6AddrPrefixes:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv6Prefix'
        relUeMac:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/MacAddr48'
```

```
        ueMac:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/MacAddr48'
        subsSessAmbr:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ambr'
        authProfIndex:
          type: string
          description: Indicates the DN-AAA authorization profile index
        subsDefQos:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/SubscribedDefaultQos'
        vplmnQos:
          $ref: 'TS29502_Nsmf_PDUSession.yaml#/components/schemas/VplmnQos'
        vplmnQosNotApp:
          type: boolean
          description: If it is included and set to true, indicates that the QoS constraints in the
VPLMN are not applicable.
        numOfPackFilter:
          type: integer
          description: Contains the number of supported packet filter for signalled QoS rules.
        accuUsageReports:
          type: array
          items:
            $ref: '#/components/schemas/AccuUsageReport'
          minItems: 1
          description: Contains the usage report
        3gppPsDataOffStatus:
          type: boolean
          description: If it is included and set to true, the 3GPP PS Data Off is activated by the
UE.
        appDetectionInfos:
          type: array
          items:
            $ref: '#/components/schemas/AppDetectionInfo'
          minItems: 1
          description: Report the start/stop of the application traffic and detected SDF
descriptions if applicable.
        ruleReports:
          type: array
          items:
            $ref: '#/components/schemas/RuleReport'
          minItems: 1
          description: Used to report the PCC rule failure.
        sessRuleReports:
          type: array
          items:
            $ref: '#/components/schemas/SessionRuleReport'
          minItems: 1
          description: Used to report the session rule failure.
        qncReports:
          type: array
          items:
            $ref: '#/components/schemas/QosNotificationControlInfo'
          minItems: 1
          description: QoS Notification Control information.
        qosMonReports:
          type: array
          items:
            $ref: '#/components/schemas/QosMonitoringReport'
          minItems: 1
        userLocationInfoTime:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DateTime'
        repPraInfos:
          type: object
          additionalProperties:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/PresenceInfo'
          minProperties: 1
          description: >
            Reports the changes of presence reporting area. The praId attribute within the
            PresenceInfo data type is the key of the map.
        ueInitResReq:
          $ref: '#/components/schemas/UeInitiatedResourceRequest'
        refQosIndication:
          type: boolean
          description: >
            If it is included and set to true, the reflective QoS is supported by the UE. If it is
            included and set to false, the reflective QoS is revoked by the UE.
        qosFlowUsage:
          $ref: '#/components/schemas/QosFlowUsage'
        creditManageStatus:
```

```
          $ref: '#/components/schemas/CreditManagementStatus'
        servNfId:
          $ref: '#/components/schemas/ServingNfIdentity'
        traceReq:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/TraceData'
        maPduInd:
          $ref: '#/components/schemas/MaPduIndication'
        atsssCapab:
          $ref: '#/components/schemas/AtsssCapability'
        tsnBridgeInfo:
          $ref: '#/components/schemas/TsnBridgeInfo'
        tsnBridgeManCont:
          $ref: '#/components/schemas/BridgeManagementContainer'
        tsnPortManContDstt:
          $ref: '#/components/schemas/PortManagementContainer'
        tsnPortManContNwtts:
          type: array
          items:
            $ref: '#/components/schemas/PortManagementContainer'
          minItems: 1
        mulAddrInfos:
          type: array
          items:
            $ref: '#/components/schemas/IpMulticastAddressInfo'
          minItems: 1
        policyDecFailureReports:
          type: array
          items:
            $ref: '#/components/schemas/PolicyDecisionFailureCode'
          minItems: 1
          description: Contains the type(s) of failed policy decision and/or condition data.
        invalidPolicyDecs:
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/InvalidParam'
          minItems: 1
          description: Indicates the invalid parameters for the reported type(s) of the failed
policy decision and/or condition data.
        trafficDescriptors:
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/DddTrafficDescriptor'
          minItems: 1
        pccRuleId:
          type: string
          description: Contains the identifier of the PCC rule which is used for traffic detection
of event.
        typesOfNotif:
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/DlDataDeliveryStatus'
          minItems: 1
        interGrpIds:
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/GroupId'
          minItems: 1
        satBackhaulCategory:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/SatelliteBackhaulCategory'
        pcfUeInfo:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/PcfUeCallbackInfo'
        nwdafDatas:
          type: array
          items:
            $ref: '#/components/schemas/NwdafData'
          minItems: 1
          nullable: true
        anGwStatus:
          type: boolean
          description: >
            When it is included and set to true, it indicates that the AN-Gateway has failed and
            that the PCF should refrain from sending policy decisions to the SMF until it is
            informed that the AN-Gateway has been recovered.
    UpPathChgEvent:
      description: Contains the UP path change event subscription from the AF.
      type: object
      properties:
        notificationUri:
```

```
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
        notifCorreId:
          type: string
          description: It is used to set the value of Notification Correlation ID in the
notification sent by the SMF.
        dnaiChgType:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DnaiChangeType'
        afAckInd:
          type: boolean
      required:
        - notificationUri
        - notifCorreId
        - dnaiChgType
      nullable: true
    TerminationNotification:
      description: Represents a Termination Notification.
      type: object
      properties:
        resourceUri:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
        cause:
          $ref: '#/components/schemas/SmPolicyAssociationReleaseCause'
      required:
        - resourceUri
        - cause
    AppDetectionInfo:
      description: Contains the detected application's traffic information.
      type: object
      properties:
        appId:
          type: string
          description: A reference to the application detection filter configured at the UPF
        instanceId:
          type: string
          description: >
            Identifier sent by the SMF in order to allow correlation of application Start and Stop
            events to the specific service data flow description, if service data flow descriptions
            are deducible.
        sdfDescriptions:
          type: array
          items:
            $ref: '#/components/schemas/FlowInformation'
          minItems: 1
          description: Contains the detected service data flow descriptions if they are deducible.
      required:
        - appId
    AccNetChId:
      description: Contains the access network charging identifier for the PCC rule(s) or for the
whole PDU session.
      type: object
      properties:
        accNetChaIdValue:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/ChargingId'
        accNetChargId:
          type: string
          description: A character string containing the access network charging id.
        refPccRuleIds:
          type: array
          items:
            type: string
          minItems: 1
          description: Contains the identifier of the PCC rule(s) associated to the provided Access
Network Charging Identifier.
        sessionChScope:
          type: boolean
          description: When it is included and set to true, indicates the Access Network Charging
Identifier applies to the whole PDU Session
      oneOf:
        - required: [accNetChaIdValue]
        - required: [accNetChargId]
    AccNetChargingAddress:
      description: Describes the network entity within the access network performing charging
      type: object
      anyOf:
        - required: [anChargIpv4Addr]
        - required: [anChargIpv6Addr]
      properties:
        anChargIpv4Addr:
```

```
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv4Addr'
        anChargIpv6Addr:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv6Addr'
    RequestedRuleData:
      description: Contains rule data requested by the PCF to receive information associated with
PCC rule(s).
      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:
      description: Contains usage data requested by the PCF requesting usage reports for the
corresponding usage monitoring data instances.
      type: object
      properties:
        refUmIds:
          type: array
          items:
            type: string
          minItems: 1
          description: >
            An array of usage monitoring data id references to the usage monitoring data instances
            for which the PCF is requesting a usage report. This attribute shall only be provided
            when allUmIds is not set to true.
        allUmIds:
          type: boolean
          description: >
            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.
    UeCampingRep:
      description: Contains the current applicable values corresponding to the policy control
request triggers.
      type: object
      properties:
        accessType:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/AccessType'
        ratType:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/RatType'
        servNfId:
          $ref: '#/components/schemas/ServingNfIdentity'
        servingNetwork:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/PlmnIdNid'
        userLocationInfo:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/UserLocation'
        ueTimeZone:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/TimeZone'
        netLocAccSupp:
          $ref: '#/components/schemas/NetLocAccessSupport'
    RuleReport:
      description: Reports the status of PCC.
      type: object
      properties:
        pccRuleIds:
          type: array
          items:
            type: string
          minItems: 1
          description: Contains the identifier of the affected PCC rule(s).
        ruleStatus:
          $ref: '#/components/schemas/RuleStatus'
        contVers:
          type: array
```

```
          items:
            $ref: 'TS29514_Npcf_PolicyAuthorization.yaml#/components/schemas/ContentVersion'
          minItems: 1
          description: Indicates the version of a PCC rule.
        failureCode:
          $ref: '#/components/schemas/FailureCode'
        finUnitAct:
          $ref: 'TS32291_Nchf_ConvergedCharging.yaml#/components/schemas/FinalUnitAction'
        ranNasRelCauses:
          type: array
          items:
            $ref: '#/components/schemas/RanNasRelCause'
          minItems: 1
          description: indicates the RAN or NAS release cause code information.
        altQosParamId:
          type: string
      required:
        - pccRuleIds
        - ruleStatus
    RanNasRelCause:
      description: Contains the RAN/NAS release cause.
      type: object
      properties:
        ngApCause:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/NgApCause'
        5gMmCause:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/5GMmCause'
        5gSmCause:
          $ref: '#/components/schemas/5GSmCause'
        epsCause:
          $ref: '#/components/schemas/EpsRanNasRelCause'
    UeInitiatedResourceRequest:
      description: Indicates that a UE requests specific QoS handling for the selected SDF.
      type: object
      properties:
        pccRuleId:
          type: string
        ruleOp:
          $ref: '#/components/schemas/RuleOperation'
        precedence:
          type: integer
        packFiltInfo:
          type: array
          items:
            $ref: '#/components/schemas/PacketFilterInfo'
          minItems: 1
        reqQos:
          $ref: '#/components/schemas/RequestedQos'
      required:
        - ruleOp
        - packFiltInfo
    PacketFilterInfo:
      description: Contains the information from a single packet filter sent from the SMF to the
PCF.
      type: object
      properties:
        packFiltId:
          type: string
          description: An identifier of packet filter.
        packFiltCont:
          $ref: '#/components/schemas/PacketFilterContent'
        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'
    RequestedQos:
      description: Contains the QoS information requested by the UE.
      type: object
      properties:
        5qi:
```

```
          $ref: 'TS29571_CommonData.yaml#/components/schemas/5Qi'
        gbrUl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'
        gbrDl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'
      required:
        - 5qi
    QosNotificationControlInfo:
      description: Contains the QoS Notification Control Information.
      type: object
      properties:
        refPccRuleIds:
          type: array
          items:
            type: string
          minItems: 1
          description: An array of PCC rule id references to the PCC rules associated with the QoS
notification control info.
        notifType:
          $ref: 'TS29514_Npcf_PolicyAuthorization.yaml#/components/schemas/QosNotifType'
        contVer:
          $ref: 'TS29514_Npcf_PolicyAuthorization.yaml#/components/schemas/ContentVersion'
        altQosParamId:
          type: string
      required:
        - refPccRuleIds
        - notifType
    PartialSuccessReport:
      description: Includes the information reported by the SMF when some of the PCC rules and/or
session rules are not successfully installed/activated.
      type: object
      properties:
        failureCause:
          $ref: '#/components/schemas/FailureCause'
        ruleReports:
          type: array
          items:
            $ref: '#/components/schemas/RuleReport'
          minItems: 1
          description: Information about the PCC rules provisioned by the PCF not successfully
installed/activated.
        sessRuleReports:
          type: array
          items:
            $ref: '#/components/schemas/SessionRuleReport'
          minItems: 1
          description: Information about the session rules provisioned by the PCF not successfully
installed.
        ueCampingRep:
          $ref: '#/components/schemas/UeCampingRep'
        policyDecFailureReports:
          type: array
          items:
            $ref: '#/components/schemas/PolicyDecisionFailureCode'
          minItems: 1
          description: Contains the type(s) of failed policy decision and/or condition data.
        invalidPolicyDecs:
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/InvalidParam'
          minItems: 1
          description: Indicates the invalid parameters for the reported type(s) of the failed
policy decision and/or condition data.
      required:
        - failureCause
    AuthorizedDefaultQos:
      description: Represents the Authorized Default QoS.
      type: object
      properties:
        5qi:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/5Qi'
        arp:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Arp'
        priorityLevel:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/5QiPriorityLevelRm'
        averWindow:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/AverWindowRm'
        maxDataBurstVol:
```

```
          $ref: 'TS29571_CommonData.yaml#/components/schemas/MaxDataBurstVolRm'
        maxbrUl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRateRm'
        maxbrDl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRateRm'
        gbrUl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRateRm'
        gbrDl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRateRm'
        extMaxDataBurstVol:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/ExtMaxDataBurstVolRm'
    ErrorReport:
      description: Contains the rule error reports.
      type: object
      properties:
        error:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/ProblemDetails'
        ruleReports:
          type: array
          items:
            $ref: '#/components/schemas/RuleReport'
          minItems: 1
          description: Used to report the PCC rule failure.
        sessRuleReports:
          type: array
          items:
            $ref: '#/components/schemas/SessionRuleReport'
          minItems: 1
          description: Used to report the session rule failure.
        polDecFailureReports:
          type: array
          items:
            $ref: '#/components/schemas/PolicyDecisionFailureCode'
          minItems: 1
          description: Used to report failure of the policy decision and/or condition data.
        invalidPolicyDecs:
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/InvalidParam'
          minItems: 1
          description: Indicates the invalid parameters for the reported type(s) of the failed
policy decision and/or condition data.
    SessionRuleReport:
      description: Represents reporting of the status of a session rule.
      type: object
      properties:
        ruleIds:
          type: array
          items:
            type: string
          minItems: 1
          description: Contains the identifier of the affected session rule(s).
        ruleStatus:
          $ref: '#/components/schemas/RuleStatus'
        sessRuleFailureCode:
          $ref: '#/components/schemas/SessionRuleFailureCode'
        policyDecFailureReports:
          type: array
          items:
            $ref: '#/components/schemas/PolicyDecisionFailureCode'
          minItems: 1
          description: Contains the type(s) of failed policy decision and/or condition data.
      required:
        - ruleIds
        - ruleStatus
    ServingNfIdentity:
      description: Contains the serving Network Function identity.
      type: object
      properties:
        servNfInstId:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/NfInstanceId'
        guami:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Guami'
        anGwAddr:
          $ref: 'TS29514_Npcf_PolicyAuthorization.yaml#/components/schemas/AnGwAddress'
        sgsnAddr:
          $ref: '#/components/schemas/SgsnAddress'
    SteeringMode:
```

```
      description: Contains the steering mode value and parameters determined by the PCF.
      type: object
      properties:
        steerModeValue:
          $ref: '#/components/schemas/SteerModeValue'
        active:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/AccessType'
        standby:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/AccessTypeRm'
        3gLoad:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uinteger'
        prioAcc:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/AccessType'
        thresValue:
          $ref: '#/components/schemas/ThresholdValue'
        steerModeInd:
          $ref: '#/components/schemas/SteerModeIndicator'
      required:
        - steerModeValue
    AdditionalAccessInfo:
      description: Indicates the combination of additional Access Type and RAT Type for a MA PDU
session.
      type: object
      properties:
        accessType:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/AccessType'
        ratType:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/RatType'
      required:
        - accessType
    QosMonitoringData:
      description: Contains QoS monitoring related control information.
      type: object
      properties:
        qmId:
          type: string
          description: Univocally identifies the QoS monitoring policy data within a PDU session.
        reqQosMonParams:
          type: array
          items:
            $ref: '#/components/schemas/RequestedQosMonitoringParameter'
          minItems: 1
          description: >
            indicates the UL packet delay, DL packet delay and/or round trip packet delay between
            the UE and the UPF is to be monitored when the QoS Monitoring for URLLC is enabled for
            the service data flow.
        repFreqs:
          type: array
          items:
             $ref: '#/components/schemas/ReportingFrequency'
          minItems: 1
        repThreshDl:
          type: integer
          description: Indicates the period of time in units of miliiseconds for DL packet delay.
          nullable: true
        repThreshUl:
          type: integer
          description: Indicates the period of time in units of miliiseconds for UL packet delay.
          nullable: true
        repThreshRp:
          type: integer
          description: Indicates the period of time in units of miliiseconds for round trip packet
delay.
          nullable: true
        waitTime:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DurationSecRm'
        repPeriod:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DurationSecRm'
        notifyUri:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/UriRm'
        notifyCorreId:
          type: string
          nullable: true
        directNotifInd:
          type: boolean
          description: Indicates that the direct event notification sent by UPF to the Local NEF or
AF is requested if it is included and set to true.
      required:
```

```
        - qmId
        - reqQosMonParams
        - repFreqs
      nullable: true
    QosMonitoringReport:
      description: Contains reporting information on QoS monitoring.
      type: object
      properties:
        refPccRuleIds:
          type: array
          items:
            type: string
          minItems: 1
          description: An array of PCC rule id references to the PCC rules associated with the QoS
monitoring report.
        ulDelays:
          type: array
          items:
            type: integer
          minItems: 1
        dlDelays:
          type: array
          items:
            type: integer
          minItems: 1
        rtDelays:
          type: array
          items:
            type: integer
          minItems: 1
      required:
        - refPccRuleIds
#
    TsnBridgeInfo:
      description: Contains parameters that describe and identify the TSC user plane node.
      type: object
      properties:
        bridgeId:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uint64'
        dsttAddr:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/MacAddr48'
        dsttPortNum:
          $ref: '#/components/schemas/TsnPortNumber'
        dsttResidTime:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uinteger'
#
    PortManagementContainer:
      description: Contains the port management information container for a port.
      type: object
      properties:
        portManCont:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Bytes'
        portNum:
          $ref: '#/components/schemas/TsnPortNumber'
      required:
        - portManCont
        - portNum
    BridgeManagementContainer:
      description: Contains the UMIC.
      type: object
      properties:
        bridgeManCont:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Bytes'
      required:
        - bridgeManCont
    IpMulticastAddressInfo:
      description: Contains the IP multicast addressing information.
      type: object
      properties:
        srcIpv4Addr:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv4Addr'
        ipv4MulAddr:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv4Addr'
        srcIpv6Addr:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv6Addr'
        ipv6MulAddr:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv6Addr'
    DownlinkDataNotificationControl:
```

```
      description: Contains the downlink data notification control information.
      type: object
      properties:
        notifCtrlInds:
          type: array
          items:
            $ref: '#/components/schemas/NotificationControlIndication'
          minItems: 1
        typesOfNotif:
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/DlDataDeliveryStatus'
          minItems: 1
    DownlinkDataNotificationControlRm:
      description: This data type is defined in the same way as the DownlinkDataNotificationControl
data type, but with the nullable:true property.
      type: object
      properties:
        notifCtrlInds:
          type: array
          items:
            $ref: '#/components/schemas/NotificationControlIndication'
          minItems: 1
          nullable: true
        typesOfNotif:
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/DlDataDeliveryStatus'
          minItems: 1
          nullable: true
      nullable: true
    ThresholdValue:
      description: Indicates the threshold value(s) for RTT and/or Packet Loss Rate.
      type: object
      properties:
        rttThres:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/UintegerRm'
        plrThres:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/PacketLossRateRm'
      nullable: true
    NwdafData:
      description: Indicates the list of Analytic ID(s) per NWDAF instance ID used for the PDU
Session consumed by the SMF.
      type: object
      properties:
        nwdafInstanceId:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/NfInstanceId'
        nwdafEvents:
          type: array
          items:
            $ref: 'TS29520_Nnwdaf_EventsSubscription.yaml#/components/schemas/NwdafEvent'
          minItems: 1
      required:
        - nwdafInstanceId
    5GSmCause:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/Uinteger'
    EpsRanNasRelCause:
      type: string
      description: Defines the EPS RAN/NAS release cause.
    PacketFilterContent:
      type: string
      description: Defines a packet filter for an IP flow.
    FlowDescription:
      type: string
      description: Defines a packet filter for an IP flow.
    TsnPortNumber:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/Uinteger'
    ApplicationDescriptor:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/Bytes'
    FlowDirection:
      anyOf:
      - type: string
        enum:
          - DOWNLINK
          - UPLINK
          - BIDIRECTIONAL
          - UNSPECIFIED
      - type: string
```

```
        description: >
          This string provides forward-compatibility with future
          extensions to the enumeration but is not used to encode
          content defined in the present version of this API.
      description: |
        Possible values are
        - DOWNLINK: The corresponding filter applies for traffic to the UE.
        - UPLINK: The corresponding filter applies for traffic from the UE.
        - BIDIRECTIONAL: The corresponding filter applies for traffic both to and from the UE.
        - UNSPECIFIED: The corresponding filter applies for traffic to the UE (downlink), but has no
specific direction declared. The service data flow detection shall apply the filter for uplink
traffic as if the filter was bidirectional. The PCF shall not use the value UNSPECIFIED in filters
created by the network in NW-initiated procedures. The PCF shall only include the value UNSPECIFIED
in filters in UE-initiated procedures if the same value is received from the SMF.
    FlowDirectionRm:
      description: This data type is defined in the same way as the "FlowDirection" data type, with
the only difference that it allows null value.
      anyOf:
        - $ref: '#/components/schemas/FlowDirection'
        - $ref: 'TS29571_CommonData.yaml#/components/schemas/NullValue'
    ReportingLevel:
      anyOf:
      - type: string
        enum:
          - SER_ID_LEVEL
          - RAT_GR_LEVEL
          - SPON_CON_LEVEL
      - $ref: 'TS29571_CommonData.yaml#/components/schemas/NullValue'
      - 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
      - $ref: 'TS29571_CommonData.yaml#/components/schemas/NullValue'
      - type: string
        description: >
          This string provides forward-compatibility with future
          extensions to the enumeration but is not used to encode
          content defined in the present version of this API.
      description: |
        Possible values are
        - DURATION: Indicates that the duration of the service data flow traffic shall be metered.
        - VOLUME: Indicates that volume of the service data flow traffic shall be metered.
        - DURATION_VOLUME: Indicates that the duration and the volume of the service data flow
traffic shall be metered.
        - EVENT: Indicates that events of the service data flow traffic shall be metered.
    PolicyControlRequestTrigger:
      anyOf:
      - type: string
        enum:
          - PLMN_CH
          - RES_MO_RE
          - AC_TY_CH
          - UE_IP_CH
          - UE_MAC_CH
          - AN_CH_COR
          - US_RE
          - APP_STA
          - APP_STO
          - AN_INFO
          - CM_SES_FAIL
          - PS_DA_OFF
          - DEF_QOS_CH
```

```
          - SE_AMBR_CH
          - QOS_NOTIF
          - NO_CREDIT
          - REALLO_OF_CREDIT
          - PRA_CH
          - SAREA_CH
          - SCNN_CH
          - RE_TIMEOUT
          - RES_RELEASE
          - SUCC_RES_ALLO
          - RAI_CH
          - RAT_TY_CH
          - REF_QOS_IND_CH
          - NUM_OF_PACKET_FILTER
          - UE_STATUS_RESUME
          - UE_TZ_CH
          - AUTH_PROF_CH
          - QOS_MONITORING
          - SCELL_CH
          - USER_LOCATION_CH
          - EPS_FALLBACK
          - MA_PDU
          - TSN_BRIDGE_INFO
          - 5G_RG_JOIN
          - 5G_RG_LEAVE
          - DDN_FAILURE
          - DDN_DELIVERY_STATUS
          - GROUP_ID_LIST_CHG
          - DDN_FAILURE_CANCELLATION
          - DDN_DELIVERY_STATUS_CANCELLATION
          - VPLMN_QOS_CH
          - SUCC_QOS_UPDATE
          - SAT_CATEGORY_CHG
          - PCF_UE_NOTIF_IND
          - NWDAF_DATA_CHG
      - type: string
        description: >
          This string provides forward-compatibility with future
          extensions to the enumeration but is not used to encode
          content defined in the present version of this API.
      description: |
        Possible values are
        - PLMN_CH: PLMN Change
        - RES_MO_RE: A request for resource modification has been received by the SMF. The SMF
always reports to the PCF.
        - AC_TY_CH: Access Type Change
        - UE_IP_CH: UE IP address change. The SMF always reports to the PCF.
        - UE_MAC_CH: A new UE MAC address is detected or a used UE MAC address is inactive for a
specific period
        - AN_CH_COR: Access Network Charging Correlation Information
        - US_RE: The PDU Session or the Monitoring key specific resources consumed by a UE either
reached the threshold or needs to be reported for other reasons.
        - APP_STA: The start of application traffic has been detected.
        - APP_STO: The stop of application traffic has been detected.
        - AN_INFO: Access Network Information report
        - CM_SES_FAIL: Credit management session failure
        - PS_DA_OFF: The SMF reports when the 3GPP PS Data Off status changes. The SMF always
reports to the PCF.
        - DEF_QOS_CH: Default QoS Change. The SMF always reports to the PCF.
        - SE_AMBR_CH: Session-AMBR Change. The SMF always reports to the PCF.
        - QOS_NOTIF: The SMF notify the PCF when receiving notification from RAN that QoS targets of
the QoS Flow cannot be guranteed or gurateed again.
        - NO_CREDIT: Out of credit
        - REALLO_OF_CREDIT: Reallocation of credit
        - PRA_CH: Change of UE presence in Presence Reporting Area
        - SAREA_CH: Location Change with respect to the Serving Area
        - SCNN_CH: Location Change with respect to the Serving CN node
        - RE_TIMEOUT: Indicates the SMF generated the request because there has been a PCC
revalidation timeout
        - RES_RELEASE: Indicate that the SMF can inform the PCF of the outcome of the release of
resources for those rules that require so.
        - SUCC_RES_ALLO: Indicates that the requested rule data is the successful resource
allocation.
        - RAI_CH: Location Change with respect to the RAI of GERAN and UTRAN.
        - RAT_TY_CH: RAT Type Change.
        - REF_QOS_IND_CH: Reflective QoS indication Change
        - NUM_OF_PACKET_FILTER: Indicates that the SMF shall report the number of supported packet
filter for signalled QoS rules
```

```
        - UE_STATUS_RESUME: Indicates that the UE's status is resumed.
        - UE_TZ_CH: UE Time Zone Change
        - AUTH_PROF_CH: The DN-AAA authorization profile index has changed
        - QOS_MONITORING: Indicate that the SMF notifies the PCF of the QoS Monitoring information.
        - SCELL_CH: Location Change with respect to the Serving Cell.
        - USER_LOCATION_CH: Indicate that user location has been changed, applicable to serving area
change and serving cell change.
        - EPS_FALLBACK: EPS Fallback report is enabled in the SMF.
        - MA_PDU: UE Indicates that the SMF notifies the PCF of the MA PDU session request
        - TSN_BRIDGE_INFO: TSC user plane node information available
        - 5G_RG_JOIN: The 5G-RG has joined to an IP Multicast Group.
        - 5G_RG_LEAVE: The 5G-RG has left an IP Multicast Group.
        - DDN_FAILURE: Event subscription for DDN Failure event received.
        - DDN_DELIVERY_STATUS: Event subscription for DDN Delivery Status received.
        - GROUP_ID_LIST_CHG: UE Internal Group Identifier(s) has changed: the SMF reports that UDM
provided list of group Ids has changed.
        - DDN_FAILURE_CANCELLATION: The event subscription for DDN Failure event is cancelled.
        - DDN_DELIVERY_STATUS_CANCELLATION: The event subscription for DDD STATUS is cancelled.
        - VPLMN_QOS_CH: Change of the QoS supported in the VPLMN.
        - SUCC_QOS_UPDATE: Indicates that the requested MPS Action is successful.
        - SAT_CATEGORY_CHG: Indicates that the SMF has detected a change between different satellite
backhaul categories, or between a satellite backhaul and a non-satellite backhaul.
        - PCF_UE_NOTIF_IND: Indicates the SMF has detected the AMF forwarded the PCF for the UE
indication to receive/stop receiving notifications of SM Policy association established/terminated
events.
        - NWDAF_DATA_CHG: Indicates that the NWDAF instance IDs used for the PDU session and/or
associated Analytics IDs used for the PDU session and available in the SMF have changed.
    RequestedRuleDataType:
      anyOf:
      - type: string
        enum:
          - CH_ID
          - MS_TIME_ZONE
          - USER_LOC_INFO
          - RES_RELEASE
          - SUCC_RES_ALLO
          - EPS_FALLBACK
      - type: string
        description: >
          This string provides forward-compatibility with future
          extensions to the enumeration but is not used to encode
          content defined in the present version of this API.
      description: |
        Possible values are
        - CH_ID: Indicates that the requested rule data is the charging identifier.
        - MS_TIME_ZONE: Indicates that the requested access network info type is the UE's timezone.
        - USER_LOC_INFO: Indicates that the requested access network info type is the UE's location.
        - RES_RELEASE: Indicates that the requested rule data is the result of the release of
resource.
        - SUCC_RES_ALLO: Indicates that the requested rule data is the successful resource
allocation.
        - EPS_FALLBACK: Indicates that the requested rule data is the report of QoS flow rejection
due to EPS fallback.
    RuleStatus:
      anyOf:
      - type: string
        enum:
          - ACTIVE
          - INACTIVE
      - type: string
        description: >
          This string provides forward-compatibility with future
          extensions to the enumeration but is not used to encode
          content defined in the present version of this API.
      description: |
        Possible values are
        - ACTIVE: Indicates that the PCC rule(s) are successfully installed (for those provisioned
from PCF) or activated (for those pre-defined in SMF), or the session rule(s) are successfully
installed
        - INACTIVE: Indicates that the PCC rule(s) are removed (for those provisioned from PCF) or
inactive (for those pre-defined in SMF) or the session rule(s) are removed.
    FailureCode:
      anyOf:
      - type: string
        enum:
          - UNK_RULE_ID
          - RA_GR_ERR
          - SER_ID_ERR
```

```
          - NF_MAL
          - RES_LIM
          - MAX_NR_QoS_FLOW
          - MISS_FLOW_INFO
          - RES_ALLO_FAIL
          - UNSUCC_QOS_VAL
          - INCOR_FLOW_INFO
          - PS_TO_CS_HAN
          - APP_ID_ERR
          - NO_QOS_FLOW_BOUND
          - FILTER_RES
          - MISS_REDI_SER_ADDR
          - CM_END_USER_SER_DENIED
          - CM_CREDIT_CON_NOT_APP
          - CM_AUTH_REJ
          - CM_USER_UNK
          - CM_RAT_FAILED
          - UE_STA_SUSP
          - UNKNOWN_REF_ID
          - INCORRECT_COND_DATA
          - REF_ID_COLLISION
          - TRAFFIC_STEERING_ERROR
          - DNAI_STEERING_ERROR
          - AN_GW_FAILE
          - MAX_NR_PACKET_FILTERS_EXCEEDED
      - type: string
        description: >
          This string provides forward-compatibility with future
          extensions to the enumeration but is not used to encode
          content defined in the present version of this API.
      description: |
        Possible values are
        - UNK_RULE_ID: Indicates that the pre-provisioned PCC rule could not be successfully
activated because the PCC rule identifier is unknown to the SMF.
        - RA_GR_ERR: Indicate that the PCC rule could not be successfully installed or enforced
because the Rating Group specified within the Charging Data policy decision which the PCC rule
refers to is unknown or, invalid.
        - SER_ID_ERR: Indicate that the PCC rule could not be successfully installed or enforced
because the Service Identifier specified within the Charging Data policy decision which the PCC rule
refers to is invalid, unknown, or not applicable to the service being charged.
        - NF_MAL: Indicate that the PCC rule could not be successfully installed (for those
provisioned from the PCF) or activated (for those pre-defined in SMF) or enforced (for those already
successfully installed) due to SMF/UPF malfunction.
        - RES_LIM: Indicate that the PCC rule could not be successfully installed (for those
provisioned from PCF) or activated (for those pre-defined in SMF) or enforced (for those already
successfully installed) due to a limitation of resources at the SMF/UPF.
        - MAX_NR_QoS_FLOW: Indicate that the PCC rule could not be successfully installed (for those
provisioned from PCF) or activated (for those pre-defined in SMF) or enforced (for those already
successfully installed) due to the fact that the maximum number of QoS flows has been reached for
the PDU session.
        - MISS_FLOW_INFO: Indicate that the PCC rule could not be successfully installed or enforced
because neither the "flowInfos" attribute nor the "appId" attribute is specified within the PccRule
data structure by the PCF during the first install request of the PCC rule.
        - RES_ALLO_FAIL: Indicate that the PCC rule could not be successfully installed or
maintained since the QoS flow establishment/modification failed, or the QoS flow was released.
        - UNSUCC_QOS_VAL: indicate that the QoS validation has failed or when Guaranteed Bandwidth >
Max-Requested-Bandwidth.
        - INCOR_FLOW_INFO: Indicate that the PCC rule could not be successfully installed or
modified at the SMF because the provided flow information is not supported by the network (e.g. the
provided IP address(es) or Ipv6 prefix(es) do not correspond to an IP version applicable for the PDU
session).
        - PS_TO_CS_HAN: Indicate that the PCC rule could not be maintained because of PS to CS
handover.
        - APP_ID_ERR: Indicate that the rule could not be successfully installed or enforced because
the Application Identifier is invalid, unknown, or not applicable to the application required for
detection.
        - NO_QOS_FLOW_BOUND: Indicate that there is no QoS flow which the SMF can bind the PCC
rule(s) to.
        - FILTER_RES: Indicate that the Flow Information within the "flowInfos" attribute cannot be
handled by the SMF because any of the restrictions defined in clause 5.4.2 of 3GPP TS 29.212 was not
met.
        - MISS_REDI_SER_ADDR: Indicate that the PCC rule could not be successfully installed or
enforced at the SMF because there is no valid Redirect Server Address within the Traffic Control
Data policy decision which the PCC rule refers to provided by the PCF and no preconfigured
redirection address for this PCC rule at the SMF.
        - CM_END_USER_SER_DENIED: Indicate that the charging system denied the service request due
to service restrictions (e.g. terminate rating group) or limitations related to the end-user, for
example the end-user's account could not cover the requested service.
```

```
        - CM_CREDIT_CON_NOT_APP: Indicate that the charging system determined that the service can
be granted to the end user but no further credit control is needed for the service (e.g. service is
free of charge or is treated for offline charging).
          - CM_AUTH_REJ: Indicate that the charging system denied the service request in order to
terminate the service for which credit is requested.
        - CM_USER_UNK: Indicate that the specified end user could not be found in the charging
system.
        - CM_RAT_FAILED: Indicate that the charging system cannot rate the service request due to
insufficient rating input, incorrect AVP combination or due to an attribute or an attribute value
that is not recognized or supported in the rating.
        - UE_STA_SUSP: Indicates that the UE is in suspend state.
        - UNKNOWN_REF_ID: Indicates that the PCC rule could not be successfully installed/modified
because the referenced identifier to a Policy Decision Data or to a Condition Data is unknown to the
SMF.
        - INCORRECT_COND_DATA: Indicates that the PCC rule could not be successfully
installed/modified because the referenced Condition data are incorrect.
        - REF_ID_COLLISION: Indicates that PCC rule could not be successfully installed/modified
because the same Policy Decision is referenced by a session rule (e.g. the session rule and the PCC
rule refer to the same Usage Monitoring decision data).
        - TRAFFIC_STEERING_ERROR: Indicates that enforcement of the steering of traffic to the N6-
LAN or 5G-LAN failed; or the dynamic PCC rule could not be successfully installed or modified at the
NF service consumer because there are invalid traffic steering policy identifier(s) within the
provided Traffic Control Data policy decision to which the PCC rule refers.
        - DNAI_STEERING_ERROR: Indicates that the enforcement of the steering of traffic to the
indicated DNAI failed; or the dynamic PCC rule could not be successfully installed or modified at
the NF service consumer because there is invalid route information for a DNAI(s) (e.g. routing
profile id is not configured) within the provided Traffic Control Data policy decision to which the
PCC rule refers.
        - AN_GW_FAILED: This value is used to indicate that the AN-Gateway has failed and that the
PCF should refrain from sending policy decisions to the SMF until it is informed that the S-GW has
been recovered. This value shall not be used if the SM Policy association modification procedure is
initiated for PCC rule removal only.
    AfSigProtocol:
      anyOf:
      - type: string
        enum:
          - NO_INFORMATION
          - SIP
      - $ref: 'TS29571_CommonData.yaml#/components/schemas/NullValue'
      - type: string
        description: >
          This string provides forward-compatibility with future
          extensions to the enumeration but is not used to encode
          content defined in the present version of this API.
      description: |
        Possible values are
        - NO_INFORMATION: Indicate that no information about the AF signalling protocol is being
provided.
        - SIP: Indicate that the signalling protocol is Session Initiation Protocol.
    RuleOperation:
      anyOf:
      - type: string
        enum:
          - CREATE_PCC_RULE
          - DELETE_PCC_RULE
          - MODIFY_PCC_RULE_AND_ADD_PACKET_FILTERS
          - MODIFY_ PCC_RULE_AND_REPLACE_PACKET_FILTERS
          - MODIFY_ PCC_RULE_AND_DELETE_PACKET_FILTERS
          - MODIFY_PCC_RULE_WITHOUT_MODIFY_PACKET_FILTERS
      - 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
        - CREATE_PCC_RULE: Indicates to create a new PCC rule to reserve the resource requested by
the UE.
        - DELETE_PCC_RULE: Indicates to delete a PCC rule corresponding to reserve the resource
requested by the UE.
        - MODIFY_PCC_RULE_AND_ADD_PACKET_FILTERS: Indicates to modify the PCC rule by adding new
packet filter(s).
        - MODIFY_ PCC_RULE_AND_REPLACE_PACKET_FILTERS: Indicates to modify the PCC rule by replacing
the existing packet filter(s).
        - MODIFY_ PCC_RULE_AND_DELETE_PACKET_FILTERS: Indicates to modify the PCC rule by deleting
the existing packet filter(s).
        - MODIFY_PCC_RULE_WITHOUT_MODIFY_PACKET_FILTERS: Indicates to modify the PCC rule by
modifying the QoS of the PCC rule.
```

```
    RedirectAddressType:
      anyOf:
      - type: string
        enum:
          - IPV4_ADDR
          - IPV6_ADDR
          - URL
          - SIP_URI
      - type: string
        description: >
          This string provides forward-compatibility with future
          extensions to the enumeration but is not used to encode
          content defined in the present version of this API.
      description: |
        Possible values are
        - IPV4_ADDR: Indicates that the address type is in the form of "dotted-decimal" IPv4
address.
        - IPV6_ADDR: Indicates that the address type is in the form of IPv6 address.
        - URL: Indicates that the address type is in the form of Uniform Resource Locator.
        - SIP_URI: Indicates that the address type is in the form of SIP Uniform Resource
Identifier.
    QosFlowUsage:
      anyOf:
      - type: string
        enum:
          - GENERAL
          - IMS_SIG
      - type: string
        description: >
          This string provides forward-compatibility with future
          extensions to the enumeration but is not used to encode
          content defined in the present version of this API.
      description: |
        Possible values are
        - GENERAL: Indicate no specific QoS flow usage information is available.
        - IMS_SIG: Indicate that the QoS flow is used for IMS signalling only.
    FailureCause:
      description: Indicates the cause of the failure in a Partial Success Report.
      anyOf:
      - type: string
        enum:
          - PCC_RULE_EVENT
          - PCC_QOS_FLOW_EVENT
          - RULE_PERMANENT_ERROR
          - RULE_TEMPORARY_ERROR
          - POL_DEC_ERROR
      - type: string
    CreditManagementStatus:
      description: Indicates the reason of the credit management session failure.
      anyOf:
      - type: string
        enum:
          - END_USER_SER_DENIED
          - CREDIT_CTRL_NOT_APP
          - AUTH_REJECTED
          - USER_UNKNOWN
          - RATING_FAILED
      - type: string
    SessionRuleFailureCode:
      anyOf:
      - type: string
        enum:
          - NF_MAL
          - RES_LIM
          - SESSION_RESOURCE_ALLOCATION_FAILURE
          - UNSUCC_QOS_VAL
          - INCORRECT_UM
          - UE_STA_SUSP
          - UNKNOWN_REF_ID
          - INCORRECT_COND_DATA
          - REF_ID_COLLISION
          - AN_GW_FAILED
      - 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
        - NF_MAL: Indicates that the PCC rule could not be successfully installed (for those
provisioned from the PCF) or activated (for those pre-defined in SMF) or enforced (for those already
successfully installed) due to SMF/UPF malfunction.
        - RES_LIM: Indicates that the PCC rule could not be successfully installed (for those
provisioned from PCF) or activated (for those pre-defined in SMF) or enforced (for those already
successfully installed) due to a limitation of resources at the SMF/UPF.
        - SESSION_RESOURCE_ALLOCATION_FAILURE: Indicates the session rule could not be successfully
enforced due to failure during the allocation of resources for the PDU session in the UE, RAN or
AMF.
        - UNSUCC_QOS_VAL: indicates that the QoS validation has failed.
        - INCORRECT_UM: The usage monitoring data of the enforced session rule is not the same for
all the provisioned session rule(s).
        - UE_STA_SUSP: Indicates that the UE is in suspend state.
        - UNKNOWN_REF_ID: Indicates that the session rule could not be successfully
installed/modified because the referenced identifier to a Policy Decision Data or to a Condition
Data is unknown to the SMF.
        - INCORRECT_COND_DATA: Indicates that the session rule could not be successfully
installed/modified because the referenced Condition data are incorrect.
        - REF_ID_COLLISION: Indicates that the session rule could not be successfully
installed/modified because the same Policy Decision is referenced by a PCC rule (e.g. the session
rule and the PCC rule refer to the same Usage Monitoring decision data).
        - AN_GW_FAILED: Indicates that the AN-Gateway has failed and that the PCF should refrain
from sending policy decisions to the SMF until it is informed that the S-GW has been recovered. This
value shall not be used if the SM Policy association modification procedure is initiated for session
rule removal only.
    SteeringFunctionality:
      anyOf:
      - type: string
        enum:
          - MPTCP
          - ATSSS_LL
      - 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
          - MPTCP: Indicates that PCF authorizes the MPTCP functionality to support traffic
steering, switching and splitting.
          - ATSSS_LL: Indicates that PCF authorizes the ATSSS-LL functionality to support traffic
steering, switching and splitting.
    SteerModeValue:
      description: Indicates the steering mode value determined by the PCF.
      anyOf:
      - type: string
        enum:
          - ACTIVE_STANDBY
          - LOAD_BALANCING
          - SMALLEST_DELAY
          - PRIORITY_BASED
      - type: string
    MulticastAccessControl:
      description: Indicates whether the service data flow, corresponding to the service data flow
template, is allowed or not allowed.
      anyOf:
      - type: string
        enum:
          - ALLOWED
          - NOT_ALLOWED
      - type: string
    RequestedQosMonitoringParameter:
      description: Indicates the requested QoS monitoring parameters to be measured.
      anyOf:
      - type: string
        enum:
          - DOWNLINK
          - UPLINK
          - ROUND_TRIP
      - type: string
    ReportingFrequency:
      description: Indicates the frequency for the reporting.
      anyOf:
      - type: string
        enum:
          - EVENT_TRIGGERED
          - PERIODIC
```

```
          - SESSION_RELEASE
      - type: string
    SgsnAddress:
      description: describes the address of the SGSN
      type: object
      anyOf:
        - required: [sgsnIpv4Addr]
        - required: [sgsnIpv6Addr]
      properties:
        sgsnIpv4Addr:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv4Addr'
        sgsnIpv6Addr:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv6Addr'
    SmPolicyAssociationReleaseCause:
      description: Represents the cause due to which the PCF requests the termination of the SM
policy association.
      anyOf:
      - type: string
        enum:
          - UNSPECIFIED
          - UE_SUBSCRIPTION
          - INSUFFICIENT_RES
          - VALIDATION_CONDITION_NOT_MET
          - REACTIVATION_REQUESTED
      - type: string
    PduSessionRelCause:
      description: Contains the SMF PDU Session release cause.
      anyOf:
      - type: string
        enum:
          - PS_TO_CS_HO
          - RULE_ERROR
      - type: string
    MaPduIndication:
      description: Contains the MA PDU session indication, i.e., MA PDU Request or MA PDU Network-
Upgrade Allowed.
      anyOf:
      - type: string
        enum:
          - MA_PDU_REQUEST
          - MA_PDU_NETWORK_UPGRADE_ALLOWED
      - type: string
    AtsssCapability:
      description: Contains the ATSSS capability supported for the MA PDU Session.
      anyOf:
      - type: string
        enum:
          - MPTCP_ATSSS_LL_WITH_ASMODE_UL
          - MPTCP_ATSSS_LL_WITH_EXSDMODE_DL_ASMODE_UL
          - MPTCP_ATSSS_LL_WITH_ASMODE_DLUL
          - ATSSS_LL
          - MPTCP_ATSSS_LL
      - type: string
#
    NetLocAccessSupport:
      anyOf:
      - type: string
        enum:
          - ANR_NOT_SUPPORTED
          - TZR_NOT_SUPPORTED
          - LOC_NOT_SUPPORTED
      - 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
        - ANR_NOT_SUPPORTED: Indicates that the access network does not support the report of access
network information.
        - TZR_NOT_SUPPORTED: Indicates that the access network does not support the report of UE
time zone.
        - LOC_NOT_SUPPORTED: Indicates that the access network does not support the report of UE
Location (or PLMN Id).
    PolicyDecisionFailureCode:
      description: Indicates the type of the failed policy decision and/or condition data.
      anyOf:
      - type: string
```

```
        enum:
          - TRA_CTRL_DECS_ERR
          - QOS_DECS_ERR
          - CHG_DECS_ERR
          - USA_MON_DECS_ERR
          - QOS_MON_DECS_ERR
          - CON_DATA_ERR
          - POLICY_PARAM_ERR
      - type: string
#
    NotificationControlIndication:
      description: Indicates that the notification of DDD Status is requested and/or that the
notification of DDN Failure is requested.
      anyOf:
      - type: string
        enum:
          - DDN_FAILURE
          - DDD_STATUS
      - type: string
#
    SteerModeIndicator:
      description: Contains Autonomous load-balance indicator or UE-assistance indicator.
      anyOf:
      - type: string
        enum:
          - AUTO_LOAD_BALANCE
          - UE_ASSISTANCE
      - type: string
#
```

Annex B (normative): 5GC and EPC interworking scenario support

B.1 Scope

This annex defines procedures for 5GC and EPC interworking, which contains the following scenarios:

- EPS and 5GS interworking (i.e. 3GPP access connected to EPC and 3GPP access connected to 5GC).
- EPC/ePDG and 5GS interworking (i.e. ePDG connected to EPC and 3GPP access connected to 5GC).
- EPS and 5GC/N3IWF interworking (i.e. 3GPP access connected to EPC and N3IWF connected to 5GC).
- EPS and 5GC/TNAN/TWAN interworking (i.e. 3GPP access connected to EPC and TNAN/TWAN connected to 5GC).

NOTE: In this Release 5GC and EPC interworking is not supported for SNPN.

B.2 Npcf_SMPolicyControl Service

B.2.1 Service Description

B.2.1.1 Overview

Session Management Policy Control Service applies to the cases where the SMF+PGW-C interacts with the PCF in the non-roaming scenario, the SMF+PGW-C interacts with the V-PCF in the local breakout roaming scenario and the H-SMF+H-PGW-C interacts with the H-PCF in the home-routed scenario.

B.2.1.2 Service Architecture

The Session Management Policy Control Service is provided by the PCF as shown in the SBI representation model in figure B.2.1.2-1 and in the reference point representation model in figure B.2.1.2.2.

In this scenario the NF Service Consumer is a combined SMF and PGW-C.

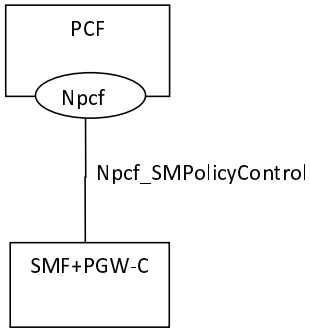

Figure B.2.1.2-1: Reference Architecture for the Npcf_SMPolicyControl Service for 5GC and EPC interworking scenario; SBI representation

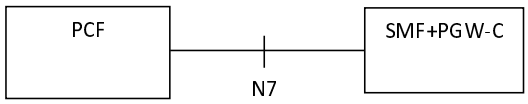

Figure B.2.1.2-2: Reference Architecture for the Npcf_SMPolicyControl Service or 5GC and EPC interworking scenario; reference point representation

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

B.3 Service Operation

B.3.1 Introduction

This clause defines the specific service operations for the 5GC and EPC interworking scenario. In addition, the service operations defined in clause 4.2 shall be applicable.

NOTE: For brevity reason, the combined SMF and PGW-C is denoted as SMF in what follows.

B.3.2 Npcf_SMPolicyControl_Create Service Operation

B.3.2.0 General

When the UE establishes the PDN connection through the EPC network and the SMF+PGW-C receives the Create Session Request message as defined in 3GPP TS 29.274 [37], the SMF+PGW-C shall behave as defined in clause 4.2.2.2 with the differences that the SMF+PGW-C shall include (if available) in SmPolicyContextData data structure:

- the IMSI of the user within the "supi" attribute;
- the MSISDN of the user within the "gpsi" attribute;
- APN within the "dnn" attribute;
- PDU Session Id determined by the SMF+PGW-C within "pduSessionId" attribute for a UE that has an EPS subscription that allows 5GC interworking but does not support 5GC NAS.

NOTE 1: For a PDN connection established via the MME or ePDG, the PDU Session ID value is assigned from a reserved range as specified in Table 5.4.2-1 of 3GPP TS 29.571 [11]. The PDU session ID value assigned at PDN connection establishment remains unchanged along the PDN connection, i.e., it does not change when the UE handovers between EPS and EPC/ePDG. In the scenarios where UE handover between EPS and EPC/ePDG is enabled, to ensure uniqueness of the assigned PDU Session ID value, the SMF+PGW-C can retrieve from UDM the already assigned PDU Session ID values, allocate a non-colliding PDU Session ID value, and register in UDM the allocated PDU session ID;

- PDN Type within the "pduSessionType" attribute;
- IMEI-SV within the "pei" attribute;
- IP-CAN type within the "accessType" attribute;
- RAT type within the "ratType" attribute;

NOTE 2: See Annex B.3.2.2 for further information.

- subscribed APN-AMBR within "subsSessAmbr" attribute;

- subscribed Default EPS bearer QoS within "subsDefQos" attribute;

NOTE 3: Subscribed APN-AMBR and the QCI within the subscribed default EPS bearer QoS are mapped to subscribed Session-AMBR and 5QI as defined in Annex B.3.6.1 respectively.

- user location information within the "userLocationInfo" attribute;

NOTE 4: See Annex B.3.2.1 for further information.

- the S-NSSAI determined by the SMF+PGW-C within the "sliceInfo" attribute; and

- the bearer usage required of the default bearer within the "qosFlowUsage" attribute.

- the UE time zone information within "ueTimeZone" attribute, if available;

NOTE 5: The UE time zone is not available in EPC untrusted WLAN.

B.3.2.1 UE Location related information

When the UE establishes the PDN connection through the EPC/E-UTRAN network, the SMF+PGW-C shall include, if available, the following user location information:

- user location information within the "eutraLocation" attribute included in the "userLocationInfo" attribute; and

- S-GW address, if available, within the "anGwAddr" attribute included in the "servNfId" attribute.

When the UE establishes the PDN connection through the EPC/UTRAN network and the feature "2G3GIWK" is supported, the SMF+PGW-C shall include, if available, the following user location information:

- user location information within the "utraLocationInfo" attribute included in the "userLocationInfo" attribute; and

- SGSN address, if available, within the "sgsnAddr" attribute included in the "servNfId" attribute.

When the UE establishes the PDN connection through the EPC/GERAN network and the feature "2G3GIWK" is supported, the SMF+PGW-C shall include, if available, the following user location information:

- user location information within the "geraLocationInfo" attribute included in the "userLocationInfo" attribute; and

- SGSN address, if available, within the "sgsnAddr" attribute included in the "servNfId" attribute.

When the UE establishes the PDN connection through the EPC/ePDG network, the SMF+PGW-C shall include, if available, the following user location information:

- user location information within the "n3gaLocation" attribute included in the "userLocationInfo" attribute. The "n3gaLocation" attribute includes the "ueIpv4Addr" or "ueIpv6Addr" attributes, and, if available the "portNumber" and "protocol" attributes; and

- ePDG identification within the "anGwAddr" attribute included in the "servNfId" attribute.

NOTE: The "n3gaLocation" attribute does not include the "n3gppTai" and "n3IwfId" attributes in EPC interworking scenarios.

B.3.2.2 Access Type related information

When the UE establishes the PDN connection through the EPC/E-UTRAN network, the SMF+PGW shall include, if available, the following access type information:

- the "3GPP_ACCESS" value within the "accessType" attribute; and

- the "EUTRA" value within the "ratType" attribute.

When the UE establishes the PDN connection through the EPC/UTRAN network and the feature "2G3GIWK" is supported, the SMF+PGW shall include, if available, the following access type information:

- the "3GPP_ACCESS" value within the "accessType" attribute; and
- the "UTRA" value within the "ratType" attribute.

When the UE establishes the PDN connection through the EPC/GERAN network and the feature "2G3GIWK" is supported, the SMF+PGW shall include, if available, the following access type information:

- the "3GPP_ACCESS" value within the "accessType" attribute; and
- the "GERA" value within the "ratType" attribute.

When the UE establishes the PDN connection through the EPC/ePDG network, the SMF+PGW shall include, if available, the following access type information:

- the "NON_3GPP_ACCESS" value within the "accessType" attribute;
- the "WLAN" or "VIRTUAL" value within the "ratType" attribute, as applicable; and
- the ePDG address in the "servNfId" attribute within the "anGwAddr" attribute.

B.3.3 Npcf_SMPolicyControl_UpdateNotify Service Operation

B.3.3.0 General

When the UE has an established PDN connection through the EPC/E-UTRAN network and the PCF provisions the policy to the SMF+PGW-C as defined in clause 4.2.3. The SMF+ PGW-C shall behave as defined in clause 4.2.3 with the differences that the SMF+PGW-C shall map the QoS information within the PCC rule and/or session rule into EPS QoS information as defined in Annex B.3.6.1.

B.3.3.1 Policy Update When UE suspends

If the PolicyUpdateWhenUESuspends feature as defined in clause 5.8 is supported the PCF and the SMF shall comply with the procedures specified in this clause. During PDU session/PDN connection establishment or modification procedure, the PCF shall subscribe to the "UE_STATUS_RESUME" policy control request trigger if not subscribed yet, as described in clause 4.2.6.4. When the SMF receives the policy decision from the PCF as defined in clause 4.2.3.1 for a PDN connection maintained when the UE's status is suspend state, the SMF shall reject the request and include an HTTP "400 Bad Request" status code together with an ErrorReport structure. Within the ErrorReport data structure, the SMF shall include the "error" attribute containing the "cause" attribute of the ProblemDetails data structure set to "UE_STATUS_SUSPEND" which indicates the failure to enforce the corresponding policy decision, except if the policy decision is for the PCC rule removal only and/or session rule removal only, and further include the information as follows:

- If the policy decision includes the installation of one or more PCC rules, the SMF shall invoke the procedure as defined in clause 4.2.3.16 with the "failureCode" attribute set to "UE_STA_SUSP" and "ruleStatus" attribute set to INACTIVE to indicate the failure to enforce those PCC rules.
- If the policy decision includes the modification of one or more PCC rules, the SMF shall invoke the procedure as defined in clause 4.2.3.16 with the "failureCode" attribute set to "UE_STA_SUSP" and "ruleStatus" attribute set to ACTIVE to indicate the failure to enforce those PCC rules.
- If the policy decision includes the modification of one or more session rules, the SMF shall within a RuleReport data structure include the "sessRuleReports" attribute. Within each SessionRuleReport data structure, the SMF shall include the affected session rules within the "ruleIds" attribute(s), the "sessRuleFailureCode" attribute set to "UE_STA_SUSP" and "ruleStatus" attribute set to ACTIVE to indicate the failure to enforce those session rules.

Upon reception of the "failureCode" attribute and/or "sessRuleFailureCode" attribute set to "UE_STA_SUSP" or the ProblemDetails data structure set to "UE_STATUS_SUSPEND", the PCF shall not initiate any PDU Session Modification procedure, except if it is initiated for the PCC rule removal only or the session rule removal only, for the given PDU session over N7 until the UE's status is resumed. When the SMF detected the UE's status is resumed from suspend state, the SMF shall inform the PCF of the UE status as defined in Annex B.3.4.2.

B.3.3.2 Request report of EPS Fallback

When the "EPSFallbackReport" feature is supported, if the AF requests the PCF to report the EPS fallback for voice media type as described in clauses 4.2.2.30 or 4.2.3.29 of 3GPP TS 29.514 [17] or in clause E.3 of 3GPP TS 29.214 [18], the PCF shall perform the PCC rule provisioning procedure as defined in clause 4.2.6.2.1 and additionally provide the request of EPS fallback report to the SMF as follows:

- it shall include the "lastReqRuleData" attribute to contain the "reqData" attribute with the value "EPS_FALLBACK" and the "refPccRuleIds" attribute to contain the related installed/modified PCC rule identifier(s) with 5QI=1.
- it shall provide the "EPS_FALLBACK" policy control request rigger within the "policyCtrlReqTriggers" attribute, if not provided before.

B.3.3.3 S-GW Restoration Support

If the SGWRest feature as defined in clause 5.8 is supported, the PCF and the SMF shall comply with the procedures specified in this clause. During PDU session/PDN connection establishment or modification procedure, the PCF shall subscribe to the "SCNN_CH" policy control request trigger if not subscribed yet, as described in clause 4.2.6.4.

When the SMF+PGW receives the policy decision from the PCF as defined in clause 4.2.3.1 for a PDN connection maintained during a S-GW failure, the SMF+PGW shall act as follows:

- For MME/S4-SGSN triggered S-GW Restoration scenarios:
  - the SMF+PGW shall reject the request and include an HTTP "400 Bad Request" status code together with an ErrorReport structure. Within the ErrorReport data structure, the SMF shall include the "error" attribute containing the "cause" attribute of the ProblemDetails data structure set to "AN_GW_FAILED" which indicates the failure to enforce the corresponding policy decision, except if the policy decision is for the PCC rule removal only and/or session rule removal only, and further include the information as follows:
    - If the policy decision is related to one or more PCC rules, the SMF+PGW shall behave as defined in clause 4.2.3.16 with the "failureCode" attribute set to "AN_GW_FAILED".
    - If the policy decision is related to one or more session rules, the SMF+PGW shall behave as defined in clause 4.2.3.20 with the "sessRuleFailureCode" attribute set to "AN_GW_FAILED".
- For SMF+PGW triggered S-GW Restoration scenarios, the SMF+PGW shall accept the procedure as per normal procedures. In the case, the PDN connection is not restored during an operator configured time period, the SMF+PGW shall behave as follows as defined in annex B.3.4.9.

Upon reception of the "cause" attribute of the ProblemDetails data structure set to "AN_GW_FAILED" or the "failureCode" attribute set to "AN_GW_FAILED" and/or the "sessRuleFailureCode" attribute set to "AN_GW_FAILED", the PCF shall not initiate any SM Policy association modification procedure, except if the I SM Policy association modification procedure is initiated for the PCC rule removal only, for the given SM Policy association over N7 until the S-GW has recovered.

The SMF+PGW shall maintain the PDN connections affected by the S-GW failure and eligible for restoration for an operator configurable time period. Upon expiry of that time period, the SMF+PGW shall release the PDN connection and inform the PCF about the SM Policy association termination as specified in clause 4.2.5.2.

The SMF+PGW should maintain the GBR bearers of the PDN connections eligible for restoration for an operator configurable time period. Upon expiry of that time period, the SMF+PGW shall release GBR bearers that have not yet been restored and inform the PCF about the PCC rule removal as specified in clause 4.2.4.7.

The SMF+PGW shall discard downlink packets received for a PDN connection maintained during a S-GW failure that has not yet been restored.

The SMF+PGW shall delete the PDN connection locally when it receives an SM Policy association termination from the PCF as described in clause 4.2.4.3.

B.3.4 Npcf_SMPolicyControl_Update Service Operation

B.3.4.0 General

When the established PDN connection through the EPC/E-UTRAN network is modified and SMF+PGW-C receives Modify Bearer Request, Modify Bearer or Delete Bearer Command message and if the SMF detects the policy control request trigger(s) is met or the error(s) needs to be reported or when the UE handed over from the 5GS to the EPS and the SMF detects the policy control request trigger(s) is met, the SMF+PGW-C shall behave as defined in clause 4.2.4.2 with the differences that the SMF+PGW-C shall include (if available) in the SmPolicyUpdateContextData data structure:

- IP-CAN type within the "accessType" attribute;
- RAT type within the "ratType" attribute;

NOTE 1: See Annex B.3.4.5 for further information.

- subscribed APN-AMBR within the "subsSessAmbr" attribute;
- subscribed Default EPS bearer QoS Information within the "subsDefQos" attribute;

NOTE 2: Subscribed APN-AMBR and the QCI within the subscribed default EPS bearer QoS are mapped to subscribed Session-AMBR and 5QI as defined in Annex B.3.6.1 respectively.

- the bearer usage required for the dedicated bearer within the "qosFlowUsage" attribute if the UE initiates a resource modification request procedure and the bearer usage request was present in the Bearer Resource Command; and
- user location information of EPC within the "userLocationInfo" attribute.

NOTE 3: See Annex B.3.4.3 for further information.

The policy control request trigger "RES_MO_RE" is not supported when the PDN connection is established through the EPC/E-UTRAN network. The SMF+PGW shall reject the PDU session modification that initiated the UE's resource modification.

B.3.4.1 Number of Supported Packet Filters Report

When the UE handed over from the EPC/E-UTRAN to the 5GS and the number of supported packet filters for signalled QoS rules is received from the UE, the SMF shall include the "NUM_OF_PACKET_FILTER" within the "repPolicyCtrlReqTriggers" attribute and the number of supported packet filters for signalled QoS rules within the "numOfPackFilter". In this case, the PCF shall behave as defined in clause 4.2.6.2.16.

NOTE: The maximum number of packet filters sent to the UE per QoS rule is additionally limited as specified in 3GPP TS 24.501 [20] when the UE is camping in 5GS.

B.3.4.2 Policy Update When UE suspends

B.3.4.2.1 Policy Update Error Report

If the PolicyUpdateWhenUESuspends feature as defined in clause 5.8 is supported, the PCF and the SMF shall comply with the procedures specified in this clause. During PDU session/PDN connection establishment or modification procedure, the PCF shall subscribe to the "UE_STATUS_RESUME" policy control request trigger if not subscribed yet, as described in clause 4.2.6.4. When the SMF receives the policy decision from the PCF as defined in clause 4.2.4.1 for a PDN connection maintained when the UE's status is suspend state, the SMF shall include the "ruleReports" attribute for the affected PCC rules and/or session rules to report the failure within the SmPolicyUpdateContextData data structure. Within the ErrorReport data structure, the SMF shall include the "error" attribute containing the "cause" attribute of the ProblemDetails data structure set to "UE_STATUS_SUSPEND" which indicates the failure to enforce the corresponding policy decision, except if the policy decision is for the PCC rule removal only and/or session rule removal only, and further include the information as follows:

- if the policy decision includes the modification of one or more session rules, within an RuleReport instance, the SMF shall include the "sessRuleReports" attribute. Within each SessionRuleReport data structure, the SMF shall include the affected session rules within the "ruleIds" attribute, the "sessRuleFailureCode" attribute set to "UE_STA_SUSP" and the "ruleStatus" attribute set to ACTIVE to indicate the failure to enforce those session rules.

- if the policy decision includes the installation of one or more PCC rules, the SMF shall invoke the procedure as defined in clause 4.2.4.15 with the "failureCode" attribute set to "UE_STA_SUSP" and "ruleStatus" attribute set to INACTIVE to indicate the failure to enforce those PCC rules.

- if the policy decision includes the modification of one or more PCC rules, the SMF shall invoke the procedure as defined in clause 4.2.4.15 with the "failureCode" attribute set to "UE_STA_SUSP" and "ruleStatus" attribute set to ACTIVE to indicate the failure to enforce those PCC rules.

Upon reception of the "failureCode" attribute and/or "sessRuleFailureCode" attribute set to "UE_STA_SUSP", the PCF shall not initiate any PDU Session Modification procedure, except if it is initiated for the PCC rule removal only and/or session rule removal only, for the given PDU session over N7 until the UE's status is resumed.

B.3.4.2.2 UE State Change Report

If the SMF detected the UE's status is resumed from suspend state, the SMF shall inform the PCF of the UE status including the "UE_STATUS_RESUME" within "repPolicyCtrlReqTriggers" attribute. The PCF shall after this update the SMF with PCC Rules or session rules if necessary.

B.3.4.3 UE Location related information

When the UE handed over from the EPC/GERAN or EPC/UTRAN and the feature "2G3GIWK" is supported, or 5GS to EPC/E-UTRAN the SMF+PGW-C shall include, together with the policy control request triggers met, the following user location information:

- If the "SAREA_CH" or "SCELL_CH" policy control request trigger is provisioned and met, the user location information within the "eutraLocation" attribute included in the "userLocationInfo" attribute.

- If the "SCNN_CH" policy control request trigger is provisioned and met, the "servNfId" attribute including the S-GW identification within the "anGwAddr" attribute.

- If the "AN_INFO" policy control request trigger is met, the user location was requested by the PCF and provided to the SMF+PGW-C, the SMF shall provide the user location information within the "eutraLocation" attribute included in the "userLocationInfo" attribute and the time when it was last known in the 3GPP access within "userLocationInfoTime" attribute (if available).

When the UE handed over from the EPC/E-UTRAN to the EPC/GERAN or EPC/UTRAN and the feature "2G3GIWK" is supported the SMF+PGW-C shall include, together with the policy control request triggers met, the following user location information:

- If the "SAREA_CH" or "SCELL_CH" policy control request trigger is provisioned and met, the user location information within the "geraLocation" attribute or "utraLocation" attribute included in the "userLocationInfo" attribute.

- If the "SCNN_CH" policy control request trigger is provisioned and met, the "servNfId" attribute including the SGSN identification within the "sgsnAddr" attribute.

When the UE handed over from the 5GS to EPC non-3GPP access, the SMF+PGW-C shall include, together with the applicable provisioned policy control request triggers, the following user location information:

- If the "SAREA_CH" policy control request trigger is provisioned and met, and the hand over is to EPC untrusted non-3GPP access, the user location information within the "n3gaLocation" attribute included in the "userLocationInfo" attribute as specified in clause B.3.2.1.

- If the "SCNN_CH" policy control request trigger is provisioned and met, the ePDG identification within the "anGwAddr" attribute included in the "servNfId" attribute.

- If the "AN_INFO" policy control request trigger is met, the user location was requested by the PCF and provided to the SMF+PGW-C, the SMF shall provide the user location information within the "n3gaLocation" attribute

included in the "userLocationInfo" attribute and the time when it was last known in the non-3GPP access within "userLocationInfoTime" attribute (if available).

NOTE 1: The "n3gaLocation" attribute does not include the "n3gppTai" and "n3IwfId" attributes in EPC interworking scenarios.

NOTE 2: SCELL_CH policy control request trigger is not supported in EPC Non-3GPP access. The PCF will not receive user location information related to this trigger in this case.

B.3.4.4 Presence Reporting Area Information Report

When the UE is connected through the EPC/E-UTRAN network, the SMF+PGW-C receives the presence reporting area information as defined in 3GPP TS 29.274 [37]. When the PRA or ePRA feature is supported, the SMF+PGW-C provides presence reporting area to the PCF as specified in clause 4.2.4.16.

If the SMF+PGW-C receives from the MME presence reporting information corresponding to the Set of Core Network predefined Presence Reporting Areas, and the individual presence reporting area as specified in 3GPP TS 29.274 [37], the SMF+PGW shall only provide the PCF with the individual presence reporting area within the "praId" attribute of the PresenceInfo data type.

B.3.4.5 Access Type related information

The SMF+PGW shall include, when the policy control request trigger "AC_TY_CH" is met, the following access type information:

- If after handover the new access type is EPC/E-UTRAN:
  a) the "3GPP_ACCESS" value within the "accessType" attribute; and
  b) the "EUTRA" value within the "ratType" attribute.
- If after handover the new access type is EPC/UTRAN and the feature "2G3GIWK" is supported:
  a) the "3GPP_ACCESS" value within the "accessType" attribute; and
  b) the "UTRA" value within the "ratType" attribute.
- If after handover the new access type is EPC/GERAN and the feature "2G3GIWK" is supported:
  a) the "3GPP_ACCESS" value within the "accessType" attribute; and
  b) the "GERA" value within the "ratType" attribute.
- If after handover the new access type is EPC/ePDG:
  a) the "NON_3GPP_ACCESS" value within the "accessType" attribute;
  b) the "WLAN" or "VIRTUAL" value within the "ratType" attribute, as applicable; and
  c) the ePDG address in the "servNfId" attribute within the "anGwAddr" attribute.

NOTE 1: In the interworking scenario, "AC_TY_CH" is met when the UE handed over from the 5GC/N3IWF or 5GC/TNAN/TWAN to the EPC/E-UTRAN, or when the UE handed over from the 5GS to the EPC/ePDG.

The SMF+PGW shall include, when the policy control request trigger "RAT_TY_CH" is met, the following RAT type information:

- If after handover the new RAT type is the E-UTRA, the "EUTRA" value within the "ratType" attribute.
- If after handover the new RAT type is the WLAN, the "WLAN" or "VIRTUAL" value within the "ratType" attribute, as applicable.

NOTE 2: In the interworking scenario, "RAT_TY_CH" is met when the UE handed over from the NR to the E-UTRA or when the UE handed over from the NR to the WLAN (untrusted) and from E-UTRA to WLAN (trusted/untrusted) or from E-UTRA to N3GA.

B.3.4.6 Report of EPS Fallback

When the "EPSFallbackReport" feature is supported, if the "PolicyCtrlReqTriggers" attribute with the value "EPS_FALLBACK" has been provided to the SMF, the SMF shall notify to the PCF of EPS fallback when a PCC rule referred from the "lastReqRuleData" attribute required the EPS fallback report within the "reqData" attribute.

When the SMF received a PDU session modification response from the access network indicating the establishment of the QoS flow with 5QI=1 is rejected due to EPS fallback, the SMF shall within the SmPolicyUpdateContextData data structure include:

- the "EPS_FALLBACK" value within the "repPolicyCtrlReqTriggers" attribute; and
- the affected PCC rules within the "pccRuleIds" attribute included in the "ruleReports" attribute, where the "ruleStatus" attribute is set to ACTIVE.

The PCF shall identify the AF session that requested the voice media type that triggered the EPS fallback and shall notify the AF as described in clauses 4.2.5.15 of 3GPP TS 29.514 [17] or in clause E.3 of 3GPP TS 29.214 [18].

B.3.4.7 MA PDU Session

If the UE or the network does not support MA PDU Session with 3GPP access connected to EPC, when the UE handed over from the EPC/E-UTRAN to the 5GS and the MA PDU Request Indication or MA PDU Network-Upgrade Allowed Indication and ATSSS Capability are received from the UE, if the "ATSSS" feature defined in clause 5.8 is supported, the SMF shall include the "MA_PDU" within the "repPolicyCtrlReqTriggers" attribute, and, as defined in clause 4.2.2.17, the SMF shall include the MA PDU session Indication within the "maPduInd" attribute and the ATSSS capability of the MA PDU session within the "atsssCapab" attribute. In this case, the PCF shall behave as defined in clause 4.2.2.17.

NOTE: If the UE and the network support MA PDU Sessions with 3GPP access connected to EPC, the MA PDU Session can be simultaneously associated with user-plane resources on 3GPP access network connected to EPC and with non-3GPP access network connected to 5GC as specified in clause B.3.6.4.

B.3.4.8 EPS RAN NAS Cause Support

If the RAN-NAS-Cause feature as defined in clause 5.8 is supported, and the PDN connection is established through the EPC network, the SMF shall report the RAN/NAS release cause(s) as specified in clauses 4.2.4.7, 4.2.4.12 and 4.2.4.15, with the exception that the received EPS RAN/NAS cause(s) are encoded within the "epsCause" attribute included in the RanNasRelCause data type. In this Release of the specification, the EPS release cause code information may include RAN/NAS release cause(s), a TWAN release cause or an untrusted WLAN release cause.

B.3.4.9 S-GW Restoration Support

If the SGWRest feature as defined in clause 5.8 is supported, the PCF and the SMF shall comply with the procedures specified in this clause. During PDU session/PDN connection establishment or modification procedure, the PCF shall subscribe to the "SCNN_CH" policy control request trigger if not subscribed yet, as described in clause 4.2.6.4.

When the SMF+PGW receives the policy decision from the PCF as defined in clause 4.2.4.1 or for a PDN connection maintained during a S-GW failure for a policy decision received as defined in clause 4.2.3.1 or 4.2.4.1, the SMF+PGW shall act as follows:

- For MME/S4-SGSN triggered S-GW Restoration scenarios:
  - When the SMF receives the policy decision from the PCF as defined in clause 4.2.4.1 for a PDN connection maintained during a S-GW failure, the SMF shall include the "ruleReports" attribute for the affected PCC rules and/or the "sessRuleReports" attribute for the affected session rules to report the failure within the SmPolicyUpdateContextData data structure and further include the information as follows.

- if the policy decision is related to one or more PCC rules, the SMF+PGW shall behave as defined in clause 4.2.4.15 with the "failureCode" attribute set to set to "AN_GW_FAILED".

- if the policy decision is related to one or more session rules the SMF+PGW shall behave as defined in clause 4.2.4.21 with the "sessRuleFailureCode" attribute set to "AN_GW_FAILED".

- For SMF+PGW triggered S-GW Restoration scenarios, if the SMF+PGW has accepted the procedure as per normal procedures but the PDN connection is not restored during an operator configured time period, the SMF+PGW shall behave as follows when the related timer expires:

  - if the policy decision is related to the PCC rule(s), the SMF+PGW shall behave as defined in clause 4.2.4.15 with the "failureCode" attribute set to "RESOURCE_ALLOCATION_FAILURE"

  - if the policy decision is related to the session rule(s), the SMF+PGW shall behave as defined in clause 4.2.4.21 with the "sessRuleFailureCode" attribute set to "SESSION_RESOURCE_ALLOCATION_FAILURE".

For MME/S4-SGSN triggered S-GW Restoration scenarios, while the S-GW restoration is in progress, if the SMF+PGW sends a request towards the PCF that is triggered by a different event (e.g. internal event at SMF+PGW), the SMF+PGW shall include the "anGwStatus" attribute set to "AN_GW_FAILED".

Upon reception of the "failureCode" attribute set to "AN_GW_FAILED" and/or the "sessRuleFailureCode" attribute set to "AN_GW_FAILED" or the "anGwStatus" attribute set to "AN_GW_FAILED", the PCF shall not initiate any SM Policy association modification procedure, except if the SM Policy association modification procedure is initiated for the PCC rule removal only, for the given SM Policy association over N7 until the S-GW has recovered.

If the SMF+PGW indicated AN_GW_FAILED previously according to the procedures described above or in annex B.3.3.3, the SMF+PGW shall inform the PCF when the S-GW has recovered by including "repPolicyCtrlReqTriggers" attribute set to the "SCNN_CH" and the "servNfId" attribute including the S-GW identification within the "anGwAddr" attribute related to the restored or new S-GW. The PCF may after this update the SMF+PGW if necessary.

NOTE 1: The PCF could reject requests from the AF and UDR when the "cause" attribute of the ProblemDetails data structure set to "AN_GW_FAILED", the "failureCode" attribute set to "AN_GW_FAILED" and/or the "sessRuleFailureCode" attribute set to "AN_GW_FAILED" or the "anGwStatus" attribute set to "AN_GW_FAILED" is received until the "repPolicyCtrlReqTriggers" attribute set to the "SCNN_CH" is received.

The SMF+PGW shall maintain the PDN connections affected by the S-GW failure and eligible for restoration for an operator configurable time period. Upon expiry of that time period, the SMF+PGW shall release the PDN connection and inform the PCF about the SM Policy association termination as specified in clause 4.2.5.2.

NOTE 2: The PCF is not aware of which PDN connections are eligible for restoration. When the SMF+PGW detects a S-GW failure, the SMF+PGW requests the PCF to terminate SM Policy associations associated to PDN connections affected by the S-GW failure and not eligible for restoration.

The SMF+PGW should maintain the GBR bearers of the PDN connections eligible for restoration for an operator configurable time period. Upon expiry of that time period, the SMF+PGW shall release GBR bearers that have not yet been restored and inform the PCF about the PCC rule removal as specified in clause 4.2.4.7.

The SMF+PGW shall discard downlink packets received for a PDN connection maintained during a S-GW failure that has not yet been restored.

The SMF+PGW shall delete the PDN connection locally when it receives an SM Policy association termination from the PCF as described in clause 4.2.4.3.

B.3.4.10 UE initiates a resource modification support

In the case that the UE initiates a resource allocation procedure as defined in clause 6.5.3 or UE initiates a resource modification procedure as defined in clause 6.5.4 of 3GPP 3GPP TS 24.301 [52], the SMF+PGW shall within the SmPolicyUpdateContextData data structure include the "RES_MO_RE" within the "repPolicyCtrlReqTriggers" attribute and shall include the UE request of specific QoS handling for selected SDF within the "ueInitResReq" attribute. Within the UeInitiatedResourceRequest data structure, the SMF+PGW shall include the "ruleOp" attribute, "packFiltInfo" attribute and "reqQos" attribute if applicable as follows:

- When the UE requests to "Create new TFT", the SMF+PGW shall include the "ruleOp" attribute set to "CREATE_PCC_RULE", the "packFiltInfo" attribute and "reqQos" attribute containing the requested QoS for the new PCC rule. Each PacketFilterInfo instance shall contain one packet filter provided by the UE. If the PCF authorizes the request, the PCF shall create a new PCC rule by including the new packet filters within the service data flow template of the PCC rule.

- When the UE requests to "Add packet filters to existing TFT", SMF+PGW shall include the "ruleOp" attribute set to "MODIFY_PCC_RULE_AND_ADD_PACKET_FILTERS", the "pccRuleId" attribute including the PCC rule identifier corresponding the packet filter identifier provided by the UE and the "packFiltInfo" attribute. Each PacketFilterInfo instance shall contain one packet filter requested for addition. If the UE request includes the modified QoS information the SMF+PGW shall also include the "reqQos" attribute to indicate the updated QoS for the affected PCC rule(s). If the PCF authorizes the request, the PCF shall update the PCC rule by adding the new packet filters to the service data flow template of the PCC rule.

- When the UE requests to "Replace packet filters in existing TFT", SMF+PGW shall include the "ruleOp" attribute set to "MODIFY_PCC_RULE_AND_REPLACE_PACKET_FILTERS", the "pccRuleId" attribute including the PCC rule identifier corresponding the packet filter identifier provided by the UE and the "packFiltInfo" attribute. Each PacketFilterInfo instance shall within the "packFiltId" attribute include the replaced packet filter identifier assigned by the PCF corresponding to the packet filter identifier received from the UE and one packet filter requested for addition. If the UE request includes the modified QoS information the SMF+PGW shall also include the "reqQos" attribute to indicate the updated QoS for the affected PCC rule. If the PCF authorizes the request, the PCF shall update PCC rule by replacing the existing packet filter with the new packet filter within the service data flow template of the PCC rule.

- When the UE requests to "Delete packet filters from existing TFT", SMF+PGW shall include the "ruleOp" attribute set to "MODIFY_PCC_RULE_AND_DELETE_PACKET_FILTERS", the "pccRuleId" attribute including the PCC rule identifier corresponding the paceket filter identifier provided by the UE and the "packFiltInfo" attribute. Each PacketFilterInfo instance shall within the "packFiltId" attribute include the removed packet filter identifier assigned by the PCF corresponding to the packet filter identifier received from the UE. If the UE request includes modified QoS information the SMF+PGW shall also include the "reqQos" attribute to indicate the updated QoS for the affected PCC rule(s). If the PCF authorizes the request, the PCF shall update PCC rule by removing the corresponding packet filters from the service data flow template of the PCC rule.

- When the UE requests to "No TFT operation", SMF+PGW shall include the "ruleOp" attribute set to "MODIFY_PCC_RULE_WITHOUT_MODIFY_PACKET_FILTERS", the "pccRuleId" attribute including the PCC rule identifier corresponding the paceket filter identifier provided by the UE and the modified QoS information within the "reqQos" attribute.

- When the UE requests to "Delete existing TFT", the SMF+PGW shall include the "ruleOp" attribute set to "DELETE_PCC_RULE", the "pccRuleId" attribute including the PCC rule identifier corresponding the packet filter identifier provided by the UE and the "packFiltInfo" attribute. The PCF shall remove the PCC rule when the PCF receives the request according to the PCC rule identifier.

NOTE 1: The UE can only modify or delete packet filters that the UE has introduced and associated resources. The packet filter identifiers contained in the FlowInformation data structure are only used for packet filters created by the UE.

The SMF+PGW shall calculate the requested GBR, for a GBR QCI, as the sum of the previously authorized GBR for the affected PCC rule, adjusted with the difference between the requested GBR for the EPS bearer and previously negotiated GBR for the EPS bearer. For the UE request to "Create new TFT", the GBR as requested by the UE for those filters shall be used.

If the request covers all the PCC rules with a bearer binding to the same bearer, then the SMF+PGW may request a change to the QCI for existing packet filters.

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

NOTE 2: The UE signalling with the network is governed by the applicable NAS signalling TS. The NAS 3GPP TS for a specific access may restrict the UE possibilities to make requests compared to what is stated above.

If the PCF authorizes the request from the UE, the PCF shall construct a PCC rule(s) based on the UeInitiatedResourceRequest data structure. For "CREATE_PCC_RULE" or "MODIFY_PCC_RULE_AND_ADD_PACKET_FILTERS" operation, the PCF shall within the FlowInformation data structure include the assigned packet filter identifier within the "packFiltId" attribute. When the SMF+PGW derives the TFT based on the PCC rule, the SMF+PGW shall assign a new packet filter identifier for each added packet filter and keep the mapping between the packet filter identifier for the packet filter within the PCC rule and TFT sento the UE.

B.3.5 Npcf_SMPolicyControl_Delete Service Operation

B.3.5.1 General

When the UE deletes the PDN connection through the EPC network and the SMF+PGW-C shall behave as defined in clause 4.2.5.2 with the difference that the SMF+PGW-C shall include the information elements contained in the Delete Session Request message within the SmPolicyDeleteData data structure.

NOTE: See Annex B.3.2.1 for location information.

B.3.5.2 EPS RAN NAS Cause Support

If the RAN-NAS-Cause feature as defined in clause 5.8 is supported, and the PDN connection is established through the EPC network, the SMF shall report the RAN/NAS release cause(s) as specified in clause 4.2.5.4.7, with the exception that the received EPS RAN/NAS cause(s) are encoded within the "epsCause" attribute included in the RanNasRelCause data type. In this Release of the specification, the EPS release cause code information may include RAN/NAS release cause(s), a TWAN release cause or an untrusted WLAN release cause.

B.3.6 Provisioning and Enforcement of Policy Decisions

B.3.6.1 QoS mapping perfomed by the SMF+PGW-C

When the UE is served by the 5GC, during PDU Session establishment and GBR QoS flow establishment, SMF+ PGW-C performs EPS QoS mappings, from the 5G QoS parameters obtained from the PCF, and allocates TFT with the PCC rules obtained from the PCF. If a TFT is to be allocated for a downlink unidirectional EPS bearer mapped from a downlink only QoS Flow, the SMF+ PGW-C shall allocate a TFT packet filter that effectively disallows any useful uplink packet as described in clause 15.3.3.4 of 3GPP TS 23.060 [26]. The SMF+PGW-C sends the mapped QoS parameters and TFT to the UE via PCO.

When the UE is served by the EPC, during PDN Connection establishment and dedicated bearer establishment/modification, SMF+ PGW-C performs EPS QoS mappings, from the 5G QoS parameters obtained from the PCF, and allocates TFT with the PCC rules obtained from the PCF. Other 5G QoS parameters corresponding to the PDN connection, e.g. Session-AMBR, and QoS rules and QoS Flow level QoS parameters if needed for the QoS Flow(s) associated with the QoS rule(s), are sent to UE in PCO.

The SMF+PGW-C shall perform EPS QoS mappings as defined in clause 4.11.1.1 and Annex C in 3GPP TS 23.502 [3] as follows:

- ignore the QNC and reflective QoS indication if received;
- for standardized 5QIs, the authorized 5QI is one to one mapped to the QCI;

NOTE: The delay critical 5QI mapping to QCI is unspecified in the present specification.

- for non-standardized 5QI,derive the authorized QCI based on the authorized 5QI and operator policy;
- one to one map the subscribed default QCI to the subscribed default 5QI;

- set the subscribed Session-AMBR according to operator policy (e.g. taking the value of subscribed APN-AMBR into account); and

- set the authorized APN-AMBR according to operator policy (e.g. taking the value of authorized Session-AMBR into account).

B.3.6.2 Provisioning of Presence Reporting Area Information

When the PRA or ePRA feature is supported, the PCF provides the SMF with Presence Reporting Area(s) information as specified in clause 4.2.6.5.6. When the UE is connected through the EPC/E-UTRAN network, the SMF+PGW-C initiates the appropriate PDN connection specific procedures specified in 3GPP TS 29.274 [37] to obtain or to deactivate the report of the presence state of a UE in a presence reporting area.

NOTE: Homogeneous support of Presence Area reporting in EPC and 5GC networks is assumed.

B.3.6.3 Request and Report of Access Network information

If the NetLoc feature as defined in clause 5.8 is supported, the PCF may request the SMF+PGW-C to report the access network information as defined in clause 4.2.6.5.4.

If the AN_INFO policy control request trigger is set, upon receiving the "lastReqRuleData" attribute with the "reqData" attribute with the value(s) MS_TIME_ZONE and/or USER_LOC_INFO and the "refPccRuleIds" attribute containing the PCC rule identifier(s) corresponding to the PCC rule(s) being installed, modified or removed:

- If the "reqData" attribute indicates MS_TIME_ZONE and USER_LOC_INFO and the SMF+PGW-C determines that the access network does not support the access network information reporting, the SMF+PGW-C shall immediately inform the PCF by including the "netLocAccSupp" attribute set to "ANR_NOT_SUPPORTED" value in the "UeCampingRep" data structure returned in the "200 OK" response to the policy update notification request.

- If the "reqData" attribute only includes the MS_TIME_ZONE value and the SMF+PGW-C determines that the access network does not support the report of the UE time zone, the SMF+PGW-C shall immediately inform the PCF by including the "netLocAccSupp" attribute set to "TZR_NOT_SUPPORTED" value in the "UeCampingRep" data structure returned in the "200 OK" response to the policy update notification request.

- If the "reqData" attribute only includes the USER_LOC_INFO value and the SMF+PGW-C determines that the access network does not support the report of the UE location, the SMF+PGW-C shall immediately inform the PCF by including the "netLocAccSupp" attribute set to "LOC_NOT_SUPPORTED" value in the "UeCampingRep" data structure returned in the "200 OK" response to the policy update notification request.

- If the "reqData" attribute includes the USER_LOC_INFO value and the MS_TIME_ZONE value, and the SMF+PGW-C determines the access network supports the report of UE location and/or UE time zone, the SMF+PGW-C shall apply appropriate procedures to the EPC access network to obtain the requested and supported access network information and shall report the available information as specified in clause 4.2.4.9.

NOTE: The SMF+PGW determines whether the access network supports access network information reporting based on access type, RAT type and trusted/untrusted type of the access network.

When the request to report access network information occurs within an EPS Fallback for IMS voice procedure, the SMF shall delay the report of access network information till the handover to EPS has been completed, as specified in 3GPP TS 23.502 [3], clause 4.13.6.1.

B.3.6.4 MA PDU sessions with connectivity over E-UTRAN/EPC and non-3GPP access to 5GC

If the "EnATSSS" feature defined in clause 5.8 is supported by both the SMF and the PCF, this scenario uses the Access Traffic Steering, Switching and Splitting functionality as described in clauses 4.2.2.17, 4.2.3.21, and 4.2.4.2 with the following specifics:

- Multi access connectivity is provided using EUTRAN/EPC as 3GPP access and non-3GPP/5GC system as non-3GPP access.

- The ATSSS rules are derived from PCC rules and provided from the PGW-C+SMF to the UE over the non-3GPP access in 5GC system.

- When the UE requests a PDN connection in EPC indicating the association with a MA PDU session, the PDN connection may be handed over to 3GPP access in 5GC without affecting the ATSSS control.

B.3.7 Detection and handling of late arriving requests for interworking scenario

B.3.7.1 Handling of requests which collide with an existing SM Policy Association

When the UE is served by the EPC and the SMF+PGW-C receives the origination time stamp from the originating entity (see clause 13.2 of 3GPP TS 29.274 [37]) during the PDN connection establishment, the SMF+PGW-C shall include the origination time stamp parameter within 3gpp-Sbi-Origination-Timestamp header in the HTTP POST request sent to the PCF, the PCF shall perform the behaviour as defined in clause 4.2.7.1.

B.3.7.2 Detection and handling of requests which have timed out at the originating entity

When the UE is served by the EPC and the SMF+PGW-C receives the origination time stamp and the maximum wait time from the originating entity (see clause 13.3 of 3GPP TS 29.274 [37]), the SMF+PGW-C shall behave as defined in annex B.3.2 with the differences that the SMF+PGW-C:

- shall include a 3gpp-Sbi-Sender-Timestamp header set to the value of the received origination time stamp;

- shall include a 3gpp-Sbi-Max-Rsp-Time header set to the value of the received maximum wait time.

When the PCF receives the request from the SMF+PGW-C, the PCF shall behave as defined in clause 6.11.2 of 3GPP TS 29.500 [4].

Annex C (normative): Wireless and wireline convergence access support

C.1 Scope

This annex defines procedures for wireless and wireline convergence access support for 5GS. The specific stage 2 definition and related procedures are contained in 3GPP TS 23.316 [42]. The System Architecture for wireless and wireline convergence access is defined in 3GPP TS 23.501 [2].

C.2 Npcf_SMPolicyControl Service

C.2.1 Service Description

C.2.1.1 Overview

Clause 4.1.1 applies with the exception that the UE is replaced by the 5G-RG and the W-AGF, which is acting as a UE towards the 5GC on behalf of the FN-RG.

C.2.1.2 Service Architecture

Clause 4.1.2 applies with the exception that roaming functionality does not apply for session policy control in this Release of the specification for 5G-RG users connecting to the 5GC via W-5GAN and FN-RG users. Roaming architecture is only applicable to a 5G-RG connecting to the 5GC via NG RAN.

The 5G-RG may support LTE access connected to EPC and EPC interworking as defined in Annex B.

C.2.1.3 Network Functions

C.2.1.3.1 Policy Control Function (PCF)

The PCF functionality defined in clause 4.1.3.1 shall apply with the exceptions described in this Annex.

C.2.1.3.2 NF Service Consumers

The functionality defined in clause 4.1.3.2 shall apply.

The enforcement of the policy decisions applies for a single access PDU session over wireline access and multiaccess PDU sessions over wireline access and 3GPP with the exceptions described in this Annex.

C.2.1.4 Rules

C.2.1.4.1 PCC Rules

Functionality as described in clause 4.1.4.2 applies with the following exceptions for the traffic of a PDU session over wireline access:

- UL/DL Maximum Packet Loss Rate information does not apply.
- QoS Notification Control Information does not apply.

C.2.1.5 Policy control request trigger

The Policy Control Request Triggers defined in clause 5.6.3.6 and related procedures are supported for a 5G-RG connecting to the 5GC via NG-RAN.

The Policy Control Request Triggers defined in clause 5.6.3.6 are supported for a 5G-RG or FN-RG connecting to the 5GC via W-5GAN with the following not supporting ones:

- PLMN_CH
- SAREA_CH
- SCNN_CH
- PRA_CH
- PS_DA_OFF
- QOS_NOTIF
- RES_RELEASE
- UE_STATUS_RESUME
- TSN_BRIDGE_INFO
- QOS_MONITORING
- SCELL_CH
- EPS_FALLBACK
- DDN_FAILURE
- DDN_DELIVERY_STATUS
- USER_LOCATION_CH

Consequently, the procedures related to above policy control request triggers are not supported in the corresponding service operations.

The PS_DA_OFF Policy Control Request Trigger may apply for the 5G-RG connecting to the 5GC via W-5GAN (see clause 4.2.2.8 and 4.2.4.8) in an hybrid access scenario (see clause C.3.6.2).

The RES_MO_RE Policy Control Request trigger is not supported for a FN-RG as described in BBF TR-456 [47] and CableLabs WR-TR-5WWC-ARCH [48] specification.

C.3 Service Operation

C.3.1 Introduction

Clause 4.2.1 applies.

C.3.2 Npcf_SMPolicyControl_Create Service Operation

C.3.2.1 General

Clause 4.2.2.2 is applied with the following differences:

- The allocated /128 IPv6 address or IPv6 /64 prefix or IPv6 prefix shorter than /64 is included within the "ipv6AddressPrefix" attribute.

- Request of Presence Reporting Area Change Report is not applicable when the 5G-RG or FN-RG connects to the 5GC via W-5GAN.

- Global Line ID including the line Id and either PLMN Id or operator Id is encoded within the "gli" attribute of the "n3gaLocation" attribute included in the "userLoc" attribute within the PolicyAssociationRequest data structure when the 5G-RG or FN-RG registers via W-5GBAN.

- The HFC Node Identifier is encoded in the "hfcNodeId" attribute of the "n3gaLocation" attribute included in the "userLocationInfo" attribute within the SmPolicyContextData data structure when the 5G-CRG or FN-CRG connects to the 5GC via W-5GCAN.

- The PEI that may be included within the "pei" attribute shall have one of the following representations:

  i. When the UE supports only wireline access, the PEI shall be a MAC address.

NOTE: When the PEI includes an indication that the MAC address cannot be used as Equipment identifier, the PEI cannot be trusted for regulatory purposes and cannot be used for equipment based policy evaluation.

  ii. When the UE supports at least one 3GPP access technology, the PEI shall be the allocated IMEI or IMEISV.

- To support of Hybrid Access for a 5G-RG with a single PDU session as described in clause C.3.6.2.2, EPC interworking specific attributes and procedures apply as described in clause B.3.2;

- Access Traffic Steering, Switching and Splitting as defined in clause 4.2.2.17 is only applicable to the case that the 5G-RG establishes:

  a) Hybrid Access with a multi-access PDU Session connectivity via NG-RAN and W-5GAN, as described in clause C.3.6.2.3; or

  b) Hybrid Access with a multi-access PDU Session connectivity via EPC/E-UTRAN and W-5GAN, as described in clause C.3.6.2.4.

- The access network transmission technology for the wireline access may be encoded:

  i. within the "ratType" attribute of the SmPolicyContextData type; or

  ii. when Access Traffic Steering, Switching and Splitting is supported, within the "ratType" attribute of the SmPolicyContextData type, or within the "ratType" attribute of the AdditionalAccessInfo type.

C.3.2.2 IPTV service support

If the PCF fetches the Multicast Access Control information from the UDR as defined in 3GPP TS 29.519 [15], the PCF shall authorize a PCC rule as defined in Annex C.3.6.1 and provision it to the SMF in the HTTP response message.

C.3.3 Npcf_SMPolicyControl_UpdateNotify Service Operation

C.3.3.1 General

The descriptions in clause 4.2.3.1 are applied with the following differences:

- To support Hybrid Access for a 5G-RG with a single PDU session as described in clause C.3.6.2.2, EPC interworking specific attributes and procedures apply as described in B.3.3;

- Access traffic steering, switching and splitting support as described in clause 4.2.3.21 is only applicable to the case that 5G-RG establishes:

  a) Hybrid Access with a multi-access PDU Session connectivity via NG-RAN and W-5GAN, as described in clause C.3.6.2.3; or

  b) Hybrid Access with a multi-access PDU Session connectivity via EPC/E-UTRAN and W-5GAN, as described in clause C.3.6.2.4.

- Request for the result of PCC rule removal is not applicable when the 5G-RG or FN-RG connects to the 5GC via W-5GAN.

C.3.3.2 IPTV service support

If the PCF fetches the Multicast Access Control information from the UDR as defined in 3GPP TS 29.519 [15], for each impacted PDU session, the PCF shall authorize a PCC rule as defined in Annex C.3.6.1 and provision it to the SMF in the HTTP POST message.

C.3.4 Npcf_SMPolicyControl_Update Service Operation

C.3.4.1 General

Clause 4.2.4.2 is applied with the following differences:

- The released /128 IPv6 address or IPv6 /64 prefix or IPv6 prefix shorter than /64 is included within the "relIpv6AddressPrefix" attribute.
- If the feature "MultiIpv6AddrPrefix" is supported, the additionally allocated IPv6 prefixes are included within the "addIpv6Prefixes" attribute and the released IPv6 prefixes are included within the "addRelIpv6Prefixes" attribute.
- RAN cause and/or the NAS cause information is not applicable when the 5G-RG or FN-RG connects the 5GC via W-5GAN.
- To support Hybrid Access for a 5G-RG with a single PDU session as described in clause C.3.6.2.2, EPC interworking specific attributes and procedures apply as described in B.3.4;
- When the report of access network information described in clause 4.2.4.9 includes the user location information, the "n3gaLocation" attribute shall be included in the "userLocationInfo" attribute and:

  a) if the UE connects via W-5GBAN access:

     - Global Line Identifier shall be encoded in the "gli" attribute; and
     - the "w5gbanLineType" attribute to indicate whether the W-5GBAN access is DSL or PON may be included; or

  b) if the UE connects via W-5GCAN access, the HFC Node Identifier shall be encoded in the "hfcNodeId" attribute.

- Access traffic steering, switching and splitting support as described in clause 4.2.4.25 is only applicable to the case that 5G-RG establishes:

  a) Hybrid Access with a multi-access PDU Session connectivity via NG-RAN and W-5GAN, as described in clause C.3.6.2.3; or

  b) Hybrid Access with a multi-access PDU Session connectivity via EPC/E-UTRAN and W-5GAN, as described in clause C.3.6.2.4.

- The access network transmission technology for the wireline access may be encoded:

  i. within the "ratType" attribute of the SmPolicyUpdateContextData type; or

  ii. when Access Traffic Steering, Switching and Splitting is supported, within the "ratType" attribute of the SmPolicyContextUpdateData type, or within the "ratType" attribute of the AdditionalAccessInfo type.

C.3.4.2 IPTV service support

If the "WWC" feature is supported and "5G_RG_JOIN" and/or "5G_RG_LEAVE" are provisioned and when the SMF detects a 5G-RG has joined or left to an IP Multicast Group, the SMF shall send an HTTP POST message as defined in clause 4.2.4.2 and include the "5G_RG_JOIN" or "5G_RG_LEAVE" within the "repPolicyCtrlReqTriggers" attribute

respectively and the received one or more IP multicast addressing information within the "mulAddrInfos" attribute. Within each IpMulticastAddressInfo data structure, the SMF shall include the destination IPv4 multicast address of the DL multicast flow within the "ipv4MulAddr" attribute and the source IPv4 address of the DL multicast flow within the "srcIpv4Addr" attribute if available or the destination IPv6 multicast address of the DL multicast flow within the "ipv6MulAddr" attribute and the source IPv6 address of the DL multicast flow within the "srcIpv6Addr" attribute if available.

NOTE: The corresponding notification can be used by the PCF to manage Preview Rights related with an IP multicast flow corresponding to an IPTV channel by provisioning the corresponding PCC rule. In this case the PCF is responsible to remove the provisioned PCC rule when the preview duration has elapsed.

C.3.5 Npcf_SMPolicyControl_Delete Service Operation

C.3.5.1 General

Clause 4.2.5.1 is applied with the following differences and limitations:

- the "n3gaLocation" attribute shall be included in the "userLocationInfo" attribute and:

  a) if the UE connects via W-5GBAN access:

     - Global Line Identifier shall be encoded in the "gli" attribute; and

     - the "w5gbanLineType" attribute to indicate whether the W-5GBAN access is DSL or PON may be included; or

  b) if the UE connects via W-5GCAN access,

     - the HFC Node Identifier shall be encoded in the "hfcNodeId" attribute; and

     - the Global Cable Identifier may be encoded within the "gci" attribute.

- RAN cause and/or the NAS cause information is not applicable when the 5G-RG or FN-RG connects the 5GC via W-5GAN.

C.3.6 Provisioning and Enforcement of Policy Decisions

C.3.6.0 General

Clause 4.2.6 applies with the following exceptions for the traffic of a PDU session over wireline access:

- Policy provisioning and enforcement of authorized QoS per service data flow as described in clause 4.2.6.6.2 applies with the following differences:

  a) Determination of Maximum Packet Loss Rate for UL/DL does not apply.

  b) PCF does not request a notification when authorized GBR or delay critical GBR cannot be guaranteed or can be guaranteed again, i.e. "qnc" attribute does not apply.

- Provisioning of PCC Rules for Multimedia Priority Services is not supported. Clause 4.2.6.2.12 does not apply.

- Provisioning of PCC Rules for Mission Critical Services is not supported. Clause 4.2.6.2.19 does not apply.

C.3.6.1 IPTV service support

If the "WWC" feature is supported by the SMF and PCF as defined in clause 5.8, when the PCF fetches the Multicast Access Control information from the UDR as defined in 3GPP TS 29.519 [15] applicable for a SUPI or Internal Group Id, the PCF authorizes the request. For impacted PDU Session that corresponds to the request, the PCF shall determine the PCC rules that are generated based on the request as follows:

- The PCF include the multicast address within the "flowInfos" attribute of the PCC rule;

- The PCF shall include the "mulAccCtrl" attribute set to "ALLOWED" within a Traffic Control Data instance which the PCC rule refers to indicate that the multicast channel is allowed.
- The PCF shall include the "mulAccCtrl" attribute set to "NOT_ALLOWED" within a Traffic Control Data instance which the PCC rule refers to indicate that the multicast channel is not allowed.

NOTE: The "flowStatus" attribute is not included in this Traffic Control Data instance.

C.3.6.2 Hybrid Access support

C.3.6.2.1 General

This clause specifies the support of policy control for Hybrid Access considering both, the support of single access PDU sessions and MA PDU sessions.

Hybrid Access applies to a 5G-RG capable of connecting to:

- both, NG-RAN and wireline access; and/or
- both, wireline access and EPC/E-UTRAN using EPC interworking as described in Annex B.

Hybrid Access does not apply to FN-RG.

C.3.6.2.2 Hybrid Access with single PDU session

Hybrid Access scenarios with single PDU sessions shall only use one of the two accesses, but the PDU session can be handover over between the two accesses.

When the "WWC" feature is supported by the SMF and the PCF as defined in clause 5.8:

- for a 5G-RG capable of connecting to the NG-RAN and the wireline access, the procedures specified in the main body of this specification apply, except:
  i. the UE is replaced by the 5G-RG; and
  ii. the non-3GPP access is replaced by the wireline access, as specified in this annex;
- for a 5G-RG capable of connecting to the wireline access and the EPC/E-UTRAN access, the procedures specified in the Annex B of this specification apply, except:
  i. the UE is replaced by the 5G-RG; and
  ii. the non-3GPP access is replaced by the wireline access.

C.3.6.2.3 Hybrid Access with MA PDU session connectivity over NG-RAN and wireline

If the "WWC" and the "ATSSS" features are supported by the SMF and the PCF as defined in clause 5.8, this scenario uses the Access Traffic Steering, Switching and Splitting functionality as described in clauses 4.2.2.17, 4.2.3.21, and 4.2.4.25.8 with the following differences:

- UE is replaced by 5G-RG.
- Non-3GPP access(es) is replaced by wireline access.

C.3.6.2.4 Hybrid Access with MA PDU session connectivity over EPC/E-UTRAN and wireline using EPC interworking scenarios

If the "WWC" and the "ATSSS" features are supported by the SMF and the PCF as defined in clause 5.8, this scenario uses the Access Traffic Steering, Switching and Splitting functionality as described in clauses 4.2.2.17, 4.2.3.21, and 4.2.4.2 with the following specifics:

- UE is replaced by 5G-RG.

- Non-3GPP access(es) is replaced by wireline access.
- Multi access connectivity is provided using ATSSS using both, EPC (as 3GPP access) and wireline access/5GC system (as non-3GPP access), where:
  i. the ATSSS rules are derived from PCC rules and provided from the PGW-C+SMF to the 5G-RG over wireline access/5GC system;
  ii. when the 5G-RG requests a PDN connection in EPC indicating the association with a MA PDU session, the PDN connection may be handed over to 3GPP access in 5GC without affecting the ATSSS control.
- MA PDU Sessions of Ethernet PDU Session type where the 3GPP access corresponds to EPC/E-UTRAN are not applicable for 5G-RG.

Annex D(informative): Change history

Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2017-10						TS skeleton of Session Management Policy Control Services specification	0.0.0
2017-10	CT3#92					Inclusion of C3-175237, C3-175353 and editorial changes from Rapporteur	0.1.0
2017-12	CT3#93					Inclusion of C3-176145, C3-176248, C3-176252, C3-176254, C3-176255, C3-176256, C3-176257, C3-176319, C3-176320, C3-176321, C3-176322, C3-176323 and editorial changes from Rapporteur	0.2.0
2018-01	CT3#94					Inclusion of C3-180035, C3-180198, C3-180097, C3-180342, C3-180303, C3-180343, C3-180202, C3-180305, C3-180307, C3- 180308, C3-180306, C3-180309, C3-180310, C3-1801311, C3-180312	0.3.0
2018-03	CT3#95					Inclusion of C3-181355, C3-181345, C3-181222, C3-181223, C3-181226, C3-181227	0.4.0
2018-04	CT3#96	C3-182515				Inclusion of C3-182056, C3-182318, C3-182322, C3-182463, C3-182325, C3-182327, C3-182330, C3-182331, C3-182132, C3-182332, C3-182324, C3-182482.	0.5.0
2018-05	CT3#97	C3-183868				Inclusion of C3-183811, C3-183889, C3-183748, C3-183749, C3-183845, C3-183461, C3-183846, C3-183847, C3-183884, C3-183850, C3-183851, C3-183852, C3-183853, C3-183470, C3-183855, C3-183854, C3-183760, C3-183885, C3-183736, C3-183848, C3-183857, C3-183858, C3-183765, C3-183766, C3-183486, C3-183886, C3-183859, C3-183887, C3-183488, C3-183489, C3-183888, C3-183815, C3-183769, C3-183793, C3-183816, C3-183763, C3-183509, C3-183865, C3-183866, C3-183771, C3-183867, C3-183772, C3-183818, C3-183255, C3-183868, C3-183284	0.6.0
2018-06	CT#80	CP-181036				TS sent to plenary for approval	1.0.0
2018-06	CT#80	CP-181036				TS approved by plenary	15.0.0
2018-09	CT#81	CP-182015	0001	5	F	Updates for TS 29.512 structure	15.1.0
2018-09	CT#81	CP-182015	0002	4	F	Update of Npcf_SMPolicyControl_Create Service Operation	15.1.0
2018-09	CT#81	CP-182015	0003	5	F	Update of Npcf_SMPolicyControl_UpdateNotify Service Operation	15.1.0
2018-09	CT#81	CP-182015	0004	3	F	Update of Npcf_SMPolicyControl_Update Service Operation	15.1.0
2018-09	CT#81	CP-182015	0005	4	F	Update of Npcf_SMPolicyControl_Delete Service Operation	15.1.0
2018-09	CT#81	CP-182015	0006	5	F	Multi-homing support	15.1.0
2018-09	CT#81	CP-182015	0007	2	F	Access Network Charging Identifier request and report	15.1.0
2018-09	CT#81	CP-182015	0008	3	F	Request result of PCC rule removal	15.1.0
2018-09	CT#81	CP-182015	0009	3	F	Request the successful resource allocation notification	15.1.0
2018-09	CT#81	CP-182168	0010	6	F	HTTP error handling procedure	15.1.0
2018-09	CT#81	CP-182169	0011	7	F	PCC Rule Error Handling	15.1.0
2018-09	CT#81	CP-182015	0012	2	F	Failure cases of Npcf_SMPolicyControl_Create Service Operation	15.1.0
2018-09	CT#81	CP-182015	0013	5	F	Failure cases of Npcf_SMPolicyControl_UpdateNotify Service Operation	15.1.0
2018-09	CT#81	CP-182015	0014	2	F	Failure cases of Npcf_SMPolicyControl_Update Service Operation	15.1.0
2018-09	CT#81	CP-182015	0015	1	F	Update of PCF and SMF function descriptions	15.1.0
2018-09	CT#81	CP-182015	0016	3	F	Rules, Session rules, PCC rules definition updates	15.1.0
2018-09	CT#81	CP-182015	0017	2	F	Policy Decision types Updates	15.1.0
2018-09	CT#81	CP-182015	0018	4	F	Policy control request trigger definition update	15.1.0
2018-09	CT#81	CP-182015	0019	2	F	Conditioned PCC rule update	15.1.0
2018-09	CT#81	CP-182015	0020	2	F	Conditioned session rule update	15.1.0
2018-09	CT#81	CP-182015	0021	2	F	IMS restoration support	15.1.0
2018-09	CT#81	CP-182015	0022	9	F	PRA support	15.1.0
2018-09	CT#81	CP-182015	0023	5	F	Update of steering the traffic to a local access of the data network	15.1.0
2018-09	CT#81	CP-182015	0024	2	F	Support for Ethernet PDU type	15.1.0
2018-09	CT#81	CP-182015	0025	6	F	Update of Provisioning of charging related information for PDU session	15.1.0
2018-09	CT#81	CP-182015	0026	4	F	UE requests specific QoS handling for selected SDF	15.1.0
2018-09	CT#81	CP-182015	0027	6	F	Provisioning of IP index information	15.1.0
2018-09	CT#81	CP-182015	0028	1	F	Update of Multimedia Priority Services	15.1.0
2018-09	CT#81	CP-182015	0029	3	F	Exclude the traffic from the session level usage monitoring	15.1.0
2018-09	CT#81	CP-182015	0030	3	F	Provisioning of specific QoS parameters together with 5QI	15.1.0
2018-09	CT#81	CP-182015	0031	1	F	Add Unspecified value to the FlowDirection data type	15.1.0
2018-09	CT#81	CP-182015	0032	2	F	Completion of definitions of UsageMonitoringData and AccuUsageReport	15.1.0
2018-09	CT#81	CP-182015	0033	4	F	Definition of FlowStatus data type	15.1.0
2018-09	CT#81	CP-182015	0034	1	F	Definition of RedirectAddressType data type	15.1.0

2018-09	CT#81	CP-182015	0035	1	F	Mandate the TrafficControlData decision	15.1.0
2018-09	CT#81	CP-182015	0036	2	F	Reflective QoS support	15.1.0
2018-09	CT#81	CP-182015	0037	1	F	Remove the DELETE method	15.1.0
2018-09	CT#81	CP-182015	0038	1	F	Remove the Packet Loss Rate from the QoS characteristics	15.1.0
2018-09	CT#81	CP-182015	0039	1	F	Re-use the ARP data type from 29.571	15.1.0
2018-09	CT#81	CP-182015	0043	1	F	Definition of DNAI	15.1.0
2018-09	CT#81	CP-182015	0044	1	F	Completion of ConditionData	15.1.0
2018-09	CT#81	CP-182015	0045	1	F	Completion of TrafficControlData data type	15.1.0
2018-09	CT#81	CP-182023	0046	1	B	Trace activation	15.1.0
2018-09	CT#81	CP-182015	0047	2	F	Corrections on the notification URIs defined for the UpdateNotify	15.1.0
2018-09	CT#81	CP-182015	0048	4	F	Corrections on attributes and data types	15.1.0
2018-09	CT#81	CP-182015	0049		F	Corrections on Supported Features	15.1.0
2018-09	CT#81	CP-182015	0050	1	F	Update custom operation for Npcf_SMPolicyControl_Update	15.1.0
2018-09	CT#81	CP-182015	0051		F	Missing Slice Information	15.1.0
2018-09	CT#81	CP-182015	0052	1	F	Solution to IPv4 overlapping	15.1.0
2018-09	CT#81	CP-182015	0053	1	F	Description of Structured data types	15.1.0
2018-09	CT#81	CP-182104	0054	1	B	Support of PCC rule versioning	15.1.0
2018-09	CT#81	CP-182015	0055	1	F	Update of Sponsored data connectivity support	15.1.0
2018-09	CT#81	CP-182015	0056	1	F	Update of resource structure	15.1.0
2018-09	CT#81	CP-182015	0057	1	F	Correction on cardinality of array and map	15.1.0
2018-09	CT#81	CP-182015	0058		F	Update of PccRule data type	15.1.0
2018-09	CT#81	CP-182015	0059	1	F	Open issues on Reused data types	15.1.0
2018-09	CT#81	CP-182015	0060		F	DNAI report	15.1.0
2018-09	CT#81	CP-182015	0061		F	Definition of maxPacketLossRate	15.1.0
2018-12	CT#82	CP-183205	0063	6	F	Correction to the AF influence traffic steering control	15.2.0
2018-12	CT#82	CP-183205	0064	2	F	Some corrections to the OpenAPI file	15.2.0
2018-12	CT#82	CP-183205	0065	3	F	Backgroud data transfer support	15.2.0
2018-12	CT#82	CP-183205	0066	4	F	Clarification of default QoS	15.2.0
2018-12	CT#82	CP-183205	0067	3	F	Clarification of Maximum Packet Loss Rate authorization	15.2.0
2018-12	CT#82	CP-183205	0068	1	F	Clarification of PCC rule enforcement	15.2.0
2018-12	CT#82	CP-183205	0069		F	Clarification of service data flow template	15.2.0
2018-12	CT#82	CP-183205	0070		F	Correction to name of maximumDataBurstVolume attribute	15.2.0
2018-12	CT#82	CP-183205	0071	1	F	Correction to the QoS notification control authorization	15.2.0
2018-12	CT#82	CP-183205	0072	3	F	IMS dedicated signalling QoS flow	15.2.0
2018-12	CT#82	CP-183205	0073	2	F	Internal Group Id during the PDU session establishment	15.2.0
2018-12	CT#82	CP-183205	0074	3	F	Number of packet filters sent to the UE	15.2.0
2018-12	CT#82	CP-183205	0075	2	F	Packet filter identifier	15.2.0
2018-12	CT#82	CP-183205	0076	1	F	Remove two values of policy control request triggers in OpenAPI	15.2.0
2018-12	CT#82	CP-183205	0077	1	F	SM policy association termination	15.2.0
2018-12	CT#82	CP-183205	0078	3	F	The procedure of QoS notification control	15.2.0
2018-12	CT#82	CP-183205	0079	4	F	Architecture of 5GS and EPS interworking scenario support	15.2.0
2018-12	CT#82	CP-183205	0083	2	F	QoS mapping in 5GS and EPS interworking scenario	15.2.0
2018-12	CT#82	CP-183205	0084		F	PCC Rules for MPS	15.2.0
2018-12	CT#82	CP-183205	0086	2	F	ExternalDocs field	15.2.0
2018-12	CT#82	CP-183205	0089	1	F	Correction of SMPolicyControl resource URI structure	15.2.0
2018-12	CT#82	CP-183205	0089	2	F	Correction of SMPolicyControl resource URI structure	15.2.0
2018-12	CT#82	CP-183205	0090	1	F	Definition on map keys in SmPolicyDecision	15.2.0
2018-12	CT#82	CP-183205	0091	1	F	Security field	15.2.0
2018-12	CT#82	CP-183205	0092	1	F	Correction of datatypes related to QoS	15.2.0
2018-12	CT#82	CP-183205	0093	1	F	Correction of 404 error information	15.2.0
2018-12	CT#82	CP-183205	0094		F	Correction of API name	15.2.0
2018-12	CT#82	CP-183205	0095	1	F	Corrections of external references in OpenAPI	15.2.0
2018-12	CT#82	CP-183205	0096	4	F	Corrections on IP index provisioning	15.2.0
2018-12	CT#82	CP-183205	0097	1	F	Corrections misused data types, attributes and error definitions	15.2.0
2018-12	CT#82	CP-183205	0098	2	F	Application Error POLICY_CONTEXT_DENIED	15.2.0
2018-12	CT#82	CP-183205	0099	2	F	Corrections on RAN-NAS-Cause feature	15.2.0
2018-12	CT#82	CP-183205	0100	1	F	Missing Policy Control Request trigger for RAT Type Change	15.2.0
2018-12	CT#82	CP-183205	0101	2	F	Corrections on rule versioning	15.2.0
2018-12	CT#82	CP-183205	0102	1	F	Corrections for Npcf_SMPolicyControl_UpdateNotify service operation.	15.2.0
2018-12	CT#82	CP-183205	0103		F	Default value for apiRoot	15.2.0
2018-12	CT#82	CP-183205	0104	1	F	Correction to RAN-NAS-Cause feature	15.2.0
2018-12	CT#82	CP-183205	0105	1	F	a new PolicyControlRequestTrigger for refQosIndication	15.2.0
2018-12	CT#82	CP-183205	0106	1	F	PCC rule error report triggerconvention	15.2.0
2018-12	CT#82	CP-183205	0108	1	F	Missing SponsoredConnectivity feature	15.2.0
2018-12	CT#82	CP-183205	0109	2	F	Correct DNAI change type in OpenAPI	15.2.0
2018-12	CT#82	CP-183205	0110	3	F	Selection of Predefined PCC Rule Base	15.2.0
2018-12	CT#82	CP-183205	0111	3	F	Correction to treatment of subscribed default QoS and authorized default QoS	15.2.0

2018-12	CT#82	CP-183123	0113	1	F	Address attribute for the network entity performing charging	15.2.0
2018-12	CT#82	CP-183205	0115	1	F	Status code update for Npcf_SMPolicyControl API	15.2.0
2018-12	CT#82	CP-183205	0116	1	F	CHF discovery and selection	15.2.0
2018-12	CT#82	CP-183205	0117	1	F	Condition Data	15.2.0
2018-12	CT#82	CP-183205	0119		F	Correction to authDefaultQos attribute	15.2.0
2018-12	CT#82	CP-183205	0120	1	F	Correction to error handling	15.2.0
2018-12	CT#82	CP-183205	0121		F	Correction to Partial Success handling	15.2.0
2018-12	CT#82	CP-183205	0122	2	F	Correction to precedence of the PCC rule	15.2.0
2018-12	CT#82	CP-183205	0123	2	F	Correction to pre-defined PCC rule activation	15.2.0
2018-12	CT#82	CP-183205	0124	-	F	Correction to the terminology of QoS notification control	15.2.0
2018-12	CT#82	CP-183205	0125	1	F	Correction to the general descriptions of Provisioning and Enforcement of Policy Decisions	15.2.0
2018-12	CT#82	CP-183205	0126	3	F	Correction to the PCC rule defintion	15.2.0
2018-12	CT#82	CP-183205	0128	1	F	Correction to the policy decision data definition	15.2.0
2018-12	CT#82	CP-183205	0129	1	F	Correction to the resource URI	15.2.0
2018-12	CT#82	CP-183205	0130		F	Correction to the RuleReport data type	15.2.0
2018-12	CT#82	CP-183205	0131	1	F	Delay critical GBR resrouce type	15.2.0
2018-12	CT#82	CP-183205	0132	1	F	Correction to the specific data type table	15.2.0
2018-12	CT#82	CP-183205	0133	1	F	HTTP custom headers	15.2.0
2018-12	CT#82	CP-183205	0134	1	F	Inactivity timer for emergency session	15.2.0
2018-12	CT#82	CP-183205	0135	1	F	Provisioning and deletion of the policy decision data	15.2.0
2018-12	CT#82	CP-183205	0136	1	F	QoS authorization for the emergency service	15.2.0
2018-12	CT#82	CP-183205	0137	1	F	Reference number alignment	15.2.0
2018-12	CT#82	CP-183205	0138		F	Supported content types	15.2.0
2018-12	CT#82	CP-183205	0140	2	F	Adding "nullable" property to data types	15.2.0
2018-12	CT#82	CP-183205	0141	2	F	VolumeRm data type	15.2.0
2018-12	CT#82	CP-183205	0142		F	Re-use PresenceInfoRm data type	15.2.0
2018-12	CT#82	CP-183205	0143	1	F	Re-use PacketLossRateRm data type	15.2.0
2018-12	CT#82	CP-183205	0144	1	F	Re-use MaxDataBurstVolRm data type	15.2.0
2018-12	CT#82	CP-183205	0145		F	Re-use DurationSecRm data type	15.2.0
2018-12	CT#82	CP-183205	0146		F	Re-use DateTimeRm data type	15.2.0
2018-12	CT#82	CP-183205	0147		F	Re-use BitRateRm data type	15.2.0
2018-12	CT#82	CP-183205	0148		F	Re-use AverWindowRm data type	15.2.0
2018-12	CT#82	CP-183205	0150		F	Re-use 5QiPriorityLevelRm data type	15.2.0
2018-12	CT#82	CP-183205	0151		F	FlowDirectionRm data type	15.2.0
2018-12	CT#82	CP-183205	0152	1	F	Correction to TrafficControlData data type	15.2.0
2018-12	CT#82	CP-183205	0153	1	F	Correction to the redirect function	15.2.0
2018-12	CT#82	CP-183205	0154		F	Correction to the modification of an attribute with a value of type map	15.2.0
2018-12	CT#82	CP-183205	0155	3	F	Correction to SmPolicyDection data type	15.2.0
2018-12	CT#82	CP-183205	0157	1	F	Correction to request rule data and requuest usage data	15.2.0
2018-12	CT#82	CP-183205	0158	1	F	Correction to QosData data structure	15.2.0
2018-12	CT#82	CP-183205	0159	2	F	Correction to Qos Characteristics	15.2.0
2018-12	CT#82	CP-183205	0160	1	F	Correction to PccRule data type	15.2.0
2018-12	CT#82	CP-183205	0161		F	Correction to FlowInformation data type	15.2.0
2018-12	CT#82	CP-183205	0162	1	F	Correction to ChargingData data type	15.2.0
2018-12	CT#82	CP-183205	0163		F	Correct the minProperties of the attributes	15.2.0
2018-12	CT#82	CP-183205	0164	1	F	Correct the minItems of the attributes	15.2.0
2018-12	CT#82	CP-183205	0166	1	F	delete UsageMonitoring in pccRule	15.2.0
2018-12	CT#82	CP-183205	0167		F	rename the heading	15.2.0
2018-12	CT#82	CP-183205	0168		F	incorrect description of online and offline	15.2.0
2018-12	CT#82	CP-183205	0169		F	Location header	15.2.0
2018-12	CT#82	CP-183205	0170	1	F	API Version Update	15.2.0
2018-12	CT#82	CP-183205	0172		F	Corrections to OpenAPI file	15.2.0
2018-12	CT#82	CP-183205	0173	1	F	Corrections of user location and session AMBR attributes	15.2.0
2018-12	CT#82	CP-183205	0174	1	F	Common data types	15.2.0
2018-12	CT#82	CP-183205	0176	2	F	Presence Info removal	15.2.0
2018-12	CT#82	CP-183205	0177	2	F	Correction of SmPolicyUpdateContext data type in OpenAPI	15.2.0
2019-03	CT#83	CP-190111	0178	1	F	The SMF may allow traffic to start before quota management for online charging	15.3.0
2019-03	CT#83	CP-190111	0179	1	F	Correction of application error codes	15.3.0
2019-03	CT#83	CP-190111	0180		F	Corrections to qosDecs attribute	15.3.0
2019-03	CT#83	CP-190111	0182		F	PCF resource cleanup	15.3.0
2019-03	CT#83	CP-190135	0183	1	F	Corrections on Traffic Steering Control	15.3.0
2019-03	CT#83	CP-190111	0184	2	F	Control of QoS parameters for default QoS Flow	15.3.0
2019-03	CT#83	CP-190157	0185	1	F	Correction to UE initiates a resource modification support	15.3.0
2019-03	CT#83	CP-190136	0186	1	F	Completion of the QoS control notification	15.3.0
2019-03	CT#83	CP-190111	0187	1	F	Correction to credit management session failure	15.3.0
2019-03	CT#83	CP-190111	0188	1	F	Correction to OpenAPI file	15.3.0
2019-03	CT#83	CP-190111	0189	1	F	Correction to Provisioning of Default Charging Method	15.3.0
2019-03	CT#83	CP-190111	0191	1	F	Correction to the access network information reporting	15.3.0

2019-03	CT#83	CP-190111	0192		F	Correction to the ARP	15.3.0
2019-03	CT#83	CP-190111	0193	1	F	Correction to the QoS data decision	15.3.0
2019-03	CT#83	CP-190111	0194	2	F	Correction to the QoS mapping perfomed by the SMF+PGW-C	15.3.0
2019-03	CT#83	CP-190111	0195	2	F	Correction to the SmPolicyDecision data type	15.3.0
2019-03	CT#83	CP-190111	0197	2	F	Correction to number of supported Packet Filters for signalled QoS rules	15.3.0
2019-03	CT#83	CP-190111	0198	1	F	PCC rule enforcement	15.3.0
2019-03	CT#83	CP-190111	0199	2	F	Policy Update When UE suspends	15.3.0
2019-03	CT#83	CP-190111	0200	1	F	Correction to the QoS characteristics	15.3.0
2019-03	CT#83	CP-190111	0201	1	F	Remove two values of failure codes	15.3.0
2019-03	CT#83	CP-190111	0205	1	F	Alignment of attributes	15.3.0
2019-03	CT#83	CP-190111	0206	2	F	HTTP response code 204 for QoS Notification	15.3.0
2019-03	CT#83	CP-190111	0208	1	F	Corrections on Charging Characteristics	15.3.0
2019-03	CT#83	CP-190111	0209		F	Correction on Provisioning of Charging Address	15.3.0
2019-03	CT#83	CP-190111	0210	1	F	Corrections for Location Change Policy Control Request Triggers	15.3.0
2019-03	CT#83	CP-190111	0211	1	F	AC_TY_CH related information	15.3.0
2019-03	CT#83	CP-190111	0212		F	Time Zone Change Policy Control Request Trigger	15.3.0
2019-03	CT#83	CP-190111	0213		F	Corrections on Reflective QoS	15.3.0
2019-03	CT#83	CP-190167	0216		F	OpenAPI version number update	15.3.0
2019-03	CT#83	CP-190121	0203	2	B	Access Type conditioned Session-AMBR	16.0.0
2019-03	CT#83	CP-190121	0207	1	B	Multiple IPV6 prefixes allocated or released in PolicyUpdate request	16.0.0
2019-03	CT#83	CP-190121	0215		F	OpenAPI version number update	16.0.0
2019-06	CT#84	CP-191072	0218	2	A	Correction of PCC rule base activation	16.1.0
2019-06	CT#84	CP-191072	0220	1	A	Corrections in main body of the specification	16.1.0
2019-06	CT#84	CP-191089	0222	2	B	DN Authorization for Policy Control	16.1.0
2019-06	CT#84	CP-191087	0223	1	B	General description for the support for traffic switching, steering and splitting	16.1.0
2019-06	CT#84	CP-191087	0225	1	B	Session Rule support for traffic switching, steering and splitting	16.1.0
2019-06	CT#84	CP-191071	0227	3	A	Correction to 5GS-EPS interworking support	16.1.0
2019-06	CT#84	CP-191072	0229	1	A	Correction to FlowInformation and rule versioning support	16.1.0
2019-06	CT#84	CP-191072	0231	2	A	Correction to PacketErrRate data type	16.1.0
2019-06	CT#84	CP-191072	0233		A	Correction to PartialSuccessReport	16.1.0
2019-06	CT#84	CP-191072	0237	2	A	Correction to the PCC bound to the default QoS flow	16.1.0
2019-06	CT#84	CP-191072	0241	1	A	MBR of Non-GBR type 5QI	16.1.0
2019-06	CT#84	CP-191072	0243	3	A	Precedence of PCC rule	16.1.0
2019-06	CT#84	CP-191071	0245	4	A	Session Rule error handling	16.1.0
2019-06	CT#84	CP-191072	0247	2	A	Usage limitiaion of the time-conditioned PCC rule	16.1.0
2019-06	CT#84	CP-191089	0248	2	B	Multiple IPv6 prefixes report for Multi-homing support	16.1.0
2019-06	CT#84	CP-191087	0249	4	B	PCC support for traffic switching, steering and splitting	16.1.0
2019-06	CT#84	CP-191072	0254	1	A	Miscellaneous corrections	16.1.0
2019-06	CT#84	CP-191072	0256	3	A	Correction to Npcf_SMPolicyControl_UpdateNotify service operation	16.1.0
2019-06	CT#84	CP-191089	0257	1	F	Update the redirection server address to support dual stack UE	16.1.0
2019-06	CT#84	CP-191072	0262		A	Precedence of OpenAPI file	16.1.0
2019-06	CT#84	CP-191072	0263	1	A	Deprecating API version	16.1.0
2019-06	CT#84	CP-191071	0264	2	B	AF acknowledgement to be expected	16.1.0
2019-06	CT#84	CP-191071	0265	2	B	UE IP address preservation indication	16.1.0
2019-06	CT#84	CP-191072	0269	1	A	Corrections to conditioned PCC rule	16.1.0
2019-06	CT#84	CP-191089	0273	2	F	Correction to IPv6 Multihoming support	16.1.0
2019-06	CT#84	CP-191072	0275		A	Correction of RuleReport type	16.1.0
2019-06	CT#84	CP-191072	0283	1	A	Correction to access network information report	16.1.0
2019-06	CT#84	CP-191072	0285	1	A	Correction to FailureCode data type	16.1.0
2019-06	CT#84	CP-191072	0291	1	A	Correction to UE_STATUS_RESUME	16.1.0
2019-06	CT#84	CP-191089	0293	1	B	Race condition handling	16.1.0
2019-06	CT#84	CP-191085	0294	1	B	Npcf_SMPolicyControl service extention of 5WWC	16.1.0
2019-06	CT#84	CP-191072	0296	1	F	Copyright Note in YAML file	16.1.0
2019-06	CT#84	CP-191101	0298	1	F	API version update	16.1.0
2019-09	CT#85	CP-192167	0302	1	B	Handling of requests colliding with an existing context	16.2.0
2019-09	CT#85	CP-192178	0303	1	B	Adding NID as input for policy decisions	16.2.0
2019-09	CT#85	CP-192156	0304	1	B	Support a set of MAC addresses in traffic filter	16.2.0
2019-09	CT#85	CP-192155	0305	1	B	Support of IMS restoration	16.2.0
2019-09	CT#85	CP-192155	0306	1	B	Support of Npcf_PolicyAuthorization invocation of priority sharing	16.2.0
2019-09	CT#85	CP-192142	0308	2	A	Correction to Resource Sharing	16.2.0
2019-09	CT#85	CP-192176	0311	1	B	Support of wireline and wireless access convergence, NFs	16.2.0
2019-09	CT#85	CP-192142	0313		A	Correction to appReloc attribute	16.2.0
2019-09	CT#85	CP-192142	0315	1	A	Correction to GBR type default QoS flow	16.2.0

2019-09	CT#85	CP-192142	0317	1	A	Correction to interworking between the 5GC and EPC	16.2.0
2019-09	CT#85	CP-192142	0319	2	A	Correction to serving node change	16.2.0
2019-09	CT#85	CP-192142	0323	1	A	Correction to UE requested resource modification	16.2.0
2019-09	CT#85	CP-192142	0325		A	Include ipDomain within SmPolicyUpdateContextData data type	16.2.0
2019-09	CT#85	CP-192142	0327	1	A	Correction to Usage Monitoring Control	16.2.0
2019-09	CT#85	CP-192142	0329	1	A	Packet filters for reflective QoS	16.2.0
2019-09	CT#85	CP-192153	0330		B	PCC rule attribute correction for ATSSS	16.2.0
2019-09	CT#85	CP-192156	0331		B	Correction to time conditioned PCC rule	16.2.0
2019-09	CT#85	CP-192152	0333	1	B	Npcf_SMPolicyControl_Create Service Operation Update of 5WWCCorrection to time conditioned PCC rule	16.2.0
2019-09	CT#85	CP-192152	0334	1	B	Npcf_SMPolicyControl_UpdateNotify Service Operation Update of 5WWC	16.2.0
2019-09	CT#85	CP-192152	0335	1	B	Npcf_SMPolicyControl_Update Service Operation Update of 5WWC	16.2.0
2019-09	CT#85	CP-192152	0336	1	B	Npcf_SMPolicyControl_Delete Service Operation Update of 5WWC	16.2.0
2019-09	CT#85	CP-192152	0337	2	B	IPTV support	16.2.0
2019-09	CT#85	CP-192175	0338	2	B	QoS Monitoring support for URLLC	16.2.0
2019-09	CT#85	CP-192171	0339	2	B	PCC rule decision enhancement for supporting xBDT	16.2.0
2019-09	CT#85	CP-192173	0341		B	OpenAPI version update TS 29.512 R-16	16.2.0
2019-12	CT#86	CP-193213	0345	2	F	Increasing the maximum MDBV value	16.3.0
2019-12	CT#86	CP-193181	0346	1	B	Open issue for AddrPreservation feature	16.3.0
2019-12	CT#86	CP-193184	0349	1	A	Correction to the usage monitoring control	16.3.0
2019-12	CT#86	CP-193184	0351	2	A	Correction to the traffic steering control	16.3.0
2019-12	CT#86	CP-193193	0352	2	B	Usage Monitoring Control for ATSSS	16.3.0
2019-12	CT#86	CP-193210	0353	1	B	Correction to handling of requests colliding with an existing context	16.3.0
2019-12	CT#86	CP-193223	0354	1	B	Multiple BDT Policies	16.3.0
2019-12	CT#86	CP-193223	0355	5	B	New cause value of association termination for xBDT	16.3.0
2019-12	CT#86	CP-193202	0356	6	B	QoS Handling for V2X Communication	16.3.0
2019-12	CT#86	CP-193197	0358	4	B	Serving 4G only UEs by SMF+PGW-C	16.3.0
2019-12	CT#86	CP-193196	0359		B	Add reference of 29.514	16.3.0
2019-12	CT#86	CP-193181	0360	1	B	Report frequency of QoS monitoring	16.3.0
2019-12	CT#86	CP-193236	0361	2	B	Line Identifier	16.3.0
2019-12	CT#86	CP-193193	0364	2	B	remove EN related to SteeringFunctionality datatype	16.3.0
2019-12	CT#86	CP-193197	0366		F	Correct the Cardinality of redirectInfo	16.3.0
2019-12	CT#86	CP-193223	0367	1	D	Background data transfer support editorials	16.3.0
2019-12	CT#86	CP-193222	0368	2	B	Transport of TSN information and containers between SMF and PCF	16.3.0
2019-12	CT#86	CP-193222	0369	2	B	Transport of TSC assistance information between SMF and PCF	16.3.0
2019-12	CT#86	CP-193184	0371		A	CHF addresses as apiRoot in the form of an FQDN	16.3.0
2019-12	CT#86	CP-193259	0372	4	B	Indication of PS to CS Handover for 5G SRVCC from SMF to PCF	16.3.0
2019-12	CT#86	CP-193215	0373	2	B	Coverage and Handover Enhancements for Media (CHEM)	16.3.0
2019-12	CT#86	CP-193197	0374	1	B	MCS Priority Level	16.3.0
2019-12	CT#86	CP-193197	0375	1	F	Removal of non-breaking spaces, TABs and $ref descriptions	16.3.0
2019-12	CT#86	CP-193197	0377	2	B	Request of SM Policy Association Termination during the Update procedur	16.3.0
2019-12	CT#86	CP-193184	0379		A	Correction to delete a PCC rule requested by the UE	16.3.0
2019-12	CT#86	CP-193184	0381		A	Termination action	16.3.0
2019-12	CT#86	CP-193233	0382	1	B	AMF change in the HR scenario	16.3.0
2019-12	CT#86	CP-193197	0383	2	B	Same PCF selection for the same UE ID, S-NSSAI and DNN combination	16.3.0
2019-12	CT#86	CP-193238	0384	2	B	Correction to the QoS monitoring Control	16.3.0
2019-12	CT#86	CP-193212	0385		F	Update of API version and TS version in OpenAPI file	16.3.0
2019-12	CT#86	CP-193197	0386		F	Correct the redirection server address to support dual stack UE	16.3.0
2019-12	CT#86	CP-193184	0388	1	A	Correction of AF Charging Identifier data type	16.3.0
2019-12	CT#86	CP-193191	0389	2	B	Clarification of PEI format, TS 29.512	16.3.0
2019-12	CT#86	CP-193230	0390	2	B	HFC node Id in Location information, TS 29.512	16.3.0
2019-12	CT#86	CP-193197	0393	1	B	Add reference to TS 29.524	16.3.0
2020-03	CT#87e	CP-200207	0402	1	B	Update of the same PCF selection	16.4.0
2020-03	CT#87e	CP-200207	0403		B	DNN Clarification	16.4.0
2020-03	CT#87e	CP-200207	0404	1	B	Cell change trigger	16.4.0
2020-03	CT#87e	CP-200207	0405	1	B	Correction to the policy decision data and condition data	16.4.0
2020-03	CT#87e	CP-200207	0406	1	B	Reallocation of credit	16.4.0
2020-03	CT#87e	CP-200207	0407	1	B	UE initiated resource modification correction	16.4.0
2020-03	CT#87e	CP-200204	0408	2	B	Complete the PCC procedure for ATSSS	16.4.0
2020-03	CT#87e	CP-200203	0410	1	B	Complete the IPTV support	16.4.0

2020-03	CT#87e	CP-200203	0411	1	B	Policy Control Request Triggers for wireline access	16.4.0
2020-03	CT#87e	CP-200203	0412	1	B	The data type of GlobalLineId	16.4.0
2020-03	CT#87e	CP-200212	0414	1	B	Complete the PCC procedure for V2XARC	16.4.0
2020-03	CT#87e	CP-200202	0415	1	B	Complete the QoS Monitoring	16.4.0
2020-03	CT#87e	CP-200218	0416	1	B	Indication of traffic correlation	16.4.0
2020-03	CT#87e	CP-200207	0417	1	B	DNN selection mode	16.4.0
2020-03	CT#87e	CP-200204	0419	2	B	interwoking with EPS for ATSSS	16.4.0
2020-03	CT#87e	CP-200285	0420	3	B	Additional Access Type for ATSSS	16.4.0
2020-03	CT#87e	CP-200231	0423	1	B	Report of EPS Fallback	16.4.0
2020-03	CT#87e	CP-200226	0424	1	B	Clarification of DS-TT and NW-TT ports identification	16.4.0
2020-03	CT#87e	CP-200226	0425	1	B	Clarification of DS-TT and NW-TT ports management information	16.4.0
2020-03	CT#87e	CP-200218	0426		B	PCF provisioning of TSN related Policy Control Request triggers	16.4.0
2020-03	CT#87e	CP-200218	0427	1	B	TSCAI input container and TSN QoS container	16.4.0
2020-03	CT#87e	CP-200214	0428		F	OpenAPI: usage of the "tags" keyword	16.4.0
2020-03	CT#87e	CP-200214	0429		F	Enumerations and "nullable" keyword	16.4.0
2020-03	CT#87e	CP-200215	0430		F	Referencing enumerations in clause 5.6.1	16.4.0
2020-03	CT#87e	CP-200200	0431		B	CHF set and instance Id in charging information	16.4.0
2020-03	CT#87e	CP-200216	0435		F	29.512 Rel-16 Update of OpenAPI version and TS version in externalDocs field	16.4.0
2020-06	CT#88e	CP-201217	0437	1	A	Correction to attributes interGrpIds and appDetectionInfos	16.5.0
2020-06	CT#88e	CP-201238	0438		F	Correction to V2XARC	16.5.0
2020-06	CT#88e	CP-201217	0440		A	String format of flow information	16.5.0
2020-06	CT#88e	CP-201217	0444	1	A	Notification URI	16.5.0
2020-06	CT#88e	CP-201233	0445	1	B	Cause Mapping of VALIDATION_CONDITION_NOT_MET	16.5.0
2020-06	CT#88e	CP-201229	0446		B	ATSSS rule derivation	16.5.0
2020-06	CT#88e	CP-201229	0447	3	B	QoS support for ATSSS	16.5.0
2020-06	CT#88e	CP-201229	0448	1	B	Enable removing the policy decision	16.5.0
2020-06	CT#88e	CP-201252	0449	2	F	Correction to bridge Information report	16.5.0
2020-06	CT#88e	CP-201252	0450	2	F	Correction to Port Management Information Container exchange	16.5.0
2020-06	CT#88e	CP-201271	0451	2	F	Correction to Provisioning of TSCAI input information and TSC QoS related data	16.5.0
2020-06	CT#88e	CP-201252	0452	1	B	PCC rule information update for vertical	16.5.0
2020-06	CT#88e	CP-201252	0453	1	B	PCF functionality update for TSN	16.5.0
2020-06	CT#88e	CP-201228	0454		B	General update of Annex C	16.5.0
2020-06	CT#88e	CP-201262	0455	3	B	Support of full Frame Routing feature	16.5.0
2020-06	CT#88e	CP-201228	0456	1	B	The data type of GlobalLineId	16.5.0
2020-06	CT#88e	CP-201338	0457	3	B	Procedure of policy provisioning of QoS monitoring control	16.5.0
2020-06	CT#88e	CP-201213	0458	1	F	QoS Monitoring Control Data correction	16.5.0
2020-06	CT#88e	CP-201217	0463	1	A	timeUsage in Accumulated Usage Report	16.5.0
2020-06	CT#88e	CP-201229	0464		F	Support the update of SteeringFunctionality	16.5.0
2020-06	CT#88e	CP-201228	0465		B	Not to support Mission Critical Services	16.5.0
2020-06	CT#88e	CP-201228	0468		F	Removal of MAC address	16.5.0
2020-06	CT#88e	CP-201244	0470		F	Removal of unbreakable space and TAB	16.5.0
2020-06	CT#88e	CP-201213	0471	1	B	Solving Editor's note on UL CL	16.5.0
2020-06	CT#88e	CP-201228	0472	1	B	Hybrid Access Support	16.5.0
2020-06	CT#88e	CP-201228	0473	1	B	Untrusted PEI	16.5.0
2020-06	CT#88e	CP-201228	0474	1	B	RAT type for WWC	16.5.0
2020-06	CT#88e	CP-201229	0475	1	B	PS Data Off for a MA PDU session	16.5.0
2020-06	CT#88e	CP-201233	0476	1	F	Correction to Reallocation of Credit	16.5.0
2020-06	CT#88e	CP-201233	0477	1	B	Local traffic routing policy	16.5.0
2020-06	CT#88e	CP-201238	0478	1	F	Referencing alternative QoS in clause 4.2.6.2.1	16.5.0
2020-06	CT#88e	CP-201252	0479	1	B	QoS information for Time Sensitive Networking	16.5.0
2020-06	CT#88e	CP-201252	0480	1	B	Update of TSN related PCRTs	16.5.0
2020-06	CT#88e	CP-201252	0481	1	B	Completion of traffic correlation	16.5.0
2020-06	CT#88e	CP-201217	0482	1	A	Correction to NetLoc feature	16.5.0
2020-06	CT#88e	CP-201217	0484	1	A	Correction to PS Data Off	16.5.0
2020-06	CT#88e	CP-201213	0486	1	F	Correct data type used in QoS monitoring	16.5.0
2020-06	CT#88e	CP-201244	0487	1	F	Storage of YAML files in ETSI Forge	16.5.0
2020-06	CT#88e	CP-201257	0489	1	B	DDN Failure and Delivery Policy Control Request triggers	16.5.0
2020-06	CT#88e	CP-201272	0490	1	B	Introduction of Bridge management information	16.5.0
2020-06	CT#88e	CP-201267	0491	1	B	Clarification of PCF behaviour to honor UE provided maximum packet filter support	16.5.0
2020-06	CT#88e	CP-201233	0492	1	B	Policy decision and condition data status report	16.5.0
2020-06	CT#88e	CP-201263	0494	1	B	New value of the ATSSS capability	16.5.0
2020-06	CT#88e	CP-201264	0495	1	B	PCC rule for Non-MPTCP traffic	16.5.0
2020-06	CT#88e	CP-201265	0496	1	B	Steering modes for GBR traffic	16.5.0
2020-06	CT#88e	CP-201252	0499	1	B	Correct the reference of the port management info container	16.5.0
2020-06	CT#88e	CP-201256	0501	1	F	URI of the Npcf_SMPolicyControl service	16.5.0
2020-06	CT#88e	CP-201233	0503	1	F	Correction to the usage of appReloc attribute	16.5.0

2020-06	CT#88e	CP-201217	0505	1	A	Correction to session rule error report	16.5.0
2020-06	CT#88e	CP-201297	0506	2	B	Clarification on the target of QoS Monitoring report	16.5.0
2020-06	CT#88e	CP-201213	0507	1	F	Correction to attributes related to QosMonitoring	16.5.0
2020-06	CT#88e	CP-201229	0508		F	Clarification on the value of 3gLoad attribute	16.5.0
2020-06	CT#88e	CP-201266	0511	1	B	Application Id in a PCC rule for ATSSS	16.5.0
2020-06	CT#88e	CP-201273	0513	1	B	QoS parameter mapping	16.5.0
2020-06	CT#88e	CP-201217	0517	1	A	Not supporting simultaneous online and offline charging	16.5.0
2020-06	CT#88e	CP-201244	0518		F	Optionality of ProblemDetails	16.5.0
2020-06	CT#88e	CP-201232	0519		F	"PCSCF-Restoration-Enhancement" feature corrections	16.5.0
2020-06	CT#88e	CP-201244	0520	1	F	Supported headers, Resource Data type, Operation Name and yaml mapping	16.5.0
2020-06	CT#88e	CP-201247	0522		F	Reallocation of credit reporting to the PCF	16.5.0
2020-06	CT#88e	CP-201255	0524		F	Update of OpenAPI version and TS version in externalDocs field	16.5.0
2020-06	CT#88e	CP-201282	0525		F	Correcting feature numbers	16.5.0
2020-09	CT#89e	CP-202068	0527	1	F	Correction of the alternative QoS profile	16.6.0
2020-09	CT#89e	CP-202052	0529		A	relIpv4Address attribute correction	16.6.0
2020-09	CT#89e	CP-202052	0531	1	A	Correction to QosData	16.6.0
2020-09	CT#89e	CP-202052	0533	2	A	Correction to QoS Flow usage negotiation	16.6.0
2020-09	CT#89e	CP-202052	0535	1	A	Correction to RedirectInformation	16.6.0
2020-09	CT#89e	CP-202209	0538	1	F	Correction to policy update when UE suspends	16.6.0
2020-09	CT#89e	CP-202059	0539		F	Correction to policy control request triggers for wireline access	16.6.0
2020-09	CT#89e	CP-202059	0553		F	Corrections related to framed routes	16.6.0
2020-09	CT#89e	CP-202077	0554		F	Correcting feature numbers	16.6.0
2020-09	CT#89e	CP-202052	0557	1	A	Correction to ADC	16.6.0
2020-09	CT#89e	CP-202052	0559		A	Correction to ChfAddress	16.6.0
2020-09	CT#89e	CP-202052	0561		A	Correction to RAN-NAS Release Cause feature	16.6.0
2020-09	CT#89e	CP-202052	0563	1	A	Correction for emergency sessions	16.6.0
2020-09	CT#89e	CP-202059	0565	1	F	Support of 5GS and EPC interworking for non-3GPP Trusted Access	16.6.0
2020-09	CT#89e	CP-202048	0566		F	Multiple traffic descriptors	16.6.0
2020-09	CT#89e	CP-202084	0567		F	Update of OpenAPI version and TS version in externalDocs field	16.6.0
2020-09	CT#89e	CP-202079	0542	1	F	Clarification of default QoS	17.0.0
2020-09	CT#89e	CP-202079	0543		B	Clarification of IP index provisioning	17.0.0
2020-09	CT#89e	CP-202079	0544	1	F	Clarification of usage monitoring control	17.0.0
2020-09	CT#89e	CP-202079	0545	1	F	Correction to indication of UE IP address preservation	17.0.0
2020-09	CT#89e	CP-202079	0546	1	F	Correction to policy control functions for TSN	17.0.0
2020-09	CT#89e	CP-202079	0547		F	Correction to the policy decision	17.0.0
2020-09	CT#89e	CP-202079	0548		F	Correction to the session-AMBR provisioning	17.0.0
2020-09	CT#89e	CP-202080	0549	1	B	Traffic steering control for 5G-LAN type of services	17.0.0
2020-09	CT#89e	CP-202079	0550	1	B	Update the definitions in 3.1	17.0.0
2020-09	CT#89e	CP-202079	0564		F	Clarification of trace control	17.0.0
2020-12	CT#90e	CP-203125	0570		A	refUmN3gData yaml correction	17.1.0
2020-12	CT#90e	CP-203139	0574		A	TS 29.512 Essential Corrections and alignments	17.1.0
2020-12	CT#90e	CP-203128	0576	1	A	Correction of the condition for the Credit Reallocation event	17.1.0
2020-12	CT#90e	CP-203159	0578	2	F	Disambiguation of the reporting and handling of triggers for PCC rule bases	17.1.0
2020-12	CT#90e	CP-203143	0582	1	A	Correction to PRA	17.1.0
2020-12	CT#90e	CP-203128	0584	3	A	Correction to access type conditioned session AMBR	17.1.0
2020-12	CT#90e	CP-203128	0586	1	A	Correction to PolicyDecisionErrorHandling feature	17.1.0
2020-12	CT#90e	CP-203128	0587	1	A	Correction to SamePcf Feature	17.1.0
2020-12	CT#90e	CP-203114	0594		A	Correction to policy based on revalidation time	17.1.0
2020-12	CT#90e	CP-203114	0597	1	A	Correction to session rule	17.1.0
2020-12	CT#90e	CP-203114	0600		A	Correction to usage monitoring control	17.1.0
2020-12	CT#90e	CP-203147	0602	1	F	Correction to FailureCode and SessionFailureCode	17.1.0
2020-12	CT#90e	CP-203148	0603	1	B	Extension of Policy Decision Failure handling	17.1.0
2020-12	CT#90e	CP-203147	0604	1	F	Correction to SM Policy Association termination due to session rule error	17.1.0
2020-12	CT#90e	CP-203147	0605	1	F	Correction to SessionRuleFailureCode	17.1.0
2020-12	CT#90e	CP-203084	0606	1	F	Correction to usage monitoring control	17.1.0
2020-12	CT#90e	CP-203147	0607		F	Correction to SMF definition for LBO	17.1.0
2020-12	CT#90e	CP-203114	0610	1	A	Correction to usage report during the policy association termination	17.1.0
2020-12	CT#90e	CP-203129	0612	1	A	Correction to the BDT policy re-negotiation	17.1.0
2020-12	CT#90e	CP-203150	0614	1	A	Remove the NW-TT port from the TSN bridge info	17.1.0
2020-12	CT#90e	CP-203139	0618		A	Storage of YAML files in 3GPP Forge	17.1.0
2020-12	CT#90e	CP-203132	0620	2	A	Correction to Alternative QoS Parameter	17.1.0
2020-12	CT#90e	CP-203111	0626	1	A	QoS monitoring report at PDU session termination	17.1.0
2020-12	CT#90e	CP-203111	0628	1	A	QoS Monitoring corrections	17.1.0
2020-12	CT#90e	CP-203147	0629	1	B	Updates to support User Location Change	17.1.0

2020-12	CT#90e	CP-203128	0631	1	A	Location change (serving cell) for Policy Control Request Trig ger	17.1.0
2020-12	CT#90e	CP-203153	0633		F	Update of OpenAPI version and TS version in externalDocs field	17.1.0
2021-03	CT#91e	CP-210226	0634	1	F	Miscellaneous corrections to the Npcf_SMPolicyControl_Create service operation	17.2.0
2021-03	CT#91e	CP-210226	0635	1	F	Miscellaneous corrections to the Npcf_SMPolicyControl_UpdateNotify service operation	17.2.0
2021-03	CT#91e	CP-210222	0637	1	A	Corrections to the procedures of policy provisioning and enforcement of authorized AMBR and default QoS	17.2.0
2021-03	CT#91e	CP-210226	0638	1	F	Clarification on the applicability of some attributes and data types to UMC featur	17.2.0
2021-03	CT#91e	CP-210226	0639	1	B	Addition of the PDU Session with offline charging only indication	17.2.0
2021-03	CT#91e	CP-210226	0640	1	F	Reference to the wrong clause for the SMF initiated PDU session termination procedure	17.2.0
2021-03	CT#91e	CP-210226	0641	1	F	Correction of a wrong reference to TS 29.514 related to AF session with required QoS procedures	17.2.0
2021-03	CT#91e	CP-210226	0642	1	F	Clarification on the applicability of some data types to the SessionRuleErrorHandling feature	17.2.0
2021-03	CT#91e	CP-210226	0643	1	F	Clarification on the applicability of some attributes to the 3GPP-PS-Data-Off feature	17.2.0
2021-03	CT#91e	CP-210226	0645	1	F	Miscellaneous corrections to TS 29.512	17.2.0
2021-03	CT#91e	CP-210205	0647	1	A	Correction to the access network information report	
2021-03	CT#91e	CP-210191	0651	2	A	Support of stateless NFs	17.2.0
2021-03	CT#91e	CP-210237	0653	1	A	Corretion to the Group Id update	17.2.0
2021-03	CT#91e	CP-210189	0655	1	A	PCC control for DDD status and availability after DDN failure events	17.2.0
2021-03	CT#91e	CP-210210	0657	3	A	Disable UE notifications at changes related to Alternative QoS Profiles	17.2.0
2021-03	CT#91e	CP-210228	0660		F	User Location Change PCRT not supported in wireline access	17.2.0
2021-03	CT#91e	CP-210202	0662	1	A	Correction to supported Policy Control Request triggers in wireline access	17.2.0
2021-03	CT#91e	CP-210192	0664	3	A	Redundant User Plane Paths	17.2.0
2021-03	CT#91e	CP-210204	0666		A	Correction to repPolicyCtrlReqTrigger attribute	17.2.0
2021-03	CT#91e	CP-210205	0668	1	A	Correction to multiple access type conditioned session rules	17.2.0
2021-03	CT#91e	CP-210205	0670		A	Correction to QOS_DEC_ERR and CH_DEC_ERR	17.2.0
2021-03	CT#91e	CP-210226	0671	1	F	Correction to Monitoring key definition	17.2.0
2021-03	CT#91e	CP-210204	0673	3	A	Correction to access type conditioned session rule	17.2.0
2021-03	CT#91e	CP-210191	0675	2	A	Correction to "resourceUri" attribute description	17.2.0
2021-03	CT#91e	CP-210227	0676		F	Correction on UE initiated PDU session modification	17.2.0
2021-03	CT#91e	CP-210237	0678	1	A	Correction to TSN scenarios.	17.2.0
2021-03	CT#91e	CP-210218	0679		F	Update of "description" field for map data types	17.2.0
2021-03	CT#91e	CP-210218	0680		F	OpenAPI reference	17.2.0
2021-03	CT#91e	CP-210237	0686	2	A	Correction to traffic correlation indication	17.2.0
2021-03	CT#91e	CP-210221	0691	1	F	Adding some missing description fields to data type definitions in OpenAPI specification files	17.2.0
2021-03	CT#91e	CP-210227	0692	1	F	Additional corrections to the Npcf_SMPolicyControl_Create service operation	17.2.0
2021-03	CT#91e	CP-210227	0693	1	F	Miscellaneous corrections to the Npcf_SMPolicyControl_Delete service operation	17.2.0
2021-03	CT#91e	CP-210227	0694	1	F	Miscellaneous corrections to the Provisioning and Enforcement of Policy Decisions clause	17.2.0
2021-03	CT#91e	CP-210227	0695	1	F	Miscellaneous corrections to the data types defined in the Npcf_SMPolicyControl API	17.2.0
2021-03	CT#91e	CP-210227	0696		F	Corrections of a reference to an non-existent subclause	17.2.0
2021-03	CT#91e	CP-210227	0697	1	F	Corrections to the P-CSCF restoration indication mechanism	17.2.0
2021-03	CT#91e	CP-210225	0698	1	F	Reference to the wrong attribute name for the QoS Monitoring Decision	17.2.0
2021-03	CT#91e	CP-210195	0701		A	Correction of a reference to the wrong attribute name for the reported presence reporting area information	17.2.0
2021-03	CT#91e	CP-210204	0706		A	Correction of the SteerModeValue attribute name in the Npcf_SMPolicyControl specific Data Types table	17.2.0
2021-03	CT#91e	CP-210227	0707		F	Corrections to the applicability column of the SmPolicyDeleteData data type	17.2.0
2021-03	CT#91e	CP-210195	0710	1	A	Correction to authDefQos attribute	17.2.0
2021-03	CT#91e	CP-210195	0716	1	A	Correction to the GBR type of default QoS flow	17.2.0
2021-03	CT#91e	CP-210217	0722		A	The apiSpecificResourceUriPart component	17.2.0
2021-03	CT#91e	CP-210221	0723	1	F	NF service consumer terminology	17.2.0
2021-03	CT#91e	CP-210220	0724		B	Optional header clarification	17.2.0
2021-03	CT#91e	CP-210195	0727	1	A	Corrections to RuleOperation	17.2.0
2021-03	CT#91e	CP-210195	0730	1	A	repPolicyCtrlReqTriggers attribute correction	17.2.0

2021-03	CT#91e	CP-210195	0733		A	Correction to session rule	17.2.0
2021-03	CT#91e	CP-210227	0734	1	F	deactivationTime for time conditioned session rule	17.2.0
2021-03	CT#91e	CP-210227	0735	1	F	Remove exUsagePccRuleIds from PCC rule definition	17.2.0
2021-03	CT#91e	CP-210222	0738		A	packFiltInfo attribute correction	17.2.0
2021-03	CT#91e	CP-210195	0741	2	A	Correction to PCF behavior when removing PCC/Session rules	17.2.0
2021-03	CT#91e	CP-210227	0742	1	F	Correction on UE initiated PDU session modification	17.2.0
2021-03	CT#91e	CP-210227	0743	1	F	Correction to conditioned rules	17.2.0
2021-03	CT#91e	CP-210227	0744	1	F	Correction to Usage Monitoring	17.2.0
2021-03	CT#91e	CP-210227	0745	1	F	Clarification about handling of valid unreferred policy decisions	17.2.0
2021-03	CT#91e	CP-210240	0748		F	Update of OpenAPI version and TS version in externalDocs field	17.2.0
2021-06	CT#92e	CP-211283	0681	2	B	Satellite backhaul change policy control request trigger	17.3.0
2021-06	CT#92e	CP-211226	0749	2	B	29.512 PCC support for MPS for DTS	17.3.0
2021-06	CT#92e	CP-211242	0751	1	F	Correction to Charging Information	17.3.0
2021-06	CT#92e	CP-211257	0752	2	B	Application Detection triggering for dynamic AM policy changes	17.3.0
2021-06	CT#92e	CP-211237	0755	2	A	Correct the error code MISS_FLOW_INFO	17.3.0
2021-06	CT#92e	CP-211198	0757	2	A	Correction to PCC control for DDD status and availability after DDN failure events	17.3.0
2021-06	CT#92e	CP-211245	0759	1	F	Correction to access network info report	17.3.0
2021-06	CT#92e	CP-211273	0760	3	B	Support Time Sensing Communication other than TSN	17.3.0
2021-06	CT#92e	CP-211272	0761	2	B	Support survival time	17.3.0
2021-06	CT#92e	CP-211218	0763	3	B	Add user plane lantecy requirement in PCC rule	17.3.0
2021-06	CT#92e	CP-211211	0764		F	Correction to policy control request trigger	17.3.0
2021-06	CT#92e	CP-211246	0765	1	F	Correction to usage monitoring for Non-3GPP	17.3.0
2021-06	CT#92e	CP-211211	0766	1	F	Clarifiction of PCF Requested Usage Report	17.3.0
2021-06	CT#92e	CP-211211	0767	1	F	Correct the disabling usage monitoring	17.3.0
2021-06	CT#92e	CP-211243	0768	1	F	Correct the Redundant PDU Session indication	17.3.0
2021-06	CT#92e	CP-211211	0769	1	F	Correct the offline charging only	17.3.0
2021-06	CT#92e	CP-211237	0771	1	A	Correction to QoS control in the VPLMN	17.3.0
2021-06	CT#92e	CP-211270	0772	4	B	Support of event trigger for GERAN and UTRAN access over N7 interface	17.3.0
2021-06	CT#92e	CP-211217	0774	1	F	Additional corrections to the PDU Session with offline charging only indication	17.3.0
2021-06	CT#92e	CP-211234	0775		F	Additional missing description fields in OpenAPI specification files	17.3.0
2021-06	CT#92e	CP-211277	0776	1	B	Support of Threshold Condition	17.3.0
2021-06	CT#92e	CP-211277	0777	1	B	Support of Steering Mode Indicator	17.3.0
2021-06	CT#92e	CP-211256	0778	2	F	Correction of tsnPortManContNwtts attribute	17.3.0
2021-06	CT#92e	CP-211215	0780	1	A	Correction on wrong referenced attributes	17.3.0
2021-06	CT#92e	CP-211276	0782	1	B	Support of Network Exposure to EAS via Local NEF	17.3.0
2021-06	CT#92e	CP-211217	0783	1	B	Handling of requests which collide with an existing SM Policy Association for interworking scenario	17.3.0
2021-06	CT#92e	CP-211217	0785	1	B	Handling of requests which have timed out at the originating entity for interworking scenario	17.3.0
2021-06	CT#92e	CP-211200	0786	1	A	Redirect Responses	17.3.0
2021-06	CT#92e	CP-211250	0790	2	F	Correction to Same PCF requests to BSF	17.3.0
2021-06	CT#92e	CP-211274	0791	1	B	Support of TSCAI time domain	17.3.0
2021-06	CT#92e	CP-211211	0792	2	F	Failure handling for traffic steering	17.3.0
2021-06	CT#92e	CP-211204	0795	1	A	Wrong referenced SmPolicyDecision data type	17.3.0
2021-06	CT#92e	CP-211265	0797		F	Update of OpenAPI version and TS version in externalDocs field	17.3.0
2021-06	CT#92e	CP-211211	0798		F	Updating the UDR upon usage report receipt	17.3.0
2021-09	CT#93e	CP-212212	0799	1	B	29.512 MPS for DTS QoS update failure	17.4.0
2021-09	CT#93e	CP-212224	0802	1	F	Correction to PRA information update	17.4.0
2021-09	CT#93e	CP-212198	0806	2	B	Duplicated notification	17.4.0
2021-09	CT#93e	CP-212193	0807	1	B	Clarification on satellite backhaul	17.4.0
2021-09	CT#93e	CP-212201	0808	1	B	Authorization of UE initiates a resource modification	17.4.0
2021-09	CT#93e	CP-212201	0809	1	B	PCC rules authorization with preliminary service information	17.4.0
2021-09	CT#93e	CP-212224	0810		B	Clarification of the charging correlation id	17.4.0
2021-09	CT#93e	CP-212224	0811		B	Removal of traffic routing information	17.4.0
2021-09	CT#93e	CP-212205	0812	1	B	Support of IMS emergency service for SNPN	17.4.0
2021-09	CT#93e	CP-212190	0815	1	A	Correction of report of User Location Info Time	17.4.0
2021-09	CT#93e	CP-212220	0817	1	A	Support of TCP and UDP ports in non-3GPP UE location	17.4.0
2021-09	CT#93e	CP-212196	0818	1	F	Align description with data type for rttThres	17.4.0
2021-09	CT#93e	CP-212196	0819		B	Congestion handling for priority-based steering mode	17.4.0
2021-09	CT#93e	CP-212196	0820		B	remove EN related to UE-assistance indicator	17.4.0
2021-09	CT#93e	CP-212211	0821	1	F	handling of SMF for TSCAI Survival Time	17.4.0
2021-09	CT#93e	CP-212211	0822	1	F	Replacement of TSN Terminology in 29.512	17.4.0

2021-09	CT#93e	CP-212189	0824	1	A	Align description with data type for thresholds in QosMonitoringData	17.4.0
2021-09	CT#93e	CP-212167	0826	1	A	correction of description of dsttResidTime	17.4.0
2021-09	CT#93e	CP-212224	0827	1	F	Corrections on the sender of the HTTP error response in the update procedure	17.4.0
2021-09	CT#93e	CP-212220	0828	1	F	Correction to the declaration of authorization credentials	17.4.0
2021-09	CT#93e	CP-212224	0829		B	Correction to the report of Netloc access information	17.4.0
2021-09	CT#93e	CP-212224	0830		B	Removal of network slice instance from service procedures	17.4.0
2021-09	CT#93e	CP-212211	0831	1	B	Introduction of TSCTSF	17.4.0
2021-09	CT#93e	CP-212220	0832	1	F	Adding a missing description field to the OpenAPI specification file of the Npcf_SMPolicyControl API	17.4.0
2021-09	CT#93e	CP-212223	0833		F	Update of OpenAPI version and TS version in externalDocs field	17.4.0
2021-09	CT#93e	CP-212224	0834	1	F	Report of 3GPP and non-3GPP User Location	17.4.0
2021-12	CT#94e	CP-213216	0836		F	Correction to the notification of satellite backhaul changes	17.5.0
2021-12	CT#94e	CP-213229	0838	1	B	PCC Support of restricted PDU Session for remote provisioning of UE using User Plane	17.5.0
2021-12	CT#94e	CP-213230	0839	2	B	Monitoring the data rate per Network Slice	17.5.0
2021-12	CT#94e	CP-213225	0840	1	B	Handling of Session Management Policy Data per PLMN	17.5.0
2021-12	CT#94e	CP-213229	0841		B	SNPN support for IMS Emergency services	17.5.0
2021-12	CT#94e	CP-213229	0842		B	Direct access to SNPN	17.5.0
2021-12	CT#94e	CP-213234	0843	1	B	Clarify the scenario where the TSC and time synchronization are not supported	17.5.0
2021-12	CT#94e	CP-213234	0844	1	B	Resolve the editor's note for bridge Id	17.5.0
2021-12	CT#94e	CP-213223	0845	2	B	Remove the editor's note for AF preference for the user plane latency	17.5.0
2021-12	CT#94e	CP-213222	0846		B	Remove the editor's note for UPF service	17.5.0
2021-12	CT#94e	CP-213227	0849	1	B	NWDAF instance provisioning to the PCF	17.5.0
2021-12	CT#94e	CP-213230	0850	1	B	Support of UE-Slice-MBR	17.5.0
2021-12	CT#94e	CP-213219	0852	1	F	Mutual exclusion between thresValue and steerModeInd	17.5.0
2021-12	CT#94e	CP-213219	0853	1	F	MA PDU sessions with connectivity over EPC and 5GC	17.5.0
2021-12	CT#94e	CP-213243	0854	1	F	Replacing PDU session in Annex B with PDN connection	17.5.0
2021-12	CT#94e	CP-213239	0855		F	API URI of the Npcf_SMPolicyControl API	17.5.0
2021-12	CT#94e	CP-213194	0856	1	B	Indication of request of notification PDU session established/terminated events	17.5.0
2021-12	CT#94e	CP-213234	0857	1	B	Handling alternative QoS related parameters received from the AF	17.5.0
2021-12	CT#94e	CP-213234	0858	1	F	Correction to TSC QoS information	17.5.0
2021-12	CT#94e	CP-213234	0859	1	F	Support of Ethernet PDU sessions and IP PDU sessions for TSC	17.5.0
2021-12	CT#94e	CP-213234	0860		F	TSCTSF as PCF consumer for TSC	17.5.0
2021-12	CT#94e	CP-213234	0861	1	F	Change the Network to TSN translator (TT) protocol aspects TS referencing	17.5.0
2021-12	CT#94e	CP-213223	0862	1	B	Adding EAS IP replacement information in PCC rules	17.5.0
2021-12	CT#94e	CP-213241	0864	1	A	PCF authorization for QoS control in the VPLMN	17.5.0
2021-12	CT#94e	CP-213219	0865	1	B	Extension of PCC rule definition for ATSSS	17.5.0
2021-12	CT#94e	CP-213244	0868		F	Correction on reused data type Uinteger	17.5.0
2021-12	CT#94e	CP-213244	0869	1	B	Error handling when no SM Policy Association exists	17.5.0
2021-12	CT#94e	CP-213244	0870		F	Correction to session rule	17.5.0
2021-12	CT#94e	CP-213225	0871	1	F	Resolving the PDU Session with offline charging only indication related Ens	17.5.0
2021-12	CT#94e	CP-213223	0872	1	B	AF Request for Simultaneous Connectivity over Source and Target PSA at Edge Relocation	17.5.0
2021-12	CT#94e	CP-213246	0873		F	Update of OpenAPI version and TS version in externalDocs field	17.5.0
2022-03	CT#95e	CP-220178	0875	1	F	29.512 MPS for DTS Notes Correction	17.6.0
2022-03	CT#95e	CP-220178	0876	1	F	29.512 MPS exemption from time conditioning	17.6.0
2022-03	CT#95e	CP-220188	0878		F	Clarification on threshold values	17.6.0
2022-03	CT#95e	CP-220183	0879	1	B	Cleanup of time sensitive communication	17.6.0
2022-03	CT#95e	CP-220183	0881	1	B	QoS determination for TSC	17.6.0
2022-03	CT#95e	CP-220182	0882	1	F	Onboarding indication	17.6.0
2022-03	CT#95e	CP-220185	0883	1	B	Support of AF triggered EAS rediscovery	17.6.0
2022-03	CT#95e	CP-220195	0884	1	F	Clarification of the packet filter identifier	17.6.0
2022-03	CT#95e	CP-220195	0886		F	Correction on UE Location related information in the interworking cases	17.6.0
2022-03	CT#95e	CP-220196	0887	1	F	Handling of number of packets in 5G	17.6.0
2022-03	CT#95e	CP-220179	0888	1	F	reusing common data type SatelliteBackhaulCategory	17.6.0
2022-03	CT#95e	CP-220195	0889	1	F	Alignment of term Session-AMBR	17.6.0
2022-03	CT#95e	CP-220195	0890		F	Update of service operation general descriptions	17.6.0
2022-03	CT#95e	CP-220187	0891	1	F	Update of service operation genenal descriptions for eNS	17.6.0
2022-03	CT#95e	CP-220182	0892	1	F	Update of 4.2.2.1	17.6.0
2022-03	CT#95e	CP-220190	0893	1	F	complete the definition of NWDAF_DATA_CHG trigger	17.6.0

2022-03	CT#95e	CP-220176	0894	2	A	Alignment of "Application Errors" clause with SBI TS template	17.6.0
2022-03	CT#95e	CP-220188	0895	1	F	Clarification to MA PDU sessions	17.6.0
2022-03	CT#95e	CP-220182	0896	1	B	Completion of the Support of restricted PDU Session for remote provisioning of UE using User Plane	17.6.0
2022-03	CT#95e	CP-220195	0898	2	B	Enhance SmPolicyAssociationReleaseCause for trigger PDU session reactivation procedure	17.6.0
2022-03	CT#95e	CP-220185	0899	1	F	Handling of supported features for Edge Computing	17.6.0
2022-03	CT#95e	CP-220191	0900		F	Corrections in attribute name and data type description related to NWDAF data.	17.6.0
2022-03	CT#95e	CP-220195	0901	1	F	Collision in SMF during UpdateNotify procedure	17.6.0
2022-03	CT#95e	CP-220195	0903	1	F	Handling of packet filters when the allowed number is exceeded	17.6.0
2022-03	CT#95e	CP-220187	0904	1	F	remove EN related to Dispersion Analytics	17.6.0
2022-03	CT#95e	CP-220201	0906	1	F	Formatting of Description Fields	17.6.0
2022-03	CT#95e	CP-220202	0907	1	B	Support of AN-GW restoration	17.6.0
2022-03	CT#95e	CP-220202	0908	1	B	UE-initiated resource modification support for interworking scenario	17.6.0
2022-03	CT#95e	CP-220167	0911	1	A	Corrections to Application Detection and Control	17.6.0
2022-03	CT#95e	CP-220201	0912		B	Updating Binding Indication for multiple resource contexts feature	17.6.0
2022-03	CT#95e	CP-220197	0913	1	F	Correction to the indication of notification to the PCF for the UE about PDU session establishment/termination events	17.6.0
2022-03	CT#95e	CP-220195	0915	1	F	Correction to enable retrieval of Network Provided Location information in a MESSAGE request	17.6.0
2022-03	CT#95e	CP-220183	0916		B	Correction to TSCAI derivation	17.6.0
2022-03	CT#95e	CP-220194	0917		F	Update of info and externalDocs fields	17.6.0
2022-03	CT#95e	CP-220335	0920		F	Correction to pvsInfo attribute	17.6.0
2022-06	CT#96	CP-221154	0922		F	Correcting the definition of the 404 status code in the OpenAPI description	17.7.0
2022-06	CT#96	CP-221145	0923	3	F	Handling of time domain	17.7.0
2022-06	CT#96	CP-221144	0924	2	F	Resolve the issue of individual QoS parameters	17.7.0
2022-06	CT#96	CP-221123	0926	1	F	MA PDU Session in EPC/E-UTRAN to 5GS handover	17.7.0
2022-06	CT#96	CP-221126	0927		F	Correction of supported features for Edge Computing functionality	17.7.0
2022-06	CT#96	CP-221130	0929	1	F	Completion of handling of NWDAF_DATA_CH trigger	17.7.0
2022-06	CT#96	CP-221138	0930	1	F	Completion of User Plane Remote Provisioning	17.7.0
2022-06	CT#96	CP-221157	0931	3	F	Correction to the charging identifier to enable uniqueness in roaming scenarios	17.7.0
2022-06	CT#96	CP-221157	0933	1	F	Correction to the PDU Session ID determination in EPC interworking scenarios	17.7.0
2022-06	CT#96	CP-221157	0935	1	F	Correction to the QoS constraints support	17.7.0
2022-06	CT#96	CP-221159	0936	1	F	Correction to the notification of PCF for a PDU session	17.7.0
2022-06	CT#96	CP-221145	0937	1	B	Burst Arrival Time adjustment	17.7.0
2022-06	CT#96	CP-221157	0939	1	F	Correction to the TrafficData and ConditionData	17.7.0
2022-06	CT#96	CP-221126	0940	2	F	Correction to QoS monitoring report	17.7.0
2022-06	CT#96	CP-221117	0941	1	A	Correction for the handling of QoS monitoring data	17.7.0
2022-06	CT#96	CP-221157	0942		F	Handling of multiple IPv6 prefixes	17.7.0
2022-06	CT#96	CP-221158	0945	1	F	Correction to traffic routing requirements	17.7.0
2022-06	CT#96	CP-221151	0947		F	Update of info and externalDocs fields	17.7.0
2022-06	CT#96	CP-221127	0949		F	The behaviour of SMF for I-SMF insertion and removal	17.7.0

History

Document history		
V17.6.0	May 2022	Publication
V17.7.0	June 2022	Publication