**3GPP TSG-SA2 Meeting #142E *S2-200xxxx***

**Online,**  **16th - 20th November 2020 (revision of S2-200xxxx)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **23.503** | **CR** | **xxx** | **rev** | **-** | **Current version:** | **16.6.0** |  |
|  | | | | | | | | |
| *For* [*HE**LP*](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* | | | | | | | | |
|  | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | General cleanup of specification | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei (Rapporteur) | | | | | | | | | |
| ***Source to TSG:*** | SA2 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI16, 5GS\_Ph1 | | | | |  | ***Date:*** | | | 2020-11-09 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-16 |
|  | *Use one of the following categories:* ***F*** *(correction)* ***A*** *(mirror corresponding to a change in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)*  Detailed explanations of the above categories can be found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | | | | | | | | *Use one of the following releases: Rel-8 (Release 8) Rel-9 (Release 9) Rel-10 (Release 10) Rel-11 (Release 11) Rel-12 (Release 12) Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | As per agreement in SA2, this CR is intended to clean up TS 23.503. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | The following changes are proposed:   1. Terminology corrections (PDU Session, QoS Flow, 5GS Bridge, Session-AMBR) 2. Replacement of “Application ID” with “Application descriptor(s)” in clause 6.1.2.2 and Annex A to align with the definition and the URSP rule structure in clause 6.6.2.1 3. Replacement of “Application ID” with “application identifier” in clause 6.1.2.3.1 to align with the rest of the text in the clause 4. Abbreviation added for Background Data Transfer (BDT) and used consistently as BDT Policy in clause 6.1.2.4 5. Removal of double mentioning of “network area information” in clause 6.1.2.4 6. Correction of Note 11 in clause 6.1.3.5 (“DN failure”->”DDN failure”) 7. Usage of correct terms “Authorized Session-AMBR” and “Authorized default 5QI/ARP” in clause 6.1.3.6 and 6.2.2.4 8. Correction of terminology (“IEEE 802.1”) and addition of references in clause 6.1.3.23 (originally proposed by S2-2004907) 9. Addition of missing “DN authorized” to “Session AMBR” in clause 6.2.1.2 10. Replacement of “SM-related” with “session management related” in clause 6.2.1.4 and 6.2.1.5 11. Completion of sentence in 6.2.9 12. Correction of punctuation and upper/lower case starting letter in several lists including Annexes. 13. Several editorial corrections (e.g. typos) 14. Make [7] Void in clause 2 because this is not referred 15. Add specific clauses for V2x Policy content in 23.287. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Readability of the specification is compromised, not improved | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 2, 3.1, 3.2, 4.1, 4.2.5, 5.1, 5.3.1, 5.3.5, 5.3.9, 5.3.10, 6.1.1.2.2, 6.1.1.3, 6.1.2.2.1, 6.1.2.2.2, 6.1.2.3.1, 6.1.2.4, 6.1.3.2.1, 6.1.3.5, 6.1.3.6, 6.1.3.17, 6.1.3.18, 6.1.3.20, 6.1.3.23, 6.2.1.1.1, 6.2.1.2, 6.2.1.3, 6.2.1.4, 6.2.1.5, 6.2.2.4, 6.2.8, 6.2.9, 6.3.1, 6.4, 6.6.2.1, 6.6.2.3, Annex A, Annex C | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **X** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  | **X** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **X** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

#### **\*\*\*FIRST CHANGE\*\*\***

# 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: "Technical Specification Group Services and System Aspects; System Architecture for the 5G System".

[3] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".

[4] 3GPP TS 23.203: "Policies and Charging control architecture; Stage 2".

[5] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[6] 3GPP TS 23.179: "Functional architecture and information flows to support mission-critical communication service; Stage 2".

[7] Void.

[8] 3GPP TS 32.240: "Charging management; Charging architecture and principles".

[9] 3GPP TS 23.402: "Architecture enhancements for non-3GPP accesses".

[10] 3GPP TS 23.161: "Network-Based IP Flow Mobility (NBIFOM); Stage 2".

[11] 3GPP TS 23.261: "IP flow mobility and seamless Wireless Local Area Network (WLAN) offload; Stage 2".

[12] 3GPP TS 23.167: "3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; IP Multimedia Subsystem (IMS) emergency sessions".

[13] 3GPP TS 29.507: "Access and Mobility Policy Control Service; Stage 3".

[14] Void.

[15] 3GPP TS 22.011: "Service Accessibility".

[16] 3GPP TS 23.221: "Architectural requirements".

[17] 3GPP TS 29.551: "5G System; Packet Flow Description Management Service; Stage 3".

[18] 3GPP TS 32.421: "Telecommunication management; Subscriber and equipment trace; Trace concepts and requirements".

[19] 3GPP TS 24.526: "UE Equipment (UE) policies for 5G System (5GS); Stage 3".

[20] 3GPP TS 32.291: "Charging management; 5G system, Charging service; stage 3".

[21] 3GPP TS 32.255: "Telecommunication management; Charging management; 5G Data connectivity domain charging; Stage 2".

[22] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

[23] 3GPP TS 23.280: "Common functional architecture to support mission critical services; Stage 2".

[24] 3GPP TS 23.288: "Architecture enhancements for 5G System (5GS) to support network data analytics services".

[25] 3GPP TS 23.216: "Single Radio Voice Call Continuity (SRVCC); Stage 2".

[26] 3GPP TS 23.272: "Circuit Switched (CS) fallback in Evolved Packet System (EPS); Stage 2".

[27] 3GPP TS 23.316: "Wireless and wireline convergence access support for the 5G System (5GS)".

[28] 3GPP TS 23.287: "Architecture enhancements for 5G System (5GS) to support Vehicle-to-Everything (V2X) services".

[29] 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[30] 3GPP TS 24.237: "IP Multimedia (IM) Core Network (CN) subsystem IP Multimedia Subsystem (IMS) Service Continuity; Stage 3".

[31] 3GPP TS 26.114: "IP Multimedia Subsystem (IMS); Multimedia telephony; Media handling and interaction".

[32] 3GPP TS 29.512: "5G System; Session Management Policy Control Service; Stage 3".

#### **\*\*\*NEXT CHANGE\*\*\***

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1], TS 23.501 [2], TS 23.502 [3] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

**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.

**Authorised QoS:** The maximum QoS that is authorised for a service data flow. In the case of an aggregation of multiple service data flows within one QoS Flow, the combination of the "Authorised QoS" information of the individual service data flows is the "Authorised QoS" for the QoS Flow. It contains the 5QI and the data rate.

**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 and/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.

**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 basis.

**Non-3GPP access network selection information:** It consists of ePDG identifier configuration, N3IWF identification and non-3GPP access node selection information, as defined in clause 6.3.6.1 in TS 23.501 [2].

**Non-Seamless Offload:** A capability of the UE to access the data networks via non-3GPP access (e.g. WLAN radio access) outside of a PDU Session.

**Operator-controlled service:** A service for which complete PCC rule information, including service data flow filter information, is available in the PCF through configuration and/or dynamic interaction with an AF.

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

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

**OS specific Application Identifier (OSAppId):** An identifier associated with a given application and uniquely identifying the application within the UE for a given operating system.

**Packet flow:** A specific user data flow from and/or to the UE.

**Packet Flow Description (PFD):** A set of information enabling the detection of application traffic provided by a 3rd party service provider.

**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 policy information 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.

**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.

**Policy counter:** A mechanism within the CHF to track spending applicable to a subscriber.

**Policy counter identifier:** A reference to a policy counter in the CHF for a subscriber.

**Policy counter status:** A label whose values are not standardized and that is associated with a policy counter's value relative to the spending limit(s) (the number of possible policy counter status values for a policy counter is one greater than the number of thresholds associated with that policy counter, i.e. policy counter status values describe the status around the thresholds). This is used to convey information relating to subscriber spending from CHF to PCF. Specific labels are configured jointly in CHF and PCF.

**Policy Section:** A Policy Section is identified by a Policy Section Identifier and consists of one or multiple URSP rule(s) or one or multiple WLANSP rule(s) or non-3GPP access network selection information or a combination of WLANSP rule(s) and non-3GPP access network selection information.

**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).

**Session based service:** An end user service requiring application level signalling, which is separated from service rendering.

**Spending limit:** A spending limit is the usage limit of a policy counter (e.g. monetary, volume, duration) that a subscriber is allowed to consume.

**Spending limit report:** a notification, containing the current policy counter status generated from the CHF to the PCF.

**Subscribed guaranteed bandwidth QoS:** The per subscriber, authorized cumulative guaranteed bandwidth QoS which is provided by the UDR to the PCF.

**Subscriber category:** is a means to group the subscribers into different classes, e.g. gold user, silver user and bronze user.

**UE Local Configuration:** Information about the association of an application to either a PDU Session or to non-seamless Offload is configured in the Mobile Termination (MT) and in the Terminal Equipment (TE). For example, UE Local Configuration can include operator specific configuration (e.g. operator provided S-NSSAI(s)), or application specific parameters to set up a PDU Session or end user configuration for specific applications.

**UE policy information:** Policy information preconfigured in the UE and/or provisioned to the UE for access selection (i.e. ANDSP), PDU Session selection (i.e. URSP) and/or V2X communications (i.e. V2XP).

**Uplink binding verification:** The network enforcement of terminal compliance with the negotiated uplink traffic mapping to QoS Flows.

**User Preferences On Non-3GPP Access Selection:** The list of configuration parameters provided by a layer (e.g. application) above NAS and used by the UE for access network discovery and selection.

#### **\*\*\*NEXT CHANGE\*\*\***

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1], TS 23.501 [2], TS 23.502 [3], TS 23.316 [27] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

AMBR Aggregated Maximum Bitrate

ANDSP Access Network Discovery & Selection Policy

ARP Allocation and Retention Priority

ASP Application Service Provider

BDT Background Data Transfer

BSF Binding Support Function

CHF CHarging Function

H-PCF A PCF in the HPLMN

H-UDR A UDR in the HPLMN

MPS Multimedia Priority Service

NBIFOM Network-based IP flow mobility

NSWO Non-Seamless WLAN Offload

NWDAF Network Data Analytics Function

OAM Operation Administration and Maintenance

OCS Online Charging System

PCC Policy and Charging Control

PFD Packet Flow Description

PFDF Packet Flow Description Function

PRA Presence Reporting Area

RAN Radio Access Network

URSP UE Route Selection Policy

V2XP V2X Policy

V-PCF A PCF in the VPLMN

V-UDR A UDR in the VPLMN

vSRVCC video Single Radio Voice Call Continuity

WLANSP WLAN Selection Policy

#### **\*\*\*NEXT CHANGE\*\*\***

## 4.1 General requirements

It shall be possible to apply policy and charging control to any kind of 3GPP and non-3GPP accesses defined in TS 23.501 [2].

The policy and charging control framework shall support the roaming scenarios defined in TS 23.501 [2].

The policy and charging control shall be enabled on a per slice instance, per DNN, or per both slice instance and DNN basis.

NOTE: In single PCF deployment, the PCF will provide all mobility, UE access selection and PDU Session related policies that it is responsible for. In deployments where different PCFs support N15 and N7 respectively, no standardized interface between them is required in this release to support policy alignment.

The policy and charging control framework shall fulfil non-session management related requirements as defined in clause 4.2 and session management related requirements as defined in clause 4.3.

#### **\*\*\*NEXT CHANGE\*\*\***

### 4.2.5 SMF selection management related policy control requirements

The policy framework may provide following functionality for the SMF selection management for a PDU Session:

- The Policy Control Function (PCF) may support interactions with the SMF selection functionality in the AMF and the PCF may provide SMF selection management related policies to the AMF;

- The PCF may provide a policy to the AMF to contact PCF for performing DNN replacement of specific DNNs;

- The PCF may provide a policy to the AMF to contact PCF for performing DNN replacement for an unsupported DNN.

#### **\*\*\*NEXT CHANGE\*\*\***

## 5.1 General

This specification describes the policy and charging control framework for the 5G system. The interaction between network functions is represented in two ways:

- A service-based representation, where network functions enable other authorized network functions to access their services. This representation also includes point-to-point reference points where necessary;

- A reference point representation, which shows that interactions exist between those network functions for which a reference point is depicted between them.

#### **\*\*\*NEXT CHANGE\*\*\***

### 5.3.1 Interactions between PCF and AF

Npcf and Naf enable transport of application level session information and Ethernet port management information from AF to PCF. Such information includes, but is not limited to:

- IP filter information or Ethernet packet filter information to identify the service data flow for policy control and/or differentiated charging;

- media/application bandwidth requirements for QoS control;

- In addition, for sponsored data connectivity:

- the sponsor's identification;

- optionally, a usage threshold and whether the PCF reports these events to the AF;

- information identifying the application service provider and application (e.g. SDFs, application identifier, etc.);

- information required to enable Application Function influence on traffic routing as defined in clause 5.6.7 of TS 23.501 [2];

- information required to enable setting up an AF session with required QoS as defined in clause 6.1.3.22;

- information required to enable setting up an AF session with support for Time Sensitive Networking (TSN) as defined in clause 6.1.3.23.

Npcf and Naf enable the AF subscription to notifications on PDU Session events, i.e. the events requested by the AF as described in clause 6.1.3.18 and the change of DNAI as defined in clause 5.6.7 of TS 23.501 [2].

The N5 reference point is defined for the interactions between PCF and AF in the reference point representation.

#### **\*\*\*NEXT CHANGE\*\*\***

### 5.3.5 Interactions between PCF and UDR

The Nudr enables the PCF to access policy control related subscription information and application specific information stored in the UDR. The Nudr interface supports the following functions:

- request for policy control related subscription information and application specific information from the UDR;

- provisioning of policy control related subscription information and application specific information to the UDR;

- notifications from the UDR on changes in the policy control related subscription information;

- subscription to the UDR for the AF requests targeting a DNN and S-NSSAI or a group of UEs (roaming UEs for LBO case) identified by an Internal Group Identifier;

- notifications from the UDR on the update of AF requests targeting a DNN and S-NSSAI or a group of UEs (roaming UEs for LBO case) identified by an Internal Group Identifier.

The N36 reference point is defined for the interactions between PCF and UDR in the reference point representation.

#### **\*\*\*NEXT CHANGE\*\*\***

### 5.3.9 Interactions between SMF and NEF

Nsmf and Nnef enable transport of PFDs from the NEF (PFDF) to the SMF for a particular application identifier or for a set of application identifiers. It is achieved with the support of the following functionality:

- Creation, updating and removal of individual or the whole set of PFDs from the NEF (PFDF) to the SMF;

- Confirmation of creation, updating and removal of PFDs from the SMF to the NEF (PFDF).

NOTE: The interactions between the SMF and the NEF (PFDF) for transporting PFDs are not related to any PDU Session.

The N29 reference point is defined for the interactions between SMF and NEF (PFDF) in the reference point representation.

#### **\*\*\*NEXT CHANGE\*\*\***

### 5.3.10 Interactions between NEF and PCF

Npcf and Nnef enable the negotiation of policy and charging control behaviour between PCF and NEF by supporting the following functionality:

- service specific policy and charging control;

- sponsor data connectivity including usage monitoring;

- AF-influenced traffic steering authorization;

- subscription and reporting of events for the event exposure;

- negotiations for future background data transfer.

The N30 reference point is defined for the interactions between PCF and NEF in the reference point representation.

#### **\*\*\*NEXT CHANGE\*\*\***

6.1.1.2.2 The Binding Support Function (BSF)

The BSF has the following characteristics:

- For a certain PDU Session, the BSF stores internally information about the user identity, the DNN, the UE (IP or MAC) address(es), the S-NSSAI, the selected PCF address and if available the associated PCF instance ID, PCF set ID and the level of binding (see clause 6.3.1.0 of TS 23.501 [2]).

NOTE 1: Only NF instance or NF set Level of Binding indication are supported at the BSF.

- The PCF registers, updates and removes the stored information in the BSF using the Nbsf management service operations defined in TS 23.502 [3].

- The PCF ensures that it is updated each time an IP address is allocated or de-allocated to the PDU Session or, for Ethernet PDU Sessions supporting binding of AF request based on MAC address, each time it has been detected that a MAC address is used or no more used by the UE in the PDU Session.

- Based on operator's policies and configuration, the PCF determines whether 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.

NOTE 2: This applies to usage monitoring.

- The selected PCF (if needed) downloads the user profile from the UDR as described in TS 23.502 [3] clause 4.16.4 step 2. If usage monitoring is enabled for the user, and based on operator's policies, the PCF checks if the BSF has already existing PCF serving the combination of SUPI, S-NSSAI, DNN.

- If no such PCF is found the PCF shall register itself to the BSF as described above in this clause.

- Else if an existing PCF is found for the above combination, the PCF shall return to the SMF the available information about the existing PCF and a redirection indication.

NOTE 3: The assumption is that for DNN, S-NSSAI combinations where usage monitoring be applied, the same BSF instance or the same BSF SET is selected for all UE PDU Sessions to the same DNN, S-NNSAI.

- For retrieval binding information, any NF, such as NEF or AF, that needs to discover the selected PCF address(es), and if available, the associated PCF instance ID, PCF set ID and level of binding (see clause 6.3.1.0 of TS 23.501 [2]) for the tuple (UE address, DNN, S-NSSAI, SUPI, GPSI) (or for a subset of this Tuple) uses the Nbsf management service discovery service operation defined in TS 23.502 [3].

- The NF may discover the BSF via NRF or based on local configuration. In the case of via NRF the BSF registers the NF profile in NRF. The Range(s) of UE IPv4 addresses, Range(s) of UE IPv6 prefixes supported by the BSF may be provided to NRF.

- If the NF received a PCF set ID or a PCF instance ID with an indication of level of binding as result of the Nbsf management service discovery service operation, it should use that information as NF set level or NF instance level Binding Indication to route requests to the PCF as defined in clause 6.3.1.0 of TS 23.501 [2] and according to the following provisions:

- For the NF set level of binding, the NF will receive a PCF set ID but no PCF instance ID. If an NF is not able to reach the received PCF address(es) and applies direct discovery, it should query the NRF for PCF instances within the PCF set and select another instance.

- For the NF instance level of binding, the NF will receive a PCF set ID and a PCF instance ID. If an NF is not able to reach the received PCF address(es) and applies direct discovery, it should query the NRF for PCF service instances within the PCF and select another instance.

- The NF should provide a Routing Binding Indication based on the received PCF set ID, level of binding and possible PCF instance ID in requests it sends to the PCF.

- For an ongoing NF service session, the PCF may provide Binding indication to the NF (see clause 6.3.1.0 of TS 23.501 [2]). This Binding indication shall then be used instead of any PCF information received from the BSF.

- If a new PCF instance is selected, the new PCF should invoke Nbsf\_Management\_Update service operation to update the binding information in BSF.

The BSF may be deployed standalone or may be collocated with other network functions, such as PCF, UDR, NRF, SMF.

NOTE 4: Collocation allows combined implementation.

#### **\*\*\*NEXT CHANGE\*\*\***

#### 6.1.1.3 Policy decisions based on network analytics

Policy decisions based on network analytics allow PCF to perform policy decisions taking into account the analytics information provided by the NWDAF. The PCF subscribes/unsubscribes to Analytics information as defined in TS 23.288 [24].

The following Analytics IDs are relevant for Policy decisions: "Load level information", "Service Experience", "Network Performance" and "Abnormal behaviour". The PCF may subscribe to notifications of network analytics related to "Load Level Information" using the Nnwdaf\_AnalyticsSubscription\_Subscribe service operation including the Analytics ID "Load level information", the Analytics Filter "S-NSSAI and NSI ID" and the Analytics Reporting Information set to a load level threshold value. The PCF is notified when the load level of the Network Slice Instance reaches the threshold, and then the PCF may verify if the RFSP index value needs to be modified for a SUPI for which an AM Policy Association is created; this is based on operator policies in the PCF, as defined in clause 6.1.2.1.

The PCF may subscribe to notifications of network analytics related to "Service Experience" using the Nnwdaf\_AnalyticsSubscription\_Subscribe service operation including the Analytics ID "Service Experience", the Target of Analytics Reporting "any UE" and the Analytics Filter including one or more "Application ID(s)". The PCF is notified on the Service Experience statistics or predictions including, for each Application Id, the list of SUPIs for which Service Experience is provided. In addition, both spatial and time validity may be provided as well as the confidence of the prediction. The PCF may check the 5QI values assigned to the Application, the number of UEs affected and may use this as input to calculate and update the authorized QoS for a service data flow template.

The NWDAF service to retrieve the service experience (i.e. the average observed Service MoS) is described in clause 6.4 of TS 23.288 [24].

The PCF may subscribe to notifications of network analytics related to "Network Performance" using the Nnwdaf\_AnalyticsSubscription\_Subscribe service operation including the Analytics ID "Network Performance", the Target of Analytics Reporting "Internal Group Id" and the Analytics Filter including the Area of Interest. The PCF is notified on the Network Performance statistics or predictions including the Area of Interest. In addition, the confidence of the prediction may be provided. The PCF may use this information as input to calculate the background data transfer policies that are negotiated with the ASP, as defined in clause 6.1.2.4.

The NWDAF services to retrieve "Network Performance" as described in clause 6.6 of TS 23.288 [24].

The PCF may subscribe to notifications of network analytics related to "Abnormal behaviour" using the Nnwdaf\_AnalyticsSubscription\_Subscribe service operation including the Analytics ID "Abnormal behaviour", the Target of Analytics Reporting "SUPI", "Internal Group Id" or "any UE" and the Analytics Filter including the expected analytics type or the list of Exceptions IDs and per each Exception Id a possible threshold and other Analytics Filter Information if needed. The list of Exception IDs is specified in TS 23.288 [24]. The PCF may use "Unexpected UE location" as input to determine the Service Area Restrictions defined in clause 6.1.2.1, "Suspicion of DDoS attack" or "Too frequent Service Access" to request the SMF to terminate the PDU Session as defined in clause 6.1.3.6, "Wrong destination address" to perform gating of a service data flow as defined in clause 6.1.3.6 and "Unexpected long-live/large rate flows" to perform QoS related policies such as gating or policing as defined in clause 6.2.1.1.

The NWDAF services to retrieve UE related analytics are described in clause 6.7 of TS 23.288 [24].

The PCF may also use the network analytics as input to its policy decision to apply operator defined actions for example for the UE context(s) or PDU Session(s).

#### **\*\*\*NEXT CHANGE\*\*\***

##### 6.1.2.2.1 General

The 5GC shall be able to provide policy information from the PCF to the UE. Such UE policy information includes:

1) Access Network Discovery & Selection Policy (ANDSP): It is used by the UE for selecting non-3GPP accesses and for selection of the N3IWF in the PLMN. The structure and the content of this policy are specified in clause 6.6.1.

2) UE Route Selection Policy (URSP): This policy is used by the UE to determine if a detected application can be associated to an established PDU Session, can be offloaded to non-3GPP access outside a PDU Session, or can trigger the establishment of a new PDU Session. The structure and the content of this policy are specified in clause 6.6.2. A URSP rule includes one Traffic descriptor that specifies the matching criteria and one or more of the following components:

2a) SSC Mode Selection Policy (SSCMSP): This is used by the UE to associate the matching application with SSC modes.

2b) Network Slice Selection Policy (NSSP): This is used by the UE to associate the matching application with S-NSSAI.

2c) DNN Selection Policy: This is used by the UE to associate the matching application with DNN.

2d) PDU Session Type Policy: This is used by the UE to associate the matching application with a PDU Session Type.

2e) Non-Seamless Offload Policy: This is used by the UE to determine that the matching application should be non-seamlessly offloaded to non-3GPP access (i.e. outside of a PDU Session).

2f) Access Type preference: If the UE needs to establish a PDU Session for the matching application, this indicates the preferred Access Type (3GPP or non-3GPP or Multi-Access).

3) V2X Policy (V2XP): This policy provides configuration parameters to the UE for V2X communication over PC5 reference point or over Uu reference point or both. V2X Policies are defined in clause 5.1.2.1 and clause 5.1.3.1 of TS 23.287 [28].

The ANDSP and URSP may be pre-configured in the UE or may be provisioned to UE from PCF. The pre-configured policy shall be applied by the UE only when it has not received the same type of policy from PCF.

The methods of configuring V2XP to the UE, including (pre-)configuration and provisioning, and the priority of the same type of parameters acquired from different sources are defined in clause 5.1.1 of TS 23.287 [28].

The PCF selects the UE policy information applicable for each UE based on local configuration, and operator policies taking into consideration the information defined in clause 6.2.1.2.

In the case of a roaming UE, the V-PCF may retrieve UE policy information from the H-PCF over N24/Npcf. When the UE is roaming and the UE has valid rules from both HPLMN and VPLMN the UE gives priority to the valid ANDSP rules from the VPLMN.

The UE policy information shall be provided from the PCF to the AMF via N15/Namf interface and then from AMF to the UE via the N1 interface as described in TS 23.502 [3] clause 4.2.4.3. The AMF shall not change the UE policy information provided by PCF.

The PCF is responsible for delivery of UE policy. If the PCF is notified about UE policy information delivery failure (e.g. because of UE unreachable), the PCF may provide a new trigger "Connectivity state changes" in Policy Control Request Trigger of UE Policy Association to AMF as defined in TS 23.502 [3] clause 4.16.12.2. After reception of the Notify message indicating that the UE enters the CM-Connected state, the PCF may retry to deliver the UE policy information.

NOTE 1: For backward compatibility the PCF may subscribe the "Connectivity state changes (IDLE or CONNECTED)" event in Rel-15 AMF as defined in TS 23.502 [3] clause 5.2.2.3.

If due to UE Local Configurations, a UE application requests a network connection using Non-Seamless Offload, the UE shall use Non-Seamless Offload for this application without evaluating the URSP rules. Otherwise, the UE shall select the PDU Session or Non-Seamless Offload in the following order:

- If the UE has an URSP rule (except the URSP rule with the "match all" Traffic descriptor) that matches the application as defined in clause 6.6.2.3, the UE shall perform the association of the application to the corresponding PDU Session or to Non-Seamless Offload according to this rule; Otherwise,

- If no URSP rule is applicable for the application (except the URSP rule with the "match all" Traffic descriptor), the UE shall perform the association of the application to a PDU Session according to the applicable UE Local Configurations, if any. If the UE attempts to establish a new PDU session according to the UE Local Configurations and this PDU Session Establishment request is rejected by the network, then the UE shall perform the association of the application to a PDU Session or to Non-Seamless Offload according to the URSP rule with the "match all" Traffic descriptor; Otherwise,

NOTE 2: It is assumed that the S-NSSAI(s) in the UE Local Configurations are operator-provided S-NSSAI(s). The provision of the S-NSSAI(s) is not specified.

NOTE 3: The application layer is not allowed to set the S-NSSAI when the UE establishes a PDU Session based on the UE Local Configurations.

NOTE 4: Any missing information in the UE Local Configurations needed to build the PDU Session Establishment request can be the appropriate corresponding component from the URSP rule with the "match all" Traffic descriptor.

- If neither the UE Local Configurations nor the URSP rules are applicable for the application (except the URSP rule with the "match all" Traffic descriptor), the UE shall perform the association of the application to a PDU Session or to Non-Seamless Offload according to the URSP rule with the "match all" Traffic descriptor.

For the existing PDU Session(s), the UE shall examine the URSP rules within the UE policy information in order to determine whether the existing PDU Session(s) (if any) are maintained or not. If not, then the UE may initiate a PDU Session release procedure for the PDU Session(s) that cannot be maintained.

If there are multiple IPv6 prefixes within the PDU Session, then the IPv6 multi-homed routing rules, described in clause 5.8.2.2.2 in TS 23.501 [2], on the UE shall be used to select which IPv6 prefix to route the traffic of the application.

NOTE 5: For the case that an application cannot be associated to any PDU Session, the UE can inform the application that association of the application to PDU Session fails.

#### **\*\*\*NEXT CHANGE\*\*\***

##### 6.1.2.2.2 Distribution of the policies to UE

The UE policy control enables the PCF to provide UE access selection related policy information, PDU Session related policy information and V2X Policy information to the UE, i.e. UE policies, that includes Access network discovery & selection policy (ANDSP) or UE Route Selection Policy (URSP) or V2X Policy (V2XP) or their combinations using Npcf and Namf service operations.

The PCF may be triggered to provide the UE policy information during UE Policy Association Establishment and UE Policy Association Modification procedures as defined in clause 4.16.11 and clause 4.16.12 of TS 23.502 [3].

NOTE 1: The PCF can install a PCC Rule and activate start and stop of application detection in the SMF. When the same PCF is selected for SM policy association control and UE policy association control, THE reporting of start and stop of an application can trigger the installation or update of a URSP rule in the UE to send the application traffic to the PDU Session as defined in the URSP rule.

NOTE 2: The PCF can subscribe to the UDR on Service specific information change, which will be taken into consideration by the PCF to determine the updated V2XP as defined in clause 4.15.6.7 of TS 23.502 [3].

Operator defined policies in the PCF may depend on input data such as UE location, time of day, information provided by other NFs, etc. as defined in clause 6.2.1.2.

The PCF includes the UE policy information delivered to the UE into a Policy Section identified by a Policy Section Identifier (PSI). The PCF may divide the UE policy information into different Policy Sections, each one identified by a PSI. Each Policy Section provides a list of self-contained UE policy information to the UE, via AMF. The PCF ensures that a Policy Section is under a predefined size limit, known by the PCF.

NOTE 3: The size limit to allow the policy information to be delivered using NAS transport is specified in TS 29.507 [13]. The size limit is configured in the PCF.

A list of self-contained UE policy information implies that:

- when the PCF delivers URSP rules to the UE, the PCF provides the list of URSP rules in the order of precedence and without splitting a URSP rule across Policy Sections;

- when the PCF delivers V2XP to the UE, the PCF provides the list of V2XP in the order of precedence and without splitting a V2XP across Policy Sections;

- when the PCF delivers WLANSP rules, the list of WLANSP rules are provided in the order of priority and without splitting a WLANSP rule across Policy Sections;

- when the PCF delivers the non-3GPP access network selection information, the whole list of non-3GPP access network selection information (as defined in clause 6.6.1.1) is provided in one Policy Section.

It is up to PCF decision how to divide the UE policy information into Policy Sections as long as the requirements for the predefined size limit and the self-contained content (described above) are fulfilled.

NOTE 4: The Policy Section list can be different per user. One PSI and its corresponding content can be the same for one or more users.

NOTE 5: The PCF may, for example, assign the URSP as one whole Policy Section, or it may subdivide the information in the URSP into multiple Policy Sections by assigning one or several URSP rules to each Policy Section.

The PLMN ID is provided to the UE together with UE policy information and it is used to indicate which PLMN a Policy Section list belongs to.

The AMF forwards the UE policy information transparently to the UE. If the (H-)PCF decides to split the UE policies to be sent to the UE, the PCF provides multiple Policy Sections separately to the AMF and then AMF uses UE configuration Update procedure for transparent UE policies delivery procedure to deliver the policies to the UE, this is defined in TS 23.502 [3] clause 4.2.4.3 and clause 4.16.

NOTE 6: The AMF does not need to understand the content of the UE policy, rather send them to the UE for storage.

The UE shall update the stored UE policy information with the one provided by the PCF as follows (details are specified in TS 24.501 [22]):

- If the UE has no Policy Sections with the same PSI, the UE stores the Policy Section;

- If the UE has an existing Policy Section with the same PSI, the UE replaces the stored Policy Section with the received information;

- The UE removes the stored Policy Section if the received information contains only the PSI.

The UE keeps the received UE policies stored even when registering in another PLMN. The number of UE policies to be kept stored in the UE for PLMNs other than the HPLMN is up to UE implementation. If necessary, e.g. the number of UE policies stored in UE for PLMNs exceeds the maximum value, the UE may remove earlier stored UE policy in UE.

The ANDSP for VPLMN, if provided within the UE policy in the UE Configuration Update procedure described in TS 23.502 [3] clause 4.2.4.3, applies to the equivalent PLMN(s) indicated in the last received list of equivalent PLMNs in Registration Accept.

At Initial Registration or the Registration to 5GS when the UE moves from EPS to 5GS:

- The UE provides the list of stored PSIs which identify the Policy Sections associated to the home PLMN and the visited PLMN (if the UE is roaming) that are currently stored in the UE. If USIM is changed, the UE does not provide any PSI. If no policies are stored in the UE for the home PLMN, the UE does not provide any PSI associated to the home PLMN. If the UE is roaming and has policies for the home PLMN but no associated policies for the visited PLMN the UE includes only the list of PSIs associated to the home PLMN.

- UE may indicate its ANDSP support to the PCF. If it is received, the PCF shall take it into account for the determination on whether to provide the ANDSP to the UE. The PCF does not provide ANDSP rules to the UE if the UE does not indicate support for ANDSP.

- UE may indicate the V2X Policy Provisioning Request in the UE Policy Container. If this indication is received, the PCF includes V2XP in the UE policy information as defined in clause 6.2.2 of TS 23.287 [28].

- The UE may also provide the OSId.

The UE may trigger an Initial registration with the list of stored PSIs to request a synchronization for example if the UE powers up without USIM being changed.

During Initial Registration, the (H-)PCF retrieves the list of PSIs and its content stored in the (H-)UDR for this SUPI while the V-PCF (in the roaming scenario) retrieves the list of PSIs and its content stored in the V-UDR for the PLMN ID of this UE (alternatively, the V-PCF can have this information configured locally).

NOTE 7: The PSI list and content stored/configured for a PLMN ID can be structured according to e.g. location areas (e.g. TAs, PRAs). The V-PCF can then provide PSIs and its content only if they correspond to the current UE location.

In the roaming scenario, the V-PCF shall also forward any UE provided PSIs that are associated to the home PLMN to the H-PCF.

When the PCF (i.e. the (H-)PCF as well as the V-PCF) receives a list of PSIs associated to the PLMN of the PCF from the UE, the PCF compares the list of PSIs provided by the UE and the list of PSIs retrieved from the UDR. In addition, the PCF checks whether the list of PSIs provided by the UE or its content needs to be updated according to operator policies, e.g. change of Location and/or time. If the two lists of PSIs are different or an update is necessary according to operator policies (which includes the case that the UE did not provide a list of PSIs associated to the PLMN of the PCF), the PCF provides the changes in the list of PSIs or the corresponding content to the AMF which forwards them to the UE.

The (H-)PCF maintains the latest list of PSIs delivered to each UE as part of the information related to the Policy Association until the UE policy association termination request is received from the AMF. Then the (H-)PCF stores the latest list of PSIs and its contents in the (H-)UDR using the Nudr\_DM\_Update including DataSet "Policy Data" and Data Subset "Policy Set Entry".

The (H-)PCF may use the PEI provided by the AMF and/or the OSId provided by the UE, to determine the operating system of the UE.

If the PEI, the OSId or the indication of UE support for ANDSP is available to the PCF, the PCF stores them in the UDR using Nudr\_DM\_Create including DataSet "Policy Data" and Data Subset "UE context policy control data" when such information is received from the UE in the UE Policy Container.

If the (H-)PCF is not able to determine the operating system of the UE, and if the (H-)PCF requires to deliver URSP rules that contain Application descriptors as Traffic Descriptors, then the Traffic Descriptors of such URSP rules include multiple instances of Application descriptors each associated to supported UE operating systems by the network operator implementation.

If the (H-)PCF determines the operating system of the UE and if the (H-)PCF requires to deliver URSP rules that contain Application descriptors as Traffic Descriptors, then the Traffic Descriptors of such URSP rules include the Application descriptors associated with the operating system determined by the PCF.

NOTE 8: If the PCF does not take into account the received PEI and/or OSId then the PCF can send URSP rules containing application traffic descriptors associated to multiple operating systems.

#### **\*\*\*NEXT CHANGE\*\*\***

##### 6.1.2.3.1 PFD management

The Management of Packet Flow Descriptions enables the UPF to perform accurate application detection when PFD(s) are provided by an ASP and then to apply enforcement actions as instructed in the PCC Rule.

The operator is able to configure pre-defined PCC Rules in the SMF or dynamic PCC Rules in the PCF that include at least an application identifier for service data flow detection, charging control information, i.e. charging key and optionally the Sponsor identifier or the ASP identifier or both. Depending on the service level agreements between the operator and the Application Server Provider, it may be possible for the ASP to provide individual PFDs or the full set of PFDs for each application identifier maintained by the ASP to the SMF via the PFD Management service in the NEF (PFDF). The PFDs become part of the application detection filters in the SMF/UPF and therefore are used as part of the logic to detect traffic generated by an application. The ASP may remove or modify some or all of the PFDs which have been provided previously for one or more application identifiers. The SMF may report the application stop to the PCF for an application instance identifier as defined in clause 5.8.2.8.4 of TS 23.501 [2] if the removed/modified PFD in SMF/UPF results in that the stop of the application instance is not being able to be detected.

NOTE 1: PFD management is optionally supported in the NEF and the SMF.

The ASP manages (provision, update, delete) the PFDs through the NEF (PFDF). The PFD(s) are transferred to the SMF through the NEF (PFDF). The PFDF is a logical functionality in the NEF which receives PFD(s) from the ASP through the NEF, stores the PFD(s) in the UDR and provides the PFD(s) to the SMF(s) either on the request from ASP PFD management through NEF (PFDF) (push mode) or on the request from SMF (pull mode). The PFDF functionality is a service provided by the NEF.

The ASP may provide/update/remove PFDs with an allowed delay to the NEF (PFDF). Upon reception of the request from the ASP, the NEF (PFDF) shall check if the ASP is authorized to provide/update/remove those PFD(s) and request the allowed delay. The NEF (PFDF) may be configured with a minimum allowed delay based on SLA to authorize the allowed delay provided by the ASP. When ASP and requested allowed delay are successfully authorized, the NEF (PFDF) shall translate each external application identifier to the corresponding application identifier known in the core network. The NEF (PFDF) stores the PDF(s) into the UDR.

NOTE 2: The Allowed Delay is an optional parameter. If the Allowed Delay is included, it indicates that the requested PFD(s) should be deployed within the time interval indicated by the Allowed Delay.

The PFDs may be retrieved by SMF from NEF (PFDF) in "pull" mode or may be provisioned from NEF (PFDF) to the SMF in "push" mode.

When the "push" mode is used, the NEF (PFDF) retrieves from the UDR the PFDs for each application identifier and distributes them to those SMFs that enable access to those applications. The NEF (PFDF) may be configured with the list of SMFs where PFD(s) should be distributed. There are three methods to provision PFD(s) from the NEF (PFDF) to the SMF:

a) Push of whole PFD(s) that can be accessed by the NEF (PFDF) according to operator configuration in NEF (PFDF) (e.g., provision per day according to operator configuration);

b) Selective push of an ASP change in the PFD set (i.e. ASP changes the PFD set while operator configuration defines when to push);

c) Selective push of an ASP change in the PFD set according to ASP request (i.e. ASP indicates to push changes in a PFD set within the time interval indicated by the Allowed Delay).

When the "pull" mode is used, at the time a PCC Rule with an application identifier for which PFDs are not available is activated or provisioned, the SMF requests all PFDs for that application identifier from the NEF (PFDF), and NEF (PFDF) retrieves them from the UDR. The PFD(s) retrieved for an application identifier from the NEF (PFDF) are cached in the SMF, and the SMF maintains a caching timer associated to the PFD(s) to control how long the PFD(s) are valid. When the caching timer expires:

- If there are still active PCC rules that refer to the corresponding application identifier, the SMF reloads the PFD(s) from the NEF (PFDF) and provides it to the UPF over N4;

- If there's no active PCC rule that refers to the corresponding application identifier or the SMF removes the last PCC rule that refers to the corresponding application identifier, the SMF removes the PFD(s) identified by the application identifier and informs the UPF to remove the PFD(s) identified by the application identifier over N4.

NOTE 3: It is assumed that all SMF(s) and PFD (s) in an operator network are configured with the same default caching time value to be applied for all application identifiers.

When the "pull" mode is used, the NEF (PFDF) may provide to the SMF a caching time value per application identifier. The SMF receives the caching time value together with the PFD(s) from the NEF (PFDF) over N29 and applies this value for the application identifier instead of the configured default caching time value. If no caching time value is received from NEF (PFDF), the SMF uses the configured default caching time value.

NOTE 4: The configuration of a caching time value per application identifier in NEF (PFDF) is based on the SLA between the operator and the ASP.

When only "pull" mode is supported in one PLMN, if the Allowed Delay is shorter than the caching time value stored for this application identifier, or shorter than the default caching time if no application-specific caching time is stored, the NEF (PFDF) may still store the PFD(s) to the UDR. The NEF (PFDF) shall provide an indication that the PFD(s) were stored and the caching time value to the ASP when informing that the Allowed Delay could not be met.

When either "pull" mode or "push" mode is used, if there's any update of the PFD(s) received and there are still active application detection rules in the UPF for the application identifier, the SMF shall provision the updated PFD set corresponding to the application identifier to the UPF.

NOTE 5: SMF should assure not to overload N4 signalling while managing PFD(s) to the UPF, e.g. forwarding the PFD(s) to the right UPF where the PFD(s) is enforced.

When the UPF receives the updated PFD(s) from either the same or different SMF for the same application identifier, the latest received PFD(s) shall overwrite any existing PFD(s) stored in the UPF.

If the PFDs are managed by local O&M procedures, PFD retrieval is not used; otherwise, the PFDs retrieved from NEF (PFDF) overrides any PFDs pre-configured in the SMF. The SMF shall manage the pre-configured PFDs and PFDs provided by the NEF (PFDF) at the UPF as defined in clause 5.8.2.8.4 of TS 23.501 [2]. The SMF may differentiate the need for PFD retrieval based on operator configuration in the SMF.

The AF requests including an application identifier may trigger the activation or provisioning of a PCC Rule in the SMF by the PCF based on operator policies.

#### **\*\*\*NEXT CHANGE\*\*\***

#### 6.1.2.4 Negotiation for future background data transfer

The AF may contact the PCF via the NEF (and Npcf\_BDTPolicyControl\_Create service operation) to request a time window and related conditions for future background data transfer.

NOTE 1: The NEF may contact any PCF in the operator network.

The AF request shall contain an ASP identifier, the volume of data to be transferred per UE, the expected amount of UEs, the desired time window, the External Group Identifier and optionally, Network Area Information, MAC address or IP 3-tuple to identify the Application server, request for notification. The AF provides as Network Area Information either a geographical area (e.g. a civic address or shapes), or an area of interest that includes a list of TAs or list of NG-RAN nodes and/or a list of cell identifiers. When the AF provides a geographical area, then the NEF maps it based on local configuration into of a short list of TAs and/or NG-RAN nodes and/or cells identifiers that is provided to the PCF. The NEF may map the ASP id based on local configuration into the DNN, S-NSSAI that is provided to the PCF. The request for notification is an indication that the ASP accepts that the BDT policy can be re-negotiated using the BDT warning notification procedure described in clause 4.16.7.3 of TS 23.502 [3].

NOTE 2: A 3rd party application server is typically not able to provide any specific network area information and if so, the AF request is for the whole operator network.

The PCF shall first retrieve all existing BDT policies stored for any ASP from the UDR. The PCF may retrieve analytics on "Network Performance" from NWDAF following the procedure and services described in TS 23.288 [24]. Afterwards, the PCF shall determine, based on the information provided by the AF, the analytics on "Network Performance" if available and other available information (e.g. network policy and existing BDT policies) one or more BDT policies. The PCF may be configured to map the ASP identifier into a target DNN and slicing information (i.e. S-NSSAI), that is used if the NEF did not provide the DNN, S-NSSAI to the PCF.

A BDT policy consists of a recommended time window for the background data transfer, a reference to a charging rate for this time window and optionally a maximum aggregated bitrate (indicating that the charging according to the referenced charging rate is only applicable for the aggregated traffic of all involved UEs that stays below this value). Finally, the PCF shall provide the candidate list of BDT policies or the selected BDT policy to the AF via NEF together with the Background Data Transfer Reference ID. If the AF received more than one BDT policy, the AF shall select one of them and inform the PCF about the selected BDT policy.

NOTE 3: The maximum aggregated bitrate (optionally provided in a BDT policy) is not enforced in the network. The operator may apply offline CDRs processing (e.g. combining the accounted volume of the involved UEs for the time window) to determine whether the maximum aggregated bitrate for the set of UEs was exceeded by the ASP and charge the excess traffic differently.

NOTE 4: It is assumed that the 3rd party application server is configured to understand the reference to a charging rate based on the agreement with the operator.

The selected BDT policy together with the Background Data Transfer Reference ID, the volume of data to be transferred per UE, the expected amount of UEs, ASP Id, MAC address or IP 3-tuple to identify the Application server, the one or more route selection component (DNN, S-NSSAI), the desired time window, the Network Area Information (if provided by the AF) and whether the AF accepts BDT policy re-negotiation or not is stored by the PCF in the UDR as Data Set "Policy Data" and Data Subset "Background Data Transfer data". The same or a different PCF can retrieve this BDT policy and corresponding related information from the UDR and take them into account for future decisions about BDT policies related to the same or other ASPs.

When the AF wants to apply the BDT Policy to an existing session, then the AF will, at the time the background data transfer is about to start, provide, for each UE, the Background Data Transfer Reference ID together with the AF session information to the PCF (via the N5 interface). The PCF retrieves the corresponding BDT policy from Policy Data Set in the UDR and derives the PCC rules for the background data transfer according to this transfer policy.

When the AF wants to apply the BDT Policy to a future session, then the AF provides, to the NEF, the Background Data Transfer Reference ID together with the External Identifier (i.e. GPSI) or External Group Identifier of the UE(s) that are to be subject to the policy. The NEF translates the External Group Identifier into the Internal Group Identifier or the External Identifier into a SUPI. The NEF stores the Background Data Transfer Reference ID, in the UDR as Application Data Set and Background Data transfer data Subset for an Internal Group Identifier or a SUPI and the ASP id requesting to apply BDT Policy to a future session for the UE(s). A PCF that serves the UE(s) (i.e. the PCF that serves the UE for UE Policies) may retrieve the Background Data Transfer Reference ID by retrieving the UE's Application Data from the UDR or by subscribing to notifications of changes to the UEs' Application Data in the UDR. Furthermore, the PCF retrieves the specific BDT Policy and if available MAC address or IP 3-tuple to identify the Application server based on the received Background Data Transfer Reference ID stored as Policy Data Set from the UDR.

When the PCF determines to send the BDT Policy information to the UE as part of a URSP rule, the PCF will store the policy in the UDR as part of the UE's Policy Set Entry and will use the associated S-NSSAI and DNN associated with the ASP id stored in the Application Data to store the Background Data Transfer Reference ID in the UE's PDU Session policy control subscription information (see clause 6.2.1.3). The PCF uses local policies to decide if and when the BDT Policy information is going to be sent to the UE as Validation Criteria in the RSD part of the URSP rule (see clause 6.6.2.1). The UE uses Validation Criteria to determine whether or not a PDU Session should be established. The Time Window and Location Criteria are not required to be checked again during the lifetime of the PDU Session.

The PCF may, based on operator configuration, trigger the UE Configuration Update procedure when the policy is selected, or the PCF may wait until receiving a notification from the AMF that the UE has entered the Tracking Area or Presence Area where the policy applies, and/or the PCF may wait until the time window when the policy applies is approaching. The UE's support of the Validation Criteria in a URSP rule is optional.

NOTE 5: If a non-supporting UE receives Validation Criteria, it ignores the URSP rule.

When the PDU Session is established, the PCF that serves the PDU Session will use the Background Data Transfer Reference ID in the UE's PDU Session policy control subscription information (see clause 6.2.1.3) to retrieve the corresponding BDT policy (i.e. Time Window and/or Location Criteria) from the UDR and derives the PCC rules for the background data transfer according to this transfer policy.

NOTE 6: The AF will typically contact the PCF for the individual UEs to request sponsored connectivity for the background data transfer.

NOTE 7: A transfer policy is only valid until the end of its time window. The removal of outdated transfer policies from the UDR is up to implementation.

The PCF may reject corresponding SM Policy Association, as described in clause 4.16.4 of TS 23.502 [3], if Validation condition is not satisfied. And based on this feedback, SMF will reject the PDU Session setup.

After successful PDU Session setup, PCF may trigger PDU Session release when Validation condition is not satisfied.

The PCF may subscribe to analytics on "Network Performance" from NWDAF for the area of interest and time window of a BDT policy following the procedure and services described in TS 23.288 [24]. When the PCF gets a notification from the NWDAF that the network performance in the area of interest and time window goes below the criteria set by the operator, the PCF may try to re-negotiate the affected BDT policies with AFs that accepted BDT policy re-negotiation. To do this, the PCF retrieves all the BDT policies together with their additionally stored AF provided information (e.g. their corresponding desired time window) from the UDR, identifies the BDT policies that are not desirable anymore due to the degradation of the network performance and tries to calculate new candidate BDT policies for the ASP(s) to select from. If the PCF does not find any new candidate BDT policy or the related AF did not accept BDT policy re-negotiation, the previously negotiated BDT policy shall be kept and no interaction with the ASP shall occur. If the PCF finds one or more new candidate BDT policies, the PCF notifies the related ASP(s) on both the BDT policy that is not valid any longer and the candidate BDT policies via NEF.

The PCF invalidates the BDT policy stored in the UDR for the corresponding background data transfer reference ID while the BDT policy re-negotiation is ongoing. The PCF shall reject a PDU Session request corresponding to an invalid BDT policy.

When the AF receives the notification, the AF may select one of the BDT policies included in the candidate list, and then inform the PCF about the selected BDT policy. The PCF stores the newly selected BDT policy into the UDR for the corresponding Background Data Transfer Reference ID and removes the BDT policy that is no longer valid. As a consequence, the PCF identifies the UEs for which the BDT policy was already applied and updates URSP rules with the new Validation Criteria as described in clause 4.16.12.2 of TS 23.502 [3].

NOTE 8: A PCF can subscribe to notifications on changes in BDT policy in UDR. Upon reception of such notification the PCF has also to identify the UEs for which the BDT policy was already applied and update URSP rules with the new Validation Criteria as described in clause 4.16.12.2 of TS 23.502 [3].

If the AF does not select one of the BDT policies included in the candidate list, the PCF removes the BDT policy stored in the UDR together with the corresponding Background Data Transfer Reference ID and all related information. As a consequence, the PCF identifies the UEs for which the BDT policy was already applied and removes the URSP rules corresponding to the BDT policy using the procedure described in clause 4.16.12.2 of TS 23.502 [3].

NOTE 9: The PCF can also remove the no longer valid BDT policy after an operator configurable time for the case that the AF does not respond.

#### **\*\*\*NEXT CHANGE\*\*\***

##### 6.1.3.2.1 General

The binding mechanism is the procedure that associates a service data flow (defined in a PCC rule by means of the SDF template), to the QoS Flow deemed to transport the service data flow. For service data flows belonging to AF sessions, the binding mechanism shall also associate the AF session information with the QoS Flow that is selected to carry the service data flow.

NOTE 1: The relation between AF sessions and rules depends only on the operator configuration. An AF session can be covered by one or more PCC rules, if applicable (e.g. one rule per media component of an IMS session).

NOTE 2: The PCF may authorize dynamic PCC rules for service data flows without a corresponding AF session.

The binding mechanism includes three steps:

1. Session binding;

2. PCC rule authorization; and

3. QoS Flow binding.

#### **\*\*\*NEXT CHANGE\*\*\***

#### **\*\*\*NEXT CHANGE\*\*\***

#### 6.1.3.4 Credit management

The credit management applies only for service data flow with online charging method and shall operate on a per charging key basis. The SMF should initiate one charging session with the CHF for each PDU Session subject to charging, in order to perform credit management within the charging session.

NOTE 1: Independent credit control for an individual service/application may be achieved by assigning a unique charging key value in the corresponding PCC rule.

The SMF shall request a quota for each charging key occurring in a PCC rule. It shall be up to operator configuration whether the SMF shall request quota in conjunction with the PCC rule being activated or when the first packet corresponding to the service is detected. The CHF may either grant or deny the request for quota. The CHF shall strictly control the rating decisions.

NOTE 2: The term quota as used here does not imply actual monetary credit, but an abstract measure of resources available to the user. The relationship between this abstract measure, actual money, and actual network resources or data transfer, is controlled by the CHF.

During PDU Session establishment and modification, the SMF shall request quota using the information after applying policy enforcement action (e.g. upgraded or downgraded QoS information), if applicable, even though the SMF has not signalled this information to the AMF or RAN.

The events trigger information which may be received from the CHF, causing the SMF to perform a usage reporting and quota request to CHF when the event occurs are specified in TS 32.255 [21].

The CHF may subscribe to Change of UE presence in Presence Reporting Area at any time during the life time of the charging session as described in TS 32.255 [21].

If the PCF set the ‘Out of credit’ event trigger (see clause 6.1.3.5), the SMF shall inform the PCF about the PCC rules for which credit is no longer available together with the applied termination action.

#### **\*\*\*NEXT CHANGE\*\*\***

#### 6.1.3.6 Policy control

QoS control refers to the authorization and enforcement of the maximum QoS that is authorized for a service data flow, for a QoS Flow or for the PDU Session. A service data flow may be either of IP type or of Ethernet type. PDU Sessions may be of IP type or Ethernet type or unstructured.

The PCF, in a dynamic PCC Rule, associates a service data flow template to an authorized QoS that is provided in a PCC Rule to the SMF. The PCF may also activate a pre-defined PCC Rule that contains that association.

The authorized QoS for a service data flow template shall include a 5QI and the ARP. For a 5QI of GBR or Delay-critical GBR resource type, the authorized QoS shall also include the MBR, GBR and may include the QoS Notification Control parameter (for notifications when authorized GFBR can no longer ( or can again) be fulfilled). For 5QI of Non-GBR resource type, the authorized QoS may include the MBR and the Reflective QoS Control parameter. The 5QI value can be standardized (i.e. referring to QoS characteristics as defined in TS 23.501 [2] clause 5.7.3), pre-configured (i.e. referring to QoS characteristics configured in the RAN) or dynamically assigned (i.e. referring to QoS characteristics provided by the PCF as Explicitly signalled QoS Characteristics in the PDU Session related policy information described in clause 6.4).

NOTE 1: Further details, special cases and additional parameters are described in clause 6.3.1.

QoS control also refers to the authorization and enforcement of the Session-AMBR and default 5QI/ARP combination. The PCF may provide the Authorized Session-AMBR and the Authorized default 5QI and ARP combination as part of the PDU Session information for the PDU Session to the SMF. The Authorized Session-AMBR and Authorized default 5QI/ARP values takes precedence over other values locally configured or received at the SMF.

For policy control, the AF interacts with the PCF and the PCF interacts with the SMF as instructed by the AF. For certain events related to policy control, the AF shall be able to give instructions to the PCF to act on its own, i.e. based on the service information currently available. The following events are subject to instructions from the AF:

- The authorization of the service based on incomplete service information;

NOTE 2: The QoS authorization based on incomplete service information is required for e.g. IMS session setup scenarios with available resources on originating side and a need for resource reservation on terminating side.

- The immediate authorization of the service;

- The gate control (i.e. whether there is a common gate handling per AF session or an individual gate handling per AF session component required);

- The forwarding of QoS Flow level information or events (see clause 6.1.3.18).

To enable the binding functionality, the UE and the AF shall provide all available flow description information (e.g. source and destination IP address and port numbers and the protocol information).

#### **\*\*\*NEXT CHANGE\*\*\***

#### 6.1.3.17 Policy decisions based on spending limits

Policy decisions based on spending limits is a function that allows PCF taking actions related to the status of policy counters that are maintained in the CHF.

The PCF uses the CHF selection mechanism defined in TS 23.501 [2] to select the CHF that provides policy counters for spending limits for a PDU Session. The PCF shall also provide the selected CHF address(es) to the SMF in the PDU Session related policy information.

The identifiers of the policy counters that are relevant for a policy decision in the PCF may be stored in the PCF or possibly in UDR. The PCF is configured with the actions associated with the policy counter status that is received from CHF.

The PCF may retrieve the status of policy counters in the CHF using the Initial or Intermediate Spending Limit Report Retrieval Procedure. The CHF provides the current status of the policy counters to the PCF. The CHF may in addition provide one or more pending statuses for a policy counter together with the time they have to be applied. The PCF shall immediately apply the current status of a policy counter. A pending status of a policy counter shall autonomously become the current status of a policy counter at the PCF when the indicated corresponding time is reached. Subsequently provided information for pending statuses of a policy counter shall overwrite the previously received information.

The PCF may subscribe to spending limit reporting for policy counters from the CHF using the Initial or Intermediate Spending Limit Report Retrieval procedure. If spending limit reporting for a policy counter is enabled, the CHF shall notify the PCF of changes in the status of this policy counter (e.g. daily spending limit of $2 reached) and optionally pending statuses of this policy counter together with their activation time (e.g. due to a billing period that will expire at midnight). The PCF may cancel spending limit reporting for specific policy counter(s) using the Intermediate Spending Limit Report Retrieval procedure, or for all policy counter(s) using the Final Spending Limit Report Retrieval procedure.

The PCF uses the status of each relevant policy counter, and optional pending policy counter statuses if known, as input to its policy decision to apply operator defined actions, e.g. change the QoS (e.g. downgrade Session-AMBR), modify the PCC Rules to apply gating or change charging conditions.

The CHF may report to the PCF the removal of the subscriber from the CHF system, and the PCF shall remove all the policy counters of the subscriber accordingly.

#### **\*\*\*NEXT CHANGE\*\*\***

#### 6.1.3.20 Access Traffic Steering, Switching and Splitting

As specified in TS 23.501 [2], the Access Traffic Steering, Switching and Splitting (ATSSS) feature is an optional feature that may be supported by the UE and the 5GC network. The ATSSS feature enables a multi-access PDU Connectivity Service, which can exchange PDUs between the UE and a data network by simultaneously using one 3GPP access network and one non-3GPP access network.

The PCF is informed of the ATSSS capabilities of a MA PDU Session by the SMF, as defined in TS 23.501 [2] clause 5.32.2. The ATSSS capabilities are both the Steering Mode and the Steering Functionality.

The PCF control of Access Traffic Steering, Switching and Splitting for a detected service data flow (SDF) is enabled by including Multi-Access PDU (MA PDU) Session Control information in the PCC rule. This allows the PCF to control:

- The Steering Mode that is used to steer/switch/split the detected SDF. The available Steering Modes are defined in TS 23.501 [2].

- The Steering Functionality that is used for the detected SDF, e.g. the MPTCP functionality or the ATSSS-LL functionality defined in TS 23.501 [2].

- Charging information depending on what Access Type is used for a detected SDF.

- Usage Monitoring information depending on what Access Type is used for a detected SDF.

The rest of the information in the PCC Rule apply to the SDF as such and are not dependent on what Access Type is used for a packet.

The MA PDU Session Control information in the PCC rules is used by the SMF in order to create applicable N4 rules for the UPF and ATSSS rules for the UE, as described in TS 23.501 [2]. The ATSSS rules are sent to UE via NAS when the MA PDU Session is created or updated by the SMF/PCF, as described in TS 23.501 [2] and TS 23.502 [3].

When MA PDU Session Control Information is provided to the SMF within a PCC Rule, the (H-)PCF provides both the Service Data Flow templates to identify a Service Data Flow in the UPF and if the Service Data Flow template includes an application identifier, then the corresponding application descriptors to identify the application traffic in the UE is also included.

The (H-) PCF may use the OSid stored in the UDR as DataSet "Policy Data" and Data Subset "UE context policy control data" to determine the OSAppId supported by the OSid. The (H-)PCF may also provide multiple application descriptors to identify application traffic in the UE, this is determined by the (H-)PCF local policies that indicates e.g. the operating system supported by the UE. If no OSid is available in the UDR, the (H-)PCF may use the PEI to determine the OSid supported by the UE.

NOTE 1: If the (H-)PCF does not take into account the received PEI and/or OSId then the (H-)PCF can send PCC rules containing application traffic descriptors associated to multiple operating systems.

The Traffic Descriptor in the ATSSS rule is generated by the SMF from the SDF template of the PCC rule. If the SDF template contains SDF filters, the SMF uses the UL SDF filters for the generation of the IP descriptors or Non-IP descriptors, respectively. If the SDF template contains an application identifier, the SMF includes the application descriptors received from the PCF as part of the MA PDU Session information in the PCC Rule within the Traffic Descriptors in the ATSSS rule.

The PCF may also provide URSP rules to the UE for instructing the UE to establish a MA PDU Session, as described in clause 6.6.2.

The PCF control of PDU Session level Usage Monitoring depending on what access type is used to carry the traffic is enabled by providing Usage Monitoring control related information per access in the PDU Session related policy control information (as described in clause 6.4).

If the MA PDU Session is capable of MPTCP and ATSSS-LL with any Steering Mode in the downlink and MPTCP and ATSSS-LL with Active-Standby in the uplink, then the PCF shall provide a PCC Rule for non-MPTCP traffic. This PCC Rule contains a "match all" SDF template, the lowest precedence, the Steering Functionality set to "ATSSS-LL" and the Steering Mode set to "Active-Standby" for the uplink direction, and the Steering Functionality set to "ATSSS-LL" and the Steering Mode set to any supported steering mode for the downlink direction.

If the MA PDU Session is capable of MPTCP with any Steering Mode in the downlink, ATSSS-LL with any steering mode except Smallest Delay steering mode in the downlink, and MPTCP and ATSSS-LL with Active-Standby in the uplink, then the PCF shall provide a PCC Rule for non-MPTCP traffic. This PCC Rule contains a "match all" SDF template, the lowest precedence, the Steering Functionality set to "ATSSS-LL" and the Steering Mode set to "Active-Standby" for the uplink direction, and the Steering Functionality set to "ATSSS-LL" and the Steering Mode set to any supported steering mode except Smallest Delay steering mode for the downlink direction.

If the MA PDU Session is capable of MPTCP and ATSSS-LL with Active-Standby in the uplink and downlink, then the PCF shall provide a PCC Rule for non-MPTCP traffic. This PCC Rule contains a "match all" SDF template, the lowest precedence, the Steering Functionality set to "ATSSS-LL" and the Steering Mode set to "Active-Standby" for the uplink direction and the downlink direction.

If the MA PDU Session is capable of MPTCP and ATSSS-LL with any Steering Mode in the uplink and downlink, then the PCF shall provide a PCC Rule for non-MPTCP traffic. This PCC Rule may contain a "match all" SDF template, the lowest precedence, the Steering Functionality set to "ATSSS-LL" and the Steering Mode set to any supported steering mode for the uplink direction and for the downlink direction.

These PCC Rules are used by the SMF to generate an ATSSS rule for the UE and an N4 rule for the UPF to route the non-MPTCP traffic of the MA PDU Session in the uplink and downlink direction respectively.

NOTE 2: The PCF can also use the ATSSS capability of the MA PDU Session to provide PCC Rules containing SDF template for some specific non-MPTCP traffic other than the PCC Rule containing a "match all" SDF template. This allows the operator to apply different policies e.g. charging key to non-MPTCP traffic other than the non-MPCTP traffic matching the "match all" PCC Rule.

#### **\*\*\*NEXT CHANGE\*\*\***

#### 6.1.3.23 Support of integration with Time Sensitive Networking

Time Sensitive Networking (TSN) support is defined in TS 23.501 [2], where the 5GS represents logical TSN bridge(s) based on the defined granularity model. The TSN AF and PCF interact to perform QoS mapping as described in clause 5.28.4 of TS 23.501 [2].

The PCF provides the following parameters to the TSN AF:

- 5GS Bridge information:

- 5GS Bridge ID;

- UE-DS-TT Residence time;

- Port Management Information Container and the related port number:

- Ethernet port of DS-TT;

- port number of the Ethernet port;

- MAC address of the Ethernet port (i.e. DS-TT port MAC address).

- Bridge Management Information Container:

- 5GS Bridge address and Bridge ID;

- Topology of 5GS Bridge.

The TSN AF may use this information to construct IEEE 802.1 managed objects, to interwork with IEEE 802.1 TSN networks, as defined in TS 23.501 [2] and TS 23.502 [3].

The TSN AF requests related to TSN configuration are sent on the AF session associated with the DS-TT port MAC address. The TSN AF decides the TSN QoS information (i.e. priority, delay, maximum TSC Burst Size and Maximum Flow Bitrate) and TSC Assistance Container based on the received configuration information of 5GS Bridge from the CNC as defined in clause 5.28.2 of TS 23.501 [2], the bridge delay information at the TSN AF and the UE-DS-TT Residence time.

The PCF receives a request from the TSN AF that may include:

- Flow Descriptions including Ethernet Packet Filters (e.g. Ethernet PCP, VLAN ID, destination MAC address of the TSN stream);

- TSN QoS Parameters for the service data flow:

- TSC Assistance Container: describes the TSC stream traffic characteristics (burst arrival time, periodicity, (both in reference to TSN GM), and Flow direction needed for TSCAI determination (as described in clauses 5.27 and 5.28 of TS 23.501 [2]);

- TSN QoS information, i.e. priority, maximum TSC Burst Size, delay and Maximum Flow Bitrate.

- Port Management Information Container and related Port number;

- Bridge Management Information Container.

The PCF performs Session binding using the DS-TT port MAC address, and then the PCF derives the 5QI based on the TSN QoS information and the PCF shall consider the delay parameter provided by the TSN AF for deriving the 5QI. The PCF generates a PCC Rule with service data flow filter (including Ethernet Packet Filter set as in TS 23.501 [2] clause 5.7.6.3) derived from the Flow Descriptions provided by the TSN AF, the mapped 5QI, ARP, GBR and MBR and the associated TSC Assistance Container as received from the AF. The PCF derives the 5QI value as defined in TS 23.501 [2], clause 5.27.3, the PCF derives the GBR using the Maximum Flow Bitrate provided by the TSN AF and the ARP is assigned a value preconfigured for TSN services. The SMF binds the PCC Rule to a QoS Flow as defined in clause 6.1.3.2.4.

NOTE: TSC burst size can represent the maximum burst size of the TSN streams that have been aggregated.

#### **\*\*\*NEXT CHANGE\*\*\***

##### 6.2.1.1.1 Session management related functionality

The PCF provides the following session management related functionality:

- Policy and charging control for a service data flows;

- PDU Session related policy control;

- PDU Session event reporting to the AF.

The PCF provides authorized QoS for a service data flow and other network control regarding service data flow detection, gating, QoS and charging (except credit management) towards the SMF.

The PCF uses the service information received from the AF (e.g. SDP information or other available application information) and/or the subscription information received from the UDR to calculate the proper QoS authorization (QoS class identifier, bitrates). The PCF may also take into account the requested QoS received from the SMF and the analytics information (e.g. analytics related to "Service Experience") received from the NWDAF.

NOTE 1: The PCF provides always the maximum values for the authorized QoS even if the requested QoS is lower than what can be authorized.

The PCF may check that the service information provided by the AF is consistent with both the operator defined policies and the related subscription information as received from the UDR during PDU Session establishment before storing the service information. The PCF may reject the request received from the AF when the service information is not consistent with either the related subscription information or the operator defined policies and may indicate, in the response to the AF, the service information that can be accepted by the PCF (e.g. the acceptable bandwidth). In the absence of other policy control mechanisms outside the scope of PCC, it is recommended that the PCF include this information in the response.

In this Release, the PCF supports only the interaction with a single AF for each AF session.

The Authorization of QoS shall be based on complete service information unless the PCF is required to perform the authorization of QoS based on preliminary service information. The PCF shall after receiving the complete service information, update the affected PCC rules accordingly.

At reception of the service information from the AF if configured through policy and taking into account information defined in TS 26.114 [31], the PCF determines the Maximum Packet Loss Rate for UL and DL based on the service information and sends it to SMF along with the PCC rule.

NOTE 2: Based on local configuration, the PCF sets the Maximum Packet Loss Rate (UL, DL) corresponding to either the most robust codec configuration (e.g., codec, mode, redundancy) or the least robust codec configuration of the negotiated set in each direction.

NOTE 3: Details for setting the Maximum Packet Loss Rate are specified by SA4.

The PCF supports usage monitoring control as described in clause 6.2.1.7.

The PCF supports sponsored data connectivity for a service as described in clause 6.2.1.8.

The PCF uses the information relating to subscriber spending available in the CHF as input for policy decisions related to e.g. QoS control, gating or charging conditions. Details for policy decisions based on spending limits are described in clause 6.1.3.17.

The PCF uses one or more pieces of information defined in the clause 6.2.1.2 as input for the selection of traffic steering policies used to control the steering of the subscriber's traffic as described in clause 6.1.3.14.

The PCF reports PDU Session events, e.g. Access Type, RAT Type (if applicable), Access Network Information, PLMN identifier where the UE is located, as described in clause 6.1.3.18.

The subscription and reporting of events when the target for reporting is an Internal Group Identifier or any UE accessing a combination of (DNN, S-NSSAI), is described in clause 5.2.5.7 of TS 23.502 [3]. The events that can be reported by the PCF are described in clause 6.1.3.18.

The subscription and reporting of events targeting an individual UE IP address (IPv4 address or IPv6 prefix) and optionally the DN information are described below. The events that can be reported by the PCF are described in clause 6.1.3.18.

The PCF shall ensure that the sum of the packet filters used by all PCC rules which trigger the generation of signalled QoS rules does not exceed the number of supported packet filters for signalled QoS rules indicated by the UE for the PDU Session, if this information is provided by the SMF (as defined in clause 6.2.1.2).

For EPC IWK, when PCF receives from the SMF of the report on UE resumed from suspend state, the PCF may provision PCC Rules to the SMF to trigger an IP-CAN Session modification procedure.

The PCF may provide the IP index as the PDU Session related policy to the SMF for IP address/Prefix allocation at SM Policy Association Establishment. If PCF receives from the SMF an allocated IP address/Prefix for the PDU Session, it shall not include IP Index into the PDU Session related policy.

On receiving the DN Authorization Profile Index provided by the SMF at the establishment or modification of the SM Policy Association for a PDU Session, the PCF takes the DN Authorization Profile Index as input for a policy decision and then obtains the list of PCC Rules (as defined in clause 6.3) and/or PDU Session related policy (as defined in clause 6.4) and provides them to the SMF as part of the Session Management Policy Control Data for enforcement.

On receiving the Session-AMBR provided by the SMF at the establishment or modification of the SM Policy Association for a PDU Session under the conditions defined in TS 23.501 [2] clause 5.6.6, the PCF provides the Authorized Session-AMBR as part of the PDU Session policy control information defined in clause 6.4.

The PCF provides DNAI(s) in the PCC rule(s) to the SMF, taking into account the AF request and the Local routing indication from the PDU Session policy control subscription information.

When the PCF detects that all PCC rules related to an AF session are removed, or the PCF detects that the SM Policy Association is terminated, the PCF shall request the AF to terminate the AF session. If the SMF indicated that the PCC rules were removed or that the SM Policy Association is terminated due to PS to CS handover, the PCF shall indicate PS to CS handover as cause within the request to terminate the AF session.

NOTE 4: For 5G-SRVCC (i.e. SRVCC from NG-RAN to UTRAN) as specified in TS 23.216 [25]), the SM Policy Association is terminated by the SMF. For SRVCC (i.e. SRVCC from E-UTRAN to GERAN/UTRAN) as specified in TS 23.216 [25], the SMF indicates that PCC rules are removed.

#### **\*\*\*NEXT CHANGE\*\*\***

#### 6.2.1.2 Input for PCC decisions

The PCF shall accept input for PCC decision-making from the SMF, the AMF, the CHF, the NWDAF if present, the UDR and if the AF is involved, from the AF, as well as the PCF may use its own predefined information. These different nodes should provide as much information as possible to the PCF. At the same time, the information below describes examples of the information provided. Depending on the particular scenario all the information may not be available or is already provided to the PCF.

The AMF may provide the following information:

- SUPI;

- PEI of the UE;

- Location of the subscriber;

- Service Area Restrictions;

- RFSP Index;

- RAT Type;

- GPSI;

- Access Type;

- Serving Network identifier (PLMN ID or PLMN ID and NID, see clause 5.34 of TS 23.501 [2]);

- Allowed NSSAI;

- UE time zone;

- Subscribed UE-AMBR;

- Mapping Of Allowed NSSAI;

- S-NSSAI for the PDU Session;

- Requested DNN.

NOTE 1: The Access Type and RAT Type parameters should allow extension to include new types of accesses.

The UE may provide the following information:

- OSId;

- List of PSIs;

- Indication of UE support for ANDSP.

The SMF may provide the following information:

- SUPI;

- PEI of the UE;

- IPv4 address of the UE;

- IPv6 network prefix assigned to the UE;

- Default 5QI and default ARP;

- Request type (initial, modification, etc.);

- Type of PDU Session (IPv4, IPv6, IPv4v6, Ethernet, Unstructured);

- Access Type;

- RAT Type;

- GPSI;

- Internal-Group Identifier;

- Location of the subscriber;

- S-NSSAI;

- NSI-ID (if available);

- DNN;

- Serving Network identifier (PLMN ID or PLMN ID and NID, see clause 5.34 of TS 23.501 [2]);

- Application identifier;

- Allocated application instance identifier;

- Detected service data flow descriptions;

- UE support of reflective QoS (as defined in clause 5.7.5.1 of TS 23.501 [2]);

- Number of supported packet filters for signalled QoS rules for the PDU Session (indicated by the UE as defined in clause 5.7.1.4 of TS 23.501 [2]);

- 3GPP PS Data Off status;

- DN Authorization Profile Index (see clause 5.6.6 of TS 23.501 [2]);

- DN authorized Session AMBR (see clause 5.6.6 of TS 23.501 [2]).

The UDR may provide the information for a subscriber connecting to a specific DNN and S-NSSAI, as described in the sub clause 6.2.1.3.

The UDR may provide the following policy information related to an ASP:

- The ASP identifier;

- A transfer policy together with a Background Data Transfer Reference ID, the volume of data to be transferred per UE, the expected amount of UEs.

NOTE 2: The information related with AF influence on traffic routing may be provided by UDR when the UDR serving the NEF is deployed and stores the application request.

The UDR may provide the service specific information as defined in clause 4.15.6.7 of TS 23.502 [3].

The AF, if involved, may provide the following application session related information directly or via NEF, e.g. based on SIP and SDP:

- Subscriber Identifier;

- IP address of the UE;

- Media Type;

- Media Format, e.g. media format sub-field of the media announcement and all other parameter information (a= lines) associated with the media format;

- Bandwidth;

- Sponsored data connectivity information;

- Flow description, e.g. source and destination IP address and port numbers and the protocol;

- AF application identifier;

- AF-Service-Identifier, or alternatively, DNN and possibly S-NSSAI;

- AF Communication Service Identifier (e.g. IMS Communication Service Identifier), UE provided via AF;

- AF Application Event Identifier;

- AF Record Information;

- Flow status (for gating decision);

- Priority indicator, which may be used by the PCF to guarantee service for an application session of a higher relative priority;

NOTE 3: The AF Priority information represents session/application priority and is separate from the MPS 5GS Priority indicator.

- Emergency indicator;

- Application service provider;

- DNAI;

- Information about the N6 traffic routing requirements;

- GPSI;

- Internal-Group Identifier;

- Temporal validity condition;

- Spatial validity condition;

- AF subscription for early and/or late notifications about UP management events;

- AF transaction identifier;

- TSN QoS information as described in clause 6.1.3.23;

- QoS information to be monitored;

- Reporting frequency.

The AF may provide the following background data transfer related information via NEF:

- BDT Reference ID;

- BDT Policy;

- Volume per UE;

- Number of UEs;

- Desired time window;

- Network Area Information.

The CHF, if involved, may provide the following information for a subscriber:

- Policy counter status for each relevant policy counter.

The NWDAF, if involved, may provide analytics information as described in clause 6.1.1.3.

In addition, the predefined information in the PCF may contain additional rules based on charging policies in the network, whether the subscriber is in its home network or roaming, depending on the QoS Flow attributes.

The 5QIs (see clause 5.7.4 of TS 23.501 [2]) in the PCC rule is derived by the PCF from AF or UDR interaction if available. The input can be SDP information or other available application information, in line with operator policy.

The Allocation and Retention Priority in the PCC Rule is derived by the PCF from AF or UDR interaction if available, in line with operator policy.

#### **\*\*\*NEXT CHANGE\*\*\***

#### 6.2.1.3 Policy control subscription information management

The PCF may request subscription information at PDU Session establishment and during the UE Policy Association Establishment procedure.

The PCF may receive notifications on changes in the subscription information. Upon reception of a notification, the PCF shall make the policy control decisions necessary to accommodate the change in the subscription and shall update the SMF and/or the AMF if needed.

NOTE 1: How the PCF provisions/retrieves information related with policy control subscription data is defined in TS 23.501 [2].

The policy control subscription profile information provided by the UDR during the UE Policy Association Establishment procedure using Nudr service for Data Set "Policy Data" and Data Subset "UE context policy control data" is described in Table 6.2-1:

Table 6.2-1: UE context policy control subscription information

| Information name | Description | Category |
| --- | --- | --- |
| Subscriber categories | List of category identifiers associated with the subscriber | Optional |
| Tracing Requirements | Tracing requirements as defined in TS 32.421 [18] | Optional |
| PEI | The Permanent Equipment Identifier of the UE. | Optional |
| OSId | Identifies the operating system supported by UE. | Optional |
| Indication of UE support for ANDSP | Indicates the UE support for ANDSP. | Optional |
| S-NSSAI subscription information | Contains the list of subscribed S-NSSAIs, its associated subscribed DNNs. For each DNN, the Allowed PDU Session types and the Allowed SSC modes. | Optional |

NOTE 2: S-NSSAI subscription information can be part of UE context policy control subscription information and Session Management Subscription data/Slice Selection Subscription data. UDR implementation and the provisioning system are responsible for keeping the consistency of this information when both Data Sets are stored in the same UDR. The provisioning system is responsible for keeping the consistency of this information when both Data Sets are stored in different UDRs.

The policy control subscription profile information provided by the UDR at PDU Session establishment, using Nudr service for Data Set "Policy Data" and Data Subset "PDU Session policy control data" is described in Table 6.2-2.

Table 6.2-2: PDU Session policy control subscription information

| Information name | Description | Category |
| --- | --- | --- |
| Allowed services | List of subscriber's allowed service identifiers | Optional |
| Subscriber categories | List of category identifiers associated with the subscriber | Optional |
| Subscribed GBR | Maximum aggregate bitrate that can be provided across all GBR QoS Flows for the DNN and S-NSSAI. | Optional |
| ADC support | Indicates whether application detection and control can be enabled for a subscriber | Optional |
| Subscriber spending limits control | Indicates whether the PCF must enforce policies based on subscriber spending limits | Optional |
| IP index information | Information that identifies the IP Address allocation method during PDU Session establishment | Optional |
| Background Data Transfer Reference ID(s) | Reference ID(s) for Background Data Transfer Policies that apply to the UE. | Optional |
| Local routing indication | Indication on whether AF influence on traffic routing is allowed or not allowed | Optional |
| **Charging related information** | This part defines the charging related information in the policy control subscription profile |  |
| Default charging method | Default charging method for the PDU Session (online / offline) | Optional |
| CHF address | The address of the Charging Function and optionally the associated CHF instance ID and CHF set ID (see clause 6.3.1.0 of TS 23.501 [2]) | Optional |
| **Usage monitoring related information** | This part includes a list of usage monitoring profiles associated with the subscriber. Each usage monitoring profile is logically associated with a particular operator offer, and includes the following elements |  |
| Monitoring key | An identifier to a usage monitoring control instance that includes one or more PCC rules | Conditional (NOTE 1) |
| Usage monitoring level | Indicates the scope of the usage monitoring instance (PDU Session level or per Service) | Optional |
| Start date | Start date and time when the usage monitoring profile applies | Optional |
| End date | End date and time when the usage monitoring profile applies | Optional |
| Volume limit | Maximum allowed traffic volume | Optional |
| Time limit | Maximum allowed resource time usage | Optional |
| Reset period | Time period to reset the remaining allowed consumed usage for periodic usage monitoring control (postpaid subscriptions) | Optional |
| **MPS subscription data** | This part defines the MPS subscription information in the policy control subscription profile |  |
| MPS priority | Indicates subscription to MPS priority service; priority applies to all traffic on the PDU Session | Conditional (NOTE 1) |
| IMS signalling priority | Indicates subscription to IMS signalling priority service; priority only applies to IMS signalling traffic | Conditional (NOTE 1) |
| MPS priority level | Relative priority level for multimedia priority services | Conditional (NOTE 1) |
| MCS priority | Indicates subscription to MCS priority service; priority applies to all traffic on the PDU Session | Conditional (NOTE 1) |
| MCS priority level | Relative priority level for MCS services | Conditional (NOTE 1) |
| NOTE 1: The information is mandatory if the specific part is included in the subscription information (e.g. the monitoring key is mandatory if the usage monitoring information part is included) | | |

Table 6.2-3: Remaining allowed usage subscription information

| Information name | Description | Category |
| --- | --- | --- |
| **Remaining allowed usage related information** | *This part includes a list of Remaining allowed usage associated with the subscriber.* |  |
| Monitoring key | An identifier to a usage monitoring control included one or more PCC rules | Conditional (NOTE 1) |
| Usage monitoring level | Iindicates the scope of the usage monitoring (PDU Session level or service level) | Optional |
| Volume usage | Remaining allowed traffic volume | Optional |
| Time usage | Remaining allowed resource time usage | Optional |
| NOTE 1: The information is mandatory if the specific part is included in the subscription information (e.g. the monitoring key is mandatory if the usage monitoring information part is included) | | |

The *Allowed services* may comprise any number of service identifiers allowed for the subscriber in the PDU Session. The PCF maps those service identifiers into PCC rules according to local configuration and operator policies.

The *Subscriber category* may comprise any number of identifiers associated with the subscriber (e.g. gold, silver, etc.). Each identifier associates operator defined policies to the subscriber that belong to that category.

The *Usage monitoring related information* may comprise any number of usage monitoring control instances associated with the subscriber. In each usage monitoring control instance is mandatory to include the *Monitoring key*. The *Reset period* only applies to usage monitoring control instances that periodically reset the allowed usage (e.g. daily, monthly, etc.). If the Reset period is not specified, the usage monitoring control instance ends when the allowed data is consumed or when the *End date* is reached. The usage monitoring related information is used by the PCF instead of the respective information for the subscriber category.

The policy subscription profile may be extended with operator-specific information. Operator-specific extensions may be added both to any specific part of the policy control subscription information (e.g. to the subscriber category part), or as a new optional information block.

Handling of operator specific policy data by the PCF is out of scope of this specification in this release.

The policy control subscription profile information provided by the UDR during the UE Policy Association Establishment procedure using Nudr service for Data Set "Policy Data" and Data Subset "Policy Set Entry" is described in Table 6.2-4.

Table 6.2-4: Policy Set Entry

| Information name | Description | Category |
| --- | --- | --- |
| Policy Set Entry | List of PSIs and content for each PSI. Content may be Access Network Discovery & Selection Policy Information or UE Route Selection Policy information or both. | Optional |

#### **\*\*\*NEXT CHANGE\*\*\***

#### 6.2.1.4 V-PCF

The V-PCF is a functional element that encompasses policy control decision functionalities in the VPLMN.

For session management related policy control, the V-PCF only includes functionality for local breakout roaming scenario based on roaming agreements.

For UE policy control, the V-PCF receives the UE policy from the H-PCF and forwards it to the UE via the AMF. The V-PCF can send additional UE policy information (i.e. ANDSP policies) to the UE which is different from the one from H-PCF.

For Access and mobility related policy control, the V-PCF generates the values for RFSP Index, UE-AMBR, Service Area Restriction and SMF selection management.

#### **\*\*\*NEXT CHANGE\*\*\***

#### 6.2.1.5 H-PCF

The H-PCF is a functional element that encompasses policy control decision functionalities in the HPLMN.

For session management related policy control, the H-PCF only includes functionality for home routed roaming scenario and provides the same functionality as the PCF in the non-roaming case.

For UE policy control, H-PCF generates the UE policy based on subscription data and transfers the UE policy to the UE via the AMF, or via the V-PCF in the roaming case.

#### **\*\*\*NEXT CHANGE\*\*\***

#### 6.2.2.4 QoS control

The SMF receives the authorized QoS for a service data flow in the PCC rule. The SMF derives the QoS parameters for a QoS Flow (other than the QoS Flow associated with the default QoS rule) based on the PCC rule information of the PCC rule(s) bound to this QoS Flow:

- The SMF shall set the QoS Flow parameters 5QI and ARP to the values of the corresponding PCC rule parameters.

- For the QoS Flow parameters QNC, Priority Level, Averaging Window and Maximum Data Burst Volume, the SMF shall use the corresponding PCC rule parameters if they are available in the PCC rule.

- For GBR QoS Flows, the SMF should set the GFBR to the sum of the GBRs of all PCC rules that are active and bound to that QoS Flow and the MFBR to the sum of the MBRs of all PCC rules that are active and bound to that GBR QoS Flow. If a set of PCC Rules is subject to resource sharing as specified in clause 6.1.3.13 the SMF should use, for each applicable direction, the highest GBR from the set of PCC Rules sharing resources as input for calculating the GFBR and may use, for each applicable direction, the highest MBR from the set of PCC Rules as input for calculating the MFBR.

- For GBR QoS Flows, the SMF shall set the QoS Flow parameter Maximum Packet Loss Rate for UL and DL if the corresponding PCC rule parameters are available in the PCC rule. In the case multiple PCC Rules are bound to the QoS Flow and the SMF received multiple Maximum Packet Loss Rates, the SMF chooses the lowest value per direction in all these PCC rules.

- If the PCC rule contains a non-standardized 5QI, the SMF shall also provide the corresponding 5G QoS characteristics parameters (as received in the PDU Session related information Explicitly signalled QoS Characteristics) for the QoS Flow.

- If the PCC rule contains Alternative QoS Parameter Sets, the SMF shall provide their attributes as Alternative QoS Profile(s) (see TS 23.501 [2] clause 5.7.1.2a) in the same prioritized order (in which they occur in the PCC rule) in addition to the QoS parameters for the QoS Flow.

The SMF shall set the QoS parameters of the QoS Flow associated with the default QoS rule to:

- the PCC rule parameters contained in the PCC rule that is bound to this QoS Flow (in the way it is described above) if the PCC rule attribute Bind to QoS Flow associated with the default QoS rule and apply PCC rule parameters is present; or otherwise

- the Authorized default 5QI/ARP received in the PDU Session related information. If the Authorized default 5QI contains a non-standardized 5QI, the SMF shall also provide the corresponding 5G QoS characteristics parameters (as received in the PDU Session related information Explicitly signalled QoS Characteristics) for the QoS Flow associated with the default QoS rule.

The SMF receives the Authorized Session-AMBR in the PDU Session related information. The SMF ensures that the Authorized Session-AMBR for a PDU Session is enforced for bandwidth policing at the UPF(s) as described in TS 23.501 [2] clause 5.7.1.

The SMF generates QoS rule(s) as described in TS 23.501 [2]. For a PDU Session of unstructured type, only one PCC Rule allowing all packets is to be activated in the SMF and only the QoS Flow associated with the default QoS rule exists as described in TS 23.501 [2] clause 5.7.1.

#### **\*\*\*NEXT CHANGE\*\*\***

### 6.2.8 Access and Mobility Management Function (AMF)

The Access and Mobility Management Function (AMF) is defined in TS 23.501 [2] and additionally supports the following policy related functionalities:

- Enforcement of access and mobility related policies received from the PCF;

- Transfers of UE policy information received from the PCF to the UE via N1 interface;

- Reporting of events to the PCF that the PCF has subscribed to.

#### **\*\*\*NEXT CHANGE\*\*\***

### 6.2.9 Network Data Analytics Function (NWDAF)

The Network Data Analytics Function (NWDAF) is defined in TS 23.288 [24].

#### **\*\*\*NEXT CHANGE\*\*\***

### 6.3.1 General

The Policy and charging control rule (PCC rule) comprises the information that is required to enable the user plane detection of, the policy control and proper charging for a service data flow. The packets detected by applying the service data flow template of a PCC rule form a service data flow.

Two different types of PCC rules exist: Dynamic rules and predefined rules. The dynamic PCC rules are provisioned by the PCF to the SMF, while the predefined PCC rules are configured into the SMF, as described in TS 23.501 [2], and only referenced by the PCF.

NOTE 1: The procedure for provisioning predefined PCC rules is out of scope for this specification.

The operator defines the PCC rules.

Table 6.3.1 lists the information contained in a PCC rule, including the information name, the description and whether the PCF may modify this information in a dynamic PCC rule which is active in the SMF. The Category field indicates if a certain piece of information is mandatory or not for the construction of a PCC rule, i.e. if it is possible to construct a PCC rule without it.

The differences with table 6.3 in TS 23.203 [4] are shown, either "none" means that the IE applies in 5GS or "removed" meaning that the IE does not apply in 5GS, this is due to the lack of support in the 5GS for this feature or "modified" meaning that the IE applies with some modifications defined in the IE.

Table 6.3.1: The PCC rule information in 5GC

| Information name | Description | Category | PCF permitted to modify for a dynamic PCC rule in the SMF | Differences compared with table 6.3. in TS 23.203 [4] |
| --- | --- | --- | --- | --- |
| Rule identifier | Uniquely identifies the PCC rule, within a PDU Session.  It is used between PCF and SMF for referencing PCC rules. | Mandatory | No | None |
| **Service data flow detection** | *This part defines the method for detecting packets belonging to a service data flow.* |  |  |  |
| Precedence | Determines the order, in which the service data flow templates are applied at service data flow detection, enforcement and charging. (NOTE 1). | Conditional (NOTE 2) | Yes | None |
| 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.  It is defined in TS 23.501 [2], clause 5.7.6.3 | Mandatory (NOTE 3) | Conditional  (NOTE 4) | Modified  (packet filters for Ethernet PDU traffic added) |
| Mute for notification | Defines whether application's start or stop notification is to be muted. | Conditional (NOTE 5) | No | None |
| **Charging** | *This part defines identities and instructions for charging and accounting that is required for an access point where flow based charging is configured* |  |  |  |
| Charging key  (NOTE 22) | The charging system (CHF) uses the charging key to determine the tariff to apply to the service data flow. |  | Yes | None |
| Service identifier | The identity of the service or service component the service data flow in a rule relates to. |  | Yes | None |
| 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. | Conditional  (NOTE 6) | Yes | None |
| 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. | Conditional  (NOTE 6) | Yes | None |
| Charging method | Indicates the required charging method for the PCC rule.  Values: online or offline or neither. | Conditional (NOTE 7) | No | None |
| 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.  Values: blocking or non-blocking |  | No | New |
| 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). |  | Yes | None |
| 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. |  | No | None |
| Service Identifier Level Reporting | Indicates that separate usage reports shall be generated for this Service Identifier.  Values: mandated or not required |  | Yes | None |
| **Policy control** | *This part defines how to apply policy control for the service data flow.* |  |  |  |
| 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). |  | Yes | None |
| 5G QoS Identifier (5QI) | The 5QI authorized for the service data flow. | Conditional (NOTE 10) | Yes | Modified  (corresponds to QCI in TS 23.203 [4]) |
| QoS Notification Control (QNC) | Indicates whether notifications are requested from 3GPP RAN when the GFBR can no longer (or can again) be guaranteed for a QoS Flow during the lifetime of the QoS Flow. | Conditional (NOTE 15) | Yes | Added |
| Reflective QoS Control | Indicates to apply reflective QoS for the SDF. |  | Yes | Added |
| UL-maximum bitrate | The uplink maximum bitrate authorized for the service data flow |  | Yes | None |
| DL-maximum bitrate | The downlink maximum bitrate authorized for the service data flow |  | Yes | None |
| UL-guaranteed bitrate | The uplink guaranteed bitrate authorized for the service data flow |  | Yes | None |
| DL-guaranteed bitrate | The downlink guaranteed bitrate authorized for the service data flow |  | Yes | None |
| UL sharing indication | Indicates resource sharing in uplink direction with service data flows having the same value in their PCC rule |  | No | None |
| DL sharing indication | Indicates resource sharing in downlink direction with service data flows having the same value in their PCC rule |  | No | None |
| Redirect | Redirect state of the service data flow (enabled/disabled) | Conditional (NOTE 8) | Yes | None |
| Redirect Destination | Controlled Address to which the service data flow is redirected when redirect is enabled | Conditional  (NOTE 9) | Yes | None |
| 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 | Conditional (NOTE 10) | Yes | None |
| Bind to QoS Flow associated with the default QoS rule | Indicates that the dynamic PCC rule shall always have its binding with the QoS Flow associated with the default QoS rule (NOTE 11). |  | Yes | Modified (corresponds to bind to the default bearer in TS 23.203 [4]) |
| Bind to QoS Flow associated with the default QoS rule and apply PCC rule parameters | Indicates that the dynamic PCC rule shall always have its binding with the QoS Flow associated with the default QoS rule.  It also indicates that the that the QoS related attributes of the PCC rule shall be applied to derive the QoS parameters of the QoS Flow associated with the default QoS rule instead of the PDU Session related parameters Authorized default 5QI/ARP. | Conditional (NOTE 17) | Yes | Added |
| PS to CS session continuity | Indicates whether the service data flow is a candidate for vSRVCC. |  |  | Removed |
| Priority Level | Indicates a priority in scheduling resources among QoS Flows (NOTE 14). |  | Yes | Added |
| Averaging Window | Represents the duration over which the guaranteed and maximum bitrate shall be calculated (NOTE 14). |  | Yes | Added |
| Maximum Data Burst Volume | Denotes the largest amount of data that is required to be transferred within a period of 5G-AN PDB (NOTE 14). |  | Yes | Added |
| 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. | Conditional  (NOTE 25) | Yes | Added |
| **Access Network Information Reporting** | *This part describes access network information to be reported for the PCC rule when the corresponding QoS Flow is established, modified or terminated.* |  |  |  |
| User Location Report | 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. |  | Yes | None |
| UE Timezone Report | The time zone of the UE is to be reported. |  | Yes | None |
| **Usage Monitoring Control** | *This part describes identities required for Usage Monitoring Control.* |  |  | None |
| Monitoring key  (NOTE 23) | The PCF uses the monitoring key to group services that share a common allowed usage. |  | Yes | None |
| Indication of exclusion from session level monitoring | Indicates that the service data flow shall be excluded from PDU Session usage monitoring |  | Yes | None |
| **N6-LAN Traffic Steering Enforcement Control (NOTE 18)** | *This part describes information required for N6-LAN Traffic Steering.* |  |  |  |
| Traffic steering policy identifier(s) | Reference to a pre-configured traffic steering policy at the SMF  (NOTE 12). |  | Yes | None |
| **AF influenced Traffic Steering Enforcement Control (NOTE 18)** | *This part describes information required for AF influenced Traffic Steering.* |  |  |  |
| Data Network Access Identifier | Identifier(s) of the target Data Network Access (DNAI). It is defined in TS 23.501 [2], clause 5.6.7. |  | Yes | Added |
| Per DNAI: Traffic steering policy identifier | Reference to a pre-configured traffic steering policy at the SMF  (NOTE 19). |  | Yes | Added |
| Per DNAI: N6 traffic routing information | Describes the information necessary for traffic steering to the DNAI. It is described in TS 23.501 [2], clause 5.6.7 (NOTE 19). |  | Yes | Added |
| Information on AF subscription to UP change events | Indicates whether notifications in the case of change of UP path are requested and optionally indicates whether acknowledgment to the notifications shall be expected (as defined in TS 23.501 [2] clause 5.6.7). |  | Yes | Added |
| Indication of UE IP address preservation | Indicates UE IP address should be preserved. It is defined in TS 23.501 [2], clause 5.6.7. |  | Yes | Added |
| Indication of traffic correlation | Indicates that the target PDU Sessions should be correlated via a common DNAI in the user plane. It is described in TS 23.501 [2], clause 5.6.7. |  | Yes | Added |
| **NBIFOM related control Information** | *This part describes PCC rule information related with NBIFOM* |  |  |  |
| Allowed Access Type | The access to be used for traffic identified by the PCC rule |  |  | Removed |
| **RAN support information** | *This part defines information supporting the RAN for e.g. handover threshold decision.* |  |  |  |
| UL Maximum Packet Loss Rate | The maximum rate for lost packets that can be tolerated in the uplink direction for the service data flow. It is defined in TS 23.501 [2], clause 5.7.2.8. | Conditional (NOTE 13) | Yes | None |
| DL Maximum Packet Loss Rate | The maximum rate for lost packets that can be tolerated in the downlink direction for the service data flow. It is defined in TS 23.501 [2], clause 5.7.2.8. | Conditional (NOTE 13) | Yes | None |
| **MA PDU Session Control**  **(NOTE 20)** | *This part defines information supporting control of MA PDU Sessions* |  | Yes | New |
| Application descriptors | identifies the application traffic to apply the Steering Functionality and the Steering mode. It is described in TS 23.501 [2], clause 5.32.8. | Conditional (NOTE 27) | Yes | New |
| Steering Functionality | Indicates the applicable traffic steering functionality. | Conditional (NOTE 21) | Yes | New |
| Steering mode | Indicates the rule for distributing traffic between accesses together with associated parameters (if any). | Conditional (NOTE 21) | Yes | New |
| Charging key for Non-3GPP access  (NOTE 22) | Indicates the Charging key used for charging packets carried via Non-3GPP access for a MA PDU Session. |  | Yes | New |
| Monitoring key for Non-3GPP access  (NOTE 23) | Indicates the Monitoring key used to monitor usage of the packets carried via Non-3GPP access for a MA PDU Session. |  | Yes | New |
| **QoS Monitoring for URLLC** | *This part describes PCC rule information related with QoS Monitoring for URLLC.* |  |  |  |
| QoS parameter(s) to be measured | UL packet delay, DL packet delay or round trip packet delay. |  | Yes | Added |
| Reporting frequency | Defines the frequency for the reporting, such as event triggered, periodic, when no packet delay measurement result is received for a delay exceeding a threshold, or when the PDU Session is released. |  | Yes | Added |
| Target of reporting | Defines the target of the QoS Monitoring reports, it can be either the PCF or the AF, decided by the PCF. |  | Yes | Added |
| **Alternative QoS Parameter Sets**  **(NOTE 24)**  **(NOTE 26)** | *This part defines Alternative QoS Parameter Sets for the service data flow.* |  |  |  |
| Packet Delay Budget | The Packet Delay Budget in this Alternative QoS Parameter Set. |  | Yes | Added |
| Packet Error Rate | The Packet Error Rate in this Alternative QoS Parameter Set. |  | Yes | Added |
| UL-guaranteed bitrate | The uplink guaranteed bitrate in this Alternative QoS Parameter Set. |  | Yes | Added |
| DL-guaranteed bitrate | The downlink guaranteed bitrate in this Alternative QoS Parameter Set. |  | Yes | Added |
| **TSC Assistance Container** | *This part defines parameters provided by TSN AF. Following are the parameters:*  *- Burst Arrival Time - Indicates the burst arrival time in reference to TSN GM and ingress port.*  *- Periodicity The time period (in reference to TSN GM) between start of two bursts.*  *- Flow Direction: Direction of the flow.* |  | No | Added |
| **Downlink Data Notification Control** | *Indicates whether downlink data notification is required and how to notify This part describes information required for controlling the sending of Downlink data delivery status event and DDN Failure event notifications as specified in clause 4.15.3 of TS 23.502 [3].* |  |  |  |
| Notification control of downlink data delivery status | Indicates whether notification of downlink data delivery status is required and related information as specified in clause 4.15.3 of TS 23.502 [3]. |  | Yes | Added |
| Notification Control of DDN Failure | Indicates whether notification of DDN Failure is requested as specified in clause 4.15.3 of TS 23.502 [3]. |  | Yes | Added |
| NOTE 1: For PCC rules based on an application detection filter, the precedence is only relevant for the enforcement, i.e. when multiple PCC rules overlap, only the enforcement, reporting of application starts and stops, monitoring, and charging actions of the PCC rule with the highest precedence shall be applied.  NOTE 2: The Precedence is mandatory for PCC rules with SDF template containing SDF filter(s). For dynamic PCC rules with SDF template containing an application identifier, the precedence is either preconfigured in SMF or provided in the PCC rule from PCF.  NOTE 3: Either service data flow filter(s) or application identifier shall be defined per each rule.  NOTE 4: YES, if the service data flow template consists of a set of service data flow filters. NO if the service data flow template consists of an application identifier  NOTE 5: Optional and applicable only if application identifier exists within the rule.  NOTE 6: Applicable to sponsored data connectivity.  NOTE 7: Mandatory if there is no default charging method for the PDU Session.  NOTE 8: Optional and applicable only if application identifier exists within the rule.  NOTE 9: If Redirect is enabled.  NOTE 10: Mandatory when Bind to QoS Flow associated with the default QoS rule is not present.  NOTE 11: The presence of this attribute causes the 5QI/ARP/QNC/Priority Level/Averaging Window/Maximum Data Burst Volume of the rule to be ignored for the QoS Flow binding.  NOTE 12: The Traffic steering policy identifier can be different for uplink and downlink direction. If two Traffic steering policy identifiers are provided, then one is for uplink direction, while the other one is for downlink direction.  NOTE 13: Optional and applicable only for voice service data flow in this release.  NOTE 14: Optional and applicable only when a value different from the standardized value for this 5QI in Table 5.7.4-1 TS 23.501 [2] is required.  NOTE 15: Optional and applicable only for GBR service data flow.  NOTE 16: Usage of the charging information in described in TS 32.255 [21].  NOTE 17: Only one PCC rule can contain this attribute and this PCC rule shall not contain the attribute Bind to QoS Flow associated with the default QoS rule.  NOTE 18: Only one of the two shall be present in a PCC rule.  NOTE 19: Per DNAI, a Traffic steering policy identifier and/or N6 traffic routing information can be provided. If the pre-configured traffic steering policy (that is referenced by the Traffic steering policy identifier) contains information that is overlapping with the N6 traffic routing information, the N6 traffic routing information shall take precedence.  NOTE 20: Only applicable to a PCC Rules provided to a MA PDU Session.  NOTE 21: Mandatory when MA PDU Session Control information is provided.  NOTE 22: When a Charging key for Non-3GPP access is provided, the parameters in the Charging Section (other than the Charging key) apply to both accesses and the Charging key (in the Charging Section) shall be used for charging packets carried via the 3GPP access.  NOTE 23: When a Monitoring key for Non-3GPP access is provided, the Monitoring key (in the Usage Monitoring Control Section) shall be used to monitor usage of the packets carried via the 3GPP access.  NOTE 24: Optional and applicable only for GBR service data flow with QoS Notification Control enabled.  NOTE 25: Optional and applicable only for GBR service data flow for which Alternative QoS Parameter Set(s) are provided.  NOTE 26: One or more Alternative QoS Parameter Sets can be provided in a prioritized order starting with the Alternative QoS Parameter Set that has the highest priority.  NOTE 27: Mandatory in MA PDU Session Control information only when there is application identifier in the service data flow template. | | | | |

The Rule identifier shall be unique for a PCC rule within a PDU Session. A dynamically provided PCC rule that has the same Rule identifier value as a predefined PCC rule shall replace the predefined rule within the same PDU Session.

The Precedence defines in what order the activated PCC rules within the same PDU Session shall be applied at the UPF for service data flow detection. When a dynamic PCC rule and a predefined PCC rule have the same precedence, the dynamic PCC rule takes precedence.

NOTE 2: The operator shall ensure that overlap between the predefined PCC rules can be resolved based on precedence of each predefined PCC rule in the SMF. The PCF shall ensure that overlap between the dynamically allocated PCC rules can be resolved based on precedence of each dynamically allocated PCC rule.

For downlink packets all the service data flow templates, activated for the PDU Session shall be applied for service data flow detection and for the mapping to the correct QoS Flow. For uplink packets the service data flow templates activated on their QoS Flow shall be applied for service data flow detection (further details are provided in clause 6.2.2.2).

The *Service data flow template* may comprise any number of *Service data flow filters* or an *application identifier* as is defined in table 6.3.1.

NOTE 3: Predefined PCC rules may include service data flow templates, which support extended capabilities, including enhanced capabilities to identify events associated with application protocols.

A Service data flow filter contains information for matching user plane packets for IP PDU traffic or Ethernet PDU traffic. All Service data flow filters of a Service data flow template shall be of the same type, i.e. either Packet Filters for IP or Ethernet PDU traffic (defined in TS 23.501 [2] clause 5.7.6). The Service data flow template information within an activated PCC rule is applied by the SMF to instruct the UPF to identify the packets belonging to a particular service data flow.

For the IP PDU Session type only, the Service data flow template may consist of an application identifier that references an application detection filter that is used for matching user plane packets. The application identifier is also identifying the application, for which the rule applies. The same application identifier value can occur in a dynamic PCC rule and one or multiple predefined PCC rules. If so, the PCF shall ensure that there is at most one PCC rule active per application identifier value at any time.

The *Mute for notification* defines whether notification to the PCF of application's starts or stops shall be muted. Absence of this parameter means that start/stop notifications shall be sent.

The *Charging key* is the reference to the tariff for the service data flow. Any number of PCC Rules may share the same charging key value. The Charging key values for each service shall be operator configurable.

NOTE 4: Assigning the same Charging key for several service data flows implies that the charging does not require the credit management to be handled separately.

The *Service identifier* identifies the service. PCC Rules may share the same service identifier value. The service identifier provides the most detailed identification, specified for flow-based charging, of a service data flow.

NOTE 5: The PCC rule service identifier need not have any relationship to service identifiers used on the AF level, i.e. is an operator policy option.

The *Sponsor Identifier* indicates the (3rd) party organization willing to pay for the operator's charge for connectivity required to deliver a service to the end user.

The *Application Service Provider Identifier* indicates the (3rd) party organization delivering a service to the end user.

The *Charging method* indicates whether online charging or offline charging is required, or the service data flow is not subject to any end user charging. If the charging method identifies that the service data flow is not subject to any end user charging, a Charging key shall not be included in the PCC rule for that service data flow, along with other charging related parameters. If the charging method is omitted the SMF shall apply the default charging method provided within the PDU Session related policy information (see clause 6.4). The Charging method is mandatory if there is no default charging method for the PDU Session.

NOTE 6: With converged charging architecture for 5GC, online charging method also includes usage reporting from the SMF to the CHF. Hence, setting the charging method to online will also result in usage reports and thus allow for offline charging being performed by the CHF.

The *Service Data Flow handling while requesting credit* indicates either "blocking" if a credit for the Charging Key needs to be granted as a condition for the PCC Rule to be active or "non-blocking" if a credit for the Charging Key has been requested as a condition for the PCC Rule to be active.

The *Measurement method* indicates what measurements apply to charging for a PCC rule.

The *Service Identifier Level Reporting* indicates whether the SMF shall generate reports per Service Identifier. The SMF shall accumulate the measurements from all PCC rules with the same combination of Charging key/Service Identifier values in a single report.

The *Application Function Record Information* identifies an instance of service usage. A subsequently generated usage report (i.e. CDR), generated as a result of the PCC rule by the SMF, may include the Application Function Record Information, if available. The Application Function Record Information may contain the AF Charging Identifier and/or the Flow identifiers. If exclusive charging information related to the Application function record information is required, the PCF shall provide a service identifier, not used by any other PCC rule of the PDU Session at this point in time, for the AF session.

NOTE 7: For example, the PCF may be configured to maintain a range of service identifier values for each service which require exclusive per instance charging information. Whenever a separate counting or credit management for an AF session is required, the PCF shall select a value, which is not used at this point in time, within that range. The uniqueness of the service identifier in the SMF ensures a separate accounting/credit management while the AF record information identifies the instance of the service.

The *Gate* indicates whether the SMF shall instruct the UPF to let a packet identified by the PCC rule pass through (gate is open) to discard the packet (gate is closed).

NOTE 8: A packet, matching a PCC Rule with an open gate, may be discarded due to credit management reasons.

The *5G QoS Identifier*, 5QI, represents the QoS parameters for the service data flow. The 5G QoS identifier is scalar and accommodates the need for differentiating QoS in both 3GPP and non-3GPP access type.

The bitrates indicate the authorized bitrates at the IP packet level of the SDF, i.e. the bitrates of the IP packets before any access specific compression or encapsulation.

The *UL maximum-bitrate* indicates the authorized maximum bitrate for the uplink component of the service data flow.

The *DL maximum-bitrate* indicates the authorized maximum bitrate for the downlink component of the service data flow.

The *UL guaranteed-bitrate* indicates the authorized guaranteed bitrate for the uplink component of the service data flow.

The *DL guaranteed-bitrate* indicates the authorized guaranteed bitrate for the downlink component of the service data flow.

The 'Maximum bitrate' is used for enforcement of the maximum bit rate that the SDF may consume, while the 'Guaranteed bitrate' is used by the SMF to determine resource allocation demands.

The *UL sharing indication* indicates that resource sharing in uplink direction for service data flows with the same value in their PCC rule shall be applied by the SMF as described in clause 6.2.2.4.

The *DL sharing indication* indicates that resource sharing in downlink direction for service data flows with the same value in their PCC rule shall be applied by the SMF as described in clause 6.2.2.4.

The *Allocation and Retention Priority* indicates the allocation, retention and priority of the service data flow. The ARP contains information about the priority level, the pre-emption capability and the pre-emption vulnerability. The Allocation and Retention Priority resolves conflicts of demands for network resources.

The *Priority Level* is signalled together with the 5QI to the (R)AN and UPF, only when a value different from the standardized value in the QoS characteristics Table 5.7.4-1 in TS 23.501 [2] is required.

The *Averaging Window* is signalled together with the 5QI to the (R)AN and UPF, only when a value different from the standardized value in the QoS characteristics Table 5.7.4-1 in TS 23.501 [2] is required.

The *Maximum Data Burst Volume* is signalled together with the 5QI to the (R)AN, only when a value different from the standardized value in the QoS characteristics Table 5.7.4-1 in TS 23.501 [2] is required.

The *Bind to QoS Flow associated with the default QoS rule* indicates that the SDF shall be bound to the QoS Flow associated with the default QoS rule. The presence of this parameter attribute causes the 5QI/ARP of the rule to be ignored by the SMF during the QoS Flow binding.

The *Bind to QoS Flow associated with the default QoS rule and apply PCC rule parameters* indicates that the SDF shall be bound to the QoS Flow associated with the default QoS rule and that the QoS related attributes of the PCC rule shall be applied by the SMF to derive the QoS parameters of the QoS Flow associated with the default QoS rule instead of the PDU Session related information Authorized default 5QI/ARP.

NOTE 9: The Bind to QoS Flow associated with the default QoS rule and apply PCC rule parameters Indication has to be used whenever the PDU Session related information Authorized default 5QI/ARP (as described in clause 6.3.1) cannot be directly used as the QoS parameters of the QoS Flow associated with the default QoS rule, for example when a GBR 5QI is used or the 5QI priority level has to be changed.

The *QoS Notification Control,* QNC*,* indicates whether notifications are requested from the access network (i.e. 3GPP RAN) when the GFBR can no longer (or can again) be guaranteed for a QoS Flow during the lifetime of the QoS Flow. If it is set and the GFBR can no longer (or can again) be guaranteed, the access network (i.e. 3GPP RAN) sends a notification towards the SMF, which then notifies the PCF.

The *Disable UE notifications at changes related to Alternative QoS Profiles* parameter 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.

The *Reflective QoS Control* indicates to apply reflective QoS for the service data flow. The indication is used to control the RQI marking in the DL packets of the service data flow and may trigger the sending of the RQA parameter for the QoS Flow the service data flow is bound to. Reflective QoS is defined in TS 23.501 [2] clause 5.7.5.

NOTE 10: While the UE applies a standardized value for the precedence of all UE derived QoS rules, PCC rules require different precedence values and PCF configuration has to ensure that there is a large enough value range for the precedence of PCC rules corresponding to UE derived QoS rules. To avoid that the precedence of network provided QoS rules need to be changed when Reflective QoS is activated and filters are overlapping, the PCF will take the standardized value for the precedence of UE derived QoS rules into account when setting the precedence value of PCC rules subject to Reflective QoS.

The *Reflective QoS Control* parameter shall not be used for the PCC rule with match-all SDF template. If PCC rule with match-all SDF template is present, the *Reflective QoS Control* parameter shall not be used for PCC rules which contain the *Bind to QoS Flow of the default QoS rule* parameter, either.

The *N6-LAN Traffic Steering Enforcement Control* contains *Traffic steering policy identifier(s)* for steering traffic onto N6-LAN to the appropriate N6 service functions deployed by the operator.

The access network information reporting parameters (*User Location Report*, *UE Timezone Report*) instruct the SMF about what information to forward to the PCF when the PCC rule is activated, modified or removed.

The *Monitoring Key* is the reference to a resource threshold. Any number of PCC Rules may share the same monitoring key value. The monitoring key values for each service shall be operator configurable.

The *Indication of exclusion from session level monitoring* indicates that the service data flow shall be excluded from the PDU Session usage monitoring.

The *AF influenced Traffic Steering Enforcement Control* contains:

*- a set of DNAI(s)* (i.e. a reference to the DNAI(s) the SMF needs to consider for UPF selection/reselection), an optional Indication of traffic correlation and, per DNAI, a corresponding Traffic steering policy identifier (i.e. a reference to a pre-configured traffic steering policy at the SMF), and/or a corresponding N6 traffic routing information (when the N6 traffic routing information is provided explicitly as part of the AF influence request, as described in TS 23.501 [2], clause 5.6.7), or;

- an *AF subscription to UP change events* parameter which contains subscription information defined in TS 23.502 [3] clause 5.2.8.3 for the change of UP path Event Id i.e. an *Indication of early and/or late notification* and information on where to provide the corresponding notifications (Notification Target Address + Notification Correlation ID as specified in TS 23.502 [3] clause 4.15.1) and optionally an indication of "AF acknowledgment to be expected" to the corresponding notifications as described in TS 23.501 [2], clause 5.6.7.

The *Traffic Steering Enforcement Control* may contain Indication of UE IP address preservation. The SMF takes this indication into account when determining whether to reselect PSA UPF, as specified in TS 23.501 [2], clause 5.6.7.

The *Redirect* indicates whether the uplink part of the service data flow should be redirected to a controlled address.

The *Redirect Destination* indicates the target redirect address when *Redirect* is enabled.

The *UL Maximum Packet Loss Rate* indicates the maximum rate for lost packets that can be tolerated in the uplink direction.

The *DL Maximum Packet Loss Rate* indicates the maximum rate for lost packets that can be tolerated in the downlink direction.

The *Application descriptors* provides one or several instances of the OSId and OSAppId combination. It is used by the UE to identify the application traffic corresponding to the application identifier to apply the Steering Functionality and the Steering mode.

The *Steering Functionality* indicates the method for how traffic matching the SDF template is sent over the MA PDU Session. The method ATSSS\_LL indicates that the traffic matching the SDF template is sent over the MA PDU Session without additional tunnelling, e.g. with IP flow switching. The method MPTCP indicates that the traffic matching the SDF template is sent over the MA PDU Session using MPTCP.

The *Steering mode* indicates the rule for distributing traffic between accesses, together with the associated parameters. The PCF may indicate separate values for up-link and down-link directions. The available steering modes are defined in TS 23.501 [2].

The *Charging key for Non-3GPP access* indicates the Charging key that shall be used for charging the detected service data flow traffic carried via Non-3GPP access. The other charging related parameters apply for both accesses.

The *Monitoring key for Non-3GPP access* indicates the Monitoring key that shall be used for monitoring the usage of the detected service data flow traffic carried via Non-3GPP access.

The *QoS parameter(s) to be measured* indicates the UL packet delay, DL packet delay 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.

The *Reporting frequency* indicates the frequency for the reporting, such as event triggered, periodic, when no packet delay measurement result is received for a delay exceeding a threshold, or when the PDU Session is released. The following applies:

- If the *Reporting frequency* indicates "periodic", the reporting time period shall also be included in the PCC rule. The reporting time period may also be used as the threshold for reporting packet delay measurement failure: if no measurement result is received for a delay exceeding this threshold, the UPF shall report to the SMF and the SMF shall report to the PCF or to the AF indicating a packet delay measurement failure.

- If the *Reporting frequency* indicates "event triggered", the *Reporting threshold(s)* and the *minimum waiting time* shall also be included in the PCC rule. The *Reporting threshold(s)* indicates the measurement threshold for each of the included *QoS parameter(s)* to be measured, i.e. the UL packet delay, DL packet delay or round trip packet delay. When *Reporting threshold(s)* is exceeded, the UPF shall report to the SMF and the SMF shall report to the PCF or to the AF. 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 SMF reports the minimum and maximum packet delays to the PCF or the AF. The SMF sends the first report when the *Reporting threshold* is exceeded and the minimum waiting time is applied for the subsequent report (if the threshold is exceeded after the waiting time). The Reporting threshold(s) may also be used as the threshold for reporting packet delay measurement failure: if no measurement result is received for a delay exceeding this threshold, the UPF shall report to the SMF and the SMF shall report to the PCF or to the AF indicating a packet delay measurement failure.

The *Target of reporting* indicates the target for the QoS Monitoring reports sent as notifications. It can be either the PCF or the AF (the NEF may be on the path between SMF and AF). The PCF shall include Notification Target Address + Notification Correlation ID as specified in TS 23.502 [3] clause 4.15.1.

The *Alternative QoS Parameter Set(s)* define alternative set(s) of QoS parameters for the service data flow. Every set consists of a PER, a PDB, as well as an UL and a DL guaranteed bitrate QoS parameter.

The TSC Assistance Container contains the following parameters:

- The Burst Arrival Time is sent to the SMF to indicate burst arrival time at the ingress port of 5GS for a given flow direction (DS-TT for UL, NW-TT for DL). It is used by the SMF to determine TSCAI burst arrival time as defined in TS 23.501 [2], clause 5.27.2 to assist transmission of deterministic flows on Uu.

The Periodicity is sent to the SMF to indicate the time between bursts. It is used by the SMF to forward to RAN as part of TSCAI in order to assist transmission of deterministic flows on Uu.

- The Flow direction is sent to SMF to indicate the direction of the flow (UL or DL).

The *Downlink Data Notification Control* applies to the control of Downlink data delivery status event notifications and DDN Failure event notifications as specified in clause 4.15.3 of TS 23.502 [3]. The Following parameters are included:

- The *Notification control of downlink data delivery status* applies as described in clause 4.15.3.2.8 of TS 23.502 [3] and contains the following parameters:

- indication if notifications of downlink data delivery status are requested; and

- the requested type of such notifications (notifications about downlink packets being buffered, and/or discarded).

- The *Notification Control of DDN Failure* applies as described in clause 4.15.3.2.8 of TS 23.502 [3] and contains the following parameters:

- indication if notifications of DDN Failure is requested.

#### **\*\*\*NEXT CHANGE\*\*\***

## 6.4 PDU Session related policy information

The purpose of the PDU Session related policy information is to provide policy and charging control related information that is applicable to a single Monitoring key or the whole PDU Session respectively. The PCF may provide PDU Session related policy information to the SMF together with PCC rules or separately.

Table 6.4-1 includes the PDU Session related policy information.

The differences with table 6.4 and table 6.6 in TS 23.203 [4] are shown, either "none" means that the IE applies in 5GS or "removed" meaning that the IE does not apply in 5GS, this is due to the lack of support in the 5GS for this feature or "modified" meaning that the IE applies with some modifications defined in the IE.

Table 6.4-1: PDU Session related policy information

| Attribute | Description | PCF permitted to modify for dynamically provided information | Scope | Differences compared with table 6.4. and 6.6 in TS 23.203 [4] |
| --- | --- | --- | --- | --- |
| Charging information | Defines the containing CHF address and optionally the associated CHF instance ID and CHF set ID. | No | PDU Session | None |
| Default charging method | Defines the default charging method for the PDU Session. | No | PDU Session | None |
| PDU Session with offline charging only | Indicates that the "online" charging method is never used for PCC rules in the PDU Session. | No | PDU Session | Added |
| Policy control request trigger | Defines the event(s) that shall cause a re-request of PCC rules for the PDU Session. | Yes | PDU Session | Explicitly subscribed by invoking Npcf\_SMPolicyControl service operation |
| Authorized QoS per bearer (UE-initiated IP‑CAN bearer activation/modification) | Defines the authorised QoS for the IP‑CAN bearer (QCI, GBR, MBR). | Yes | IP‑CAN bearer | Removed |
| Authorized MBR per QCI (network initiated IP‑CAN bearer activation/modification) | Defines the authorised MBR per QCI. | Yes | IP‑CAN session | Removed |
| Revalidation time limit | Defines the time period within which the SMF shall perform a PCC rules request. | Yes | PDU Session | None |
| PRA Identifier(s) | Defines the Presence Reporting Area(s) to monitor for the UE with respect to entering/leaving | Yes | PDU Session | None but only applicable to PCF |
| List(s) of Presence Reporting Area elements (NOTE 14) | Defines the elements of the Presence Reporting Area(s) | Yes | PDU Session | None but only applicable to PCF |
| Default NBIFOM access | The access to be used for all traffic that does not match any existing Routing Rule | Yes (only at the addition of an access to the IP-CAN session) | IP-CAN session | Removed |
| IP Index  (NOTE 11) | Provided to SMF to assist in determining the IP Address allocation method (e.g. which IP pool to assign from) when a PDU Session requires an IP address – as defined in TS 23.501 [2] clause 5.8.2.2.1. | No | PDU Session | Added |
| Explicitly signalled QoS Characteristics (NOTE 1) | Defines a dynamically assigned 5QI value (from the non-standardized value range) and the associated 5G QoS characteristics as defined in TS 23.501 [2] clause 5.7.3. | No | PDU Session | Added |
| Reflective QoS Timer | Defines the lifetime of a UE derived QoS rule belonging to the PDU Session. | No | PDU Session | Added |
| Authorized Session-AMBR  (NOTE 2) (NOTE 3) | Defines the Aggregate Maximum Bit Rate for the Non-GBR QoS Flows of the PDU Session. | Yes | PDU Session | Modified |
| Authorized default 5QI/ARP  (NOTE 3) (NOTE 10) | Defines the default 5QI and ARP of the QoS Flow associated with the default QoS rule. | Yes | PDU Session | Modified |
| Time Condition (NOTE 4) | Defines the time at which the corresponding Subsequent Authorized Session-AMBR or Subsequent Authorized default 5QI/ARP shall be applied. | No (NOTE 5) | PDU Session | Modified |
| Subsequent Authorized Session-AMBR (NOTE 4) (NOTE 2) | Defines the Aggregate Maximum Bit Rate for the Non-GBR QoS Flows of the PDU Session when the Time Condition is reached. | No (NOTE 5) | PDU Session | Modified |
| Subsequent Authorized default 5QI/ARP (NOTE 4) (NOTE 10) | Defines the default 5QI and ARP when the Time Condition is reached. | No (NOTE 5) | PDU Session | Modified |
| **Usage Monitoring Control related information**  **(NOTE 12) (NOTE 13)** | Defines the information that is required to enable user plane monitoring of resources for individual applications/services, groups of applications/services, for a PDU Session. |  |  |  |
| Monitoring key | The PCF uses the monitoring key to group services that share a common allowed usage. | No | PDU Session (NOTE 12) | None |
| Volume threshold  (NOTE 7) | Defines the traffic volume value after which the SMF shall report usage to the PCF for this monitoring key. | Yes | Monitoring key | None |
| Time threshold  (NOTE 7) | Defines the resource time usage after which the SMF shall report usage to the PCF. | Yes | Monitoring key | None |
| Monitoring time | Defines the time at which the SMF shall reapply the Volume and/or Time Threshold. | No (NOTE 6) | Monitoring Key | None |
| Subsequent Volume threshold (NOTE 9) | Defines the traffic volume value after which the SMF shall report usage to the PCF for this Monitoring key for the period after the Monitoring time. | No (NOTE 6) | Monitoring Key | None |
| Subsequent Time threshold (NOTE 9) | Defines resource time usage after which the SMF shall report usage to the PCF for this Monitoring key for the period after the Monitoring time. | No (NOTE 6) | Monitoring Key | None |
| Inactivity Detection Time (NOTE 8) | Defines the period of time after which the time measurement shall stop, if no packets are received. | Yes | Monitoring Key | None |
| **Ethernet port management related** |  |  |  |  |
| Port number | Port number for which Port Management Information Container is provided. | Yes | PDU Session | New |
| Port Management Information Container | Includes Ethernet port management information | Yes | PDU Session | New |
| Bridge Management Information Container | Includes Bridge management information | Yes |  | New |
| NOTE 1: Multiple Non-standardized QoS Characteristics can be provided by the PCF. Operator configuration is assumed to ensure that the non-standardized 5QI to QoS characteristic relation is unique within the PLMN.  NOTE 2: The Authorized Session-AMBR and the Subsequent Authorized Session-AMBR may be provided together with a list of Access Types possibly complemented by RAT types.  NOTE 3: There is always an unconditional value for the Authorized Session-AMBR and Authorized default 5QI/ARP available at the SMF. The initial value is received as Subscribed Session-AMBR/Subscribed default 5QI/ARP, and the PCF can overwrite it with these parameters.  NOTE 4: The Time Condition and Subsequent Authorized Session-AMBR/ Subsequent Authorized default 5QI/ARP are used together. The PCF may provide up to four instances of them. When multiple instances are provided, the values of the associated Time Condition have to be different.  NOTE 5: The PCF may replace all instances that have been provided previously with a new instruction. A previously provided Time Condition and Subsequent Authorized Session-AMBR/ Subsequent Authorized default 5QI/ARP pair cannot be individually modified.  NOTE 6: The PCF may replace all instances that have been provided previously with a new instruction. A previously provided Volume threshold/Time threshold and Monitoring Time pair cannot be individually modified.  NOTE 7: This attribute is also used by the SMF, e.g. during PDU Session termination, to inform the PCF about the resources that have been consumed by the UE.  NOTE 8: This attribute is applicable in presence of Time threshold only.  NOTE 9: This attribute is applicable in presence of Monitoring Time only.  NOTE 10: The Authorized default 5QI and the Subsequent Authorized default 5QI shall be of Non-GBR Resource Type.  NOTE 11: This attribute is applicable only when no IP address/Prefix for the PDU Session is received from the SMF.  NOTE 12: A Monitoring Key can either be used to monitor the traffic of a PDU Session, the traffic of a PDU Session per access (for a MA PDU Session) or the traffic of specific SDF(s) in the PCC Rule(s) that share the same Monitoring Key.  NOTE 13: For a MA PDU Session, the PDU Session level Usage Monitoring shall be possible per access (i.e. 3GPP and/or Non-3GPP) and irrespective of the access.  NOTE 14: The list of PRA elements shall be a short list of elements. | | | | |

Upon the initial interaction with the SMF, the PCF may provide the following attributes to the SMF:

The *Charging information* contains addresses of the CHF that manages charging for the PDU Session and optionally the associated CHF instance ID and CHF set ID (see clause 6.3.1.0 of TS 23.501 [2]). If received, the SMF shall apply it as defined in TS 23.501 [2] clause 6.3.11.

The *Default charging method* indicates what charging method shall be used in the PDU Session for every PCC rule where the charging method identifier is omitted, including predefined PCC rules that are activated by the SMF. If received by the SMF, it supersedes the *Default charging method* in the charging characteristics profile.

The *PDU Session with offline charging only* can be assigned to a PDU Session by the PCF to indicate that the online charging method is never set for any of the PCC Rules activated during the lifetime of the PDU Session nor provided as Default charging method.

NOTE 1: If this parameter is provided by the PCF or configured in the SMF charging characteristics the SMF can use the Nchf\_OfflineOnlyCharging service instead of the Nchf\_ConvergedCharging service for a PDU Session as defined in TS 32.255 [21].

The *IP Index* indicates the IP Address/Prefix allocation method which is used by the SMF for IP Address/Prefix allocation during PDU Session Establishment procedure as defined in TS 23.501 [2] clause 5.8.2.2.1.

Upon every interaction with the SMF, the PCF may provide the following attributes to the SMF:

The *Revalidation time limit* defines the time period within which the SMF shall trigger a request for PCC rules for an established PDU Session.

The *Reflective QoS Timer* defines the lifetime of a UE derived QoS rule belonging to the PDU Session. It is used in the UE as defined in TS 23.501 [2] clause 5.7.5.3.

NOTE 2: The Reflective QoS Timer that is sent to the UE has to be in alignment with the corresponding timer configured in the UPF (defined in TS 23.501 [2], clause 5.7.5.3).

The *Authorized Session-AMBR* defines the UL/DL Aggregate Maximum Bit Rate for the Non-GBR QoS Flows of the PDU Session, which is enforced in the UPF as defined in TS 23.501 [2] clause 5.7.1. The PCF may provide the *Authorized Session-AMBR* in every interaction with the SMF. When the SMF receives it from the PDU Session policy, it is provided to the UPF over N4 interface for the enforcement.

The *Authorized default 5QI/ARP* defines the 5QI and ARP values of the QoS Flow associated with the default QoS rule as described in clause 6.2.2.4. The SMF applies the *Authorized default 5QI/ARP* also for the QoS Flow binding as described in clause 6.1.3.2.4.

The *Time Condition* and *Subsequent Authorized Session-AMBR / Subsequent Authorized default 5QI/ARP* are used together and up to four instances with different values of the *Time Condition* parameter may be provided by the PCF. *Time Condition* indicates that the associated *Subsequent Authorized Session-AMBR/ Subsequent Authorized default 5QI/ARP* is only applied when the time defined by this attribute is met. When the SMF receives a *Time Condition* and *Subsequent Authorized Session-AMBR/ Subsequent Authorized default 5QI/ARP* pair, it stores it locally. The SMF shall discard any previously received *Subsequent Authorized Session-AMBR* / *Subsequent Authorized default 5QI/ARP* instances on explicit instruction as well as whenever the PCF provides a new instruction for one or more *Subsequent Authorized Session-AMBR* / *Subsequent Authorized default 5QI/ARP*. When the time defined by the *Time Condition* parameter is reached, the SMF shall apply (or instruct the UPF to apply) *Subsequent Authorized Session-AMBR/ Subsequent Authorized default 5QI/ARP*.

NOTE 3: In order to reduce the risk for signalling overload, the PCF should avoid simultaneous provisioning of the *Subsequent Authorized Session-AMBR/ Subsequent Authorized default 5QI/ARP* for many UEs (e.g. by spreading over time).

NOTE 4: In order to provide further *Subsequent Authorized Session-AMBR/ Subsequent Authorized default 5QI/ARP* in a timely fashion the PCF can use its own clock to issue the desired changes or use the Revalidation time limit parameter to trigger an SMF request for a policy decision.

NOTE 5: For services that depend on specific Session-AMBR and/or default 5QI/ARP (e.g. MPS session) the PCF is responsible to ensure that no *Subsequent Authorized Session-AMBR* or *Subsequent Authorized default 5QI/ARP* interfere with the service, e.g. by removing the *Subsequent Authorized Session-AMBR* or *Subsequent Authorized default 5QI/ARP* before the respective change time is reached.

The *Monitoring Key* is the reference to a resource threshold. Any number of PCC Rules may share the same monitoring key value. The monitoring key values for each service shall be operator configurable.

It shall also be possible for an operator to use the *Monitoring Key* parameter to indicate usage monitoring on an PDU Session level or, in the case of an MA PDU Session, to indicate usage monitoring on PDU Session level for the 3GPP access and/or the Non-3GPP access.

Usage monitoring on PDU Session level is active when a PDU Session is active when a *Monitoring Key* for the PDU Session and a corresponding volume and/or time threshold value have been provided to the SMF. Usage monitoring on Monitoring key level is active when a volume and/or time threshold has been provided for a *Monitoring Key* to the SMF and there is at least one PCC rule active for the PDU Session that is associated with that *Monitoring Key*.

The *Volume threshold* indicates the overall user traffic volume value after which the SMF shall report the Usage threshold reached trigger to the PCF.

The *Time threshold* indicates the overall resource time usage after which the SMF shall report the Usage threshold reached trigger to the PCF.

The *Monitoring time* indicates the time at which the SMF shall store the accumulated usage information.

The *Subsequent Volume threshold* indicates the overall user traffic volume value measured after Monitoring time, after which the SMF shall report the Usage threshold reached trigger to the PCF.

The *Subsequent Time threshold* indicates the overall resource time usage measured after Monitoring time, after which the SMF shall report the Usage threshold reached trigger to the PCF.

The *Inactivity Detection Time* indicates the period of time after which the time measurement shall stop, if no packets are received during that time period.

The *Port Management Information Container* carries Ethernet port management information for an Ethernet port located in DS-TT or NW-TT. The port for which the container is provided is identified by the port number.

The *Bridge Management Information Container* carries Bridge management information for a 5GS TSN bridge.

#### **\*\*\*NEXT CHANGE\*\*\***

#### 6.6.2.1 Structure Description

The UE Route Selection Policy (URSP) includes a prioritized list of URSP rules.

Table 6.6.2.1-1: UE Route Selection Policy

| Information name | Description | Category | PCF permitted to modify in a URSP | Scope |
| --- | --- | --- | --- | --- |
| URSP rules | 1 or more URSP rules as specified in table 6.6.2.1-2 | Mandatory | Yes | UE context |

The structure of the URSP rules is described in Table 6.6.2.1-2 and Table 6.6.2.1-3.

Table 6.6.2.1-2: UE Route Selection Policy Rule

| Information name | Description | Category | PCF permitted to modify in a UE context | Scope |
| --- | --- | --- | --- | --- |
| Rule Precedence | Determines the order the URSP rule is enforced in the UE. | Mandatory (NOTE 1) | Yes | UE context |
| **Traffic descriptor** | *This part defines the Traffic descriptor components for the URSP rule.* | Mandatory (NOTE 3) |  |  |
| Application descriptors | It consists of OSId and OSAppId(s). (NOTE 2) | Optional | Yes | UE context |
| IP descriptors  (NOTE 5) | Destination IP 3 tuple(s) (IP address or IPv6 network prefix, port number, protocol ID of the protocol above IP). | Optional | Yes | UE context |
| Domain descriptors | Destination FQDN(s) or a regular expression as a domain name matching criteria. | Optional | Yes | UE context |
| Non-IP descriptors  (NOTE 5) | Descriptor(s) for destination information of non-IP traffic | Optional | Yes | UE context |
| DNN | This is matched against the DNN information provided by the application. | Optional | Yes | UE context |
| Connection Capabilities | This is matched against the information provided by a UE application when it requests a network connection with certain capabilities. (NOTE 4) | Optional | Yes | UE context |
| **List of Route Selection Descriptors** | A list of Route Selection Descriptors. The components of a Route Selection Descriptor are described in table 6.6.2.1-3. | Mandatory |  |  |
| NOTE 1: Rules in a URSP shall have different precedence values.  NOTE 2: The information is used to identify the Application(s) that is(are) running on the UE's OS. The OSId does not include an OS version number. The OSAppId does not include a version number for the application.  NOTE 3: At least one of the Traffic descriptor components shall be present.  NOTE 4: The format and some values of Connection Capabilities, e.g. "ims", "mms", "internet", etc., are defined in TS 24.526 [19]. More than one connection capabilities value can be provided.  NOTE 5: A URSP rule cannot contain the combination of the Traffic descriptor components IP descriptors and Non-IP descriptors. | | | | |

Table 6.6.2.1-3: Route Selection Descriptor

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Information name | Description | Category | PCF permitted to modify in URSP | Scope |
| Route Selection Descriptor Precedence | Determines the order in which the Route Selection Descriptors are to be applied. | Mandatory (NOTE 1) | Yes | UE context |
| **Route selection components** | *This part defines the route selection components* | Mandatory (NOTE 2) |  |  |
| SSC Mode Selection | One single value of SSC mode.  (NOTE 5) | Optional | Yes | UE context |
| Network Slice Selection | Either a single value or a list of values of S-NSSAI(s). | Optional  (NOTE 3) | Yes | UE context |
| DNN Selection | Either a single value or a list of values of DNN(s). | Optional | Yes | UE context |
| PDU Session Type Selection | One single value of PDU Session Type | Optional  (NOTE 8) | Yes | UE context |
| Non-Seamless Offload indication | Indicates if the traffic of the matching application is to be offloaded to non-3GPP access outside of a PDU Session. | Optional  (NOTE 4) | Yes | UE context |
| Access Type preference | Indicates the preferred Access Type (3GPP or non-3GPP or Multi-Access) when the UE establishes a PDU Session for the matching application. | Optional | Yes | UE context |
| **Route Selection Validation Criteria**  (NOTE 6) | *This part defines the Route Validation Criteria components* | Optional |  |  |
| Time Window | The time window when the matching traffic is allowed. The RSD is not considered to be valid if the current time is not in the time window. | Optional | Yes | UE context |
| Location Criteria | The UE location where the matching traffic is allowed. The RSD rule is not considered to be valid if the UE location does not match the location criteria. | Optional | Yes | UE context |
| NOTE 1: Every Route Selection Descriptor in the list shall have a different precedence value.  NOTE 2: At least one of the route selection components shall be present.  NOTE 3: When the Subscription Information contains only one S-NSSAI in UDR, the PCF needs not provision the UE with S-NSSAI in the Network Slice Selection information. The "match all" URSP rule has one S-NSSAI at most.  NOTE 4: If this indication is present in a Route Selection Descriptor, no other components shall be included in the Route Selection Descriptor.  NOTE 5: The SSC Mode 3 shall only be used when the PDU Session Type is IP.  NOTE 6: The Route Selection Descriptor is not considered valid unless all the provided Validation Criteria are met.  NOTE 7: In this Release of specification, inclusion of the Validation Criteria in Roaming scenarios is not considered.  NOTE 8: When the PDU Session Type is "Ethernet" or "Unstructured", this component shall be present. | | | | |

Each URSP rule contains a Traffic descriptor (containing one or more components described in Table 6.6.2.1-2) that determines when the rule is applicable. A URSP rule is determined to be applicable when every component in the Traffic descriptor matches the corresponding information from the application. A URSP rule is determined not to be applicable when for any given component in the Traffic descriptor:

- No corresponding information from the application is available; or

- The corresponding information from the application does not match any of the values in the Traffic descriptor component.

NOTE 1: It is recommended to avoid listing more than two components in the Traffic descriptor of a URSP rule.

If a URSP rule is provided that contains a Traffic descriptor with two or more components, it is recommended to also provide URSP rule(s) with lower precedence and a Traffic descriptor with less components, in order to increase the likelihood of URSP rule matching for a particular application.

Each URSP rule contains a list of Route Selection Descriptors containing one or multiple Route Selection Descriptors each having a different Route Selection Descriptor Precedence value. A Route Selection Descriptor contains one or more of the following components:

- Session and Service Continuity (SSC) Mode: Indicates that the traffic of the matching application shall be routed via a PDU Session supporting the included SSC Mode.

- Network Slice Selection: Indicates that the traffic of the matching application shall be routed via a PDU Session supporting any of the included S-NSSAIs, see clause 5.15.4 in TS 23.501 [2]. It includes one or more S-NSSAI(s).

- DNN Selection: Indicates that the traffic of the matching application shall be routed via a PDU Session supporting any of the included DNNs. It includes one or more DNN(s). When DNN is used in Traffic descriptor, corresponding Route Selection Descriptor of the rule shall not include DNN Selection component.

- PDU Session Type Selection: Indicates that the traffic of matching application shall be routed via a PDU Session supporting the included PDU Session Type. The possible PDU Session Types are defined in clause 5.6.10 in TS 23.501 [2].

- Non-Seamless Offload indication: Indicates that traffic of the matching application is to be offloaded to non-3GPP access outside of a PDU Session when the rule is applied. If this component is present in a Route Selection Descriptor, no other components shall be included in the Route Selection Descriptor.

- Access Type Preference: If the UE needs to establish a PDU Session when the rule is applied, this indicates the Access Type (3GPP or non-3GPP or multi-access) on which the PDU Session should be established. The type "Multi-Access" indicates that the PDU Session should be established as a MA PDU Session, using both 3GPP access and non-3GPP access.

- Time Window: The Route Selection Descriptor is not be considered valid unless the UE is in the time window.

- Location Criteria: The Route Selection Descriptor is not be considered valid unless the UE's location matches the Location Criteria.

NOTE 2: The structure of the URSP does not define how the PCF splits the URSP when URSP cannot be delivered to the UE in a single NAS message.

NOTE 3: It is expected that UE applications will not be able to change or override the PDU Session parameters in the URSP rules. A UE application can express preferences when it requests a network connection (e.g. certain Connection Capabilities), which can be mapped into specific PDU Session parameters by the URSP rules.

NOTE 4: When one Route Selection Descriptor in a URSP rule contains a Time Window or Location Criteria, all Route Selection Descriptors in the URSP rule must contain a Time Window or Location Criteria.

In the case of network rejection of the PDU Session Establishment Request, the UE may trigger a new PDU Session establishment based on the rejection cause and the URSP policy.

When the PCF provisions URSP rules to the UE, one URSP rule with a "match all" Traffic descriptor may be included.

NOTE 5: When URSP rules containing NSSP are available to the UE and the URSP rule with the "match all" Traffic descriptor is not part of them, a UE application that has no matching URSP rule and no UE Local Configuration cannot request a network connection.

The URSP rule with the "match all" Traffic descriptor is used to route the traffic of applications which do not match any other URSP rules and shall therefore be evaluated as the last URSP rule, i.e. with lowest priority. There shall be only one Route Selection Descriptor in this URSP rule. The Route Selection Descriptor in this URSP rule includes at most one value for each Route Selection Component.

NOTE 6: How to set the URSP rule with the "match all" Traffic descriptor as the URSP rule with lowest priority is defined in TS 24.526 [19].

#### **\*\*\*NEXT CHANGE\*\*\***

#### 6.6.2.3 UE procedure for associating applications to PDU Sessions based on URSP

For every newly detected application the UE evaluates the URSP rules in the order of Rule Precedence and determines if the application is matching the Traffic descriptor of any URSP rule.

When a URSP rule is determined to be applicable for a given application (see clause 6.6.2.1), the UE shall select a Route Selection Descriptor within this URSP rule in the order of the Route Selection Descriptor Precedence.

When a valid Route Selection Descriptor is found, the UE determines if there is an existing PDU Session that matches all components in the selected Route Selection Descriptor. The UE compares the components of the selected Route Selection Descriptor with the existing PDU Session(s) as follows:

- For a component which only contains one value (e.g. SSC mode), the value of the PDU Session has to be identical to the value specified in the Route Selection Descriptor.

- For a component which contains a list of values (e.g. Network Slice Selection), the value of the PDU Session has to be identical to one of the values specified in the Route Selection Descriptor.

- When some component(s) is not present in the Route Selection Descriptor, a PDU Session is considered matching only if it was established without including the missing component(s) in the PDU Session Establishment Request.

- When the Route Selection Descriptor includes a Time Window or a Location Criteria, the PDU Session is considered matching only if the PDU Session is associated with an RSD that has the same Time Window or a Location Criteria Validity Conditions.

When a matching PDU Session exists the UE associates the application to the existing PDU Session, i.e. route the traffic of the detected application on this PDU Session.

If the UE determines that there is more than one existing PDU Session which matches (e.g. the selected Route Selection Descriptor only specifies the Network Slice Selection, while there are multiple existing PDU Sessions matching the Network Slice Selection with different DNNs), it is up to UE implementation to select one of them to use.

NOTE 1: When more than one PDU Sessions of SSC mode 3 to the same DNN and S-NSSAI exist due to PDU Session anchor change procedure as described in clause 4.3.5.2 of TS 23.502 [3], the UE can take the PDU Session Address Lifetime value into account when selecting the PDU Session.

If none of the existing PDU Sessions matches, the UE tries to establish a new PDU Session using the values specified by the selected Route Selection Descriptor. If the PDU Session Establishment Request is accepted, the UE associates the application to this new PDU Session. If the PDU Session Establishment Request is rejected, based on the rejection cause, the UE selects another combination of values in the currently selected Route Selection Descriptor if any other value for the rejected component in the same Route Selection Description can be used. Otherwise, the UE selects the next Route Selection Descriptor, which contains a combination of component value which is not rejected by network, in the order of the Route Selection Descriptor Precedence, if any. If the UE fails to establish a PDU Session with any of the Route Selection Descriptors, it tries other URSP rules in the order of Rule Precedence with matching Traffic descriptors, except the URSP rule with the "match-all" Traffic descriptor, if any. The UE shall not use the UE Local Configuration in this case.

The UE receives the updated URSP rules and (re-)evaluates their validities in a timely manner when certain conditions are met, for example:

- the URSP is updated by the PCF;

- the UE moves from EPC to 5GC;

- change of Allowed NSSAI or Configured NSSAI;

- change of LADN DNN availability;

- UE registers over 3GPP or non-3GPP access;

- UE establishes connection to a WLAN access.

Details of the conditions are defined by TS 24.526 [19].

NOTE 2: When providing the updated URSP rules to the UE with a new DNN, the PCF can set the SMF selection management trigger in the AMF to contact the PCF at PDU Session establishment (as specified in clause 6.1.2.5) if the old DNN is requested by the UE.

The Route Selection Descriptor of a URSP rule shall be only considered valid if all of the following conditions are fulfilled:

- If any S-NSSAI(s) is present, the S-NSSAI(s) is in the Allowed NSSAI for the non-roaming case and in the mapping of the Allowed NSSAI to HPLMN S-NSSAI(s) for the roaming case.

- If any DNN is present and the DNN is an LADN DNN, the UE is in the area of availability of this LADN.

- If Access Type preference is present and set to Multi-Access, the UE supports ATSSS.

- If a Time Window is present and the time matches what is indicated in the Time Window.

- If a Location Criteria is present and the UE location matches what is indicated in the Location Criteria.

If a matching URSP rule has no valid RSD, the UE tries other URSP rules in the order of Rule Precedence with matching Traffic descriptors, except the URSP rule with "match-all" Traffic descriptor. The UE shall not use the UE Local Configuration in this case.

When URSP rules are updated or their validity according to the conditions above change, the association of existing applications to PDU Sessions may need to be re-evaluated. The UE may also re-evaluate the application to PDU Session association due to the following reasons:

- periodic re-evaluation based on UE implementation;

- an existing PDU Session that is used for routing traffic of an application based on a URSP rule is released;

- The expiration of Time Window in Route Selection Validation Criteria, i.e. the expiration of Time Window, or UE's location no longer matches the Location Criteria.

NOTE 3: It is up to UE implementation to avoid frequent re-evaluation due to location change.

If the re-evaluation leads to a change of the application to PDU Session association, e.g. the application is to be associated with another PDU Session or a new PDU Session needs to be established, the UE may enforce such changes in a timely manner based on implementation, e.g. immediately or when UE enters CM-IDLE state.

If the selected Route Selection Descriptor contains a Non-Seamless Offload indication and the UE has established a connection to a WLAN access, the UE routes the traffic matching the Traffic descriptor of the URSP rule via the WLAN access outside of a PDU Session.

#### **\*\*\*NEXT CHANGE\*\*\***

Annex A (informative):  
URSP rules example

As an example, the URSP rules provisioned in the UE may include the following rules:

Table A-1: Example of URSP rules

|  |  |  |
| --- | --- | --- |
| Example URSP rules | | Comments |
| Rule Precedence =1  Traffic Descriptor: Application descriptor=App1 | Route Selection Descriptor Precedence=1  Network Slice Selection: S-NSSAI-a  SSC Mode Selection: SSC Mode 3  DNN Selection: internet  Access Type preference: 3GPP access | This URSP rule associates the traffic of application "App1" with S-NSSAI-a, SSC Mode 3, 3GPP access and the "internet" DNN.  It enforces the following routing policy:  The traffic of App1 should be transferred on a PDU Session supporting S-NSSAI-a, SSC Mode 3 and DNN=internet over 3GPP access. If this PDU Session is not established, the UE shall attempt to establish a PDU Session with S-NSSAI-a, SSC Mode 3 and the "internet" DNN over 3GPP access. |
| Rule Precedence =2  Traffic Descriptor: Application descriptor=App2 | Route Selection Descriptor Precedence =1  Network Slice Selection: S-NSSAI-a  Access Type preference: Non-3GPP access | This URSP rule associates the traffic of application "App2" with S-NSSAI-a and Non-3GPP access.  It enforces the following routing policy:  The traffic of application App2 should be transferred on.  a PDU Session supporting S-NSSAI-a using a Non-3GPP access. If this PDU Session is not established, the UE shall attempt to establish a PDU Session with S-NSSAI-a over Access Type=non-3GPP access. |
|  | Route Selection Descriptor Precedence =2  Non-seamless Offload indication: Permitted (WLAN SSID-a) | If the PDU Session cannot be established, the traffic of App2 shall be directly offloaded to WLAN, if the UE is connected to a WLAN with SSID-a (based on the 2nd RSD) |
| Rule Precedence =3  Traffic Descriptor: DNN=DNN\_1 | Route Selection Descriptor Precedence =1  Network Slice Selection: S-NSSAI-a  Access Type preference: Non-3GPP access | This URSP rule associates the traffic of applications that are configured to use DNN\_1 with DNN\_1, S-NSSAI-a over Non-3GPP access.  It enforces the following routing policy:  The traffic of application(s) that are configured to use DNN\_1 should be transferred on a PDU Session supporting S-NSSAI-a over Non-3GPP access. If this PDU Session is not established, the UE shall attempt to establish the PDU Session with S-NSSAI-a over Non-3GPP access. |
| Rule Precedence =4  Traffic Descriptor:  Application descriptor=App1  Connection Capabilities="internet", "supl" | Route Selection Descriptor Precedence =1  Network Slice Selection: S-NSSAI-a  DNN Selection: DNN\_1  Access Type preference: Non-3GPP access | This URSP rule associates the application "App1" and the Connection Capabilities "internet" and "supl" with DNN\_1, S-NSSAI-a over Non-3GPP access.  It enforces the following routing policy:  When the "App1" requests a network connection with Connection Capability "internet" or "supl", the UE establishes (if not already established) a PDU Session with DNN\_1 and S-NSSAI-a over Non-3GPP access. After that, the UE routes the traffic of "App1" over this PDU Session. |
| Rule Precedence =5  Traffic Descriptor:  OSAppId=App3  Connection Capabilities="ims" | Route Selection Descriptor Precedence =1  Network Slice Selection: S-NSSAI-c  DNN Selection: DNN\_1  Access Type preference: Multi-Access | This URSP rule associates the application "App3" and the Connection Capability "ims" with DNN\_1, S-NSSAI-c and multi-access connectivity.  It enforces the following routing policy:  When the "App3" requests a network connection with Connection Capability "ims", the UE establishes (if not already established) a MA PDU Session with DNN\_1 and S-NSSAI-c. After that, the UE routes the traffic of "App3" over this MA PDU Session by using the received ATSSS rules. |
| Rule Precedence =6  Traffic Descriptor: Application descriptor=App1 | Route Selection Descriptor Precedence =1  DNN Selection: DNN\_1  Network Slice Selection: S-NSSAI-a  Access Type preference: Multi Access | This URSP rule associates App 1 with DNN\_1, S-NSSAI-a with Multi Access connectivity.  It enforces the following routing policy:  The traffic of Application 1 should be transferred on a PDU Session supporting S-NSSAI-a and DNN\_1 according to the received ATSSS rules. After that the UE routes the traffic of any other application according to the ATSSS rule with match all packet filters if available. |
| Rule Precedence = lowest priority  Traffic Descriptor: \* | Route Selection Descriptor Precedence =1  Network Slice Selection: S-NSSAI-b  SSC Mode Selection: SSC Mode 3  DNN Selection: internet | This URSP rule associates all traffic not matching any prior rule a PDU Session with S-NSSAI-b, SSC Mode 3 and the "internet" DNN.  It enforces the following routing policy:  All traffic not matching any prior rule should be transferred on a PDU Session supporting S-NSSAI-b, SSC Mode 3 and DNN=internet with no access network preference. |

#### **\*\*\*NEXT CHANGE\*\*\***

Annex C (Normative):  
Support for Application Functions supporting Rx interface

To allow the 5G system to interwork with AFs related to existing services, e.g. IMS based services as described in TS 23.228 [5], Mission Critical Push To Talk services as described in TS 23.179 [6], the PCF shall support the corresponding IMS procedures defined in the main body of this TS via Rx interface. This facilitates the migration from EPC to 5GC without requiring these AFs to upgrade to support the Npcf\_PolicyAuthorization services in Rel-16.



Figure C-1: Interworking between 5G Policy framework and AFs supporting Rx interface

Session Binding applies for PDU Sessions of IP type only.

The functionality described for Multimedia Priority Services (clause 6.11) and Mission Critical service (clause 6.19) applies via Rx interface.

In order to support IMS Emergency services over Rx interface, in addition to the functional description in clause 6.10, the following applies: The PCF shall provide the IMEI and the subscriber identifiers (IMSI, MSISDN) (if available), received from the SMF at PDU Session establishment, if so requested by the P-CSCF. The PCF derives the IMEI from the PEI, the IMSI from the SUPI and the MSISDN from the GPSI.

NOTE 1: TS 23.501 [2] defines both 5G identifiers, SUPI, PEI and GPSI and then how they are allocated to allow interworking with functional entities not supporting 5G identifies such as P-CSCF.

Any AF using Rx, such as P-CSCF, the BSF determines the selected PCF address according to the information included in the incoming Rx requests and the information stored at the BSF. The BSF is able to proxy or redirect Rx requests targeting an IP address of a UE to the selected PCF.

The following event reporting is supported over Rx interface:

Table C-1: Events relevant for reporting from the PCF

|  |  |  |
| --- | --- | --- |
| Event | Description | Availability for Rx Session |
| PLMN Identifier Notification | The PLMN identifier where the UE is currently located. | Yes |
| Change of Access Type | The Access Type and, if applicable, the RAT Type of the PDU Session has changed. | Yes |
| EPS fallback | EPS fallback is initiated | Yes |
| Signalling path status | The status of the resources related to the signalling traffic of the AF session. | Yes |
| Access Network Charging Correlation Information | The Access Network Charging Correlation Information of the resources allocated for the AF session. | Yes |
| Access Network Information Notification | The user location and/or timezone when the PDU Session has changed in relation to the AF session. | Yes |
| Reporting Usage for Sponsored Data Connectivity | The usage threshold provided by the AF has been reached; or the AF session is terminated. | Yes |
| Resource allocation status | The status of the resources related to the AF session (established/released). | Yes |
| QoS targets can no longer (or can again) be fulfilled | The QoS targets can no longer (or can again) be fulfilled by the network for (a part of) the AF session. | No |
| Out of credit | Credit is no longer available. | Yes |

#### **\*\*\*END OF CHANGES\*\*\***