TTA Standard

정보통신단체표준(기술규격) 제정일: 2018 년 9 월
TTAT.3G-23.503(R15-15.2.0)

3GPP-(Technical Speciation Group Services and System Aspects; Policy and Charging Control Framework for the 5G System; Stage 2)

한국정보통신기술협회
Telecommunications Technology Association

3GPP TS 23.503 V15.2.0 (2018-06)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and Charging Control Framework for the 5G System; Stage 2 (Release 15)

Keywords
5G System, Policy, Charging, Performance

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword 6
Introduction 6
1 Scope 7
2 References 7
3 Definitions and abbreviations 8
3.1 Definitions 8
3.2 Abbreviations 8
4 High level architectural requirements 8
4.1 General requirements 8
4.2 Non-session management related policy control requirements 9
4.2.1 Access and mobility related policy control requirements 9
4.2.2 UE access selection and PDU Session selection related policy (UE policy) control requirements 9
4.2.3 Network status analytics information requirements 9
4.2.4 Management of packet flow descriptions 9
4.3 Session management related policy control requirements 10
4.3.1 General requirements 10
4.3.2 Charging related requirements 10
4.3.3 Policy control requirements 10
4.3.3.1 Gating control requirements 10
4.3.3.2 QoS control requirements 11
4.3.3.2.1 QoS control at service data flow level 11
4.3.3.2.2 QoS control at QoS Flow level 11
4.3.3.2.3 QoS control at PDU Session level 11
4.3.3.3 Subscriber spending limits requirements 11
4.3.4 Usage monitoring control requirements 12
4.3.5 Application detection and control requirements 12
4.3.6 Support for service capability exposure 12
4.3.7 Traffic steering control 12
5 Architecture model and reference points 13
5.1 General 13
5.2 Reference architecture 13
5.2.1 Non-roaming architecture 13
5.2.2 Roaming architecture 14
5.2.3 Interworking with AFs supporting Rx interface 16
5.3 Service-based interfaces and reference points 17
5.3.1 Interactions between PCF and AF 17
5.3.2 Interactions between PCF and SMF 17
5.3.3 Interactions between PCF and AMF 18
5.3.4 Interactions between V-PCF and H-PCF 18
5.3.5 Interactions between PCF and UDR 18
5.3.6 Interactions between SMF and CHF 18
5.3.7 Void 18
5.3.8 Interactions between PCF and CHF 19
5.3.9 Interactions between SMF and NEF 19
5.3.10 Interactions between NEF and PCF 19
5.3.11 Interactions between NWDAF and PCF 19
6 Functional description 20
6.1 Overall description 20
6.1.1 General 20
6.1.1.1 PCF Discovery and Selection 20
6.1.1.2 Binding an AF request targeting an UE address to the relevant PCF 20
6.1.1.2.1 General 20
6.1.1.2.2 The Binding Support Function (BSF) 20

6.1.1.3 Policy decisions based on network analytics 21
6.1.2 Non-session management related policy control 21
6.1.2.1 Access and mobility related policy control 21
6.1.2.2 UE access selection and PDU Session selection related policy (UE policy) control 22
6.1.2.2.1 General 22
6.1.2.2.2 Distribution of the policies to UE 23
6.1.2.3 Management of packet flow descriptions 24
6.1.2.3.1 PFD management 24
6.1.2.3.2 Packet Flow Description 26
6.1.2.4 Negotiation for future background data transfer 26
6.1.2.5 Policy Control Request Triggers relevant for AMF 27
6.1.3 Session management related policy control 27
6.1.3.1 General 27
6.1.3.2 Binding mechanism 28
6.1.3.2.1 General 28
6.1.3.2.2 Session binding 28
6.1.3.2.3 PCC rule authorization 28
6.1.3.2.4 QoS Flow binding 29
6.1.3.3 Reporting 29
6.1.3.4 Credit management 30
6.1.3.5 Policy Control Request Triggers relevant for SMF 30
6.1.3.6 Policy control 34
6.1.3.7 Service (data flow) prioritization and conflict handling 35
6.1.3.8 Termination action 35
6.1.3.9 Handling of packet filters provided to the UE by SMF 35
6.1.3.10 IMS emergency session support 35
6.1.3.11 Multimedia Priority Service support 36
6.1.3.12 Redirection 37
6.1.3.13 Resource sharing for different AF sessions 37
6.1.3.14 Traffic steering control 37
6.1.3.15 Resource reservation for services sharing priority 37
6.1.3.16 3GPP PS Data Off 38
6.1.3.17 Policy decisions based on spending limits 39
6.2 Network functions and entities 40
6.2.1 Policy Control Function (PCF) 40
6.2.1.1 General 40
6.2.1.2 Input for PCC decisions 41
6.2.1.3 Policy control subscription information management 43
6.2.1.4 V-PCF 45
6.2.1.5 H-PCF 45
6.2.1.6 Application specific policy information management 45
6.2.2 Session Management Function (SMF) 46
6.2.2.1 General 46
6.2.2.2 Service data flow detection 46
6.2.2.3 Measurement 46
6.2.2.4 QoS control 46
6.2.2.5 Application detection 47
6.2.2.6 Traffic steering 47
6.2.3 Application Function (AF) 47
6.2.4 Unified Data Repository (UDR) 47
6.2.5 Charging Function (CHF) 47
6.2.6 Void 48
6.2.7 Network Exposure Function (NEF) 48
6.2.8 Access and Mobility Management Function (AMF) 48
6.2.9 Network Data Analytics Function (NWDAF) 48
6.3 Policy and charging control rule 48
6.3.1 General 48
6.3.2 Policy and charging control rule operations 53
6.4 PDU Session related policy information 54
6.5 Access and mobility related policy information 58
6.6 UE access selection and PDU Session selection related policy information 59
6.6.1 Access Network Discovery & Selection Policy Information 59

6.6.1.1 General 59
6.6.1.2 UE selecting a WLANSP rule 59
6.6.1.3 UE procedure for selecting a WLAN access based on WLANSP rules 59
6.6.2 UE Route Selection Policy information 60
6.6.2.1 Structure Description 60
6.6.2.2 Configuration and Provision of URSP 62
6.6.2.3 UE procedure for associating applications to PDU Sessions based on URSP 62

Annex A(informative): URSP rules example 64

Annex B (informative): Deployment option to support of BSF and DRA coexistence due to network migration 65

Annex C (informative): Change history 66

Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

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

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

Introduction

For references to TS 23.203 [4] made in this document,

- the IP-CAN session of TS 23.203 [4] maps to the PDU Session in 5GC.
- the APN of TS 23.203 [4] maps to DNN in 5GC.
- the IP-CAN bearer of TS 23.203 [4] maps to the QoS Flow in 5GC.
- The PCRF of TS 23.203 [4] maps to the PCF in 5GC.
- The PCEF of TS 23.203 [4] maps to the combination of SMF and UPF in 5GC.
- The BBF shall be considered as being located in the PCEF.
- TDF related description does not apply.
- NBIFOM related description does not apply.

1 Scope

The present document defines the Stage 2 policy and charging control framework for the 5G System specified in TS 23.501 [2] and TS 23.502 [3].

The policy and charging control framework encompasses the following high level functions:

- Flow Based Charging for network usage, including charging control and online credit control, for service data flows;
- Policy control for session management and service data flows (e.g. gating control, QoS control, etc.);
- Management for access and mobility related policies;
- Management for UE access selection and PDU Session selection related policies.

It refers to the policy and charging control functionality specified in TS 23.203 [4] for policy and charging control for PDU Sessions, depicting the differences where those exist.

Interworking with E-UTRAN connected to EPC is described in TS 23.501 [2].

TS 23.502 [3] contains the stage 2 procedures and flows for the policy and charging control framework and it is a companion specification to this specification.

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] 3GPP TS 23.335: "User Data Convergence (UDC); Technical realization and information flows; Stage 2".

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

[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".

3 Definitions and abbreviations

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], TS 23.203 [4] 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].

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].

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 the above.

User Preferences: The list of configuration parameters provided by the layer (e.g. application) over NAS and used by the UE for access network and discovery selection and PDU Session selection.

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 23.203 [4] 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].

ANDSP	Access Network Discovery & Selection Policy
BSF	Binding Support Function
CHF	CHarging Function
H-PCF	A PCF in the HPLMN
NWDAF	Network Data Analytics Function
OCS	Online Charging System
PFD	Packet Flow Description
URSP	UE Route Selection Policy
V-PCF	A PCF in the VPLMN
WLANSP	WLAN Selection Policy

4 High level architectural requirements

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, access and 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.

4.2 Non-session management related policy control requirements

4.2.1 Access and mobility related policy control requirements

The policy framework shall provide following functionality for the access and mobility enforcement:

- Policy Control Function (PCF) shall support interactions with the access and mobility policy enforcement in the AMF, through service-based interfaces.
- The PCF shall be able to provide Access and Mobility Management related policies to the AMF.
- The PCF shall be able to evaluate operator policies that are triggered by events received from the AMF.

4.2.2 UE access selection and PDU Session selection related policy (UE policy) control requirements

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

- Access Network Discovery & Selection Policy (ANDSP): It is used by the UE for selecting non-3GPP accesses network.
- UE Route Selection Policy (URSP): This policy is used by the UE to determine how to route outgoing traffic. Traffic can be routed 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

4.2.3 Network status analytics information requirements

The PCF shall be able to collect directly slice specific network status analytic information from NWDAF. NWDAF provides network data analytics (i.e. load level information) to PCF on a network slice level and the NWDAF is not required to be aware of the current subscribers using the slice. PCF shall be able to use that data in its policy decisions.

4.2.4 Management of packet flow descriptions

Management of Packet Flow Descriptions (PFDs) refers to the capability to create, update or remove PFDs in the NEF (PFDF) and the distribution from the NEF (PFDF) to the SMF and finally to the UPF. This feature may be used when the UPF is configured to detect a particular application provided by an ASP.

NOTE 1: A possible scenario for the management of PFDs in the SMF is when an application, identified by an application detection filter in the UPF, deploys a new server or a reconfiguration occurs in the ASP network which impacts the application detection filters of that particular application.

NOTE 2: The management of application detection filters in the SMF can still be performed by using operation and maintenance procedures.

NOTE 3: This feature aims for both: to enable accurate application detection at the UPF and to minimize storage requirements for the UPF and the SMF.

The management of PFDs is supported in non-roaming and home-routed scenarios for those ASPs that have a business relation with the home operator.

4.3 Session management related policy control requirements

4.3.1 General requirements

It shall be possible for the PCC framework to base decisions upon subscription information, Access Type and the RAT Type.

The PCC framework shall perform Gating Control and discard packets that don't match any service data flow of the active PCC rules. It shall also be possible for the operator to define PCC rules, with wild-carded service data flow filters, to allow sending or receiving packets that do not match any service data flow template of any other active PCC rules.

The PCC framework shall allow the charging control to be applied on a per service data flow and on a per application basis, independent of the policy control.

The PCC framework shall have a binding method that allows the unique association between service data flows and specific QoS Flow.

A single service data flow detection shall suffice for the purpose of both policy control and flow based charging.

A PCC rule may be predefined or dynamically provisioned at establishment and during the lifetime of a PDU Session. The latter is referred to as a dynamic PCC rule.

It shall be possible to take a PCC rule into service, and out of service, at a specific time of day, without any PCC interaction at that point in time.

It shall be possible to take DNN-related policy information into service, and out of service, once validity conditions specified as part of the DNN-related policy information are fulfilled or not fulfilled anymore, respectively, without any PCC interaction at that point in time.

PCC shall be enabled on a per DNN basis at the SMF. It shall be possible for the operator to configure the PCC framework to perform charging control, policy control or both for a DNN access.

The PCC framework shall allow the resolution of conflicts which would otherwise cause a subscriber's Subscribed Guaranteed Bandwidth QoS to be exceeded.

It should be possible to use PCC framework for handling IMS-based emergency service.

It shall be possible with the PCC framework, in real-time, to monitor the overall amount of resources that are consumed by a user and to control usage independently from charging mechanisms, the so-called usage monitoring control.

It shall be possible for the PCC framework to provide application awareness even when there is no explicit service level signalling.

The PCC framework shall support making policy decisions based on subscriber spending limits.

The PCC framework shall support making policy decisions for N6 traffic steering.

4.3.2 Charging related requirements

The charging related requirements defined in clause 4.2 of TS 23.203 [4] apply.

4.3.3 Policy control requirements

4.3.3.1 Gating control requirements

Gating control shall be applied by the UPF on a per service data flow basis.

To enable the PCF gating control decisions, the AF shall report session events (e.g. session termination, modification) to the PCF. For example, session termination, in gating control, may trigger the blocking of packets or "closing the gate".

Gating Control applies for service data flows of IP type.

4.3.3.2 QoS control requirements

4.3.3.2.1 QoS control at service data flow level

It shall be possible to apply QoS control on a per service data flow basis in the SMF, applicable for service data flows of both IP type and Ethernet type.

QoS control per service data flow allows the PCC framework to provide the SMF with the authorized QoS to be enforced for each specific service data flow. Criteria such as the QoS subscription information may be used together with policy rules such as, service-based, subscription-based, or predefined PCF internal policies to derive the authorized QoS to be enforced for a service data flow.

It shall be possible to apply multiple PCC rules, without application provided information, using different authorised QoS within a single PDU Session and within the limits of the Subscribed QoS profile.

4.3.3.2.2 QoS control at QoS Flow level

It shall be possible for the PCC framework to support control of QoS reservation procedures (UE-initiated or network-initiated). It shall be possible to determine the QoS to be applied in QoS reservation procedures (QoS control) based on the authorised QoS of the service data flows that are applicable to the QoS Flow and on criteria such as the QoS subscription information, service based policies, and/or predefined PCF internal policies.

It shall be possible for the SMF to determine the authorized QoS of a QoS Flow using the PCC rules associated to the QoS Flow, and the SMF shall be able to notify the PCF if the QoS targets for a QoS Flow cannot be fulfilled.

It shall be possible for the PCC framework to support control of QoS for the packet traffic of the PDU Session.

The PCC framework shall be able to provide policy control in the presence of NAT devices. This may be accomplished by providing appropriate address and port information to the PCF.

The enforcement of the control for QoS reservation procedures for a QoS Flow shall allow for a downgrading or an upgrading of the requested QoS as part of a UE-initiated QoS Flow establishment and modification. The PCC framework shall be able to provide a mechanism to initiate QoS Flow establishment and modification as part of the QoS control.

The PCC framework shall be able to handle QoS Flows that require a guaranteed bitrate (GBR bearers) and QoS Flows for which there is no guaranteed bitrate (non-GBR bearers).

4.3.3.2.3 QoS control at PDU Session level

It shall be possible for the PCF to provide the authorized Session-AMBR values, default 5QI/ARP combination for PDU Session of IP type, Ethernet type and unstructured type unconditionally or conditionally, i.e. per PDU Session type and/or RAT type.

It shall be possible for the PCF to request a change of the unconditional or conditional authorized Session-AMBR value(s) at a specific point in time.

4.3.3.3 Subscriber spending limits requirements

It shall be possible to enforce policies based on subscriber spending limits. The CHF shall maintain policy counter(s) to track spending for a subscription. These policy counters must be available in the CHF prior to their use over the N28 interface.

NOTE: The mechanism for provisioning the policy counters in the CHF is out of scope of this document.

The PCF shall request information regarding the subscriber's spending from the CHF, to be used as input for dynamic policy decisions for the subscriber, using subscriptions to spending limit reports. The CHF shall make information regarding the subscriber's spending available to the PCF using spending limit reports.

4.3.4 Usage monitoring control requirements

The requirements to monitor, both volume and time usage, and report the accumulated usage of network resources described in clause 4.4 of TS 23.203 [4] apply for PDU Sessions of type IP and Ethernet.

It shall be possible to apply usage monitoring for the accumulated usage of network resources on a per Session and user basis. This capability is required for enforcing dynamic policy decisions based on the total network usage in real-time.

The PCF that uses usage monitoring for making dynamic policy decisions shall set and send the applicable thresholds to the SMF for monitoring. The usage monitoring thresholds shall be based either on time, or on volume. The PCF may send both thresholds to the SMF. The SMF shall notify the PCF when a threshold is reached and report the accumulated usage since the last report for usage monitoring. If both time and volume thresholds were provided to the SMF, the accumulated usage since last report shall be reported when either the time or the volume thresholds are reached.

NOTE: There are reasons other than reaching a threshold that can cause the SMF to report accumulated usage to the PCF as defined in clauses 6.2.2.3.

The usage monitoring capability shall be possible for an individual or a group of service data flow(s), or for all traffic of a PDU Session in the SMF. When usage monitoring for all traffic of a PDU Session is enabled, it shall be possible to exclude an individual SDF or a group of service data flow(s) from the usage monitoring for all traffic of this PDU Session. It shall be possible to activate usage monitoring both to service data flows associated with predefined PCC rules and dynamic PCC rules, including rules with deferred activation and/or deactivation times while those rules are active.

If service data flow(s)/application(s) need to be excluded from PDU Session level usage monitoring and PDU Session level usage monitoring is enabled, the PCF shall be able to provide the an indication of exclusion from session level monitoring associated with the respective PCC rule(s).

It shall be possible to apply different usage monitoring depending on the access used to carry a Service Data Flow. PDU Session level usage monitoring is not dependent on the access used to carry a Service Data Flow.

4.3.5 Application detection and control requirements

The application detection and control feature comprise the request to detect the specified application traffic, report to the PCF on the start or stop of application traffic and to apply the specified enforcement and charging actions.

The PCF shall instruct the SMF on which applications to detect and whether to report start or stop event to the PCF by activating the appropriate PCC rules in the SMF. Reporting notifications of start and stop of application detection to the PCF may be muted.

The report to the PCF shall include the report is for start or stop, the detected application identifier and, if deducible, the service data flow descriptions for the detected application traffic.

Upon receiving the report from SMF, the PCF may make policy decisions based on the information received and may send the corresponding updated or new PCC rules to the SMF.

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

4.3.6 Support for service capability exposure

The requirements defined in clause 4.7 of TS 23.203 [4] apply.

4.3.7 Traffic steering control

Traffic Steering Control refers to the capability to activate/deactivate traffic steering policies from the PCF in the SMF for the purpose of steering the subscriber's traffic to appropriate operator or 3rd party service functions (e.g. NAT, antimalware, parental control, DDoS protection) in the (S)Gi-LAN.

AF influenced traffic diversion enables the routing of the user traffic matching the traffic filters provided in the PCC rule to a local Data Network identified by the DNAI per AF request.

The traffic steering control is supported in non-roaming and home-routed scenarios only.

5 Architecture model and reference points

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.

For each of the NFs, such as for PCF, the interfaces to the AF, to the CHF and NEF are similar to the PCRF interfaces to the AF, to the OCS and to the SCEF as specified in TS 23.203 [4]. Therefore, the PCF description refers to the PCRF for the functionality supported in 5G and the same approach applies for the AF and the NEF.

5.2 Reference architecture

5.2.1 Non-roaming architecture

The reference architecture of policy and charging control framework for the 5G System is comprised by the functions of the Policy Control Function (PCF), the Session Management Function (SMF), the User Plane Function (UPF), the Access and Mobility Management Function (AMF), the Network Exposure Functionality (NEF), the Network Data Analytics Function (NWDAF), the Charging Function (CHF), the Application Function (AF) and UDR (Unified Data Repository).

Figure 5.2.1-1 shows the service based representation and Figure 5.2.1-1a shows the reference point representation of the reference architecture of policy and charging control framework for the 5G System.

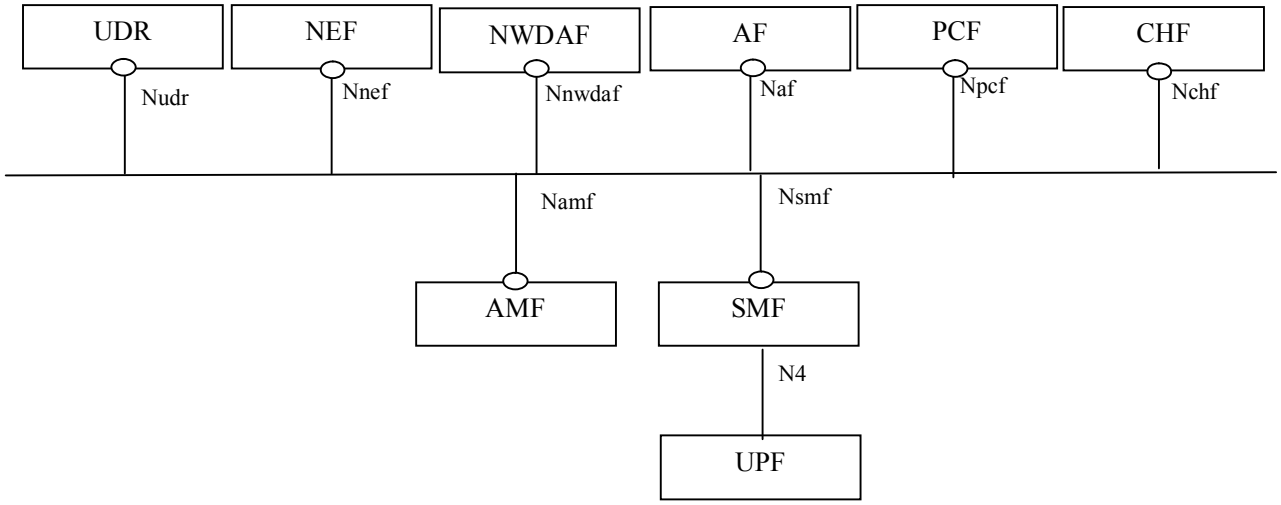

Figure 5.2.1-1: Overall non-roaming reference architecture of policy and charging control framework for the 5G System (service based representation)

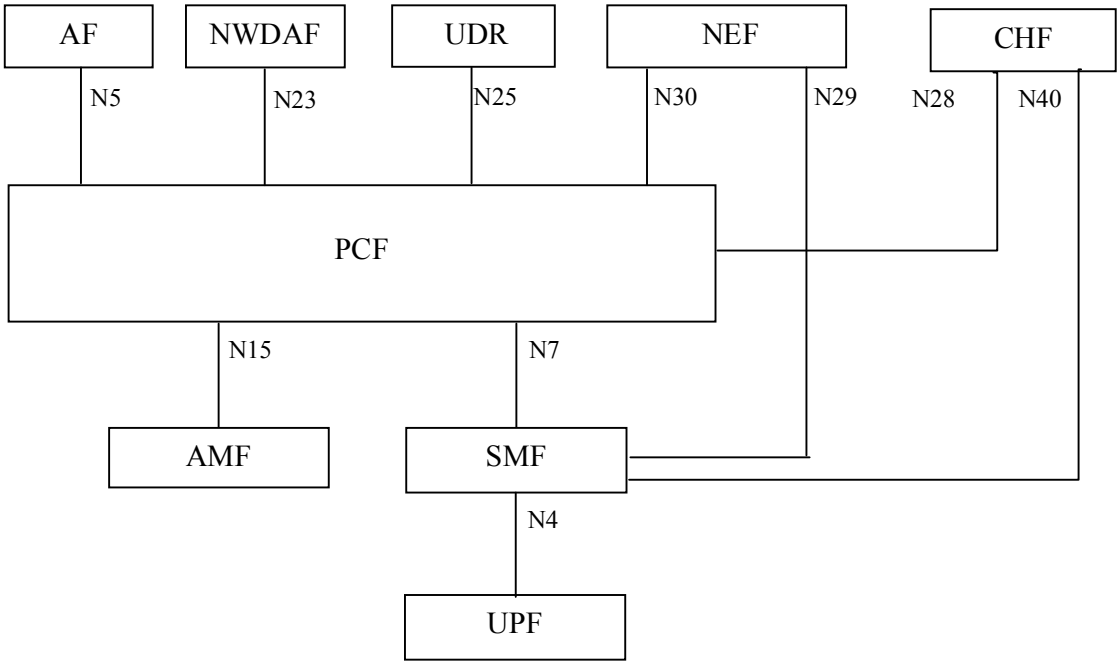

Figure 5.2.1-1a: Overall non-roaming reference architecture of policy and charging control framework for the 5G System (reference point representation)

NOTE 1: The N4 reference point is not part of the 5G Policy Framework architecture but shown in the figures for completeness. See TS 23.501 [2] for N4 reference point definition.

NOTE 2: How the PCF/NEF stores/retrieves information related with policy subscription data or with application data is defined in TS 23.501 [2].

The Nchf service for online and offline charging consumed by the SMF is defined in TS 32.240 [8].

The Nchf service for Spending Limit Control consumed by the PCF is defined in TS 23.502 [3].

5.2.2 Roaming architecture

Figure 5.2.2-1 shows the local breakout roaming policy framework architecture in 5G:

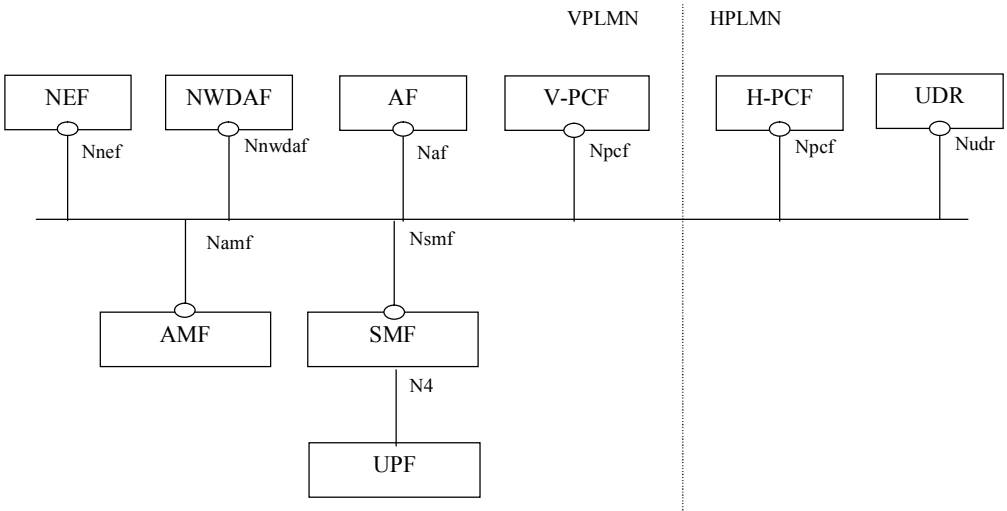

Figure 5.2.2-1: Overall roaming reference architecture of policy and charging control framework for the 5G System - local breakout scenario

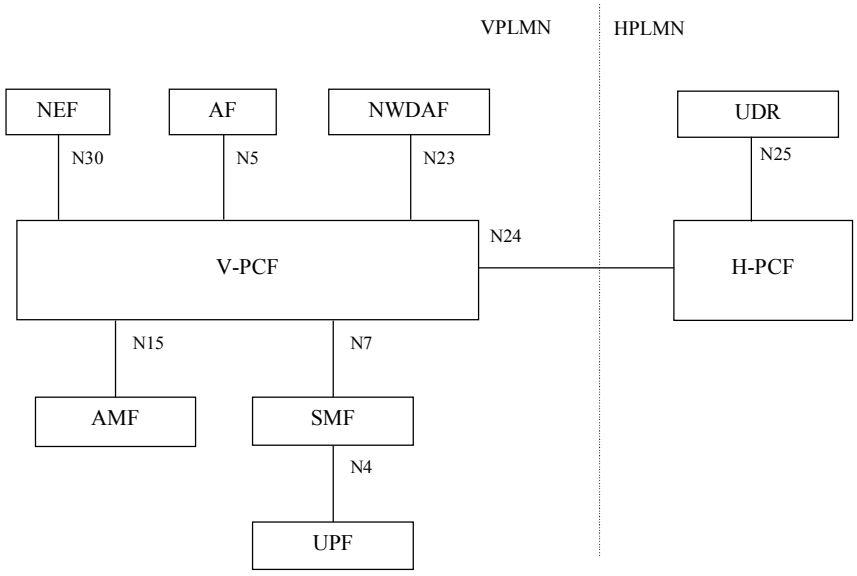

Figure 5.2.2-1a: Overall roaming reference architecture of policy and charging control framework for the 5G System - local breakout scenario (reference point representation)

NOTE 1: In the LBO architecture, the PCF in the VPLMN may interact with the AF in order to generate PCC Rules for services delivered via the VPLMN. The PCF in the VPLMN uses locally configured policies according to the roaming agreement with the HPLMN operator as input for PCC Rule generation. The PCF in VPLMN has no access to subscriber policy information from the HPLMN for PCC Rule generation.

NOTE 2: In the LBO architecture, N24 can be used to deliver UE access selection and PDU Session selection policy from the PCF in the HPLMN to the PCF in the VPLMN. The PCF in the VPLMN can provide access and motility policy information without contacting the PCF in the HPLMN.

NOTE 3: In the LBO architecture, AF requests providing routing information for roamers targeting a DNN and S-NSSAI (targeting all roamers) or an External-Group-Identifier (identifying a group of roamers) are stored as Application Data in the UDR(in the VPLMN) by the NEF (in the VPLMN).

Figure 5.2.2-2 shows the roaming policy framework architecture (home routed scenario) in 5G:

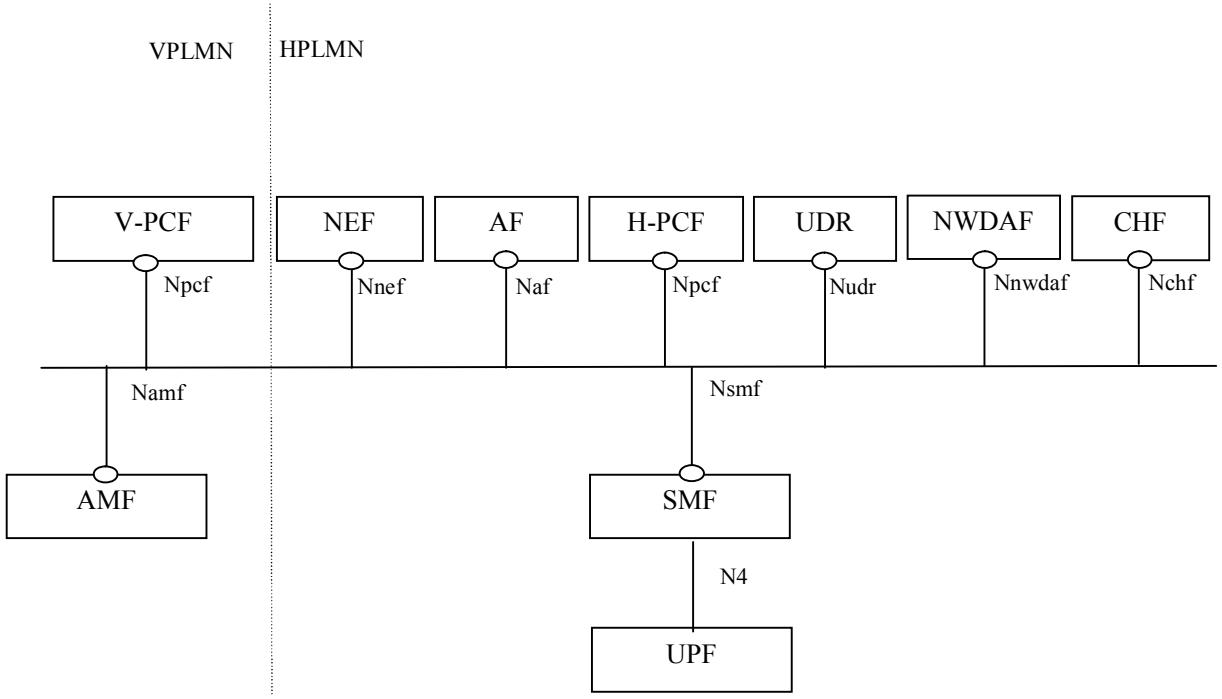

Figure 5.2.2-2: Overall roaming reference architecture of policy and charging control framework for the 5G System - home routed scenario

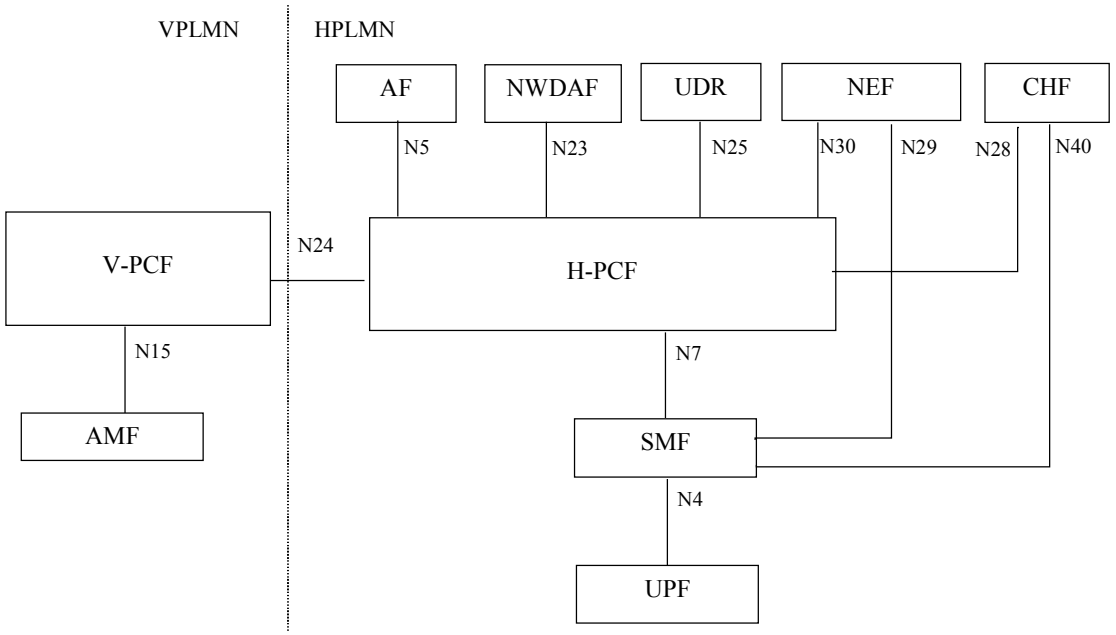

Figure 5.2.2-2a: Overall roaming reference architecture of policy and charging control framework for the 5G System - home routed scenario (reference point representation)

NOTE 3: All functional entities as described in Figure 5.2.1-1 non-roaming scenario applies also to the HPLMN in the home routed scenario above.

5.2.3 Interworking with AFs 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 Rx procedures and requirements defined in TS 23.203 [4]. This facilitates the migration from EPC to 5GC without requiring these AFs to upgrade to support the N5 interface.

Figure 5.2.3-1: Interworking between 5G Policy framework and AFs supporting Rx interface

NOTE: The use of the N5 interface by the e.g. IMS subsystem (e.g. P-CSCF) is not precluded.

5.3 Service-based interfaces and reference points

5.3.1 Interactions between PCF and AF

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

- IP filter information to identify the IP PDU traffic or the Ethernet packet filter information to identify the Ethernet PDU traffic 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].

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 6.2.1.0 of TS 23.203 [4] and change of DNAI as defined in Clause 5.6.7 of TS 23.501 [2].

NOTE: The interactions between PCF and AF need to provide the Rx functionalities for services e.g. IMS based services and Mission Critical Push To Talk services. In addition, Npcf and Naf also provide additional services.

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

5.3.2 Interactions between PCF and SMF

Npcf and Nsmf enable the PCF to have dynamic policy and charging control at a SMF.

Npcf and Nsmf enable the signalling of policy and charging decision and support the following functions:

- Creation of a SM Policy Association as defined in clause 4.16 of TS 23.502 [3];
- Request for policy and charging control decision from the SMF to the PCF when a Policy Control Request Trigger related to Session Management has been met;
- Provision of policy and charging control decision from the PCF to the SMF;
- Deletion of a SM Policy Association as defined in clause 4.16 of TS 23.502 [3].

The N7 reference point is defined for the interactions between PCF and SMF in the reference point representation.

5.3.3 Interactions between PCF and AMF

Npcf and Namf enable the PCF to provide Access and Mobility Management related policies to the AMF and it support the following functions:

- Creation of an AM Policy Association as defined in clause 4.16 of TS 23.502 [3];
- Request for access and mobility management related policies from the AMF to the PCF when a Policy Control Request Trigger related to Access and Mobility Management has been met;
- Provision of access and mobility management decision from the PCF to the AMF;
- Deletion of an AM Policy Association as defined in clause 4.16 of 23.502 [3];
- Handling of transparent delivery UE access selection and PDU Session selection policy from PCF to the UE via the AMF.

The N15 reference point is defined for the interactions between PCF and AMF in the reference point representation.

5.3.4 Interactions between V-PCF and H-PCF

For roaming scenario, the interactions between V-PCF and H-PCF through Npcf enables the H-PCF to:

- Creation of an AM Policy Association as defined in clause 4.16 of 23.502 [3];
- Provision of UE access selection and PDU Session selection related policies to the V-PCF in the VPLMN;
- Deletion of an AM Policy Association as defined in clause 4.16 of 23.502 [3].

The N24 reference point is defined for the interactions between V-PCF and H-PCF in the reference point representation.

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 N25 reference point is defined for the interactions between PCF and UDR in the reference point representation.

5.3.6 Interactions between SMF and CHF

The interactions between SMF and CHF enable online and offline charging.

The N40 reference point is defined for the interactions between SMF and CHF in the reference point representation.

Since the N40 reference point resides between the SMF and CHF in the HPLMN, roaming with home routed and non-roaming scenarios are supported in the same manner.

NOTE: The functionality of this interface/reference point is defined in TS 32.240 [8].

5.3.7 Void

5.3.8 Interactions between PCF and CHF

The Nchf_spending limit support service enables the PCF to access policy counter status information relating to subscriber spending from CHF and support the following functions:

- Request for reporting of policy counter status information from PCF to CHF and subscribe to or unsubscribe from spending limit reports (i.e. notifications of policy counter status changes).
- Report of policy counter status information upon a PCF request from CHF to PCF.
- Notification of spending limit reports from CHF to PCF.
- Cancellation of spending limit reporting from PCF to CHF.

The N28 reference point is defined for the interactions between PCF and CHF in the reference point representation.

Since the N28 reference point resides between the PCF and CHF in the HPLMN, roaming with home routed and non-roaming scenarios are supported in the same manner.

NOTE: In this Release of the specification, there is no support by the Nchf_SpendingLimitControl service between the PCF in VPLMN and the CHF in the HPLMN.

5.3.9 Interactions between SMF and NEF

Nsmf and Nnef enable transport of PFDs from the NEF to the SMF for a particular Application Identifier or for a set of Application Identifiers. It is achieved with the support of the following functions:

- Creation, updating and removal of individual or the whole set of PFDs from the NEF to the SMF.
- Confirmation of creation, updating and removal of PFDs from the SMF to the NEF.

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

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

5.3.10 Interactions between NEF and PCF

Npcf and Nnef enable the negotiation of policy and charging control behavior 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.

5.3.11 Interactions between NWDAF and PCF

The Nnwdaf is a service-based interface, which enables PCF to subscribe to and be notified on network status analytics. The following information are notified by the NWDAF:

- Identifier of network slice instance
- Load level information of network slice instance.

NOTE: How this information is used by the PCF is not standardized in this release of the specification.

The N23 reference point is defined for the interactions between NWDAF and PCF in the reference point representation.

6 Functional description

6.1 Overall description

6.1.1 General

6.1.1.1 PCF Discovery and Selection

The procedures for PCF Discovery and Selection by the AMF and by the SMF are described in TS 23.501 [2].

The procedure to ensure that an AF reaches the PCF selected for a PDU Session is described in clause 6.1.1.2.

6.1.1.2 Binding an AF request targeting an UE address to the relevant PCF

6.1.1.2.1 General

When multiple and separately addressable PCFs have been deployed, a network functionality is required in order to ensure that an AF needing to send policies about UE traffic identified by an UE address can reach over N5/Rx the PCF holding the corresponding PDU Session information. This network functionality has the following characteristics:

- It has information about the user identity, the DNN, the UE (IP or Ethernet) address(es), the DN information (e.g. S-NSSAI) and the selected PCF address for a certain PDU Session.
    - For IP PDU Session type, it shall receive information when an IP address is allocated or released for a PDU Session.
    - For Ethernet PDU Sessions supporting binding of AF request based on MAC address, it shall receive information when a MAC address is detected as being used by the UE over the PDU Session; this detection takes place at the UPF under control of SMF; This is defined in TS 23.501 [2] clause 5.8.2.
- The functionality determines the PCF address, selected by the PCF discovery and selection function described in TS 23.501 [2], according to the information carried by the incoming requests from the AF or the NEF.
- This functionality is able to proxy or redirect Rx requests targeting a UE IP address.

A private IPv4 address may be allocated to different PDU sessions, e.g.:

- The same UE IPv4 address is allocated to different PDU sessions to the same DNN and different S-NSSAI;
- The same UE IPv4 address is allocated to different PDU sessions to the same S-NSSAI and different DNN.

In the case of private IPv4 address being used for the UE, the AF or the NEF may send DNN and DN information (e.g. S-NSSAI), in addition, in Npcf_ PolicyAuthorization_Create request and Nbsf_Management_Discovery request. The DNN and DN information can be used by the PCF for session binding, and they can be also used to help selecting the correct PCF.

6.1.1.2.2 The Binding Support Function (BSF)

The BSF has the following characteristics:

- The BSF stores information about the user identity, the DNN, the UE (IP or Ethernet) address(es), the DN information (e.g. S-NSSAI) and the selected PCF address for a certain PDU Session. This information may be stored in the UDR as structured data or internally in the BSF.
- The PCF registers, updates and removes the binding information from 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.

- For retrieval binding information, any NF, such as NEF or AF, that needs to discover the selected PCF 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 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.

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

NOTE: Collocation allows combined implementation.

For any AF using Rx, such as P-CSCF, the BSF determines the selected PCF address according to the information carried by the incoming Rx requests. The BSF is able to proxy or redirect Rx requests targeting an IP address of a UE to the selected PCF.

6.1.1.3 Policy decisions based on network analytics

Policy decisions based on network analytics is a function that allows PCF taking actions related to the network analytics reported by the NWDAF as defined in TS 23.501 [2]. The requested and reported analytics type are identified by an Event ID and the scope of the analytics type is identified by the Event Filter.

The PCF may subscribe to notifications of network analytics using the Nnwdaf_Events_Subscription_Subscribe service operation including the Event ID "load level", the Event Filter are "network slice instance" and the Event Reporting Information set to either a threshold value or a time period.

When the Event Reporting Information are a threshold value, then the NWDAF notifies the PCF when the load level for a network slice instance is above the threshold and then when the load level is below the threshold. When the Event Reporting Information are a time period then the NWDAF notifies the PCF at the time the time period is reached. Notifications are performed using Nnwdaf_Events_Subscription_Notify service operation including the Event ID "load level", the Event Filter "network slice instance" and the load level information The PCF may cancel subscription to network analytics using Nnwdaf_Events_Subscription_Unsubscribe.

The PCF may request a report of a specific Event ID to the NWDAF using the Nnwdaf_Analytics_Info_Request service operation. The NWDAF provides the load level information to the PCF at the time of the request.

The PCF uses 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).

6.1.2 Non-session management related policy control

6.1.2.1 Access and mobility related policy control

The access and mobility policy control encompasses the management of service area restrictions and the management of the RFSP functionalities.

The management of service area restrictions enables the PCF of the serving PLMN (e.g. V-PCF in roaming case) to modify the service area restrictions used by AMF as described in TS 23.501 [2] clause 5.3.4.

A UE's subscription may contain service area restrictions, which may be further modified by PCF based on operator defined policies at any time, either by expanding a list of allowed TAIs or by reducing a non-allowed TAIs or by increasing the maximum number of allowed TAIs. Operator defined policies in the PCF may depend on input data such as UE location, time of day, information provided by other NFs, etc.

The AMF may report the subscribed service area restrictions received from UDM during Registration procedure or when the AMF changed, the conditions for reporting are that local policies in the AMF indicate that Access and Mobility Control is enable. The AMF reports the subscribed service area restrictions to the PCF also when the policy control request trigger for service area restrictions change, as described in clause 6.1.2.5, is met. The AMF receives the modified service area restrictions from the PCF. The AMF stores them then use it to determine mobility restriction for a UE. The PCF may indicate the AMF that there is an unlimited service area.

The service area restrictions consist of a list of allowed TAI(s) or a list of non-allowed TAI(s) and optionally the maximum number of allowed TAIs.

NOTE 1: The enforcement of the service area restrictions is performed by the UE, when the UE is in CM-IDLE state or in CM-CONNECTED state when in RRC Inactive, and in the RAN/AMF when the UE is in CM-CONNECTED state.

The management of the RFSP Index enables the PCF to modify the RFSP Index used by the AMF to perform radio resource management functionality as described in TS 23.501 [2] clause 5.3.4. PCF modifies the RFSP Index based on operator policies that take into consideration e.g. accumulated usage, load level information per network slice instance etc. The subscribed RSFP Index may be further adjusted by the PCF based on operator policies at any time.

For radio resource management, the AMF may report the subscribed RFSP Index received from UDM during the Registration procedure or when the AMF changed. The conditions for reporting are that local policies in the AMF indicate that Access and Mobility Control is enable. The AMF reports the subscribed RFSP Index to the PCF when the subscription to RFSP Index change to the PCF is met. The AMF receives the modified RFSP Index from the PCF.

NOTE 2: The enforcement of the RFSP Index is performed in the RAN.

Upon change of AMF, the source AMF informs the PCF that the UE context was removed in the AMF in the case of inter-PLMN mobility.

6.1.2.2 UE access selection and PDU Session selection related policy (UE policy) control

6.1.2.2.1 General

The 5GC shall be able to provide policy information from the PCF to the UE. Such 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. The URSP rules include traffic descriptors that specify 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).

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 PCF selects the ANDSP and URSP applicable for each UE based on local configuration, Subscribed S-NSSAIs and operator policies taking into consideration e.g. accumulated usage, load level information per network slice instance, UE location.

In the case of a roaming UE, the V-PCF may retrieve ANDSP and URSP 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 ANDSP and URSP shall be provided from the PCF to the AMF via N15/Npcf interface and then from AMF to the UE via the N1 interface. The AMF shall not change the ANDSP and the URSP provided by PCF.

When the UE has valid URSP rules, the UE shall perform the association based on user preference and these rules. URSP rules are applied as defined in clause 6.6.2.3. When there is applicable user preference for the matching application, the user preference takes precedence over any present route selection component, except for the SSC Mode Selection and Network Slice Selection components.

For the existing PDU Session(s), the UE shall examine the URSP rules within the UE Policy 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 routing rules, described in clause 5.8.1.2 in TS 23.501 [2], on the UE shall be used to select which IPv6 prefix to route the traffic of the application.

6.1.2.2.2 Distribution of the policies to UE

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

The PCF may provide the UE access selection and PDU Session related policy information at the initial Registration procedure, when Subscribed S-NSSAIs changes or when the operator policies indicate that the conditions for updating the UE are met, i.e. at change of UE location or at mobility with change the AMF, or at any time, as defined in 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 ensures that UE access selection and PDU Session related policy information delivered to the AMF, is under a predefined size limit, known by the PCF. If this predefined limit is exceeded then PCF splits the UE access selection and PDU related policy information into different Policy Sections, each one identified by a Policy Section Identifier (i.e. PSI). Each Policy Section provides a list of self-contained UE access selection and PDU Session related policy information to the UE, via AMF. The PCF delivers to the UE transparently via the AMF.

A list of self-contained UE access selection and PDU session related 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;
- when the PCF delivers WLANSP rules, the list of WLANSP rules relevant for the UE are provided in the order of priority;
- when the PCF delivers the non-3GPP access network selection information the list of non-3GPP access network selection information relevant fo the UE are provided.

The PCF may divide the UE access selection and PDU Session related policy information into different Policy Sections, each one identified by a Policy Section Identifier (i.e. PSI). It is up to PCF decision how to divide the UE access selection and PDU Session related policy information into Policy Sections.

NOTE 1: PSI list can be different per user. One PSI and its corresponding content can be the same for one or more users.

NOTE 2: 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 AMF forwards the UE access selection and PDU Session related policy information to the UE. The UE updates the stored UE access selection and PDU Session selection policies by the one provided by the PCF as follows:

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

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

- The UE may remove the stored Policy Section if the received information content is empty.

NOTE 3: The AMF does not need to understand the content of the UE policy, rather send them to the UE for storage.

At Initial Registration the UE provides the list of stored PSIs identifying the Policy Sections that are currently stored in the UE, if no policies are stored in the UE or the USIM is changed, the UE does not provide any PSI. The UE shall indicate that it does not support ANDSP to PCF if the UE does not support non-3GPP access. The PCF shall not send ANDSP to UE in this case. The AMF provides the UE access selection and PDU Session related policy information to PCF in the Npcf_AMPolicyControl_Create procedure.

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.

When the PCF receives Npcf_AMPolicyControl_Create including a list of PSIs then it retrieves the list of PSIs and its content stored in the UDR for this SUPI. The PCF compares the two lists of PSIs, in addition the PCF checks whether the list of PSIs and its content needs to be updated according to operator policies. If two list of PSIs provided by the UE and the list of PSIs stored in the UDR are different or an update is necessary, the PCF provide an updated list of PSIs and corresponding contents to the AMF in the Npcf_AMPolicyControl_Create Response. If the PCF decides to split the UE policies to be sent to the UE, the PCF uses Npcf_AMPolicyControl_UpdateNotify service and then AMF uses using 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.

The PCF maintains the latest list of PSIs delivered to each UE as part of the information related to the Policy Association until the Npcf_AMPolicyControl_Delete is received from the AMF. Then PCF stores the latest list of PSIs and its contents in the UDR using the Nudr_UDM_Update including DataSet "Policy Data" and Data Subset "Policy Set Entry".

PLMN ID is provided to UE and used to indicate which PLMN a PSI list belongs to.

NOTE 4: The UE doesn't provide to the PCF the list of pre-configured PSIs stored in the UE.

NOTE 5: 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.

6.1.2.3 Management of packet flow descriptions

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 or application 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. 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.

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

The ASP manages (provision, update, delete) the PFDs through the NEF. 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 (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. Upon reception of the request from the ASP, the NEF shall check if the ASP is authorized to provide/update/remove those PFD(s) and request the allowed delay. The NEF 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 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. In case 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 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 ID, the SMF shall provision the updated PFD set corresponding to the Application ID 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.

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 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.

6.1.2.3.2 Packet Flow Description

PFD (Packet Flow Description) is a set of information enabling the detection of application traffic.

Each PFD may be identified by a PFD id. A PFD id is unique in the scope of a particular application identifier. Conditions for when PFD ID is included in the PFD is described in TS 29.551 [17]. There may be different PFD types associated to an application identifier.

A PFD include the following information:

- PFD id; and
- one or more of the following:
  - a 3-tuple including protocol, server side IP address and port number;
  - the significant parts of the URL to be matched, e.g. host name;
  - a Domain name matching criteria and information about applicable protocol(s).

NOTE: Based on the agreement between AF and mobile operator, the PFD can be designed to convey proprietary extension for proprietary application traffic detection mechanisms.

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 and optionally, network area information (e.g. list of TAs/RAs).

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 transfer policies stored for any ASP from the UDR. Afterwards, the PCF shall determine, based on the information provided by the AF and other available information (e.g. network policy, congestion level (if available), load status estimation for the required time window, network area, and network slice existing transfer policies) one or more transfer policies. The PCF may recognize the network slice to which the ASP belongs from the ASP identifier.

A transfer 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 transfer policies to the AF together with a reference ID. If the AF received more than one transfer policy, the AF shall select one of them and inform the PCF about the selected transfer policy.

NOTE 3: The maximum aggregated bitrate (optionally provided in a transfer 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 transfer policy is finally stored by the PCF in the UDR together with the reference ID and the network area information. The same or a different PCF can retrieve this transfer policy and the corresponding network area

information from the UDR and take them into account for future decisions about transfer policies for background data related to the same or other ASPs.

At the time the background data transfer is about to start, the AF provides for each UE the reference ID together with the AF session information to the PCF (via the N5 interface). The PCF retrieves the corresponding transfer policy from the UDR and derives the PCC rules for the background data transfer according to this transfer policy.

NOTE 5: The AF will typically contact the PCF for the individual UEs to request sponsored connectivity for the background data transfer.

NOTE 6: 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.

6.1.2.5 Policy Control Request Triggers relevant for AMF

The Policy Control Request Triggers relevant for AMF and 3GPP access type are listed in table 6.1.2.5-2 and define the conditions when the AMF shall interact again with PCF after the Policy Association Establishment.

The PCF provides Policy Control Request Triggers to the AMF in the Policy Association establishment and modification procedures defined in the TS 23.502 [3].

Table 6.1.2.5-2: Policy Control Request Triggers relevant for AMF and 3GPP access type

Policy Control Request Trigger	Description	Condition for reporting
Location change (tracking area)	The tracking area of the UE has changed.	PCF
Change of UE presence in Presence Reporting Area	The UE is entering/leaving a Presence Reporting Area	PCF
Service Area restriction change	The subscribed service area restriction information has changed.	PCF
RFSP index change	The subscribed RFSP index has changed	PCF

NOTE: In the following description of the Policy Control Request Triggers relevant for AMF and 3GPP access type, the term trigger is used instead of Policy Control Request Trigger where appropriate.

If the Location change trigger and/or Change of UE presence in Presence Reporting Area trigger are armed, the AMF shall activate the relevant procedure which reports any changes in location to the level indicated by the trigger.

If the Change of UE presence in Presence Reporting Area trigger is armed, the AMF shall activate the relevant procedure of Change of UE presence in Area of Interest reporting as explained in TS 23.501 [2], clause 5.3.4.4.

The Service Area restriction change trigger and the RFSP index change trigger shall trigger the AMF to interact with the PCF for all changes in the Service Area restriction or RFSP index data received in AMF from UDM.

6.1.3 Session management related policy control

6.1.3.1 General

The session management relate policy control functionality of the Policy and Charging control framework for the 5G system provides the functions for policy and charging control as well as event reporting for service data flows.

The PCF evaluates operator policies that are triggered by events received from the Application Function, from the Session Management Function, from the Access and Mobility Management Function from the Online Charging System as well as changes in User subscription Profile or changes in global policy related instructions received from AF (as described in TS 23.501 [2] clause 5.6.7).

NOTE 1: Credit management and reporting are defined in SA WG5 specification.

NOTE 2: In single PCF deployment, the PCF will provide all mobility, access and 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.

NOTE 3: Policy control in multiple administrative areas is not defined in this release.

The following clauses describe the most relevant session management related functionality in detail or provide a reference to a clause in TS 23.203 [4] where this functionality is described.

6.1.3.2 Binding mechanism

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.

6.1.3.2.2 Session binding

Session binding is the association of the AF session information to one and only one PDU Session. The PCF shall perform the session binding, which may take the following PDU Session parameters into account:

a) For an IP type PDU Session, the UE IPv4 address and/or IPv6 network prefix;

   For an Ethernet type PDU Session, the UE MAC address(es);

b) The UE identity (e.g. SUPI), if present;

c) The information about the Data Network (DN) the user is accessing, i.e. DNN, if present.

Once it has determined the impacted PDU Session, the PCF shall identify the PCC rules affected by the AF session information, including new PCC rules to be installed and existing PCC rules to be modified or removed.

Session Binding applies for PDU Sessions of IP type. It may also apply to Ethernet PDU Session type but only when especially allowed by PCC related Policy Control Request triggers. In the case of Ethernet PDU Session type, session binding does not apply to AF requests sent over Rx.

6.1.3.2.3 PCC rule authorization

PCC Rule authorization is the selection of the 5G QoS parameters, described in TS 23.501 [2] clause 5.7.2, for the PCC rules.

The PCF shall perform the PCC rule authorization for dynamic PCC rules belonging to AF sessions that have been selected in step 1, as described in clause 6.1.3.2.2, as well as for PCC rules without corresponding AF sessions.

For the authorization of a PCC rule the PCF shall consider any 5GC specific restrictions, subscription information and other information available to the PCF. Each PCC rule receives a set of QoS parameters that are supported by the specific Access Network. The authorization of a PCC rule associated with an emergency service shall be supported without subscription information. The PCF shall apply local policies configured for the emergency service.

6.1.3.2.4 QoS Flow binding

QoS Flow binding is the association of a PCC rule to a QoS Flow within a PDU Session. The binding is performed using the following binding parameters:

- 5QI;
- ARP;
- QNC (if available in the PCC rule);
- Priority Level (if available in the PCC rule);
- Averaging Window (if available in the PCC rule);
- Maximum Data Burst Volume (if available in the PCC rule).

When the PCF provisions a PCC Rule, the SMF shall evaluate whether a QoS Flow with QoS parameters identical to the binding parameters exists unless the PCF requests to bind the PCC rule to the QoS Flow associated with the default QoS rule. If no such QoS Flow exists, the SMF derives the QoS parameters, using the parameters in the PCC Rule, for a new QoS Flow, binds the PCC Rule to the QoS Flow and then proceeds as described TS 23.501 [2] sub-clause 5.7. If a QoS Flow with QoS parameters identical to the binding parameters exists, the SMF updates the QoS Flow, so that the new PCC Rule is bound to this QoS Flow.

NOTE 1: For PCC rules containing a delay critical GBR 5QI value, the SMF can bind PCC Rules with the same binding parameters to different QoS Flows to ensure that the GFBR of the QoS Flow can be achieved with the Maximum Data Burst Volume of the QoS Flow.

When the PCF request that a PCC rule is bound to the QoS Flow associated with the default QoS rule by including the Bind to QoS Flow associated with the default QoS rule Indication in a dynamic PCC rule, the SMF shall bind the dynamic PCC rule to the QoS Flow associated with the default QoS rule and keep the binding as long as this indication remains set. When the PCF removes the association of a PCC rule to the QoS Flow associated with the default QoS rule, a new binding may need to be created between this PCC rule and the QoS Flow as described above.

The binding is created between a PCC Rule and a QoS Flow. The association shall cause the downlink part of the service data flow to be directed to the QoS Flow in the association. In the UE, the QoS rule associated with the QoS Flow instructs the UE to direct the uplink part of the service data flow to the QoS Flow in the association.

Whenever the authorized QoS of a PCC rule changes, the existing bindings shall be re-evaluated. The re-evaluation may, for a service data flow, require a new binding with another QoS Flow.

NOTE 2: A QoS change of the default 5QI/ARP values doesn't cause the QoS Flow rebinding for PCC rules previously bound to the QoS Flow associated with the default QoS rule set, with the Bind to QoS Flow associated with the default QoS rule Indication set.

When the PCF removes a PCC Rule, the SMF shall remove the association of the PCC Rule to the QoS Flow.

The SMF shall report to the PCF that the PCC Rules bound to a QoS Flow are removed when the corresponding QoS Flow is removed.

6.1.3.3 Reporting

The reporting functionality is the same as specified in clause 6.1.2 of TS 23.203 [4] with the following differences:

- The reporting is per PDU Session
- The measurement occurs in the UPF (CTF/AMC)
- The SMF represents the network (CTF/ADF)
- When QoS information is to be reported, the QoS parameters defined in TS 23.501 [2] apply

6.1.3.4 Credit management

The credit management functionality is the same as specified in clause 6.1.3 of TS 23.203 [4] with the following differences:

- The measurement occurs in the UPF (CTF/AMC)

NOTE: Credit management and reporting are defined in SA WG5 specification and further differences can exist.

6.1.3.5 Policy Control Request Triggers relevant for SMF

The Policy Control Request Triggers relevant for SMF define the conditions when the SMF shall interact again with PCF after a PDU Session establishment as defined in the Session Management Policy Establishment and Session Management Policy Modification procedure as defined in TS 23.502 [3].

The access independent Policy Control Request Triggers relevant for SMF are listed in table 6.1.3.5-1.

Table 6.1.3.5-1: Access independent Policy Control Request Triggers relevant for SMF

Policy Control Request Trigger	Description	Difference compared with table 6.2 and table A.4.3-2 in TS 23.203 [4]	Conditions for reporting	Motivation
PLMN change	The UE has moved to another operators' domain.	None	PCF	
QoS change	The QoS parameters of the QoS Flow has changed	Removed		Only applicable when binding of bearers was done in PCRF.
QoS change exceeding authorization	The QoS parameters of the QoS Flow has changed and exceeds the authorized QoS	Removed		Only applicable when binding of bearers was done in PCRF.
Traffic mapping information change	The traffic mapping information of the QoS profile has changed	Removed		Only applicable when binding of bearers was done in PCRF.
Resource modification request	A request for resource modification has been received by the SMF.	None	SMF always reports to PCF	
Routing information change	The IP flow mobility routing information has changed (when IP flow mobility as specified in TS 23.261 [11] applies) or the PCEF has received Routing Rules from the UE (when NBIFOM as specified in TS 23.161 [10] applies)	Removed		Not in 5GS yet.
Change in Access Type	The Access Type and, if applicable, the RAT Type of the PDU Session has changed.	None	PCF	
Loss/recovery of transmission resources	The Access type transmission resources are no longer usable/again usable.	Removed		Not in 5GS yet.
Location change (serving cell)	The serving cell of the UE has changed.	Removed		Not in 5GS yet.
Location change (serving area)	The serving area of the UE has changed.	None	PCF	
Location change (serving CN node)	The serving core network node of the UE has changed.	None	PCF	
Change of UE presence in Presence Reporting Area (see NOTE 1)	The UE is entering/leaving a Presence Reporting Area	None	PCF	Only applicable to PCF
Out of credit	Credit is no longer available.	None	PCF	May need validation with SA5.
Enforced PCC rule request	SMF is performing a PCC rules request as instructed by the PCF.	None	PCF	
Enforced ADC rule request	TDF is performing an ADC rules request as instructed by the PCRF.	Removed		ADC Rules are not applicable.
UE IP address change	A UE IP address has been allocated/released	None	SMF always reports allocated or released UE IP addresses	
UE MAC address change	A new UE MAC address is detected or a used UE MAC address is inactive for a specific period	New	PCF	
Access Network	Access Network Charging	None	PCF	

Charging Correlation Information	Correlation Information has been assigned.			
Usage report	The PDU Session or the Monitoring key specific resources consumed by a UE either reached the threshold or needs to be reported for other reasons.	None	PCF	
Start of application traffic detection and Stop of application traffic detection	The start or the stop of application traffic has been detected.	None	PCF	
SRVCC CS to PS handover	A CS to PS handover has been detected	Removed		No support in 5GS yet
Access Network Information report	Access information as specified in the Access Network Information Reporting part of a PCC rule.	None	PCF	
Credit management session failure	Transient/Permanent failure as specified by the OCS	None	PCF	
Addition / removal of an access to an IP-CAN session	The PCEF reports when an access is added or removed	Removed		No support in 5GS yet
Change of usability of an access	The PCEF reports that an access becomes unusable or usable again	Removed		No support in 5GS yet
3GPP PS Data Off status change	The SMF reports when the 3GPP PS Data Off status changes	None	SMF always reports to PCF	
Session AMBR change	The subscribed Session AMBR has changed	Added	SMF always reports to PCF	
Default QoS change	The subscribed QoS has changed	Added	SMF always reports to PCF	
Removal of PCC rule	The SMF reports when the PCC rule is removed	Added	SMF always reports to PCF	
QoS targets of the QoS Flow cannot be fulfilled or can be fulfilled again	The SMF notify the PCF when receiving notification from RAN that QoS targets of the QoS Flow cannot be fulfilled or can be fulfilled again	Added		
NOTE 1: The maximum number of PRA(s) per UE per PDU Session is configured in the PCF. The PCF may have independent configuration of the maximum number for Core Network pre-configured PRAs and UE-dedicated PRAs. The exact number(s) should be determined by operator in deployment.				

NOTE 1: In the following description of the access independent Policy Control Request Triggers relevant for SMF, the term trigger is used instead of Policy Control Request Trigger where appropriate.

The Resource modification request trigger shall trigger the PCF interaction for all resource modification requests not tied to a specific QoS Flow received by SMF. The resource modification request received by SMF may include request for guaranteed bit rate changes for a traffic aggregate and/or the association/disassociation of the traffic aggregate with a 5QI and/or a modification of the traffic aggregate.

If the Location change trigger is armed, the SMF shall activate the relevant access specific procedure which reports any changes in location to the level indicated by the trigger. If credit-authorization triggers (specified in clause 6.1.3 of TS 23.203 [4]) and Policy Control Request Triggers require different levels of reporting of location change for a single UE, the location to be reported should be changed to the highest level of detail required. However, there should be no report to PCF being triggered if the report received is more detailed than requested by the PCF.

The enforced PCC rule request trigger shall trigger a SMF interaction to request PCC rules from the PCF for an established PDU Session. This SMF interaction shall take place within the Revalidation time limit set by the PCF in the PDU Session related policy information.

The UE IP address change trigger shall trigger a SMF interaction with the PCF in case a UE IP address is allocated or released during the lifetime of the PDU session.

The UE MAC address change trigger shall trigger a SMF interaction with the PCF in case a new UE MAC address is detected or a used UE MAC address is inactive for a specific period during the lifetime of the Ethernet type PDU session.

NOTE 2: The SMF instructs the UPF to detect new UE MAC addresses or used UE MAC address is inactive for a specific period as described in TS 23.501 [2].

The Access Network Charging Correlation Information trigger shall trigger the SMF to report the assigned access network charging identifier for the PCC rules that are accompanied with a request for this trigger at activation.

If the Usage report trigger is set and the volume or the time thresholds, earlier provided by the PCF, are reached, the SMF shall report this situation to the PCF. If both volume and time thresholds were provided and the thresholds, for one of the measurements, are reached, the SMF shall report this situation to the PCF and the accumulated usage since last report shall be reported for both measurements.

The management of the Presence Reporting Area (PRA) functionality enables the PCF to subscribe to reporting change of UE presence in a particular Presence Reporting Area.

NOTE 3: PCF decides whether to subscribe to AMF or to SMF for those triggers that are present in both tables 6.1.2.5-2 and 6.1.3.5-1. If the Change of UE presence in Presence Reporting Area trigger is available on both AMF and SMF, PCF should not subscribe to both AMF and SMF simultaneously.

Upon every interaction with the SMF, the PCF may activate / deactivate reporting changes of UE presence in Presence Reporting Area by setting / unsetting the corresponding trigger by providing the PRA Identifier(s) and additionally the list(s) of elements comprising the Presence Reporting Area for UE-dedicated Presence Reporting Area(s).

The SMF shall subscribe to the UE Location Change notification from the AMF by providing an area of interest containing the PRA Identifier(s) and additionally the list(s) of elements provided by the PCF as specified in TS 23.501 [2], clause 5.6.11 and TS 23.502 [3], clause 5.2.2.3.1.

When the Change of UE presence in Presence Reporting Area trigger is armed, i.e. when the PCF subscribes to reporting change of UE presence in a particular Presence Reporting Area and the reporting change of UE presence in this Presence Reporting Area was not activated before, the SMF shall activate the relevant PDU Session specific procedure which reports when the UE enters or leaves a Presence Reporting Area (an initial report is received when the PDU Session specific procedure is activated). The SMF reports the PRA Identifier(s) and indication(s) whether the UE is inside or outside the Presence Reporting Area(s), and indication(s) if the corresponding Presence Reporting Area(s) is set to inactive by the AMF to the PCF.

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

When PCF is not subscribed to change of UE presence in Presence Reporting Area for a particular Presence Reporting Area, the SMF shall deactivate the relevant PDU Session specific procedure which reports when the UE enters or leaves a Presence Reporting Area.

The SMF stores PCF subscription to reporting for changes of UE presence in Presence Reporting Area and notifies the PCF with the PRA Identifier(s) and indication(s) whether the UE is inside or outside the Presence Reporting Area(s) based on UE location change notification in area of interest received from the serving node according to the corresponding subscription.

When a PRA set identified by a PRA Identifier was subscribed to report changes of UE presence in Presence Reporting Area by the PCF, the SMF additionally receives the PRA Identifier of the PRA set from the AMF, along with the individual PRA Identifier(s) belonging to the PRA set and indication(s) of whether the UE is inside or outside the individual Presence Reporting Area(s), as described in TS 23.501 [2].

The Start of application traffic detection and Stop of application traffic detection triggers shall trigger an interaction with PCF once the requested application traffic is detected (i.e. Start of application traffic detection) or the end of the requested application traffic is detected (i.e. Stop of application traffic detection) unless it is requested within a specific PCC Rule to mute such interaction for solicited application reporting or unconditionally in case of unsolicited application reporting. The application identifier and service data flow descriptions, if deducible, shall also be included in the report. An application instance identifier shall be included in the report both for Start and for Stop of application

traffic detection when service data flow descriptions are deducible. This is done to unambiguously match the Start and the Stop events.

At PCC rule activation, modification and deactivation the SMF shall send, as specified in the PCC rule, the User Location Report and/or UE Timezone Report to the PCF.

NOTE 5: At PCC rule deactivation the User Location Report includes information on when the UE was last known to be in that location.

The PCF shall send the User Location Report and/or UE Timezone Report to the AF upon receiving an Access Network Information report corresponding to the AF session from the SMF.

If the trigger for Access Network Information reporting is set, the SMF shall check the need for access network information reporting after successful installation/modification or removal of a PCC rule or upon termination of the PDU Session. The SMF shall check the Access Network Information report parameters (User Location Report, UE Timezone Report) of the PCC rules and report the access network information to the PCF. The SMF shall not report any subsequent access network information updates received from the PDU Session without any previous updates of related PCC rule unless the associated QoS Flow or PDU Session has been released.

If the SMF receives a request to install/modify or remove a PCC rule with Access Network Information report parameters (User Location Report, UE Timezone Report) set the SMF shall initiate a PDU Session modification to retrieve the current access network information of the UE and forward it to the PCF afterwards.

If the Access Network Information report parameter for the User Location Report is set and the user location (e.g. cell) is not available to the SMF, the SMF shall provide the serving PLMN identifier to the PCF which shall forward it to the AF.

The Credit management session failure trigger shall trigger a SMF interaction with the PCF to inform about a credit management session failure and to indicate the failure reason, and the affected PCC rules.

NOTE 6: As a result, the PCF may decide about e.g. PDU Session termination, perform gating of services, switch to offline charging, change rating group, etc.

NOTE 7: The Credit management session failure trigger applies to situations wherein the PDU Session is not terminated by the SMF due to the credit management session failure.

The Session AMBR change and the default QoS change triggers shall trigger the PCF interaction for all changes in the Session AMBR or default QoS data received in SMF from the UDM.

The default QoS change trigger reports a change in the default 5QI/ARP retrieved by SMF from UDM, as explained in clause 5.7.2.7 of TS 23.501 [2].

If the PCC Rules bound to a QoS Flow are removed when the corresponding QoS Flow is removed or the PCC rules are failed to be enforced, the SMF shall report this situation to the PCF and the PCF may update the PCC rules for an established PDU Session.

If the QoS targets of the QoS Flow cannot be fulfilled or can be fulfilled again trigger is armed and the SMF receives notification from (R)AN indicating that QoS targets of the QoS Flow cannot be fulfilled or can be fulfilled again, the SMF shall report this situation to the PCF for those PCC rules which are bound to this QoS Flow and have the QoS Notification Control (QNC) parameter set. The PCF may update the PCC rules for an established PDU Session.

In an interworking scenario between 5GS and EPC/E-UTRAN, as explained in the TS 23.501 [2], clause 4.3, the PCF may subscribe via the SMF also to the Policy Control Request Triggers described in clause 6.1.2.5 when the UE is served by the EPC/E-UTRAN.

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. For 5QI of GBR type, the authorized QoS includes the ARP, MBR, GBR and may include a request for notification when authorized GBR cannot be fulfilled or can be fulfilled again. For 5QI of non-GBR type, the authorized QoS may include the ARP and the Reflective QoS indication; if no ARP is included a default ARP applies for the service data flow template. The authorized QoS for a service data flow template may also refer to QoS characteristics as defined in TS 23.501 [2] clause 5.7.3.

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 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 as described in clause 6.1.5 of TS 23.203 [4] with clarifications that no IP-CAN bearer level information is sent by PCF to AF but PDU Session information is sent by PCF to AF instead.

6.1.3.7 Service (data flow) prioritization and conflict handling

The functional description for SDF prioritization and conflict handling in clause 6.1.6 of TS 23.203 [4] applies.

6.1.3.8 Termination action

The functional description for termination actions in clause 6.1.8 of TS 23.203 [4] applies.

6.1.3.9 Handling of packet filters provided to the UE by SMF

The functional description for the handling of packet filters provided to the UE by SMF in clause 6.1.9 of TS 23.203 [4] applies with the difference that traffic mapping information that effectively disallows any useful packet flows in uplink direction does not need to be provided for a QoS Flow. In case of interworking with E-UTRAN connected to EPC, the specific aspects of the handling of packet filters at the SMF are described in clause 4.11.1 of TS 23.502 [3].

6.1.3.10 IMS emergency session support

PDU Sessions for IMS Emergency services are provided by the serving network to support IMS emergency when the network is configured to support emergency services. Emergency services are network services provided through an Emergency DNN and may not require a subscription depending on operator policies and local regulatory requirements. For emergency services, the architecture for the non-roaming case is the only applicable architecture model.

For emergency services, the N25 reference point does not apply. Emergency services are handled locally in the serving network.

For a PDU Session serving an IMS emergency session, the PCF makes authorization and policy decisions that restrict the traffic to emergency destinations, IMS signalling and the traffic to retrieve user location information (in the user plane) for emergency services. A PDU Session serving an IMS emergency session shall not serve any other service and shall not be converted to/from any PDU Session serving other services. The PCF shall determine based on the DNN if a PDU Session concerns an IMS emergency session.

The PCC Rule Authorization function selects QoS parameters that allow prioritization of IMS Emergency sessions. If an IMS Emergency session is prioritized the QoS parameters in the PCC Rule shall contain an ARP value that is reserved for intra-operator use of IMS Emergency services. The PCF does not perform subscription check; instead it utilizes the locally configured operator policies to make authorization and policy decisions.

NOTE 1: Reserved value range for intra-operator use is defined in TS 23.501 [2].

For an emergency DNN, the PCF does not perform subscription check; instead it utilizes the locally configured operator policies to make authorization and policy decisions.

It shall be possible for the PCF to verify that the IMS service information is associated with a UE IP address belonging to an emergency DNN. If the IMS service information does not contain an emergency related indication and the UE IP address is associated with an emergency DNN, the PCF shall reject the IMS service information provided by the P-CSCF (and thus to trigger the release of the associated IMS session), see TS 23.167 [12].

In addition, upon Rx session establishment 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 2: 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.

If the PCF removes all PCC Rules with a 5QI other than the default 5QI and the 5QI used for IMS signalling, the SMF shall start a configurable inactivity timer (e.g., to enable PSAP Callback session). When the configured period of time expires the SMF shall terminate the PDU Session serving the IMS Emergency session as defined in TS 23.502 [3]. If the SMF receives new PCC rule(s) with a 5QI other than the default 5QI and the 5QI used for IMS signalling for the PDU Session serving the IMS Emergency session, the SMF shall cancel the inactivity timer.

6.1.3.11 Multimedia Priority Service support

Multimedia Priority Services (MPS) is defined in TS 23.501 [2], TS 23.502 [3] and in TS 23.228 [5], utilising the architecture defined for 5GS.

Subscription data for MPS is provided to PCF through the N25/Nudr. To support MPS service, the PCF shall subscribe to changes in the MPS subscription data for Priority PDU connectivity service. Dynamic invocation for MPS provided from an AF using the Priority indicator over Rx or over N5/Npcf takes precedence over MPS subscription.

For dynamic invocation of MPS service, the PCF shall generate the corresponding PCC rule(s) with the ARP and 5QI parameters as appropriate for the prioritized service, as defined in TS 23.501 [2].

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

In the case of IMS MPS, in addition to the above, the following QoS Flow handling applies:

- At reception of the indication from subscription information that the IMS Signalling Priority is set for the PDU Session or at reception of service authorization from the P-CSCF (AF) including an MPS session indication and the service priority level as defined in TS 23.228 [5], the PCF shall (under consideration of the requirement described in clauses 5.16.5 and 5.22.3 in TS 23.501 [2]) modify the ARP in all the PCC rules that describe the IMS signalling traffic to the value appropriate for IMS Multimedia Priority Services, if upgrade of the QoS Flow carrying IMS Signalling is required. To modify the ARP of the QoS Flow associated with the default QoS rule the PCF shall modify the Authorized default 5QI/ARP.

- When the PCF detects that the P-CSCF (AF) released all the MPS session and the IMS Signalling Priority is not set for the PDU Session the PCF shall consider changes of the requirement described in clauses 5.16.5 and 5.22.3 in TS 23.501 [2] and modify the ARP in all PCC rules that describe the IMS signalling traffic to an appropriate value according to PCF decision. The PCC rules bound to the QoS Flow associated with the default QoS rule have to be changed accordingly.

NOTE: To keep the PCC rules bound to this QoS Flow, the PCF can either modify the ARP of these PCC rules accordingly or set the Bind to QoS Flow associated with the default QoS rule.

The Priority PDU connectivity service targets the ARP and/or 5QI of the QoS Flows, enabling the prioritization of all traffic on the same QoS Flow.

For non-MPS service, the PCF shall generate the corresponding PCC rule(s) as per normal procedures (i.e. without consideration whether the MPS Priority PDU connectivity service is active or not), and shall upgrade the ARP/5QI values suitable for MPS when the Priority PDU connectivity service is invoked. When the Priority PDU connectivity service is revoked, the PCF shall change the ARP/5QI values modified for the Priority PDU connectivity service to an appropriate value according to PCF decision.

The PCF shall, at the activation of the Priority PDU connectivity service:

- modify the ARP of PCC rules installed before the activation of the Priority PDU connectivity service to the ARP as appropriate for the Priority PDU connectivity service under consideration of the requirement described in clause 5.16.5 of TS 23.501 [2]; and

- if modification of the 5QI of the PCC rule(s) is required, modify the 5QI of the PCC rules installed before the activation of the Priority PDU connectivity service to the 5QI as appropriate for this service.

The PCF shall, at the deactivation of the Priority PDU connectivity service modify any 5QI and ARP value to the value according to the PCF policy decision.

For PCC rules modified due to the activation of Priority PDU connectivity service:

- modify the ARP to an appropriate value according to PCF decision under consideration of the requirement described in clauses 5.16.5 and 5.22.3 in TS 23.501 [2]; and

- if modification of the 5QI of PCC rule(s) is required, modify the 5QI to an appropriate value according to PCF decision.

6.1.3.12 Redirection

The functional description of the redirection in clause 6.1.13 of TS 23.203 [4] applies with the difference that the redirection is enforced in the UPF.

6.1.3.13 Resource sharing for different AF sessions

The functional description for resource sharing for different AF sessions in clause 6.1.14 of TS 23.203 [4] applies.

6.1.3.14 Traffic steering control

Traffic steering control is triggered by the PCF initiated request and consists of steering the detected service data flows matching application detection filters or service data flow filter(s) in PCC Rules. The traffic steering control consists in:

- applying a specific N6 traffic steering policy for the purpose of steering the subscriber's traffic to appropriated N6 service functions deployed by the operator or a 3rd party service provider as described for service functions deployed at (S)Gi in clause 6.1.17 of TS 23.203 [4] with the clarification that the description of the PCRF and PCEF applies to the PCF and SMF respectively.

- diverting (at DNAI(s) provided in PCC rules) traffic matching traffic filters provided by the PCF, as described in TS 23.501 [2] clause 5.6.7.

The actual traffic steering applies at the UPF.

6.1.3.15 Resource reservation for services sharing priority

An AF may indicate to the PCF that a media flow of an AF session is allowed to use the same priority as media flows belonging to other AF sessions (instead of the service priority provided for this media flow). In this case, the AF will provide a priority sharing indicator in addition to the application identifier and the service priority. For MCPTT, the service priority and the priority sharing indicator are defined in TS 23.179 [6]. The priority sharing indicator is used to indicate what media flows are allowed to share priority.

The PCF makes authorization and policy decisions for the affected AF sessions individually and generates a PCC rule for every media flow as specified in clause 6.1.1.3. The application identifier and the service priority are used to calculate the ARP priority. The AF may also provide suggested pre-emption capability and vulnerability values per media flow to the PCF. The ARP pre-emption capability and the ARP pre-emption vulnerability are set according to operator policies and regulatory requirements, also taking into consideration the application identifier and suggested values, when provided by the AF. The priority sharing indicator is stored for later use.

For PCC rules with the same 5QI assigned and having an associated priority sharing indicator, the PCF shall try to make authorization and policy decisions taking the priority sharing indicator into account and modify the ARP of these PCC rules as follows, (the original ARP values are stored for later use):

- The modified ARP priority is set to the highest of the original priority among all the PCC rules that include the priority sharing indicator;

- The modified ARP pre-emption capability is set if any of the original PCC rules have the ARP pre-emption capability set;

- The modified ARP pre-emption vulnerability is set if all the original PCC rules have the ARP pre-emption vulnerability set.

If the PCF receives an indication that a PCC rule provisioning or modification failed (due to resource reservation failure) then, the PCF may apply pre-emption and remove active PCC rules from the SMF and then retry the PCC rule provisioning or modification. If the PCF does not apply pre-emption, the AF is notified using existing procedures that the resource reservation for the new media flow failed.

The AF may optionally provide pre-emption control information, including pre-emption capability and vulnerability values, in addition to the priority sharing indicator to the PCF. If so, the PCF shall apply pre-emption and remove active PCC rules according to this information when receiving an indication that a PCC rule provisioning or modification failed. The pre-emption control information indicates:

- whether media flows sharing priority are candidates to being pre-empted taking into account pre-emption capability and vulnerability values;

- how to perform pre-emption among multiple potential media flow candidates of same priority: most recently added media flow, least recently added media flow, media flow with highest requested bandwidth in the AF request.

6.1.3.16 3GPP PS Data Off

This feature, when activated by the user, prevents traffics via 3GPP access except for 3GPP PS Data Off Exempt Services. The 3GPP PS Data Off Exempt Services are a set of operator services, defined in TS 22.011 [15] and TS 23.221 [16], that are the only allowed services in both downlink and uplink direction when the 3GPP PS Data Off feature has been activated by the user.

When PCF is deployed, it shall be able to configure the list(s) of 3GPP PS Data Off Exempt Services, and the event trigger of 3GPP PS Data Off status change used to inform the PCF from SMF about every change of the 3GPP PS Data Off status.

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

NOTE 2: For the PDU Session used for IMS services, the 3GPP Data Off Exempt Services are enforced in the IMS domain as specified TS 23.228 [5]. Policies configured in the PCF need to ensure that IMS services are allowed when the 3GPP Data Off status of the UE is set to "activated", e.g. by treating any service within a well-known IMS DNN as 3GPP PS Data Off Exempt Services.

When the PCF is informed about the activation of 3GPP PS Data Off, it shall update the PCC rules in such a way that only packets for services belonging to the list(s) of 3GPP PS Data Off Exempt Services are forwarded while all other packets are discarded.

NOTE 3: In order for the SMF/UPF to prevent the services that do not belong to the list(s) of 3GPP PS Data Off Exempted Services, if the services are controlled by dynamic PCC rules, the PCF could modify the PCC rules by setting the gate status to "closed" for downlink and optionally uplink direction in all active dynamic PCC rules or remove those dynamic PCC rules. If the services are controlled by predefined PCC rules, the PCF can deactivate those predefined PCC rules. PCC rule with wild-carded service data flow filters can be among the PCC rules that are modified, removed or deactivated in that manner. In this case, it can be necessary that the PCF at the same time installs or activates PCC rules for data-off exempt services.

NOTE 4: For example, four PCC rules (A, B, C, D) are active for a PDU Session with PCC rule A representing a 3GPP PS Data Off Exempt Service. When 3GPP PS Data Off is activated, the PCF could either modify PCC rules B, C and D if they are dynamic PCC rules by closing the gate in downlink and optionally uplink direction or remove/deactivate PCC rules B, C and D if they are predefined PCC rules. PCC rule A does not need to be changed as it represents 3GPP PS Data Off Exempt Service. Assuming that PCC rule B contained wild-carded service data flow filters which has enabled some 3GPP PS Data Off Exempt Service is removed or deactivated, an additional PCC rule E can be installed or activated as well to enable downlink and optionally uplink traffic for that 3GPP PS Data Off Exempt Service.

NOTE 5: The network configuration can ensure that at least one PCC Rule is activated for the PDU Session when Data Off is activated in order to avoid deletion of an existing PDU Session or in order not to fail a PDU Session establishment.

When the PCF receives service information from the AF, in addition to what is specified in clause 6.2.1, PCF shall check if the requested service information belongs to the 3GPP PS Data Off Exempt Services. If the requested service belongs to 3GPP PS Data Off Exempt Services, PCF shall continue as specified in clause 6.2.1. If the requested service doesn't belong to the 3GPP PS Data Off Exempt Services, PCF shall reject the service request.

When the PCF is informed about the deactivation of 3GPP PS Data Off, it shall perform policy control decision as specified in clause 6.2.1 and perform PCC rule operations as specified in clause 6.3.2 to make sure that the services are allowed according to user's subscription and operator policy (irrespective of whether they belong to the list(s) of 3GPP PS Data Off Exempt Services).

When PCF is not deployed, predefined PCC rules, as example, can be configured in the SMF to ensure the following:

- when the SMF is informed about activation of 3GPP PS Data Off, the SMF ensures in UPF only downlink and optionally uplink packets for services belonging to the list(s) of 3GPP PS Data Off Exempt Services are forwarded while all other downlink and uplink packets are discarded, and

- When SMF is informed about deactivation of 3GPP PS Data Off, the SMF ensures in UPF downlink and uplink packets are forwarded according to the operator policy for the subscriber.

NOTE 6: For example, the SMF can be configured with two sets of predefined PCC rules: one set for UE 3GPP PS Data Off status "inactive" and another set for UE 3GPP PS Data Off status "active". The set of predefined PCC rules for UE 3GPP PS Data Off status "active" can be equivalent to the set of predefined PCC rules for UE with 3GPP PS Data Off status "inactive" with the following two differences: All services belonging to the list(s) of 3GPP PS Data Off Exempt Services can be represented by PCC rule(s) which allows the traffic to pass while in all other PCC rules (not belonging to the list(s) of 3GPP PS Data Off Exempt Services) the gate status can be "closed" for downlink and optionally uplink direction. When the SMF is informed about the change of UE 3GPP PS Data Off status, it can replace the currently active set of predefined PCC rules with the other set of predefined PCC rules.

When the UE 3GPP PS Data Off status is "active" and a handover from one access-system to another occurs, the PCF performs the above operations so that the downlink and optionally uplink traffic for services not belonging to the list(s) of 3GPP PS Data Off Exempt Services is only prevented via the 3GPP access.

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 as defined in clause 6.9 of TS 23.203 [4] apply.

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.

6.2 Network functions and entities

6.2.1 Policy Control Function (PCF)

6.2.1.1 General

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. The authorization of QoS resources based on AF information described in clause 6.2.1.0 of TS 23.203 [4] applies with the clarification that the subscription information is retrieved as defined in TS 23.501 [2].

At reception of the service information from the AF, if configured through policy, the PCF determines the Maximum Packet Loss Rate for UL and DL based on the service information e.g. codec and sends it to SMF along with the PCC rule.

NOTE 1: Based on local configuration, the PCF sets the Maximum Packet Loss Rate (UL, DL) corresponding to either the most robust codec mode or the least robust codec mode of the negotiated set in each direction.

NOTE 2: Details for setting the Maximum Packet Loss Rate are specified by SA4.

The PCF supports usage monitoring control for a PDU Session or per Monitoring Key. The PCF support for usage monitoring control in clause 6.2.1.0 of TS 23.203 [4] applies.

The PCF may authorise an application service provider to request specific PCC decisions (e.g. authorisation to request sponsored IP flows, authorisation to request QoS resources) based on sponsored data connectivity profile from the UDR. For sponsored data connectivity, the PCF may receive a usage threshold from the AF. If the AF specifies a usage threshold, the PCF shall use the Sponsor Identity to construct a Monitoring key for monitoring the volume, time, or both volume and time of user plane traffic, and invoke usage monitoring on the SMF. The PCF shall notify the AF when the SMF reports that a usage threshold for the Monitoring key is reached provided that the AF requests to be notified for this event. If the usage threshold is reached, the AF may terminate the AF session or provide a new usage threshold to the PCF. Alternatively, the AF may allow the session to continue without specifying a usage threshold. If the AF decides to allow the session to continue without specifying a usage threshold, then monitoring in the SMF shall be discontinued for that monitoring key by the PCF, unless there are other reasons for continuing the monitoring.

If the H-PCF detects that the UE is accessing the sponsored data connectivity in the roaming scenario with home routed access, it may allow the sponsored data connectivity in the service authorization request, reject the service authorization request, or initiate the AF session termination based on home operator policy.

NOTE 3: Sponsored data connectivity is not supported in the roaming with visited access scenario in this Release.

If the AF revokes the service information and the AF has notified previously a usage threshold to the PCF, the PCF shall report the usage up to the time of the revocation of service authorization.

If the PDU session terminates and the AF has specified a usage threshold then the PCF shall notify the AF of the accumulated usage (i.e. either volume, or time, or both volume and time) of user plane traffic since the last usage report.

The PCF reports PDU Session events, e.g. Access Type, RAT Type (if applicable), Access Network Information, PLMN identifier where the UE is located. The reporting of events to the AF described in clause 6.2.1.0 of TS 23.203 [4] applies. The events that can be reported from the PCF to the AF are described in clause 5.2.5.3.5 of TS 23.502 [3].

If an AF requests the PCF to report on the event that QoS targets cannot be fulfilled, the PCF shall set the QNC indication in the corresponding PCC rule(s) that includes a GBR or delay critical GBR QCI value and provision them

together with the corresponding Policy Control Request Trigger to the SMF. At the time, the SMF notifies that QoS targets cannot be fulfilled for a PCC Rule(s) the PCF shall report to the AF, if subscribed to, The PCF may also apply local policy decisions if the AF subscription is not provided.

The PCF needs to report to the AF (e.g. P-CSCF) the Access Network Information. If an AF requests the PCF to report Access Network Information, the PCF shall set the Access Network Information report parameters in the corresponding PCC rule(s) and subscribe the corresponding Policy Control Request Triggers to the SMF. The PCF shall, upon receiving the subsequent Access Network Information report from the SMF corresponding to the AF session, notifies the Access Network Information to the AF. For those PCC rule(s) based on preliminary service information the PCF may assign the default 5QI and ARP to avoid signalling to the UE. In addition, the SDF filter(s) shall not be marked to be used for signalling to the UE in a QoS rule.

NOTE 4: AF subscribing from the PCF on the Access Network information is to enable Rx support by the PCF.

The PCF provides the following non-session management related functionality:

- Access and mobility related policy control (as described in clause 6.1.2.1);
- UE access selection and PDU Session selection related policy control (as described in clause 6.1.2.2);
- Negotiation for future background data transfer (as described in clause 6.1.2.4).

6.2.1.2 Input for PCC decisions

The PCF shall accept input for PCC decision-making from the SMF, the AMF, the OCS 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;
- The PEI of the UE;
- Location of the subscriber;
- Service Area Restrictions;
- RFSP Index;
- RAT Type;
- GPSI;
- Access Type;
- Serving PLMN identifier;

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

The SMF may provide the following information:

- SUPI;
- The 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;
- A DNN
- A PLMN identifier;
- 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]);
- 3GPP PS Data Off status.

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 reference ID, the volume of data to be transferred per UE, the expected amount of UEs and the network area information.

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 AF, if involved, may provide the following application session related information, 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;

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

- Policy counter status for each relevant policy counter.

The NWDAF, if involved, may provide the following slice specific network status analytic information:

- Identifier of network slice instance.
- Load level information of network slice instance.

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.

6.2.1.3 Policy control subscription information management

The PCF may request subscription information at PDU Session establishment and at UE Context Establishment.

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: 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 at UE context establishment using Nudr service for Data Set "Policy Data" and Data Subset "UE context policy control" 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

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" 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 in the DNN	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
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	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)
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 at UE context establishment 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

The subscriber data provided by the UDR using Nudr service for Data Set "Subscriber Data" and Data Subset "Access and Mobility Subscriber Data" is described in TS 23.502 [3], Table 5.2.3.3.1-1.

6.2.1.4 V-PCF

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

For SM-related policy control, the V-PCF only includes functionality for local breakout based on roaming agreement.

For UE policy control, V-PCF receives the UE policy from H-PCF and forwards it to the UE. V-PCF can send additional UE policy (i.e. ANDSP policies) to the UE. In that case, the UE policy from the V-PCF may be different from the one from H-PCF.

For Access and mobility related policy control, V-PCF generates RFSP Index and Service Area Restriction.

6.2.1.5 H-PCF

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

For SM-related policy control, the H-PCF only includes functionality for home routed and provide the same functionality as PCF in non-roaming case.

For UE policy control, H-PCF will generate its own UE policy based on subscription data and transfer the UE policy to V-PCF.

6.2.1.6 Application specific policy information management

The application specific information used for policy control includes:

- Negotiation of background data transfer information stored in the UDR as Data Set "Policy Data" and Data Subset "Background Data Transfer data": It contains an ASP identifier, A transfer policy together with a reference ID, the volume of data to be transferred per UE, the expected amount of UEs and the network area information;

- Sponsored data connectivity profile information stored in the UDR as Data Set "Policy Data" and Data Subset "Sponsored data connectivity profile data": It contains a list of ASP identifiers and their applications per sponsor identity;

- Application Function request information for multiple UEs (per group of UEs or all UEs) stored in the UDR as Data Set "Application Data" and Data Subset "AF request information for multiple UEs".

The application specific policy information may be requested/updated by the PCF per AF request.

The management of Application Function request information for multiple UEs is defined in clause 6.3.7.2 of TS 23.501 [2], the management of policies for the negotiation of background data transfer is defined in clause 6.1.2.4 of this specification and the provision and usage of sponsored data connectivity profile is defined in clause 6.2.1.1 of this specification.

6.2.2 Session Management Function (SMF)

6.2.2.1 General

The SMF is responsible for the enforcement of the policy decisions related to service data flow detection, authorized QoS, charging, gating, traffic usage reporting, packet routing and forwarding and traffic steering. The SMF controls the policy and charging enforcement which includes the binding of service data flows to QoS Flows (as described in clause 6.1.3.2.4) as well as the interaction with the CHF. The SMF interacts with the UPF(s), the RAN and the UE to achieve the appropriate treatment of the user plane traffic.

The SMF control of the UPF(s) is described in TS 23.501 [2] as well as the interaction principles between SMF and RAN and between SMF and UE. The procedures for the interaction between SMF and UPF, SMF and RAN as well as SMF and UE are described in TS 23.502 [3].

The SMF forwards the Maximum Packet Loss Rate for UL and DL, if received from PCF for the PCC rule. In the case multiple PCC Rules share one QoS Flow and the SMF received multiple Maximum Packet Loss Rates, the SMF chooses the lowest value per direction related to these PCC rules.

6.2.2.2 Service data flow detection

The Service Data Flow detection uses the service data flow template included in a PCC Rule provide by the PCF. The service data flow template defines the data for the service data flow detection as a set of service data flow filters or an application identifier referring to an application detection filter.

The application detection filters provided to the SMF may be extended with the PFDs provided by the UDR as described in 6.1.20 of TS 23.203 [4]. How the SMF uses the service data flow detection capabilities in the UPF is described in TS 23.501 [2] clause 5.8.2.

For IP PDU Session type and Ethernet PDU Session type, the service data flow filters that may apply for traffic on a PDU Session are defined in TS 23.501 [2] clause 5.7.6.

6.2.2.3 Measurement

For usage monitoring, the PCEF functional description in clause 6.2.2.3 of TS 23.203 [4] applies. The SMF instructs the UPF to provide usage reports to the SMF as described in TS 23.501, clause 5.8.2.6.

6.2.2.4 QoS control

The SMF receives the authorized QoS for a service data flow in the PCC rule. The SMF calculates the QoS parameters for a QoS Flow as described in TS 23.501 [2] clause 5.7.1. In addition, for GBR QoS Flows, the SMF should set the QoS Flow GBR to the sum of the GBRs of all PCC rules that are bound to that QoS Flow and the QoS Flow MBR to the sum of the MBRs of all PCC rules that are active and bound to that GBR QoS Flow.

The SMF receives the authorized Session AMBR and the default 5QI and default ARP in the PDU Session 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. For PDU Sessions of unstructured type the default 5QI and default ARP is the authorized QoS for all traffic in the PDU Session as described in TS 23.501 [2] clause 5.7.1.

The SMF generates QoS rule(s) as described in TS 23.501 [2]. During the PDU Session establishment, the SMF generates the default QoS rule based on the PCC rule in which the authorized default 5QI and ARP are used.

For a PDU session of unstructured type, only one PCC Rule allowing all packets is to be activated in the SMF.

6.2.2.5 Application detection

The SMF shall instruct the UPF to detect the Start and Stop of the application traffic for the PCC rules used for application detection (i.e. with application identifier) that the PCF has activated at the SMF.

If the PCF has subscribed to the event and notification is not muted for the specific PCC Rule, the SMF shall also instruct the UPF to report the Start/Stop of application, as described in the TS 23.501 [2].

When receiving the application detection report from UPF, the SMF shall forward the application identifier, the start/stop indication and, when service data flow descriptions were deduced, the application instance identifier(s) and the service data flow description(s), to the PCF.

NOTE: The PCF can make policy decision when receiving the application detection report.

6.2.2.6 Traffic steering

The SMF shall support traffic steering control as defined in Clause 6.1.3.14.

The SMF may be configured with the traffic steering policy IDs related to the mechanism enabling traffic steering to the DN and/or DNAIs associated with N6 traffic routing requirements.

Upon receiving a PCC rule which contains the traffic steering control information, the SMF shall provide the information to the UPF for the enforcement.

NOTE: The UPF may, for example, perform marking packets in order to indicate a certain type of traffic to the DN side of the N6 reference point which enables those packets to be steered in the DN. As another example the UPF may forward, i.e. offload, traffic identified by the traffic descriptor to a local tunnel.

6.2.3 Application Function (AF)

The AF functional description in clause 6.2.3 of TS 23.203 [4] applies with the following clarifications:

- the mechanism for an AF to select a PCF associated to a PDU Session is described in clause 6.1.1.2 of the present specification
- the mechanism for RAN user plane congestion mitigation is not specified in this release and as a consequence will not trigger a re-try interval in the interaction between PCF and the AF.
- In case of private IP address being used for the end user, the AF may send additional DN information (e.g. DNN). This information is used by the PCF for session binding, and it is also used to help selecting the correct PCF

In addition to the functionality described in clause 6.2.3 of TS 23.203 [4] the AF may contact the PCF via the NEF following the same functional description as when the AF contacts the PCRF via the SCEF described in TS 23.203 [4].

The AF may subscribe in the PCF to receive notifications when the QoS targets cannot be fulfilled or can be fulfilled again for a particular media flow. At the time, the PCF notifies that the AF, the affected media and the indication that the QoS targets are not fulfilled or are fulfilled again are provided over N5. The AF behaviour is out of the scope of this TS.

To support sponsored data connectivity the AF may provide the PCF with the sponsored data connectivity information, including optionally a usage threshold, as specified in clause 6.2.1.1. The AF may request the PCF to report events related to sponsored data connectivity.

NOTE: Annex N in TS 23.203 [4] describes the scenario for sponsored data connectivity.

6.2.4 Unified Data Repository (UDR)

The Unified Data Repository (UDR) is defined in TS 23.501 [2].

6.2.5 Charging Function (CHF)

The Charging Function is specified in TS 32.240 [8].

6.2.6 Void

6.2.7 Network Exposure Function (NEF)

The Network Exposure Function (NEF) is defined in TS 23.501 [2] and additionally supports the following policy related functionalities:

- Service specific policy and charging control;
- Management of packet flow descriptions;
- Sponsor data connectivity including usage monitoring (as defined in TS 23.203 [4]);
- Negotiations for future background data transfer.

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 access selection and PDU Session selection policies received from the PCF to the UE via N1 interface.
- Reporting of events to the PCF that the PCF has subscribed to.

6.2.9 Network Data Analytics Function (NWDAF)

NWDAF is defined in TS 23.501 [2].

6.3 Policy and charging control rule

6.3.1 General

To enable the enforcement in the 5GC of the policy decisions made by the PCF for the policy and charging control of a service data flow, the 5GC shall provide 5G Policy and Charging Control information from the PCF to the SMF as described in table 6.3.1.

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.

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 3GPP 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	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, offline or neither.	Conditional (NOTE 7)	No	None
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

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]
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)	Identifier for the authorized QoS parameters 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 again) be fulfilled 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.	Conditional (NOTE 11)	Yes	Modified (corresponds to bind to the default bearer in TS 23.203 [4])
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

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]
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
Access Network Information Reporting	This part describes access network information to be reported for the PCC rule when the corresponding bearer is established, modified or terminated.			
User Location Report	The serving cell of the UE is to be reported. When the corresponding bearer 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	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
Traffic Steering Enforcement Control	This part describes identities required for Traffic Steering Enforcement Control.			
Traffic steering policy identifier(s)	Reference to a pre-configured traffic steering policy at the SMF (NOTE 12).		Yes	None
Data Network Access Identifier	Identifier of the target Data Network Access. It is defined in 3GPP TS 23.501 [2], clause 5.6.7.		Yes	Added
Data Network Access Change report	Indicates whether a notification in case of change of DNAI at addition/change/removal of the UPF is requested, as well as the destination(s) for where to provide the notification. The notification information includes the target DNAI and an indication of early and/or late notification. It is defined in 3GPP 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

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]
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

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, in case the service data flow template consists of a set of service data flow filters. NO in case 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.
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.

The *Service data flow template* may comprise any number of *Service data flow filters* or an *application identifier* for IP PDU traffic as is defined in table 6.3. Additionally, it may also comprise any combination of traffic patterns of the Ethernet PDU traffic.

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 *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 *QoS Notification Control,* QNC*,* indicates whether notifications are requested from the access network (i.e. 3GPP RAN) when the GFBR can no longer (or again) be fulfilled for a QoS Flow during the lifetime of the QoS Flow. If it is set and QoS targets cannot be fulfilled or can be fulfilled again, the access network (i.e. 3GPP RAN) sends a notification towards SMF, which notifies to PCF.

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: 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 Traffic Steering Enforcement Control contains:

- The *Target DNAI* is a reference to the DNAI the SMF needs to consider for UPF selection/reselection.
- The Data Network Access Change report parameters (*Target DNAI* and *Indication of early and/or late notification*) instruct the SMF about what information to forward to the PCF when DNAI changes at change of the UPF and where to provide the indication.

6.3.2 Policy and charging control rule operations

Policy and Charging Rule operations consist of activation, modification and de-activation of PCC rules performed by PCF to SMF.

An active PCC rule means that:

- the service data flow template shall be used for service data flow detection;
- the service data flow template shall be used for mapping of downlink packets to the QoS Flow determined by the QoS Flow binding;
- the service data flow template shall be used for service data flow detection of uplink packets on the PDU Session;
- usage data for the service data flow shall be recorded;
- policies associated with the PCC rule, if any, shall be invoked;
- for service data flow detection with an application detection filter, the start or the stop of the application traffic is reported to the PCF, if applicable and requested by the PCF. In that case, the notification for start may include service data flow filters, (if possible to provide) and the application instance identifier associated with the service data flow filters.

A predefined PCC rule is known at least, within the scope of one PDU Session.

NOTE 1: The same predefined PCC rule can be activated for multiple QoS Flows in multiple PDU Sessions.

A predefined PCC rule is bound to one and only one QoS Flow per PDU Session. For a predefined PCC rule whose service data flow cannot be fully reflected for the uplink direction in terms of traffic mapping information sent to the UE, the SMF may request the UPF to apply the uplink service data flow detection at additional QoS Flows with non-GBR 5QI of the same PDU Session. The deactivation of such a predefined PCC rule ceases its service data flow detection for the whole PDU Session.

The PCF may, at any time, deactivate an active PCC rule in the SMF. At QoS Flow termination all active PCC rules on that QoS Flow are deactivated without explicit instructions from the PCF to do so.

Policy and charging control rule operations can be also performed in a deferred mode. A PCC rule may have either a single deferred activation time, or a single deferred deactivation time or both. How activation and deactivation works is described in clause 6.3.2.

Deferred activation and deactivation of PCC rules can only be used for PCC rules that belong to the QoS Flow without traffic mapping information.

NOTE 2: This limitation prevents dependencies on the signalling of changed traffic mapping information towards the UE.

6.4 PDU Session related policy information

The PCF may provide PDU Session related policy information to the SMF.

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

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.	No	PDU Session	None
Default charging method	Defines the default charging method for the PDU Session.	No	PDU Session	None
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 4)	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	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 5.8.1.1.	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)	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

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]
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)	Defines the default 5QI and ARP when the Time Condition is reached.	No (NOTE 5)	PDU Session	Modified
Usage Monitoring Control related information	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	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

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.

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

The *Charging information* contains CHF addresses defining the addresses defining the charging function addresses respectively. These shall override any possible predefined addresses at the SMF. If received by the SMF, it supersedes the Primary CHF address and Secondary CHF address in the charging characteristics profile.

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.

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 1: 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 default 5QI and ARP values of the QoS Flow, i.e. the QoS Flow associated with the default QoS rule as described in TS 23.501 [2] clause 5.7.2. The PCF may provide the *Authorized default 5QI/ARP* in every interaction with the SMF. The SMF shall apply the *Authorized default 5QI/ARP* for the PDU Session, including the necessary QoS Flow binding actions.

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. 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 2: 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 3: 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 4: 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 at the SMF.

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.

6.5 Access and mobility related policy information

To enable the enforcement in the 5GC system of the access and mobility policy decisions made by the PCF for the control of the service area restrictions and RFSP Index, the 5GC system may provide the Access and mobility related policy control information from the PCF to the AMF.

Table 6.5-1 lists the AMF access and mobility related policy information.

Table 6.5-1: Access and mobility related policy control information

Information name	Description	Category	PCF permitted to modify in a UE context in the AMF	Scope
Service Area Restrictions	*This part defines the service area restrictions*			
List of allowed TAIs.	List of allowed TAIs (NOTE 3) (NOTE 4).	Conditional (NOTE 1)	Yes	UE context
List of non-allowed TAIs.	List of non-allowed TAIs (NOTE 3).	Conditional (NOTE 1)	Yes	UE context
Maximum number of allowed TAIs	The maximum number of allowed TAIs. (NOTE 4)	Conditional (NOTE 1)	Yes	UE context
RFSP Index	*This part defines the RFSP index*			
RFSP Index	Defines the RFSP Index that applies for a UE	Conditional (NOTE 2)	Yes	UE context
NOTE 1: If service area restrictions is enable. NOTE 2: If RFSP index is enable. NOTE 3: Either the list of allowed TAIs or the list of non-allowed TAIs are provided by the PCF. NOTE 4: Both the maximum number of allowed TAIs and the list of allowed TAIs may be sent by PCF.				

The *list of allowed TAIs* indicates the TAIs where the UE is allowed to be registered, see TS 23.501 [2] clause 5.3.4 for the description on how AMF uses this information.

The *list of non-allowed TAIs* indicates the TAIs where the UE is not allowed to be registered, see TS 23.501 [2] clause 5.3.4 for the description on how AMF uses this information.

The *Maximum number of allowed TAs* indicates the maximum number of allowed Tracking Areas, the list of TAI is defined in the AMF and not explicitly provided by the PCF.

The *RFSP Index* defines the RFSP Index for radio resource management functionality.

6.6 UE access selection and PDU Session selection related policy information

6.6.1 Access Network Discovery & Selection Policy Information

6.6.1.1 General

The Access Network Discovery & Selection policy is an optional policy that may be provided to UE by the network.

In this release of the specification, the Access Network Discovery & Selection policy shall contain only rules that aid the UE in selecting a WLAN access network. Rules for selecting other types of non-3GPP access networks are not specified.

The WLAN access network selected by the UE with the use of Access Network Discovery & Selection policy may be used for direct traffic offload (i.e. sending traffic to the WLAN outside of a PDU Session) and for registering to 5GC using the non-3GPP access network selection information.

The procedure for WLAN access network selection is defined in clause 6.6.1.3, the procedure for N3IWF selection is defined in TS 23.501 [2] clause 6.3.6.1.

The Access Network Discovery & Selection policy shall contain one or more WLAN Selection Policy (WLANSP) rules defined in clause 4.8.2.1.6 of TS 23.402 [9].

The Access Network Discovery & Selection policy may contain information to select ePDG or N3IWF by the UE as specified in TS 23.501 [2]

Table 6.6.1-1: Access Network Discovery & Selection Policy

Information name	Description	Category	PCF permitted to modify in a UE context	Scope
WLANSP rules	1 or more WLANSP rules as specified in 4.8.2.1.6 of TS 23.402 [9]	Mandatory	Yes	UE context
ePDG identifier configuration	The UE uses this information to select ePDG as defined in clause 6.3.6.1 of TS 23.501 [2]	Optional	Yes	UE context
N3IWF identifier configuration	The UE uses this information to select N3IWF as defined in clause 6.3.6.1 of TS 23.501 [2]	Optional	Yes	UE context
Non-3GPP access node (N3AN) selection information	The UE uses this information to select ePDG or N3IWF as defined in clause 6.3.6.1 of TS 23.501 [2]	Optional	Yes	UE context

6.6.1.2 UE selecting a WLANSP rule

The UE may be provisioned with multiple valid WLANSP rules (by the HPLMN and by the VPLMN when the UE is roaming). A WLANSP rule is valid if it meets the validity conditions included in the WLANSP rule (if provided).

When the UE is in the home the UE uses the valid WLANSP rules from the home PLMN to select an available WLAN. When the UE is roaming and the UE has valid rules from both HPLMN and VPLMN the UE gives priority to the valid WLANSP rules from the VPLMN.

6.6.1.3 UE procedure for selecting a WLAN access based on WLANSP rules

When the UE has valid 3GPP subscription credentials (i.e. a valid USIM) and WLANSP rules, the UE shall perform WLAN selection based on these rules, the applicable user preferences and the corresponding procedures specified in this document. User preferences take precedence over the WLANSP rules.

The UE determines the most preferred WLAN access network using WLANSP rules when a WLAN access network cannot be selected based on user preferences (e.g. when there are no user preferences or when there is no user-preferred WLAN access network available).

The UE constructs a prioritized list of the available WLANs by discovering the available WLANs and comparing their attributes / capabilities against the groups of selection criteria in the valid WLANSP rule(s). When there are multiple valid WLANSP rules the UE evaluates the valid WLANSP rules in priority order. The UE evaluates first if an available WLAN access meets the criteria of the highest priority valid WLANSP rule. The UE then evaluates if an available WLAN access meets the selection criteria of the next priority valid WLANSP rule.

Within a valid WLANSP rule, the WLAN(s) that match the group of selection criteria with the highest priority are considered as the most preferred WLANs, the WLAN(s) that match the group of selection criteria with the second highest priority are considered as the second most preferred WLANs, etc.

When a group of selection criteria includes the HomeNetwork attribute and is set, then the UE (a) shall create a list of available WLANs that directly interwork with the home operator (as specified in clause 4.8.2.1.6 of 3GPP TS 23.402 [9]) and (b) shall apply the group of selection criteria to all the WLANs in this list. Otherwise, when the HomeNetwork attribute is not set or is not present, the UE shall apply the group of selection criteria to all available WLANs. The UE may need to perform ANQP procedures (as specified in the HS2.0 Rel-2 specification [ref]) or other procedures in order to discover the attributes / capabilities of the available WLANs.

When the UE is roaming the UE may have valid WLANSP rules from both the VPLMN and the HPLMN. In such a case the UE gives priority to the valid WLANSP rules from the VPLMN. The UE constructs a prioritised list of the available WLANs when the available WLAN accesses meet the selection criteria of the valid rules from the VPLMN and the valid rules from the HPLMN. The prioritised WLAN accesses based on the WLANSP rules from the HPLMN will have lower priority from the prioritised list of WLAN access based on the WLANSP rules of the VPLMN.

6.6.2 UE Route Selection Policy information

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 descriptors for the policy*			
Application identifiers	Application identifier(s)	Optional	Yes	UE context
IP descriptors	IP 3 tuple(s) (destination IP address or IPv6 network prefix, destination port number, protocol ID of the protocol above IP)	Optional	Yes	UE context
Non-IP descriptors	Descriptor(s) for non-IP traffic	Optional	Yes	UE context
DNN	This is the DNN information provided by the application	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.				

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.	Optional	Yes	UE context
Network Slice Selection	Either a single value or a list of values of S-NSSAI(s).	Optional	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	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 3)	Yes	UE context
Access Type preference	Indicates the preferred Access Type (3GPP or non-3GPP) when the UE establishes a PDU Session for the matching application.	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 component shall be present. NOTE 3: If this indication is present in a Route Selection Descriptor, no other components shall be included in the Route Selection Descriptor.				

Each URSP rule contains a Rule Precedence value that determines the priority of the rule within the policy. Rules in a URSP shall have different precedence values.

Each URSP rule contains a Traffic descriptor that determines when the rule is applicable.

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

- Session Continuity Mode: Indicates that the traffic of the matching application shall be routed via a PDU Session supporting 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) on which the PDU Session should be established.

NOTE 1: 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.

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.

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.

NOTE 2: How to set the URSP rule with the "match all" traffic descriptor as the URSP rule with lowest priority is defined in TS 24.501 [14].

6.6.2.2 Configuration and Provision of URSP

The UE may be provisioned with URSP rules by PCF of the HPLMN. When the UE is roaming, the PCF in the HPLMN may update the URSP rule in the UE. In addition, the UE may be also pre-configured with URSP rules (e.g. by the operator).

Only the URSP rules provisioned by the PCF is used by the UE, if both URSP rules provisioned by the PCF and pre-configured URSP rules are present.

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 the Application ID, DNN or traffic of the application is found matching a Traffic descriptor in an URSP rule, the UE shall select a Route Selection Descriptor within this URSP rule in the order of the Route Selection Descriptor Precedence. The selected Route Selection Descriptor shall be only valid if all of the following criteria are fulfilled:

- If any S-NSSAI(s) is present, the S-NSSAI(s) is in the Allowed S-NSSAI(s).

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

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 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.

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 in the order of the Route Selection Descriptor Precedence, if any.

The UE re-evaluates the URSP rules and may change the association of applications to PDU Sessions if the UE experiences certain conditions, for example:

- periodic URSP rules 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 URSP is updated by the PCF;
- the UE moves from EPC to 5GC;
- UE registers over 3GPP or non-3GPP access;
- UE establishes connection to a WLAN access.

Details of the conditions are defined by TS 24.501 [14].

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 descriptors of the URSP rule via the WLAN access outside of a PDU session.

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 filter: App=App 1	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 filter: App=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 applications "App2" as follows:. It enforces the following routing policy: The traffic of application App2should 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. If the PDU session cannot be established, the traffic of these applications shall be directly offloaded to non-3GPP access with SSID-a (based on the 2nd RSD)
	Route Selection Descriptor Precedence =2 Non-seamless Offload indication: Permitted (WLAN SSID-a)	
Rule Precedence =3 Traffic filter: 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 = lowest priority Traffic filter: *	Network Slice Selection: S-NSSAI-b SSC Mode Selection: Type-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.

Annex B (informative): Deployment option to support of BSF and DRA coexistence due to network migration

During the network migration, DRA and BSF may coexist in operator's network. The DRA can be a consumer of Nbsf services and the BSF can provide binding functionality for different subscribers. When the AF using Rx, such as P-CSCF, sends Rx request to the DRA, if the DRA has no binding information for the subscriber, based on configuration or via NRF, it selects the BSF. Then the DRA can query the BSF by invoking Nbsf_Management discovery service operation, to get the relevant PCF address, based on which the DRA routes the Rx request to the selected PCF.

NOTE: The DRA decides to select a BSF based on user IP address range.

Annex C (informative): Change history

Change history							
Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2017-12	SP-78	SP-170933	-	-	-	MCC Editorial update for presentation to TSG SA#78 for approval	1.0.0
2017-12	SP-78	-	-	-	-	MCC Editorial update after TSG SA#78 Approval	15.0.0
2018-03	SP-79	SP-180107	0001	-	F	Clarification on PCF interaction	15.1.0
2018-03	SP-79	SP-180092	0002	3	F	Remove EN related with Session binding	15.1.0
2018-03	SP-79	SP-180107	0003	1	F	Correction for background data transfer for TS 23.503	15.1.0
2018-03	SP-79	SP-180093	0004	-	F	Correction on Notification control for GBR QoS flow	15.1.0
2018-03	SP-79	SP-180093	0005	1	F	Addition of Reflective QoS Timer in PDU session related policy information	15.1.0
2018-03	SP-79	SP-180107	0006	2	F	Removal of editor's notes and addition of references to empty sections	15.1.0
2018-03	SP-79	SP-180107	0007	1	F	Influence of additional non-standardized QoS parameters on QoS Flow Binding	15.1.0
2018-03	SP-79	SP-180107	0008	1	F	Description of components in URSP	15.1.0
2018-03	SP-79	SP-180107	0010	1	F	QoS rule generation	15.1.0
2018-03	SP-79	SP-180093	0011	2	F	UE policies granularity and UE assistance for policy evaluation	15.1.0
2018-03	SP-79	SP-180091	0012	1	F	Resource reservation for services sharing priority	15.1.0
2018-03	SP-79	SP-180093	0013	2	F	Add Nchf service in service base representation architecture	15.1.0
2018-03	SP-79	SP-180107	0014	-	F	Traffic mapping information that disallows UL packets	15.1.0
2018-03	SP-79	SP-180091	0016	1	F	Moving NWDAF to 23.501	15.1.0
2018-03	SP-79	SP-180107	0017	3	F	Default URSP Rule	15.1.0
2018-03	SP-79	SP-180107	0018	2	F	UE selects a PDU Session based on URSP	15.1.0
2018-03	SP-79	SP-180107	0020	2	F	Clarification on the handling of event triggers	15.1.0
2018-03	SP-79	SP-180107	0021	3	F	Update of UDR policy related subscription	15.1.0
2018-03	SP-79	SP-180107	0022	1	F	Remove EN related with EPC IWK	15.1.0
2018-03	SP-79	SP-180107	0023	-	F	Remove some ENs	15.1.0
2018-03	SP-79	SP-180107	0024	3	F	AF subscription to AMF and SMF events and events reporting	15.1.0
2018-03	SP-79	SP-180107	0025	1	F	Corrections to description of session management related policy enforcement	15.1.0
2018-03	SP-79	SP-180095	0028	2	B	Supporting 3GPP PS Data Off in 5GS	15.1.0
2018-03	SP-79	SP-180107	0031	2	F	Session Binding Mechanism for non-IP PDU Session	15.1.0
2018-03	SP-79	SP-180107	0032	2	F	Clarification on enforcement of Application Detection Control	15.1.0
2018-03	SP-79	SP-180092	0033	2	F	Resolve the Editor's Note on Presence Reporting Area	15.1.0
2018-03	SP-79	SP-180107	0034	2	F	Update of event trigger section	15.1.0
2018-03	SP-79	SP-180107	0035	5	F	Clarification on AF using legacy Rx binding with relevant PCF	15.1.0
2018-03	SP-79	SP-180125	0036	1	B	Addition of PDU Session type IPv4v6	15.1.0
2018-06	SP-80	SP-180478	0019	7	B	Additional PDU Session Type in Route Selection Descriptor	15.2.0
2018-06	SP-80	SP-180483	0037	1	F	Correction to URSP and UE preferences for NSSP and SSCMSP	15.2.0
2018-06	SP-80	SP-180481	0043	7	F	Clarification on using PSI	15.2.0
2018-06	SP-80	SP-180481	0044	7	F	Clarification on UE policy configuration	15.2.0
2018-06	SP-80	SP-180483	0046	1	F	Correction on Policy Control Request Triggers	15.2.0
2018-06	SP-80	SP-180480	0049	2	F	Clarification on match all URSP rule	15.2.0
2018-06	SP-80	SP-180480	0050	2	F	Clarification on policy provision in roaming case	15.2.0
2018-06	SP-80	SP-180478	0051	2	F	Alignment with the definition of PCF-AMF and PCF-SMF interfaces	15.2.0
2018-06	SP-80	SP-180482	0053	1	F	Cleanups on the support of session binding for Ethernet PDU session Type	15.2.0
2018-06	SP-80	SP-180486	0054	2	F	NEF and UDR in LBO architecture for AF influence on traffic routing	15.2.0
2018-06	SP-80	SP-180486	0055	5	F	Network slicing information for binding the AF request to the relevant PCF	15.2.0
2018-06	SP-80	SP-180489	0058	4	F	Support use of DNN for URSP traffic descriptor	15.2.0
2018-06	SP-80	SP-180490	0060	1	F	TS23.503 Clarification on Access and mobility related policy	15.2.0
2018-06	SP-80	SP-180490	0061	2	F	TS23.503 Clarification on BSF	15.2.0
2018-06	SP-80	SP-180490	0062	2	F	TS23.503 ePDG/N3IWF selection information	15.2.0
2018-06	SP-80	SP-180483	0063	2	F	Correction to the UE Policy Section 6.1.2.2.1	15.2.0
2018-06	SP-80	SP-180489	0064	-	F	The interaction between PCF and AF	15.2.0
2018-06	SP-80	SP-180484	0067	-	F	Corrections to PFD management descriptions	15.2.0
2018-06	SP-80	SP-180487	0068	1	F	Protocol criteria for domain name matching	15.2.0
2018-06	SP-80	SP-180484	0071	3	F	Delivery of UE policies	15.2.0
2018-06	SP-80	SP-180485	0073	2	F	How to differentiate the PSIs in different PLMNs	15.2.0
2018-06	SP-80	SP-180477	0079	-	D	Corrected the name of a PCF service operation in clause 6.1.2.2.2	15.2.0
2018-06	SP-80	SP-180485	0081	2	F	Handling of Configured NSSAIs in Roaming Scenarios - 23.503	15.2.0
2018-06	SP-80	SP-180478	0082	2	F	Alignement for policy control application specific information	15.2.0

2018-06	SP-80	SP-180490	0084	2	F	Update for usage monitoring support	15.2.0
2018-06	SP-80	SP-180490	0085	2	F	Update for sponsored data connectivity support	15.2.0
2018-06	SP-80	SP-180487	0087	5	F	Provisioning of ANDSP via signalling	15.2.0
2018-06	SP-80	SP-180483	0088	4	F	Provisioning of ANDSP via signalling	15.2.0
2018-06	SP-80	SP-180487	0089	2	F	QoS flow binding for URLLC services	15.2.0
2018-06	SP-80	SP-180487	0093	1	F	Removal of editor's notes	15.2.0