

Statement of Compliance towards 3GPP Technical Specification 23.203 (Release 14)

Ericsson Service-Aware Policy Controller

Statement of Compliance

Copyright

© Ericsson AB 2018. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document [Trademark Information](#).



Contents

| | | |
|----------|---|-----------|
| 1 | Introduction | 1 |
| 2 | General Considerations | 2 |
| 3 | Scope, References and Abbreviations | 3 |
| 3.1 | Scope | 3 |
| 3.2 | References | 3 |
| 3.3 | Definitions and Abbreviations | 3 |
| 3.3.1 | Definitions | 3 |
| 3.3.2 | Abbreviations | 3 |
| 4 | High Level Requirements | 4 |
| 4.1 | General Requirements | 4 |
| 4.2 | Charging Related Requirements | 7 |
| 4.2.1 | General | 7 |
| 4.2.2 | Charging Models | 7 |
| 4.2.3 | Examples of Service Data Flow Charging | 8 |
| 4.3 | Policy Control Requirements | 8 |
| 4.3.1 | General | 8 |
| 4.3.2 | Gating Control | 8 |
| 4.3.3 | QoS Control | 8 |
| 4.3.3.1 | QoS Control at Service Data Flow Level | 8 |
| 4.3.3.2 | QoS Control at IP CAN Bearer Level | 9 |
| 4.3.3.3 | QoS Conflict Handling | 10 |
| 4.3.3.4 | QoS Control at APN Level | 11 |
| 4.3.4 | Subscriber Spending Limits | 11 |
| 4.4 | Usage Monitoring Control | 12 |
| 4.5 | Application Detection and Control | 14 |
| 4.6 | RAN User Plane Congestion Detection, Reporting and Mitigation | 17 |
| 4.7 | Support for Service Capability Exposure | 17 |
| 4.8 | Traffic Steering Control | 17 |
| 4.9 | Management of Packet Flow Descriptions in the PCEF/TDF Using the PFDF | 17 |
| 5 | Architecture Model and Reference Points | 18 |
| 5.1 | Reference Architecture | 18 |
| 5.2 | Reference Points | 18 |
| 5.2.1 | Rx Reference Point | 18 |



| | | |
|----------|---|-----------|
| 5.2.2 | Gx Reference Point | 18 |
| 5.2.3 | Reference Points to Subscriber Databases | 19 |
| 5.2.3.1 | Sp Reference Point | 20 |
| 5.2.3.2 | Ud Reference Point | 20 |
| 5.2.4 | Gy Reference Point | 20 |
| 5.2.5 | Gz Reference Point | 21 |
| 5.2.6 | S9 Reference Point | 21 |
| 5.2.7 | Gxx Reference Point | 21 |
| 5.2.8 | Sd Reference Point | 21 |
| 5.2.9 | Sy Reference Point | 22 |
| 5.2.10 | Gyn Reference Point | 23 |
| 5.2.11 | Gzn Reference Point | 23 |
| 5.2.12 | Np Reference Point | 23 |
| 5.2.13 | Nt Reference Point | 23 |
| 5.2.14 | St Reference Point | 23 |
| 5.2.15 | Nu Reference Point | 23 |
| 5.2.16 | Gw Reference Point | 23 |
| 5.2.17 | Gwn Reference Point | 23 |
| 6 | Functional Description | 24 |
| 6.1 | Overall Description | 24 |
| 6.1.1 | Binding Mechanism | 24 |
| 6.1.1.1 | General | 24 |
| 6.1.1.2 | Session Binding | 25 |
| 6.1.1.3 | PCC Rule Authorization and QoS Rule Generation | 26 |
| 6.1.1.4 | Bearer Binding | 31 |
| 6.1.2 | Reporting | 32 |
| 6.1.3 | Credit Management | 32 |
| 6.1.4 | Event Triggers | 33 |
| 6.1.5 | Policy Control | 39 |
| 6.1.6 | Service (Data Flow) Prioritization and Conflict Handling | 42 |
| 6.1.7 | Standardized QoS Characteristics | 42 |
| 6.1.7.1 | General | 42 |
| 6.1.7.2 | Standardized QCI Characteristics | 43 |
| 6.1.7.3 | Allocation and Retention Priority Characteristics | 43 |
| 6.1.8 | Termination Action | 43 |
| 6.1.9 | Handling of Packet Filters Provided to the UE by PCEF/BBERF | 43 |
| 6.1.10 | IMS Emergency Session Support | 43 |
| 6.1.10.1 | Architecture Model and Reference Points | 43 |
| 6.1.10.2 | PCC Rule Authorization and QoS Rule Generation | 43 |
| 6.1.10.3 | Functional Entities | 44 |
| 6.1.10.4 | PCC Procedures and Flows | 46 |
| 6.1.11 | Multimedia Priority Service Support | 46 |
| 6.1.11.1 | Architecture model and Reference points | 46 |
| 6.1.11.2 | PCC rule authorization and QoS rule generation | 47 |
| 6.1.11.3 | Priority EPS Bearer Service | 48 |
| 6.1.11.4 | Bearer priority for IMS Multimedia Priority Services | 49 |



| | | |
|---------|---|-----|
| 6.1.12 | ADC Rule Authorization | 50 |
| 6.1.13 | Redirection | 51 |
| 6.1.14 | Resource Sharing for Different AF Sessions | 51 |
| 6.1.15 | Reporting of RAN User Plane Congestion Information | 51 |
| 6.1.16 | Negotiation for Future Background Data Transfer | 51 |
| 6.1.17 | Traffic Steering Control | 52 |
| 6.1.18 | PCC Support of NBIFOM | 52 |
| 6.1.19 | Resource Reservation for Services Sharing Priority | 52 |
| 6.1.20 | Management of Packet Flow Descriptions Using the PFDF | 52 |
| 6.1.21 | 3GPP PS Data Off | 52 |
| 6.2 | Functional Entities | 52 |
| 6.2.1 | Policy Control and Charging Rules Function (PCRF) | 52 |
| 6.2.1.1 | Input for PCC Decisions | 68 |
| 6.2.1.2 | Subscription Information Management in the PCRF | 73 |
| 6.2.1.3 | V-PCRF | 73 |
| 6.2.1.4 | H-PCRF | 74 |
| 6.2.1.5 | Handling of Multiple BBFs Associated with the Same IP CAN Session | 74 |
| 6.2.2 | Policy and Charging Enforcement Function (PCEF) | 74 |
| 6.2.3 | Application Function (AF) | 74 |
| 6.2.4 | Subscription Profile Repository (SPR) | 75 |
| 6.2.5 | Online Charging System | 76 |
| 6.2.6 | Offline Charging System (OFCS) | 76 |
| 6.2.7 | Bearer Binding and Event Reporting Function (BBERF) | 76 |
| 6.2.8 | User Data Repository (UDR) | 77 |
| 6.2.9 | Traffic Detection Function (TDF) | 77 |
| 6.2.10 | RAN Congestion Awareness Function (RCAF) | 77 |
| 6.2.11 | Service Capability Exposure Function (SCEF) | 77 |
| 6.2.12 | Traffic Steering Support Function (TSSF) | 77 |
| 6.2.13 | Packet Flow Description Function (PFDF) | 77 |
| 6.3 | Policy and Charging Control Rule | 77 |
| 6.3.1 | General | 77 |
| 6.3.2 | Policy and Charging Control Rule Operations | 88 |
| 6.4 | IP-CAN Bearer and IP-CAN Session Related Policy Information | 90 |
| 6.4.1 | TDF Session Related Policy Information | 93 |
| 6.4.2 | APN Related Policy Information | 95 |
| 6.5 | Quality of Service Control Rule | 97 |
| 6.6 | Usage Monitoring Control Specific Information | 97 |
| 6.6.1 | General | 98 |
| 6.6.2 | Usage Monitoring Control Operations | 99 |
| 6.7 | S2c Based IP Flow Mobility Routing Rule | 99 |
| 6.8 | Application Detection and Control Rule | 99 |
| 6.8.1 | General | 99 |
| 6.8.2 | Application Detection and Control Rule Operations over Sd | 106 |



| | | |
|----------|--|------------|
| 6.9 | Policy Decisions Based on Spending Limits | 108 |
| 6.10 | Traffic Steering Control Information | 109 |
| 6.11 | NBIFOM Routing Rule | 109 |
| 7 | PCC Procedures and Flows | 110 |
| 7.1 | Introduction | 110 |
| 7.2 | IP-CAN Session Establishment | 110 |
| 7.3 | IP-CAN Session Termination | 117 |
| 7.3.1 | UE Initiated IP-CAN Session Termination | 117 |
| 7.3.2 | GW (PCEF) Initiated IP-CAN Session Termination | 121 |
| 7.4 | IP-CAN Session Modification | 125 |
| 7.4.1 | IP-CAN Session Modification; GW (PCEF) Initiated | 125 |
| 7.4.2 | IP-CAN Session Modification; PCRF Initiated | 129 |
| 7.4.3 | Void | 135 |
| 7.5 | Update of the Subscription Information in the PCRF | 135 |
| 7.6 | PCRF Discovery and Selection | 136 |
| 7.6.1 | General Principles | 136 |
| 7.6.2 | Solution Principles | 137 |
| 7.7 | Gateway Control Session Procedures | 137 |
| 7.8 | Change in Subscription for MPS Priority Services | 138 |
| 7.9 | Procedures over Sy Reference Point | 138 |
| 7.9.1 | Initial Spending Limit Report Request | 138 |
| 7.9.2 | Intermediate Spending Limit Report Request | 139 |
| 7.9.3 | Final Spending Limit Report Request | 139 |
| 7.9.4 | Spending Limit Report | 140 |
| 7.10 | Procedures over Np Reference Point | 140 |
| 7.11 | Procedures over Nt reference point | 140 |
| 7.12 | Procedures for Management of PFDs | 140 |
| 8 | Annex A (Normative): Access Specific Aspects (3GPP) | 141 |
| 8.1 | A.1 GPRS | 141 |
| 8.1.1 | A.1.0 General | 141 |
| 8.1.2 | A.1.1 High level requirements | 141 |
| 8.1.2.1 | A.1.1.1 General | 141 |
| 8.1.2.2 | A.1.1.2 Charging Related Requirements | 141 |
| 8.1.2.3 | A.1.1.3 Policy Control Requirements | 141 |
| 8.1.2.4 | A.1.1.4 QoS Control | 141 |
| 8.1.3 | A.1.2 Architecture Model and Reference Points | 141 |
| 8.1.3.1 | A.1.2.1 Reference Points | 141 |
| 8.1.3.2 | A.1.2.2 Reference Architecture | 142 |
| 8.1.4 | A.1.3 Functional Description | 142 |
| 8.1.4.1 | A.1.3.1 Overall Description | 142 |
| 8.1.4.2 | A.1.3.2 Functional Entities | 144 |



| | | |
|---------|---|-----|
| 8.1.4.3 | A.1.3.3 Policy and Charging Control Rule | 144 |
| 8.1.4.4 | A.1.3.4 IP-CAN bearer and IP-CAN Session Related Policy Information | 145 |
| 8.1.4.5 | A.1.3.4a TDF Session Related Policy Information | 145 |
| 8.1.4.6 | A.1.3.5 Void | 145 |
| 8.1.5 | A.1.4 PCC Procedures and Flows | 145 |
| 8.1.5.1 | A.1.4.1 Introduction | 145 |
| 8.1.5.2 | A.1.4.2 IP-CAN Session Establishment | 145 |
| 8.1.5.3 | A.1.4.3 IP-CAN Session Termination | 145 |
| 8.1.5.4 | A.1.4.4 IP-CAN Session Modification | 146 |
| 8.2 | A.2 Void | 146 |
| 8.3 | A.3 Void | 146 |
| 8.4 | A.4 3GPP Accesses (GERAN/UTRAN/E-UTRAN) - GTP-Based EPC | 146 |
| 8.4.1 | A.4.0 General | 146 |
| 8.4.2 | A.4.1 High Level Requirements | 146 |
| 8.4.2.1 | A.4.1.1 Charging Related Requirements | 146 |
| 8.4.2.2 | A.4.1.2 QoS Control | 146 |
| 8.4.3 | A.4.2 Architectural Model and Reference Points | 148 |
| 8.4.3.1 | A.4.2.1 Reference Architecture | 148 |
| 8.4.4 | A.4.3 Functional Description | 148 |
| 8.4.4.1 | A.4.3.1 Overall Description | 148 |
| 8.4.4.2 | A.4.3.2 Functional Entities | 149 |
| 8.4.4.3 | A.4.3.3 Void | 151 |
| 8.4.4.4 | A.4.3.4 IP-CAN Bearer and IP-CAN Session Related Policy Information | 151 |
| 8.4.4.5 | A.4.3.5 TDF Session Related Policy Information | 151 |
| 8.4.5 | A.4.4 PCC Procedures and Flows | 151 |
| 8.4.5.1 | A.4.4.1 Introduction | 151 |
| 8.4.5.2 | A.4.4.2 IP-CAN Session Establishment | 151 |
| 8.4.5.3 | A.4.4.3 GW (PCEF) Initiated IP CAN Session Termination | 151 |
| 8.4.5.4 | A.4.4.4 IP-CAN Session Modification | 151 |
| 8.5 | A.5 3GPP Accesses (GERAN/UTRAN/E-UTRAN) - PMIP-Based EPC | 152 |
| 8.5.1 | A.5.0 General | 152 |
| 8.5.2 | A.5.1 High Level Requirements | 152 |
| 8.5.2.1 | A.5.1.0 General | 153 |
| 8.5.2.2 | A.5.1.1 QoS Control | 153 |
| 8.5.3 | A.5.2 Architectural Model and Reference Points | 153 |
| 8.5.3.1 | A.5.2.1 Reference Architecture | 153 |
| 8.5.4 | A.5.3 Functional Description | 153 |
| 8.5.4.1 | A.5.3.1 Overall Description | 153 |
| 8.5.4.2 | A.5.3.2 Functional Entities | 153 |
| 8.5.4.3 | A.5.3.3 Void | 154 |
| 8.5.4.4 | A.5.3.4 Void | 154 |
| 8.5.4.5 | A.5.3.5 IP-CAN Bearer and IP-CAN Session Related Policy Information | 154 |



| | | |
|---------|--|------------|
| 8.5.4.6 | A.5.3.6 TDF Session Related Policy Information | 154 |
| 8.5.5 | A.5.4 PCC Procedures and Flows | 154 |
| 8.5.5.1 | A.5.4.1 Introduction | 154 |
| 8.5.5.2 | A.5.4.2 Gateway Control Session Establishment | 154 |
| 8.5.5.3 | A.5.4.3 Gateway Control and QoS Rules Request | 154 |
| 8.5.5.4 | A.5.4.4 Gateway Control and QoS Rules Provisioning | 154 |
| 8.5.5.5 | A.5.4.5 IP-CAN Session Establishment | 154 |
| 8.5.5.6 | A.5.4.6 IP CAN Session Modification | 155 |
| 9 | Annex B (Informative): Void | 156 |
| 10 | Annex C (Informative): Void | 157 |
| 11 | Annex D (Informative): Access Specific Aspects (Non-3GPP) | 158 |
| 12 | Annex E (Informative): Void | 159 |
| 13 | Annex F (Informative): Void | 160 |
| 14 | Annex G (Informative): PCC Rule Precedence Configuration | 161 |
| 15 | Annex H (Normative): Access Specific Aspects (EPC-Based Non-3GPP) | 162 |
| 15.1 | H.1 General | 162 |
| 15.2 | H.2 EPC-Based cdma2000 HRPD Access | 162 |
| 15.3 | H.3 EPC-Based Trusted WLAN Access with S2a | 162 |
| 15.4 | H.4 EPC-Based Untrusted Non-3GPP Access | 162 |
| 16 | Annex I (Informative): Void | 164 |
| 17 | Annex J (Informative): Standardized QCI Characteristics - Rationale and Principles | 165 |
| 18 | Annex K (Informative): Limited PCC Deployment | 166 |
| 19 | Annex L (Normative): Limited PCC Deployment | 167 |
| 20 | Annex M (Informative): Handling of UE or Network Responsibility for the Resource Management of Services | 168 |
| 21 | Annex N (Informative): PCC Usage for Sponsored Data Connectivity | 169 |
| 22 | Annex P (Normative): Fixed Broadband Access Interworking with EPC | 170 |
| 23 | Annex Q (Informative): How to Achieve Usage Monitoring via the OCS | 171 |



| | | |
|----|--|-----|
| 24 | Annex R (Informative): Disabling/Re-Enabling Usage Monitoring for a PCC/ADC Rule | 172 |
| 25 | Annex S (Normative): Fixed Broadband Access | 173 |
| 26 | Annex T (Informative): How to Accumulate PCC/ADC Rule Usage in Multiple Monitoring Groups | 174 |
| 27 | Annex U (Normative): Policy and Charging Control in the Downlink Direction for Traffic Marked with DSCP by the TDF | 175 |
| 28 | Annex V (Informative): Policy Control for Remote UEs behind a ProSe UE-to-Network Relay UE | 178 |
| 29 | Annex W (Informative): Void | 179 |
| 30 | Annex X (Informative): Encrypted Traffic Detection by Using Domain Name Matching | 180 |
| 31 | Annex Y (Informative): Change History | 181 |
| 32 | Reference List | 182 |





1 Introduction

This document describes to what extent SAPC implementation of Policy Charging Rule Function (PCRF) role conforms with the 3GPP Technical Specification (TS) 23. 203 V14.5.0 (2017-09) standard with the exemptions or additions stated in this document.



2 General Considerations

This document is structured following the chapters of the 3GPP Technical Specification 23.203 V14.5.0 (2017-09) .

Please note that the compliance statements for the specifications referenced in the TS are not in the scope of this SoC.

The following terms explain the columns in the fill-in tables in the document:

| | |
|----------------------------|--|
| Qualifier | Defines whether the implementation of a certain entity is Mandatory (M), Optional (Op) or Conditional (C). |
| Compliance | Defines whether the implementation of a certain entity is Compliant by the system. |
| Comment | It may contain additional information. |
| No requirement (NR) | The TS statement contains general information for the understanding of other statements not applicable to the SAPC (the statements may be applicable for other nodes). |

One of the following statements (with the associated interpretation) is given to each of the requirements of the Technical Specification:

| | |
|---------------------------------|--|
| Not compliant (NC) | The TS statement is not fulfilled. |
| Compliant (C) | All of the TS statements are fulfilled. |
| Partially compliant (PC) | Not completely all of the TS statements are fulfilled, the exceptions are described. |

In this context, 'is/shall/will' statements are considered as mandatory, 'may' statements are considered as optional, and 'can' statements are considered as conditional.



3 Scope, References and Abbreviations

3.1 Scope

No requirement

3.2 References

No requirement

3.3 Definitions and Abbreviations

3.3.1 Definitions

No requirement

3.3.2 Abbreviations

No requirement

4 High Level Requirements

No requirement

4.1 General Requirements

Table 1 General Requirements

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|--|
| It shall be possible for the PCC architecture to base decisions upon subscription information. | M | C | |
| It shall be possible to apply policy and charging control to any kind of 3GPP IP CAN and any non-3GPP accesses connected via EPC complying with TS 23.402 [18]. Applicability of PCC to other IP CANs is not restricted. However, it shall be possible for the PCC architecture to base decisions upon the type of IP CAN used (e.g. GPRS, etc.). | M | PC | The SAPC does not support Gxc interface nor Gxa interface. |
| The policy and charging control shall be possible in the roaming and local breakout scenarios defined in TS 23.401 [17] and TS 23.402 [18]. | M | PC | The SAPC does not support local breakout scenarios (S9 interface is not supported) |
| The PCC architecture shall discard packets that don't match any service data flow template 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 for the passage and charging for packets that do not match any service data flow template of any other active PCC rules. | M | C | |
| The PCC architecture shall allow the charging control to be applied on a per service data flow and on | M | C | |



| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|--|
| a per application basis, independent of the policy control. | | | |
| The PCC architecture shall have a binding method that allows the unique association between service data flows and their IP CAN bearer. | M | C | |
| A single service data flow detection shall suffice for the purpose of both policy control and flow based charging. | M | C | |
| A PCC rule may be predefined or dynamically provisioned at establishment and during the lifetime of an IP CAN session. The latter is referred to as a dynamic PCC rule. | M | C | |
| The number of real-time PCC interactions shall be minimized although not significantly increasing the overall system reaction time. This requires optimized interfaces between the PCC nodes. | M | C | |
| 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. | M | C | |
| PCC shall be enabled on a per PDN basis (represented by an access point and the configured range of IP addresses) at the PCEF. It shall be possible for the operator to configure the PCC architecture to perform charging control, policy control or both for a PDN access. | M | C | |
| PCC shall support roaming users. | M | PC | The SAPC does not support local breakout scenarios (S9 interface is not supported) |
| The PCC architecture shall allow the resolution of conflicts which would otherwise cause a | M | C | |

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---|
| subscriber's Subscribed Guaranteed Bandwidth QoS to be exceeded. | | | |
| The PCC architecture shall support topology hiding. | M | C | The Diameter peers connected to the SAPC must belong to the possible Destination Realms of the receiver Destination Host. |
| It should be possible to use PCC architecture for handling IMS-based emergency service. | M | C | |
| It shall be possible with the PCC architecture, 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. | M | C | |
| It shall be possible for the PCC architecture to provide application awareness even when there is no explicit service level signalling. | M | NC | |
| The PCC architecture shall support making policy decisions based on subscriber spending limits. | M | C | |
| The PCC architecture shall support making policy decisions based on RAN user plane congestion status. | M | NC | |
| The PCC architecture shall support making policy decisions for multi-access IP flow mobility solution described in TS 23.161 [43]. | M | NC | |
| The PCC architecture shall support making policy decisions for (S)Gi-LAN traffic steering. | M | NC | |



4.2 Charging Related Requirements

No requirement

4.2.1 General

Table 2 General

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| In order to allow for charging control on service data flow, the information in the PCC rule identifies the service data flow and specifies the parameters for charging control. The PCC rule information may depend on subscription data. | M | C | |
| In order to allow for charging control on detected application traffic identified by ADC Rule for the TDF, the information in the ADC rule contains the application identifier and specifies the parameters for charging control. The ADC rule information may depend on subscription data. | M | PC | |
| For the purpose of charging correlation between application level (e.g. IMS) and service data flow level, applicable charging identifiers shall be passed along within the PCC architecture, if such identifiers are available. | M | C | |
| For the purpose of charging correlation between service data flow level and application level (e.g. IMS) as well as on-line charging support at the application level, applicable charging identifiers and IP CAN type identifiers shall be passed from the PCRF to the AF, if such identifiers are available. | M | NC | |

4.2.2 Charging Models

4.2.2a Charging Requirements

Table 3 Charging Requirements

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---|
| It shall be possible to indicate to the PCEF or TDF that interactions with the charging systems are not required for a PCC or ADC rule, i.e. to perform neither accounting nor credit control for this the service data flow/detected application traffic, and then no offline charging information is generated. | M | PC | Only predefined ADC rules are supported |

4.2.3 Examples of Service Data Flow Charging

No requirement

4.3 Policy Control Requirements

No requirement

4.3.1 General

No requirement

4.3.2 Gating Control

No requirement

4.3.3 QoS Control

No requirement

4.3.3.1 QoS Control at Service Data Flow Level

Table 4 QoS Control at Service Data Flow Level

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| It shall be possible to apply QoS control on a per service data flow basis in the PCEF. QoS control per service data flow allows the PCC architecture to provide the PCEF | M | C | |



| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| 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 PCRF internal policies to derive the authorized QoS to be enforced for a service data flow | | | |

4.3.3.2

QoS Control at IP CAN Bearer Level

Table 5 QoS Control at IP CAN Bearer Level

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---|
| It shall be possible for the PCC architecture to support control of QoS reservation procedures (UE-initiated or network-initiated) for IP CANs that support such procedures for its IP CAN bearers in the PCEF or the BBERF, if applicable. 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 IP CAN bearer and on criteria such as the QoS subscription information, service based policies, and/or pre-defined PCRF internal policies. Details of QoS reservation procedures are IP CAN specific and therefore, the control of these procedures is described in Annex A and Annex D. | M | PC | UE-Init procedures only supported for the default bearer. |
| It shall be possible for the PCC architecture to support control of QoS for the packet traffic of IP CANs. | M | C | |
| The PCC architecture shall be able to provide policy control in the presence of NAT devices. This may be accomplished by | M | C | |

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---|
| providing appropriate address and port information to the PCRF. | | | |
| The enforcement of the control for QoS reservation procedures for an IP CAN bearer shall allow for a downgrading or an upgrading of the requested QoS as part of a UE-initiated IP CAN bearer establishment and modification. The PCC architecture shall be able to provide a mechanism to initiate IP CAN bearer establishment and modification (for IP CANs that support such procedures for its bearers) as part of the QoS control. | M | PC | UE-Init procedures only supported for the default bearer. |
| The IP CAN shall prevent cyclic QoS upgrade attempts due to failed QoS upgrades. NOTE: These measures are IP CAN specific. | M | C | |
| The PCC architecture shall be able to handle IP CAN bearers that require a guaranteed bitrate (GBR bearers) and IP CAN bearers for which there is no guaranteed bitrate (non-GBR bearers). | M | C | |

4.3.3.3 QoS Conflict Handling

Table 6 QoS Conflict Handling

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| It shall be possible for the PCC architecture to support conflict resolution in the PCRF when the authorized bandwidth associated with multiple PCC rules exceeds the Subscribed Guaranteed bandwidth QoS. | M | C | |



4.3.3.4

QoS Control at APN Level

Table 7 QoS Control at APN Level

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|--|
| It shall be possible for the PCRF to authorize the APN-AMBR to be enforced by the PCEF as defined in 3GPP TS 23.401 [17]. The APN-AMBR applies to all IP CAN sessions of a UE to the same APN and has separate values for the uplink and downlink direction. | M | C | |
| It shall be possible for the PCRF to provide the authorized APN-AMBR values unconditionally or conditionally, i.e. per IP-CAN type and/or RAT type. | M | PC | The SAPC does not support the authorized APN-AMBR values conditionally |
| It shall be possible for the PCRF to request a change of the unconditional or conditional authorized APN-AMBR value(s) at a specific point in time. | M | NC | |

4.3.4

Subscriber Spending Limits

Table 8 Subscriber Spending Limits

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| It shall be possible to enforce policies based on subscriber spending limits as per TS 22.115 [27]. | M | C | |
| The PCRF shall request information regarding the subscriber's spending from the OCS, to be used as input for dynamic policy decisions for the subscriber, using subscriptions to spending limit reports. | M | C | |

4.4 Usage Monitoring Control

Table 9 Usage Monitoring Control

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|--|
| It shall be possible to apply usage monitoring for the accumulated usage of network resources on a per IP-CAN session and user basis. This capability is required for enforcing dynamic policy decisions based on the total network usage in real-time. | M | C | |
| The PCRF that use usage monitoring for making dynamic policy decisions shall set and send the applicable thresholds to the PCEF or TDF for monitoring. The usage monitoring thresholds shall be based either on time, or volume. The PCRF may send both thresholds to the PCEF or TDF. The PCEF or TDF shall notify the PCRF when a threshold is reached and report the accumulated usage since the last report for usage monitoring. | M | PC | Only application detection and control interactions with TDF are supported |
| The usage monitoring capability shall be possible for an individual or a group of service data flow(s), or for all traffic of an IP-CAN session in the PCEF | M | C | |
| When usage monitoring for all traffic of an IP-CAN 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 IP-CAN session. | M | NC | |
| 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. | M | PC | Usage monitoring only supported for the predefined PCC rules |



| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|-----------------------------------|
| The usage monitoring capability shall be possible for an individual or a group of detected application(s) traffic or all detected traffic belonging to a specific TDF session. | M | NC | |
| When usage monitoring for all traffic of a TDF session is enabled, it shall be possible to exclude an individual application or a group of detected application(s) from the usage monitoring for all traffic belonging to this TDF session if usage monitoring. | M | NC | |
| It shall be possible to activate usage monitoring both to predefined ADC rules and to dynamic ADC rules, including rules with deferred activation and/or deactivation times while those rules are active. | M | NC | |
| If service data flow(s)/ application(s) need to be excluded from IP-CAN/TDF session level usage monitoring and IP CAN /TDF session level usage monitoring is enabled, the PCRF shall be able to provide the an indication of exclusion from session level monitoring associated with the respective PCC/ADC rule(s). | M | NC | |
| It shall be possible to apply different usage monitoring depending on the access used to carry a Service Data Flow. This applies also to a PDN connection supporting NBIFOM. | M | PC | The SAPC does not support NBIFOM. |

4.5 Application Detection and Control

Table 10 Application Detection and Control

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---|
| The application detection and control feature comprise the request to detect the specified application traffic, report to the PCRF on the start or stop of application traffic and to apply the specified enforcement and charging actions. The application detection and control shall be implemented either by the TDF or by the PCEF enhanced with ADC. | M | C | |
| Solicited application reporting: The PCRF shall instruct the TDF, or the PCEF enhanced with ADC, on which applications to detect and whether to report start or stop event to the PCRF by activating the appropriate ADC/PCC rules in the TDF/PCEF enhanced with ADC. | M | C | |
| Reporting notifications of start and stop of application detection to the PCRF may be muted, in addition, per specific ADC/PCC rule. The PCRF may, in a dynamic ADC/PCC rule, instruct the TDF or PCEF enhanced with ADC, what enforcement actions to apply to the detected application traffic. The PCRF may activate application detection only if user profile configuration allows this. | Op | PC | Only predefined ADC rules are supported |
| Unsolicited application reporting: The TDF is pre-configured on which applications to detect and report. The PCRF may enable enforcement in the PCEF based on the service data flow description provided to PCRF by the TDF. It is assumed that user profile configuration indicating whether application detection and control can be enabled is not required. | Op | NC | |



| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|--|
| The report to the PCRF shall include the same information for solicited and unsolicited application reporting that is whether the report is for start or stop, the detected application identifier and, if deducible, the service data flow descriptions for the detected application traffic. | M | PC | Unsolicited application reporting is not supported |
| For the application types, where service data flow descriptions are deducible, the Start and Stop of the application may be indicated multiple times, including the application instance identifier to inform the PCRF about the service data flow descriptions belonging to that application instance. The application instance identifier is dynamically assigned by the TDF or by the PCEF enhanced with ADC in order to allow correlation of application Start and Stop events to the specific service data flow description. | Op | C | |
| NOTE 2: Redirection may not be possible for all types of detected application traffic (e.g. this may only be performed on specific HTTP based flows). | Op | C | |
| - When the TDF provides to the PCRF the service data flow description, the PCRF may take control over the actions resulting of application detection, by applying the charging and policy enforcement per service data flow as defined in this document, or the TDF may perform charging, gating, redirection and bandwidth limitation as described above. It is the PCRF's responsibility to coordinate the PCC rules with ADC rules in order to ensure consistent service delivery. | Op | PC | Only predefined ADC are supported, PCRF is not aware about whether TDF is applying charging or enforcement per service data flow |

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|--|
| Usage monitoring as described in clause 4.4 may be activated in conjunction with application detection and control. The usage monitoring functionality is only applicable to the solicited application reporting model. | M | PC | Usage monitoring not supported in TDF interactions |
| For TDF, ADC rule based charging is applicable. ADC rule based charging, as described in clause 4.2.2a, may be activated in conjunction with application detection and control. The charging functionality is only applicable to the solicited application reporting model. | M | PC | Only predefined ADC rules are supported |
| The ADC rules are used to determine the online and offline characteristics for charging. For offline charging, usage reporting over the Gzn interface shall be used. For online charging, credit management and reporting over the Gyn interface shall be used. The PCEF is in this case not used for charging and enforcement (based on active PCC rules and APN-AMBR configuration), but shall still be performing bearer binding based on the active PCC rules. In order to avoid having traffic that is charged in the TDF later discarded by the policing function in the PCEF, the assumption is that no GBR bearers are required when TDF is the charging and policy enforcement point. In addition, the DL APN-AMBR in PCEF shall be configured with such high values that it does not result in discarded packets. | M | C | |
| NOTE 3: An example of applicability is IMS APN, which would require dynamic PCC rules, would be configured such that PCEF based charging and enforcement is employed, but for regular internet access APN, the | M | C | |



| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| network would be configured such that the TDF performs both charging and enforcement. | | | |
| NOTE 4: An operator may also apply this solution with both PCEF and TDF performing enforcement and charging for a single IP-CAN session as long as the network is configured in such a way that the traffic charged and enforced in the PCEF does not overlap with the traffic charged and enforced by the TDF. | Op | C | |

4.6 RAN User Plane Congestion Detection, Reporting and Mitigation

Not compliant

4.7 Support for Service Capability Exposure

Not compliant

4.8 Traffic Steering Control

Not compliant

4.9 Management of Packet Flow Descriptions in the PCEF/TDF Using the PFDF

Not compliant

5 Architecture Model and Reference Points

5.1 Reference Architecture

Partially compliant

Only Gx, Sy, Sd and Rx interface are implemented.

Note: Note that the SAPC product, the SPR database is integrated by default with the PCRF.

5.2 Reference Points

No requirement

5.2.1 Rx Reference Point

Partially compliant

Not all subscriptions to notifications on IP CAN bearer level events are supported by the SAPC.

Sponsored data connectivity is not supported by the SAPC.

5.2.2 Gx Reference Point

Table 11 Gx Reference Point

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| The Gx reference point resides between the PCEF and the PCRF. | M | C | |
| The Gx reference point enables the PCRF to have dynamic control over the PCC behaviour at a PCEF. The Gx reference point enables the signalling of PCC decision, which governs the PCC behaviour, and it supports the following functions: - Establishment of Gx session (corresponding to an IP CAN session) by the PCEF; | M | C | |



| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|--|
| - Request for PCC decision from the PCEF to the PCRF; | | | |
| - Provision of IP flow mobility routing information from PCEF to PCRF; this applies only when IP flow mobility as defined in TS 23.261 [23] is supported; | M | NC | IP flow mobility is not supported by the SAPC. |
| - Reporting of the start and the stop of detected applications and transfer of service data flow descriptions and application instance identifiers for detected applications from the PCEF to the PCRF; | M | C | |
| - Provision of PCC decision from the PCRF to the PCEF; | M | C | |
| - Reporting of the accumulated usage of network resources on a per IP-CAN session basis from the PCEF to the PCRF; | M | C | |
| - Delivery of IP CAN- session specific parameters from the PCEF to the PCRF, if Gxx is deployed, from the PCRF to the PCEF per corresponding request; | M | NC | |
| - Negotiation of IP CAN bearer establishment mode (UE-only or UE/NW); | M | C | |
| - Termination of Gx session (corresponding to an IP CAN session) by the PCEF or the PCRF. | M | C | |
| Note: The PCRF decision to terminate a Gx session is based on operator policies. It should only occur in rare situations (e.g. the removal of a UE subscription) to avoid service interruption due to the termination of the IP CAN session. | M | C | |

5.2.3

Reference Points to Subscriber Databases

No requirement

5.2.3.1 Sp Reference Point

Table 12 Sp Reference Point

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| The Sp reference point lies between the SPR and the PCRF. | M | C | |
| The Sp reference point allows the PCRF to request subscription information related to the IP CAN transport level policies from the SPR based on a subscriber ID, a PDN identifier and possible further IP CAN session attributes, see Annex A and Annex D. For example, the subscriber ID can be IMSI. The reference point allows the SPR to notify the PCRF when the subscription information has been changed if the PCRF has requested such notifications. The SPR shall stop sending the updated subscription information when a cancellation notification request has been received from the PCRF. | M | C | |

5.2.3.2 Ud Reference Point

Table 13 Ud Reference Point

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| The Ud reference point resides between the UDR and the PCRF, acting as an Application Frontend as defined in TS 23.335 [25]. It is used by the PCRF to access PCC related subscription data when stored in the UDR. | M | NC | |

5.2.4 Gy Reference Point

No requirement



5.2.5 Gz Reference Point

No requirement

5.2.6 S9 Reference Point

Not compliant

5.2.7 Gxx Reference Point

Not compliant

5.2.8 Sd Reference Point

Table 14 Sd Reference Point

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|--|
| The Sd reference point resides between the PCRF and the TDF. | M | C | |
| The Sd reference point enables a PCRF to have dynamic control over the application detection and control behaviour at a TDF. | M | C | |
| The Sd reference point enables the signalling of ADC decision, which governs the ADC behaviour, and it supports the following functions: | M | C | |
| 1. Establishment of Sd session between the PCRF and the TDF; | | | |
| 2. Termination of Sd session between the PCRF and the TDF; | M | C | |
| 3. Provision of ADC decision from the PCRF for the purpose of application's traffic detection, enforcement and charging at the TDF; | M | C | |
| 4. Request for ADC decision from the TDF to the PCRF; | M | PC | Only APPLICATION_START and APPLICATION_STOP Event-Triggers are supported |

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|--|
| 5. Reporting of the start and the stop of a detected applications and transfer of service data flow descriptions and application instance identifiers for detected applications from the TDF to the PCRF; | M | C | |
| 6. Reporting of the accumulated usage of network resources on a per TDF session basis from the TDF to the PCRF; | M | NC | Usage monitoring not supported in TDF interactions |
| 7. Request and delivery of IP CAN session specific parameters between the PCRF and the TDF. | M | PC | Location information is not delivered to the TDF |
| When Sd is used for traffic steering control only, then the following function is supported: - Provision of ADC Rules from the PCRF for the purpose of application's traffic detection and traffic steering control. | M | PC | Only predefined ADC rules are supported |

5.2.9

Sy Reference Point

Table 15 Sy Reference Point

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------------------------------|
| The Sy reference point resides between the PCRF and the OCS. | M | C | |
| The Sy reference point enables transfer of policy counter status information relating to subscriber spending from OCS to PCRF and supports the following functions: - Request for reporting of policy counter status information from PCRF to OCS and subscribe to or unsubscribe from spending limit reports (i.e. notifications of policy counter status changes). | M | PC | UnSubscription is not supported |



| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| - Report of policy counter status information upon a PCRF request from OCS to PCRF. | M | C | |
| - Notification of spending limit reports from OCS to PCRF. | M | C | |
| - Cancellation of spending limit reporting from PCRF to OCS. | M | C | |

5.2.10 Gyn Reference Point

No requirement

5.2.11 Gzn Reference Point

No requirement

5.2.12 Np Reference Point

Not compliant

5.2.13 Nt Reference Point

Not compliant

5.2.14 St Reference Point

Not compliant

5.2.15 Nu Reference Point

Not compliant

5.2.16 Gw Reference Point

Not compliant

5.2.17 Gwn Reference Point

Not compliant

6 Functional Description

No requirement

6.1 Overall Description

No requirement

6.1.0 General

Table 16 General

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| The PCC architecture works on a service data flow level. The PCC architecture provides the functions for policy and charging control as well as event reporting for service data flows. | M | C | |

6.1.1 Binding Mechanism

No requirement

6.1.1.1 General

No requirement

Table 17 General

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| For service data flows belonging to AF sessions, the binding mechanism shall also associate the AF session information with the IP CAN bearer that is selected to carry the service data flow. | M | C | |
| 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 and QoS rules, if applicable (e.g. one rule per media component of an IMS session). Alternatively, a rule | M | C | |



| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| could comprise multiple AF sessions. | | | |
| NOTE 2: The PCRF may authorize dynamic PCC rules for service data flows without a corresponding AF session. Such PCC rules may be statically configured at the PCRF or dynamically filled with the UE provided traffic mapping information. | M | C | |

6.1.1.2

Session Binding

Table 18 Session Binding

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|--|
| <p>The PCRF shall perform the session binding, which shall take the following IP CAN parameters into account:</p> <ul style="list-style-type: none"> a) The UE IPv4 address and/or IPv6 network prefix b) The UE identity (of the same kind), if present. <p>NOTE 1: In case the UE identity in the IP CAN and the application level identity for the user are of different kinds, the PCRF needs to maintain, or have access to, the mapping between the identities. Such mapping is not subject to specification within this TS.</p> <ul style="list-style-type: none"> c) The information about the packet data network (PDN) the user is accessing, if present. | M | C | The SAPC uses the UE IP address, UE Identity (if present) and the APN (if present) to perform the session binding. |
| For an IP-CAN session to the dedicated APN for UE-to-Network Relay connectivity (as defined in TS 23.303 [44]) and using IPv6 prefix delegation (i.e. the assigned IPv6 network prefix is shorter than 64) the PCRF shall perform session binding based on the IPv6 network prefix only. A | M | NC | |

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| <p>successful session binding occurs whenever a longer prefix received from an AF matches the prefix value of the IP-CAN session. PCRF shall not use the UE identity for session binding for this IP-CAN session.</p> <p>NOTE 2: For UE-to-Network Relay connectivity, the UE identity that the PCEF has provided (i.e. UE-to-Network Relay UE Identity) and a UE identity provided by the AF (i.e. Remote UE Identity) can be different, while the binding with the IP-CAN session is valid.</p> <p>NOTE 3: In this Release of the specification the support for policy control of Remote UEs behind a ProSe UE-Network Relay using IPv4 is not available.</p> | | | |
| The PCRF shall identify the PCC rules affected by the AF session information, including new rules to be installed and existing rules to be modified or removed. | M | C | |

6.1.1.3

PCC Rule Authorization and QoS Rule Generation

Table 19 PCC Rule Authorization and QoS Rule Generation

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| The PCRF shall perform the PCC rule authorization for complete dynamic PCC rules belonging to AF sessions that have been selected in step 1, as described in clause 6.1.1.2, as well as for PCC rules without corresponding AF sessions. Based on AF instructions (as described in clause 6.1.5) dynamic PCC rules can be authorized even if they are not complete (e.g. due to missing service information regarding QoS or traffic filter parameters). | M | C | |



| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---|
| The PCC rule authorization depends on the IP CAN bearer establishment mode of the IP CAN session and the mode (UE or NW) of the PCC rule: | M | PC | See next items |
| - In UE/NW bearer establishment mode, the PCRF shall perform the authorization for all PCC rules that are to be handled in NW mode. | M | C | |
| - In UE/NW bearer establishment mode, for PCC rules that are to be handled in UE mode or when in UE-only bearer establishment mode, the PCRF shall first identify the PCC rules that correspond to a UE resource request and authorize only these. | M | PC | If the selected bearer control mode is UE_NW the SAPC supports UE initiated for the default bearer and NW initiated for the dedicated bearers. In UE_Only only the default bearer is supported. |
| The PCRF shall compare the traffic mapping information of the UE resource request with the service data flow filter information of the services that are allowed for the user. Each part of the traffic mapping information shall be evaluated separately in the order of their related precedence. Any matching service data flow filter leads to an authorization of the corresponding PCC rule for the UE resource request unless the PCC rule is already authorized for a more specific traffic mapping information or the PCC rule cannot be authorized for the QCI that is related to the UE resource request (the details are described in the next paragraph). Since a PCC rule can contain multiple service data flow filters it shall be ensured by the PCRF that a | M | NC | |

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| service data flow is only authorized for a single UE resource request. | | | |
| NOTE 1: For example, a PCC rule containing multiple service data flow filters that match traffic mapping information of different UE resource requests could be segmented by the PCRF according to the different matching traffic mapping information. Afterwards, the PCRF can authorize the different PCC rules individually. | M | NC | |
| The PCRF knows whether a PCC rule can be authorized for a single QCI only or a set of QCIs (based on SPR information or local configuration). If the processing of the traffic mapping information would lead to an authorization of a PCC rule, the PCRF shall also check whether the PCC rule can be authorized for the QCI that is related to the UE resource request containing the traffic mapping information. If the PCC rule cannot be authorized for this QCI, the PCRF shall reject the traffic mapping information unless otherwise stated in an access-specific Annex. | M | NC | |
| If there is any traffic mapping information not matching to any service data flow filter known to the PCRF and the UE is allowed to request for enhanced QoS for traffic not belonging to operator-controlled services, the PCRF shall authorize this traffic mapping information by adding the respective service data flow filter to a new or existing PCC. If the PCRF received an SDF filter identifier together with this traffic mapping information, the PCRF shall modify the existing PCC rule | M | NC | |



| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| if the PCC rule is authorized for a GBR QCI. | | | |
| NOTE 2: If the PCC rule is authorized for a non-GBR QCI, the PCRF may either create a new PCC rule or modify the existing PCC rule. | M | NC | |
| The PCC rule that needs to be modified can be identified by the service data flow filter the SDF filter identifier refers to. The requested QoS shall be checked against the subscription limitations for traffic not belonging to operator-controlled services. | M | NC | |
| If the PCRF needs to perform the authorization based on incomplete service information and thus cannot associate a PCC rule with a single IP CAN bearer, then the PCRF shall generate for the affected service data flow an individual PCC rule per IP CAN bearer that could carry that service data flow. Once the PCRF receives the complete service information, the PCC rule on the IP CAN bearer with the matching traffic mapping information shall be updated according to the service information. Any other PCC rule(s) previously generated for the same service data flow shall be removed by the PCRF. | M | NC | |
| NOTE 3: This is required to enable the successful activation or modification of IP CAN bearers before knowing the intended use of the IP CAN bearers to carry the service data flow(s). | M | NC | |
| For an IP CAN, where the PCRF gains no information about the uplink IP flows (i.e. the UE provided traffic mapping information contains no information about the uplink IP flows), the binding mechanism | M | NC | |

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| shall assume that, for bi-directional service data flows, both downlink and uplink packets travel on the same IP CAN bearer. | | | |
| Whenever the service data flow template or the UE provided traffic mapping information change, the existing authorizations shall be re-evaluated, i.e. the authorization procedure specified in this clause, is performed. The re-evaluation may, for a service data flow, require a new authorization for a different UE provided mapping information. | M | NC | |
| Based on PCRF configuration or AF instructions (as described in clause 6.1.5) dynamic PCC rules may have to be first authorized for the default QCI/default bearer (i.e. bearer without UE provided traffic mapping information) until a corresponding UE resource request occurs. | M | C | |
| NOTE 4: This is required to enable services that start before dedicated resources are allocated. | NR | | |
| A PCC rule for a service data flow that is a candidate for vSRVCC according to TS 23.216 [28] shall have the PS to CS session continuity indicator set. | M | NC | |
| For the authorization of a PCC rule the PCRF shall take into account the IP CAN specific restrictions and other information available to the PCRF. Each PCC rule receives a set of QoS parameters that can be supported by the IP CAN. The authorization of a PCC rule associated with an emergency service shall be supported without subscription information (e.g. information stored in the SPR). The PCRF shall apply | M | C | |



| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|--------------------------------|
| policies configured for the emergency service. | | | |
| When both a Gx and a Gxx interface exist for an IP CAN session, the PCRF shall generate QoS rules for all the authorized PCC rules in this step. The PCRF shall ensure consistency between the QoS rules and PCC rules authorized for the same service data flow when QoS rules are derived from corresponding PCC rules. | M | NC | Gxx interface is not supported |
| When flow mobility applies for the IP-CAN Session, one IP CAN session may be associated to multiple Gateway Control Sessions with separate BBERFs. In this case, the PCRF shall provision QoS rules only to the appropriate BBERF based on IP flow mobility routing rules received from the PCEF. | M | NC | |

6.1.1.4

Bearer Binding

Table 20 Bearer Binding

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|--|
| The Bearer Binding Function may also be located in the PCRF as specified in Annex A and Annex D (e.g. for GPRS running UE only IP CAN bearer establishment mode). NOTE 1: For an IP CAN, limited to a single IP CAN bearer per IP CAN session, the bearer is implicit, so finding the IP CAN session is sufficient for successful binding. | Op | PC | The SAPC bearer binding is not supported by the SAPC, only default bearer is supported for UE-Init procedures. |
| For an IP CAN which allows for multiple IP CAN bearers for each IP CAN session, the binding mechanism shall use the QoS parameters of the existing IP CAN bearers to create the bearer binding for a rule, in addition to | M | NC | The SAPC bearer binding is not supported by the SAPC, only default bearer is supported for |

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|--|
| the PCC rule and the QoS rule (if applicable) authorized in the previous step. | | | UE-Init procedures. |
| The set of QoS parameters assigned in step 2, as described in clause 6.1.1.3, to the service data flow is the main input for bearer binding. | M | NC | |
| Whenever the QoS authorization of a PCC/QoS rule changes, the existing binding shall be re-evaluated, i.e. the bearer binding procedures specified in this clause, is performed. The re-evaluation may, for a service data flow, require a new binding with another IP CAN bearer. | M | NC | The SAPC bearer binding is not supported by the SAPC, only default bearer is supported for UE-Init procedures. |

6.1.2 Reporting

Table 21 Reporting

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| For the case where the BBF is not located in the PCEF, charging information shall be reported based on the result from the service data flow detection and measurement, separately per QCI and ARP combination (used by any of the active PCC rules). In case 2a, defined in clause 7.1, charging ID is provided to the BBERF via the PCRF if charging correlation is needed. | M | NC | |

6.1.3 Credit Management

Table 22 Credit Management

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|--|
| For each charging key, the PCEF/TDF may receive credit re-authorisation trigger information from the OCS, which shall cause | M | PC | Only application detection and control |



| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|--|
| the PCEF/TDF to perform a credit re-authorisation when the event occurs. If there are events which can not be monitored in the PCEF/TDF, the PCEF/TDF shall provide the information about the required event triggers to the PCRF. If information about required event triggers is provided to the PCRF, it is an implementation option whether a successful confirmation is required from the PCRF in order for the PCEF/TDF to consider the credit (re-)authorization procedure to be successful. The credit re-authorisation trigger detection shall cause the PCEF/TDF to request re-authorisation of the credit in the OCS. It shall be possible for the OCS to instruct the PCEF/TDF to seek re-authorisation of credit in case of the events listed in table 6.1. | | | interactions with TDF are supported |
| If the PCRF set the Out of credit event trigger (see clause 6.1.4), the PCEF/TDF shall inform the PCRF about the PCC rules for which credit is no longer available together with the applied termination action. | M | PC | Only application detection and control interactions with TDF are supported |

6.1.4 Event Triggers

Table 23 Event Triggers

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|--------------------------------------|
| The Event Reporting Function (ERF) performs event trigger detection. When an event matching the event trigger occurs, the ERF shall report the occurred event to the PCRF. The Event Reporting Function is located either at the PCEF or, at the BBERF (if applicable) or, at | M | PC | BBERF interactions are not supported |

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---|
| the TDF for solicited application reporting (if applicable). | | | |
| The event triggers define the conditions when the ERF shall interact again with PCRF after an IP CAN session establishment. The event triggers that are required in procedures shall be unconditionally reported from the ERF, while the PCRF may subscribe to the remaining events. Whether an event trigger requires a subscription by the PCRF is indicated in column 4 in table 6.2 below. | M | C | |
| The PCRF subscribes to new event triggers or remove armed event triggers unsolicited at any time or upon receiving a request from the AF, an event report or rule request from the ERF (PCEF or BBERF or TDF) using the Provision of PCC Rules procedure or the Provision of QoS Rules procedure (if applicable). or the Provision of ADC Rules procedure (if applicable). | M | PC | Only subscription to APPLICATION_START and APPLICATION_STOP Event-Triggers during TDF session establishment is supported BBERF interactions are not supported. |
| PLMN change | M | C | |
| QoS change | M | C | |
| QoS change exceeding authorization | M | C | |
| Traffic mapping information change | C | NC | |
| Resource modification request | M | NC | |
| Routing information change | M | NC | |
| Change in type of IP CAN (see note 1) | M | C | |
| Loss/recovery of transmission resources | M | NC | |
| Location change (serving cell) | M | C | |
| Location change (serving area) (see note 4) | M | C | |



| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| Location change (serving CN node) (see note 5) | M | C | |
| Change of UE presence in Presence Reporting Area | M | C | |
| Out of credit | M | C | |
| Enforced PCC rule request | M | C | |
| Enforced ADC rule request | M | NC | |
| UE IP address change | M | NC | |
| Access Network Charging Correlation Information | M | NC | |
| Usage report (see note 7) | M | C | |
| Start of application traffic detection and Stop of application traffic detection (see note 8) | M | C | |
| SRVCC CS to PS handover | M | NC | |
| Access Network Information report | M | C | |
| Credit management session failure | M | NC | |
| Addition / removal of an access to a IP-CAN session | M | NC | |
| Change of availability of an Access | M | NC | |
| The PCRF determines at IP-CAN session establishment/ modification, based on local configuration, if the UE is located in an access type that supports reporting changes of UE presence in Presence Reporting Area. If the access type supports it, the PCRF may subscribe to Change of UE presence in Presence Reporting Area at any time during the life time of the IP-CAN session | M | C | |
| NOTE 2: If Presence Reporting Area reporting is not supported, the PCRF may instead activate Location change reporting at cell and/or serving area level but due to the potential increase in signalling load, it is recommended that such | M | C | |

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| reporting is only applied for a limited number of subscribers. | | | |
| The PCRF may be notified during the life time of an IP-CAN session that the UE is located in an access type where local PCRF configuration indicates that reporting changes of UE presence in Presence Reporting Area is not supported. The PCRF unsubscribes to Change of UE presence in Presence Reporting Area, if previously activated. | Op | C | |
| The QoS change event trigger shall trigger the PCRF interaction for all changes of the IP CAN bearer QoS. The QoS change exceeding authorization event trigger shall only trigger the PCRF interaction for those changes that exceed the QoS of the IP CAN bearer that has been authorized by the PCRF previously. The ERF shall check the QoS class identifier and the bandwidth. | M | C | |
| The Resource modification request event trigger shall trigger the PCRF interaction for all resource modification requests not tied to a specific IP CAN bearer received by PCEF/BBERF. The resource modification request received by PCEF/BBERF may include request for guaranteed bit rate changes for a traffic aggregate and/or the association/disassociation of a traffic aggregate with a QCI and/or a modification of a traffic aggregate. | M | NC | |
| The routing information change event trigger shall trigger the PCRF interaction for any change in how the IP flow is routed (i.e. IP flow mobility routing rules). The routing information change received by the PCEF is specified in TS 23.261. | M | NC | |



| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|--|
| The enforced PCC rule request event trigger shall trigger a PCEF interaction to request PCC rules from the PCRF for an established IP CAN session. This PCEF interaction shall take place within the Revalidation time limit set by the PCRF in the IP CAN session related policy information (clause 6.4). | M | C | |
| The enforced ADC rule request event trigger shall trigger a TDF interaction to request ADC rules from the PCRF for an established TDF session for solicited application reporting. This TDF interaction shall take place within the ADC Revalidation time limit set by the PCRF in the TDF session related policy information (clause 6.4). | M | NC | |
| The UE IP address change event trigger applies to the PCEF only and shall trigger a PCEF interaction with the PCRF in case a UE IPv4 address is allocated or released during the lifetime of the IP CAN session. | M | NC | |
| The Access Network Charging Correlation Information event shall trigger the PCEF to report the assigned access network charging identifier for the PCC rules that are accompanied with a request for this event at activation. | M | NC | |
| To activate usage monitoring, the PCRF shall set the Usage report event trigger and provide applicable usage thresholds for the Monitoring key(s) that are subject to usage monitoring in the requested node (PCEF or TDF, solicited application reporting). | M | PC | Usage monitoring not supported in TDF interactions |
| The PCRF shall not remove the Usage report event trigger while usage monitoring is still active in the PCEF/TDF. | M | PC | Usage monitoring not supported in |

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|--|
| | | | TDF interactions |
| If the Usage report event trigger is set and the volume or the time thresholds, earlier provided by the PCRF, are reached, the PCEF shall report this event to the PCRF. | M | C | |
| If both volume and time thresholds were provided and the thresholds, for one of the measurements, are reached, the PCEF or TDF shall report this event to the PCRF and the accumulated usage since last report shall be reported for both measurements. | M | PC | Usage monitoring not supported in TDF interactions |
| The SRVCC CS to PS handover event trigger shall trigger a PCEF interaction with the PCRF to inform that a CS to PS handover procedure has been detected. The PCRF shall ensure, as specified in TS 23.216 [28], to allow voice media over the default bearer during the course of the CS to PS SRVCC procedure. | M | NC | |
| The PCRF 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 ERF. | M | C | |
| If the Access Network Information report parameter for the User Location Report is set and the user location (i.e. cell) is not available to the ERF, the ERF shall provide the serving PLMN identifier to the PCRF which shall forward it to the AF. | M | C | |
| The Credit management session failure event trigger shall trigger a PCEF or TDF interaction with the PCRF to inform about a credit management session failure and to indicate the failure reason, and the affected PCC/ADC rules. | M | NC | |



| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| NOTE 5: As a result, the PCRF may decide about e.g. TDF session termination, IP-CAN session termination (via PCC rule removal), perform gating of services in the PCEF/TDF, switch to offline charging, rating group change, etc. | | | |

6.1.5

Policy Control

Table 24 Policy Control

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---|
| <p>Policy control comprises functionalities for:</p> <ul style="list-style-type: none"> - Binding, i.e. the generation of an association between a service data flow and the IP CAN bearer transporting that service data flow; - Gating control, i.e. the blocking or allowing of packets, belonging to a service data flow, to pass through to the desired endpoint; - Event reporting, i.e. the notification of and reaction to application events to trigger new behaviour in the user plane as well as the reporting of events related to the resources in the GW(PCEF); - QoS control, i.e. the authorisation and enforcement of the maximum QoS that is authorised for a service data flow, an Application identified by application identifier or an IP CAN bearer. - Redirection, i.e. the steering of packets, belonging to an application defined by the application identifier to the specified redirection address; | M | PC | UE Init mode for dedicated bearers is not supported |

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---|
| - IP CAN bearer establishment for IP CANs that support network initiated procedures for IP CAN bearer establishment. | | | |
| In case of an aggregation of multiple service data flows (e.g. for GPRS a PDP context), the combination of the authorised QoS information of the individual service data flows is provided as the authorised QoS for this aggregate. | M | C | |
| The enforcement of the authorized QoS of the IP CAN bearer may lead to a downgrading or upgrading of the requested bearer QoS by the GW(PCEF) as part of a UE-initiated IP CAN bearer establishment or modification. Alternatively, the enforcement of the authorised QoS may, depending on operator policy and network capabilities, lead to network initiated IP CAN bearer establishment or modification. If the PCRF provides authorized QoS for both, the IP CAN bearer and PCC rule(s), the enforcement of authorized QoS of the individual PCC rules shall take place first. | M | PC | UE Init procedures for dedicated bearers is not supported |
| QoS authorization information may be dynamically provisioned by the PCRF or, if the conditions mentioned in clause 6.3.1 apply, it can be a pre-defined PCC rule in the PCEF. In case the PCRF provides PCC rules dynamically, authorised QoS information for the IP CAN bearer (combined QoS) may be provided. For a predefined PCC rules within the PCEF the authorized QoS information shall take affect when the PCC rule is activated. The PCEF shall combine the different sets of authorized QoS information, i.e. the information | M | C | |



| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---|
| received from the PCRF and the information corresponding to the predefined PCC rules. The PCRF shall know the authorized QoS information of the predefined PCC rules and shall take this information into account when activating them. This ensures that the combined authorized QoS of a set of PCC rules that are activated by the PCRF is within the limitations given by the subscription and operator policies regardless of whether these PCC rules are dynamically provided, predefined or both. | | | |
| For policy control, the AF interacts with the PCRF and the PCRF interacts with the PCEF as instructed by the AF. For certain events related to policy control, the AF shall be able to give instructions to the PCRF to act on its own, i.e. based on the service information currently available. The following events are subject to instructions from the AF: | M | PC | See steps below |
| <p>- The authorization of the service based on incomplete service information;</p> <p>NOTE 1: The QoS authorization based on incomplete service information is required for e.g. IMS session setup scenarios with available resources on originating side and a need for resource reservation on terminating side.</p> | M | C | |
| - The immediate authorization of the service; | M | C | |
| - The gate control (i.e. whether there is a common gate handling per AF session or an individual gate handling per AF session component required); | M | C | |
| - The forwarding of IP CAN bearer level information or events; | M | PC | See Rx interface description document for |

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---|
| <ul style="list-style-type: none"> - Type of IP CAN (e.g. GPRS,etc.); - Transmission resource status (established/released/lost); - Access Network Charging Correlation Information; - Credit denied. <p>NOTE 2: The credit denied information is only relevant for AFs not performing service charging.</p> | | | the list of supported IP-CAN events (Specific-Action AVP) |

6.1.6 Service (Data Flow) Prioritization and Conflict Handling

Not compliant

Note that normative PCRF requirements for conflict handling are not defined. Alternative procedures may use a combination of pre-emption priority and AF provided priority indicator.

6.1.7 Standardized QoS Characteristics

No requirement

6.1.7.1 General

Table 25 General

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| <p>The service level (i.e., per SDF or per SDF aggregate) QoS parameters are QCI, ARP, GBR, and MBR.</p> <p>Each Service Data Flow (SDF) is associated with one and only one QoS Class Identifier (QCI). For the same IP CAN session multiple SDFs with the same QCI and ARP can be treated as a single traffic aggregate which is referred to as an SDF aggregate. An SDF is a special case of an SDF aggregate. The QCI is scalar that is used as a reference to node specific parameters that control packet</p> | M | C | |



| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| forwarding treatment (e.g. scheduling weights, admission thresholds, queue management thresholds, link layer protocol configuration, etc.) and that have been pre-configured by the operator owning the node (e.g. eNodeB). | | | |

6.1.7.2 Standardized QCI Characteristics

No requirement

6.1.7.3 Allocation and Retention Priority Characteristics

No requirement

6.1.8 Termination Action

No requirement

6.1.9 Handling of Packet Filters Provided to the UE by PCEF/BBERF

Not compliant

It is an optional feature in PCRF.

6.1.10 IMS Emergency Session Support

No requirement

6.1.10.1 Architecture Model and Reference Points

No requirement

6.1.10.2 PCC Rule Authorization and QoS Rule Generation

Table 26 IMS Emergency Session Support - PCC Rule Authorization and QoS Rule Generation

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| The PCC Rule Authorization and QoS Rule generation function selects QoS parameters that | M | C | |

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| allow prioritization of IMS Emergency sessions. If an IMS Emergency session is prioritized the QoS parameters shall contain an ARP value that is reserved for intra-operator use of IMS Emergency. | | | |

6.1.10.3 Functional Entities

No requirement

6.1.10.3.1 PCRF

Table 27 IMS Emergency Session Support - PCRF

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| The PCRF shall determine based on the PDN-id if an IP-CAN Session concerns an IMS emergency session. | M | C | |
| For an IP-CAN session serving an IMS emergency session, the PCRF makes authorization and policy decisions that restricts the traffic to emergency destinations, IMS signalling and the traffic to retrieve user location information (in the user plane) for emergency services. An IP-CAN session serving an IMS emergency session shall not serve any other service and shall not be converted to/from any IP-CAN session serving other services. | M | C | |
| If the UE IP address belongs to an emergency APN, the PCRF does not perform subscription check; instead it utilizes the locally configured operator policies to make authorization and policy decisions. | M | C | |
| For IMS, it shall be possible for the PCRF to verify that the IMS service information is associated with a UE IP address belonging to an emergency APN. If the IMS | M | C | |



| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| service information does not contain an emergency related indication and the UE IP address is associated with an emergency APN, the PCRF 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 [21]. | | | |
| <p>The PCRF performs according to existing procedure:</p> <ul style="list-style-type: none"> - If IMS service information containing an emergency related indication is received from the P-CSCF with an UE IP address associated to an Emergency APN, the PCRF initiates an IP-CAN session Modification Request for the IP-CAN session serving the IMS session to the PCEF to provide PCC Rule(s) that authorize media flow(s). - At reception of an indication that the IMS emergency session is released from the P-CSCF, the PCRF removes the PCC rule(s) for that IMS session with an IP-CAN session Modification Request. | M | C | |
| In addition, upon Rx session establishment the PCRF shall provide the IMEI(SV) (if available) and the EPC-level subscriber identifiers (IMSI, MSISDN) (if available), received from the PCEF at IP-CAN session establishment, if so requested by the P-CSCF. | M | NC | |

- 6.1.10.3.2 PCEF
- No requirement
- 6.1.10.3.3 P-CSCF
- No requirement

6.1.10.4

PCC Procedures and Flows

Table 28 IMS Emergency Session Support - PCC Rule Procedures and Flows

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| At Indication of IP-CAN Session Establishment that includes a PDN-id that identifies an Emergency APN the PCRF ignores subscription information from the SPR. The PCRF uses locally configured operator policies to make authorization and policy decisions. | M | C | |
| At Indication of IP-CAN Session Establishment and Gateway Control Session Establishment, the user identity (e.g. IMSI) may not be available, or can not be authenticated. In this case, the IMEI shall be used to identify the UE. | M | C | |
| An IP-CAN session for an emergency service shall be restricted to the destination address(es) associated with the emergency service only. | M | C | |

6.1.11

Multimedia Priority Service Support

6.1.11.1

Architecture model and Reference points

Table 29 Architecture model and Reference points

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---|
| Subscription data for MPS is provided to PCC through the Sp reference point. | M | C | |
| To support MPS service, the PCRF shall subscribe to changes in the MPS subscription data for Priority EPS Bearer Service. | M | C | The SAPC does not request notifications from the SPR. They are by default always activated. |



| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| Dynamic invocation for MPS is provided from an AF, using the Priority indicator, over Rx. | M | C | |

6.1.11.2

PCC rule authorization and QoS rule generation

Table 30 PCC rule authorization and QoS rule generation

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| For MPS service, the PCRF shall generate the corresponding PCC/QoS rule(s) with the ARP/QCI parameters as appropriate for the prioritized service. | M | C | |
| For non-MPS service, the PCRF shall generate the corresponding PCC/QoS rule(s) as per normal procedures, without consideration whether the MPS Priority EPS Bearer Service is active or not, but upgrade the ARP/QCI values suitable for MPS when the Priority EPS Bearer Service is invoked. | M | C | |
| <p>When the priority EPS Bearer Service is revoked, the PCRF shall change ARP/QCI values modified for Priority EPS bearer service to an appropriate value according to PCRF decision.</p> <p>NOTE 1: This ensures that services using dedicated bearers are not terminated because of a default bearer with a lower ARP priority level or disabled ARP pre-emption capability being dropped during mobility events.</p> <p>NOTE 2: This PCRF capability does not cover interactions with services other than MPS services.</p> | M | C | |

6.1.11.3

Priority EPS Bearer Service

Table 31 Priority EPS Bearer Service

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| The PCRF shall, at the activation of the Priority EPS Bearer Service: - modify the ARP of the default bearer as appropriate for the Priority EPS Bearer Service under consideration of the requirement described in clause 6.1.11.2; and | M | C | |
| - if modification of the QCI of the default bearer is required, modify the QCI of the default bearer as appropriate for the Priority EPS Bearer Service; and | M | C | |
| - modify the ARP of PCC/QoS Rules installed before the activation of the Priority EPS Bearer Service to the ARP as appropriate for the Priority EPS Bearer Service under consideration of the requirement described in clause 6.1.11.2; and | M | C | |
| - if modification of the QCI of the PCC/QoS Rules is required, modify the QCI of the PCC/QoS Rules installed before the activation of the Priority EPS Bearer Service to the QCI as appropriate for the Priority EPS Bearer Service. | M | C | |
| The PCRF shall, at the deactivation of the Priority EPS Bearer Service: - modify the ARP of the default bearer to an appropriate value according to PCRF decision under consideration of the requirement described in clause 6.1.11.2; and | M | C | |
| - if modification of the QCI of the default bearer is required, modify the QCI of the default bearer to an appropriate value according to PCRF decision; and | M | C | |



| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| for PCC/QoS rules modified due to the activation of Priority EPS bearer service: - modify the ARP to an appropriate value according to PCRF decision under consideration of the requirement described in clause 6.1.11.2; and | M | C | |
| - if modification of the QCI of PCC/QoS Rules is required, modify the QCI to an appropriate value according to PCRF decision. | M | C | |

6.1.11.4 Bearer priority for IMS Multimedia Priority Services

Table 32 Bearer priority for IMS Multimedia Priority Services

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| At reception of the indication that the IMS Signalling Priority is set for the IP-CAN Session or at reception of service authorization from the P-CSCF (AF) including an MPS session indication and the service priority level the PCRF shall under consideration of the requirement described in clause 6.1.11.2: - modify the ARP of the default bearer as appropriate for the IMS Multimedia Priority Service; and | M | C | |
| - if upgrade of the dedicated IM CN signalling bearer is required, modify the ARP in all the PCC/QoS rules that describe the IM CN signalling traffic to the value appropriate for IMS Multimedia Priority Services. | M | C | |
| When the PCRF detects that the P-CSCF (AF) released all the MPS session and the IMS Signalling Priority is not set for the IP-CAN session the PCRF shall under consideration of the requirement described in clause 6.1.11.2: | M | C | |

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| - modify the ARP of the default bearer to an appropriate value according to PCRF decision; and | | | |
| - modify the ARP in all PCC/QoS Rules that describe the IM CN signalling traffic to an appropriate value according to PCRF decision. | M | C | |

6.1.12 ADC Rule Authorization

Table 33 ADC Rule Authorization

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|--|
| ADC Rule authorization refers to the PCRF decision about which predefined and/or dynamic ADC rules to activate for a TDF session and is only applicable in case of solicited application reporting. | M | PC | Only predefined ADC rules are supported |
| It may also comprise the selection of parameters (monitoring key, enforcement actions etc.) for dynamic ADC rules to be applied once the traffic is detected. | Op | NC | |
| User profile configuration, received within subscription information, indicating whether application detection and control can be enabled, shall be taken into account by PCRF, when deciding on ADC rule authorization. NOTE 1: The enforcement actions are only applicable in case of solicited application reporting. NOTE 2: For unsolicited application reporting, all ADC rules pre-provisioned at TDF are authorized. | M | PC | Unsolicited application reporting is not supported |



6.1.13 Redirection

Table 34 Redirection

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---|
| PCRF may control redirection by provisioning and modifying dynamic ADC rules over the Sd interface for a TDF, or dynamic PCC rules over the Gx interface for a PCEF enhanced with ADC. The PCRF may enable/disable redirection and set a redirect destination for every dynamic ADC rule or PCC rule. | Op | PC | Only predefined ADC rules are supported |
| Redirect information (redirection enabled/disabled and redirect destination) within a PCC Rule or within an ADC rule respectively, instructs the PCEF enhanced with ADC, or the TDF whether or not to perform redirection towards a specific redirect destination. The redirect destination may be provided as part of the dynamic PCC/ADC Rule, or may be preconfigured in the PCEF enhanced with ADC or the TDF. A redirect destination provided in a dynamic PCC/ADC Rule overrides the redirect destination preconfigured in the PCEF enhanced with ADC or in the TDF for this PCC/ADC Rule. | M | PC | Only predefined ADC rules are supported |

6.1.14 Resource Sharing for Different AF Sessions

Not compliant

6.1.15 Reporting of RAN User Plane Congestion Information

Not compliant

6.1.16 Negotiation for Future Background Data Transfer

Not compliant

**6.1.17 Traffic Steering Control**

Not compliant

6.1.18 PCC Support of NBIFOM

Not compliant

6.1.19 Resource Reservation for Services Sharing Priority

Not compliant

6.1.20 Management of Packet Flow Descriptions Using the PFDF

Not compliant

6.1.21 3GPP PS Data Off

Not compliant

6.2 Functional Entities

No requirement

6.2.1 Policy Control and Charging Rules Function (PCRF)

No requirement

6.2.1.0 General

Table 35 General

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---|
| The PCRF encompasses policy control decision and flow based charging control functionalities. | M | C | |
| The PCRF provides network control regarding the service data flow detection, gating, QoS and flow based charging (except credit management) towards the PCEF and/or TDF. | M | PC | Only predefined ADC rules are supported |



| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---|
| The PCRF provides network control regarding the application detection, gating, QoS and application based charging (except credit management) towards the TDF and the PCEF enhanced with ADC. | M | PC | Only predefined ADC rules are supported |
| The PCRF shall apply the security procedures, as required by the operator, before accepting service information from the AF. | M | C | |
| The PCRF shall decide whether application traffic detection is applicable, as per operator policies, based on user profile configuration, received within subscription information. | M | C | |
| The PCRF shall decide how certain service/application traffic shall be treated in the PCEF and in the TDF, if applicable, and ensure that the PCEF user plane traffic mapping and treatment is in accordance with the user's subscription profile. | M | C | |
| If Gxx applies, the PCRF shall provide QoS rules with identical service data flow templates as provided to the PCEF in the PCC rules. If the service data flow is tunnelled at the BBERF, the PCRF shall provide the BBERF with information received from the PCEF to enable the service data flow detection in the mobility tunnel at the BBERF. In case 2a, defined in clause 7.1, the PCRF may also provide to the BBERF the charging ID information received from the PCEF. | M | NC | |
| When IP flow mobility scenarios are supported as specified in TS 23.261 [23] if the PCRF receives IP flow mobility routing rules from the PCEF, it shall provide authorized QoS rules to the applicable BBERF as specified in clause 6.1.1.3. | M | NC | |

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|--|
| The PCRF should for an IP CAN session derive, from IP CAN specific restrictions, operator policy and SPR data, the list of permitted QoS class identifiers and associated GBR and MBR limits for the IP CAN session. | M | C | |
| The PCRF may check that the service information provided by the AF is consistent with both the operator defined policy rules and the related subscription information as received from the SPR during IP CAN session establishment before storing the service information. The service information shall be used to derive the QoS for the service. The PCRF may reject the request received from the AF when the service information is not consistent with either the related subscription information or the operator defined policy rules and as a result the PCRF shall indicate that this service information is not covered by the subscription information or by operator defined policy rules and may indicate, in the response to the AF, the service information that can be accepted by the PCRF (e.g. the acceptable bandwidth). In the absence of other policy control mechanisms outside the scope of PCC, it is recommended that the PCRF include this information in the response. | Op | PC | The SAPC does not indicate in the response to the AF the service information that can be accepted in case of reject an AF request. |
| When receiving service information from the AF, the PCRF may temporarily reject the AF request (e.g. if the service information is not consistent with the operator defined policy rules for the congestion status of the user). To temporarily reject the AF request the PCRF shall indicate a re-try interval to the AF. When receiving a re-try interval from | M | NC | |



| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| <p>the PCRF the AF shall not send the same service information to the PCRF again (for the same IP CAN session) until the re-try interval has elapsed.</p> <p>NOTE 1: How the PCRF derives the re-try interval is up to implementation.</p> | | | |
| In this Release, the PCRF supports only a single Rx reference point, i.e. there is one AF for each AF session. | M | C | |
| <p>The PCRF authorizes QoS resources. The PCRF uses the service information received from the AF (e.g. SDP information or other available application information) and/or the subscription information received from the SPR to calculate the proper QoS authorization (QoS class identifier, bitrates). The PCRF may also take into account the requested QoS received from the PCEF via Gx interface.</p> <p>NOTE 2: The PCRF provides always the maximum values for the authorized QoS even if the requested QoS is lower than what can be authorized.</p> | M | C | |
| The Authorization of QoS resources shall be based on complete service information unless the PCRF is required to perform the authorization of QoS resources based on incomplete service information. The PCRF shall after receiving the complete service information, update the affected PCC rules accordingly. | M | C | |
| The PCRF may use the subscription information as basis for the policy and charging control decisions. The subscription information may apply for both session based and non-session based services. | Op | C | |

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---|
| The PCRF determines whether a Gx session from the PCEF is to be linked with a Gateway Control Session from the BBERF by matching the IPv4 address and/or IPv6 network prefix and conditionally the UE Identity, PDN Connection ID and PDN ID towards open Gateway Control Sessions. When IP flow mobility as specified in TS 23.261 [23] applies, one Gx session may be linked with multiple Gateway Control Sessions | M | NC | The SAPC does not support Gateway Control sessions from BBERF |
| If the BBERF does not provide any PDN ID at the Gateway Control Session Establishment, then the PCRF maintains Gateway Control Session to Gx session linking to the Gx sessions where the assigned CoA and UE Identity (if available over Gxx) are equal. The PCRF and BBERF shall be capable of separating information for each IP CAN session within the common Gateway Control Session. | M | NC | |
| If the BBERF provides a PDN ID at the Gateway Control Session Establishment, then the PCRF maintains Gateway Control Session to Gx session linking where the UE identity and PDN ID are equal. If the BBERF provides a PDN ID at Gateway Control Session establishment, it may also indicate in the Gateway Control Session establishment that the PCRF shall not attempt linking the new Gateway Control Session with an existing Gx session immediately. If the PCRF receives such an indication, it keeps the new Gateway Control Session pending and defers linking until an IP-CAN session establishment or an IP-CAN session modification with | M | NC | |



| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| matching UE Identity, PDN ID and IP-CAN type arrives via Gx. | | | |
| If the BBERF provides a PDN ID and a PDN Connection ID at the Gateway Control Session establishment, then the PCRF maintains Gateway Control Session to Gx session linking where the UE identity, PDN Connection ID and PDN ID are equal. | M | NC | |
| When a BBERF establishes multiple Gateway Control Sessions for the same PDN ID and the IP CAN type changes, the PCRF assumes that this constitutes inter-system BBERF relocations of existing Gateway Control Sessions. The BBERF may supply UE IP address(es) (if known) that can be used for linking the new Gateway Control Session to the existing Gx session. If the UE IP address(es) is not provided in the new Gateway Control Session establishment, the PCRF shall defer the linking with existing Gx session until receiving an IP-CAN Session modification with matching UE Identity, IP CAN type, PDN Connection ID, and PDN ID. | M | NC | |
| The PCRF determines which case applies as described on clause 7.1. | M | NC | |
| If an AF requests the PCRF to report on the signalling path status, for the AF session, the PCRF shall, upon indication of loss of resources from the PCEF, for PCC rules corresponding to the signalling traffic notify the AF on changes to the signalling path status. The PCRF needs to have the knowledge of which PCC rules identify signalling traffic. | M | NC | |

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---|
| <p>Negotiation of IP CAN bearer establishment mode takes place via Gx for 3GPP IP CANs via Gxx for non-3GPP IP CANs specified in TS 23.402 [18]. For other accesses supporting multiple IP CAN bearer establishment modes, if Gxx applies, the negotiation takes place via Gxx, otherwise via Gx.</p> <p>To support the different IP CAN bearer establishment modes (UE-only or UE/NW) the PCRF shall:</p> | M | PC | The SAPC does not support IP CAN bearer establishment via Gxx |
| <p>- shall set the IP CAN bearer establishment mode for the IP CAN session based on operator configuration, network and UE capabilities;</p> | M | C | The SAPC decides the bearer establishment mode taking into account the network and UE capabilities. |
| <p>- shall, if the bearer establishment mode is UE/NW, decide what mode (UE or NW) shall apply for a PCC rule and resolve race conditions between for requests between UE-initiated and NW-initiated requests;</p> <p>NOTE 3: For an operator-controlled service, the UE and the PCRF may be provisioned with information indicating which mode is to be used.</p> | M | C | The SAPC always decide NW. |
| <p>- may reject a UE request that is already served by a NW-initiated procedure in progress. When rejecting a UE-initiated request by sending a reject indication, the PCRF shall use an appropriate cause value which shall be delivered to the UE.</p> <p>NOTE 4: This situation may e.g. occur if the PCRF has already triggered a NW-initiated procedure that corresponds to the UE request</p> | Op | NC | UE-Init procedures (multiple IP-CAN bearers) are not supported. |



| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|------------------------|
| - guarantee the precedence of dynamic PCC rules for network controlled services in the service data flow detection process at the PCEF by setting the PCC rule precedence information to appropriate values. | M | C | |
| If an AF requests the PCRF to report on the change of type of IP CAN, the PCRF shall provide to the AF the information about the IP CAN type the user is currently using and upon indication of change of IP CAN type, notify the AF on changes of the type of IP CAN. In the case of 3GPP IP CAN, the information of the Radio Access Technology Type (e.g. UTRAN) shall be also reported to the AF. | M | NC | |
| If IP flow mobility as specified in TS 23.161 [43] or in TS 23.261 [23] applies, the PCRF shall provide to the AF the new IP-CAN type information together with the affected service information. When IP flow mobility is allowed within an IP CAN session, the PCRF shall only report to an AF the IP CAN type change when the IP flow mobility applies to the service information provided by this AF. | M | NC | |
| If an AF requests the PCRF to report Access Network Information, the PCRF shall set the Access Network Information report parameters in the corresponding PCC rule(s) or QoS rule(s) and provision them together with the corresponding event trigger to the PCEF or BBERF as per procedure in clause 7.4.2. For those PCC rule(s) or QoS rule(s) based on preliminary service information the PCRF may assign the QCI and ARP of the default bearer to avoid signalling to the UE. In addition | M | PC | BBERF is not supported |

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|------------------------|
| the SDF filter(s) shall not be marked as to be used for signalling to the UE as traffic mapping information. | | | |
| If an AF requests the PCRF to report Access Network Information, the PCRF shall also set the corresponding event trigger to the PCEF or BBERF as per procedure in clause 7.4.2. The PCRF shall, upon receiving the subsequent Access Network Information report corresponding to the AF session from the PCEF or BBERF, forward the Access Network Information as requested by the AF. | M | PC | BBERF is not supported |
| If an AF requests the PCRF to report the PLMN identifier where the UE is currently located, then the PCRF shall provide the PLMN identifier to the AF if available. Otherwise, the PCRF shall provision both the corresponding PCC rules and QoS Rules if applicable, and the event trigger to report PLMN change to the PCEF. The PCRF shall, upon receiving of the PLMN identifier from the PCEF forward this information to the AF as defined in the procedures in clause 6.1.4. | M | NC | |
| If an AF requests the PCRF to report Access Network Charging Correlation Information, the PCRF shall provide to the AF the Access Network Charging Correlation Information, that will identify the usage reports that include measurement for the flows, once the Access Network Charging Correlation Information is known at the PCRF. If not known in advance, the PCRF subscribes for the Access Network Charging Correlation Information event for the applicable PCC rule(s), unless a | C | NC | |



| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| single charging identifier per IP-CAN session is used as described below. | | | |
| The PCEF provides at IP-CAN session establishment both a charging identifier and an optional indication that the charging identifier is the only one for that IP-CAN session, as defined in TS 32.251 [9], clause 5.1.3. In absence of the indication there is a separate charging identifier for each IP-CAN bearer to identify usage reports that include measurements for flows served by each individual bearer. When the PCEF indicates that a single charging identifier is used for the IP-CAN session, the PCRF uses the charging identifier received at IP-CAN session establishment to provide Access Charging Correlation information to the AF for all flows, instead of subscribing to the Access Network Charging Correlation Information event trigger for the applicable PCC Rule(s) as described above. | M | NC | |
| If Gxx applies and the PCEF provided information about required event triggers, the PCRF shall provide these event triggers to the BBERF and notify the PCEF of the outcome of the provisioning procedure by using the PCRF initiated IP CAN Session Modification procedure, as defined in clause 7.4.2. The PCRF shall include the parameter values received in the response from the BBERF in the notification to the PCEF. | C | NC | |
| When multiple BBERFs exist (e.g. in IP flow mobility case), the PCEF may subscribe to different or common set of event triggers at different BBERFs; when the PCRF receives event notification | M | NC | |

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|-------------------------------------|
| from any BBERF, the PCRF shall include both the parameters values received from the BBERF and also the information for identifying the BBERF in the notification to the PCEF | | | |
| If Sd applies and the TDF provided information about required event triggers, the PCRF shall provide these event triggers to the PCEF or BBERF, if Gxx applies, and notify the TDF of the outcome of the provisioning procedure within the PCEF initiated IP CAN Session Modification procedure, as defined in clause 7.4.1. The PCRF shall include the parameter values, received in the response from the PCEF/BBERF, in the notification to the TDF. The relevant Event Triggers are: PLMN change, Location change, Change in type of IP CAN, RAT type change, SGSN change, Serving GW change, User CSG Information change in CSG cell, User CSG Information change in subscribed hybrid cell, User CSG Information change in un-subscribed hybrid cell, Change of UE presence in Presence Reporting Area. | M | NC | |
| When the PCRF gets an event report from the BBERF that is required by the PCEF, the PCRF shall forward this event report to the PCEF. | M | NC | |
| When the PCRF gets an Event Report from the PCEF/BBERF that is required by the TDF, the PCRF shall forward this Event Report to the TDF. | M | NC | |
| The PCRF may support usage monitoring control. Usage is defined as volume or time of user plane traffic. | Op | PC | Time usage monitoring not supported |



| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|--|
| The PCRF may receive information about total allowed usage per PDN and UE from the SPR, i.e. the overall amount of allowed resources (based either on traffic volume and/or traffic time) that are to be monitored for the PDN connections of a user. In addition information about total allowed usage for Monitoring key(s) per PDN and UE may also be received from the SPR. | M | PC | Time usage monitoring not supported |
| For the purpose of usage monitoring per access type, the PCRF receives an individual Monitoring key per access type from SPR. | M | NC | |
| For the purpose of usage monitoring control the PCRF shall request the Usage report trigger and provide the necessary usage threshold(s), either volume threshold, time threshold, or both volume threshold and time threshold upon which the requested node (PCEF or TDF) shall report to the PCRF. | M | PC | Usage monitoring not supported in TDF interactions |
| The PCRF shall decide if and when to activate usage monitoring to the PCEF and TDF. | M | PC | Usage monitoring not supported in TDF interactions |
| The PCRF may provide a Monitoring time to the PCEF/TDF for the Monitoring keys(s) and optionally specify a subsequent threshold value for the usage after the Monitoring time. | Op | NC | |
| If the PCEF reports usage before the Monitoring time is reached, the Monitoring time is not retained by the PCEF. Therefore the PCRF may again provide a Monitoring time and optionally the subsequent threshold value for the usage after the Monitoring time in the response. | Op | NC | |

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|--|
| It shall be possible for the PCRF to request a usage report from the requested node (PCEF or TDF). | M | PC | Usage monitoring not supported in TDF interactions |
| NOTE 6: The PCRF ensures that the number of requests/following policy decisions provided over Gx/Sd reference point do not cause excessive signalling load by e.g. assigning the same time for the report only for a preconfigured number of IP-CAN/TDF sessions. | M | NC | |
| Once the PCRF receives a usage report from the requested node (PCEF or TDF), the PCRF shall deduct the value of the usage report from the totally allowed usage for that PDN and UE (in case usage per IP-CAN session is reported). If usage is reported from the TDF or the PCEF, the PCRF shall deduct the value of the usage report from the totally allowed usage for individual Monitoring key(s) for that PDN and UE (in case of usage for one or several Monitoring keys is reported). NOTE 7: The PCRF maintains usage thresholds for each Monitoring key and IP CAN session that is active for a certain PDN and UE. Updating the total allowance usage after the PCEF reporting, minimizes the risk of exceeding the usage allowance. | M | PC | Usage monitoring not supported in TDF interactions |
| If the PCEF or TDF reports usage for a certain Monitoring key and if monitoring shall continue for that Monitoring key then the PCRF shall provide new threshold values in the response to the PCEF or TDF respectively. | M | PC | Usage monitoring not supported in TDF interactions |
| If Monitoring time and subsequent threshold value are | M | NC | |



| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|--|
| used then the PCRF provides them to the PCEF or TDF as well. | | | |
| The PCRF may provide a new volume threshold and/or a new time threshold to the PCEF or TDF, the new threshold values overrides the existing threshold values in the PCEF or TDF. | Op | PC | Usage monitoring not supported in TDF interactions |
| If monitoring shall no longer continue for that Monitoring key, then the PCRF shall not provide a new threshold in the response to the PCEF or TDF. | M | PC | Usage monitoring not supported in TDF interactions |
| NOTE 8: If the PCRF decides to deactivate all PCC-rules or ADC rules associated with a certain Monitoring key, then the conditions defined in clause 6.6.2 for continued Monitoring will no longer be fulfilled for that Monitoring key. | M | PC | ADC rules not supported for usage monitoring |
| If all IP-CAN session of a user to the same APN is terminated, the PCRF shall store the remaining allowed usage, i.e. the information about the remaining overall amount of resources, in the SPR. | M | C | |
| The PCRF may authorise an application service provider to request specific PCC decisions (e.g. authorisation to request sponsored IP flows, authorisation to request QoS resources). | Op | NC | |
| For sponsored data connectivity (see Annex N), the PCRF may receive a usage threshold from the AF. | Op | NC | |
| If the AF specifies a usage threshold, the PCRF 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 PCEF/TDF. | M | NC | |

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| The PCRF shall notify the AF when the PCEF/TDF reports that a usage threshold for the Monitoring key is reached provided that the AF requests to be notified for this event. | M | NC | |
| If the AF decides to allow the session to continue without specifying a usage threshold, then monitoring in the PCEF/TDF shall be discontinued for that monitoring key by the PCRF, unless there are other reasons for continuing the monitoring. | M | NC | |
| If the AF revokes the service information and the AF has notified previously a usage threshold to the PCRF, the PCRF shall report the usage up to the time of the revocation of service authorization. | M | NC | |
| If the IP-CAN session terminates and the AF has specified a usage threshold then the PCRF 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. | M | NC | |
| The PCRF performs authorizations based on sponsored data connectivity profiles stored in the SPR. | M | NC | |
| If the AF is in the operator's network and is based on the OSA/Parlay-X GW (TS 23.198 [24]), the PCRF is not required to verify that a trust relationship exists between the operator and the sponsors. | M | NC | |
| If the H-PCRF 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, | M | NC | |



| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| reject the service authorization request, or initiate the AF session termination based on home operator policy. | | | |
| If the AF request includes an AF application identifier then, based on the operator policies the PCRF may trigger the activation of a predefined PCC/ADC Rule or provide a dynamic PCC/ADC rule with an appropriate application identifier in the PCEF/TDF. | Op | NC | |
| For the solicited application reporting, it is PCRF's responsibility to coordinate the PCC rules and QoS rules, if applicable, with ADC rules in order to ensure consistent service delivery. | M | NC | |
| The PCRF uses the information relating to subscriber spending available in the OCS as input for policy decisions related to e.g. QoS control, gating or charging conditions. | M | C | |
| The PCRF uses the RUCI received from the RCAF as input for policy decisions. | M | NC | |
| If the AF contacts the PCRF via the SCEF (and the Nt interface) to request a time window and related conditions for future background data transfer, the PCRF shall determine possible transfer policies (as described in clause 6.1.16) and send them to the AF together with a reference ID. If the AF received more than one transfer policy, the AF selects one of them and informs the PCRF about the selected transfer policy. The PCRF shall store the selected transfer policy in the SPR together with the reference ID and the network area information. Whenever the PCRF receives a reference ID from the AF during a subsequent transfer | M | NC | |

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| of AF session information (via the Rx interface), the PCRF shall retrieve the corresponding transfer policy from the SPR and apply it as one of the inputs for policy decisions for this IP-CAN session. | | | |
| The PCRF uses one or more pieces of information defined in the clause 6.2.1.1 as input for the selection of traffic steering policies used to control the steering of the subscriber's traffic to appropriate (S)Gi-LAN service functions. NOTE 10: In order to allow the PCRF to select and provision an application based traffic steering policy, the reporting of detected applications to the PCRF or any other information such as the RAT type, the RUCI etc. defined in clause 6.2.1.1 can be used. | M | NC | |

6.2.1.1 Input for PCC Decisions

Table 36 Input for PCC Decisions

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---|
| The PCRF shall accept input for PCC decision-making from the PCEF, the BBERF if present, the TDF if present, the SPR and if the AF is involved, from the AF, as well as the PCRF may use its own pre-defined information | M | PC | BBERF interactions are not supported |
| The PCEF and/or BBERF may provide the following information: - Subscriber Identifier; - The IMEI(SV) of the UE; - IPv4 address of the UE; - IPv6 network prefix assigned to the UE; | Op | PC | IP flow routing information (if IP flow mobility is not supported |



| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---|
| <ul style="list-style-type: none"> - NBIFOM Routing Rules received from the UE via the PCEF (when UE-initiated NBIFOM mode as specified in TS 23.161 [43] applies); - IP flow routing information (when IP flow mobility as specified in TS 23.261 [23] applies); - IP CAN bearer attributes; if IP flow mobility as specified in TS 23.161 [43] or in TS 23.261 [23] applies, an IP-CAN session may be active over multiple accesses and thus some IP CAN bearer attributes have a value per access type; - Request type (initial, modification, etc.); - Type of IP CAN (e.g. GPRS, etc.); - Location of the subscriber; - A PDN ID; - A PLMN identifier; - IP-CAN bearer establishment mode; - 3GPP PS Data Off status. | | | |
| <p>The PCEF enhanced with ADC or the TDF may provide the following information:</p> <ul style="list-style-type: none"> - Detected application identifier; - Allocated application instance identifier; - Detected service data flow descriptions. | Op | C | |
| <p>The SPR may provide the following information for a subscriber, connecting to a specific PDN:</p> <ul style="list-style-type: none"> - Subscriber's allowed services, i.e. list of Service IDs; - For each allowed service, a pre-emption priority; | Op | PC | <p>The SAPC does not support Subscriber Guaranteed Bandwidth QoS per subscriber.</p> <p>The SAPC does not support</p> |

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---|
| <ul style="list-style-type: none"> - Information on subscriber's allowed QoS, including: the Subscribed Guaranteed Bandwidth QoS; a list of QoS class identifiers together with the MBR limit and, for real-time QoS class identifiers, GBR limit. - Subscriber's charging related information; - Spending limits profile containing an indication that policy decisions depend on policy counters available at the OCS that has a spending limit associated with it and optionally the list of relevant policy counters. - Subscriber category; - Subscriber's usage monitoring related information; - Subscriber's profile configuration; - Sponsored data connectivity profiles; - MPS EPS Priority, MPS Priority Level; - IMS Signalling Priority. | | | Sponsored data connectivity profiles. |
| <p>The AF, if involved, may provide the following application session related information, e.g. based on SIP and SDP:</p> <ul style="list-style-type: none"> - 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; | Op | PC | <p>Some data are not used for input decisions:</p> <p>Sponsored data connectivity</p> <p>AF communication Service Identifier</p> <p>AF Record Information</p> <p>Application service provider</p> |



| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| <ul style="list-style-type: none"> - Sponsored data connectivity information (see clause 5.2.1); - Flow description, e.g. source and destination IP address and port numbers and the protocol; - AF application identifier; - 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 PCRF to guarantee service for an application session of a higher relative priority; NOTE 7: The AF Priority information represents session/application priority and is separate from the MPS EPS Priority indicator. - Emergency indicator; - Application service provider. | | | |
| <p>The OCS, if involved, may provide the following information for a subscriber:</p> <ul style="list-style-type: none"> - Policy counter status for each relevant policy counter. | Op | C | |
| <p>The RCAF, if involved, may provide the following information for a subscriber: - Subscriber Identifier. - Identifier of the eNB, E-UTRAN cell or Service Area serving the subscriber.</p> <p>NOTE 9: Whether in case of E-UTRAN the eNB identifier or the ECGI are included in the RUCI is up to operator configuration in the RCAF.</p> <p>NOTE 10: Depending on the RUCI reporting interval configured in the RCAF, a UE may move</p> | Op | NC | |

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| <p>outside the area indicated without the RCAF immediately notifying the PCRF. The PCRF can avoid receiving information about the cell currently serving a UE from multiple sources (i.e. via the Np and the Gx interface) by deactivating reporting of the congested cell's identifier over Np. In case PCRF receives information about the cell currently serving a UE via Np and Gx, then the information received via Gx is expected to take precedence.</p> <ul style="list-style-type: none"> - APNs. - Congestion level or an indication of the "no congestion" state. | | | |
| <p>In addition, the predefined information in the PCRF may contain additional rules based on charging policies in the network, whether the subscriber is in its home network or roaming, depending on the IP CAN bearer attributes.</p> | Op | C | |
| <p>The QoS Class Identifier (see clause 6.3.1) in the PCC rule is derived by the PCRF from AF or SPR interaction if available. The input can be SDP information or other available application information, in line with operator policy.</p> | M | C | |
| <p>The Allocation/Retention Priority in the PCC Rule is derived by the PCRF from AF or SPR interaction if available, in line with operator policy.</p> | M | C | |



6.2.1.2 Subscription Information Management in the PCRF

Table 37 Subscription Information Management in the PCRF

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|--|
| The PCRF may request subscription information from the SPR for an IP CAN session at establishment or a gateway control session at establishment. The subscription information may include user profile configuration indicating whether application detection and control should be enabled. The PCRF should specify the subscriber ID and, if available, the PDN identifier in the request. The PCRF should retain the subscription information that is relevant for PCC decisions until the IP CAN session termination and the gateway control session termination. | Op | PC | The SAPC may not retain the subscription information during all the IP CAN session lifetime. |
| The PCRF may request notifications from the SPR on changes in the subscription information. Upon reception of a notification, the PCRF shall make the PCC decisions necessary to accommodate the change in the subscription and updates the PCEF and/or the BBERF, and/or the TDF by providing the new PCC, and/or QoS and/or ADC decisions if needed. The PCRF shall send a cancellation notification request to the SPR when the related subscription information has been deleted. | Op | PC | Notification requests are by default always activated in the SAPC BBERF interactions are not supported. |

6.2.1.3 V-PCRF

No requirement

6.2.1.3.1 General

Not compliant



| | |
|----------------|--|
| 6.2.1.3.2 | V-PCRF and Home Routed Access |
| | Not compliant |
| 6.2.1.3.3 | V-PCRF and Visited Access (Local Breakout) |
| | Not compliant |
| 6.2.1.4 | H-PCRF |
| | No requirement |
| 6.2.1.4.1 | General |
| | Not compliant |
| 6.2.1.4.2 | H-PCRF and Home Routed Access |
| | Not compliant |
| 6.2.1.4.3 | H-PCRF and Visited Access (Local Breakout) |
| | Not compliant |
| 6.2.1.5 | Handling of Multiple BBFs Associated with the Same IP CAN Session |
| | Not compliant |
| 6.2.1.5.1 | Handling of Two BBFs Associated with the Same IP-CAN Session during Handover |
| | Not compliant |
| 6.2.1.5.2 | Handling of Multiple BBFs with IP-CAN Session Flow Mobility |
| | Not compliant |
| 6.2.2 | Policy and Charging Enforcement Function (PCEF) |
| | No requirement |
| 6.2.3 | Application Function (AF) |
| | No requirement |



6.2.4 Subscription Profile Repository (SPR)

Note: The SAPC product may also include the SPR, apart from the PCRF.

Table 38 Subscription Profile Repository (SPR)

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---|
| The SPR logical entity contains all subscriber/subscription related information needed for subscription-based policies and IP CAN bearer level PCC rules by the PCRF. | M | C | |
| The SPR may be combined with or distributed across other databases in the operator's network, but those functional elements and their requirements for the SPR are out of scope of this document. | Op | NC | |
| <p>The SPR may provide the following subscription profile information (per PDN, which is identified by the PDN identifier):</p> <ul style="list-style-type: none"> - Subscriber's allowed services; - For each allowed service, a pre-emption priority; - Information on subscriber's allowed QoS, including the Subscribed Guaranteed Bandwidth QoS; - Subscriber's charging related information (e.g. location information relevant for charging); - Subscriber's User CSG Information reporting rules; - List of Presence Reporting Area identifiers and optionally the elements for one or more of the Presence Reporting Areas; - Subscriber category; - Subscriber's usage monitoring related information; | Op | PC | <p>The SAPC does not support Subscriber's User CSG Information.</p> <p>The SAPC does not support Subscriber Guaranteed Bandwidth QoS per subscriber</p> <p>Elements for one or more of the Presence Reporting Areas not supported</p> |

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| <ul style="list-style-type: none"> - MPS EPS Priority and MPS Priority Level; - IMS Signalling Priority. - Subscriber's profile configuration indicating whether application detection and control can be enabled. - Spending limits profile containing an indication that policy decisions are based on policy counters available at OCS that has a spending limit associated with it and optionally the list of policy counters. | | | |
| <p>The SPR may provide the following sponsored data connectivity profile information:</p> <ul style="list-style-type: none"> - A list of Application Service Providers and their applications per sponsor identity. | Op | NC | |
| <p>The SPR may provide the following policy information related to an ASP (see clause 6.1.16):</p> <ul style="list-style-type: none"> - 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. | Op | NC | |

6.2.5 Online Charging System

No requirement

6.2.6 Offline Charging System (OFCS)

No requirement

6.2.7 Bearer Binding and Event Reporting Function (BBERF)

No requirement



- 6.2.8 User Data Repository (UDR)
No requirement.
- 6.2.9 Traffic Detection Function (TDF)
No requirement
- 6.2.10 RAN Congestion Awareness Function (RCAF)
No requirement
- 6.2.11 Service Capability Exposure Function (SCEF)
No requirement
- 6.2.12 Traffic Steering Support Function (TSSF)
No requirement
- 6.2.13 Packet Flow Description Function (PFDF)
Not compliant
- 6.3 Policy and Charging Control Rule
No requirement
- 6.3.1 General

Table 39 General

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| The Policy and charging control rule (PCC rule) comprises the information that is required to enable the user plane detection of, the policy control and proper charging for a service data flow. The packets detected by applying the service data flow template of a PCC rule are designated a service data flow. | M | C | |

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| <p>Two different types of PCC rules exist: Dynamic rules and predefined rules. The dynamic PCC rules are provisioned by the PCRF via the Gx reference point, while the predefined PCC rules are directly provisioned into the PCEF and only referenced by the PCRF. The usage of pre-defined PCC rules for QoS control is possible if the BBF remains in the PCEF during the lifetime of an IP-CAN session. In addition, pre-defined PCC rules may be used in a non-roaming situation and if it can be guaranteed that corresponding pre-defined QoS rules are configured in the BBF and activated along with the pre-defined PCC rules.</p> <p>NOTE 1: The procedure for provisioning predefined PCC rules is out of scope for this TS.</p> <p>NOTE 2: There may be another type of predefined rules that are not explicitly known in the PCRF and not under the control of the PCRF. The operator may define such predefined PCC rules, to be activated by the PCEF on one IP CAN bearer within the IP CAN session. The PCEF may only activate such predefined PCC rules if there is no UE provided traffic mapping information related to that IP CAN bearer. The IP CAN session termination procedure deactivates such predefined PCC rules.</p> | M | C | |
| <p>There are defined procedures for activation, modification and deactivation of PCC rules (as described in clause 6.3.2). The PCRF may activate, modify and deactivate a PCC rule at any time, over the Gx reference point. However, the modification procedure is applicable to dynamic PCC rules only.</p> | M | C | |



| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| Each PCC rule shall be installed for a single IP CAN bearer only (for further details about predefined PCC rules see clause 6.3.2). | M | C | |
| The operator defines the PCC rules. | M | C | |
| Table 6.3 lists the information contained in a PCC rule, including the information name, the description and whether the PCRF may modify this information in a dynamic PCC rule which is active in the PCEF. The Category field indicates if a certain piece of information is mandatory or not for the construction of a PCC rule, i.e. if it is possible to construct a PCC rule without it. | NR | | |
| Rule identifier | M | C | |
| Precedence | M | C | |
| Service data flow template | M | C | |
| Mute for notification | Op | C | |
| Charging key | M | C | |
| Service identifier | M | C | |
| Sponsor Identifier | Op | NC | |
| Application Service Provider Identifier | Op | NC | |
| Charging method | M | C | |
| Measurement method | M | C | |
| Application Function Record Information | M | C | |
| Service identifier level reporting | M | C | |
| Gate status | M | C | |
| QoS class identifier | M | C | |
| UL/(DL)-maximum/(guaranteed) bitrate | M | C | |
| UL/(DL) sharing indication | M | NC | |
| Redirect | Op | C | |

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| Redirect Destination | Op | C | |
| ARP | M | C | |
| Bind to Default Bearer | Op | NC | |
| PS to CS session continuity | Op | NC | |
| User Location Report | M | C | |
| UE Timezone Report | M | C | |
| Monitoring key | M | NC | |
| Indication of exclusion from session level monitoring | M | NC | |
| Traffic Steering Enforcement Control | M | NC | |
| Traffic steering policy identifier(s) | M | NC | |
| NBIFOM related control Information | M | NC | |
| Allowed Access Type | M | NC | |
| Routing Rule Identifier | M | NC | |
| The PCC Rule identifier shall be unique for a PCC rule within an IP CAN session. A dynamically provided PCC rule that has the same Rule identifier value as a predefined PCC rule shall replace the predefined rule within the same IP CAN session. | M | C | |
| The Service data flow template may comprise any number of Service data flow filters. A Service data flow filter contains information for matching user plane packets. A Service data flow filter, provided from the PCRF, contains information elements as described in clause 6.2.2.2. The Service data flow template filtering information within an activated PCC rule is applied at the PCEF to identify the packets belonging to a particular service data flow. NOTE 3: Predefined PCC rules may include service data flow filters, which support extended capabilities, including enhanced | Op | C | |



| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| capabilities to identify events associated with application protocols. | | | |
| Alternatively, the Service data flow template consists of an application identifier that references an application detection filter that is used for matching user plane packets. The application identifier is also identifying the application, for which the rule applies. | Op | C | |
| <p>The same application identifier value can occur in more than one PCC rule with the following restrictions:</p> <ul style="list-style-type: none"> - The same application identifier value can be used for a dynamic PCC rule and one or multiple predefined PCC rules. If so, the PCRF shall ensure that there is at most one PCC rule active per application identifier value at any time. <p>Note 4: The configuration of the Application Identifier in the PCEF can include the set of information required for encrypted traffic detection as defined in Annex X.</p> | Op | NC | |
| The Mute for notification defines whether notification to the PCRF of application's starts or stops shall be muted. Absence of this parameter means that start/stop notifications shall be sent. | M | C | |
| The Precedence defines in what order the activated PCC rules within the same IP CAN session shall be applied at the PCEF for service data flow detection. When a dynamic PCC rule and a predefined PCC rule have the same precedence, the dynamic PCC rule takes precedence. | M | C | |
| For dynamic PCC rules that contain an application identifier, the Precedence shall be either | M | C | |

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| preconfigured at the PCEF or provided dynamically by the PCRF within the PCC Rules | | | |
| NOTE 5: The operator shall ensure that overlap between the predefined PCC rules can be resolved based on precedence of each predefined PCC rule in the PCEF. The PCRF shall ensure that overlap between the dynamically allocated PCC rules can be resolved based on precedence of each dynamically allocated PCC rule. Further information about the configuration of the PCC rule precedence is described in Annex G. | M | C | |
| NOTE 6: Whether precedence for dynamic PCC rules that contain an application identifier is preconfigured in PCEF or provided in the PCC rule from the PCRF depends on network configuration. | M | C | |
| For downlink packets all the service data flow templates, activated for the IP CAN session shall be applied for service data flow detection and for the mapping to the correct IP CAN bearer. For uplink packets the service data flow templates activated on their IP CAN bearer shall be applied for service data flow detection (further details provided in clause 6.2.2.2 and the IP-CAN specific annexes). | M | C | |
| The PCC Charging key is the reference to the tariff for the service data flow. Any number of PCC Rules may share the same charging key value. The charging key values for each service shall be operator configurable. NOTE 7: Assigning the same Charging key for several service data flows implies that the charging does not require the | M | C | |



| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| credit management to be handled separately. | | | |
| NOTE 8: If the IP flow mobility is supported and the tariff depends on what access network is in use for the service data flow, then a separate Charging key can be allocated for each access network, and the PCRF can set the Charging key in accordance with the access network in use. | M | C | |
| The PCC Service identifier identifies the service. PCC Rules may share the same service identifier value. The service identifier provides the most detailed identification, specified for flow based charging, of a service data flow. NOTE 9: The PCC rule service identifier need not have any relationship to service identifiers used on the AF level, i.e. is an operator policy option | M | C | |
| The Sponsor Identifier indicates the (3rd) party organization willing to pay for the operator's charge for connectivity required to deliver a service to the end user. | M | NC | |
| The Charging method indicates whether online charging, offline charging, or both are required or the service data flow is not subject to any end user charging. If the charging method identifies that the service data flow is not subject to any end user charging, a Charging key shall not be included in the PCC rule for that service data flow, along with other charging related parameters. If the charging method is omitted the PCEF shall apply the default charging method as determined at IP CAN session establishment (see clause 6.4). The Charging method is | M | C | |

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| mandatory if there is no default charging method for the IP CAN session. | | | |
| The Measurement method indicates what measurements apply for charging for PCC rule. | M | C | |
| The Service Identifier Level Reporting indicates whether the PCEF shall generate reports per Service Identifier. The PCEF shall accumulate the measurements from all PCC rules with the same combination of Charging key/ Service identifier values in a single report. | M | C | |
| <p>The Application function record information identifies an instance of service usage. A subsequently generated usage report, generated as a result of the PCC rule, may include the Application function record information, if available. The Application Function Record Information may contain the AF Charging Identifier and/or the Flow identifiers. The report is however not restricted to include only usage related to the Application function record information reported, as the report accumulates the usage for all PCC rules with the same combination of Charging key/ Service identifier values. If exclusive charging information related to the Application function record information is required, the PCRF shall provide a service identifier, not used by any other PCC rule of the IP CAN session at this point in time, for the AF session.</p> <p>NOTE 10: For example, the PCRF may be configured to maintain a range of service identifier values for each service which require exclusive per instance charging information. Whenever a</p> | M | NC | |



| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| <p>separate counting or credit management for an AF session is required, the PCRF shall select a value, which is not used at this point in time, within that range. The uniqueness of the service identifier in the PCEF ensures a separate accounting/credit management while the AF record information identifies the instance of the service.</p> | | | |
| <p>The Gate indicates whether the PCEF shall let a packet matching the PCC Service data flow template, pass through (gate is open) the PCEF or the PCEF shall discard (gate is closed) the packet.</p> <p>NOTE 11: A packet, matching a PCC Rule with an open gate, may be discarded due to credit management reasons.</p> | M | C | |
| <p>The QoS Class Identifier for the service data flow. The QoS class identifier represents the QoS parameters for the service data flow. The PCEF maintains the mapping between QoS class identifier and the QoS concept applied within the specific IP CAN. The bitrate information is separate from the QoS class identifier value.</p> | M | C | |
| <p>The bitrates indicate the authorized bitrates at the IP packet level of the SDF, i.e. the bitrates of the IP packets before any IP CAN specific compression or encapsulation.</p> | M | C | |
| <p>The UL maximum-bitrate indicates the authorized maximum bitrate for the uplink component of the service data flow.</p> <p>The DL maximum-bitrate indicates the authorized maximum bitrate for the</p> | M | C | |

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| <p>downlink component of the service data flow.</p> <p>The UL guaranteed-bitrate indicates the authorized guaranteed bitrate for the uplink component of the service data flow.</p> <p>The DL guaranteed-bitrate indicates the authorized guaranteed bitrate for the downlink component of the service data flow.</p> | | | |
| The 'Maximum bitrate' is used for enforcement of the maximum bit rate that the SDF may consume, while the 'Guaranteed bitrate' is used by the PCEF to determine resource allocation. | M | C | |
| The UL sharing indication indicates that resource sharing in uplink direction for service data flows with the same value in their PCC rule shall be applied by the PCEF as described in clauses 6.1.14 and 6.2.2.4. | M | NC | |
| The DL sharing indication indicates that resource sharing in downlink direction for service data flows with the same value in their PCC rule shall be applied by the PCEF as described in clauses 6.1.14 and 6.2.2.4. | M | NC | |
| The Allocation/ Retention Priority indicates the priority of allocation and retention of the service data flow. The ARP contains information about the priority level, the pre-emption capability and the pre-emption vulnerability. The Allocation/ Retention Priority resolves conflicts of demands for network resources. | M | C | |
| The Bind to Default Bearer indicates that the dynamic PCC rule shall be bound to the default bearer. | M | NC | |



| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---|
| The Redirect indicates whether the uplink part of the service data flow should be redirected to a controlled address. | M | C | |
| The Redirect Destination indicates the target redirect address when Redirect is enabled. | M | C | |
| The PS to CS session continuity is present if the service data flow is a candidate for vSRVCC according to TS 23.216 [28]. | M | NC | |
| The access network information reporting parameters (User Location Report, UE Timezone Report) instruct the PCEF about what information to forward to the PCRF when the PCC rule is activated, modified or removed. | M | C | |
| 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. | M | NC | The SAPC only supports usage monitoring for predefined PCC rules. |
| The Indication of exclusion from session level monitoring indicates that the service data flow shall be excluded from the IP-CAN session usage monitoring. | M | NC | |
| The Traffic Steering Policy Identifier(s) is a reference to a pre-configured traffic steering policy at the PCEF as defined in clause 6.11.1. | M | NC | |
| The Allowed Access Type applies only in case of NBIFOM. The Allowed Access Type indicates the IP-CAN type that is to be used for the transfer of traffic identified by the PCC rule. When the Allowed Access Type is not provided within a PCC rule, the traffic identified by the PCC rule is to be transferred on the NBIFOM default access. | M | NC | |

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| The Routing Rule Identifier applies only in case of NBIFOM. The PCRF provides it to the PCEF only when network-initiated NBIFOM mode applies. | M | NC | |

6.3.2

Policy and Charging Control Rule Operations

Table 40 Policy and Charging Control Rule Operations

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---|
| Policy and charging control rule operations consist of activation, modification and de-activation of PCC rules. | M | C | |
| Activation of a dynamic PCC rule provides the PCC rule information to the PCEF via the Gx reference point. | M | C | |
| Activation of a predefined PCC rule provides an identifier of the relevant PCC rule to the PCEF via the Gx reference point. | M | C | |
| A predefined PCC rule is known at least, within the scope of one access point. NOTE 1: The same predefined PCC rule can be activated for multiple IP CAN bearers in multiple IP CAN sessions. | M | C | |
| A predefined PCC rule is bound to one and only one IP-CAN bearer per IP CAN 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 PCEF may apply the uplink service data flow detection at additional IP CAN bearers with non-GBR QCI of the same IP CAN session. The deactivation of such a predefined PCC rule ceases its | M | C | UE-Init procedures are only supported for the default bearer. In UE_NW the PCEF decides the bearer/s to install the PCC rule. |



| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| service data flow detection for the whole IP CAN session. | | | |
| The PCRF may, at any time, modify an active, dynamic PCC rule. | Op | C | |
| The PCRF may, at any time, deactivate an active PCC rule in the PCEF via the Gx reference point. At IP CAN bearer termination all active PCC rules on that bearer are deactivated without explicit instructions from the PCRF to do so. | Op | C | |
| Policy and charging control rule operations can be also performed in a deferred mode. . | M | C | |
| A PCC Rule may have either a single deferred activation time, or a single deferred deactivation time or both. | Op | C | |
| An inactive PCC rule, that has not been activated yet, is still considered to be installed, and may be removed by the PCRF. | Op | C | |
| The PCRF may modify a currently installed PCC rule, including setting, modifying or clearing its deferred activation and/or deactivation time | Op | C | |
| When modifying a dynamic PCC rule with a prior and/or new deferred activation and/or deactivation time, the PCRF shall provide all attributes of that rule, including attributes that have not changed. | M | C | |
| Deferred activation and deactivation of PCC rules can only be used for PCC rules that belong to the IP CAN bearer without traffic mapping information. NOTE 2: This limitation prevents dependencies on the signalling of changed traffic mapping information towards the UE | M | C | |

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| Deferred modification of PCC rules shall not be applied for changes of the QoS or service data flow filter information of PCC rules. | M | C | |

6.4 IP-CAN Bearer and IP-CAN Session Related Policy Information

Table 41 PCC related IP-CAN Bearer and IP-CAN Session Related Policy Information

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---|
| The purpose of the IP CAN bearer and IP CAN session related policy information is to provide policy and charging control related information that is applicable to a single IP CAN bearer or the whole IP CAN session respectively. The PCRF provides the IP CAN bearer and IP CAN session related policy information to the PCEF and BBERF (if applicable) using the PCC rule and QoS rule (if applicable) provision procedure. The IP CAN bearer related policy information may be provided together with rules or separately. | M | C | |
| Charging information | M | C | |
| Default charging method | M | C | |
| Event trigger | M | C | |
| Authorized QoS per bearer (UE-initiated IP CAN bearer activation/modification) | M | NC | UE-Init procedures are only supported for the default bearer. |
| Authorized MBR per QCI (network initiated IP CAN bearer activation/modification). | M | NC | |
| Revalidation time limit | M | C | |
| PRA Identifier(s) | M | C | |



| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| Lists of Presence Reporting Area elements | M | C | |
| Default NBIFOM access | M | NC | |
| Upon the initial interaction with the PCEF, the PCRF may provide Charging information containing OFCS and/or OCS addresses to the PCEF defining the offline and online charging system addresses respectively. These shall override any possible predefined addresses at the PCEF. If received by the PCEF, it supersedes the Primary OFCS/OCS address and Secondary OFCS/OCS address in the charging characteristics profile. | Op | C | |
| Upon the initial interaction with the PCEF, the PCRF may provide Default charging method indicating what charging method shall be used in the IP CAN session for every PCC rule where the charging method identifier is omitted, including predefined PCC rules that are activated by the PCEF. If received by the PCEF, it supersedes the Default charging method in the charging characteristics profile. | Op | C | |
| Upon every interaction with the ERF, the PCRF may provide event triggers for the IP CAN session. Event triggers are used to determine which IP CAN bearer modification causes the ERF to re-request PCC rules. The triggers are listed in clause 6.1.4. | Op | C | |
| The semantics of the authorized QoS per bearer (UE-initiated IP CAN bearer activation/modification) and the authorized MBR per QCI (network initiated IP CAN bearer activation/modification) are captured in clause 6.2.2.4. | M | C | |

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| The Revalidation time limit defines the time period within which the PCEF shall trigger a request for PCC rules for an established IP CAN session. | M | C | |
| Upon every interaction with the PCEF, the PCRF and the OCS may activate / deactivate reporting changes of UE presence in Presence Reporting Area by setting / unsetting the corresponding event trigger or credit reauthorization 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), as described in clauses 6.1.4 and 6.1.3, respectively. | Op | NC | |
| The PCEF shall combine the requests from PCRF and the OCS. | M | NC | |
| When the Change of UE presence in Presence Reporting Area is armed, i.e. when the PCRF or the OCS 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 PCEF shall activate the relevant IP CAN specific procedure which reports when the UE enters or leaves a Presence Reporting Area (an initial report is received when the IP CAN specific procedure is activated). | M | NC | |
| When neither the PCRF nor the OCS are subscribed to change of UE presence in Presence Reporting Area for a particular Presence Reporting Area, the PCEF shall deactivate the relevant IP CAN specific procedure which reports when | M | NC | |



| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| the UE enters or leaves a Presence Reporting Area. | | | |

6.4.1

TDF Session Related Policy Information

Table 42 TDF Session Related Policy Information

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|--|
| The purpose of the TDF session related information is to provide information that is applicable to the whole TDF session. The PCRF provides the TDF session related information to the TDF (if applicable) using ADC rule provision procedure. | M | C | |
| Charging Characteristics | M | NC | |
| Charging information | M | NC | |
| Default charging method | M | NC | |
| Event trigger | M | PC | Only APPLICATION_START and APPLICATION_STOP Event triggers supported |
| Maximum downlink bit rate | M | NC | |
| Maximum uplink bit rate | M | NC | |
| ADC Revalidation time limit | M | NC | |
| Upon the initial interaction with the TDF, the PCRF may provide Charging Characteristics to the TDF, if received from the PCEF, defining how to control TDF behaviour regarding online and offline charging. | Op | NC | |
| Upon the initial interaction with the TDF, the PCRF may provide Charging information containing OFCS and/or OCS addresses to the TDF defining the offline and online charging system addresses respectively. These shall override any possible predefined | Op | NC | |

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---|
| addresses at the TDF. If received by the TDF, it supersedes the Primary OFCS/OCS address and Secondary OFCS/OCS address predefined at the TDF. | | | |
| Upon the initial interaction with the TDF, the PCRF may provide Default charging method indicating what charging method shall be used in the TDF session for every ADC rule where the charging method identifier is omitted. If received by the TDF, it supersedes the defined Default charging method. | Op | NC | |
| If Charging Characteristics are received by the PCRF from the PCEF, the PCRF may take them into account when providing Charging information and Default charging method to the TDF. In case the TDF receives both Charging Characteristics and Charging information and Default charging method parameters, the Charging Information and Default charging method shall supersede the values received in Charging Characteristics. | Op | NC | |
| <p>Upon every interaction with the TDF, the PCRF may provide Maximum downlink bit rate and/or Maximum uplink bit rate for the TDF session.</p> <p>NOTE: To avoid down-link packets being discarded in PCEF when TDF performs charging, the PCRF should set the Maximum downlink bit rate to the DL APN-AMBR.</p> | Op | NC | |
| Upon every interaction with the TDF, the PCRF may provide event triggers for the TDF session. Event triggers are used to determine which event causes the TDF to re-request ADC rules. The triggers applicable for the TDF are listed in clause 6.1.4. | Op | PC | Event triggers are only provided during TDF session establishment |



| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| The ADC Revalidation time limit defines the time period within which the TDF shall trigger a request for ADC rules for an established TDF session. | M | NC | |

6.4.2 APN Related Policy Information

Table 43 APN Related Policy Information

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| The purpose of the APN related policy information is to provide policy and charging control related information that is applicable to all IP CAN sessions of a UE to the same APN. The PCRF provides APN related policy information to the PCEF using the PCC provision procedure together with PCC rules or separately. | M | PC | |
| Authorized APN-AMBR | M | C | |
| Subsequent APN-AMBR | M | NC | |
| APN-AMBR change time | M | NC | |
| <p>The PCRF may provide the (unconditional) Authorized APN-AMBR in every interaction with the PCEF. The PCEF shall apply the Authorized APN-AMBR as APN-AMBR for all IP CAN sessions of the UE to the same APN and shall communicate the changed APN-AMBR to the UE.</p> <p>NOTE 1: There is always an unconditional value for the APN-AMBR available at the PCEF. The initial value is received as Subscribed APN-AMBR in an access specific manner and the PCRF can overwrite it by providing an Authorized APN-AMBR.</p> <p>NOTE 2: In order to reduce the risk for signalling overload, the</p> | Op | C | |

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| PCRF should avoid simultaneous provisioning of Authorized APN-AMBR for many UEs (e.g. by spreading over time). | | | |
| <p>The Authorized APN-AMBR may be provided together with conditions, i.e. a list of RAT types and/or a list of IP-CAN types. One or multiple instances of conditional APN-AMBR, with different conditions, may be provided by the PCRF. The PCEF shall apply a conditional Authorized APN-AMBR as APN-AMBR only if the current RAT type and IP-CAN type match one of the RAT types and IP-CAN types specified in the conditions, respectively. Otherwise the PCEF shall apply the unconditional Authorized APN-AMBR as APN-AMBR. A changed APN-AMBR shall be communicated to the UE.</p> <p>NOTE 3: Guidance what conditional Authorized APN-AMBR value to use in case the current RAT type and IP-CAN type match multiple conditional Authorized APN-AMBRs is specified in stage 3.</p> | Op | C | |
| Conditional Authorized APN-AMBR(s) are not applied for a PDN connection supporting NBIFOM. | M | C | |
| Upon PCRF changing the unconditional Authorized APN-AMBR or providing a conditional Authorized APN-AMBR, the PCEF shall discard any previously received conditional Authorized APN-AMBR. | M | C | |
| The PCRF may provide the unconditional and/or one or multiple instances of conditional Authorized APN-AMBR together with an APN-AMBR change time, referred to as Subsequent APN-AMBR. When the APN-AMBR | Op | C | |



| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| <p>change time is reached, the PCEF shall apply the unconditional and/or conditional Subsequent APN-AMBR as unconditional and/or conditional Authorized APN-AMBR and discard any previously applied conditional Authorized APN-AMBRs.</p> <p>NOTE 4: The modification is made in the same way as if the PCRF had modified the Authorized APN-AMBR at that point in time.</p> | | | |
| <p>Up to four instances of Subsequent APN-AMBR may be provided by the PCRF. The PCEF shall discard any previously received Subsequent APN-AMBR instances on explicit instruction as well as whenever the PCRF provides a new instruction for one or more subsequent changes to the APN-AMBR or any other subsequent parameter.</p> <p>NOTE 5: In order to provide further Subsequent APN-AMBRs in a timely fashion the PCRF can use its own clock to issue the desired changes or use the Revalidation time limit parameter (clause 6.4) to trigger a PCEF request for a policy decision.</p> | Op | C | |

6.5 Quality of Service Control Rule

Not compliant

6.6 Usage Monitoring Control Specific Information

No requirement

6.6.1

General

Table 44 General

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|--|
| The Usage Monitoring Control information comprises the information that is required to enable user plane monitoring of resources for individual applications/services, groups of applications/services, for an IP-CAN session or for a TDF session. | NR | | |
| Monitoring key | M | C | |
| Volume threshold | M | C | |
| Time Threshold | M | NC | |
| Monitoring time | Op | NC | |
| Subsequent Volume threshold | Op | NC | |
| Subsequent Time threshold | Op | NC | |
| Inactivity Detection Time | Op | NC | |
| The Monitoring Key is the reference to a resource threshold. Any number of PCC/ADC Rules may share the same monitoring key value. The monitoring key values for each service shall be operator configurable. | M | PC | Only supported for predefined PCC rules |
| It shall also be possible for an operator to use the Monitoring Key parameter to indicate usage monitoring on an IP CAN session level at the PCEF or on a TDF session level at the TDF. | M | PC | Usage monitoring not supported in TDF interactions |
| The Volume threshold indicates the overall user traffic volume after which the PCEF shall report the Usage threshold reached trigger to the PCRF. | M | C | |
| The Time threshold indicates the overall resource time usage after which the PCEF or the TDF shall report the Usage threshold reached trigger to the PCRF. | M | NC | |
| The Monitoring time indicates the time at which the PCEF or the | M | NC | |



| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| TDF shall store the accumulated usage information. | | | |
| The Subsequent Volume threshold indicates the overall user traffic volume value measured after Monitoring time, after which the PCEF or the TDF shall report the Usage threshold reached trigger to the PCRF. | M | NC | |
| The Subsequent Time threshold indicates the overall resource time usage measured after Monitoring time, after which the PCEF or the TDF shall report the Usage threshold reached trigger to the PCRF. | M | NC | |
| 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. | M | NC | |

6.6.2 Usage Monitoring Control Operations

No requirement

6.7 S2c Based IP Flow Mobility Routing Rule

Not compliant

6.8 Application Detection and Control Rule

No requirement

6.8.1 General

Table 45 General

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---|
| The Application Detection and Control rule (ADC rule) comprises the information that is required in order to: | M | PC | The SAPC only supports the identity of the ADC rule |

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|--|
| <ul style="list-style-type: none"> - identify the rule; - detect the Start and Stop of traffic for a certain application; - apply enforcement actions and charging for the application traffic detected by the rule; - apply charging for the application traffic detected by the rule. | | | |
| ADC rules are applicable over the Sd reference point. Over the Sd reference point, the ADC rules are used to support application detection and control as defined in clause 4.5 including traffic steering control as defined in clause 4.8. | M | PC | ADC rules supported only for application detection and control |
| ADC Rules are also applicable over the St reference point. Over the St reference point, the ADC rules are used to transfer traffic steering control information as defined in clause 6.11.1. | M | NC | |
| <p>ADC rules definitions are assumed to be directly provisioned into the TDF or TSSF and referenced by the PCRF with the ADC Rule identifier.</p> <p>NOTE 1: The method to perform the detection, in particular for the Start and Stop, may extend beyond the IP header and is out of scope for this document.</p> | M | PC | TSSF not supported |
| Two types of ADC rules exist: Predefined and dynamic ADC rules. A predefined ADC rule is constant and shall not be changed. For a dynamic ADC rule, some parameters can be provided and modified by the PCRF as defined in Table 6.8. | M | PC | Only predefined ADC rules supported |
| There are defined procedures for activation, modification and deactivation of ADC rules (as described in clause 6.8.2). The PCRF may activate, modify and | M | PC | Only predefined ADC rules supported |



| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| deactivate an ADC rule at any time. The modification procedure is applicable to dynamic ADC rules only. | | | |
| The operator defines the ADC rules. | M | C | |
| ADC Rule identifier | M | C | |
| Precedence | Op | NC | |
| Application identifier | C | NC | |
| Service data flow filter list | C | NC | |
| Mute for notification | Op | NC | |
| Monitoring key | Op | NC | |
| Indication of exclusion from session level monitoring | Op | NC | |
| Gate status | Op | NC | |
| UL-maximum bit rate | Op | NC | |
| DL-maximum bit rate | Op | NC | |
| Redirect | Op | NC | |
| Redirect Destination | C | NC | |
| DSCP value | Op | NC | |
| Charging key | Op | NC | |
| Service identifier | Op | NC | |
| Sponsor Identifier | C | NC | |
| Application Service Provider Identifier | C | NC | |
| Charging method | C | NC | |
| Measurement method | Op | NC | |
| Service identifier level reporting | Op | NC | |
| Traffic steering policy identifier(s) | Op | NC | |
| <p>The ADC Rule identifier shall be unique for an ADC rule within a TDF/TSSF session.</p> <p>NOTE 2: The PCRF has to ensure that there is no dynamically provided ADC rule that has the same Rule identifier value as any of the predefined ADC rules.</p> | M | NC | |

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| <p>The Precedence defines, if multiple ADC rules overlap, which ADC Rule shall be applied for the purpose of enforcement, reporting of application start and stop, monitoring, and charging. When a dynamic ADC rule and a predefined ADC rule have the same precedence, the dynamic ADC rule takes precedence. For dynamic ADC rules, the Precedence shall be either preconfigured at the TDF/TSSF or provided dynamically by the PCRF within the ADC Rules.</p> <p>NOTE 3: The operator shall ensure that overlap between the predefined ADC rules can be resolved based on precedence of each predefined ADC rule in the TDF. For dynamic ADC rules, if precedence is not preconfigured in the TDF, the PCRF shall ensure that overlap between the dynamic ADC rules can be resolved based on precedence of each dynamic ADC rule.</p> | M | NC | |
| <p>The Application identifier references the corresponding application detection filter that is used for matching user plane packets. It is also used for identifying the application, for which the rule applies, during reporting to the PCRF. The same application identifier value can occur in more than one ADC rule. If so, the PCRF shall ensure that there is at most one ADC rule active per application identifier value at any time.</p> <p>NOTE 4: The same application identifier value could be used for a dynamic ADC rule and a predefined ADC rule or for multiple predefined ADC rules.</p> <p>NOTE 5: The configuration of the Application Identifier in the TDF</p> | M | NC | |



| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| can include the set of information required for encrypted traffic detection as defined in Annex X. | | | |
| Instead of Application identifier, the Service data flow filter list may be provided which comprises one or more Service data flow filters and is used by the TDF or TSSF to identify the packets belonging to a detected traffic. The format of the Service data flow filter is described in clause 6.2.2.2, except the filters extending the inspection to look further into the packet and/or define other operations as those are identified by Application Identifier. | Op | NC | |
| The Mute for notification defines whether notification of application's start or stop shall be muted to the PCRF. Absence of this parameter means that start/stop notifications shall be sent. | M | NC | |
| The Monitoring Key is the reference to a resource threshold. Any number of ADC Rules may share the same monitoring key value. The monitoring key values for each application shall be operator configurable. | M | NC | |
| The Indication of exclusion from session level monitoring indicates that the application shall be excluded from the TDF session usage monitoring. | M | NC | |
| The Gate status indicates whether the TDF shall let detected application traffic pass through (gate is open) the TDF or the TDF shall discard (gate is closed) the application traffic. | M | NC | |
| The UL maximum-bitrate indicates the authorized maximum bitrate for the uplink component of the detected application traffic. | M | NC | |

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| <p>The DL maximum-bitrate indicates the authorized maximum bitrate for the downlink component of the detected application traffic.</p> <p>NOTE 6: The maximum bit rate is an average value, which is measured over some time period. Services may generate media with variable bitrate. The policing function should take such bitrate variations into account.</p> | M | NC | |
| <p>The Redirect indicates whether the uplink part of the detected application traffic should be redirected to a controlled address.</p> | M | NC | |
| <p>The Redirect Destination indicates the target redirect address when Redirect is enabled.</p> | M | NC | |
| <p>The DSCP value indicates the value with which a TDF marks downlink application traffic identified by an ADC rule.</p> | M | NC | |
| <p>The Charging key is the reference to the tariff for the application. Any number of ADC Rules may share the same charging key value. The charging key values for each application shall be operator configurable.</p> <p>NOTE 7: Assigning the same Charging key for several applications implies that the charging does not require the credit management to be handled separately.</p> | M | NC | |
| <p>The Service identifier identifies one or more applications to the charging system. ADC Rules may share the same Service identifier value. The service identifier provides the most detailed identification specified for application based charging.</p> | M | NC | |



| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| NOTE 8: The Service Identifier need not have any relationship to service identifiers used on the AF level, i.e. is an operator policy option. | | | |
| The Sponsor Identifier indicates the (3rd) party organization willing to pay for the operator's charge for connectivity required to deliver a service to the end user. | M | NC | |
| The Application Service Provider Identifier indicates the (3rd) party organization delivering a service to the end user. | M | NC | |
| The Charging method indicates whether online charging, offline charging, or both are required or the application is not subject to any end user charging. If the charging method identifies that the application is not subject to any end user charging, a Charging key shall not be included in the ADC rule for that application, along with other charging related parameters. If the charging method is omitted, the TDF shall apply the default charging method as determined at TDF session establishment (see clause 6.4a). The Charging method is mandatory if there is no default charging method for the TDF session. | M | NC | |
| The Measurement method indicates what measurements apply for charging for ADC rule. | M | NC | |
| The Service Identifier Level Reporting indicates whether the TDF shall generate reports per Service Identifier. The TDF shall accumulate the measurements from all ADC rules with the same combination of Charging key/ Service Identifier values in a single report. | M | NC | |

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| The Traffic Steering Policy Identifier(s) is a reference to a pre-configured traffic steering policy at the TDF/TSSF as defined in clause 6.11.1. | M | NC | |

6.8.2

Application Detection and Control Rule Operations over Sd

Table 46 Application Detection and Control Rule Operations over Sd

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|--|
| Application Detection and Control rule operations apply to solicited reporting and consist of activation, modification and deactivation of ADC rules. | M | PC | Modification of ADC rules is not supported |
| Activation: The PCRF provides the ADC Rule identifier to the TDF. | M | C | |
| The PCRF may provide data for usage monitoring and enforcement control for a dynamic ADC rule. | Op | NC | Only predefined ADC rules are supported |
| An active ADC rule means that: <ul style="list-style-type: none"> - The application traffic, matching the corresponding application, can be detected; and - Start or stop of application traffic is reported to the PCRF, if applicable and requested by the PCRF; 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 filter; and - Monitoring and enforcement, as specified within the rule, is applied. | M | C | |
| The PCRF may, at any time, modify an active, dynamic ADC rule. | Op | NC | |
| The PCRF may, at any time, deactivate an active ADC rule. | Op | C | |



| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| The TDF session termination shall deactivate all ADC rules for that IP CAN session. | | | |
| Application Detection and Control rule activation/deactivation operations can also be performed in a deferred mode. | Op | NC | |
| An ADC rule may have either a single deferred activation time, or a single deferred deactivation time or both. | Op | NC | |
| An ADC rule with only a deferred activation time shall be inactive until that time. An ADC rule with only a deferred deactivation time shall be active until that time. When the rule activation time occurs prior to the rule deactivation time, the rule is inactive until the activation and remains active until the deactivation time occurs. When the rule deactivation time occurs prior to the rule activation time, the rule is initially active until the deactivation time, then remains inactive until the activation time, and then becomes active again. | M | NC | |
| An inactive ADC rule, that has not been activated yet, is still considered to be installed, and may be removed by the PCRF. | Op | NC | |
| The PCRF may modify a currently installed dynamic ADC rule, including setting, modifying or clearing its deferred activation and/or deactivation time. | Op | NC | |
| When modifying a dynamic ADC rule with a prior and/or new deferred activation and/or deactivation time, the PCRF shall provide all attributes of that rule, including attributes that have not changed. NOTE: In this case, the PCRF omission of an attribute that has | M | NC | |

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| a prior value will erase that attribute from the rule. | | | |

6.9 Policy Decisions Based on Spending Limits

Table 47 Policy Decisions Based on Spending Limits

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---|
| Policy decisions based on spending limits is a function that allows PCRF taking actions related to the status of policy counters that are maintained in the OCS. | M | C | |
| The identifiers of the policy counters that are relevant for a policy decision in the PCRF may be stored in the PCRF or possibly in SPR. The PCRF is configured with the actions associated with the policy counter status that is received from OCS. | M | C | |
| The PCRF may request the status of policy counters in the OCS using the Initial or Intermediate Spending Limit Report Request Procedure. The OCS provides the current status of the requested policy counters to the PCRF. | M | PC | Intermediate Spending Limit Report is not supported |
| The PCRF shall immediately apply the current status of a policy counter. | M | C | |
| A pending status of a policy counter shall autonomously become the current status of a policy counter at the PCRF when the indicated corresponding time is reached. Subsequently provided information for pending statuses of a policy counter shall overwrite the previously received information. | M | NC | |
| Subsequently provided information for pending statuses of a policy counter shall overwrite | M | C | |



| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---|
| the previously received information. | | | |
| The PCRF may subscribe to spending limit reporting for policy counters from the OCS using the Initial or Intermediate Spending Limit Report Request procedure. | Op | PC | Intermediate Spending Limit Report is not supported |
| The PCRF may cancel spending limit reporting for specific policy counter(s) using the Intermediate Spending Limit Report Request procedure, or for all policy counter(s) using the Final Spending Limit Report Request procedure. | Op | NC | |
| The PCRF 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 APN-AMBR), modify the PCC/QoS/ADC Rules to apply gating or change charging conditions. | M | PC | Pending policy counter statuses are not supported |

6.10 Traffic Steering Control Information

Not compliant

6.11 NBIFOM Routing Rule

Not compliant

7 PCC Procedures and Flows

No requirement

7.1 Introduction

Partially compliant

The SAPC does not support S9 interface so roaming cases are not supported.

7.2 IP-CAN Session Establishment

Table 48 IP-CAN Session Establishment

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|--|
| This procedure concerns both roaming and non-roaming scenarios. In the roaming case when a Gateway Control Session is used, the V-PCRF should proxy the Gateway Control Session Establishment information between the BBERF in the VPLMN and the H-PCRF over S9 based on PDN-Id and roaming agreements. | M | PC | S9 Interface is not supported by the SAPC. |
| For the Local Breakout scenario (Figure 5.1.3) the V-PCRF shall proxy the Indication and Acknowledge of IP CAN Session Establishment over S9 between the PCEF in the VPLMN and the H-PCRF | M | NC | |
| For TDF and solicited application reporting, the V-PCRF shall generate ADC rules from PCC Rules containing application detection and control information as instructed by the H-PCRF over S9. Then, the V-PCRF shall install PCC Rules to the PCEF and ADC Rules to the TDF, if applicable. | M | NC | |



| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---|
| 1. The BBERF initiates a Gateway Control Session Establishment procedure as defined in clause 7.7.1 (applicable for cases 2a during initial attach and 2b, as defined in clause 7.1). | M | NC | The SAPC does not support Gxx interfaces. |
| 3. The PCEF determines that the PCC authorization is required, requests the authorization of allowed service(s) and PCC Rules information. The PCEF includes the following information: UE Identity (e.g. MN NAI), a PDN identifier (e.g. APN), the IP CAN type and the IPv4 address and IPv6 network prefix, if available, the PDN Connection Identifier received for IP CAN Bearer establishment if multiple PDN connections to the same APN are supported and, if available, the default charging method and the IP CAN bearer establishment modes supported and information on whether PCEF is enhanced with ADC. It may also include the TDF IP address, in case of solicited application reporting, if applicable. If the UE has declared support for the extended TFT filter format and the PCEF does not prevent the use thereof, then the PCEF shall indicate that support to the PCRF. The PDN identifier, IP address(es) and UE identity enables identification of the IP CAN session. The IP CAN Type identifies the type of access from which the IP CAN session is established. If the service data flow is tunnelled at the BBERF, the PCEF shall provide information about the mobility protocol tunnelling encapsulation header. The PCEF may also include the Default Bearer QoS and APN-AMBR (applicable to case 1 and case 2a, as defined in clause 7.1). In case 2a the PCEF | M | PC | The SAPC does not support Charging Characteristic forwarded by the GW/PCEF. |

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| <p>may also include charging ID information. If the GW/PCEF allocates a shorter IPv6 prefix for use with IPv6 Prefix Delegation, the GW/PCEF provides this shorter prefix as the IPv6 network prefix. If Charging Characteristics were received by GW/PCEF according to TS 23.401 [17] and TS 23.402 [18], the GW/PCEF also forwards Charging Characteristics to the PCRF. Based on local configuration the GW/PCEF may also include the following information: its control plane IPv4 and/or IPv6 address(es), an indication on how the APN was selected, indications on whether IP address(es) were statically or dynamically allocated, the charging identifier of the default bearer to identify different records belonging to the same PDN connection and an indication on whether this charging identifier is the only one for the IP-CAN session.</p> <p>NOTE 1: In case of TDF and solicited application reporting, either PCEF informs PCRF with TDF IP address, or PCRF has it preconfigured per each one of PCEFs</p> | | | |
| <p>4. If the PCRF does not have the subscriber's subscription related information, it sends a request to the SPR in order to receive the information related to the IP CAN session. The PCRF provides the subscriber ID and, if applicable, the PDN identifier to the SPR. The PCRF may request notifications from the SPR on changes in the subscription information.</p> | M | C | |
| <p>5. The PCRF stores the subscription related information containing the information about the allowed service(s) and PCC Rules information, and may</p> | M | C | |



| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|--|
| include MPS EPS Priority, MPS Priority Level and IMS Signalling Priority for establishing a PS session with priority and may also include user profile configuration indicating whether application detection and control should be enabled for the IP-CAN session. | | | |
| 6. If the PCRF determines that the policy decision depends on the status of the policy counters available at the OCS and such reporting is not established for the subscriber, the PCRF sends an Initial Spending Limit Report Request as defined in clause 7.9.1. If policy counter status reporting is already established for the subscriber, and the PCRF determines that the status of additional policy counters are required, the PCRF sends an Intermediate Spending Limit Report Request as defined in clause 7.9.2 | M | PC | Intermediate Spending Limit Report is not supported |
| 7. The PCRF makes the authorization and policy decision. If MPS EPS Priority, MPS Priority Level, and IMS Signalling Priority are present for the user, the PCRF takes the information into account. | M | C | |
| 8. For the solicited application reporting, the PCRF requests the TDF to establish the relevant session towards PCRF and provides ADC Rules to the TDF, as per user profile configuration, if traffic steering control over Sd applies, ADC Rules may contain traffic steering control information. The PCRF shall include the following information: a PDN identifier (e.g. APN), the IPv4 address and/or IPv6 network prefix, if available, and may also include the UE Identity Information and the location/ | M | PC | Only application detection and control interactions with TDF are supported |

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| <p>access network information, if available. If Charging Characteristics were received by the PCRF according to step 3 and charging is applicable for the TDF, the PCRF shall also forward received Charging Characteristics to the TDF. Additionally, if received from the PCEF and if charging is applicable for the TDF, the PCRF shall also forward the following parameters to the TDF: the GW/PCEF control plane IPv4 and/or IPv6 address (es), an indication on how the APN was selected, indications on whether IP address (es) were statically or dynamically allocated, and the PDN charging identifier of the default bearer. The PCRF may also subscribe to the Event Triggers applicable for the TDF, according to table 6.2.</p> <p>NOTE 2: If Charging Characteristics are received by the PCRF from the PCEF, PCRF may take them into account when providing Charging information and Default charging method to the TDF.</p> | | | |
| <p>9. If online charging is applicable for the TDF, and at least one ADC rule with charging parameters was activated, the TDF activates the online charging session, and provides relevant input information for the OCS decision. Depending on operator configuration, the TDF may request credit from the OCS for each charging key of the activated ADC rules.</p> | NR | | |
| <p>10. If online charging is applicable for the TDF, the OCS provides the possible credit information to the TDF and may provide re-authorisation triggers for each of the credits.</p> | NR | | |



| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---|
| 11. The TDF sends an Ack (accept or reject of the ADC rule operation(s)) to inform the PCRF about the outcome of the actions related to the decision(s) received in step 8. The Ack also includes the list of Event Triggers to report, including the case when the OCS provides any credit re-authorisation trigger, e.g. PLMN change, Location change (serving CN node), which cannot be monitored at the TDF. The Event Triggers indicate to the PCRF what events to be forwarded from the PCRF to the TDF, once PCRF gets the corresponding Event Report from the PCEF/BBERF. | M | PC | SAPC does not support Event Report Indication provided by TDF |
| 12. If traffic steering control over St applies, the PCRF determines the traffic steering control information needed for the IP-CAN session; the PCRF provides the UE IPv4 address and/or UE IPv6 prefix and one or more sets of traffic steering control information to the TSSF. The TSSF identifier is pre-configured on the PCRF per e.g. PCEF. | M | NC | |
| 13. The TSSF sends an acknowledgement to the PCRF to inform the PCRF about the outcome of the actions related to the traffic steering control information received in step 12. | M | NC | |
| 14. The PCRF sends the decision(s) including the chosen IP CAN bearer establishment mode and indicates whether the use of the extended TFT filter format is allowed in the IP-CAN session, to the PCEF. The GW (PCEF) enforces the decision. The PCRF may provide the default charging method and may include the following information: the PCC Rules to activate and the Event Triggers to report. If PCEF | M | PC | SAPC does not support Event triggers provided by TDF |

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|-------------------------------------|
| is enhanced with ADC, the applicable PCC rules are provided, according to the user profile configuration, if traffic steering control over Gx applies, PCC Rules may contain traffic steering control information. The Policy and Charging Rules allow the enforcement of policy associated with the IP CAN session. The Event Triggers indicate to the PCEF what events must be reported to the PCRF. If the TDF provided a list of Event Triggers to the PCRF in the previous step, the PCRF shall also provide those Event Triggers to the PCEF. | | | |
| 15. If online charging is applicable, and at least one PCC rule with charging parameters was activated, the PCEF activates the online charging session, and provides relevant input information for the OCS decision. Depending on operator configuration, the PCEF may request credit from the OCS for each charging key of the activated PCC rules. | NR | | |
| 16. If online charging is applicable the OCS provides the possible credit information to the PCEF and may provide re-authorisation triggers for each of the credits. In cases 2a and 2b if the OCS provides any re-authorisation trigger, which can not be monitored at the PCEF, the PCEF shall request PCRF to arrange those to be reported by the BBERF via the PCRF. | OP | PC | BBERF is not supported by the SAPC. |
| 17. If at least one PCC rule was successfully activated and if online charging is applicable, and credit was not denied by the OCS, the GW(PCEF) acknowledges the IP CAN Bearer Establishment Request. | NR | | |



| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| 18. If network control applies the GW may initiate the establishment of additional IP-CAN bearers. See Annex A and Annex D for details. | NR | | |
| 19. If the PCRF in step 12 requested an acknowledgement based on PCC rule operations, the GW(PCEF) sends the IP CAN Session Establishment Acknowledgement to the PCRF in order to inform the PCRF of the activated PCC rules result. | M | C | |

7.3 IP-CAN Session Termination

No requirement

7.3.1 UE Initiated IP-CAN Session Termination

Table 49 UE Initiated IP-CAN Session Termination

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---|
| This procedure concerns both roaming and non-roaming scenarios. In the roaming case when home routed access is used (figure 5.1.2) or if case 2a applies (as defined in clause 7.1) for Local Breakout (figure 5.1.3), the V PCRF should proxy the GW(BBERF) initiated Gateway Control Session Termination or the Gateway Control and QoS Rules Provision between the BBERF in the VPLMN and the H PCRF. For those cases it is also the H-PCRF that initiates the PCRF initiated Gateway Control Session Termination procedure or the Gateway Control and QoS Rules Provision procedure and proxy the information over S9 to the BBERF through the V PCRF. For the Local breakout scenario (figure 5.1.3) the V-PCRF shall | M | PC | S9 Interface is not supported by SAPC. The SAPC does not support BBERF. AF interactions for eHRPD 3GPP2 accesses are not supported. |

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|--|
| proxy Indication and Acknowledge of IP CAN Session Termination over S9 between the PCEF in the VPLMN and the H PCRF. If the AF resides in the VPLMN, the V PCRF shall proxy AF session signalling over S9 between the AF and the H PCRF. NOTE 1: The case when the AF resides in the VPLMN is not showed in the figure. For the same scenario if either case 1 or case 2b applies (as defined in clause 7.1), the V-PCRF may respond to/initiate the Gateway Control Session procedures locally without notifying the H PCRF. | | | |
| 3. The GW(PCEF) indicates that the IP CAN Session is being removed and provides relevant information to the PCRF. NOTE 2: The GW(PCEF) may proceed to step 9 in parallel with the indication of IP CAN Session termination. | M | C | |
| 4. The PCRF finds the PCC Rules that require an AF to be notified and removes PCC Rules for the IP CAN session. | M | C | |
| 6. The PCRF notifies the AF that there are no transmission resources for the service if this is requested by the AF. | C | C | |
| 7. The AF acknowledges the notification of the loss of transmission resources. | M | C | |
| 8. If this is the last IP-CAN session for this subscriber requiring policy counter status reporting, the Final Spending Limit Report Request as defined in clause 7.9.3 is sent. If any existing IP-CAN sessions for this subscriber require policy counter status reporting, the Intermediate Spending Limit Report Request as defined in clause 7.9.2 may be | M | PC | Intermediate Spending Limit Report is not sent |



| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|--|
| sent to alter the list of subscribed policy counters. | | | |
| 9. If there is an active Sd session between TDF and PCRF, the PCRF terminates it. | M | C | |
| 10. For the solicited application reporting, the TDF deactivates all the ADC Rules associated with the TDF session. The TDF acknowledges the termination request from the PCRF. | M | C | |
| 11. If online charging is applicable for the TDF, the TDF issues the final reports and returns the remaining credit to the OCS. | NR | | |
| 12. The OCS acknowledges the credit report and terminates the online charging session with the TDF. | NR | | |
| 13. The PCRF removes the information related to the terminated IP CAN Session (subscription information etc.), and acknowledges to the GW (PCEF) that the PCRF handling of the IP CAN session has terminated. This interaction is the response to the GW (PCEF) request in step 3. | M | C | |
| 15. If case 2a applies, the GW Control and QoS Rules Provision procedure as defined in clause 7.7.4 may be initiated to remove the QoS rules associated with the IP CAN session being terminated. This applies e.g. in case the Gateway Control Session shall remain to serve other IP CAN sessions. Alternatively, if case 2a applies and the PCRF determines that all QoS rules are to be removed and the Gateway Control Session shall be terminated, the PCRF-initiated GW Control Session Termination procedure as defined in clause 7.7.2.2 is initiated. This applies | C | NC | QoS rules are not supported by the SAPC. |

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|--|
| e.g. in case the UE is detached and the CoA acquired by the UE is not used for any other IP CAN session. | | | |
| 18. The PCRF sends a cancellation notification request to the SPR if it has subscribed such notification. If all IP-CAN sessions of the user to the same APN are terminated, the PCRF stores the remaining usage allowance in the SPR. NOTE 5: Step 18 may be initiated any time after step 13. | C | PC | The SAPC does not support a specific operation to subscribe to notifications from the SPR, and instead SAPC is subscribed by default to any change performed in the SPR. |
| 19. The SPR sends a response to the PCRF. | C | NC | |
| 20. If RUCI reporting from RCAF to PCRF is used, the PCRF sends a Release context request message to the RCAF using the previously stored identity of the RCAF. | C | NC | |
| 21. RCAF acknowledges this by sending the Release context response message to the PCRF. The RCAF releases the context corresponding to the given UE for the given APN, including any reporting restrictions. This also implies that the RCAF does not indicate to the PCRF that the congestion state is over. In case of multiple PCRFs being in simultaneous use for a given UE, a Release context request message from a PCRF applies to the UE context specific to the given Np connection only, identified by the APN. The RCAF can completely release all context information for a given UE when it has released the context for each Np connection of the given UE. | C | NC | |



| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| NOTE 6: The IP CAN Session removal procedure may proceed in parallel with the indication of IP CAN Session termination. | | | |
| 22. If the PCRF has provided traffic steering control information to the TSSF for the IP-CAN session, the PCRF sends a request to the TSSF to remove the traffic steering control information associated to the UE IPv4 address and/or to the UE IPv6 prefix for the terminated IP-CAN session. NOTE 7: Step 22 may be initiated any time after step 13. | C | NC | |
| 23. The TSSF acknowledges the removal of the traffic steering control information. | C | NC | |

7.3.2

GW (PCEF) Initiated IP-CAN Session Termination

Table 50 GW (PCEF) Initiated IP-CAN Session Termination

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|--|
| This procedure concerns both roaming and non-roaming scenarios. In the roaming case when home routed access is used (figure 5.1.2) or if case 2a applies (as defined in clause 7.1) for Local Breakout (figure 5.1.3), the V PCRF should proxy the GW(BBERF) initiated Gateway Control Session Termination or the Gateway Control and QoS Rules Provision between the BBERF in the VPLMN and the H PCRF. For those cases it is also the H-PCRF that initiates the PCRF initiated Gateway Control Session Termination procedure or the Gateway Control and QoS Rules Provision procedure and proxy the information over S9 to the BBERF through the V PCRF. For the Local breakout scenario | M | PC | S9 Interface is not supported by SAPC. BBERF is not supported by the SAPC. AF interactions for eHRPD 3GPP2 accesses are not supported. |

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---|
| (figure 5.1.3) the V-PCRF shall proxy Indication and Acknowledge of IP CAN Session Termination over S9 between the PCEF in the VPLMN and the H PCRF. If the AF relies in the VPLMN, the V PCRF shall proxy AF session signalling over S9 between the AF and the H PCRF. NOTE 1: The case when the AF resides in the VPLMN is not showed in the figure. For the same scenario if either case 1 or case 2b applies (as defined in clause 7.1), the V PCRF may respond to/initiate the Gateway Control Session procedures locally without notifying the H PCRF. | | | |
| 5. The GW(PCEF) indicates the IP CAN Session termination and provides the relevant information to the PCRF. | M | C | |
| 6. The PCRF finds the PCC Rules that require an AF to be notified. | M | C | |
| 7. The PCRF notifies the AF that there are no transmission resources for the service if this is requested by the AF. | M | C | |
| 8. The AF acknowledges the notification on the loss of transmission resources. | M | C | |
| 9. If this is the last IP-CAN session for this subscriber requiring policy counter status reporting, the Final Spending Limit Report Request as defined in clause 7.9.3 is sent. If any existing IP-CAN sessions for this subscriber require policy counter status reporting, the Intermediate Spending Limit Report Request as defined in clause 7.9.2 may be sent to alter the list of subscribed policy counters. | M | PC | Intermediate Spending Limit Report is not sent. |
| 11. If there is an active TDF session between Sd and PCRF, | M | C | |



| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|--|
| the PCRF informs TDF about IP-CAN session termination | | | |
| 12. For the solicited application reporting, the TDF deactivates all the ADC Rules associated with the TDF session. The TDF acknowledges the termination request from the PCRF. | M | C | |
| 15. The PCRF removes the information related to the terminated IP CAN Session (subscription information etc.), and acknowledges the IP CAN Session termination. | M | C | |
| 16. If case 2a applies, the GW Control and QoS Rules Provision procedure as defined in clause 7.7.4 may be initiated to remove the QoS rules associated with the IP CAN session being terminated. This applies e.g. in case the Gateway Control Session shall remain to serve other IP CAN sessions. Alternatively, if case 2a applies and the PCRF determines that the Gateway Control session shall be terminated, the PCRF-initiated GW Control Session Termination procedure as defined in clause 7.7.2.2 is initiated. This applies e.g. in case the UE is detached and the CoA acquired by the UE is not used for any other IP CAN session. | M | NC | BBERF is not supported by SAPC. |
| 19. The PCRF sends a cancellation notification request to the SPR if it has subscribed such notification. If all IP-CAN sessions of the user to the same APN are terminated, the PCRF stores the remaining usage allowance in the SPR. NOTE 3: Step 14 may be initiated any time after step 8. | C | PC | SAPC does not support a specific operation to subscribe to notifications from the SPR, and instead SAPC is subscribed by default to any change performed in the SPR. |

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| 20. The SPR sends a response to the PCRF. | C | NC | |
| 21. If RUCI reporting from RCAF to PCRF is used, the PCRF sends a Release context request message to the RCAF using the previously stored identity of the RCAF. | C | NC | |
| 22. RCAF acknowledges this by sending the Release context response message to the PCRF. The RCAF releases the context corresponding to the given UE for the given APN, including any reporting restrictions. This also implies that the RCAF does not indicate to the PCRF that the congestion state is over. In case of multiple PCRFs being in simultaneous use for a given UE, a Release context request message from a PCRF applies to the UE context specific to the given Np connection only, identified by the APN. The RCAF can completely release all context information for a given UE when it has released the context for each Np connection of the given UE. | C | NC | |
| 23. If the PCRF has provided traffic steering control information to the TSSF for the IP-CAN session, the PCRF sends a request to the TSSF to remove the traffic steering control information associated to the UE IPv4 address and/or the UE IPv6 prefix for the terminated IP-CAN session. NOTE 5: Step 23 may be initiated any time after step 6. | C | NC | |
| 24. The TSSF acknowledges the removal of the traffic steering control information. | C | NC | |



7.4 IP-CAN Session Modification

No requirement

7.4.1 IP-CAN Session Modification; GW (PCEF) Initiated

Table 51 IP-CAN Session Modification; GW (PCEF) Initiated

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|--|
| This procedure concerns both roaming and non-roaming scenarios. In the roaming case when home routed access applies (figure 5.1.3) or if case 2a applies (as defined in clause 7.1) for Local Breakout (figure 5.1.4), when a Gateway Control Session is used, the H PCRF may initiate a Gateway Control and QoS Rules Provisioning procedure towards the BBERF and proxy the information through the V PCRF over S9. For case 2b in the Local Breakout scenario (figure 5.1.4) and if the Gateway Control Session is terminated locally at the V PCRF, the V PCRF shall initiate the Gateway Control and QoS Rules Provisioning procedure locally without notifying the H PCRF. For this case the V-PCRF shall proxy the Indication and Acknowledge of IP CAN Session Modification over S9 between the PCEF in the VPLMN and the H PCRF. If the AF is located in the VPLMN for this scenario, the V PCRF shall proxy AF session signalling over S9 between the AF and the H PCRF. NOTE 1: The case when the AF resides in the VPLMN is not shown in the figure. In the non-roaming case (figure 5.1.1) the V PCRF is not involved at all. | M | PC | S9 Interface is not supported by SAPC. BBERF is not supported by SAPC. AF interactions for eHRPD 3GPP2 accesses are not supported. |
| 1. Optionally, the AF provides/revokes service information to the PCRF due to AF session signalling. The AF may subscribe | Op | PC | See Rx interface description document for |

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---|
| at this point to notification of bearer level events related to the service information. NOTE 2: For the PCRF to generate the applicable events, the PCRF instructs the PCEF to report events related to the corresponding PCC rules. Such events are not shown in this sequence diagram. | | | the list of supported IP-CAN events (Specific-Action AVP) |
| 2. The PCRF stores the service information and responds with the Acknowledgement to the AF. | M | C | |
| 5. The GW(PCEF) determines that the PCC interaction is required and sends an Indication of IP CAN Session modification (Event Report, affected PCC Rules, if available, the PDN Connection Identifier) to the PCRF together with, if available, User Location Information and/or UE Time Zone and RAN/NAS Release Cause and, if changed, the new IP CAN bearer establishment modes supported. If there is a limitation or termination of the transmission resources for a PCC Rule, the GW(PCEF) reports this to the PCRF. | M | C | |
| 6. The PCRF correlates the request for PCC Rules with the IP CAN session and service information available at the GW(PCEF). | M | C | |
| 7. The PCRF may need to report to the AF an event related to the transmission resources if the AF requested it at initial authorisation. | Op | C | See Rx interface description document for the list of supported IP-CAN events (Specific-Action AVP) |
| 8. The AF acknowledges the event report and/or responds with the requested information. | M | C | |



| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|--|
| 9. If the PCRF determines a change to policy counter status reporting is required, it may alter the subscribed list of policy counters using the Initial, Intermediate or Final Spending Limit Report Request procedures as defined in clauses 7.9.1, 7.9.2 and 7.9.3. | Op | NC | Initial Spending Limit Report is used only at IP-CAN session establishment |
| 10. The PCRF makes the authorization and policy decision. | M | C | |
| <p>11. For the TDF solicited application reporting, the steps 11-14 take place. The PCRF provides all new ADC decisions to the TDF. This may include ADC Rules activation, deactivation and modification, if traffic steering control over Sd applies, ADC Rules may contain traffic steering control information. This may also include the list of Event triggers and also Event Report for the Event triggers, if reported by the PCEF/BBERF to the PCRF, if the TDF has previously subscribed for such an Event Report. In case of local breakout, the V-PCRF shall provide ADC rules generated from PCC Rules providing application detection and control as instructed by the H PCRF over S9.</p> <p>For unsolicited application reporting and if the PCRF has recorded the release of an IPv4 address in step 5, the PCRF terminates the related Sd session.</p> | M | PC | <p>Only application detection and control interactions with TDF supported</p> <p>Unsolicited application reporting not supported</p> |
| 14. The TDF sends an Ack (accept or reject of the ADC rule operation(s)) to inform the PCRF about the outcome of the actions related to the decision(s) received in step 11. The Ack also includes the list of Event Triggers to report, including the case when the OCS provides any credit re-authorisation trigger, e.g. PLMN | M | PC | SAPC does not support Event Report Indication provided by TDF |



| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---|
| change, Location change (serving CN node), which cannot be monitored at the TDF. The Event Triggers indicate to the PCRF what events to be forwarded from the PCRF to the TDF, once PCRF gets the corresponding Event Report from the PCEF/BBERF. | | | |
| 15. If traffic steering control over St applies, the PCRF determines if traffic steering control information needs to be modified/provisioned for the IP-CAN session; the PCRF provides to the TSSF the traffic steering control information associated to the UE IPv4 address and/or to the UE IPv6 prefix. | C | NC | |
| 16. The TSSF sends an acknowledgement to the PCRF to inform the PCRF about the outcome of the actions related to the traffic steering control information received in step 15. | C | NC | |
| 17. The PCRF sends an Acknowledge of IP CAN Session modification (PCC Rules, Event Triggers and, if changed, the chosen IP CAN bearer establishment mode) to the GW(PCEF). If traffic steering control over Gx applies, PCC Rules may contain traffic steering control information. The GW(PCEF) enforces the decision. If the TDF provided a list of Event Triggers to the PCRF in the previous step, the PCRF shall also provide those Event Triggers to the PCEF. | M | PC | SAPC does not support Event Report Indication provided by TDF |
| 22. The GW(PCEF) sends a Provision Ack (accept or reject of the PCC rule operation(s)) to inform the PCRF about the outcome of the GW(PCEF) actions related to the decision(s) received in step 15. NOTE 3: For | M | C | |



| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---|
| Cases 2a and 2b, the rejection of PCC rule operation can only occur as a result of online charging interaction. | | | |
| 23. Based on the result of PCC rule operations, the PCRF decides whether to initiate a Gateway Control and QoS Rules provision procedure as defined in clause 7.7.4, if required to keep the PCC and QoS rules aligned (applicable for case 2a and 2b, as defined in clause 7.1). If there are multiple BBERFs associated with the IP CAN session, Step 15 is performed with all the BBERFs. | C | NC | BBERF is not supported by the SAPC. |
| 24. If the AF requested it, the PCRF notifies the AF of related bearer level events (e.g. transmission resources are established/released/lost). NOTE 4: Based on the outcome reported in this step the AF performs the appropriate action, e.g. starting charging or terminating the AF session. | C | C | See Rx interface description document for the list of supported IP-CAN events (Specific-Action AVP) |
| 25. The AF acknowledges the notification from the PCRF. | M | C | |

7.4.2 IP-CAN Session Modification; PCRF Initiated

Table 52 IP-CAN Session Modification; PCRF Initiated

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|--|
| This procedure concerns both roaming and non-roaming scenarios. In the roaming case when home routed access applies (figure 5.1.2) or if case 2a applies (as defined in clause 7.1) for Local Breakout (figure 5.1.3), when a Gateway Control Session is used, the V PCRF shall proxy Gateway Control and QoS Rules Request between the BBERF in the VPLMN and the H PCRF over S9. For this case the H PCRF may | M | PC | S9 Interface is not supported by SAPC. BBERF is not supported by the SAPC. AF interactions for eHRPD 3GPP2 accesses are not supported. |

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---|
| also initiate a Gateway Control and QoS Rules Provisioning procedure towards the BBERF in the VPLMN and proxy the information via the V PCRF over S9. For case 2b in the Local Breakout scenario (figure 5.1.3) and if the Gateway Control Session is terminated locally at the V PCRF, the V-PCRF shall reply to/initiate Gateway Control Session and QoS Rules Request/ Provisioning procedures locally without notifying the H PCRF. For this case the V PCRF shall proxy the Policy and Charging Rules Provisioning and Acknowledge over S9 between the PCEF in the VPLMN and the H PCRF. If the AF is located in the VPLMN for this scenario, the V PCRF shall proxy AF session signalling over S9 between the AF and the H PCRF. NOTE 1: The case when the AF resides in the VPLMN is not showed in the figure. In the non-roaming case (figure 5.1.1) the V PCRF is not involved at all. | | | |
| 1a. Optionally, the AF provides/ revokes service information to the PCRF due to AF session signalling. The AF may subscribe at this point to notification of bearer level events related to the service information. The AF may also provide a reference ID to a transfer policy that the AF previously negotiated with the PCRF (as described in clauses 6.1.16 and 7.11.1). NOTE 2: For the PCRF to generate the applicable events, the PCRF instructs the PCEF to report events related to the corresponding PCC rules. Such events are not shown in this sequence diagram. | C | PC | See Rx interface description document for the list of supported IP-CAN events (Specific-Action AVP). The SAPC does not support the policy negotiation with the AF. |
| 1b. Alternatively, optionally, for TDF, e.g. the TDF detects the | Op | PC | Only solicited application |



| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------------------|
| <p>start/stop of an application traffic that matches with one of the active ADC Rules.</p> <p>For solicited application reporting, if the start/stop of application traffic detection Event Trigger was received from the PCRF and the reporting is not muted for the ADC rule, the TDF shall provide application information to the PCRF, including the application identifier, start or stop of application traffic detection event trigger and, for the start of application's traffic detection, the service data flow descriptions, if deducible. Additionally, the application instance identifier should be included in the report both for Start and for Stop of application traffic detection, when the service data flow descriptions are provided.</p> <p>For unsolicited application reporting, the Sd reports the same application information to the PCRF unconditionally. The TDF establishes a new Sd session if it detects an application for an IPv4 address or IPv6 address for which no corresponding Sd session exists.</p> | | | reporting supported |
| 1c. Alternatively, optionally, the OCS provides a Spending Limit Report to the PCRF as described in clause 7.9.4. | Op | C | See clause 7.9.4 |
| <p>1d. Alternatively, optionally, the RCAF provides a Congestion Report to the PCRF as described in clause 7.10.1.</p> <p>NOTE 3: This step is not shown on the diagram.</p> | Op | NC | |
| 2a. The PCRF stores the service information if available and responds with the Acknowledgement to the AF. | M | C | |

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|--|
| 2a This is applicable to 1a case NOTE 4: Without AF interaction, a trigger event in the PCRF may cause the PCRF to determine that the PCC rules require updating at the PCEF, e.g. change to configured policy. | | | |
| 3. If the PCRF determines a change to policy counter status reporting is required, it may alter the subscribed list of policy counters using the Initial, Intermediate or Final Spending Limit Report Request procedures as defined in clauses 7.9.1, 7.9.2 and 7.9.3. | M | NC | Initial Spending Limit Report is used only at IP-CAN session establishment |
| 4. The PCRF makes the authorization and policy decision. If the AF provided a reference ID to a transfer policy in step 1a, the PCRF shall retrieve the corresponding transfer policy from the SPR before making any decisions. | M | PC | The SAPC does not support the policy negotiation with the AF. |
| 5. The PCRF may store the application information if provided and responds with an Acknowledgement to the TDF (for unsolicited application reporting) or a TDF session modification (for solicited application reporting). For the TDF solicited application reporting, the PCRF may provide a new ADC decision to the TDF. If the last ADC rule is deactivated, the PCRF requests the TDF to terminate the TDF session towards the PCRF. If there is no active TDF session yet between the TDF and the PCRF, the PCRF requests the TDF to establish the TDF session towards PCRF and provides an ADC decision to the TDF, if traffic steering control over Sd applies, ADC Rules may contain traffic steering control information. | Op | PC | Only solicited application reporting supported TDF session termination is only requested when IP-CAN session is finished. |



| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| In case of local breakout, the V-PCRF shall provide ADC rules generated from PCC Rules providing application detection and control as instructed by the H PCRF over S9. | | | |
| 8. For the TDF solicited application reporting, in the case of an existing on-going session, if requested by the PCRF the TDF sends a Provision Ack (accept or reject of the ADC Rule operation(s)). For a new session, the TDF sends an Ack. This is to inform the PCRF about the outcome of the actions related to the received ADC decision(s). The Provision Ack / Ack also includes the list of Event Triggers to report, including the case when the OCS provides any credit re-authorisation trigger, e.g. PLMN change, Location change (serving CN node), which cannot be monitored at the TDF. The Event Triggers indicate to the PCRF what events to be forwarded from the PCRF to the TDF, once PCRF gets the corresponding Event Report from the PCEF/ BBERF. | M | NC | |
| 9. If traffic steering control over St applies, the PCRF determines if traffic steering control information needs to be modified/provisioned for the IP-CAN session; the PCRF provides to the TSSF the traffic steering control information associated to the UE IPv4 address and/or to the UE IPv6 prefix. | C | NC | |
| 10. The TSSF sends an acknowledgement to the PCRF to inform the PCRF about the outcome of the actions related to the traffic steering control information received in step 9. | C | NC | |

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---|
| <p>11. If there is no Gateway Control and QoS Rules Reply pending and there is a need to provision QoS rules, the PCRF initiates a Gateway Control and QoS Rules Provision Procedure as defined in 7.7.4 (applicable for cases 2a and 2b, as defined in clause 7.1). If there are multiple BBERFs associated with the IP CAN session, Step 9 is performed with the BBERFs that support UE/NW bearer establishment mode.</p> <p>NOTE 6: If there is a Gateway Control and QoS Rules Reply pending, e.g. this procedure was invoked from the Gateway Control and QoS Rules Request procedure as defined in clause 7.7.3, the PCRF shall use that opportunity for provisioning the applicable QoS rules. If there are multiple BBERFs associated with the IP CAN session, and the procedure was invoked by a Gateway Control and QoS Rules Request procedure from the primary BBERF, the PCRF may receive a Gateway Control and QoS Rules Request from the non-primary BBERFs.</p> | C | NC | BBERF is not supported by the SAPC. |
| <p>12. The PCRF sends the Policy and Charging Rules Provision (PCC Rules, Event Trigger, Event Report) to the PCEF.</p> <p>If the TDF provided a list of Event Triggers to the PCRF in the previous step, the PCRF shall also provide those Event Triggers to the PCEF.</p> | M | PC | SAPC does not support Event Report Indication provided by TDF |
| 18. The PCEF sends Acknowledge Policy and Charging Rules Provisioning (accept or reject of the PCC rule operation(s)) to the PCRF. | M | C | |
| 19. If the AF requested it, the PCRF notifies the AF related bearer level events (e.g. | C | C | See Rx interface description |



| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|--|
| transmission resources are established/released/lost). | | | document for the list of supported IP-CAN events (Specific-Action AVP) |
| 20. The AF acknowledges the notification from the PCRF. | M | C | |

7.4.3

Void

No requirement

7.5

Update of the Subscription Information in the PCRF

Table 53 Update of the Subscription Information in the PCRF

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|--|
| 1. The SPR detects that the related subscription profile of an IP CAN session has been changed. | M | C | |
| 2. If requested by the PCRF, the SPR notifies the PCRF on the changed profile. | M | C | Note that the SAPC does not request notifications from the SPR. They are by default always activated |
| 3. The PCRF responds to the SPR. | M | C | |
| 4. The PCRF stores the updated profile. | M | C | |
| 5. If the updated subscriber profile requires the status of new policy counters available at the OCS then an Initial/Intermediate Spending Limit Report Request is sent from PCRF as defined in clauses 7.9.1, and 7.9.2. If the updated subscriber profile implies that no policy counter status is needed an Intermediate Spending Limit Report Request is | M | PC | Initial Spending Limit Report is used only at IP-CAN session establishment |

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|--------------------------------------|
| sent from PCRF, if this is the last policy counter status Final Spending Limit Report Request is sent from PCRF as specified in clause 7.9.3. | | | |
| 6. PCRF makes an authorization and policy decision. | M | C | |
| 7. The PCRF provides all new PCC decisions to the PCEF and BBERF (if applicable), using the PCRF initiated IP CAN session modification procedure in clause 7.4.2. The PCRF also provides all new ADC decisions to the TDF, if applicable. | M | PC | BBERF interactions are not supported |

7.6 PCRF Discovery and Selection

No requirement

7.6.1 General Principles

Table 54 General Principles

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|--|
| - A single logical PCRF entity may be deployed by means of multiple and separately addressable PCRFs. | M | C | |
| The H-PCRF must be able to correlate the AF service session information received over Rx with the right IP CAN session (PCC Session binding). | M | C | |
| - The PCRF must be able to associate sessions established over the different reference points (Gx, Rx, S9, Gxa/Gxc, Sd, Np), for the same UE's IP CAN session. The actual reference points that need to be correlated depend on the scenario (e.g. roaming, LBO etc.). | M | PC | The SAPC does not support either S9 or Gxa/Gxc. The SAPC does not support Np. It is able to establish associations |



| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------------------------------------|
| | | | between Gx and Rx reference points. |
| <p>- It shall be possible to deploy a network so that a PCRF may serve only specific PDN(s). For example, PCC may be enabled on a per APN basis.</p> <p>For the case 2a (as defined in clause 7.1), the same PCRF shall support all the PDNs for which PCC is enabled and for which there are potential users accessing by means of case 2a (as defined in clause 7.1). It shall also be possible to deploy a network so that the same PCRF can be allocated for all PDN connections for a UE.</p> <p>It shall also be possible to deploy a network so that the same PCRF can be allocated for all PDN connections for a UE.</p> | M | PC | Case 2a is not supported by the SAPC. |
| - Unique identification of an IP CAN session in the PCRF shall be possible based on the (UE ID, PDN ID)-tuple, the (UE IP Address(es), PDN ID)-tuple and the (UE ID, UE IP Address(es), PDN ID). | M | C | |

7.6.2 Solution Principles

No requirement

7.7 Gateway Control Session Procedures

Not compliant

7.8 Change in Subscription for MPS Priority Services

Table 55 Change in Subscription for MPS Priority Services

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| Once the PCRF receives a notification of a change in MPS EPS Priority, MPS Priority Level and/or IMS Signalling Priority from the SPR, the PCRF shall make the corresponding policy decisions (i.e. ARP and/or QCI change) and initiates the necessary IP-CAN session modification procedure(s) to apply the change. | M | C | |

7.9 Procedures over Sy Reference Point

7.9.1 Initial Spending Limit Report Request

Table 56 Initial Spending Limit Report Request

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|--|
| If the H-PCRF provides the list of policy counter identifier(s), the OCS returns the policy counter status per policy counter identifier provided by the PCRF. | M | NC | List of policy counter is always sent empty |
| If the H-PCRF does not provide the list of policy counter identifier(s), the OCS returns the policy counter status of all policy counter(s), which are available for this subscriber. | M | C | |
| The Initial Spending Limit Report Request includes all subscriber Identifiers associated with the UE available at the PCRF. | M | NC | Just one subscriber identifier is sent, the one used in Gx to identify the subscriber. |
| 1. The H-PCRF retrieves subscription information that indicates that policy decisions | M | C | |



| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|--|
| depend on the status of policy counter(s) held at the OCS and optionally the list of policy counter identifier(s). | | | |
| 2. The H-PCRF sends an Initial Spending Limit Report Request if this is the first time policy counter status information is requested for the user and the PDN connection. It includes in the request: the subscriber ID (e.g. IMSI) and , optionally, the list of policy counter identifier(s). | M | C | List of policy counter identifiers is never sent |

7.9.2 Intermediate Spending Limit Report Request

Not compliant

The SAPC always obtains and subscribes to the information of all policy counters at IP-CAN session establishment by means of Initial Spending Limit Report Request procedure.

7.9.3 Final Spending Limit Report Request

Table 57 Final Spending Limit Report Request

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| 1. The H-PCRF decides that notifications of policy counter status changes are no longer needed. | M | C | |
| 2. The H-PCRF sends a Final Spending Limit Report Request to the OCS to cancel the subscription to notifications of policy counter status changes from the OCS. | M | C | |



7.9.4 Spending Limit Report

Table 58 Spending Limit Report

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|------------------------------------|
| 2. The OCS sends the policy counter status, and optionally pending policy counter statuses and their activation times, for each policy counter that has changed and for which the H-PCRF subscribed to spending limit reporting. Alternatively, the OCS sends one or more pending statuses for any of the subscribed policy counters together with the time they have to be applied. | M | PC | Pending statuses are not supported |
| 3. The H-PCRF acknowledges the Spending Limit Report and takes that information into account as input for a policy decision. | M | C | |

7.10 Procedures over Np Reference Point

Not compliant

7.11 Procedures over Nt reference point

Not compliant

7.12 Procedures for Management of PFDs

Not compliant



8 Annex A (Normative): Access Specific Aspects (3GPP)

No requirement

8.1 A.1 GPRS

No requirement

8.1.1 A.1.0 General

No requirement

8.1.2 A.1.1 High level requirements

No requirement

8.1.2.1 A.1.1.1 General

No requirement

8.1.2.2 A.1.1.2 Charging Related Requirements

Compliant

8.1.2.3 A.1.1.3 Policy Control Requirements

Compliant

8.1.2.4 A.1.1.4 QoS Control

Compliant

8.1.3 A.1.2 Architecture Model and Reference Points

No requirement

8.1.3.1 A.1.2.1 Reference Points

No requirement

8.1.3.1.1 A.1.2.1.1 Gx Reference Point

Compliant

8.1.3.2 A.1.2.2 Reference Architecture

No requirement

8.1.4 A.1.3 Functional Description

No requirement

8.1.4.1 A.1.3.1 Overall Description

No requirement

8.1.4.1.1 A.1.3.1.1 Binding Mechanism

A.1.3.1.1.0 General

Table 59 General

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---|
| For the authorization of a PCC rule with a GBR QCI the PCRF shall assign a GBR value within the limit supported by the serving network. | M | C | |
| For the GPRS case bearer binding is performed by: - PCRF, when the selected operation mode is UE-only, see TS 23.060 [12], either due to PCRF decision or network/UE capability; - PCRF and PCEF (i.e. the PCRF performs the binding of the PCC rules for user controlled services while the PCEF performs the binding of the PCC rules for the network controlled services), when the selected operation mode is UE/NW. | M | PC | When the network and UE supports UE initiated procedures, the SAPC always select the value UE_NW for the IP-CAN session |
| The bearer binding performed by the PCRF shall bind a PCC rule that is authorized for a TFT packet filter to the PDP context | M | NC | The SAPC does not support TFT packet filters. |



| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| the TFT packet filter has been assigned by the UE if the PCC rule can be authorized for the QCI of the PDP context. If a new PDP context is established, the PCRF can also bind PCC rule(s) to the PDP context if the QCI of the PDP context is different from the QCI, the PCC rule(s) can be authorized for since the PCRF can modify the QCI of the new PDP context. The binding mechanism shall comply with the established traffic flow template (TFT) packet filters (for the whole IP CAN session). | | | |

A.1.3.1.1.1 Bearer Binding Mechanism Allocated to the PCEF

Compliant

A.1.3.1.1.2 Bearer Binding Mechanism Allocated to the PCRF

Partially compliant

The SAPC does not perform bearer binding, as UE-Init procedures (multiple IP-CAN bearers) are not supported.

The SAPC does not support event trigger either "PDP context activity" or "traffic mapping information change".

8.1.4.1.2 A.1.3.1.2 Reporting

Compliant

8.1.4.1.3 A.1.3.1.3 Credit management

No requirement

8.1.4.1.4 A.1.3.1.4 Event Triggers

Table 60 Event triggers

| Text | Qualifier | Compliance | Comment |
|----------------------|-----------|------------|---------|
| SGSN change | M | C | |
| RAT type change | M | C | |
| PDP Context Activity | M | NC | |



| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| Location change (routeing area) | M | C | |
| Location change (CGI/SAI) | M | C | |
| Subscribed APN-AMBR change | M | C | |
| User CSG Information change in CSG cell | M | NC | |
| User CSG Information change in subscribed hybrid cell | M | NC | |
| User CSG Information change in un-subscribed hybrid cell (see note) | M | NC | |

8.1.4.1.5 A.1.3.1.5 Policy Control

Not compliant

The SAPC does not support notification IP-CAN Type Change to the AF.

8.1.4.2 A.1.3.2 Functional Entities

No requirement

8.1.4.2.1 A.1.3.2.1 Policy Control and Charging Rules Function (PCRF)

No requirement

A.1.3.2.1.0 General

Not compliant

A.1.3.2.1.1 Input for PCC Decisions

Compliant

8.1.4.2.2 A.1.3.2.2 Policy and Charging Enforcement Function (PCEF)

No requirement

8.1.4.2.3 A.1.3.2.3 Application Function (AF)

No requirement

8.1.4.3 A.1.3.3 Policy and Charging Control Rule

No requirement



| | |
|----------------|---|
| 8.1.4.3.1 | A.1.3.3.1 General No requirement |
| 8.1.4.3.2 | A.1.3.3.2 Policy and Charging Control Rule Operations Compliant |
| 8.1.4.4 | A.1.3.4 IP-CAN bearer and IP-CAN Session Related Policy Information Not compliant The SAPC does not support the provisioning of CSG information. |
| 8.1.4.5 | A.1.3.4a TDF Session Related Policy Information Not compliant |
| 8.1.4.6 | A.1.3.5 Void |
| 8.1.5 | A.1.4 PCC Procedures and Flows No requirement |
| 8.1.5.1 | A.1.4.1 Introduction No requirement |
| 8.1.5.2 | A.1.4.2 IP-CAN Session Establishment Compliant |
| 8.1.5.3 | A.1.4.3 IP-CAN Session Termination No requirement |
| 8.1.5.3.1 | A.1.4.3.1 UE initiated IP-CAN Session Termination No requirement |
| 8.1.5.3.2 | A.1.4.3.2 GW initiated IP-CAN Session Termination No requirement |

8.1.5.4 A.1.4.4 IP-CAN Session Modification

No requirement

8.1.5.4.1 A.1.4.4.1 IP CAN Session Modification; GW (PCEF) Initiated

Not compliant

8.1.5.4.2 A.1.4.4.2 IP CAN Session Modification; PCRF Initiated

Compliant

8.2 A.2 Void

8.3 A.3 Void

8.4 A.4 3GPP Accesses (GERAN/UTRAN/E-UTRAN) - GTP-Based EPC

No requirement

8.4.1 A.4.0 General

No requirement

8.4.2 A.4.1 High Level Requirements

No requirement

8.4.2.1 A.4.1.1 Charging Related Requirements

No requirement

8.4.2.2 A.4.1.2 QoS Control

Table 61 QoS Control

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| For 3GPP Access (GTP based) it shall be possible to apply QoS control at APN-level. | M | C | |



| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| QoS control per APN allows the PCC architecture to control the authorized APN-AMBR to be enforced for the total bandwidth usage of non-GBR QCI at the PCEF within the same APN. | | | |
| NOTE 1: For the enforcement of the APN-AMBR for all IP CAN sessions to the same APN, the IP CAN is required to select the same PCEF for all of them. | M | C | |
| If there is a QCI assigned to a PCC/QoS rule which is not supported by all RATs of the IP-CAN, the PCRF shall subscribe to the event trigger 'RAT change'. | M | NC | |
| At inter-RAT mobility, the PCRF will be informed and shall then modify those PCC/QoS rules in the PCEF/BBERF to align their QCI values with those supported by the current RAT. | M | C | |
| NOTE 2: It is assumed that the PCRF is configured with the same mapping rules as the MME. NOTE 3: Subscription to RAT changes ensure that the PCRF is invoked in case the UE moves to a RAT not supporting the assigned QCI in the PCC Rules as well as in case the UE moves back to a RAT supporting the originally assigned QCI. In the latter case, the PCRF can then modify the QCI in the PCC Rules back to the originally assigned value. | M | C | |
| It shall be possible for the PCRF to authorize the QCI and ARP of the default EPS bearer to be enforced by the PCEF immediately and/or at a specific point in time by providing the default EPS bearer related policy information as defined in clause A.4.3.4. | M | NC | |

8.4.3 A.4.2 Architectural Model and Reference Points

No requirement

8.4.3.1 A.4.2.1 Reference Architecture

No requirement

8.4.4 A.4.3 Functional Description

No requirement

8.4.4.1 A.4.3.1 Overall Description

No requirement

8.4.4.1.1 A.4.3.1.1 Credit Management

No requirement

8.4.4.1.2 A.4.3.1.2 Event Triggers

Table 62 Event triggers

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| SGSN change | M | C | |
| Serving GW change | M | NC | |
| RAT type change | M | C | |
| Location change (routeing area) | M | C | |
| Location change (tracking area) | M | C | |
| Location change (ECGI) | M | C | |
| Location change (CGI/SAI) | M | C | |
| Location change (eNodeB ID) | M | NC | |
| Change of UE presence in Presence Reporting Area | M | C | |
| Subscribed APN-AMBR change | M | C | |
| EPS Subscribed QoS change | M | C | |
| User CSG Information change in CSG cell | M | NC | |
| User CSG Information change in subscribed hybrid cell User | M | NC | |



| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| User CSG Information change in un-subscribed hybrid cell (see note) | M | NC | |
| The PCRF determines at IP-CAN session establishment/ modification whether the UE is located in an access type that supports reporting changes of UE presence in Presence Reporting Area. This determination relies on local configuration and may rely on whether the UE is served by a Gn-SGSN (where this reporting is not defined) or by a S4-SGSN. The "SGSN change" trigger and the "Serving GW change" trigger may be used to determine whether the UE is served by a S4-SGSN. If the access type supports it, the PCRF may subscribe to Change of UE presence in Presence Reporting Area at any time during the life time of the IP-CAN session. | Op | C | |

8.4.4.1.3 A.4.3.1.3 Binding Mechanism

Compliant

8.4.4.1.4 A.4.3.1.4 Policy Control

Compliant

8.4.4.2 A.4.3.2 Functional Entities

No requirement

8.4.4.2.1 A.4.3.2.1 Policy Control and Charging Rules Function (PCRF)

Table 63 Policy Control and Charging Rules Function (PCRF)

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| The SPR may provide the following information for a subscriber (in addition to the | Op | C | |

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| information in clause 6.2.1.1) connecting to a specific PDN: - Authorized APN-AMBR for 3GPP Access; - Authorized Default EPS Bearer QoS | | | |
| The Authorized APN-AMBR and the Authorized Default EPS Bearer QoS are derived by the PCRF from SPR interaction, according to operator policy. | M | C | |
| The PCRF shall upon indication of PCC rule removal due to PS to CS handover notify the AF that the associated flows are no longer served by the PS-domain due to PS to CS handover. | M | C | |
| If vSRVCC is supported in the serving network, the PCRF (V-PCRF if roaming) provides an indicator via Gx to the PCEF to indicate that vSRVCC is allowed for the flow corresponding to the video component of the voice/ video call. | M | NC | |
| The PCRF shall provide SDF filters in the PCC rule as received in the packet filter information from the PCEF | M | NC | |
| If the PCRF receives a request for addition of service data flow(s) with a reference to existing SDF filter identities (and by that to existing PCC rule(s)), the PCRF shall use the QCI or ARP of the existing PCC rule for the new service data flow(s). NOTE: The reference to existing SDF filter identities informs the PCRF that the request is confined to an existing bearer, having bearer bindings with PCC rules that have the same QCI/ARP combination. Assigning a different QCI or ARP to the new SDFs would cause the procedure | M | NC | |



| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| to fail, since the PCEF cannot map the new SDFs to another bearer. | | | |

| | | | |
|-----------|---|--|--|
| 8.4.4.2.2 | A.4.3.2.2 Policy and Charging Enforcement Function (PCEF) | | |
| | No requirement | | |
| 8.4.4.2.3 | A.4.3.2.3 Application Function (AF) | | |
| | No requirement | | |
| 8.4.4.3 | A.4.3.3 Void | | |
| 8.4.4.4 | A.4.3.4 IP-CAN Bearer and IP-CAN Session Related Policy Information | | |
| | Not compliant | | |
| 8.4.4.5 | A.4.3.5 TDF Session Related Policy Information | | |
| | Not compliant | | |
| 8.4.5 | A.4.4 PCC Procedures and Flows | | |
| | No requirement | | |
| 8.4.5.1 | A.4.4.1 Introduction | | |
| | No requirement | | |
| 8.4.5.2 | A.4.4.2 IP-CAN Session Establishment | | |
| | Compliant | | |
| 8.4.5.3 | A.4.4.3 GW (PCEF) Initiated IP CAN Session Termination | | |
| | No requirement | | |
| 8.4.5.4 | A.4.4.4 IP-CAN Session Modification | | |
| | No requirement | | |

8.4.5.4.1 A.4.4.4.1 IP-CAN Session Modification; GW (PCEF) Initiated

Compliant

8.4.5.4.2 A.4.4.4.2 IP-CAN Session Modification; PCRF Initiated

Compliant

Table 64 IP-CAN Session Modification; PCRF Initiated

| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---------|
| The PCRF may provide the following parameters in the Policy and Charging Rule Provision to the PDN GW (in addition to the parameters in clause 7.4.2): Authorized APN-AMBR, Authorized Default EPS Bearer QoS. | Op | C | |
| Whenever the PCRF modifies the Authorized Default EPS Bearer QoS, the PCRF shall simultaneously modify the QCI and ARP of all PCC Rules that, according to the operator policy, shall have the same QoS as the default bearer. | M | NC | |
| A modification of the Authorized Default EPS Bearer QoS requires that at least one PCC Rule with a matching QoS can be bound to the default bearer as defined in clause 6.1.1.4. | M | NC | |

8.5 A.5 3GPP Accesses (GERAN/UTRAN/E-UTRAN) - PMIP-Based EPC

No requirement

8.5.1 A.5.0 General

Not compliant

Gxc interface towards BBERF is not supported.

8.5.2 A.5.1 High Level Requirements

No requirement



| | |
|-----------|--|
| 8.5.2.1 | A.5.1.0 General |
| | No requirement |
| 8.5.2.2 | A.5.1.1 QoS Control |
| | See A.4.1.2 QoS Control on page 146. |
| 8.5.3 | A.5.2 Architectural Model and Reference Points |
| | No requirement |
| 8.5.3.1 | A.5.2.1 Reference Architecture |
| | The SAPC does not support Gxc interface. |
| 8.5.4 | A.5.3 Functional Description |
| | No requirement |
| 8.5.4.1 | A.5.3.1 Overall Description |
| | No requirement |
| 8.5.4.1.1 | A.5.3.1.1 Binding Mechanism |
| | See A.4.3.1.3 Binding Mechanism on page 149. |
| 8.5.4.1.2 | A.5.3.1.2 Credit Management |
| | No requirement |
| 8.5.4.1.3 | A.5.3.1.3 Event Triggers |
| | Not compliant |
| 8.5.4.2 | A.5.3.2 Functional Entities |
| | No requirement |
| 8.5.4.2.1 | A.5.3.2.1 Policy Control and Charging Rules Function (PCRF) |
| | According to A.4.3.2.1 Policy Control and Charging Rules Function (PCRF) on page 149 with the exception that SAPC does not support interworking with BBERF over Gxc. |

| | |
|-----------|--|
| 8.5.4.2.2 | A.5.3.2.2 Policy and Charging Enforcement Function (PCEF) No requirement |
| 8.5.4.2.3 | A.5.3.2.3 Bearer Binding and Event Reporting Function (BBERF) No requirement |
| 8.5.4.3 | A.5.3.3 Void No requirement. |
| 8.5.4.4 | A.5.3.4 Void |
| 8.5.4.5 | A.5.3.5 IP-CAN Bearer and IP-CAN Session Related Policy Information See A.4.3.4 IP-CAN Bearer and IP-CAN Session Related Policy Information on page 151. |
| 8.5.4.6 | A.5.3.6 TDF Session Related Policy Information Not compliant |
| 8.5.5 | A.5.4 PCC Procedures and Flows No requirement |
| 8.5.5.1 | A.5.4.1 Introduction No requirement |
| 8.5.5.2 | A.5.4.2 Gateway Control Session Establishment Not compliant |
| 8.5.5.3 | A.5.4.3 Gateway Control and QoS Rules Request Not compliant |
| 8.5.5.4 | A.5.4.4 Gateway Control and QoS Rules Provisioning Not compliant |
| 8.5.5.5 | A.5.4.5 IP-CAN Session Establishment Partially compliant |



The SAPC does not support Gxc interface.

8.5.5.6

A.5.4.6 IP CAN Session Modification

Partially compliant

The SAPC does not support Gxc interface.



9 Annex B (Informative): Void

No requirement



10 Annex C (Informative): Void

No requirement



11 Annex D (Informative): Access Specific Aspects (Non-3GPP)

No requirement



12 Annex E (Informative): Void

No requirement



13 Annex F (Informative): Void

No requirement



14 Annex G (Informative): PCC Rule Precedence Configuration

No requirement.

15 Annex H (Normative): Access Specific Aspects (EPC-Based Non-3GPP)

15.1 H.1 General

Compliant

15.2 H.2 EPC-Based cdma2000 HRPD Access

Partially compliant

Optimised EUTRAN-to-HRPD handovers are not supported.

15.3 H.3 EPC-Based Trusted WLAN Access with S2a

Not compliant

TWAN location information is not supported.

15.4 H.4 EPC-Based Untrusted Non-3GPP Access

Table 65 EPC-Based Untrusted Non-3GPP Access

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| <p>The Access Network Information Report event trigger defined in clause 6.1.4 applies.</p> <p>The user location information within the Access Network Information reporting may contain:</p> <ul style="list-style-type: none"> - The local IP address and the UDP or TCP port number (if NAT was detected) detected by the ePDG as the source of the UE traffic over Swu. - WLAN Location Information and the WLAN Location Information Age.. | Op | C | |
| The PCRF reports the ePDG IP address used in IKEv2 tunnel procedures to the AF (i.e. P-CSCF) at the time the AF | M | C | |



| Text | Qualifier | Compliance | Comment |
|--|-----------|------------|---|
| <p>instructions as described in clause 6.2.3 are received and the ePDG IP address is available, i.e. at the time the AF session is established and at the time the PCRF reports IP-CAN type change, if the AF (i.e. P-CSCF) subscribes to it.</p> <p>The AF instruction to report changes of the IP CAN type is described in clause 6.2.3 including an indication that the access type is untrusted.</p> | | | |
| <p>It shall be possible for the PCRF to authorize the QCI and ARP of the default bearer to be enforced by the PCEF immediately or at a specific point in time by providing the default EPS bearer related policy information as defined in clause A.4.3.4.</p> | M | PC | <p>The SAPC does not send subsequent default EPS bearer QoS or change time information towards the PCEF</p> |



16 Annex I (Informative): Void

No requirement



17 Annex J (Informative): Standardized QCI Characteristics - Rationale and Principles

No requirement



18 Annex K (Informative): Limited PCC Deployment

No requirement



19 Annex L (Normative): Limited PCC Deployment

Not compliant



20 Annex M (Informative): Handling of UE or Network Responsibility for the Resource Management of Services

No requirement



21 Annex N (Informative): PCC Usage for Sponsored Data Connectivity

Not compliant



22 Annex P (Normative): Fixed Broadband Access Interworking with EPC

Not compliant



23 Annex Q (Informative): How to Achieve Usage Monitoring via the OCS

No requirement



24 Annex R (Informative): Disabling/Re-Enabling Usage Monitoring for a PCC/ADC Rule

No requirement



25 Annex S (Normative): Fixed Broadband Access

Not compliant



26 Annex T (Informative): How to Accumulate PCC/ADC Rule Usage in Multiple Monitoring Groups

No requirement



27 Annex U (Normative): Policy and Charging Control in the Downlink Direction for Traffic Marked with DSCP by the TDF

Table 66 Policy and Charging Control in the Downlink Direction for Traffic Marked with DSCP by the TDF

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| <p>The TDF shall be able to mark detected downlink application traffic with a DSCP value received within an installed ADC Rule matching this traffic.</p> <p>NOTE 1: Unless a class of applications matches the definition of a DSCP value standardised by IETF, DSCP values with no standardised meaning in IETF are used. DSCP values in ranges reserved by IANA for "experimental or Local Use" are suitable.</p> <p>NOTE 2: Using DSCP values with no standardised meaning in IETF prevents any IP router between TDF and PCEF to perform differentiated service scheduling for related IP packets unless it is updated or configured to support those DSCP values. This implies that sufficient network capacity must be guaranteed along the path between the TDF and PCEF so that the disabling of DiffServ packet forwarding has no detrimental impact on the end-to-end QoS.</p> <p>NOTE 3: Marking of DSCP bits for this purpose can interfere with appropriate traffic handling in some operator transport networks. The DSCP marking may also get remarked by routing entities within the operator networks.</p> <p>NOTE 4: If the application sets DSCP marking that is used for policy and charging control in the PCEF, either no ADC Rule is installed in the TDF</p> | M | NC | |

| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| matching this application traffic or if an ADC Rule is installed, then DSCP marking is not enabled. When TDF sets DSCP to values used for policy and charging control, network configuration needs to prevent an untrusted source from getting unplanned QoS and charging and also prevent remapping of this traffic between the application and the TDF. | | | |
| To ensure that the DSCP value used for service data flow detection is not visible to the operator's transport network, based on operator configuration, a tunnelling protocol may be used between TDF and PCEF. | Op | NC | |
| In case tunnelling is used then the DSCP value used for service data flow detection shall be carried in the inner IP header. The DSCP marking used in the operator's transport network is carried in the outer IP header of the tunnel. NOTE 5: The tunnel connections are preconfigured in the IP infrastructure connecting the TDF and the PCEF. The operator needs to ensure the same tunnel configuration is used for the TDF and for the PCEF. The tunnel protocol can be any applicable IP-based tunnel depending on operator's choice. | M | NC | |
| In order to support policy and charging control in the downlink direction by the PCEF/BBERF for an application detected by the TDF (typically for services with non-deductible service data flows), the PCRF shall either install a dynamic PCC/QoS Rule or activate a pre-defined PCC rule, which identifies traffic based on the corresponding DSCP value (provided by the ToS/Traffic Class mask field within the service data flow filter). In case tunnelling is used, the PCEF shall use the inner header's DSCP for the service data flow detection defined in clause 6.2.2.2. | M | NC | |



| Text | Qualifier | Compliance | Comment |
|---|-----------|------------|---------|
| NOTE 6: This solution is particularly useful for QoS enforcement in the downlink direction procedures performed by the PCEF/BBERF. The TDF may still perform application detection and control as per received ADC Rules, including application detection reporting to the PCRF, enforcement control, usage monitoring control and charging, while applying DSCP marking. The PCEF/BBERF may also perform then policy and charging control in the downlink direction. | | | |



28 Annex V (Informative): Policy Control for Remote UEs behind a ProSe UE-to-Network Relay UE

No requirement



29 Annex W (Informative): Void

No requirement



30 Annex X (Informative): Encrypted Traffic Detection by Using Domain Name Matching

Not compliant



31 Annex Y (Informative): Change History

No requirement



32 Reference List

Standard

1. 3GPP Technical Specification Policy and Charging Control Architecture - 23.203