ETSI TS 123 203 V18.0.0 (2024-04)

**Digital cellular telecommunications system (Phase 2+) (GSM);
Universal Mobile Telecommunications System (UMTS);
LTE;
Policy and charging control architecture
(3GPP TS 23.203 version 18.0.0 Release 18)**

Reference
RTS/TSGS-0223203vi00

Keywords
GSM,LTE,UMTS

ETSI

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

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

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

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Legal Notice

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

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

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

Modal verbs terminology

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

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

Contents

Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

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

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

In the present document, modal verbs have the following meanings:

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

can indicates that something is possible

cannot indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

will indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

will not indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

might indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

might not indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

is (or any other verb in the indicative mood) indicates a statement of fact

is not (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

Introduction

Policy and Charging Control functionality encompasses two main functions:

- Flow Based Charging, including charging control and online credit control, for service data flows and application traffic;
- Policy control (e.g. gating control, QoS control, QoS signalling, etc.).

The present document specifies the generic PCC aspects within the body, while the specifics for each type of IP-CAN are specified in Annexes. For one type of IP-CAN the corresponding clause in an Annex shall be understood to be a realization of the TS main body. The Annexes are therefore not stand-alone specifications for an IP-CAN. Annexes may specify additional restrictions to the specification body.

1 Scope

The present document specifies the overall stage 2 level functionality for Policy and Charging Control that encompasses the following high level functions for IP-CANs (e.g. GPRS, Fixed Broadband, EPC, etc.):

- Flow Based Charging for network usage, including charging control and online credit control, for service data flows and application traffic;
- Policy control (e.g. gating control, QoS control, QoS signalling, etc.).

The present document specifies the Policy and Charging Control functionality for Evolved 3GPP Packet Switched domain, including both 3GPP accesses GERAN/UTRAN/E-UTRAN and Non-3GPP accesses, according to TS 23.401 [17] and TS 23.402 [18].

The present document specifies functionality for unicast bearers. Broadcast and multicast bearers, such as MBMS contexts for GPRS, are out of scope of the present document.

NOTE: For E-UTRAN access, the usage of functionalities covered in this specification for features such as MBMS, CIoT and V2X is described in TS 23.246 [6], TS 23.682 [42] and TS 23.285 [48], respectively.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TS 41.101: "Technical Specifications and Technical Reports for a GERAN-based 3GPP system".

[2] Void.

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

[4] IETF RFC 4006: "Diameter Credit-Control Application".

[5] 3GPP TS 23.207: "End-to-end Quality of Service (QoS) concept and architecture".

[6] 3GPP TS 23.246: "Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description".

[7] 3GPP TS 23.125: "Overall high level functionality and architecture impacts of flow based charging; Stage 2".

[8] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[9] 3GPP TS 32.251: "Telecommunication management; Charging management; Packet Switched (PS) domain charging".

[10] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)".

[11] 3GPP TR 33.919: "3G Security; Generic Authentication Architecture (GAA); System description".

[12] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[13] Void.

[14] 3GPP TS 23.107: "Quality of Service (QoS) concept and architecture".

[15] "WiMAX End-to-End Network Systems Architecture" (http://www.wimaxforum.org/technology/documents).

[16] 3GPP TS 23.003: "Numbering, addressing and identification".

[17] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[18] 3GPP TS 23.402: "Architecture Enhancements for non-3GPP accesses".

[19] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2".

[20] 3GPP2 X.S0057-B v2.0: "E UTRAN - HRPD Connectivity and Interworking: Core Network Aspects", July 2014.

[21] 3GPP TS 23.167: "IP Multimedia Subsystem (IMS) emergency sessions".

[22] 3GPP TS 29.213: "Policy and Charging Control signalling flows and QoS parameter mapping".

[23] 3GPP TS 23.261: "IP Flow Mobility and seamless WLAN offload; Stage 2".

[24] 3GPP TS 23.198: "Open Service Access (OSA); Stage 2".

[25] 3GPP TS 23.335: "User Data Convergence (UDC); Technical realization and information flows; Stage 2".

[26] 3GPP TS 29.335: "User Data Convergence (UDC); User Data Repository Access Protocol over the Ud interface; Stage 3".

[27] 3GPP TS 22.115: "Service aspects; Charging and billing".

[28] 3GPP TS 23.216: "Single Radio Voice Call Continuity (SRVCC); Stage 2".

[29] 3GPP TS 23.139:"3GPP-Fixed Broadband Access Interworking".

[30] Broadband Forum TR-203: "Interworking between Next Generation Fixed and 3GPP Wireless Access" (work in progress).

[31] Broadband Forum TR-134: "Policy Control Framework " (work in progress).

[32] 3GPP TS 25.467: "UTRAN architecture for 3G Home Node B (HNB); Stage 2".

[33] Broadband Forum TR-291: "Nodal Requirements for Interworking between Next Generation Fixed and 3GPP Wireless Access" (work in progress).

[34a] Broadband Forum TR-124 issue 2: "Functional Requirements for Broadband Residential Gateway Devices".

[34b] Broadband Forum TR-124 issue 3: "Functional Requirements for Broadband Residential Gateway Devices".

[35] Broadband Forum TR-101: "Migration to Ethernet-Based Broadband Aggregation".

[36] Broadband Forum TR-146: "Internet Protocol (IP) Sessions".

[37] Broadband Forum TR-300: "Nodal Requirements for Converged Policy Management".

[38] 3GPP TS 22.278: "Service requirements for the Evolved Packet System (EPS)".

[39] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[40] Broadband Forum TR-092: "Broadband Remote Access Server (BRAS) Requirements Document".

[41] Broadband Forum TR-134: "Broadband Policy Control Framework (BPCF)".

[42] 3GPP TS 23.682: "Architecture enhancements to facilitate communications with packet data networks and applications".

[43] 3GPP TS 23.161: "Network-based IP flow mobility and Wireless Local Area Network (WLAN) offload; Stage 2".

[44] 3GPP TS 23.303: "Proximity-based services (ProSe); Stage 2".

[45] 3GPP TS 26.114: "Multimedia telephony over IP Multimedia Subsystem (IMS); Multimedia telephony; media handling and interaction".

[46] 3GPP TS 23.179: "Functional architecture and information flows to support mission-critical communication service; Stage 2".

[47] IETF RFC 6066: "Transport Layer Security (TLS) Extensions: Extension Definitions".

[48] 3GPP TS 23.285: "Architecture enhancements for V2X services".

[49] 3GPP TS 22.011: "Service accessibility".

[50] 3GPP TS 24.008: "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3".

[51] 3GPP TS 22.261: "Service requirements for the 5G system; Stage1".

[52] 3GPP TS 23.272: "Circuit Switched (CS) fallback in Evolved Packet System (EPS); Stage 2".

[53] 3GPP TS 26.238: "Uplink streaming".

[54] 3GPP TR 26.939: "Guidelines on the Framework for Live Uplink Streaming (FLUS)".

[55] 3GPP TS 23.221: "3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; Architectural Requirements".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [8] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [8].

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

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

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

ADC decision: A decision consists of references to ADC rules, associated enforcement actions (for dynamic ADC rules) and TDF session attributes and is provided by the PCRF to the TDF for application detection and control.

ADC rule: A set of information enabling the detection of application traffic and associated enforcement actions. ADC rules are directly provisioned into the TDF and referenced by the PCRF.

authorised QoS: The maximum QoS that is authorised for a service data flow. In case of an aggregation of multiple service data flows within one IP-CAN bearer (e.g. for GPRS a PDP context), the combination of the "Authorised QoS" information of the individual service data flows is the "Authorised QoS" for the IP-CAN bearer. It contains the QoS class identifier and the data rate.

binding: The association between a service data flow and the IP-CAN bearer (for GPRS the PDP context) transporting that service data flow.

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

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

charging key: information used by the online and offline charging system for rating purposes.

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

dynamic ADC Rule: an ADC rule, for which the PCRF can provide and modify some parameters via the Sd reference point.

dynamic PCC Rule: a PCC rule, for which the definition is provided to the PCEF via the Gx reference point.

event report: a notification, possibly containing additional information, of an event which occurs that corresponds with an event trigger. Also, an event report is a report from the PCRF to the AF concerning transmission resources or requesting additional information.

event trigger: a rule specifying the event reporting behaviour of a PCEF or BBERF or TDF. Also, it is a trigger for credit management events.

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

Gateway Control Session: An association between a BBERF and a PCRF (when GTP is not used in the EPC), used for transferring access specific parameters, BBERF events and QoS rules between PCRF and BBERF.

GBR bearer: An IP-CAN bearer with reserved (guaranteed) bitrate resources.

GPRS IP-CAN: This IP-CAN incorporates GPRS over GERAN and UTRAN, see TS 23.060 [12].

IP-CAN bearer: An IP transmission path of defined capacity, delay and bit error rate, etc. See TR 21.905 [8] for the definition of bearer.

IP-CAN session: The association between a UE and an IP network. The association is identified by one IPv4 and/or an IPv6 prefix together with UE identity information, if available, and a PDN represented by a PDN ID (e.g. an APN). An IP-CAN session incorporates one or more IP-CAN bearers. Support for multiple IP-CAN bearers per IP-CAN session is IP-CAN specific. An IP-CAN session exists as long as UE IP addresses/prefix are established and announced to the IP network.

non-GBR bearer: An IP-CAN bearer with no reserved (guaranteed) bitrate resources.

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

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

Presence Reporting Area: An area defined within 3GPP Packet Domain for the purposes of reporting of UE presence within that area due to policy control and/or charging reasons. There are two types of Presence Reporting Areas: "UE-dedicated Presence Reporting Areas", and "Core Network pre-configured Presence Reporting Areas". They are further defined in TS 23.401 [17].

PCC decision: A decision consists of PCC rules and IP-CAN bearer attributes and is provided by the PCRF to the PCEF for policy and charging control and, for PCEF enhanced with ADC, application detection and control.

PCC rule: A set of information enabling the detection of a service data flow and providing parameters for policy control and/or charging control and, for PCEF enhanced with ADC, for application detection and control.

PCEF enhanced with ADC: PCEF, enhanced with application detection and control feature.

policy control: The process whereby the PCRF indicates to the PCEF how to control the IP-CAN bearer. Policy control includes QoS control and/or gating control.

predefined PCC Rule: a PCC rule that has been provisioned directly into the PCEF by the operator.

policy counter: A mechanism within the OCS to track spending applicable to a subscriber.

policy counter identifier: A reference to a policy counter in the OCS for a subscriber.

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

Packet Flow Description (PFD): A set of information enabling the detection of application traffic provided by a 3rd party service provider. A PFD is further defined in TS 23.682 [42].

QoS class identifier (QCI): A scalar that is used as a reference to a specific packet forwarding behaviour (e.g. packet loss rate, packet delay budget) to be provided to a SDF. This may be implemented in the access network by the QCI referencing node specific parameters that control packet forwarding treatment (e.g. scheduling weights, admission thresholds, queue management thresholds, link layer protocol configuration, etc.), that have been pre-configured by the operator at a specific node(s) (e.g. eNodeB).

QoS rule: A set of information enabling the detection of a service data flow and defining its associated QoS parameters.

Monitoring key: information used by the PCEF, TDF and PCRF for usage monitoring control purposes as a reference to a given set of service data flows or application (s), that all share a common allowed usage on a per UE and APN basis.

RAN user plane congestion: RAN user plane congestion occurs when the demand for RAN resources exceeds the available RAN capacity to deliver the user data for a prolonged period of time.

NOTE 1: Short-duration traffic bursts is a normal condition at any traffic load level, and is not considered to be RAN user plane congestion. Likewise, a high-level of utilization of RAN resources (based on operator configuration) is considered a normal mode of operation and might not be RAN user plane congestion.

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

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

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

service data flow filter identifier: A scalar that is unique for a specific service data flow (SDF) filter (used on Gx and Gxx) within an IP-CAN session.

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

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

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

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

spending limit report: a notification, containing the current policy counter status generated from the OCS to the PCRF via the Sy reference point.

subscribed guaranteed bandwidth QoS: The per subscriber, authorized cumulative guaranteed bandwidth QoS which is provided by the SPR/UDR to the PCRF.

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

(S)Gi-LAN: The network infrastructure connected to the 3GPP network over the SGi or Gi reference point that provides various IP-based services.

(S)Gi-LAN service function: A function located in the (S)Gi-LAN that provides value-added IP-based services e.g. NAT, anti-malware, parental control, DDoS protection.

TDF session: An association between an IP-CAN session and the assigned TDF for the purpose of application detection and control.

uplink bearer binding verification: The network enforcement of terminal compliance with the negotiated uplink traffic mapping to bearers.

For the purposes of the present document, the following terms and definitions given in TS 23.401 [17] apply:

Narrowband-IoT: See TS 23.401 [17].

WB-E-UTRAN: See TS 23.401 [17].

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [8] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [8].

ADC	Application Detection and Control
AF	Application Function
AMBR	Aggregated Maximum Bitrate
ARP	Allocation and Retention Priority
ASP	Application Service Provider
BBERF	Bearer Binding and Event Reporting Function
BBF	Bearer Binding Function
BBF AAA	Broadband Forum AAA
BNG	Broadband Network Gateway
BPCF	Broadband Policy Control Function
BRAS	Broadband Remote Access Server
CSG	Closed Subscriber Group
CSG ID	Closed Subscriber Group Identity
DRA	Diameter Routing Agent
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
H-PCEF	A PCEF in the HPLMN
H-PCRF	A PCRF in the HPLMN
HRPD	High Rate Packet Data
HSGW	HRPD Serving Gateway
IP-CAN	IP Connectivity Access Network
MPS	Multimedia Priority Service
NB-IoT	Narrowband IoT
NBIFOM	Network-based IP flow mobility
NSWO	Non-Seamless WLAN Offload
OAM	Operation Administration and Maintenance
OFCS	Offline Charging System
OCS	Online Charging System
PCC	Policy and Charging Control
PCEF	Policy and Charging Enforcement Function
PCRF	Policy and Charging Rules Function
PFDF	Packet Flow Description Function
PRA	Presence Reporting Area
QCI	QoS Class Identifier
RAN	Radio Access Network
RCAF	RAN Congestion Awareness Function

RLOS	Restricted Local Operator Services
RUCI	RAN User Plane Congestion Information
RG	Residential Gateway
SCEF	Service Capability Exposure Function
vSRVCC	video Single Radio Voice Call Continuity
SPR	Subscription Profile Repository
TDF	Traffic Detection Function
TSSF	Traffic Steering Support Function
UDC	User Data Convergence
UDR	User Data Repository
V-PCEF	A PCEF in the VPLMN
V-PCRF	A PCRF in the VPLMN
WB-E-UTRAN	Wide Band E-UTRAN

4 High level requirements

4.1 General requirements

It shall be possible for the PCC architecture to base decisions upon subscription information.

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.).

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].

The PCC architecture shall discard packets that don't match any service data flow of the active PCC rules. It shall also be possible for the operator to define PCC rules, with wild-carded service data flow filters, to allow for the passage and charging for packets that do not match any service data flow template of any other active PCC rules.

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

The PCC architecture shall have a binding method that allows the unique association between service data flows and their IP-CAN bearer.

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

A PCC rule may be predefined or dynamically provisioned at establishment and during the lifetime of an IP-CAN session. The latter is referred to as a dynamic PCC rule.

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.

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

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

PCC shall be enabled on a per 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.

PCC shall support roaming users.

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

The PCC architecture shall support topology hiding.

It should be possible to use PCC architecture for handling IMS-based emergency service and Restricted Local Operator Services.

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.

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

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

The PCC architecture shall support making policy decisions based on RAN user plane congestion status.

The PCC architecture shall support making policy decisions for multi-access IP flow mobility solution described in TS 23.161 [43].

The PCC architecture shall support making policy decisions for (S)Gi-LAN traffic steering.

4.2 Charging related requirements

4.2.1 General

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.

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.

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.

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.

4.2.2 Charging models

The PCC charging shall support the following charging models both for charging performed by PCEF and charging performed by TDF:

- Volume based charging;
- Time based charging;
- Volume and time based charging;
- Event based charging;
- No charging.

NOTE 1: The charging model - "No charging" implies that charging control is not applicable.

Shared revenue services shall be supported. In this case settlement for all parties shall be supported, including the third parties that may have been involved providing the services.

NOTE 2: When developing a charging solution, the PCC charging models may be combined to form the solution. How to achieve a specific solution is however not within the scope of this TS.

NOTE 3: The Event based charging defined in this specification applies only to session based charging as defined by the charging specifications.

4.2.2a Charging requirements

The requirements in this clause apply to both PCC rules based charging and ADC rules based charging unless exceptions are explicitly mentioned.

It shall be possible to apply different rates and charging models when a user is identified to be roaming from when the user is in the home network. Furthermore, it shall be possible to apply different rates and charging models based on the location of a user, beyond the granularity of roaming.

It shall be possible to apply different rates and charging models when a user consuming network services via a CSG cell or a hybrid cell according to the user CSG information. User CSG information includes CSG ID, access mode and CSG membership indication.

It shall be possible to apply a separate rate to a specific service, e.g. allow the user to download a certain volume of data, reserved for the purpose of one service for free, and then continue with a rate causing a charge.

It shall be possible to change the rate based on the time of day.

It shall be possible to enforce per-service identified by PCC Rule/per-application identified by ADC Rule usage limits for a service data flow using online charging on a per user basis (may apply to prepaid and post-paid users).

It shall be possible to apply different rates depending on the access used to carry a Service Data Flow. This applies also to a PDN connection supporting NBIFOM.

It shall be possible for the online charging system to set and send the thresholds (time and/or volume based) for the amount of remaining credit to the PCEF or TDF for monitoring. In case the PCEF or TDF detects that any of the time based or volume based credit falls below the threshold, the PCEF or TDF shall send a request for credit re-authorization to the OCS with the remaining credit (time and/or volume based).

It shall be possible for the charging system to select the applicable rate based on:

- home/visited IP-CAN;
- User CSG information;
- IP-CAN bearer characteristics (e.g. QoS);
- QoS provided for the service;
- time of day;
- IP-CAN specific parameters according to Annex A.

IP-CAN bearer characteristics are not applicable to charging performed in TDF.

NOTE 1: The same IP-CAN parameters related to access network/subscription/location information as reported for service data flow based charging may need to be reported for the application based charging at the beginning of the session and following any of the relevant re-authorization triggers.

The charging system maintains the tariff information, determining the rate based on the above input. Thus the rate may change e.g. as a result of IP-CAN session modification to change the bearer characteristics provided for a service data flow.

The charging rate or charging model applicable to a service data flow/detected application traffic may change as a result of events in the service (e.g. insertion of a paid advertisement within a user requested media stream).

The charging model applicable to a service data flow/detected application traffic may change as a result of events identified by the OCS (e.g. after having spent a certain amount of time and/or volume, the user gets to use some services for free).

The charging rate or charging model applicable to a service data flow/detected application traffic may change as a result of having used the service data flow/detected application traffic for a certain amount of time and/or volume.

For online charging, it shall be possible to apply an online charging action upon PCEF or TDF events (e.g. re-authorization upon QoS change).

It shall be possible to apply an online charging action for detected application upon Application Start/Stop events.

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 the service data flow/detected application traffic, and then no offline charging information is generated.

This specification supports charging and enforcement being done in either the PCEF or the TDF for a certain IP-CAN session, but not both for the same IP-CAN session (applies to all IP-CAN sessions belonging to the same APN).

NOTE 2: The above requirement is to ensure that there is no double charging in both TDF and PCEF or over charging in case of packet discarded at PCEF or TDF.

4.2.3 Examples of Service Data Flow Charging

There are many different services that may be used within a network, including both user-user and user-network services. Service data flows from these services may be identified and charged in many different ways. A number of examples of configuring PCC rules for different service data flows are described below.

EXAMPLE 1: A network server provides an FTP service. The FTP server supports both the active (separate ports for control and data) and passive modes of operation. A PCC rule is configured for the service data flows associated with the FTP server for the user. The PCC rule uses a filter specification for the uplink that identifies packets sent to port 20 or 21 of the IP address of the server, and the origination information is wildcarded. In the downlink direction, the filter specification identifies packets sent from port 20 or 21 of the IP address of the server.

EXAMPLE 2: A network server provides a "web" service. A PCC rule is configured for the service data flows associated with the HTTP server for the user. The PCC rule uses a filter specification for the uplink that identifies packets sent to port 80 of the IP address of the server, and the origination information is wildcarded. In the downlink direction, the filter specification identifies packets sent from port 80 of the IP address of the server.

EXAMPLE 3: The same server provides a WAP service. The server has multiple IP addresses, and the IP address of the WAP server is different from the IP address of the web server. The PCC rule uses the same filter specification as for the web server, but with the IP addresses for the WAP server only.

EXAMPLE 4: An operator offers a zero rating for network provided DNS service. A PCC rule is established setting all DNS traffic to/from the operators DNS servers as offline charged. The data flow filter identifies the DNS port number, and the source/destination address within the subnet range allocated to the operators network nodes.

EXAMPLE 5: An operator has a specific charging rate for user-user VoIP traffic over the IMS. A PCC rule is established for this service data flow. The filter information to identify the specific service data flow for the user-user traffic is provided by the P-CSCF (AF).

EXAMPLE 6: An operator is implementing UICC based authentication mechanisms for HTTP based services utilizing the GAA Framework as defined in TR 33.919 [11] by e.g. using the Authentication Proxy. The Authentication Proxy may appear as an AF and provide information to the PCRF for the purpose of selecting an appropriate PCC Rule.

4.3 Policy control requirements

4.3.1 General

The policy control features comprise gating control and QoS control.

The concept of QoS class identifier and the associated bitrates specify the QoS information for service data flows and bearers on the Gx and Gxx reference points.

4.3.2 Gating control

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

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

4.3.3 QoS control

4.3.3.1 QoS control at service data flow level

It shall be possible to apply QoS control on a per service data flow basis in the PCEF.

QoS control per service data flow allows the PCC architecture to provide the PCEF 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.

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

4.3.3.2 QoS control at IP-CAN bearer level

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 predefined 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.

It shall be possible for the PCC architecture to support control of QoS for the packet traffic of IP-CANs.

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

The IP-CAN shall prevent cyclic QoS upgrade attempts due to failed QoS upgrades.

NOTE: These measures are IP-CAN specific.

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).

4.3.3.3 QoS Conflict Handling

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.

4.3.3.4 QoS control at APN level

It shall be possible for the PCRF to authorize the APN-AMBR to be enforced by the PCEF as defined in 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.

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.

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.

The details are specified in clause 6.4b.

4.3.4 Subscriber Spending Limits

It shall be possible to enforce policies based on subscriber spending limits as per TS 22.115 [27]. The OCS shall maintain policy counter(s) to track spending for a subscription. These policy counters must be available in the OCS prior to their use over the Sy interface.

NOTE 1: The mechanism for provisioning the policy counters in the OCS is out of scope of this document.

NOTE 2: A policy counter in the OCS can represent the spending for one or more services, one or more devices, one or more subscribers, etc. The representation is operator dependent. There is no explicit relationship between Charging-Key and policy counter.

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. The OCS shall make information regarding the subscriber's spending available to the PCRF using spending limit reports.

4.4 Usage Monitoring Control

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.

The PCRF that uses 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 on 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. If both time and volume thresholds were provided to the PCEF or TDF, the accumulated usage since last report shall be reported when either the time or the volume thresholds are reached.

NOTE: There are reasons other than reaching a threshold that may cause the PCEF/TDF to report accumulated usage to the PCRF as defined in clauses 6.2.2.3 and 6.6.2.

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. 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. 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.

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. 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. 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.

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).

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. IP-CAN session level usage monitoring is not dependent on the access used to carry a Service Data Flow.

4.5 Application Detection and Control

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.

Two models may be applied, depending on operator requirements: solicited and unsolicited application reporting. The unsolicited application reporting is only supported by the TDF.

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. 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.

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.

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.

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.

NOTE 1: The reporting to the PCRF on the start or stop of application traffic is not depending on any enforcement action of the ADC/PCC rule. Unless the PCRF muted the reporting for the ADC/PCC rule, every detected start or stop event is reported even if the application traffic is discarded due to enforcement actions of the ADC/PCC rule.

For the TDF operating in the solicited application reporting model:

- When the TDF cannot provide to the PCRF the service data flow description for the detected applications, the TDF shall perform charging, gating, redirection and bandwidth limitation for the detected applications, as defined in the ADC rule. The existing PCEF functionality remains unchanged.

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).

- 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.

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.

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.

In order to avoid charging for the same traffic in both the TDF and the PCEF, this specification supports charging and enforcement implemented in either the PCEF or the TDF for a certain IP-CAN session, but not both for the same IP-CAN session.

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.

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 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.

NOTE 5: The PCEF may still do enforcement actions on uplink traffic without impacting the accuracy of the charging information produced by the TDF.

If only charging for a service data flow identified by a PCC Rule is required for the corresponding IP-CAN session, the PCEF performs charging and policy enforcement for the IP-CAN session. The TDF may be used for application detection and reporting of application start/stop and for enforcement actions on downlink traffic.

4.6 RAN user plane congestion detection, reporting and mitigation

It shall be possible to transfer RAN user plane congestion information from the RAN to the Core Network in order to mitigate the congestion by measures selected by the PCRF and applied by the PCEF/TDF/AF. The detailed description of this functionality can be found in TS 23.401 [17] and TS 23.060 [12].

4.7 Support for service capability exposure

It shall be possible to transfer information related to service capability exposure between the PCRF and the AF via an SCEF (see TS 23.682 [42]).

4.8 Traffic Steering Control

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

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

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

Management of Packet Flow Descriptions in the PCEF/TDF using the PFDF refers to the capability to create, update or remove PFDs in the PFDF via the SCEF (as described in TS 23.682 [42]) and the distribution from the PFDF to the PCEF or the TDF or both. This feature may be used when the PCEF or the TDF is configured to detect a particular application provided by an ASP.

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

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

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

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

5 Architecture model and reference points

5.1 Reference architecture

The PCC functionality is comprised by the functions of the Policy and Charging Enforcement Function (PCEF), the Bearer Binding and Event Reporting Function (BBERF), the Policy and Charging Rules Function (PCRF), the Application Function (AF), the Traffic Detection Function (TDF), the Traffic Steering Support Function (TSSF), the Online Charging System (OCS), the Offline Charging System (OFCS) and the Subscription Profile Repository (SPR) or the User Data Repository (UDR). UDR replaces SPR when the UDC architecture as defined in TS 23.335 [25] is applied to store PCC related subscription data. In this deployment scenario Ud interface between PCRF and UDR is used to access subscription data in the UDR.

NOTE 1: When UDC architecture is used, SPR and Sp, whenever mentioned in this document, can be replaced by UDR and Ud.

The PCRF can receive RAN User Plane Congestion Information from the RAN Congestion Awareness Function (RCAF).

The PCC architecture extends the architecture of an IP-CAN, where the Policy and Charging Enforcement Function is a functional entity in the Gateway node implementing the IP access to the PDN. The allocation of the Bearer Binding and Event Reporting Function is specific to each IP-CAN type and specified in the corresponding Annex.

The non-3GPP network relation to the PLMN is the same as defined in TS 23.402 [18].

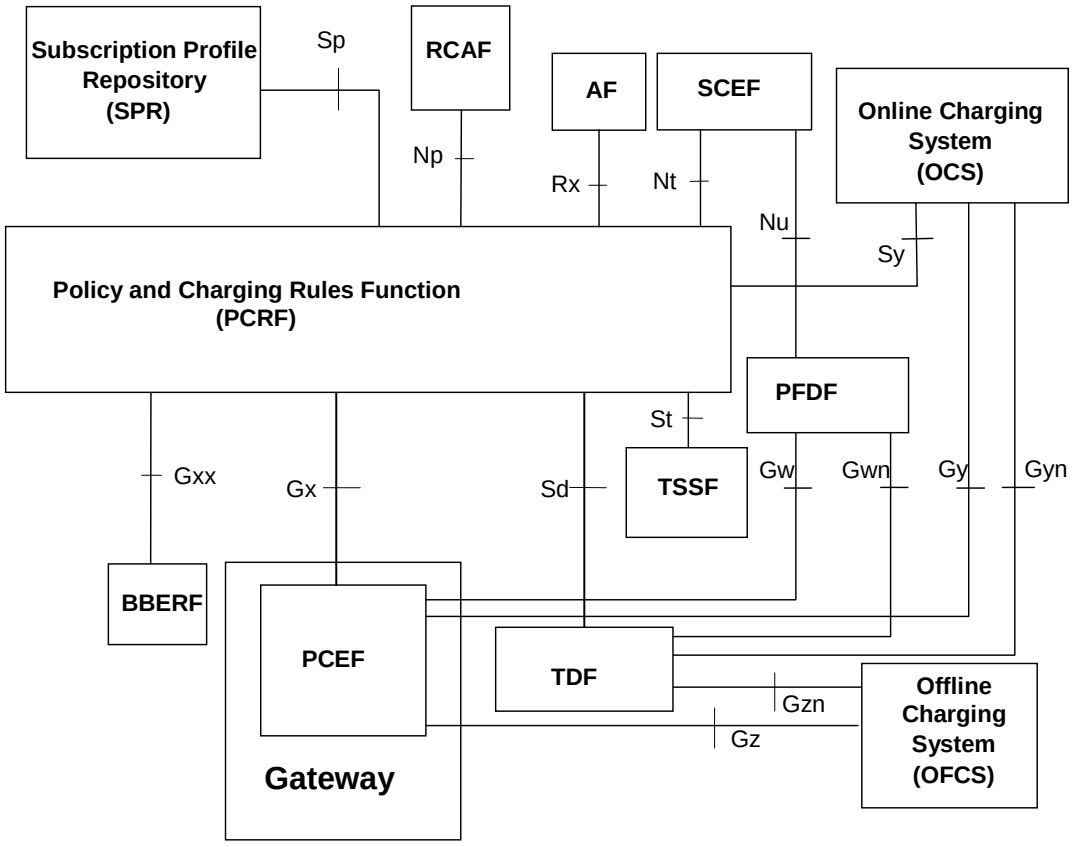

Figure 5.1-1: Overall PCC logical architecture (non-roaming) when SPR is used

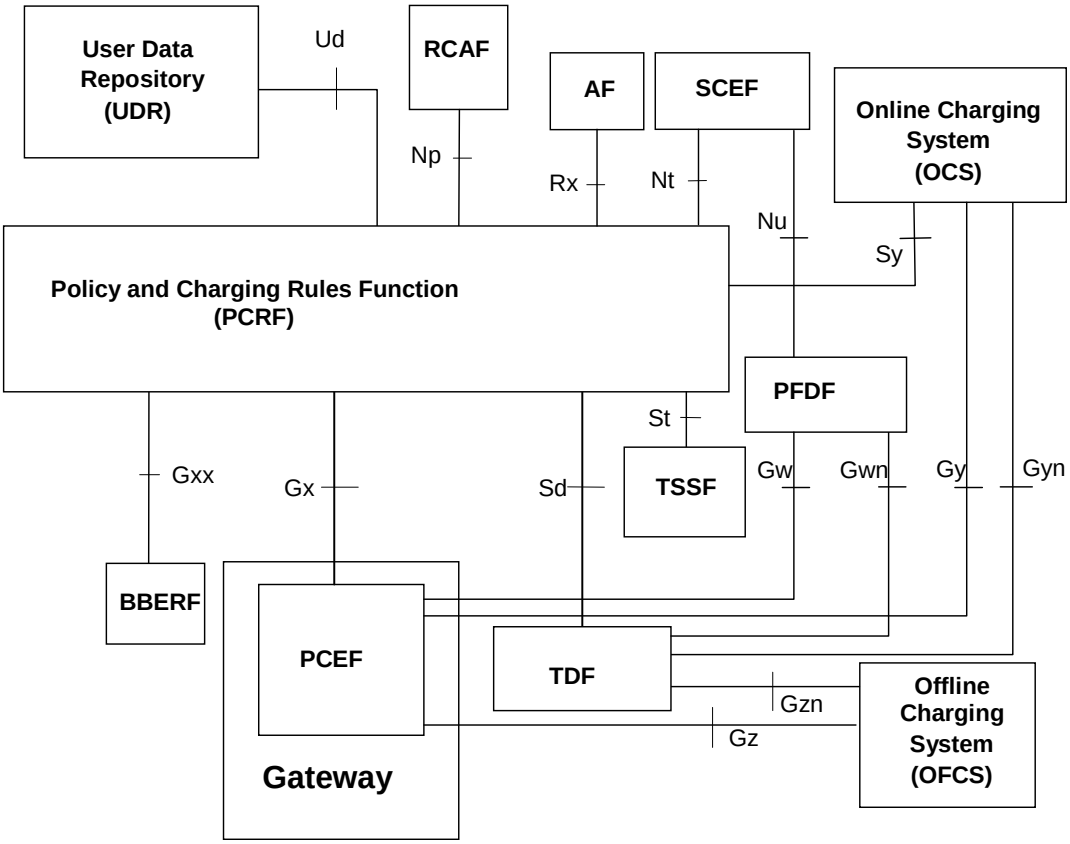

Figure 5.1-2: Overall PCC logical architecture (non-roaming) when UDR is used

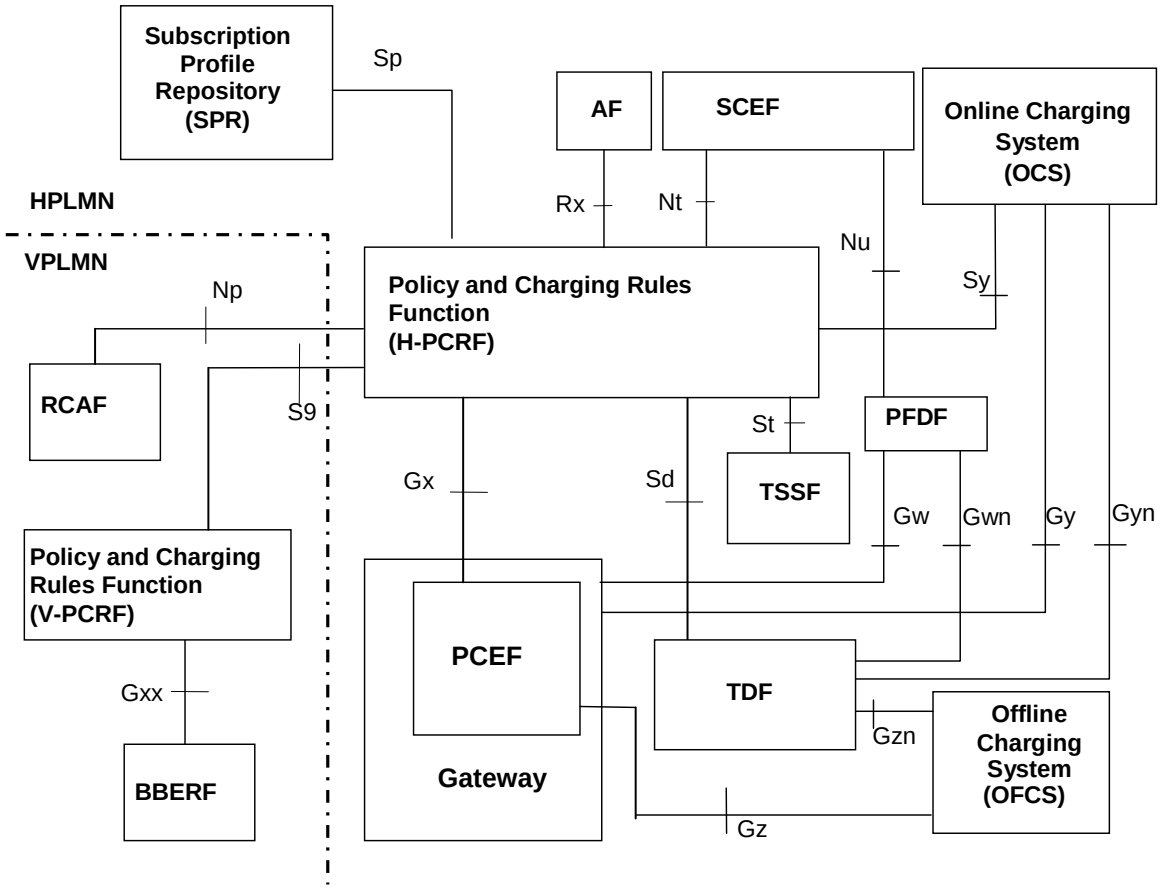

Figure 5.1-3: Overall PCC architecture (roaming with home routed access) when SPR is used

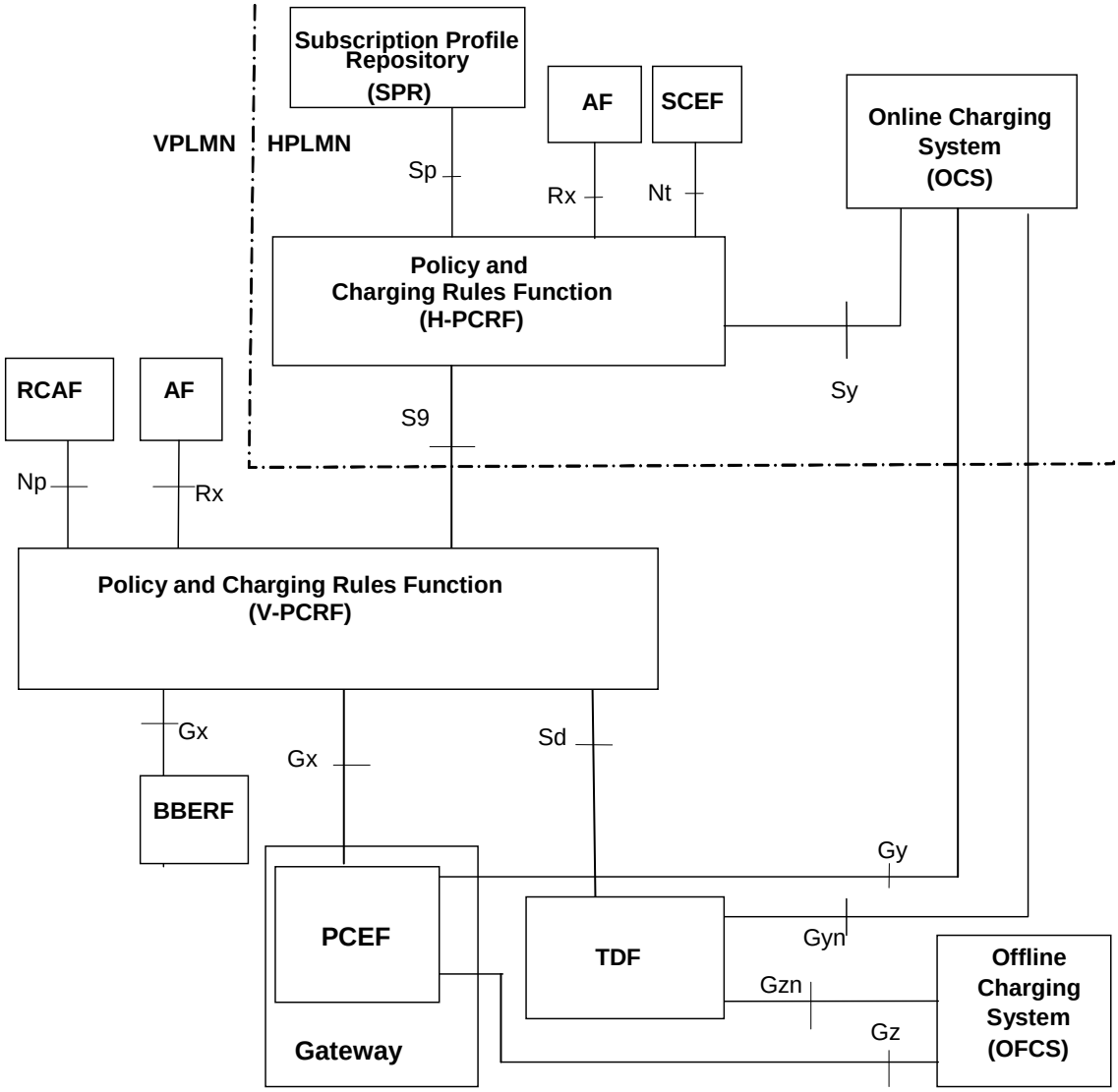

Figure 5.1-4: Overall PCC architecture for roaming with PCEF in visited network (local breakout) when SPR is used

NOTE 2: Similar figures for the roaming cases apply when UDR is used instead of SPR and Ud instead of Sp.

NOTE 3: PCEF may be enhanced with application detection and control feature.

NOTE 4: In general, Gy and Gyn don't apply for the same IP-CAN session, and Gz and Gzn also doesn't apply for the same IP-CAN session. For the description of the case where simultaneous reports apply, please refer to the clause 4.5).

NOTE 5: RCAF also supports Nq/Nq' interfaces for E-UTRAN and UTRAN as specified in TS 23.401 [17] and TS 23.060 [12], respectively.

NOTE 6: Use of TSSF in roaming scenarios is in this release only specified for the home routed access case.

NOTE 7: The SCEF acts as an AF (using Rx) in some service capability exposure use cases as described in TS 23.682 [42].

NOTE 8: Gw and Gwn interface are not supported in roaming scenario with PCEF/TDF in visited network.

5.2 Reference points

5.2.1 Rx reference point

The Rx reference point resides between the AF and the PCRF.

NOTE 1: The AF may be a third party application server.

This reference point enables transport of application level session information from AF to PCRF. Such information includes, but is not limited to:

- IP filter information to identify the service data flow for policy control and/or differentiated charging;
- Media/application bandwidth requirements for QoS control.
- In addition, for sponsored data connectivity:
  - the sponsor's identification,
  - optionally, a usage threshold and whether the PCRF reports these events to the AF,
  - information identifying the application service provider and application (e.g. SDFs, application identifier, etc.).

The Rx reference point enables the AF subscription to notifications on IP-CAN bearer level events (e.g. signalling path status of AF session) in the IP-CAN.

In order to mitigate RAN user plane congestion, the Rx reference point enables transport of the following information from the PCRF to the AF:

- Re-try interval, which indicates when service delivery may be retried on Rx.

NOTE 2: Additionally, existing bandwidth limitation parameters on Rx interface during the Rx session establishment are available in order to mitigate RAN user plane congestion.

5.2.2 Gx reference point

The Gx reference point resides between the PCEF and the PCRF.

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;
- 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;
- Provision of PCC decision from the PCRF to the PCEF;
- 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;
- Reporting of the accumulated usage of network resources on a per IP-CAN session basis from the PCEF to the PCRF;
- Delivery of IP-CAN session specific parameters from the PCEF to the PCRF or, if Gxx is deployed, from the PCRF to the PCEF per corresponding request;
- Negotiation of IP-CAN bearer establishment mode (UE-only or UE/NW);
- Termination of Gx session (corresponding to an IP-CAN session) by the PCEF or the PCRF.

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.

The information contained in a PCC rule is defined in clause 6.3.

5.2.3 Reference points to subscriber databases

5.2.3.1 Sp reference point

The Sp reference point lies between the SPR and the PCRF.

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.

NOTE: The details associated with the Sp reference point are not specified in this Release.

5.2.3.2 Ud reference point

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.

The details for this reference point are described in TS 23.335 [25] and TS 29.335 [26].

5.2.4 Gy reference point

The Gy reference point resides between the OCS and the PCEF.

The Gy reference point allows online credit control for service data flow based charging. The functionalities required across the Gy reference point are defined in TS 32.251 [9] and is based on RFC 4006 [4].

5.2.5 Gz reference point

The Gz reference point resides between the PCEF and the OFCS.

The Gz reference point enables transport of service data flow based offline charging information.

The Gz interface is specified in TS 32.240 [3].

5.2.6 S9 reference point

The S9 reference point resides between a PCRF in the HPLMN (H-PCRF) and a PCRF in the VPLMN (V-PCRF).

For roaming with a visited access (PCEF and, if applicable, BBERF in the visited network), the S9 reference point enables the H-PCRF to (via the V-PCRF):

- have dynamic PCC control, including the PCEF and, if applicable, BBERF, and, if applicable, TDF, in the VPLMN;
- deliver or receive IP-CAN-specific parameters from both the PCEF and, if applicable, BBERF, in the VPLMN;
- serve Rx authorizations and event subscriptions from an AF in the VPLMN;
- receive application identifier, service data flow descriptions, if available, application instance identifiers, if available, and application detection start/stop event triggers report.

For roaming with a home routed access, the S9 enables the H-PCRF to provide dynamic QoS control policies from the HPLMN, via a V-PCRF, to a BBERF in the VPLMN.

5.2.7 Gxx reference point

The Gxx reference point resides between the PCRF and the BBERF. This reference point corresponds to the Gxa and Gxc, as defined in TS 23.402 [18] and further detailed in the annexes.

The Gxx reference point enables a PCRF to have dynamic control over the BBERF behaviour.

The Gxx reference point enables the signalling of QoS control decisions and it supports the following functions:

- Establishment of Gxx session by BBERF;

  Termination of Gxx session by BBERF or PCRF;

- Establishment of Gateway Control Session by the BBERF;
- Termination of Gateway Control Session by the BBERF or PCRF;
- Request for QoS decision from BBERF to PCRF;
- Provision of QoS decision from PCRF to BBERF;
- Delivery of IP-CAN-specific parameters from PCRF to BBERF or from BBERF to PCRF;
- Negotiation of IP-CAN bearer establishment mode (UE-only and UE/NW).

A QoS control decision consists of zero or more QoS rule(s) and IP-CAN attributes. The information contained in a QoS rule is defined in clause 6.5.

NOTE: The Gxx session serves as a channel for communication between the BBERF and the PCRF. A Gateway Control Session utilizes the Gxx session and operates as defined in TS 23.402 [18], which includes both the alternatives as defined by cases 2a and 2b in clause 7.1.

5.2.8 Sd reference point

The Sd reference point resides between the PCRF and the TDF.

The Sd reference point enables a PCRF to have dynamic control over the application detection and control behaviour at a TDF.

The Sd reference point enables the signalling of ADC decision, which governs the ADC behaviour, and it supports the following functions:

1. Establishment of Sd session between the PCRF and the TDF;
2. Termination of Sd session between the PCRF and the TDF;
3. Provision of ADC decision from the PCRF for the purpose of application's traffic detection, enforcement and charging at the TDF;
4. Request for ADC decision from the TDF to the PCRF;
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;
6. Reporting of the accumulated usage of network resources on a per TDF session basis from the TDF to the PCRF;
7. Request and delivery of IP-CAN session specific parameters between the PCRF and the TDF.

   While 1-7 are relevant for solicited application reporting; only 1, 2 and 5 are relevant for unsolicited application reporting.

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.

The information contained in an ADC rule is defined in clause 6.8.

5.2.9 Sy reference point

The Sy reference point resides between the PCRF and the OCS.

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).
- Report of policy counter status information upon a PCRF request from OCS to PCRF.
- Notification of spending limit reports from OCS to PCRF.
- Cancellation of spending limit reporting from PCRF to OCS.

Since the Sy reference point resides between the PCRF and OCS in the HPLMN, roaming with home routed or visited access as well as non-roaming scenarios are supported in the same manner.

5.2.10 Gyn reference point

The Gyn reference point resides between the OCS and the TDF.

The Gyn reference point allows online credit control for charging in case of ADC rules based charging in TDF. The functionalities required across the Gyn reference point are defined in TS 32.251 [9] and is based on RFC 4006 [4].

5.2.11 Gzn reference point

The Gzn reference point resides between the TDF and the OFCS.

The Gzn reference point enables transport of offline charging information in case of ADC rule based charging in TDF.

The Gzn interface is specified in TS 32.240 [3].

5.2.12 Np reference point

The Np reference point resides between the RCAF and the PCRF.

The Np reference point enables transport of RAN User Plane Congestion Information (RUCI) sent from the RCAF to the PCRF for all or selected subscribers, depending on the operator's congestion mitigation policy.

The Np reference point supports the following functions:

- Reporting of RUCI from the RCAF to the PCRF.
- Sending, updating and removal of the reporting restrictions from the PCRF to the RCAF as defined in clause 6.1.15.2.

5.2.13 Nt reference point

The Nt reference point enables the negotiation between the SCEF and the PCRF about the recommended time window(s) and the related conditions for future background data transfer. The SCEF is triggered by an SCS/AS (as described in TS 23.682 [42]) which requests for this negotiation and provides necessary information to the SCEF. The SCEF will forward the information received from the SCS/AS to the PCRF as well as the information received from the PCRF to the SCS/AS.

Whenever the SCEF contacts the PCRF, the PCRF shall use the information provided by the SCS/AS via the SCEF to determine the policies belonging to the application service provider (ASP).

NOTE: This interaction between the SCEF and the PCRF over the Nt reference point is not related to any IP-CAN session.

5.2.14 St reference point

The St reference point resides between the TSSF and the PCRF.

The St reference point enables the PCRF to provide traffic steering control information to the TSSF.

The St reference point supports the following functions:

- Provision, modification and removal of traffic steering control information from PCRF to the TSSF.

5.2.15 Nu reference point

The Nu reference point resides between the SCEF and the PFDF, and enables the 3rd party service provider to manage PFDs in the PFDF as specified in TS 23.682 [42].

5.2.16 Gw reference point

The Gw reference point resides between the PFDF and the PCEF.

The Gw reference point enables transport of PFDs from the PFDF to the PCEF for a particular Application Identifier or for a set of Application Identifiers.

The Gw reference point supports the following functions:

- Creation, updating and removal of individual or the whole set of PFDs from the PFDF to the PCEF.
- Confirmation of creation, updating and removel of PFDs from the PCEF to the PFDF.

NOTE: The interaction between the PCEF and the PFDF is not related to any IP-CAN session.

5.2.17 Gwn reference point

The Gwn reference point resides between the PFDF and the TDF.

The Gwn reference point enables transport of PFDs from the PFDF to the TDF for a particular Application Identifier or for a set of Application Identifiers.

The Gwn reference point supports the following functions:

- Creation, updating and removal of individual or the whole set of PFDs from the PFDF to the TDF.
- Confirmation of creation, updating and removel of PFDs from the PCEF to the TDF.

NOTE: The interaction between the PCEF and the TDF is not related to any IP-CAN session.

6 Functional description

6.1 Overall description

6.1.0 General

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.

6.1.1 Binding mechanism

6.1.1.1 General

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

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

NOTE 3: For PCC rules with application identifier, and for certain IP-CAN types, up-link traffic may be received on other/additional IP-CAN bearers than the one determined by the binding mechanism (further details provided in clause 6.2.2.2 and the IP-CAN specific annexes).

The binding mechanism creates bindings. The algorithm, employed by the binding mechanism, may contain elements specific for the kind of IP-CAN.

The binding mechanism includes three steps:

1. Session binding.

2 PCC rule authorization and QoS rule generation, if applicable.

3. Bearer binding.

6.1.1.2 Session binding

Session binding is the association of the AF session information to one and only one IP-CAN session.

The PCRF shall perform the session binding, which shall take the following IP-CAN parameters into account:

a) The UE IPv4 address and/or IPv6 network prefix;

b) The UE identity (of the same kind), if present.

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.

c) The information about the packet data network (PDN) the user is accessing, if present.

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 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.

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.

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.

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.

6.1.1.3 PCC rule authorization and QoS rule generation

PCC Rule authorization is the selection of the QoS parameters (QCI, ARP, GBR, MBR, etc.) for the PCC rules.

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).

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:

- In UE/NW bearer establishment mode, the PCRF shall perform the authorization for all PCC rules that are to be handled in NW mode.

- 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.

  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 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.

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.

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 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.

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.

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.

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).

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 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.

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.

NOTE 4: This is required to enable services that start before dedicated resources are allocated.

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.

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 and Restricted Local Operator Services shall be supported without subscription information (e.g. information stored in the SPR). The PCRF shall apply policies configured for the emergency service and Restricted Local Operator Services.

When both a Gx and associated Gxx interface(s) 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.

When flow mobility applies for the IP-CAN Session, one IP-CAN session may be associated to multiple Gateway Control Sessions with separate BBRFs. 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.

6.1.1.4 Bearer Binding

Bearer binding is the association of the PCC rule and the QoS rule (if applicable) to an IP-CAN bearer within that IP-CAN session. This function resides in the Bearer Binding Function (BBF).

The Bearer Binding Function is located either at the BBERF or at the PCEF, depending on the architecture (see clause 5.1). The BBF is located at the PCEF if GTP is used as the mobility protocol towards the PCEF; otherwise, the BBF is located at the BBERF.

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.

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 the PCC rule and the QoS rule (if applicable) authorized in the previous step.

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. The BBF should not use the same bearer for rules with different settings for the PS to CS session continuity indicator.

NOTE 2: When NBIFOM applies for the IP-CAN session, additional information has to be taken into account as described in clause 6.1.18.1.

The BBF shall evaluate whether it is possible to use one of the existing IP-CAN bearers or not and whether initiate IP-CAN bearer modification if applicable. If none of the existing bearers are possible to use, the BBF should initiate the establishment of a suitable IP-CAN bearer. The binding is created between service data flow(s) and the IP-CAN bearer which have the same QoS class identifier and ARP.

NOTE 3: The handling of a rule with MBR>GBR is up to operator policy (e.g. an independent IP-CAN bearer may be maintained for that SDF to prevent unfairness between competing SDFs).

Requirements, specific for each type of IP-CAN, are defined in the IP-CAN specific Annex.

Whenever the QoS authorization of a PCC/QoS rule changes, the existing bindings 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. The BBF should, if the PCRF requests the same change to the ARP/QCI value for all PCC/QoS Rules with the bearer binding to the same bearer, modify the bearer ARP/QCI value as requested.

NOTE 4: A QoS change of the default EPS bearer causes the bearer binding for PCC/QoS rules previously bound to the default EPS bearer to be re-evaluated. At the end of the re-evaluation of the PCC/QoS rules of the IP-CAN session, there needs to be at least one PCC rule that successfully binds with the default bearer.

6.1.2 Reporting

Reporting refers to the differentiated IP-CAN resource usage information (measured at the PCEF/TDF) being reported to the online or offline charging functions.

NOTE 1: Reporting usage information to the online charging function is distinct from credit management. Hence multiple PCC/ADC rules may share the same charging key for which one credit is assigned whereas reporting may be at higher granularity if serviced identifier level reporting is used.

The PCEF/TDF shall report usage information for online and offline charging.

The PCEF/TDF shall report usage information for each charging key value.

For service data flow charging, for the case of sponsored data connectivity, the reports for offline charging shall report usage for each charging key, Sponsor Identity and Application Service Provider Identity combination if Sponsor Identity and Application Service Provider Identifier have been provided in the PCC rules.

NOTE 2: Usage reports for online charging that include Sponsor Identity and Application Service Provider Identity is not within scope of the specification in this release. Online charging for sponsored data connectivity can be based on charging key as described in Annex N.

The PCEF shall report usage information for each charging key/service identifier combination if service identifier level reporting is requested in the PCC/ADC rule.

NOTE 3: For reporting purposes when charging is performed by the PCEF:

a) the charging key value identifies a service data flow if the charging key value is unique for that particular service data flow, and

b) if the service identifier level reporting is present then the service identifier value of the PCC rule together with the charging key identify the service data flow.

The TDF shall report usage information for each charging key/service identifier combination if service identifier level reporting is requested in the ADC rule.

NOTE 4: For reporting purposes in case charging is performed by the TDF a) the charging key value identifies an application if the charging key value is unique for that application identified by ADC Rule and b) if the service identifier level reporting is present then the service identifier value of the ADC rule together with the charging key identify the application

NOTE 5: If operator applies this solution with both PCEF and TDF performing enforcement and charging for a single IP-CAN session, the PCRF is recommended to use a different charging keys provided to the PCEF and to the TDF.

For the case where the BBF locates in the PCEF, charging information shall be reported based on the result from the service data flow detection and measurement on a per IP-CAN bearer basis.

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.

A report may contain multiple containers, each container associated with a charging key, charging key and Sponsor Identity (in case of sponsored connectivity) or charging key/service identifier.

6.1.3 Credit management

The credit management applies for online charging only and shall operate on a per charging key basis. The PCEF should initiate one credit management session with the OCS for each IP-CAN Session subject to online charging, unless specified otherwise in an IP-CAN specific annex. Alternatively, the PCEF may initiate one credit management session for each IP-CAN bearer as defined in the applicable annex. The TDF should initiate one credit management session with the OCS for each TDF Session subject to online charging.

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

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

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

During IP-CAN session establishment and modification, the PCEF shall request credit using the information after applying policy enforcement action (e.g. upgraded or downgraded QoS information), if applicable, even though the PCEF has not signalled it yet in the IP-CAN.

It shall be possible for the OCS to form a credit pool for multiple (one or more) charging keys, applied at the PCEF/TDF, e.g. with the objective of avoiding credit fragmentation. Multiple pools of credit shall be allowed per IP-CAN bearer/TDF session. The OCS shall control the credit pooling decisions. The OCS shall, when credit authorization is sought, either grant a new pool of credit, together with a new credit limit, or give a reference to a pool of credit that is already granted for that IP-CAN bearer/TDF session. The grouping of charging keys into pools shall not restrict the ability of the OCS to do credit authorisation and provide termination action individually for each charging key of the pool. It shall be possible for the OCS to group service data flows/applications charged at different rates or in different units (e.g. time/volume/event) into the same pool.

For each charging key, the PCEF/TDF may receive credit re-authorisation trigger information from the OCS, which shall cause 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.

Table 6.1: Credit re-authorization triggers

Credit re-authorization trigger	Description	Applicable for
Credit authorisation lifetime expiry	The OCS has limited the validity of the credit to expire at a certain time.	PCEF, TDF
Idle timeout	The service data flow identified by a PCC Rules or the application identified by an ADC Rule has been empty for a certain time.	PCEF, TDF
PLMN change	The UE has moved to another operators' domain.	PCEF, TDF
QoS changes	The QoS of the IP-CAN bearer has changed.	PCEF
Change in type of IP-CAN	The type of the IP-CAN has changed.	PCEF, TDF
Location change (serving cell)	The serving cell of the UE has changed.	PCEF, TDF
Location change (serving area) (see note 2)	The serving area of the UE has changed.	PCEF, TDF
Location change (serving CN node) (see note 3)	The serving core network node of the UE has changed.	PCEF, TDF
Change of UE presence in Presence Reporting Area (see note 4)	The UE has entered or left a Presence Reporting Area	PCEF, TDF
NOTE 1: This list is not exhaustive. Events specific for each IP-CAN are specified in Annex A, and the protocol description may support additional events. NOTE 2: A change in the serving area may also result in a change in the serving cell, and possibly a change in the serving CN node. NOTE 3: A change in the serving CN node may also result in a change in the serving cell, and possibly a change in the serving area. NOTE 4: The Presence Reporting Area(s) is provided by the OCS to the PCEF/TDF. The maximum number of PRA(s) per UE per PDN connection is configured in the OCS. The OCS may have independent configuration of the maximum number for Core Network pre-configured PRAs and UE-dedicated PRAs. The exact number(s) should be determined by operator in deployment.		

If the Location change trigger is armed, the PCEF shall activate the relevant IP-CAN specific procedure which reports any changes in location to the level indicated by the trigger. If credit-authorization triggers and event triggers require different levels of reporting of location change for a single UE, the location to be reported should be changed to the highest level of detail required. However, there should be no request being triggered for credit re-authorization to the OCS if the report received is more detailed than requested by the OCS.

NOTE 1: The access network may be configured to report location changes only when transmission resources are established in the radio access network.

The OCS determines at credit management 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 OCS may subscribe to Change of UE presence in Presence Reporting Area at any time during the life time of the credit management session.

NOTE 2: If Presence Reporting Area reporting is not supported, the OCS 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 reporting is only applied for a limited number of subscribers.

When activating reporting for change of UE presence in Presence Reporting Area, the OCS provides all of the PRA Identifier(s) to be activated for Core Network pre-configured Presence Reporting Area(s) and additionally all of PRA Identifier(s) and the list(s) of its elements for UE- dedicated Presence Reporting Area(s). (See Table 6.4 in clause 6.4 for details of the PRA Identifier(s) and the list(s) of elements comprising each Presence Reporting Area). If OCS is configured with a PRA identifier referring to the list of PRA Identifier(s) within a Set of Core Network predefined Presence Reporting Areas as defined in TS 23.401 [17], it activates the reporting of UE entering/leaving the individual PRA in the Set of Core Network predefined Presence Reporting Areas without providing the complete set of individual PRAs.

The OCS may change (activate/modify/remove) the Presence Reporting Area(s) to be reported by providing the updated PRA Identifier(s) to PCEF. For UE dedicated PRAs, the OCS may also change the list(s) of Presence Reporting Area elements related to the PRA Identifier(s).

The OCS may unsubscribe to Change of UE presence in Presence Reporting Area at any time during the life time of the credit management session.

The OCS may be notified during the life time of a credit management session that the UE is located in an access type where local OCS configuration indicates that reporting changes of UE presence in Presence Reporting Area is not supported. If so, the OCS unsubscribes to Change of UE presence in Presence Reporting Area, if previously activated.

Some of the re-authorization triggers are related to IP-CAN bearer modifications. IP-CAN bearer modifications, which do not match any credit re-authorization trigger (received from the OCS for the bearer) shall not cause any credit re-authorization interaction with the OCS.

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/ADC rules for which credit is no longer available together with the applied termination action.

6.1.4 Event Triggers

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 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.

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). If the provided event triggers are associated with certain parameter values then the ERF shall include those values in the response back to the PCRF. Event triggers are associated with all rules at the ERF of an IP-CAN session (ERF is located at PCEF) or Gateway Control session (ERF is located at BBERF) or with Traffic Detection session (ERF is located in TDF). Event triggers determine when the ERF shall signal to the PCRF that an IP-CAN bearer has been modified. It shall be possible for the ERF to react on the event triggers listed in table 6.2.

Table 6.2: Event triggers

Event trigger	Description	Reported from	Condition for reporting
PLMN change	The UE has moved to another operators' domain.	PCEF	PCRF
QoS change	The QoS of the IP-CAN bearer has changed (note 3).	PCEF, BBERF	PCRF
QoS change exceeding authorization	The QoS of the IP-CAN bearer has changed and exceeds the authorized QoS (note 3).	PCEF	PCRF
Traffic mapping information change	The traffic mapping information of the IP-CAN bearer has changed (note 3).	PCEF	Always set
Resource modification request	A request for resource modification has been received by the BBERF/PCEF (note 6).	PCEF, BBERF	Always set
Routing information change	The IP flow mobility routing information has changed (when IP flow mobility as specified in TS 23.261 [23] applies) or the PCEF has received Routing Rules from the UE (when NBIFOM as specified in TS 23.161 [43] applies) (note 11) (note 16).	PCEF	Always set (note 15)
Change in type of IP-CAN (see note 1)	The access type of the IP-CAN bearer has changed.	PCEF	PCRF
Loss/recovery of transmission resources	The IP-CAN transmission resources are no longer usable/again usable.	PCEF, BBERF	PCRF
Location change (serving cell) (see note 10)	The serving cell of the UE has changed.	PCEF, BBERF	PCRF
Location change (serving area) (see notes 4 and 10)	The serving area of the UE has changed.	PCEF, BBERF	PCRF
Location change (serving CN node) (see notes 5 and 10)	The serving core network node of the UE has changed.	PCEF, BBERF	PCRF
Change of UE presence in Presence Reporting Area (see note 17)	The UE is entering/leaving a Presence Reporting Area	PCEF, BBERF	PCRF
Out of credit	Credit is no longer available.	PCEF, TDF	PCRF
Enforced PCC rule request	PCEF is performing a PCC rules request as instructed by the PCRF.	PCEF	PCRF
Enforced ADC rule request	TDF is performing an ADC rules request as instructed by the PCRF.	TDF	PCRF
UE IP address change (see note 9)	A UE IP address has been allocated/released	PCEF	Always set
Access Network Charging Correlation Information	Access Network Charging Correlation Information has been assigned.	PCEF	PCRF
Usage report (see note 7)	The IP-CAN session or the Monitoring key specific resources consumed by a UE either reached the threshold or needs to be reported for other reasons.	PCEF, TDF	PCRF
Start of application traffic detection and Stop of application traffic detection (see note 8)	The start or the stop of application traffic has been detected.	PCEF, TDF	PCRF
SRVCC CS to PS handover	A CS to PS handover has been detected	PCEF	PCRF
Access Network Information report	Access information as specified in the Access Network Information Reporting part of a PCC rule.	PCEF, BBERF	PCRF
Credit management session failure	Transient/Permanent Failure as specified by the OCS	PCEF, TDF	PCRF for PCEF, Always set for TDF
Addition / removal of an access to an IP-CAN session (note 11)	The PCEF reports when an access is added or removed	PCEF	Always set
Change of usability of an access (note 11)	The PCEF reports that an access becomes unusable or usable again (note 14)	PCEF	Always set
UE resumed from suspend state	The PCEF reports to the PCRF when it detects that the UE is resumed from suspend state.	PCEF	PCRF

NOTE 1: This list is not exhaustive. Events specific for each IP-CAN are specified in clause A.
NOTE 2: A change in the type of IP-CAN may also result in a change in the PLMN.
NOTE 3: Available only when the bearer binding mechanism is allocated to the PCRF.
NOTE 4: A change in the serving area may also result in a change in the serving cell, and a change in the serving CN node.
NOTE 5: A change in the serving CN node may also result in a change in the serving cell, and possibly a change in the serving area.
NOTE 6: Available only when the IP-CAN supports corresponding procedures for bearer independent resource requests.
NOTE 7: Usage is defined as either volume or time of user plane traffic.
NOTE 8: The start and stop of application traffic detection are separate event triggers, but received under the same subscription from the PCRF. For unsolicited application reporting, these event triggers are always set for the TDF.
NOTE 9: If TDF for solicited application reporting is applicable, upon receiving this event report from PCEF, PCRF always updates the TDF.
NOTE 10: Due to the potential increase in signalling load, it is recommended that such event trigger subscription is only applied for a limited number of subscribers.
NOTE 11: Used when NBIFOM is supported by the IP-CAN session. Refer to clause 6.1.18 for the description of NBIFOM impacts to PCC. NBIFOM Routing Rules are defined in clause 6.12.
NOTE 12: Void.
NOTE 13: Void..
NOTE 14: Used in Network-initiated NBIFOM mode. The PCEF reports that an access becomes unusable or usable again are based on notifications received from the UE. This may correspond to the procedure "Access becomes Unusable and Usable" and to the procedure "IP flow mobility triggered by RAN Rule indication" defined in TS 23.161 [43].
NOTE 15: This event is always set when IFOM per TS 23.261 [23] applies or when NBIFOM per TS 23.161 [43] applies. In the latter case it applies in both Network-initiated NBIFOM mode and in UE-initiated NBIFOM mode.
NOTE 16: In UE-initiated NBIFOM mode this event indicates that the UE has created, modified or deleted Routing Rules. In Network-initiated NBIFOM mode this event indicates that the UE requests the network to create, modify or delete Routing Rules.
NOTE 17: The maximum number of PRA(s) per UE per PDN connection is configured in the PCRF. The PCRF may have independent configuration of the maximum number for Core Network pre-configured PRAs and UE-dedicated PRAs. The exact number(s) should be determined by operator in deployment.

If the Location change trigger is armed, the PCEF shall activate the relevant IP-CAN specific procedure which reports any changes in location to the level indicated by the trigger. If credit-authorization triggers and event triggers require different levels of reporting of location change for a single UE, the location to be reported should be changed to the highest level of detail required. However, there should be no request being triggered for PCC rules or QoS rules (if applicable) update to the PCRF if the report received is more detailed than requested by the PCRF.

NOTE 1: The access network may be configured to report location changes only when transmission resources are established in the radio access network.

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

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 reporting is only applied for a limited number of subscribers.

When activating reporting for change of UE presence in Presence Reporting Area, the PCRF provides all of the PRA Identifier(s) to be activated for Core Network pre-configured Presence Reporting Area(s) and additionally all of PRA Identifier(s) and list(s) of its elements for UE-dedicated Presence Reporting Area(s) (See Table 6.4 in clause 6.4 for details of the PRA Identifier(s) and the list(s) of elements comprising each Presence Reporting Area). Setting the Change of UE presence in Presence Reporting Area event trigger shall not preclude the PCRF from simultaneously setting another Location change event trigger. If PCRF is configured with a PRA identifier referring to the list of PRA Identifier(s) within a Set of Core Network predefined Presence Reporting Areas as defined in TS 23.401 [17], it activates the reporting of UE entering/leaving the individual PRA in the Set of Core Network predefined Presence Reporting Areas without providing the complete set of individual PRAs.

The PCRF may change (activate/modify/remove) the Presence Reporting Area(s) to be reported by providing the updated PRA Identifier(s) to PCEF. For UE dedicated PRAs, the PCRF may also change the list(s) of Presence Reporting Area elements related to the PRA Identifier(s).

The PCRF may unsubscribe to Change of UE presence in Presence Reporting Area at any time during the life time of the IP-CAN session.

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.

IP-CAN bearer modifications, which do not match any event trigger, shall cause no interaction with the PCRF.

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.

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 the traffic aggregate with a QCI and/or a modification of the traffic aggregate.

The routing information change event trigger shall trigger the PCRF interaction for any change in how the IP flow is routed. The routing information change received by the PCEF is specified in TS 23.261 [23] (i.e. IP flow mobility routing rules) or TS 23.161 [43] (i.e. Routing Rules).

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).

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).

NOTE 3: The enforced PCC rule request and the enforced ADC rule request mechanisms can be used to avoid signalling overload situations e.g. due to time of day based PCC/ADC rule changes.

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.

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.

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). The PCRF shall not remove the Usage report event trigger while usage monitoring is still active in the PCEF/TDF.

If the Usage report event trigger is set and the volume or the time thresholds, earlier provided by the PCRF, are reached, the PCEF or TDF (whichever received the event trigger) shall report this event to the PCRF. 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.

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

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.

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

NOTE 4: At PCC rule deactivation the User Location Report includes information on when the UE was last known to be in that location.

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.

If the event trigger for Access Network Information reporting is set, the ERF shall check the need for access network information reporting after successful installation/modification or removal of a PCC/QoS rule or upon termination of the IP-CAN session/bearer. The ERF shall check the Access Network Information report parameters (User Location Report, UE Timezone Report) of the PCC/QoS rules and report the access network information received in the corresponding IP-CAN bearer establishment, modification or termination procedure to the PCRF. The ERF shall not report any subsequent access network information updates received from the IP-CAN without any previous updates of related PCC/QoS rules unless the associated IP-CAN bearer or connection has been released.

If the ERF receives a request to install/modify or remove a PCC/QoS rule with Access Network Information report parameters (User Location Report, UE Timezone Report) set and there is no bearer signalling related to this PCC/QoS rule (i.e. pending IP-CAN bearer signalling initiated by the UE or bearer signalling initiated by the ERF), the ERF shall initiate a bearer signalling to retrieve the current access network information of the UE and forward it to the PCRF afterwards.

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

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.

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.

NOTE 6: For the PCEF the Credit management session failure event trigger applies to situations wherein the IP-CAN session is not terminated by the PCEF due to the credit management session failure.

If the UE resumed from suspend state event trigger is set and the UE is resumed from suspend state in EPC, the PCEF shall report this event to the PCRF. The PCEF shall not report any subsequent UE resumed from suspend state updates received from the IP-CAN to the PCRF. When receiving the event report that the UE is resumed, the PCRF may provision PCC Rules to the PCEF to trigger an IP-CAN Session modification procedure.

6.1.5 Policy Control

Policy control comprises functionalities for:

- 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 or specified by an application identifier, 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;
- 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.

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.

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 predefined 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 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:

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

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.

- The immediate authorization of the service;
- The gate control (i.e. whether there is a common gate handling per AF session or an individual gate handling per AF session component required);
- The forwarding of IP-CAN bearer level information or events:
  - Type of IP-CAN (e.g. GPRS, etc.);
  - Transmission resource status (established/released/lost);
  - Access Network Charging Correlation Information;
  - Credit denied.

NOTE 2: The credit denied information is only relevant for AFs not performing service charging.

To enable the binding functionality, the UE and the AF shall provide all available flow description information (e.g. source and destination IP address and port numbers and the protocol information). The UE shall use the traffic mapping information to indicate downlink and uplink IP flows.

If PCEF indicates that a PDN connection is carried over satellite access (of WB-E-UTRAN, NB-IoT or LTE-M RAT Types and specific values as defined in TS 23.401 [17]), the PCRF may take this information into account for the policy decision, e.g. together with any delay requirements provided by the AF.

6.1.6 Service (data flow) Prioritization and Conflict Handling

Service pre-emption priority enables the PCRF to resolve conflicts where the activation of all requested active PCC rules for services would result in a cumulative authorized QoS which exceeds the Subscribed Guaranteed bandwidth QoS.

For example, when supporting network controlled QoS, the PCRF may use the pre-emption priority of a service, the activation of which would cause the subscriber's authorized QoS to be exceeded. If this pre-emption priority is greater than that of any one or more active PCC rules, the PCRF can determine whether the deactivation of any one or more such rules would allow the higher pre-emption priority PCC rule to be activated whilst ensuring the resulting cumulative QoS does not exceed a subscriber's Subscribed Guaranteed Bandwidth QoS.

If such a determination can be made, the PCRF may resolve the conflict by deactivating those selected PCC rules with lower pre-emption priorities and accepting the higher priority service information from the AF. If such a determination cannot be made, the PCRF may reject the service information from the AF.

NOTE: 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

6.1.7.1 General

The service level (i.e., per SDF or per SDF aggregate) QoS parameters are QCI, ARP, GBR, and MBR.

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 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). When required by operator policy, the eNodeB can be configured to also use the ARP priority level in addition to the QCI to control the packet forwarding treatment in the eNodeB for SDFs having high priority ARPs.

6.1.7.2 Standardized QCI characteristics

This clause specifies standardized characteristics associated with standardized QCI values. The characteristics describe the packet forwarding treatment that an SDF aggregate receives edge-to-edge between the UE and the PCEF (see figure 6.1.7-1) in terms of the following performance characteristics:

1 Resource Type (GBR or Non-GBR);

2 Priority;

3 Packet Delay Budget;

4 Packet Error Loss Rate;

5 Maximum Data Burst Volume (for some GBR QCIs);

6 Data Rate Averaging Window (for some GBR QCIs).

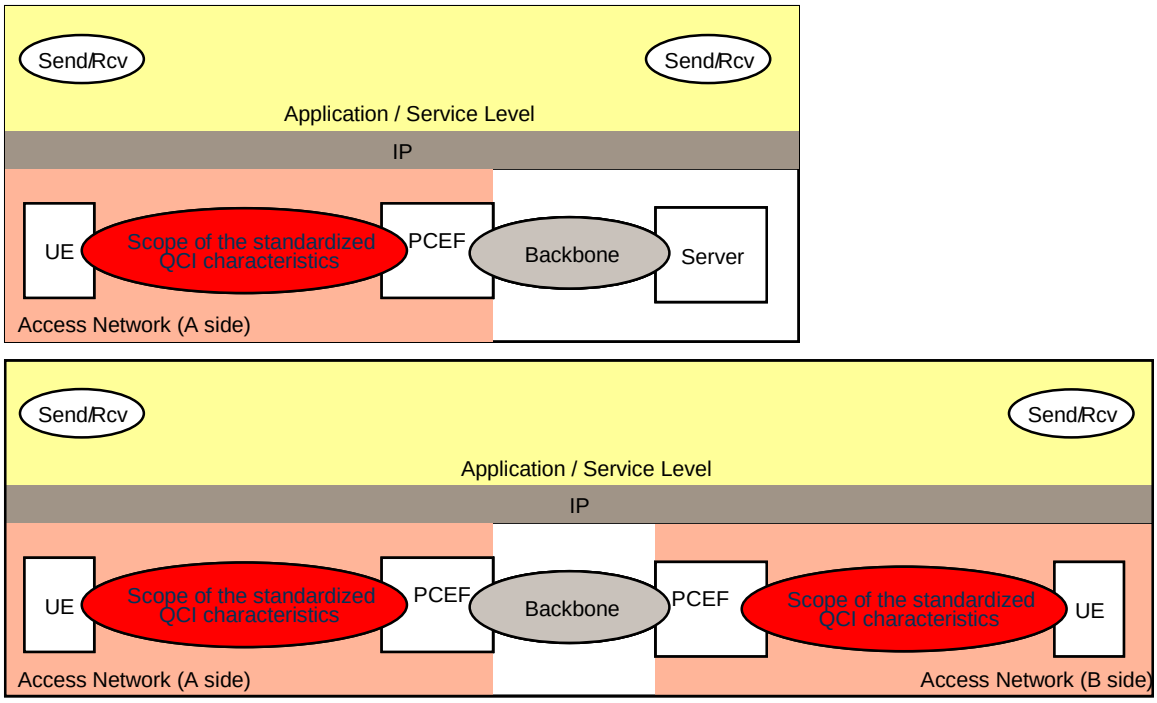

Figure 6.1.7-1: Scope of the Standardized QCI characteristics for client/server (upper figure) and peer/peer (lower figure) communication

The standardized characteristics are not signalled on any interface. They should be understood as guidelines for the pre-configuration of node specific parameters for each QCI. The goal of standardizing a QCI with corresponding characteristics is to ensure that applications / services mapped to that QCI receive the same minimum level of QoS in multi-vendor network deployments and in case of roaming. A standardized QCI and corresponding characteristics is independent of the UE's current access (3GPP or Non-3GPP).

The one-to-one mapping of standardized QCI values to standardized characteristics is captured in table 6.1.7-A and table 6.1.7-B. The main differences between the two parts are that, in contrast to Part A, Part B of Table 6.1.7 describes QCIs for which the Packet Error Loss Rate calculation includes those packets that are not delivered within the Packet Delay Budget; and, it provides additional information on the Data Rate Averaging Window as well as the Maximum Data Burst Volume that needs to be delivered within the Packet Delay Budget.

Table 6.1.7-A: Standardized QCI characteristics

QCI	Resource Type	Priority Level	Packet Delay Budget (NOTE 13)	Packet Error Loss Rate (NOTE 2)	Example Services
1 (NOTE 3)	GBR	2	100 ms (NOTE 1, NOTE 11)	10^{-2}	Conversational Voice
2 (NOTE 3)		4	150 ms (NOTE 1, NOTE 11)	10^{-3}	Conversational Video (Live Streaming)
3 (NOTE 3, NOTE 14)		3	50 ms (NOTE 1, NOTE 11)	10^{-3}	Real Time Gaming, V2X messages Electricity distribution - medium voltage (e.g. clause 7.2.2 of TS 22.261 [51]) Process automation - monitoring (e.g. clause 7.2.2 of TS 22.261 [51])
4 (NOTE 3)		5	300 ms (NOTE 1, NOTE 11)	10^{-6}	Non-Conversational Video (Buffered Streaming)
65 (NOTE 3, NOTE 9, NOTE 12)		0.7	75 ms (NOTE 7, NOTE 8)	10^{-2}	Mission Critical user plane Push To Talk voice (e.g., MCPTT)
66 (NOTE 3, NOTE 12)		2	100 ms (NOTE 1, NOTE 10)	10^{-2}	Non-Mission-Critical user plane Push To Talk voice
67 (NOTE 3, NOTE 12)		1.5	100 ms (NOTE 1, NOTE 10)	10^{-3}	Mission Critical Video user plane
75 (NOTE 14)		2.5	50 ms (NOTE 1)	10^{-2}	V2X messages
71		5.6	150ms (NOTE 1, NOTE 16)	10^{-6}	"Live" Uplink Streaming (e.g. TS 26.238 [53])
72		5.6	300ms (NOTE 1, NOTE 16)	10^{-4}	"Live" Uplink Streaming (e.g. TS 26.238 [53])
73		5.6	300ms (NOTE 1, NOTE 16)	10^{-8}	"Live" Uplink Streaming (e.g. TS 26.238 [53])
74		5.6	500ms (NOTE 1, NOTE 16)	10^{-8}	"Live" Uplink Streaming (e.g. TS 26.238 [53])
76		5.6	500ms (NOTE 1, NOTE 16)	10^{-4}	"Live" Uplink Streaming (e.g. TS 26.238 [53])
5 (NOTE 3)	Non-GBR	1	100 ms (NOTE 1, NOTE 10)	10^{-6}	IMS Signalling
6 (NOTE 4)		6	300 ms (NOTE 1, NOTE 10)	10^{-6}	Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)
7 (NOTE 3)		7	100 ms (NOTE 1, NOTE 10)	10^{-3}	Voice, Video (Live Streaming) Interactive Gaming
8 (NOTE 5)		8	300 ms (NOTE 1)	10^{-6}	Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file
9 (NOTE 6)		9			sharing, progressive video, etc.)

10	9	1100 ms (NOTE 1, NOTE 17)	10^{-6}	Video (Buffered Streaming) TCP-based (e.g. www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.) and any service that can be used over satellite access with these characteristics
69 (NOTE 3, NOTE 9, NOTE 12)	0.5	60 ms (NOTE 7, NOTE 8)	10^{-6}	Mission Critical delay sensitive signalling (e.g., MC-PTT signalling, MC Video signalling)
70 (NOTE 4, NOTE 12)	5.5	200 ms (NOTE 7, NOTE 10)	10^{-6}	Mission Critical Data (e.g. example services are the same as QCI 6/8/9)
79 (NOTE 14)	6.5	50 ms (NOTE 1, NOTE 10)	10^{-2}	V2X messages
80 (NOTE 3)	6.8	10 ms (NOTE 10, NOTE 15)	10^{-6}	Low latency eMBB applications (TCP/UDP-based); Augmented Reality

NOTE 1: A delay of 20 ms for the delay between a PCEF and a radio base station should be subtracted from a given PDB to derive the packet delay budget that applies to the radio interface. This delay is the average between the case where the PCEF is located "close" to the radio base station (roughly 10 ms) and the case where the PCEF is located "far" from the radio base station, e.g. in case of roaming with home routed traffic (the one-way packet delay between Europe and the US west coast is roughly 50 ms). The average takes into account that roaming is a less typical scenario. It is expected that subtracting this average delay of 20 ms from a given PDB will lead to desired end-to-end performance in most typical cases. Also, note that the PDB defines an upper bound. Actual packet delays - in particular for GBR traffic - should typically be lower than the PDB specified for a QCI as long as the UE has sufficient radio channel quality.

NOTE 2: The rate of non congestion related packet losses that may occur between a radio base station and a PCEF should be regarded to be negligible. A PELR value specified for a standardized QCI therefore applies completely to the radio interface between a UE and radio base station.

NOTE 3: This QCI is typically associated with an operator controlled service, i.e., a service where the SDF aggregate's uplink / downlink packet filters are known at the point in time when the SDF aggregate is authorized. In case of E-UTRAN this is the point in time when a corresponding dedicated EPS bearer is established / modified.

NOTE 4: If the network supports Multimedia Priority Services (MPS) then this QCI could be used for the prioritization of non real-time data (i.e. most typically TCP-based services/applications) of MPS subscribers.

NOTE 5: This QCI could be used for a dedicated "premium bearer" (e.g. associated with premium content) for any subscriber / subscriber group. Also in this case, the SDF aggregate's uplink / downlink packet filters are known at the point in time when the SDF aggregate is authorized. Alternatively, this QCI could be used for the default bearer of a UE/PDN for "premium subscribers".

NOTE 6: This QCI is typically used for the default bearer of a UE/PDN for non privileged subscribers. Note that AMBR can be used as a "tool" to provide subscriber differentiation between subscriber groups connected to the same PDN with the same QCI on the default bearer.

NOTE 7: For Mission Critical services, it may be assumed that the PCEF is located "close" to the radio base station (roughly 10 ms) and is not normally used in a long distance, home routed roaming situation. Hence delay of 10 ms for the delay between a PCEF and a radio base station should be subtracted from this PDB to derive the packet delay budget that applies to the radio interface.

NOTE 8: In both RRC Idle and RRC Connected mode, the PDB requirement for these QCIs can be relaxed (but not to a value greater than 320 ms) for the first packet(s) in a downlink data or signalling burst in order to permit reasonable battery saving (DRX) techniques.

NOTE 9: It is expected that QCI-65 and QCI-69 are used together to provide Mission Critical Push to Talk service (e.g., QCI-5 is not used for signalling for the bearer that utilizes QCI-65 as user plane bearer). It is expected that the amount of traffic per UE will be similar or less compared to the IMS signalling.

NOTE 10: In both RRC Idle and RRC Connected mode, the PDB requirement for these QCIs can be relaxed for the first packet(s) in a downlink data or signalling burst in order to permit battery saving (DRX) techniques.

NOTE 11: In RRC Idle mode, the PDB requirement for these QCIs can be relaxed for the first packet(s) in a downlink data or signalling burst in order to permit battery saving (DRX) techniques.

NOTE 12: This QCI value can only be assigned upon request from the network side. The UE and any application running on the UE is not allowed to request this QCI value.

NOTE 13: Packet delay budget is not applicable on NB-IoT or when Enhanced Coverage is used for WB-E-UTRAN (see TS 36.300 [19]).

NOTE 14: This QCI could be used for transmission of V2X messages as defined in TS 23.285 [48].

NOTE 15: A delay of 2 ms for the delay between a PCEF and a radio base station should be subtracted from the given PDB to derive the packet delay budget that applies to the radio interface.

NOTE 16: For "live" uplink streaming (see TS 26.238 [53]), guidelines for PDB values of the different QCIs correspond to the latency configurations defined in TR 26.939 [54]. In order to support higher latency reliable streaming services (above 500ms PDB), if different PDB and PELR combinations are needed these configurations will have to use non-standardised QCIs.

NOTE 17: The worst case one way propagation delay for GEO satellite is expected to be ~270 ms, ~ 21 ms for LEO at 1200 km, and ~13 ms for LEO at 600 km. The UL scheduling delay that needs to be added is also typically a two way propagation delay e.g. ~540 ms for GEO, ~42 ms for LEO at 1200 km, and ~26 ms for LEO at 600 km. Based on that, the access network Packet delay budget is not applicable for QCIs that require access network PDB lower than the sum of these values when the specific types of satellite access are used (see TS 36.300 [19]). QCI-10 can accommodate the worst case PDB for GEO satellite type.

Table 6.1.7-B: Standardized QCI characteristics

QCI	Resource Type	Priority Level	Packet Delay Budget (NOTE B1)	Packet Error Loss Rate (NOTE B2)	Maximum Data Burst Volume (NOTE B1)	Data Rate Averaging Window	Example Services
82 (NOTE B6)	GBR	1.9	10 ms (NOTE B4)	10^{-4} (NOTE B3)	255 bytes	2000 ms	Discrete Automation (TS 22.278 [38], clause 8 bullet g, and TS 22.261 [51], table 7.2.2-1, "small packets")
83 (NOTE B6)		2.2	10 ms (NOTE B4)	10^{-4} (NOTE B3)	1354 bytes (NOTE B5)	2000 ms	Discrete Automation (TS 22.278 [38], clause 8 bullet g, and TS 22.261 [51], table 7.2.2-1, "big packets")
84 (NOTE B6)		2.4	30 ms (NOTE B7)	10^{-5} (NOTE B3)	1354 bytes (NOTE B5)	2000 ms	Intelligent Transport Systems (TS 22.278 [38], clause 8, bullet h, and TS 22.261 [51], table 7.2.2).
85 (NOTE B6)		2.1	5 ms (NOTE B8)	10^{-5} (NOTE B3)	255 bytes	2000 ms	Electricity Distribution- high voltage (TS 22.278 [38], clause 8, bullet i, and TS 22.261 [51], table 7.2.2 and Annex D, clause D.4.2).

NOTE B1: The PDB applies to bursts that are not greater than Maximum Data Burst Volume.
NOTE B2: This Packet Error Loss Rate includes packets that are not successfully delivered over the access network plus those packets that comply with the Maximum Data Burst Volume and GBR requirements but which are not delivered within the Packet Delay Budget.
NOTE B3: Data rates above the GBR, or, bursts larger than the Maximum Data Burst Volume, are treated as best effort, and, in order to serve other packets and meet the PELR, this can lead to them being discarded.
NOTE B4: A delay of 1 ms for the delay between a PCEF and a radio base station should be subtracted from a given PDB to derive the packet delay budget that applies to the radio interface.
NOTE B5: This Maximum Data Burst Volume value is set to 1354 bytes to avoid IP fragmentation on an IPv6 based, IPSec protected GTP tunnel to the eNB (the value is calculated as in Annex C of TS 23.060 [12] and further reduced by 4 bytes to allow for the usage of a GTP-U extension header).
NOTE B6: This QCI is typically associated with a dedicated EPS bearer.
NOTE B7: A delay of 5 ms for the delay between a PCEF and a radio base station should be subtracted from a given PDB to derive the packet delay budget that applies to the radio interface.
NOTE B8: A delay of 2 ms for the delay between a PCEF and a radio base station should be subtracted from a given PDB to derive the packet delay budget that applies to the radio interface.

The Resource Type determines if dedicated network resources related to a service or bearer level Guaranteed Bit Rate (GBR) value are permanently allocated (e.g. by an admission control function in a radio base station). GBR SDF aggregates are therefore typically authorized "on demand" which requires dynamic policy and charging control. A Non GBR SDF aggregate may be pre-authorized through static policy and charging control.

The Maximum Data Burst Volume, if defined for the QCI (see Table 6.1.7-B), is the amount of data which the RAN is expected to deliver within the part of the Packet Delay Budget allocated to the link between the UE and the radio base station as long as the data is within the GBR requirements. If more data is transmitted from the application, delivery within the Packet Delay Budget cannot be guaranteed for packets exceeding the Maximum Data Burst Volume or GBR requirements.

The Data Rate Averaging Window, if defined for the QCI (see Table 6.1.7-B), is the 'sliding window' duration over which the GBR and MBR for a GBR SDF aggregate shall be calculated (e.g. in the RAN, PDN-GW, and UE).

The Packet Delay Budget (PDB) defines an upper bound for the time that a packet may be delayed between the UE and the PCEF. For a certain QCI the value of the PDB is the same in uplink and downlink. The purpose of the PDB is to

support the configuration of scheduling and link layer functions (e.g. the setting of scheduling priority weights and HARQ target operating points). Except for QCIs 82 and 83, the PDB shall be interpreted as a maximum delay with a confidence level of 98 percent. For services using QCI 82 or 83, a packet delayed by more than the PDB is included in the calculation of the PELR if the packet is within the Maximum Data Burst Volume and GBR requirements.

NOTE 1: The PDB denotes a "soft upper bound" in the sense that an "expired" packet, e.g. a link layer SDU that has exceeded the PDB, does not need to be discarded (e.g. by RLC in E-UTRAN). The discarding (dropping) of packets is expected to be controlled by a queue management function, e.g. based on pre-configured dropping thresholds.

The support for SRVCC requires QCI=1 only be used for IMS speech sessions in accordance to TS 23.216 [28].

NOTE 2: Triggering SRVCC will cause service interruption and/or inconsistent service experience when using QCI=1 for non-IMS services.

NOTE 3: Triggering SRVCC for WebRTC IMS session will cause service interruption and/or inconsistent service experience when using QCI=1. Operator policy (e.g. use of specific AF application identifier) can be used to avoid using QCI 1 for a voice service, e.g. WebRTC IMS session.

Services using a Non-GBR QCI should be prepared to experience congestion related packet drops, and, except for QCI 80, 98 percent of the packets that have not been dropped due to congestion should not experience a delay exceeding the QCI's PDB. This may for example occur during traffic load peaks or when the UE becomes coverage limited. See Annex J for details. Packets that have not been dropped due to congestion may still be subject to non congestion related packet losses (see PELR below). Owing to its low latency objective, services using QCI 80 should anticipate that more than 2 percent of packets might exceed the PDB of QCI 80.

Except for services using QCI 82 or 83 services using a GBR QCI and sending at a rate smaller than or equal to GBR can in general assume that congestion related packet drops will not occur, and 98 percent of the packets shall not experience a delay exceeding the QCI's PDB. Exceptions (e.g. transient link outages) can always occur in a radio access system which may then lead to congestion related packet drops even for services using a GBR QCI and sending at a rate smaller than or equal to GBR. Packets that have not been dropped due to congestion may still be subject to non congestion related packet losses (see PELR below). For services using QCI 82 or 83 a packet which is delayed by more than the PDB but is within the Maximum Data Burst Volume and GBR requirements, is counted as lost when calculating the PELR.

Every QCI (GBR and Non-GBR) is associated with a Priority level (see Table 6.1.7). The lowest Priority level value corresponds to the highest Priority. The Priority levels shall be used to differentiate between SDF aggregates of the same UE, and it shall also be used to differentiate between SDF aggregates from different UEs. Via its QCI an SDF aggregate is associated with a Priority level and a PDB. Scheduling between different SDF aggregates shall primarily be based on the PDB. If the target set by the PDB can no longer be met for one or more SDF aggregate(s) across all UEs that have sufficient radio channel quality then the QCI Priority level shall be used as follows: in this case a scheduler shall meet the PDB of an SDF aggregate on QCI Priority level N in preference to meeting the PDB of SDF aggregates on next QCI Priority level greater than N, until the priority N SDF aggregate's GBR (in case of a GBR SDF aggregate) has been satisfied.

Other aspects related to the treatment of traffic exceeding an SDF aggregate's GBR are out of scope of this specification.

When required by operator policy, the eNodeB can be configured to use the ARP priority level in addition to the QCI priority level to determine the relative priority of the SDFs in meeting the PDB of an SDF aggregate. This configuration applies only for high priority ARPs as defined in clause 6.1.7.3.

NOTE 4: The definition (or quantification) of "sufficient radio channel quality" is out of the scope of 3GPP specifications.

NOTE 5: In case of E-UTRAN a QCI's Priority level, and when required by operator policy, the ARP priority level may be used as the basis for assigning the uplink priority per Radio Bearer (see TS 36.300 [19] for details).

The Packet Error Loss Rate (PELR) defines an upper bound for the rate of SDUs (e.g. IP packets) that have been processed by the sender of a link layer protocol (e.g. RLC in E-UTRAN) but that are not successfully delivered by the corresponding receiver to the upper layer (e.g. PDCP in E-UTRAN). Thus, the PELR defines an upper bound for a rate of non congestion related packet losses. The purpose of the PELR is to allow for appropriate link layer protocol

configurations (e.g. RLC and HARQ in E-UTRAN). For a certain QCI the value of the PELR is the same in uplink and downlink.

NOTE 6: The characteristics PDB and PELR are specified only based on application / service level requirements, i.e., those characteristics should be regarded as being access agnostic, independent from the roaming scenario (roaming or non-roaming), and independent from operator policies.

6.1.7.3 Allocation and Retention Priority characteristics

The QoS parameter ARP contains information about the priority level, the pre-emption capability and the pre-emption vulnerability. The priority level defines the relative importance of a resource request. This allows deciding whether a bearer establishment or modification request can be accepted or needs to be rejected in case of resource limitations (typically used for admission control of GBR traffic). It can also be used to decide which existing bearers to pre-empt during resource limitations.

NOTE 1: The ARP priority level can be used in addition to the QCI to determine the transport level packet marking, e.g. to set the DiffServ Code Point of the associated EPS bearer, as described in TS 23.401 [17].

NOTE 2: When required by operator policy, the eNodeB can be configured to use the ARP priority level in addition to QCI priority level to control the packet forwarding treatment for SDFs having high priority ARPs.

The range of the ARP priority level is 1 to 15 with 1 as the highest level of priority. The pre-emption capability information defines whether a service data flow can get resources that were already assigned to another service data flow with a lower priority level. The pre-emption vulnerability information defines whether a service data flow can lose the resources assigned to it in order to admit a service data flow with higher priority level. The pre-emption capability and the pre-emption vulnerability can be either set to 'yes' or 'no'.

The ARP priority levels 1-8 should only be assigned to resources for services that are authorized to receive prioritized treatment within an operator domain (i.e. that are authorized by the serving network). The ARP priority levels 9-15 may be assigned to resources that are authorized by the home network and thus applicable when a UE is roaming.

NOTE 3: This ensures that future releases may use ARP priority level 1-8 to indicate e.g. emergency and other priority services within an operator domain in a backward compatible manner. This does not prevent the use of ARP priority level 1-8 in roaming situation in case appropriate roaming agreements exist that ensure a compatible use of these priority levels.

6.1.8 Termination Action

The termination action applies only in case of online charging. The termination action indicates the action, which the PCEF/TDF should perform when no more credit is granted. A packet that matches a PCC rule/ADC rule, indicating a charging key for which no credit has been granted, is subject to a termination action.

The defined termination actions include:

- Allowing the packets to pass through;
- Dropping the packets;
- The PCEF/TDF Default Termination Action;
- The re-direction of packets to an application server (e.g. defined in the termination action).

NOTE: Such a re-direction may cause an application protocol specific asynchronous close event and application protocol specific procedures may be required in the UE and/or AF in order to recover, e.g. as specified in RFC 2616 for HTTP.

The Default Termination Action for all charging keys, for which no more credit is granted and there is no specific termination action shall be pre-configured in the PCEF/TDF according to operator's policy. For instance, the default behaviour may consist of allowing packets of any terminated service to pass through the PCEF/TDF.

The OCS may provide a termination action for each charging key over the Gy interface. Any previously provided termination action may be overwritten by the OCS. A termination action remains valid and shall be applied by the PCEF/TDF until all the corresponding PCC/ADC rules of that charging key are removed or the corresponding IP-CAN bearer is removed (for GPRS the PDP context).

The OCS shall provide the termination action to the PCEF/TDF before denying credit; otherwise the PCEF/TDF default termination action will be performed.

6.1.9 Handling of packet filters provided to the UE by PCEF/BBERF

The network shall ensure that the traffic mapping information negotiated with the UE reflects the bearer binding of PCC/QoS rules, except for those extending the inspection beyond what can be signalled to the UE. The PCC/QoS rules may restrict what traffic is allowed compared to what is explicitly negotiated with the UE. The PCRF may, per service data flow filter, indicate that the PCEF/BBERF is required to explicitly signal the corresponding traffic mapping information to the UE, e.g. for the purpose of IMS precondition handling at the UE. In absence of that indication, it is a PCEF/BBERF decision whether to signal the traffic mapping information that is redundant from a traffic mapping point of view.

NOTE 1: A new/modified PCC/QoS rule can cause that previously redundant, and therefore omitted, traffic mapping information to cease being redundant and causing the PCEF/BBERF to signal the corresponding traffic mapping information to the UE.

NOTE 2: In order to signal a specific traffic mapping to a PDP context/EPS bearer without any previous TFT, if the operator policy is to continue allowing previously allowed traffic on that bearer, TFT filters that correspond to the previous traffic mapping need to be introduced as well.

NOTE 3: The PCEF/BERF can use all SDF filters for the generation of traffic mapping information. However if the number of SDF filters for an IP-CAN bearer exceeds the maximum number of filters that may be signalled to the UE (e.g. as specified in TS 24.008 [50]) another bearer needs to be established and a rebinding of PCC rules to bearers (by PCEF/BBERF) or even the splitting of the SDF template into two or more PCC rules (by PCRF) may be required.

The traffic mapping information (e.g. TFT filters for GPRS and EPS) that the network provides to the UE shall include the same content as the corresponding SDF filters in the SDF template received over the Gx/Gxx interface. The representation/format of the packet filters provided by the network to the UE is access-system dependent and may vary between accesses and may also be different from the representation/format of the SDF filters in the SDF template on the Gx/Gxx interface.

NOTE 4: After handover from one access-system to another, if the UE needs to determine the QoS provided in the target access to the pre-existing IP flows in the source access, the UE can perform packet filter comparison between the packet filters negotiated in the old access and those provided by the target access during QoS resource activation.

NOTE 5: If UE initiated procedures are supported and handover between access systems is to be supported, the content of the packet filters provided on the Gx/Gxx interface by the PCRF is restricted to the packet filter fields that all the accesses can provide to the UE.

In case traffic mapping information is required for a dedicated bearer and in the PCC/QoS rules corresponding to the bearer there is no SDF filter for the uplink direction having an indication to signal corresponding traffic mapping information to the UE, the PCEF/BBERF derives traffic mapping information based on implementation specific logic (e.g. traffic mapping information that effectively disallows any useful packet flows in uplink direction as described in clause 15.3.3.4 of TS 23.060 [12]) and provides it to the UE.

NOTE 6: For GPRS and EPS, the state of TFT packet filters, as defined in TS 23.060 [12], for an IP-CAN session requires that there is at most one bearer with no TFT packet filter for the uplink direction.

NOTE 7: This PCEF behaviour covers also the case that a PCC rule with an application identifier is the only PCC rule that is bound to a dedicated bearer.

NOTE 8: For a default bearer, the PCEF/BBERF will not add traffic mapping information that effectively disallows any useful packet flows in uplink direction on its own. Traffic mapping information is only generated from SDF filters which have an indication to signal corresponding traffic mapping information to the UE.

6.1.10 IMS Emergency Session Support

6.1.10.1 Architecture model and Reference points

Emergency bearer services (i.e. IP-CAN session for the IMS emergency services) are provided by the serving network to support IMS emergency when the network is configured to support emergency services. Emergency services are network services provided through an Emergency APN and may not require a subscription depending on operator policies and local regulatory requirements. For emergency services the architecture for the non-roaming case as described in clause 5.1 is the only applicable architecture model.

For emergency services, the Sp reference point does not apply.

Emergency services are handled locally in the serving network. Therefore the S9 reference point does not apply.

6.1.10.2 PCC Rule Authorization and QoS rule generation

The PCC Rule Authorization and QoS Rule generation function selects QoS parameters that 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 services.

6.1.10.3 Functional Entities

6.1.10.3.1 PCRF

The PCRF shall determine based on the PDN-id if an IP-CAN Session concerns an IMS emergency session.

For an IP-CAN session serving an IMS emergency session, the PCRF makes authorization and policy decisions that restrict the traffic to emergency destinations, IMS signalling and the traffic to retrieve user location information (in the user plane) for emergency services. 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.

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.

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 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].

The PCRF performs according to existing procedure:

- 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.

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.

6.1.10.3.2 PCEF

The PCEF initiates the IP-CAN Session termination if the last PCC rule for this IP-CAN session is removed according to existing procedure.

In addition, at reception of an IP-CAN Session Modification Request triggered by the PCRF for an IP-CAN session serving an IMS emergency session that removes all PCC rules with a QCI other than the default bearer QCI and the QCI used for IMS signalling, the PCEF shall start a configurable inactivity timer (e.g., to enable PSAP Callback session). When the configured period of time expires the PCEF shall initiate an IP-CAN Session Termination Request for the IP-CAN session serving the IMS Emergency session.

If a PCRF-Initiated IP-CAN Session Modification Request, providing new PCC rule(s) with a QCI other than the default bearer QCI and the QCI used for IMS signalling, the PCEF shall cancel the inactivity timer.

6.1.10.3.3 P-CSCF

The P-CSCF performs according to existing procedure:

- At reception of an indication that an IMS emergency session is established, the P-CSCF sends IMS service information to the PCRF.
- At reception of an indication that an IMS emergency session is released, the P-CSCF interacts with the PCRF to revoke the IMS service information.

In addition, the P-CSCF shall include an emergency related indication when providing IMS service information to the PCRF; see TS 23.167 [21].

Moreover, the P-CSCF upon Rx session establishment may request the PCRF to provide the IMEI(SV) and the EPC-level subscriber identifiers (IMSI, MSISDN) corresponding to the Rx session.

NOTE: The IMEI(SV) and the EPC-level subscriber identifiers (IMSI, MSISDN) can be used to support authentication of roaming users in deployments with no IMS-level roaming interfaces or to support PSAP callback functionality for anonymous IMS emergency sessions, as described in TS 23.167 [21].

6.1.10.4 PCC Procedures and Flows

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.

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.

An IP-CAN session for an emergency service shall be restricted to the destination address(es) associated with the emergency service only.

6.1.10a Restricted Local Operator Services Support

Restricted Local Operator Services (i.e. IP-CAN session for the Restricted Local Operator Services) (as specified in TS 23.221 [55]) are provided by the serving network when the network is configured to support Restricted Local Operator Services.

The PCC handling of Restricted Local Operator Services is very similar to that of emergency service as specified in clause 6.1.10 with the following differences:

- RLOS APN and IMS RLOS session are used for Restricted Local Operator Services.
- Architecture model and Reference points (clause 6.1.10.1).

  Restricted Local Operator Services do not require a subscription.
- PCC Rule Authorization and QoS rule generation (clause 6.1.10.2).

  The Restricted Local Operator Services is not a prioritized services, and the ARP can be determined based on operator policy.
- Functional Entity: PCRF (clause 6.1.10.3.1).

  The PCRF shall determine based on the RLOS APN if an IP-CAN Session relates to an IMS RLOS session.
- Functional Entity: PCEF (clause 6.1.10.3.2).

  Duration of PDN connection for RLOS is controlled through local policies in PCEF. Handling of inactivity timer for the emergency PDN connection is not applicable for RLOS.
- Functional Entity: P-CSCF (clause 6.1.10.3.3).

Indication of IMS RLOS session is used.

- PCC Procedures and Flows (clause 6.1.10.4).

  The PDN-id identifies an RLOS APN.

6.1.11 Multimedia Priority Service Support

6.1.11.1 Architecture model and Reference points

Subscription data for MPS is provided to PCC through the Sp reference point. To support MPS service, the PCRF shall subscribe to changes in the MPS subscription data for Priority EPS Bearer Service. Dynamic invocation for MPS is provided from an AF, using the Priority indicator, over Rx.

6.1.11.2 PCC rule authorization and QoS rule generation

For MPS service, the PCRF shall generate the corresponding PCC/QoS rule(s) with the ARP/QCI parameters as appropriate for the prioritized service.

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. When the Priority EPS Bearer Service is revoked, the PCRF shall change the ARP/QCI values modified for Priority EPS Bearer Service to appropriate values.

NOTE 1: The above statements for the Priority EPS Bearer Service are also applicable for the MPS for Data Transport Service.

Whenever one or more AF sessions of an MPS service are active within the same PDN connection, the PCRF shall ensure that the ARP priority level of the default bearer is at least as high as the highest ARP priority level used by any authorized PCC rules belonging to an MPS service. If the ARP pre-emption capability is enabled for any of the authorized PCC rules belonging to an MPS service, the PCRF shall also enable the ARP pre-emption capability for the default bearer.

NOTE 2: 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.

NOTE 3: This PCRF capability does not cover interactions with services other than MPS services.

6.1.11.3 Priority EPS Bearer Service

The MPS Priority EPS Bearer Service targets the ARP and/or QCI of bearer(s), enabling the prioritization of all traffic on the same bearer.

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

- 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

- 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

- 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.

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

- 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

- 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

  - if modification of the QCI of PCC/QoS Rules is required, modify the QCI to an appropriate value according to PCRF decision.

6.1.11.4 Bearer priority for IMS Multimedia Priority Services

In addition to the mechanism specified in clause 6.1.11.2, IMS Multimedia Priority Services may require upgrade of the dedicated IM CN signalling bearer and the default bearer, e.g. in order to mitigate the IP-CAN session termination due to resource limitation at a location change the default bearer and dedicated IM CN signalling bearer may need an upgraded ARP.

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

- 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.

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:

- 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.

6.1.11.5 Bearer priority for MPS for Data Transport Service

MPS for Data Transport Service enables the prioritization of all traffic on the default bearer and other bearers upon AF request. The QoS modification to the default bearer and other bearers is done based on operator policy and regulatory rules by means of local PCRF configuration.

NOTE 1: If no configuration is provided, MPS for Data Transport Service applies only to the default bearer.

Upon receipt of an MPS for Data Transport Service invocation/revocation request from the UE, the AF or the PCRF authorizes the request. If the UE has an MPS subscription, MPS for Data Transport Service is authorized by the AF or the PCRF, based on AF decision. If the Service User is using a UE that does not have an MPS subscription, the AF authorizes MPS for Data Transport Service.

- In the case that the AF authorizes the MPS for Data Transport Service request, after successful authorization, the AF sends the MPS for Data Transport Service request to the PCRF over Rx for QoS modifications, including an indication that PCRF authorization is not needed. In this case, the PCRF shall not perform a subscription check for MPS for Data Transport Service requests. The AF also indicates to the PCRF whether the request is for invoking or revoking MPS for Data Transport Service.

- In the case that the AF does not authorize the MPS for Data Transport Service request, the AF sends the request over Rx to the PCRF for authorization and QoS modifications, including an indication that PCRF authorization is needed. In this case, the PCRF shall perform an MPS subscription check for the MPS for Data Transport Service request. The AF also indicates whether the request is for invoking or revoking MPS for Data Transport Service. The PCRF will inform the AF when the UE does not have an MPS subscription associated with the request.

After successful authorization by either AF or PCRF as described above, the PCRF shall, at the activation of MPS for Data Transport Service over Rx, perform the same steps for QoS modifications as described in clause 6.1.11.3 for the activation of the Priority EPS Bearer Service.

NOTE 2: To keep the PCC rules bound to the default bearer, the PCRF can either modify the ARP/QCI of these PCC rules accordingly or set the Bind to Default Bearer PCC rule attribute.

The PCRF shall inform the AF of the success or failure of the MPS for Data Transport Service invocation/revocation request.

The PCRF shall at the deactivation of MPS for Data Transport Service over Rx perform the same steps described in clause 6.1.11.3 for the deactivation of the Priority EPS Bearer Service.

If the bearers are deactivated for other reasons than an AF request, the PCRF shall notify the AF by terminating the Rx session.

The AF may also request an SDF for priority signalling between the UE and the AF, where the AF includes the Priority indicator over Rx, in order to enable the PCRF to set appropriate QoS values for the signalling bearer.

6.1.12 ADC rule authorization

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.

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.

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.

6.1.13 Redirection

Redirection of application traffic is an option applicable in the TDF or the PCEF enhanced with ADC.

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.

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.

The redirection is enforced by the PCEF enhanced with ADC or the TDF on uplink application's traffic matching the ADC or PCC rule for which redirection is enabled.

6.1.14 Resource sharing for different AF sessions

The P-CSCF (i.e. AF) may indicate to the PCRF that media of an AF session may share resources with media belonging to other AF sessions according to TS 23.228 [39]. For every media flow, the P-CSCF may indicate that the media flow may share resources in both directions or in one direction only (UL or DL).

The PCRF makes authorization and policy decisions for the affected AF sessions individually and generates a PCC/QoS rule for every media flow in any AF session.

If the PCRF received identical indication(s) for resource sharing for multiple AF sessions, the PCRF may request the PCEF/BBERF to realize resource sharing for the corresponding set of PCC/QoS rules. The PCRF provides a DL and/or UL sharing indication with the same value for those PCC/QoS Rules that are candidate to share resources according to the direction of resource sharing indicated by the AF.

For each direction, the PCEF/BBERF shall take the highest GBR value from each set of PCC/QoS Rules related with the same sharing indication for this direction and bound to the same bearer and uses that value as input for calculating the GBR of the bearer. For each direction, the PCEF/BBERF may take the MBR value of the most demanding PCC/QoS Rule included in each set of PCC Rules related with the same sharing indication for this direction and bound to the same bearer and uses that as input for calculating the MBR of the bearer.

The AF session termination or modification procedure that removes media flows triggers the removal of the corresponding PCC/QoS Rules from the PCEF/BBERF. The PCEF/BBERF shall recalculate the GBR (and MBR) value of the bearer whenever a set of PCC/QoS Rules with the same sharing indication changes.

Resource sharing is applied as long as there are at least two active PCC/QoS rules with the same sharing indication bound to the same bearer.

Resource sharing for different AF sessions is possible only if the P-CSCF, the PCRF and the PCEF/BBERF support it.

NOTE: This procedure assumes that applications/service logic must do the necessary coordination, e.g. pause sending or employ gating, to avoid service data flows interfering and to ensure that multiple flows comply with the combined QoS parameters.

6.1.15 Reporting of RAN user plane congestion information

6.1.15.1 General

RAN User Plane Congestion Information (RUCI) is reported to the PCRF to enable the PCRF to take the RAN user plane congestion status into account for policy decisions.

The RUCI includes the following information:

- The IMSI identifying the UE impacted by congestion;
- eNB identifier, ECGI or SAI identifying the eNB, E-UTRAN cell or Service Area, respectively, serving the UE.

NOTE: Whether in case of E-UTRAN the eNB identifier or the ECGI is included in the RUCI is up to operator configuration in the RCAF.

- APN for which congestion information is reported;
- Congestion level or an indication of the "no congestion" state.

6.1.15.2 Reporting restrictions

Depending on the operator's congestion mitigation policy, it may not be necessary to have RUCI reporting for all users. An operator shall be able to specify restrictions for RUCI reporting on a per UE per APN basis. Reporting restrictions can be used to activate or deactivate the RUCI reporting. Reporting restrictions can also be used to limit RUCI reporting. This is achieved by defining one or more sets of congestion levels, such that the RCAF indicates only that the UE experiences a congestion level within the given set but does not indicate the congestion level itself within that set. The sets must be non-overlapping such that a congestion level belongs to a single set only. Reporting restrictions can also be used to deactivate reporting of the congested cell's identifier as part of the RUCI.

NOTE: The support for the reporting restrictions is optional, and used only if both the PCRF and the RCAF support this feature.

6.1.15.3 UE mobility between RCAFs

A RCAF is assumed to serve a geographical area. A UE may move from the area handled by one RCAF to an area handled by a different RCAF. RCAF nodes cannot detect mobility by themselves: an RCAF node cannot differentiate whether a UE that is no longer affected by congestion has moved to another RCAF or not. When a given RCAF indicates no congestion to the PCRF for a given UE on the Np interface, this should be interpreted as no congestion experienced at the given RCAF which does not exclude that another RCAF may report that the same UE experiences congestion.

Consistent operation for UE mobility is ensured by applying the following rules at the PCRF.

- The PCRF maintains the RCAF which has last indicated that the UE is affected by congestion.
- When a new RCAF indicates that the UE is affected by congestion, the PCRF sends a message to the old RCAF to explicitly release context at the old RCAF.

6.1.16 Negotiation for future background data transfer

The AF may contact the PCRF via the SCEF (and the Nt interface) to request a time window and related conditions for future background data transfer.

NOTE 1: The SCEF may contact any PCRF in the operator network.

The AF request shall contain an ASP identifier, the volume of data to be transferred per UE, the expected amount of UEs, the desired time window and optionally, network area information (e.g. list of cell ids, TAs/RAs).

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

The PCRF shall first retrieve all existing transfer policies stored for any ASP from the SPR. Afterwards, the PCRF shall determine, based on the information provided by the AF and other available information (e.g. network policy, congestion level (if available), load status estimation for the required time window and network area, existing transfer policies) one or more transfer policies.

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

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

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

The selected transfer policy is finally stored by the PCRF in the SPR together with the reference ID and the network area information. The same or a different PCRF can retrieve this transfer policy and the corresponding network area information from the SPR and take them into account for future decisions about transfer policies for background data related to the same or other ASPs.

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

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

NOTE 6: A transfer policy is only valid until the end of its time window. The removal of outdated transfer policies from the SPR is up to implementation.

6.1.17 Traffic Steering Control

Traffic steering control is triggered by the PCRF initiated request and consists in applying a specific (S)Gi-LAN traffic steering policy for traffic detected based on application level information or service data flow level information for the purpose of steering the subscriber's selected traffic to appropriate (S)Gi-LAN service functions deployed by the operator or 3rd party service provider.

The PCRF uses one or more pieces of information such as network operator's policies, user subscription, user's current RAT, network load status, application identifier, time of day, UE location, APN, related to the subscriber session and the application traffic as input for selecting a traffic steering policy.

The PCRF controls traffic steering in the PCEF, TDF or TSSF by provisioning and modifying traffic steering control information. Traffic steering control information consists of a traffic description and a reference to a traffic steering policy that is configured in the PCEF, TDF or TSSF.

The PCEF, TDF or TSSF performs necessary actions to enforce the traffic steering policy referenced by the PCRF. For enforcing the traffic steering policy, the PCEF, TDF or TSSF may support traffic steering related functions as defined by other standard organizations. The mechanism used for routing the traffic between the service functions within the (S)Gi-LAN, is out of 3GPP scope.

The traffic steering control may be deployed using PCEF only, using TDF only, or using TSSF only, or using a combination of PCEF/TDF and TSSF.

When a combination of PCEF/TDF with traffic steering control feature and TSSF is deployed, the PCEF/TDF is utilized for application detection and packet marking while traffic steering is done using TSSF. In this case the PCC/ADC Rules provided to the PCEF/TDF for application detection shall be at application level while the traffic steering control information provided to the TSSF for traffic detection and steering control shall be at service data flow level only, i.e. the Application identifier and Traffic steering policy identifier shall be included over Gx/Sd reference point for detection of the traffic and packet marking, and the Service data flow filter(s) and Traffic steering policy identifier shall be included over St reference point for traffic steering control. The value used for packet marking at the PCEF/TDF (according to the Traffic steering policy identifier received from the PCRF) shall be the same as the one within the Service data flow filter (using filter information described in clause 6.2.2.2) that is sent to the TSSF and used for traffic steering. Alternatively, the Application Identifier may be used for traffic detection at the TSSF. In this case the value used for packet marking at the PCEF/TDF (according to the Traffic steering policy identifier received from the PCRF) shall be the same as the one configured in the TSSF for that Application Identifier.

NOTE 1: The above principle also enables a deployment scenario in which the PCEF/TDF acts as an uplink traffic classifier while the downlink traffic classifier, located in (S)Gi-LAN, acts only at service data flow filter level. This deployment scenario is applicable for applications with deducible service data flow filters only. In this case, the PCEF/TDF deduces the downlink service data flow description and communicates the related information to the downlink classifier.

NOTE 2: The SDF filter(s) can be used for traffic detection at the TSSF when the PCEF/TDF is configured to do packet marking and forwarding using ToS or TC values in the IP header. The Application Identifier can be used when the PCEF/TDF is configured to do packet marking and forwarding using e.g. GRE or NSH.

6.1.18 PCC support of NBIFOM

6.1.18.1 General

Clause 6.1.18 refers to Network Based IP Flow Mobility as described in TS 23.161 [43].

When PCC control for NBIFOM applies for an IP-CAN session:

- Multiple IP-CAN types (3GPP EPS and Non 3GPP EPS) may be simultaneously associated with the same IP-CAN session.
- The PCRF sends PCC rules including NBIFOM related information as defined in clause 6.3.1.
  - In UE-initiated NBIFOM mode this is based on Routing Rules received from the UE.
  - For network-initiated NBIFOM mode, the PCRF determines the NBIFOM related information for a PCC rule as defined in clause 6.2.1.1 (including information about UE requested mapping of IP flows to an access, Change of usability of an Access).
- A change of access may trigger the modification of the charging key or the monitoring key in a PCC rule if access dependent charging or usage monitoring is required by the operator.
- The PCRF decides whether NBIFOM applies for the IP-CAN session, based on information about the support for NBIFOM received from the PCEF and operator policies that may take into account subscription information.
- The PCEF notifies the PCRF when an access is added or removed using the event trigger defined in clause 6.1.4.

- The PCEF notifies the PCRF when an access becomes Unusable or Usable again or when the move-to-WLAN or move-from-WLAN event occurs, both events are notified to the PCRF using the event trigger "Change of the usability of an access" as defined in clause 6.1.4.

- The PCRF may reject the NBIFOM Routing Rules received from the UE based on user subscription.

In following conditions the PCRF mentioned above is the H-PCRF:

- The UE is served by its HPLMN, or

- The PDN connection is served by a PGW in the Home PLMN (Home Routed roaming configuration), or

- The PDN connection is served by a PGW in the V-PLMN (LBO configuration), and S9 is deployed and the V-PCRF supports NBIFOM. In that case, the V-PCRF acts as a relay of information.

The PCRF mentioned above is the V-PCRF in the case when, through roaming agreement, the HPLMN operator allows the VPLMN operator to operate the V-PCRF without S9; this includes authorization of roamers to use NBIFOM. In that case, network control related with subscription such as checking the total usage allowance does not apply.

NOTE 1: If the Home operator wants to enforce control of the NBIFOM functionality on a PDN connection by the H-PCRF, the Home operator should ensure that the Home Routed roaming configuration applies to this PDN connection.

NOTE 2: NBIFOM may be deployed without PCC support. This is defined in TS 23.161 [43].

In a multi access IP-CAN session, every PCC Rule is associated to one allowed access within the IP-CAN session. The information about the allowed access may be explicitly included in the PCC Rule, within the Allowed Access Type. Otherwise, the default NBIFOM access for the traffic on the IP-CAN session shall be applied as allowed access for a PCC rule. The bearer binding mechanism in the PCEF shall, in addition to the requirements defined in 6.1.1.4, ensure that a PCC Rule is associated to an IP-CAN bearer belonging to the allowed access.

The PCEF may provide the following information for each access in a multi access IP-CAN session:

- Location of the subscriber as defined in clauses A.4, H.3 and H.4.

- A serving PLMN identifier as defined in clauses A.4, H.3 and H.4.

- RAT type as defined in clauses A.4, H.3 and H.4.

For the purpose of usage monitoring in the PCEF when NBIFOM applies for an IP-CAN session, the PCRF may receive an individual Monitoring key per access from SPR.

6.1.18.2 NBIFOM impacts on IP-CAN procedures

PCC support of NBIFOM requires following modifications to IP-CAN session procedures:

- IP-CAN session establishment.

  During the IP-CAN session establishment, the PCEF informs the PCRF about the UE and network support of NBIFOM and the requested NBIFOM mode (defined in TS 23.161 [43]). The PCRF takes a policy decision on whether NBIFOM may apply to the IP-CAN session (the hPCRF decides the NBIFOM mode according to TS 23.161 [43]) and informs the PCEF about its decision.

- Addition of an access.

  When the PCEF receives both a handover request and a NBIFOM indication from the UE, the PCEF initiates an IP-CAN Session Modification procedure, to:

  - Notify the PCRF about the addition of an access to the IP-CAN session together with the IP-CAN type and the RAT type of this access. If UE-initiated NBIFOM mode was selected at IP-CAN session establishment the notification contains also the default NBIFOM access selected by the UE.

  - Notify the PCRF with the NBIFOM Routing Rules, if the UE included Routing Rules with the access addition request in UE-initiated NBIFOM mode.

  The PCRF takes policy decisions and communicates them to the PCEF:

- The PCRF may reject the addition of the access if the multi-access IP-CAN session would correspond to an invalid combination of IP-CAN and RAT Types or is not allowed by the subscription. In this release of the specification the only allowed combination corresponds to the UE using a 3GPP access and a WLAN access.

- If network-initiated NBIFOM mode was selected at IP-CAN session establishment, the PCRF indicates the default NBIFOM access to the PCEF.

- In UE-initiated NBIFOM mode the PCRF verifies the default NBIFOM access provided by the UE. If it complies with the subscription the PCRF provides this default NBIFOM access to the PCEF. If not, the PCRF selects a different default NBIFOM access and provides it to the PCEF.

- In UE-initiated NBIFOM mode, the PCRF may receive NBIFOM Routing Rules created by the UE. The PCRF may reject a NBIFOM Routing Rule due to subscription limitations. Otherwise, the PCRF determines for each NBIFOM Routing Rule the impacted PCC rule and provides or modifies this PCC rule.

- The PCRF shall ensure that there is at least one PCC Rule that can be bound to the default bearer of each access.

- Removal of an access.

  When the PCEF is informed about the removal of an access of a multi-access IP-CAN session, the PCEF initiates an IP-CAN Session Modification procedure, to notify the PCRF about the removal of an access together with the IP-CAN type and the RAT type of this access. The PCRF determines the affected PCC rules and replies with updated PCC Rules or informs about the PCC Rules that are to be removed.

  The PCC rules corresponding to the removed access are then modified or deleted by the PCEF accordingly. This shall not trigger the sending of Routing Rules deletion to the UE in Network-initiated NBIFOM mode.

NOTE 2: The UE deletes the Routing Rules locally in case of removal of access as described in TS 23.161 [43].

NOTE 3: The PCRF can also decide to trigger the removal of an access by updating or removing all PCC rules that are bound to this access. The removal of all PCC Rules bound to an access removes the access unless there are PCC Rules not known to the PCRF defined in the PCEF for this particular access.

- Network-initiated IP flow mobility within a PDN connection (Network-initiated NBIFOM mode).

  When a multi-access IP-CAN session has been set-up in Network-initiated NBIFOM mode, the PCRF may at any time determine that flows should be moved from a source access to a target access. In that case, the PCRF provides updated PCC Rules with a modified Allowed Access Type and the Routing Rule Identifier using an IP-CAN Session Modification procedure (i.e. the Allowed Access Type can be added, changed or removed).

  The PCRF request triggers the sending of Routing Rules creation (when the Allowed Access Type is added) or Routing Rules modification (when the Allowed Access Type is changed) to the UE which may be rejected by the UE due to local radio conditions. In that case the PCRF gets notified which PCC rules cannot be modified. This notification from the PCEF contains an indication of the cause of the rejection received from the UE.

  The PCRF request triggers the sending of Routing Rules deletion to the UE when the Allowed Access Type is removed.

- UE-initiated IP flow mobility within a PDN connection (UE-initiated NBIFOM mode).

  When the PCEF has received a request from the UE to create / modify / delete a Routing Rule, the PCEF initiates an IP-CAN Session Modification procedure and provides the Routing Rule received from the UE to the PCRF as an NBIFOM Routing Rule. The PCRF may reject an NBIFOM Routing Rule received from the UE due to subscription limitations. Otherwise the PCRF determines and updates the impacted PCC rule (as described in 6.12.2) and provides the updated PCC rule to the PCEF.

- UE requested mapping of IP flows to an access (Network-initiated NBIFOM mode).

  This procedure is only used in Network-initiated NBIFOM mode when the UE wants to request the network to apply specific mappings of IP flows to an access.

  When the PCEF has received a request from the UE to have the network create / modify / delete a Routing Rule, the PCEF initiates an IP-CAN Session Modification procedure and provides the information received from the UE to the PCRF as an NBIFOM Routing Rule. The PCRF may reject an NBIFOM Routing Rule received from the UE due to subscription limitations. Otherwise the PCRF determines and updates the impacted PCC rule (as

described in clause 6.12.2) and provides the updated PCC rule to the PCEF. The updated PCC rule triggers the sending of a Routing Rules creation / modification / deletion to the UE (as described above for Network-initiated IP flow mobility).

- Indication that an access becomes unusable / usable again or indication of move-to-WLAN / move-from-WLAN (Network-initiated NBIFOM mode).

  The PCEF initiates an IP-CAN Session Modification procedure to notify the PCRF about the change of usability of an access to the PCRF. For every PCC rule that is currently bound to this access, the PCRF shall either change the Allowed Access Type and provide the updated PCC rule to the PCEF or remove this PCC rule. This triggers the sending of Routing Rules modification to the UE. If the PCRF receives an indication that an access become usable again, The PCRF may update the PCC rules, e.g. by changing the Allowed Access Type and provide the updated PCC rules to the PCEF. This triggers the sending of Routing Rules modification to the UE.

- Reporting Access Network Information to the AF.

  The PCRF reports to the AF only Access Network Information associated with one access even though different media of the AF session are carried by different accesses.

  If the PCRF has received a request for Access Network Information from the AF and PCC rules related with the AF request are bound to multiple accesses, the PCRF selects one PCC rule to be associated with Access Network Information reporting from the PCEF. The selected PCC rule should correspond to the 3GPP access: Using the 3GPP access reduces the risk of getting non-trustable location information from the S2b access of the IP-CAN session.

- UE resource request for a multi-access IP-CAN session.

  When the UE wants to request the network to allocate resources for one or more IP flows in the non-default NBIFOM access, the UE shall provide a corresponding Routing Rule in the same request in the UE-initiated mode. Without such Routing Rule, the network shall reject the UE resource request.

NOTE 4: UE resource requests in the default NBIFOM access do not require a Routing Rule as the generated PCC rule will be bound to dedicated bearer in this access.

- PCRF initiated IP-CAN session modification.

  When network-initiated NBIFOM mode applies and the PCRF modifies the service data flow filter or precedence in a PCC rule for which a corresponding Routing Rule exists, the PCEF shall also modify this Routing Rule at the UE accordingly.

  When network-initiated NBIFOM mode applies and the PCRF removes a PCC rule for which a corresponding Routing Rule exists, the PCEF shall also remove the corresponding Routing Rule at the UE.

  When UE-initiated NBIFOM mode applies and if a new PCC rule is created due to the request from the network (e.g. request from the AF or application detection information from the PCEF/TDF), the PCRF shall determine that the new PCC rule is bound to the default access. UE may initiate IP flow mobility request to bind the IP flow to another access later.

6.1.19 Resource reservation for services sharing priority

To enable the usage of the same bearer, an AF may indicate to the PCRF that a media flow of an AF session is allowed to use the same priority as media flows belonging to other AF sessions (instead of the service priority provided for this media flow). In this case, the AF will provide a priority sharing indicator in addition to the application identifier and the service priority. For MCPTT, the service priority and the priority sharing indicator are defined in TS 23.179 [46]. The priority sharing indicator is used to indicate what media flows are allowed to share priority.

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

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

- The modified ARP priority is set to the highest of the original priority among all the PCC/QoS rules that include the priority sharing indicator;
- The modified ARP pre-emption capability is set if any of the original PCC/QoS rules have the ARP pre-emption capability set;
- The modified ARP pre-emption vulnerability is set if all the original PCC/QoS rules have the ARP pre-emption vulnerability set.

NOTE 1: Having the same setting for the ARP parameter in the PCC/QoS rules with the priority sharing indicator set enables the usage of the same bearer. Furthermore, a combined modification of the ARP parameter in the PCC/QoS rules ensures that a bearer modification is triggered when a media flow with higher service priority starts.

If the PCRF receives an indication that a PCC/QoS rule provisioning or modification failed (due to resource reservation failure) then, the PCRF may apply pre-emption and remove active PCC/QoS rules from the PCEF and then retry the PCC/QoS rule provisioning or modification procedure. If the PCRF does not apply pre-emption, the AF is notified using existing procedures (as defined in clause 6.1.5) that the resource reservation for the new media flow failed.

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

- whether media flows sharing priority are candidates to being pre-empted taking into account pre-emption capability and vulnerability values;
- how to perform pre-emption among multiple potential media flow candidates of same priority: most recently added media flow, least recently added media flow, media flow with highest requested bandwidth in the AF request.

6.1.20 Management of Packet Flow Descriptions using the PFDF

The Management of Packet Flow Descriptions (PFDs) enables the PCEF and TDF to perform accurate application detection when PFDs are provided by an ASP (via the SCEF and the PFDF) and then to apply enforcement actions as instructed in the PCC/ADC Rule.

The operator is able to configure pre-defined PCC/ADC Rules in the PCEF/TDF or dynamic PCC/ADC Rules in the PCRF that include at least an application identifier for service data flow or application detection, charging control information, i.e. charging key and optionally the Sponsor identifier or the ASP identifier or both. Depending on the service level agreements between the operator and the Application Server Provider, it may be possible for the ASP to provide individual PFDs or the full set of PFDs for each application identifier maintained by the ASP to the PCEF/TDF via the SCEF and the PFDF. The PFDs become part of the application detection filters in the PCEF/TDF and therefore are used as part of the logic to detect traffic generated by an application. The ASP may remove or modify some or all of the PFDs which have been provisioned previously for one or more application identifiers. When a removed/modified PFD was used to detect application traffic related to an application identifier in a PCC/ADC Rule of an IP-CAN/TDF session and the PCEF/TDF has reported the application start as described in clause 4.5 to the PCRF for the application instance corresponding to this PFD, the PCEF/TDF shall report the application stop to the PCRF for the corresponding application instance identifier if the removed/modified PFD in PCEF/TDF results in that the stop of the application instance is not being able to be detected.

NOTE 1: The management of Packet Flow Descriptions is optional, and is only used if the PFDF is deployed and the PCEF or the TDF supports this feature.

Each PFD may be identified by a PFD id. A PFD id is unique in the scope of a particular application identifier. There may be different PFD types associated to an application identifier, see TS 23.682 [42] for the definition of PFD.

The PFDs may be retrieved by PCEF/TDF from PFDF in "pull" mode or may be provisioned from PFDF to the PCEF/TDF in "push" mode.

When the "push" mode is used, the PFDF distributes PFDs for each application identifier to those PCEFs/TDFs that enable access to those applications. The PFDF may be configured with the list of PCEFs/TDFs where PFDs should be distributed. There are three methods to provision PFDs from the PFDF to the PCEF/TDF, as described in clause 7.12.2:

a) Push of whole PFDF state according to operator configuration in PFDF (e.g., provision per day according to operator configuration);

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

c) Selective push of an ASP change in the PFD set according to ASP request (i.e. ASP indicates to push changes in a PFD set within the time interval indicated by the Allowed Delay as described in TS 23.682 [42]).

NOTE 2: In all cases listed above, how to protect the PCEF/TDF from overload during the procedure to provision PFDs is up to Stage 3.

The SCEF may be configured with a minimum allowed delay based on SLA to authorize the allowed delay provided by the ASP, as defined in TS 23.682 [42].

When the "pull" mode is used, at the time a PCC/ADC Rule with an application identifier for which PFDs provisioned by the PFDF are not available is activated or provisioned, the PCEF/TDF requests all PFDs for that application identifier from the PFDF. The PFDs retrieved for an application identifier from the PFDF are cached in the PCEF/TDF with an associated caching timer to control how long the PFDs are valid. When the caching timer elapses, if there are still active PCC/ADC rules that refer to the corresponding application identifier, the PCEF/TDF reloads the PFD(s) from the PFDF. When the PCEF/TDF removes the last PCC/ADC rule that refers to the corresponding application identifier, or when the caching timer expires and no PCC/ADC rule refers to the application identifier, the PCEF/TDF may remove the PFD(s) related with the application identifier.

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

Within one PLMN, "push" mode only, "pull" mode only, or a combination of "pull" and "push" mode may be supported if the feature is supported.

When the "pull" mode is used, the PFDF may provide to the PCEF/TDF a caching time value per application identifier. The PCEF/TDF receives the caching time value together with the PFD(s) from the PFDF over Gw/Gwn and applies this value for the application identifier instead of the configured default caching time value. In case no caching time value is received from PFDF, the PCEF/TDF uses the configured default caching time value.

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

When only "pull" mode is supported in one PLMN, if the Allowed Delay is shorter than the caching time value stored for this application identifier, or shorter than the default caching time if no application-specific caching time is stored, the PFDF sends a response to SCEF with an indication that the Allowed Delay cannot be met. The PFDF may still store the PFD(s) and if so, indicate this to the SCEF. The PFDF shall also include the caching time value in the response to the SCEF. The SCEF shall forward the indication that the PFDF stored the PFD(s) (if available) and the caching time value to the ASP when informing that the Allowed Delay could not be met.

If the PFDs are managed by local O&M procedures, PFD retrieval is not used; otherwise, the PFDs retrieved from PFDF overrides any PFDs pre-configured in the PCEF/TDF. If all PFDs retrieved from the PFDF are removed for an application identifier, the pre-configured PFDs shall be applied again for the application identifier. The PCEF/TDF may differentiate the need for PFD retrieval based on operator configuration in the PCEF/TDF.

The AF requests including an application identifier may trigger the activation or provisioning of a PCC/ADC Rule in the PCEF/TDF by the PCRF based on operator policies.

6.1.21 3GPP PS Data Off

This feature, when activated by the user, prevents downlink traffic and may prevent uplink traffic via 3GPP access except for 3GPP PS Data Off Exempt Services.

NOTE 1: Preventing uplink packets that don't belong to 3GPP Data Off Exempt Services in PDN GW implies that the exempt uplink packets in the UE have traversed the Serving GW but get dropped in the PDN GW. If this happens, it's not possible to verify accounting information collected at the Serving GW for inter-operator charging. However, the subscriber may not be charged for those packets.

The 3GPP PS Data Off Exempt Services are a set of operator services, defined in TS 22.011 [49], that are the only allowed services in downlink direction when the 3GPP PS Data Off feature has been activated by the user.

When PCRF is deployed, it shall be configured with the list of 3GPP PS Data Off Exempt Services and the event trigger of 3GPP PS Data Off status change is used to inform the PCRF about every change of the 3GPP PS Data Off status.

NOTE 2: The PCRF can be configured with a list of 3GPP PS Data Off Exempt Services per APN. The list of 3GPP PS Data Off Exempt Services for an APN can also be empty, or can allow for any service within that APN, according to operator policy.

NOTE 3: The PCRF can be configured with up to two lists of 3GPP PS Data Off Exempt Services for UEs in HPLMN and for UEs camping in any VPLMNs using mechanism as specified in clause 6.2.1.1.

NOTE 4: For the PDN connection used for IMS services, the 3GPP Data Off Exempt Services are enforced in the IMS domain as specified TS 23.228 [39]. Policies configured in the PCRF need to ensure that IMS services are allowed when the 3GPP Data Off status of the UE is set to "activated", e.g. by treating any service within a well-known IMS APN as 3GPP PS Data Off Exempt Services.

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

NOTE 5: In order for the PCEF to prevent the services that do not belong to the list of 3GPP PS Data Off Exempted Services, if the services are controlled by dynamic PCC rules, the PCRF could modify the PCC rules by setting the gate status to "closed" for the downlink and optionally uplink directions in all active dynamic PCC rules or remove those dynamic PCC rules. If the services are controlled by predefined PCC rules, the PCRF can deactivate those predefined PCC rules. PCC rule with wild-carded service data flow filters can be among the PCC rules that are modified, removed or deactivated in that manner. In this case, it can be necessary that the PCRF at the same time installs or activates PCC rules for data-off exempt services.

NOTE 6: For example, four PCC rules (A, B, C, D) are active for a PDN connection with PCC rule A representing a 3GPP PS Data Off Exempt Service. When 3GPP PS Data Off is activated, the PCRF could either modify PCC rules B, C and D if they are dynamic PCC rules by closing the gate in downlink and optionally in uplink direction or remove/deactivate PCC rules B, C and D if they are predefined PCC rules. PCC rule A does not need to be changed as it represents 3GPP PS Data Off Exempt Service. Assuming that PCC rule B contained wild-carded service data flow filters which has enabled some 3GPP PS Data Off Exempt Service is removed or deactivated, an additional PCC rule E can be installed or activated as well to enable the downlink traffic for that 3GPP PS Data Off Exempt Service.

NOTE 7: The network configuration can ensure that at least one PCC Rule is bound to the default bearer when Data Off is activated in order to avoid deletion of an existing PDN connection or in order not to fail a PDN connection establishment.

When the PCRF receives service information from the AF, in addition to what is specified in clause 6.2.1.0, PCRF shall check if the requested service information belongs to the 3GPP PS Data Off Exempt Services. If the requested service belongs to 3GPP PS Data Off Exempt Services, PCRF shall continue as specified in clause 6.2.1.0. If the requested service doesn't belong to the 3GPP PS Data Off Exempt Services, PCRF shall reject the service request.

When the PCRF is informed about the deactivation of 3GPP PS Data Off, it shall perform policy control decision as specified in clause 6.2.1.0 and perform PCC rule operations as specified in clause 6.3.2 2 to make sure that the services are allowed according to user's subscription and operator policy (irrespective of whether they belong to the list of 3GPP PS Data Off Exempt Services).

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

- when the PCEF is informed about activation of 3GPP PS Data Off, only packets for services belonging to the list of 3GPP PS Data Off Exempt Services are forwarded while all other packets are discarded. The list of 3GPP PS

Data Off Exempt Services for UEs camping in HPLMN and the list of 3GPP PS Data Off Exempt Services for UEs camping in VPLMN can be different, and

- When PCEF is informed about deactivation of 3GPP PS Data Off, downlink packets are forwarded according to the operator policy for the subscriber.

NOTE 8: For example, the PCEF can be configured with three sets of predefined PCC rules: one set for UEs with 3GPP PS Data Off status "inactive", the second set for UE camping in the HPLMN with 3GPP PS Data Off status "active", and the third set for UEs camping in the VPLMN with 3GPP PS Data Off status "active". The set of predefined PCC rules for UE 3GPP PS Data Off status "active" can be equivalent to the set of predefined PCC rules for UE 3GPP PS Data Off status "inactive" with the following two differences: All services belonging to the list of 3GPP PS Data Off Exempt Services can be represented by PCC rule(s) which allows the traffic to pass while in all other PCC rules (not belonging to the list of 3GPP PS Data Off Exempt Services) the gate status can be "closed" for the downlink direction. When the PCEF is informed about the change of UE 3GPP PS Data Off status, it can replace the currently active set of predefined PCC rules with the other set of predefined PCC rules.

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

When NBIFOM applies for the IP-CAN session, the PCRF shall not modify PCC rules associated to the IP-CAN type "Non 3GPP EPS".

6.2 Functional entities

6.2.1 Policy Control and Charging Rules Function (PCRF)

6.2.1.0 General

The PCRF encompasses policy control decision and flow based charging control functionalities.

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.

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.

The PCRF shall apply the security procedures, as required by the operator, before accepting service information from the AF.

The PCRF shall decide whether application traffic detection is applicable, as per operator policies, based on user profile configuration, received within subscription information.

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.

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. If IP flow mobility as specified in TS 23.261 [23] applies, the PCRF shall, based on IP flow mobility routing rules received from the PCEF, provide the authorized QoS rules to the applicable BBERF as specified in clause 6.1.1.3.

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.

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.

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 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.

NOTE 1: How the PCRF derives the re-try interval is up to implementation.

In this Release, the PCRF supports only a single Rx reference point, i.e. there is one AF for each AF session.

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.

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.

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.

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.

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.

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.

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 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.

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 IPv4 address and/or IPv6 network prefix (if known) that can be used for linking the new Gateway Control Session to the existing Gx session. If the UE IPv4 address and/or IPv6 network prefix is/are 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.

The PCRF determines which case applies as described on clause 7.1.

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.

Negotiation of IP-CAN bearer establishment mode takes place via Gx for 3GPP IP-CANs. For non-3GPP IP-CANs specified in TS 23.402 [18] negotiation of bearer establishment mode takes place via Gx when GTP is used and via Gxx for the rest of the cases. For other accesses supporting multiple IP-CAN bearer establishment modes, if Gxx applies, the negotiation takes place via Gxx, otherwise via Gx. To support the different IP-CAN bearer establishment modes (UE-only or UE/NW) the PCRF shall:

- shall set the IP-CAN bearer establishment mode for the IP-CAN session based on operator configuration, network and UE capabilities;

- 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;

NOTE 3: For an operator-controlled service, the UE and the PCRF may be provisioned with information indicating which mode is to be used.

- 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.

NOTE 4: This situation may e.g. occur if the PCRF has already triggered a NW-initiated procedure that corresponds to the UE request.

- guarantee the precedence of dynamic PCC rules with SDF template containing SDF filter(s) (and optionally also for SDF templates consisting of an application identifier) for network controlled services in the service data flow detection process at the PCEF by setting the PCC rule precedence information to appropriate values.

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. 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.

NOTE 5: The PCRF can also use the dynamic or pre-defined PCC Rules related to the IMS signalling to request Access Network Information reporting. This can be used to support e.g., regulatory requirements for SMS over IP, where the IMS network (i.e. P-CSCF) needs to retrieve the user location and/or UE Time Zone information. Note that due to regulatory requirements, the Access Network Information can be requested for SMS over IP, impacting a large number of PDN Connections, that can lead to significant increase in signalling load when the Access Network Information is requested from the Access Node (e.g. MME).

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 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.

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.

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, which 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 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 clause 5.1.3 of TS 32.251 [9]. 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.

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. 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 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.

NOTE 6: For IP flow mobility feature enabled, the TDF doesn't have accurate information about the location and the type of RAT the user is attached to.

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.

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.

The PCRF may support usage monitoring control. Usage is defined as either volume or time of user plane traffic.

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. For the purpose of usage monitoring per access type , the PCRF receives an individual Monitoring key per access type from SPR.

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. The PCRF shall decide if and when to activate usage monitoring to the PCEF and TDF.

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.

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.

It shall be possible for the PCRF to request a usage report from the requested node (PCEF or TDF).

NOTE 7: 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.

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 8: 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 allowanced usage after the PCEF reporting, minimizes the risk of exceeding the usage allowance.

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 value(s) in the response to the PCEF or TDF respectively. If Monitoring time and subsequent threshold value are 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.

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 / TDF.

NOTE 9: 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.

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.

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). For sponsored data connectivity (see Annex N), the PCRF may receive a usage threshold from the AF.

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. 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. If the usage threshold is reached, the AF may terminate the AF session or provide a new usage threshold to the PCRF. Alternatively, the AF may allow the session to continue without specifying a usage threshold. If the AF decides to allow the session to continue without specifying a usage threshold, then monitoring in the PCEF/TDF shall be discontinued for that monitoring key by the PCRF, unless there are other reasons for continuing the monitoring.

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.

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.

The PCRF performs authorizations based on sponsored data connectivity profiles stored in the SPR. 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.

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, reject the service authorization request, or initiate the AF session termination based on home operator policy.

NOTE 10: Sponsored data connectivity is not supported in the roaming with visited access scenario in this Release.

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.

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.

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.

The PCRF uses the RUCI received from the RCAF as input for policy decisions.

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 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 11: 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.

At reception of the IMS service information from the P-CSCF, if configured through policy, the PCRF determines the Maximum Packet Loss Rate for UL and DL based on the IMS service information and taking into account information defined in TS 26.114 [45] and sends it to PCEF along with the PCC rule for the voice media.

NOTE 12: Based on local configuration, the PCRF sets the Maximum Packet Loss Rate (UL, DL) corresponding to either the most robust codec configuration (e.g., codec, mode, redundancy) or the least robust codec configuration of the negotiated set in each direction.

6.2.1.1 Input for PCC decisions

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 predefined information. These different nodes should provide as much information as possible to the PCRF. At the same time, the information below describes examples of the information provided. Depending on the particular scenario all the information may not be available or is already provided to the PCRF.

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;
- NBIFOM Routing Rules (when NBIFOM as specified in TS 23.161 [43] applies);
- IP flow routing information (when IP flow mobility as specified in TS 23.261 [23] applies);

NOTE 1: IP flow routing information and NBIFOM Routing Rules are provided only by the PCEF.

- Change of usability of an Access (when NBIFOM as specified in TS 23.161 [43] applies);
- IP-CAN bearer attributes;

NOTE 2: 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 may have a different value depending on the access type;

- Request type (initial, modification, etc.);
- Type of IP-CAN (e.g. GPRS, etc.);

NOTE 3: The Type of IP-CAN parameter should allow extension to include new types of accesses.

- Location of the subscriber;

NOTE 4: See clause 6.1.4 for the description of this location information.

NOTE 5: Depending on the type of IP-CAN, the limited update rate for the location information at the PCEF may lead to a UE moving outside the area indicated in the detailed location information without notifying the PCEF.

- A PDN ID;
- A PLMN identifier;
- IP-CAN bearer establishment mode;
- 3GPP PS Data Off status.

The PCEF enhanced with ADC or the TDF may provide the following information:

- Detected application identifier;
- Allocated application instance identifier;
- Detected service data flow descriptions.

The SPR may provide the following information for a subscriber, connecting to a specific PDN:

- Subscriber's allowed services, i.e. list of Service IDs;
- For each allowed service, a pre-emption priority;
- 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 (See TS 23.401 [17] for more detail on MPS Subscription);
- IMS Signalling Priority.

NOTE 6: The MPS Priority Level represents user priority.

NOTE 7: The MPS Priority Level is one among other input data such as operator policy for the PCRF to set the ARP value. The MPS EPS Priority, and MPS Priority Level are consistent with the corresponding parameters defined in the HSS.

The SPR may provide the following policy information related to an ASP (see clause 6.1.16):

- 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.

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

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

- Bandwidth;
- Sponsored data connectivity information (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 8: The AF Priority information represents session/application priority and is separate from the MPS EPS Priority indicator.

- Emergency indicator;
- Indicator for Restricted Local Operator Services;
- Application service provider.

NOTE 9: The application service provider may be identified in numerous forms e.g. the AF application identifier or the host realm at Diameter level.

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

- Policy counter status for each relevant policy counter.

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.

NOTE 10: 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.

NOTE 11: Depending on the RUCI reporting interval configured in the RCAF, a UE may move 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.

- APNs.
- Congestion level or an indication of the "no congestion" state.

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.

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.

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.

6.2.1.2 Subscription information management in the PCRF

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.

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.

6.2.1.3 V-PCRF

6.2.1.3.1 General

The V-PCRF (Visited-Policy and Charging Rules Function) is a functional element that encompasses policy and charging control decision functionalities in the V-PLMN. The V-PCRF includes functionality for both home routed access and visited access (local breakout).

The V-PCRF determines based on the subscriber identity if a request is for a roaming user.

A Gateway Control Session request received over the Gxx reference point may trigger a request over the S9 reference point from the V-PCRF to the H-PCRF.

If a Gateway Control Session establishment request is received that can not be bound to an existing Gx session then the associated IP-CAN session is either home routed or it is visited access but the IP-CAN session establishment request has not yet been received over Gx.

For this case the V-PCRF may determine based on PDN-Id carried in the GW control session and roaming agreements if the request shall be proxied to the H-PCRF over S9 or not. The V-PCRF may choose not to proxy the Gateway Control Session Establishment only if the PDN-Id indicates the request is for visited access.

The Gateway Control Session Establishment request should only be proxied to the H-PCRF over S9 in case the V-PCRF is configured to do so e.g. based on roaming agreement.

NOTE: Proxying the Gateway Control Session Establishment makes the H-PCRF aware of the Gateway Control Session and enables binding in case a subsequent IP-CAN Session is established with home routed access or visited access.

If the V-PCRF determines that a Gateway Control Session Establishment shall be proxied to the H-PCRF over S9 then the reply from the H-PCRF shall also be communicated back to the GW (BBERF) over Gxx.

In case the V-PCRF determines that a Gateway Control Session Establishment request shall not be proxied, then the V-PCRF shall respond to the request made by the GW (BBERF) without notifying the H-PCRF.

If an IP-CAN session establishment request is received for a roaming user over the Gx reference point, then the V-PCRF shall conclude that the IP-CAN session use visited access and act as described in clause 6.2.1.3.3.

NOTE 2: Through roaming agreement, the HPLMN operator may allow the VPLMN operator to operate the V-PCRF without using the capabilities described in clause 6.2.1.3.3 (i.e. no S9 is used). In such case, the PCRF in the VPLMN has no access to subscriber policy information from the HPLMN, only static policies will apply based on roaming agreements. The VPCRF may also interact with the AF in the VPLMN in order to generate PCC Rules for services delivered via the VPLMN. V-PCRF uses locally configured policies according to the roaming agreement with the HPLMN operator as input for PCC Rule generation.

If a Gateway Control and QoS rules provision is received by the V-PCRF over the S9 reference point for a Gateway Control session which is not associated, at the V-PCRF, with an existing Gx session, the V-PCRF shall conclude that the IP-CAN session associated with the Gateway Control session is home routed, and act as described in clause 6.2.1.3.2.

6.2.1.3.2 V-PCRF and Home Routed Access

The V-PCRF provides functions to proxy Gxx interactions between the BBERF and the H-PCRF as follows:

- Gateway Control Session establishment and termination;
- Gateway Control and QoS Policy Rules Provision;
- Gateway Control and QoS Rule Request.

The V-PCRF provides functions to enforce visited operator policies regarding QoS authorization requested by the home operator as indicated by the roaming agreements. The V-PCRF informs the H-PCRF when a request has been denied and may provide the acceptable QoS Information.

Within an IP-CAN session, a different V-PCRF may be selected when a new Gateway Control Session is established.

6.2.1.3.3 V-PCRF and Visited Access (local breakout)

The V-PCRF provides functions to:

- Enforce visited operator policies regarding QoS authorization requested by the home operator e.g. on a per QCI or service basis as indicated by the roaming agreements. The V-PCRF informs the H-PCRF when a request has been denied and may provide the acceptable QoS Information for the service.
- When Gxx interaction is terminated locally at the V-PCRF, perform Gx to Gateway Control Session linking.
- When Gxx interaction is terminated locally at the V-PCRF, extract QoS rules (defined in clause 6.5) from PCC rules (defined in clause 6.3) provided by the H-PCRF over the S9 reference point. The V-PCRF provides updated PCC rules to the PCEF and QoS rules to the BBERF, if appropriate.
- For the case of AF in the VPLMN:
  - Proxy Rx authorizations over the S9 reference point to the H-PCRF;
  - Relay event subscriptions and notifications between the H-PCRF and V-AF

When Gx interactions are proxied between the PCEF and the H-PCRF, the V-PCRF proxies:

- Indication of IP-CAN Session Establishment and Termination;
- Policy and Charging Rule Provisioning;
- Request Policy and Charging Rules.

If a Gateway Control Session is used and if during the IP-CAN Session Establishment the Gateway Control Session Establishment procedure was proxied to the H-PCRF (according to the logic in clause 6.2.1.3.1), then the V-PCRF shall also proxy all other Gateway Control Session procedures to the H-PCRF.

If the Gateway Control Session was not proxied to the H-PCRF then the V-PCRF shall handle all Gateway Control Session procedures locally and not proxy them to the H-PCRF. This has the following implications:

- An IP-CAN Session modification may trigger the V-PCRF to update the Gateway Control Session if required in order to maintain the alignment of PCC and QoS Rules.
- An IP-CAN Session termination procedure may trigger the V-PCRF to terminate the Gateway Control Session if the Gateway Control Session was established for the purpose of a single IP-CAN session. Otherwise a Gateway Control and QoS Rules Provision procedure may be initiated to remove the QoS Rules associated with the IP-CAN session.
- On receiving a Gateway Control and QoS Rules Request message from the BBERF, the V-PCRF performs the procedure described in clause 7.7.3.2 for the event reporting for PCEF in visited network and locally terminated Gxx interaction.

NOTE 1: The V-PCRF has to set the event triggers at the PCEF in a way that the PCEF would trigger a PCEF initiated IP-CAN Session Modification Procedure if an interaction with the H-PCRF is required.

When Rx components are proxied between an AF in the VPLMN and the H-PCRF, the V-PCRF shall proxy service session information between the AF and the H-PCRF.

The V-PCRF shall support functionality to generate ADC rules from the PCC rules providing application detection and control as instructed by the H-PCRF over S9. The V-PCRF shall provide updated PCC Rules to the PCEF, and generated ADC rules to the TDF, as appropriate in the VPLMN configuration.

NOTE 2: There may be situations where the TDF or PCEF enhanced with ADC is not able to detect the traffic requested by the H-PCRF. Prior agreements could be arranged to ensure that there is a common understanding of the meaning of application identifiers transferred between PLMNs.

The V-PCRF shall install the event triggers in the PCEF, in the TDF and in the BBERF that were provided for the IP-CAN session and install additional event triggers in the BBERF that are relevant only to the PCEF (i.e. such event triggers are typically set by the OCS) or the TDF. On receiving an Event report from the PCEF/BBERF, the V-PCRF forwards it to the TDF, if TDF has previously subscribed for it.

NOTE 3: Event reports over Gxx that are relevant only to the PCEF will not trigger a PCEF initiated IP-CAN session modification procedure.

For UEs in a local breakout scenario, the RCAF may contact the V-PCRF with the RUCI information. Congestion information shall not be exposed via the S9 interface.

Within an IP-CAN session the same V-PCRF remains for the whole lifetime of the IP-CAN session.

6.2.1.4 H-PCRF

6.2.1.4.1 General

The H-PCRF (Home-Policy and Charging Rules Function) is a functional element that encompasses policy and charging control decision functionalities in the H-PLMN and in the VPLMN. The H-PCRF includes functionality for both home routed access and visited access (local breakout).

If a Gateway Control Session is used and a Gateway Control Session Establishment is indicated over S9, then one or more of the following cases applies:

1. One (or several) home routed IP-CAN sessions are known to the H-PCRF that can be bound to the Gateway Control session. For such IP-CAN sessions, the H-PCRF shall act as described in clause 6.2.1.4.2.

2. No IP-CAN session is known to the H-PCRF that can be bound to the Gateway Control session. This is the case when an IP-CAN session establishment process has not yet been initiated over Gx or S9.

If an IP-CAN Session Establishment is received over Gx then the H-PCRF shall conclude that the IP-CAN session is home routed and act as described in clause 6.2.1.4.2.

If an IP-CAN Session Establishment is received over S9 then the H-PCRF shall conclude that the IP-CAN session use visited access and act as described in clause 6.2.1.4.3.

6.2.1.4.2 H-PCRF and Home Routed Access

The H-PCRF shall use the S9 reference point to proxy information to the BBERF via the V-PCRF for the following related Gxx procedures:

- Gateway Control Session establishment and termination;

- Gateway Control and QoS Policy Rules Provision;

- Gateway Control and QoS Rule Request.

If an IP-CAN session termination is received over the Gx reference point, then the H-PCRF shall initiate a Gateway Control Session Termination procedure over S9 if the Gateway Control Session was established for the purpose of a single IP-CAN session. Otherwise a Gateway Control and QoS Rules Provision procedure may be initiated over S9 to remove the QoS Rules in the BBERF associated with the IP-CAN session.

6.2.1.4.3 H-PCRF and Visited Access (Local Breakout)

The H-PCRF shall use the S9 reference point to proxy information to the PCEF (and indirectly also to the BBERF when the Gateway Control Session is not proxied to the H-PCRF, and indirectly also to the TDF) via the V-PCRF for the following related Gx procedures:

- Indication of IP-CAN Session Establishment and Termination messages;
- Policy and Charging Rule Provisioning messages;
- Request Policy and Charging Rules messages.

When the Gateway Control Session is proxied to the H-PCRF, the H PCRF shall use the S9 reference point to proxy information to the BBERF via the V PCRF for the following related Gxx procedures:

- Indication of Gateway Control Session Establishment and Termination messages;
- QoS Rules Provisioning messages;
- Request QoS Rules messages.

The H-PCRF shall generate PCC rules for application traffic detection, notification and policy control when the TDF is located in the VPLMN.

The H-PCRF should generate PCC rules for both of the cases when the AF is located in the VPLMN and when the AF is located in the HPLMN. The H-PCRF provides the PCC rules to the V-PCRF over the S9 reference point.

6.2.1.5 Handling of Multiple BBFs associated with the same IP-CAN session

6.2.1.5.1 Handling of two BBFs associated with the same IP-CAN session during handover

The procedures specified in this clause apply when the case of multiple BBFs occurs during handovers. The two BBFs can be located in two separate BBERFs, or one BBF is located in the PCEF and the other one in a BBERF. If the PCRF determines that there is more than one BBF associated with the same IP-CAN session, the PCRF handles the multiple BBFs as follows:

- The PCRF classifies the BBERF which reports the same IP-CAN type as that reported by the PCEF as the primary BBERF and a BBERF that reports an IP-CAN type different from that reported by the PCEF as non-primary BBERF. If there are more than one BBERFs that report the same IP-CAN type as that reported by the PCEF, the BBERF that last created the GW Control Session with the PCRF is classified as the primary BBERF and other BBERF(s) are classified as non-primary BBERF(s).

NOTE 1: During handover where the BBF moves from a BBERF to the PCEF (e.g. handover from PMIP to GTP), when the PCEF reports a new IP-CAN type, the BBERF is classified as a non-primary BBERF. There is no primary BBERF but the active BBF is in the PCEF.

NOTE 2: During handover where the BBF moves from the PCEF to a BBERF (e.g. handover from GTP to PMIP), when the BBERF creates a Gateway Control Session, it is classified as a non-primary BBERF. This BBERF subsequently gets classified as the primary BBERF when the PCEF reports an IP-CAN type which is the same as that reported by the BBERF.

- When a new (primary/non-primary) BBERF supporting NW/UE bearer establishment mode creates a GW Control session, the PCRF provides to the new BBERF QoS rules corresponding to SDFs. For a change of IP-CAN type, the QoS parameters of some of the QoS rules may be changed or some QoS rules may not be provided to the new BBERF, e.g. depending of the capability of the target RAT. When a new (primary/non-primary) BBERF supporting only UE bearer establishment mode creates a GW Control session, the PCRF authorizes the setup of the default bearer and only pushes down QoS rules in response to specific requests from the BBERF.

NOTE 3: After completion of the handover procedure to the new BBERF, the UE can still initiate the access specific procedures to modify or release the resources that were originally allocated based on UE-initiated resource allocation. Such operations and the associated changes to QoS rules are handled following the normal UE-initiated resource management procedures.

NOTE 4: To facilitate the UE's determination of QoS resources in the target access allocated to pre-existing IP flows the access system is required to provide packet filters with the same content as that in the SDF template filters received over the Gx/Gxx interface (see clause 6.1.9).

- If the BBF is located in any of the BBERF, the PCRF keeps track of QoS rules activation by all the BBERFs. The PCRF updates PCC rules to the PCEF based on activation status of QoS rules in the primary BBERF.

- If the primary-BBERF reports failure to activate a QoS rule, the PCRF also removes the same QoS rule from the non-primary BBERFs, if any are already installed, and the corresponding PCC rule from the PCEF. If a non-primary BBERF reports failure to install a QoS rule, the PCRF updates the status for that particular BBERF in its record but does not perform any further action.

- When path-switch occurs and the PCEF informs the PCRF of a new IP-CAN type, if a BBERF is re-classified as a primary BBERF, the PCRF may update QoS rules in the BBERF corresponding to the PCC rules in the PCEF.

- For the case of UE initiated resource reservation through the non-primary BBERF: If a non-primary BBERF request results in a change of the QoS rules active in the primary-BBERF, e.g. creation of a new QoS rule or results in modification of an existing QoS rule, then the PCRF shall reject the request.

6.2.1.5.2 Handling of multiple BBFs with IP-CAN session flow mobility

The procedures specified in this clause apply when the case of multiple BBFs occurs during flow mobility scenarios as specified in TS 23.261 [23]. The multiple BBFs can be located in either separate BBERFs, or one BBF is located in the PCEF and the other ones in separate BBERFs. If the PCRF determines that there is more than one BBF associated with the same IP-CAN session due to flow mobility, the PCRF handles the multiple BBFs as follows:

- The default route may be associated with one of the BBFs. The PCRF does not differentiate between primary and secondary BBF.

- If, based on routing information received from the PCEF, the PCRF determines that the bearer binding for a service data flow is located in a BBERF, the PCRF provides QoS rules for bearer binding to the appropriate BBERF/BBF. Each service data flow is associated with one BBF based on the routing information. If no explicit routing information for a service data flow is available from the PCEF, the PCRF provides PCC/QoS rules for the service data flow based on the default route.

- When the route of a service data flow changes from one source BBF to another target BBF, the PCRF removes the QoS rules related to the service data flow from the source BBF (if the source BBF is located in a BBERF) and provisions the QoS rules related to the service data flow to the target BBF (if the target BBF is located in a BBERF).

- The PCRF may select different bearer establishment mode for different BBFs. Provision of PCC/QoS rules to a specific BBF follows the rule provision procedures based on the bearer establishment mode selected for that BBF.

6.2.2 Policy and Charging Enforcement Function (PCEF)

6.2.2.1 General

The PCEF encompasses service data flow detection, policy enforcement and flow based charging functionalities.

This functional entity is located at the Gateway (e.g. GGSN in the GPRS case, and PDG in the WLAN case). It provides service data flow detection, user plane traffic handling, triggering control plane session management (where the IP-CAN permits), QoS handling, and service data flow measurement as well as online and offline charging interactions.

A PCEF shall ensure that an IP packet, which is discarded at the PCEF as a result from PCC rule enforcement or flow based charging, is neither reported for offline charging nor cause credit consumption for online charging.

NOTE 1: For certain cases e.g. suspected fraud an operator shall be able to block the service data flow but still be able to account for any packets associated with any blocked service data flow.

The PCEF is enforcing the Policy Control as indicated by the PCRF in two different ways:

- Gate enforcement. The PCEF shall allow a service data flow, which is subject to policy control, to pass through the PCEF if and only if the corresponding gate is open;

- QoS enforcement:

  - QoS class identifier correspondence with IP-CAN specific QoS attributes. The PCEF shall be able to convert a QoS class identifier value to IP-CAN specific QoS attribute values and determine the QoS class identifier value from a set of IP-CAN specific QoS attribute values.

  - PCC rule QoS enforcement. The PCEF shall enforce the authorized QoS of a service data flow according to the active PCC rule (e.g. to enforce uplink DSCP marking).

  - IP-CAN bearer QoS enforcement. The PCEF controls the QoS that is provided to a combined set of service data flows. The policy enforcement function ensures that the resources which can be used by an authorized set of service data flows are within the "authorized resources" specified via the Gx interface by "authorized QoS". The authorized QoS provides an upper bound on the resources that can be reserved (GBR) or allocated (MBR) for the IP-CAN bearer. The authorized QoS information is mapped by the PCEF to IP-CAN specific QoS attributes. During IP-CAN bearer QoS enforcement, if packet filters are provided to the UE, the PCEF shall provide packet filters with the same content as that in the SDF template filters received over the Gx interface.

The PCEF is enforcing the charging control in the following way:

- For a service data flow (defined by an active PCC rule) that is subject to charging control, the PCEF shall allow the service data flow to pass through the PCEF if and only if there is a corresponding active PCC rule with and, for online charging, the OCS has authorized credit for the charging key. The PCEF may let a service data flow pass through the PCEF during the course of the credit re-authorization procedure.

For a service data flow (defined by an active PCC rule) that is subject to both Policy Control and Charging Control, the PCEF shall allow the service data flow to pass through the PCEF if and only if the right conditions from both policy control and charging control happen. I.e. the corresponding gate is open and in case of online charging the OCS has authorized credit for its charging key.

For a service data flow (defined by an active PCC rule) that is subject to policy control only and not charging control, the PCEF shall allow the service data flow to pass through the PCEF if and only if the conditions for policy control are met.

A PCEF may be served by one or more PCRF nodes. The PCEF shall contact the appropriate PCRF based on the packet data network (PDN) connected to, together with, a UE identity information (if available, and which may be IP-CAN specific). It shall be possible to ensure that the same PCRF is contacted for a specific UE irrespective of the IP-CAN used.

The operator may configure an indicator in HSS which is delivered to the PCEF within the Charging Characteristics and used by the PCEF to not establish the Gx session during the IP-CAN session establishment procedure.

NOTE 2: The decision to not establish the Gx session applies for the life time of the IP-CAN session.

NOTE 3: The indicator in the HSS is operator specific, therefore its value is understood within the HPLMN and can be used in both non-roaming or home routed roaming cases.

The PCEF shall, on request from the PCRF, modify a PCC rule, using the equivalent PCEF behaviour as the removal of the old and the activation of the new (modified) PCC rule. The PCEF shall modify a PCC rule as an atomic operation. The PCEF shall not modify a predefined PCC rule on request from the PCRF.

The PCEF should support predefined PCC rules.

For online charging, the PCEF shall manage credit as defined in clause 6.1.3.

The operator may apply different PCC rules depending on different PLMN. The PCEF shall be able to provide identifier of serving network to the PCRF, which may be used by the PCRF in order to select the PCC rule to be applied.

The operator may configure whether Policy and Charging Control is to be applied based on different access point.

The PCEF shall gather and report IP-CAN bearer usage information according to clause 6.1.2. The PCEF may have a pre-configured Default charging method. Upon the initial interaction with the PCRF, the PCEF shall provide pre-configured Default charging method if available.

At IP-CAN session establishment the PCEF shall initiate the IP-CAN Session Establishment procedure, as defined in clause 7.2. In case the SDF is tunnelled at the BBERF, the PCEF shall inform the PCRF about the mobility protocol tunnelling header of the service data flows. In case 2a, defined in clause 7.1, the PCEF may provide charging ID information to the PCRF. The PCEF shall inform the PCRF on whether it is enhanced with ADC, or provide the TDF address, if one is configured at the PCEF. If no PCC rule was activated for the IP-CAN session, the PCEF shall reject the IP-CAN session establishment.

If there is no PCC rule active for a successfully established IP-CAN session at any later point in time, e.g., through a PCRF initiated IP-CAN session modification, the PCEF shall initiate an IP-CAN session termination procedure, as defined in clause 7.3.2. If the PCRF terminates the Gx session, the PCEF shall initiate an IP-CAN session termination procedure, as defined in clause 7.3.2.

If there is no PCC rule active for a successfully established IP-CAN bearer at any later point in time, e.g., through a PCRF initiated IP-CAN session modification, the PCEF shall initiate an IP-CAN bearer termination procedure, as defined in clause 7.4.1.

If the IP-CAN session is modified, e.g. by changing the characteristics for an IP-CAN bearer, the PCEF shall first use the event trigger to determine whether to request the PCC rules for the modified IP-CAN session from the PCRF; afterwards, the PCEF shall use the re-authorisation triggers, if available, in order to determine whether to require re-authorisation for the PCC rules that were either unaffected or modified. If the PCEF receives an unsolicited update of the PCC rules from the PCRF (IP-CAN session modification, clause 7.4.2), the PCC rules shall be activated, modified or removed as indicated by the PCRF.

The PCEF shall inform the PCRF about the outcome of a PCC rule operation. If network initiated procedures apply to the PCC rule and the corresponding IP-CAN bearer can not be established or modified to satisfy the bearer binding, then the PCEF shall reject the activation of a PCC rule.

The PCEF shall inform the PCRF about any removal of a PCC rule, that the PCRF has activated, that occurs without explicit instruction from the PCRF.

When IP-CAN bearer resources are released, i.e. at IP-CAN session termination or PCEF-initiated IP-CAN session modification notifying that PCC Rules are removed, the PCEF shall also provide, if available, the reason why resources are released, i.e. RAN/NAS Release Cause, TWAN Release Cause or UWAN Release Cause.

NOTE 4: In case of a rejection of a PCC rule activation the PCRF may e.g. modify the attempted PCC rule, de-activate or modify other PCC rules and retry activation or abort the activation attempt and, if applicable, inform the AF that transmission resources are not available.

If network initiated procedures for IP-CAN bearer establishment apply this also includes provisioning the UE with traffic mapping information. See clause 6.1.9, Annex A and Annex D for details.

If another IP-CAN session is established by the same user, this is treated independently from the existing IP-CAN session.

To support the different IP-CAN bearer establishment modes (UE-only or UE/NW) the PCEF shall:

- forward the network and UE capabilities to the PCRF;
- apply the IP-CAN bearer establishment mode for the IP-CAN session set by the PCRF.

During an IP-CAN session modification, the PCEF shall provide information (belonging to the IP-CAN bearer established or modified) to the PCRF as follows:

- in UE-only bearer establishment mode, the PCEF shall send the full QoS and traffic mapping information;
- in UE/NW bearer establishment mode, the PCEF shall:
  - at UE-initiated bearer establishment, send the full QoS and traffic mapping information;
  - at UE-initiated bearer modification, send information on the requested change to QoS bitrates and changes to the traffic mapping information;
- at NW-initiated bearer establishment or modification, the PCEF shall not send any QoS or traffic mapping information.

When flow mobility as specified in TS 23.261 [23] applies, the PCEF shall provide IP flow mobility routing information to the PCRF as follows:

- the default route to be used if no explicit routing information for a service data flow is provided;
- the route for an IP flow.

The PCEF shall derive the routing information from the IP flow mobility flow bindings installed in the PCEF, as defined in TS 23.261 [23].

If there are events which can not be monitored in the PCEF, the PCEF shall provide the information about the required event triggers to the PCRF using the PCEF initiated IP-CAN Session Modification procedure, as defined in clause 7.4.1, or in the response to a PCRF initiated IP-CAN Session Modification, as defined in clause 7.4.3. If the triggers were provided by the OCS at credit authorization, it is an implementation option whether a successful confirmation is required from the PCRF in order for the PCEF to consider the credit (re-)authorization procedure to be successful.

IP-CAN-specific parameters may be sent by the PCRF to the PCEF or the PCEF to the PCRF. The IP-CAN Session Modification procedure may be used to deliver these parameters to allow interaction between the BBERF and the PCEF by way of the PCRF. This is required in accesses that require these parameters to be sent indirectly.

The PCEF shall support usage monitoring as specified in clause 4.4.

The PCEF enhanced with ADC shall handle application traffic detection as per request from PCRF as well as report about the detected application traffic along with service data flow descriptions, if deducible, to the PCRF, if requested by the PCRF.

The PCEF shall support traffic steering as specified in clause 6.1.17.

The PCEF shall support 3GPP PS Data Off as specified in clause 6.1.21.

The PCEF forwards the Maximum Packet Loss Rate for UL and DL, if received from PCRF for the PCC rule bound to a QCI=1 bearer. In the case multiple PCC Rules share one QCI=1 bearer and the PCEF received multiple Maximum Packet Loss Rates, the PCEF chooses the lowest value per direction related to these PCC rules.

When the PCRF provides updated PCC rules for the IP-CAN session to the PCEF, and the PCC rules were not enforced due to that the UE is in suspend state, e.g. due to SRVCC to GERAN without DTM support as specified in clause 6.2.2.1 in the TS 23.216 [28] or CSFB to UTRAN without PS Handover as specified in clause 6.5 in the TS 23.272 [52], the PCEF shall indicate to the PCRF that the PCC Rules were not enforced with the reason that the UE is in suspend state. Upon reception of the failure indication, the PCRF may subscribe to UE resumed from suspend state event trigger.

6.2.2.2 Service data flow detection

This clause refers to the detection process that identifies the packets belonging to a service data flow. Each PCC rule contains a service data flow template, which defines the data for the service data flow detection as a set of service data flow filters or an application identifier referring to an application detection filter.

For PCC rules that contain an application identifier (i.e. that refer to an application detection filter), the order and the details of the detection are implementation specific. The application detection filter may be extended with the PFDs provided by the PFDF as described in clause 6.1.20. The new PFDs provided by the PFDF replace the existing ones in the PCEF. When multiple PFDs are associated with application identifier, the application is detected when any of the PFDs associated with the application identifier is matched. In addition, if a PFD contains multiple attributes, the PFD is only matched when every attribute contained in the PFD has a matching value.

Once an application has been detected, enforcement and charging shall however be applied under consideration of the PCC rule precedence, i.e. when multiple PCC rules overlap, only the enforcement and charging actions of the PCC rule with the highest precedence shall be applied.

For PCC Rules that contain an application identifier (i.e. that refer to an application detection filter) the detection of the uplink part of the service data flow may be active in parallel on other bearers with non-GBR QCI (e.g. the default bearer) in addition to the bearer where the PCC rule is bound to.

NOTE 1: When PCC rules with application detection filters cannot be used to generate traffic mapping information for the UE, the application detection may need to inspect traffic on multiple bearers. The PCEF uses implementation specific logic to determine for what bearers the up-link service data flow detection applies. The uplink traffic will get the QoS of the bearer carrying the traffic. The QCI of the bearer may therefore be different than the QCI of the PCC rule detecting the service data flow. The charging and other enforcement functions performed by the PCEF will still be carried out based on parameters of the PCC rule detecting the service data flow. If the PCC rule contains a GBR QCI, the GBR resource reservation will only apply on the bearer where the PCC rule is bound to. The PCRF can prevent that uplink GBR resources are reserved by providing an uplink GBR value of zero in the PCC rule.

The PCEF shall discard a packet in the case that there is no service data flow template of the same direction (i.e. of the IP-CAN session for the downlink or of the IP-CAN bearer for the uplink) detecting the packet.

NOTE 2: For the uplink direction, discarding packets due to no matching service data flow template is also referred to as uplink bearer binding verification. For the case a BBERF is present, uplink bearer binding verification is done by the BBERF.

NOTE 3: If PCC Rule containing an Application Identifier inspects traffic on multiple bearers in the uplink, such detected traffic counts as detection by that PCC rule.

The remainder of this clause describes the detection of service data flows identified by a service data flow filter (i.e. does not apply to PCC rules containing an application identifier):

- Each service data flow template may contain any number of service data flow filters;
- Each service data flow filter is applicable uplink, downlink or both uplink and downlink;
- Service data flow filters are applied for each direction, so that the detection is applied independently for the downlink and uplink directions;

NOTE 4: Service data flow filters that apply in both uplink and downlink should be used whenever the underlying IP-CAN and access type supports this.

NOTE 5: A service data flow template may include service data flow filters for one direction, or for both directions.

- Each service data flow filter may contain information about whether the explicit signalling of the corresponding traffic mapping information to the UE is required.

NOTE 6: This information enables e.g. the generation/removal of traffic mapping information for a default IP-CAN bearer as well as the usage of PCC rules with specific service data flow filters on a default IP-CAN bearer without the need to generate traffic mapping information.

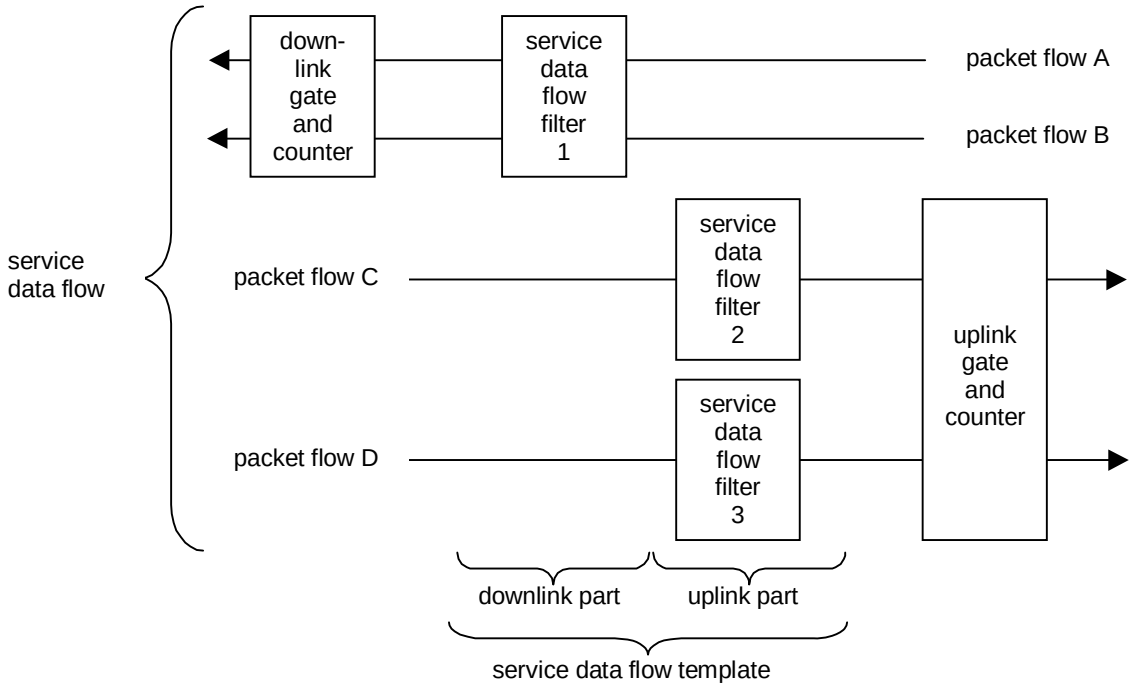

Figure 6.3: Relationship of service data flow, packet flow, service data flow template and service data flow filter

Service data flow filters identifying the service data flow may:

- be a pattern for matching the IP 5 tuple (source IP address or IPv6 network prefix, destination IP address or IPv6 network prefix, source port number, destination port number, protocol ID of the protocol above IP). In the pattern:
  - a value left unspecified in a filter matches any value of the corresponding information in a packet;
  - an IP address may be combined with a prefix mask;
  - port numbers may be specified as port ranges.
  - the pattern can be extended by the Type of Service (TOS) (IPv4) / Traffic class (IPv6) and Mask;
- consist of the destination IP address and optional mask, protocol ID of the protocol above IP, the Type of Service (TOS) (IPv4) / Traffic class (IPv6) and Mask and the IPSec Security Parameter Index (SPI);
- consist of the destination IP address and optional mask, the Type of Service (TOS) (IPv4) / Traffic class (IPv6) and Mask and the Flow Label (IPv6).

NOTE 7: The details about the IPSec Security Parameter Index (SPI), the Type of Service (TOS) (IPv4) / Traffic class (IPv6) and Mask and the Flow Label (IPv6) are defined in clause 15.3 of TS 23.060 [12].

- extend the packet inspection beyond the possibilities described above and look further into the packet and/or define other operations (e.g. maintaining state). Such service data flow filters must be predefined in the PCEF.

NOTE 8: Such filters may be used to support filtering with respect to a service data flow based on the transport and application protocols used above IP. This shall be possible for HTTP and WAP. This includes the ability to differentiate between TCP, Wireless-TCP according to WAP 2.0, WDP, etc, in addition to differentiation at the application level. Filtering for further application protocols and services may also be supported.

For downlink traffic, the downlink parts of all the service data flow templates associated with the IP-CAN session for the destination address are candidates for matching in the detection process.

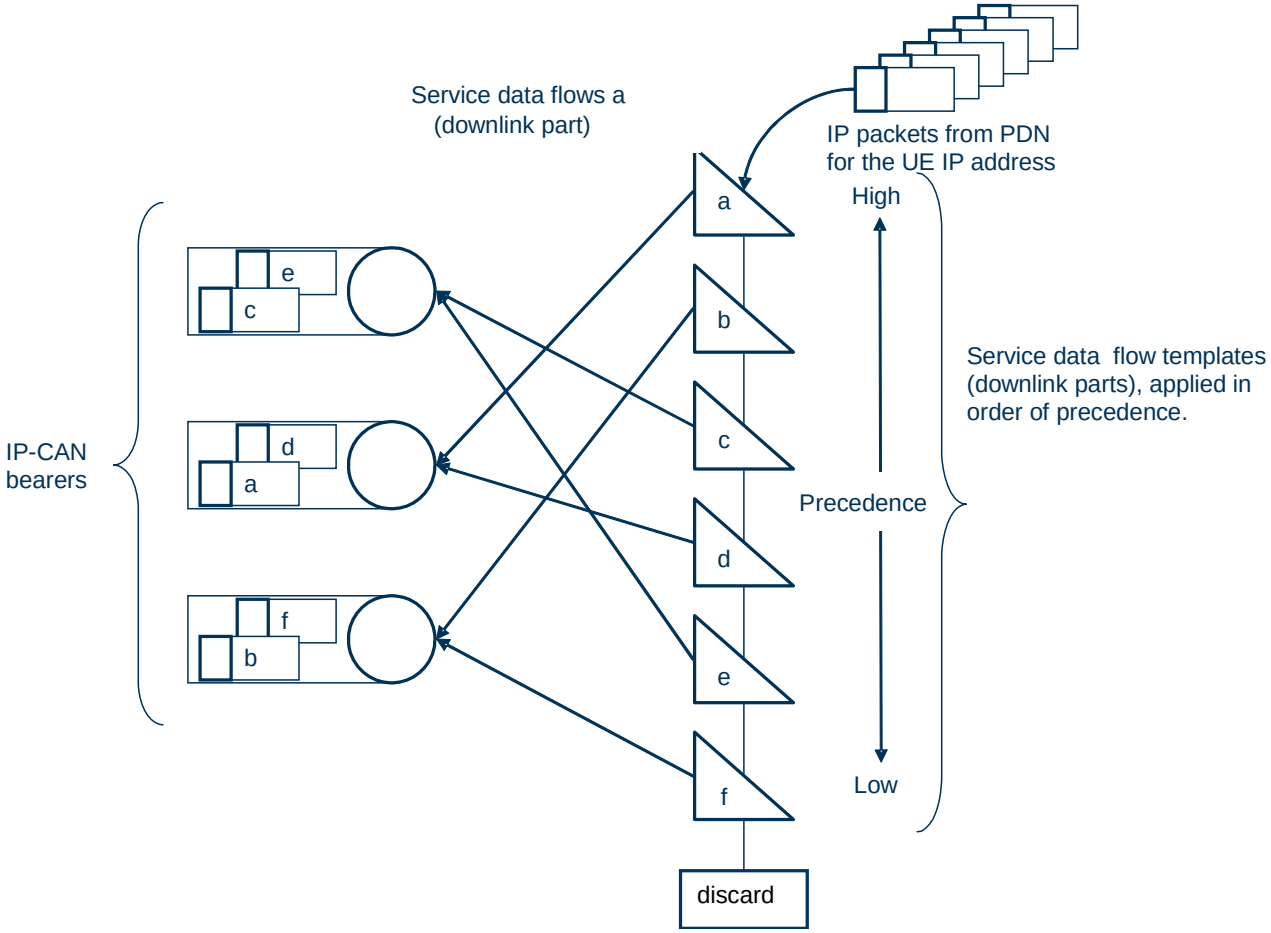

Figure 6.4: The service data flow template role in detecting the downlink part of a service data flow and mapping to IP-CAN bearers

For uplink traffic, the uplink parts of all the service data flow templates associated with the IP-CAN bearer (details according to clause A), are candidates for matching in the detection process.

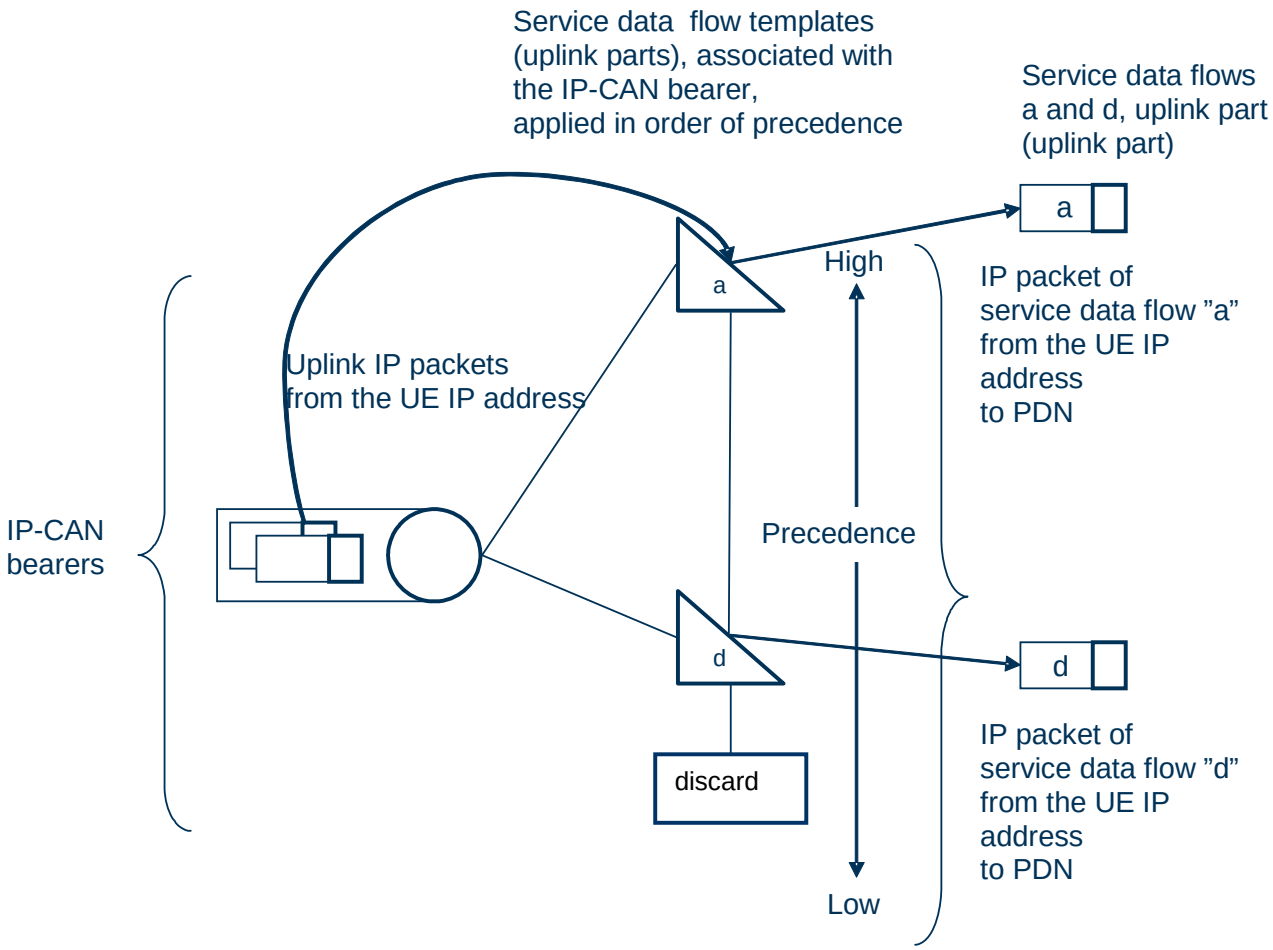

Figure 6.5: The service data flow template role in detecting the uplink part of a service data flow

NOTE 9: To avoid the PCEF discarding packets due to no matching service data flow template, the operator may apply open PCC rules (with wild-carded service data flow filters) to allow for the passage of packets that do not match any other candidate service data flow template.

Service data flow templates shall be applied in the order of their precedence.

6.2.2.3 Measurement

The PCEF shall support data volume, duration, combined volume/duration and event based measurement for charging. The Measurement method indicates what measurement type is applicable to the PCC rule.

NOTE 1: Event based charging is only applicable to predefined PCC rules and PCC rules using an application detection filter (i.e. with an application identifier).

The PCEF measurement measures all the user plane traffic, except traffic that PCC causes to be discarded.

The PCEF shall maintain a measurement per IP-CAN bearer (IP-CAN specific details according to Annex A and Annex D), and Charging Key combination.

If Service identifier level reporting is mandated in a PCC rule, the PCEF shall maintain a measurement for that Charging Key and Service Identifier combination, for the IP-CAN bearer (IP-CAN specific details according to Annex A and Annex D).

NOTE 2: In addition, the GW may maintain IP-CAN bearer level measurement if required by the operator.

For usage monitoring, the PCEF shall support volume and time measurement for an IP-CAN session and maintain a measurement for each IP-CAN session for which the PCRF has requested the Usage report trigger and provided threshold values on an IP-CAN session level. The PCEF shall be able to support volume and time measurements simultaneously for a given IP-CAN session.

The PCEF shall support volume and time measurement per Monitoring key and maintain a measurement for each Monitoring key if the PCRF has requested the Usage report trigger and provided threshold values on Monitoring key level. The PCEF shall be able to support volume and time measurements simultaneously for a given Monitoring Key.

The PCEF shall support simultaneous volume and time measurement for usage monitoring on IP-CAN session level and Monitoring key level for the same IP-CAN session.

Volume and time measurements for usage monitoring purposes on IP-CAN session level and on Monitoring key level shall be performed independently of each other. If the PCC rule is associated with an indication of exclusion from session level monitoring, the PCEF shall not consider the corresponding service data flow for the volume and time measurement on IP-CAN session level.

If the Usage report reached event trigger is set and a volume or a time threshold is reached, the PCEF shall report this event to the PCRF. The PCEF shall continue to perform volume or time measurement after the threshold is reached and before a new threshold is provided by the PCRF. At IP-CAN session termination or if the conditions defined in clause 6.6.2 for continued monitoring are no longer met, or if the PCRF explicitly requests a usage report, the PCEF shall inform the PCRF about the resources that have been consumed by the user since the last usage report for the affected Monitoring keys, including the resources consumed before and after the Monitoring time was reached, if provided according to clause 6.2.1.0.

If combined volume and time measurements are requested by the PCRF, then the reporting shall be done for both together. For example, if the volume threshold is reached, the consumed time shall be reported as well and, in order to continue combined volume and time measurements, the PCRF shall provide a new time threshold along with a new volume threshold. The PCEF shall continue to perform volume and time measurement after the threshold is reached and before a new threshold is provided by the PCRF. If new threshold is provided only for time or volume, then the measurements shall continue only for that provided type and the accumulated usage for the non provided type shall be discarded by the PCEF.

When the PCRF requests to report usage, the PCEF shall report the accumulated usage to the PCRF according to the provided usage threshold, i.e. the PCEF reports accumulated volume when the volume threshold was provided by the PCRF, accumulated time when the time threshold was provided by the PCRF and both accumulated volume and accumulated time when volume threshold and time threshold were provided by the PCRF.

If the Usage thresholds for a Monitoring key are not provided to the PCEF in the acknowledgement of an IP-CAN Session modification where its usage was reported, then the usage monitoring shall not continue in the PCEF for that Monitoring key.

When the Monitoring time occurs, the accumulated volume and/or time usage shall be recorded by the PCEF and:

- If the subsequent usage threshold value is provided, the usage threshold shall be reset to this value by the PCEF.
- Otherwise, the usage threshold shall be set by the PCEF to the remaining value of the threshold previously sent by the PCRF (i.e. excluding the accumulated usage).

The first usage report after the Monitoring Time was reached shall indicate the usage up to the Monitoring time and usage after the Monitoring time.

In order to support time based usage monitoring, the PCRF may optionally indicate to the PCEF, along with other usage monitoring information provided, the Inactivity Detection Time. This value represents the time interval after which the time measurement shall stop for the Monitoring key, if no packets are received belonging to the corresponding Monitoring Key during that time period. Time measurement shall resume on receipt of a further packet belonging to the Monitoring key.

Time measurement for a Monitoring key shall also be stopped when time based usage monitoring is disabled, if this happens before the Inactivity Detection Time is reached.

If an Inactivity Detection Time value of zero is provided, or if no Inactivity Detection Time is present within the usage monitoring information provided by the PCRF, the time measurement shall be performed continuously from the point at which it was started until time based usage monitoring is disabled.

6.2.2.4 QoS control

The PCEF enforces the authorized QoS for an IP-CAN bearer according to the information received via the Gx interface and depending on the bearer establishment mode.

Only the GBR per bearer is used for resource reservation (e.g. admission control in the RAN). The MBR (per PCC rule / per bearer) is used for rate policing.

For a UE-initiated IP-CAN bearer establishment or modification the PCEF receives the authorized QoS (QCI, ARP, GBR, MBR) for a bearer that the PCEF has identified for the PCRF. The PCEF shall enforce it which may lead to a downgrading or upgrading of the requested bearer QoS.

NOTE 1: The MBR is an average value, which is measured over some time period. Services may generate media with variable bitrate. For example, TS 26.114 [45] describes the bitrate variations that may be generated for real-time conversational media in the MTSI service. The policing function in the PCEF should take such bitrate variations into account.

For a network initiated IP-CAN bearer establishment or modification the PCEF receives the authorized QoS per PCC rule (QCI, ARP, GBR, MBR). For GBR bearers the PCEF should set the bearer's GBR to the sum of the GBRs of all PCC rules that are active and bound to that GBR bearer. If a set of PCC Rules is subject to resource sharing as specified in clause 6.1.14 the PCEF should use, for each applicable direction, the highest GBR from the set of PCC Rules sharing resources as input for calculating the bearer´s GBR. For GBR bearers the PCEF should set the bearer's MBR to the sum of the MBRs of all PCC rules that are active and bound to that GBR bearer. If a set of PCC Rules is subject to resource sharing as specified in clause 6.1.14 the PCEF may, for each applicable direction, use the highest MBR from the set of PCC Rules as input for calculating the bearer´s MBR.

NOTE 2: Since the PCRF controls the GBR value in the PCC rule, the PCRF can prevent that uplink GBR resources are reserved by providing an uplink GBR value of zero for that PCC rule, This may be useful e.g. for a PCC rule with application identifier as the uplink traffic can be received in other bearers than the one the PCC rule is bound to.

For an IP-CAN that supports non-GBR bearers that have a separate MBR (e.g. GPRS) the PCEF may, before or in connection with activation of the first PCC rule with a certain QCI, receive the authorized QoS (QCI, MBR) for that QCI. The authorized MBR per QCI only applies to non-GBR bearers, and it sets an upper limit for the MBR that the PCEF assigns to a non-GBR bearer with that QCI. In case multiple IP-CAN bearers within the same IP-CAN session are assigned the same QCI, the authorized MBR per QCI applies independently to each of those IP-CAN bearers. The PCRF may change the authorized MBR per QCI at any time. An authorized GBR per QCI shall not be signalled on Gx.

NOTE 3: The intention of the authorized MBR per QCI is to avoid frequent IP-CAN bearer modifications as PCC rules are dynamically activated and deactivated. That is, the PCEF may choose to assign the authorized MBR per QCI to a non-GBR bearer with that QCI.

6.2.2.5 Application Detection

The PCEF shall detect Start and Stop of the application traffic for the PCC rules used for application detection (i.e. with application identifier) that the PCRF has activated at the PCEF. The PCEF shall report, if the PCRF has subscribed to the event, unless the notification is muted for the specific PCC Rule, to the PCRF:

- For the Start of application event trigger: the application identifier and, when service data flow descriptions are deducible, the application instance identifier and the service data flow descriptions to use for detecting that application traffic with a dynamic PCC rule as defined in clause 6.1.4.

- For the Stop of application event trigger: the application identifier and if the application instance identifier was reported for the Start, also the application instance identifier as defined in the clause 6.1.4.

6.2.2.6 Traffic steering

When the PCRF provides a Traffic Steering Policy Identifier(s) in a PCC rule, the PCEF shall enforce the referenced traffic steering policy for the service data flow. A traffic steering policy is locally configured and can be used for the uplink, the downlink or for both directions.

To enforce the traffic steering policy, the PCEF performs deployment specific actions as configured for that traffic steering policy. The PCEF may for example perform packet marking where, for the traffic identified by the service data flow template (defined by an active PCC rule), the PCEF provides information for traffic steering, as part of the packets, to the (S)Gi-LAN. This information for traffic steering identifies, explicitly or implicitly, a specific set of service functions and their order via which the traffic needs to be steered in the (S)Gi-LAN.

6.2.3 Application Function (AF)

The Application Function (AF) is an element offering applications that require dynamic policy and/or charging control over the IP-CAN user plane behaviour. The AF shall communicate with the PCRF to transfer dynamic session information, required for PCRF decisions as well as to receive IP-CAN specific information and notifications about IP-CAN bearer level events. One example of an AF is the P-CSCF of the IM CN subsystem.

The AF may receive an indication that the service information is not accepted by the PCRF together with service information that the PCRF would accept. In that case, the AF rejects the service establishment towards the UE. If possible the AF forwards the service information to the UE that the PCRF would accept.

An AF may communicate with multiple PCRFs. The AF shall contact the appropriate PCRF based on either:

- the end user IP Address; and/or
- a UE identity that the AF is aware of.

NOTE 1: By using the end user IP address, an AF is not required to acquire any UE identity in order to provide information, for a specific user, to the PCRF.

In case of private IP address being used for the end user, the AF may send additional PDN information (e.g. PDN ID) over the Rx interface. This PDN information is used by the PCRF for session binding, and it is also used to help selecting the correct PCRF.

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 as described in clause 6.1.5.

The AF may use the IP-CAN bearer level information in the AF session signalling or to adjust the IP-CAN bearer level event reporting.

The AF may request the PCRF to report on IP-CAN bearer level events (e.g. the signalling path status for the AF session). The AF shall cancel the request when the AF ceases handling the user.

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

The AF may request the PCRF to report on the change of type of IP-CAN. The PCRF shall report the IP-CAN type and subsequent changes to the AF together with the information of the Radio Access Technology Type (e.g. UTRAN) as defined in access specific annexes. The change of the Radio Access Technology Type (e.g. UTRAN) shall be also reported to the AF, even if the IP-CAN type is unchanged.

The AF may request the PCRF to report any combination of the user location and/or UE Timezone at AF session establishment, modification or termination. For AF session termination the communication between the AF and the PCRF shall be kept alive until the PCRF report is received.

The AF may request the PCRF to report changes of the PLMN identifier where the UE is currently located at AF session establishment. The PLMN identifier reporting remains until the AF session is terminated.

If IP-CAN bearer resources corresponding to the AF session are released, the PCRF reports to the AF, if available, the reason why IP-CAN bearer resources are released i.e. RAN/NAS Release Cause, TWAN Release Cause or UWAN Release Cause.

If IP-CAN bearer resources corresponding to the AF session are released, the PCRF reports to the AF, if available, the User Location Information and/or the UE Timezone.

NOTE 3: The H-PCRF informs the AF of event triggers that cannot be reported. For detail see Annex L.

To support sponsored data connectivity (see Annex N), the AF may provide the PCRF with the sponsored data connectivity information, including optionally a usage threshold, as specified in clause 5.2.1. The AF may request the PCRF to report events related to sponsored data connectivity.

If the user plane traffic traverses the AF, the AF may handle the usage monitoring and therefore it is not required to provide a usage threshold to the PCRF as part of the sponsored data connectivity information.

In order to mitigate RAN user plane congestion, the Rx reference point enables transport of the following information from the PCRF to the AF:

- Re-try interval, which indicates when service delivery may be retried on Rx.

NOTE 4: Additionally, existing bandwidth limitation parameters on Rx interface during the Rx session establishment are available in order to mitigate RAN user plane congestion.

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 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.

The AF may contact the PCRF via the SCEF (and the Nt interface) to request a time window and related conditions for future background data transfer (as described in clause 6.1.16). If the PCRF replies with more than one transfer policy, the AF shall select one of them and inform the PCRF about the selected transfer policy. The reference ID provided by the PCRF shall be used by the AF during every subsequent transfer of AF session information related to this background data transfer (via the Rx interface).

6.2.4 Subscription Profile Repository (SPR)

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. 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.

NOTE 1: The SPR's relation to existing subscriber databases is not specified in this Release.

The SPR may provide the following subscription profile information (per PDN, which is identified by the PDN identifier):

- 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;
- 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.

The SPR may provide the following sponsored data connectivity profile information:

- A list of Application Service Providers and their applications per sponsor identity.

NOTE 2: The sponsored data connectivity profile may be locally configured at the PCRF.

If the IMS Signalling Priority is set, it indicates that the IMS Signalling Bearer and the Default Bearer are assigned ARP appropriate for MPS at the time of the establishment of the PDN connection for IMS, i.e. EPS Attach or PDN Connectivity Request.

The SPR may provide the following policy information related to an ASP (see clause 6.1.16):

- The ASP identifier;
- A transfer policy together with a reference ID, the volume of data to be transferred per UE, the expected amount of UEs and the network area information.

NOTE 3: The information related to an ASP is only available in the SPR after being stored by the PCRF as described in clauses 6.1.16 and 7.11.1.

NOTE 4: A transfer policy is only valid until the end of its time window. The removal of outdated transfer policies from the SPR is up to implementation.

6.2.5 Online Charging System

The Online Charging System (OCS) performs online credit control functions as specified in TS 32.240 [3].

The OCS may trigger the PCEF to initiate an IP-CAN bearer service termination at any point in time.

NOTE: As the OCS performs the credit control per charging key basis (and thus has not necessarily the knowledge about the existence of any specific service/application), it is recommended to use different charging keys for any service/application that shall not be unintentionally interrupted.

There may be several OCSs in a PLMN. The default OCS addresses (i.e. the primary address and secondary address) shall be locally pre-configured within the PCEF and TDF. OCS addresses may also be passed once per IP-CAN session or TDF session from the PCRF to the PCEF or TDF. The OCS addresses provided by the PCRF shall have a higher priority than the pre-configured ones.

6.2.6 Offline Charging System (OFCS)

The Offline Charging System is specified in TS 32.240 [3].

There may be several OFCSs in a PLMN. The default OFCS addresses (i.e. the primary address and secondary address) shall be locally pre-configured within the PCEF and TDF. OFCS addresses may also be passed once per IP-CAN session or TDF session from the PCRF to the PCEF or TDF. The addresses provided by the PCRF shall have a higher priority than the pre-configured ones.

6.2.7 Bearer Binding and Event Reporting Function (BBERF)

6.2.7.1 General

The BBERF includes the following functionalities:

- Bearer binding.
- Uplink bearer binding verification.
- Event reporting to the PCRF.
- Sending or receiving IP-CAN-specific parameters, to or from the PCRF.

6.2.7.2 Service data flow detection

The service data flow detection at the BBERF is identical to the detection at PCEF with the following modifications:

- If the service data flow is tunnelled at the BBERF, the BBERF uses information on the mobility protocol tunnelling header provided by the PCRF and the QoS rules to detect the service data flows.

For the uplink direction, the BBERF applies QoS rules with a bearer binding to the bearer that the packet arrived on. The uplink bearer binding verification is successful if there is a QoS rule with a matching uplink SDF filter. The BBERF shall discard packets for which the uplink bearer binding verification fails.

6.2.7.3 QoS Control

The ARP, GBR, MBR and QCI are used by the BBERF in the same way as in the PCEF for resource reservation.

When access network is not utilizing QCI based QoS parameters, the BBERF shall be able to convert a QoS class identifier value to QoS attribute values used in the access network and determine the QoS class identifier value from a set of QoS attribute values used in the access network.

NOTE: The definition of the mapping between QCI and Non 3GPP access specific QoS is outside of scope for 3GPP.

The BBERF controls the QoS that is provided to a combined set of service data flows. BBERF ensures that the resources which can be used by an authorized set of service data flows are within the "authorized resources" specified via the Gxx interface by "authorized QoS". The authorized QoS provides an upper bound on the resources that can be reserved (GBR) or allocated (MBR) for the service data flows.

In order to support the different IP-CAN bearer establishment modes (UE-only or UE/NW), the BBERF shall support the same procedures for handling different IP-CAN bearer establishment modes as specified for the PCEF in clauses 6.2.2.1 and 6.2.2.4.

6.2.8 User Data Repository (UDR)

The UDR is a functional entity that acts as a single logical repository storing user data. As such it may contain all subscriber/subscription related information needed by the PCRF. In deployment scenarios where the UDR is used it replaces the SPR. The UDR provides a unique reference point to fetch these subscriber/subscription data. This reference point is named Ud. More information on the UDR can be found in TS 23.335 [25].

The SPR data listed in clause 6.2.4 are stored in the UDR, the information model remains unspecified.

6.2.9 Traffic Detection Function (TDF)

6.2.9.1 General

The TDF is a functional entity that performs application detection and reporting of detected application and its service data flow description to the PCRF. The TDF supports solicited application reporting and/or unsolicited application reporting. The application detection filter may be extended with the PFDs provided by the PFDF as described in clause 6.1.20. The new PFDs provided by the PFDF replace the existing ones in the PCEF.

The TDF shall detect Start and Stop of the application traffic for the ADC rules that the PCRF has activated at the TDF (solicited application reporting) or which are pre-provisioned at the TDF (unsolicited application reporting). The TDF shall report, unless the notification is muted for the specific ADC Rule in case of solicited application reporting, to the PCRF:

- For the Start of application event trigger: the application identifier and, when service data flow descriptions are deducible, the application instance identifier and the service data flow descriptions to use for detecting that application traffic with a dynamic PCC rule as defined in clause 6.1.4.

- For the Stop of application event trigger: the application identifier and if the application instance identifier was reported for the Start, also the application instance identifier as defined in the clause 6.1.4.

For solicited application reporting, the PCRF can request the TDF to also perform enforcement actions, charging and usage monitoring.

For those cases where service data flow description is not possible to be provided by the TDF to the PCRF, the TDF performs:

- Gating;

- Redirection;
- Bandwidth limitation;
- Charging.

for the detected applications.

For those cases where service data flow description is provided by the TDF to the PCRF the actions resulting of application detection may be performed by the PCEF as part of the charging and policy enforcement per service data flow as defined in this document or may be performed by the TDF.

NOTE: The PCEF can be enhanced with application detection and control feature as specified in clause 6.2.2.5.

The TDF shall support usage monitoring as specified in clause 4.4 and the usage reporting functions as specified in clause 6.2.2.3 for the PCEF.

The TDF shall support data volume, duration, combined volume/duration and event based measurement for charging. The Measurement method indicates what measurement type is applicable for the ADC rule.

NOTE 1: Events to be charged are predefined in the TDF.

The TDF measurement measures all the user plane traffic, except packets discarded by ADC-rule enforcement or due to MBR-enforcement.

The TDF shall maintain a measurement per TDF session and Charging Key combination.

If Service identifier level reporting is mandated in an ADC rule, the TDF shall maintain a measurement for that Charging Key and Service identifier combination, for the TDF session.

If there are required events which cannot be monitored in the TDF (e.g. related to the location changes), the TDF shall request the information about these Event Triggers from the PCRF using either:

- The IP-CAN Session Establishment procedure, as defined in clause 7.2, or
- The PCEF initiated IP-CAN Session Modification procedure, as defined in clause 7.4.1, or
- In the response to a PCRF initiated IP-CAN Session Modification, as defined in clause 7.4.2, or
- Within the Update of the subscription information in the PCRF procedure, as defined in clause 7.5.

For unsolicited application reporting, the TDF performs only application detection and reporting functionality but neither enforcement actions nor usage monitoring. The TDF should handle each IPv4 address and IPv6 prefix, assuming the max prefix length used in the access network, within a separate TDF session. The PCRF shall, if needed, correlate TDF sessions that correspond to the same IP-CAN session.

The TDF shall support traffic steering as specified in clause 6.1.17.

6.2.9.2 Traffic steering

When the PCRF provides a Traffic Steering Policy Identifier(s) in an ADC rule, the TDF shall enforce the referenced traffic steering policy for the application. A traffic steering policy is locally configured and can be used for the uplink, the downlink or for both directions.

To enforce the traffic steering policy, the TDF performs deployment specific actions as configured for that traffic steering policy. The TDF may for example perform packet marking where, for the traffic identified by the Application Identifier or by the service data flow filter list (defined by an active ADC rule), the TDF provides information for traffic steering, as part of the packets, to the (S)Gi-LAN. This information for traffic steering identifies, explicitly or implicitly, a specific set of service functions and their order via which the traffic needs to be steered in the (S)Gi-LAN.

6.2.10 RAN Congestion Awareness Function (RCAF)

A RAN Congestion Awareness Function (RCAF) is an element which reports RAN User Plane Congestion Information (RUCI) via the Np interface to the PCRF to enable the PCRF to take the RAN user plane congestion status into account for policy decisions. The RCAF sends the RUCI to the PCRFs serving the UEs' PDN connections as follows:

- For a PDN connection in a non-roaming scenario the RCAF reports the RUCI to the PCRF.
- For a PDN connection in a local breakout scenario, based on operator configuration, the RCAF reports the RUCI to the V-PCRF.
- For a PDN connection in a home routed scenario, based on the roaming agreement with the HPLMN and operator configuration, the RCAF reports the RUCI to the H-PCRF.

NOTE 1: Reporting of congestion information to the HPLMN may be used e.g. in case of a group of PLMNs which belong to a single business entity.

The RCAF determines whether a given PDN connection is served in a local breakout or a home routed roaming scenario based on the APN operator identifier received as part of the APN information from the MME or the S4-SGSN as documented in TS 23.401 [17] and TS 23.060 [12], respectively.

NOTE 2: Operator configuration can be used to limit RUCI reporting on the Np interface to certain APNs only.

In addition if the RCAF detects that a UE is no longer subject to congestion (i.e. the UE is no longer detected in any of the congested cells that the RCAF is monitoring) then the RCAF shall indicate the no congestion state to the PCRFs serving the UE.

Any RUCI changes shall be reported by RCAF unless reporting restrictions apply.

The RCAF maintains a context on per UE and per APN basis. The context is identified by the IMSI and the APN. It contains the following information:

- The previously reported congestion level over the Np reference point.
- The reporting restrictions received from the PCRF. The reporting restrictions are stored by the RCAF until the PCRF explicitly signals to remove the reporting restrictions.
- The logical PCRF id received from the PCRF to identify the PCRF that is the Np destination for the RCAF when sending aggregate messages.

6.2.11 Service Capability Exposure Function (SCEF)

A Service Capability Exposure Function (SCEF) is an element which provides a means to securely expose the services and capabilities provided by 3GPP network interfaces (for further details see TS 23.682 [42]).

6.2.12 Traffic Steering Support Function (TSSF)

The TSSF is a function that receives traffic steering control information from the PCRF and ensures that the related traffic steering policy is enforced in the (S)Gi-LAN.

A traffic steering policy is locally configured in TSSF and can be used for uplink, downlink or for both directions. To ensure that the traffic steering policy is enforced, the TSSF performs deployment specific actions as configured for that traffic steering policy. For example, the TSSF may configure traffic detection and forwarding entities in the (S)Gi-LAN to fulfil the traffic steering policy.

6.2.13 Packet Flow Description Function (PFDF)

A Packet Flow Description Function (PFDF) is an element which stores PFDs associated with an application identifier and transfers them to the PCEF/TDF via Gw/Gwn interface to enable the PCEF/TDF to perform application detection when the PFDs are managed by a 3rd party SP.

The PFDF receives PFDs for an application identifier from the SCEF as defined in TS 23.682 [42].

6.3 Policy and charging control rule

6.3.1 General

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

Two different types of PCC rules exist: Dynamic rules and predefined rules. The dynamic PCC rules are provisioned by the 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 predefined PCC rules for QoS control is possible if the BBF remains in the PCEF during the lifetime of an IP-CAN session. In addition, predefined PCC rules may be used in a non-roaming situation and if it can be guaranteed that corresponding predefined QoS rules are configured in the BBF and activated along with the predefined PCC rules.

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

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.

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.

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).

The operator defines the PCC rules.

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.

Table 6.3: The PCC rule information

Information name	Description	Category	PCRF permitted to modify for a dynamic PCC rule in the PCEF
Rule identifier	Uniquely identifies the PCC rule, within an IP-CAN session. It is used between PCRF and PCEF for referencing PCC rules.	Mandatory	no
Service data flow detection	*This part defines the method for detecting packets belonging to a service data flow.*		
Precedence	Determines the order, in which the service data flow templates are applied at service data flow detection, enforcement and charging. (NOTE 9).	Conditional (NOTE 13)	yes
Service data flow template	Either a list of service data flow filters or an application identifier that references the corresponding application detection filter for the detection of the service data flow.	Mandatory (NOTE 7)	Conditional (NOTE 12)
Mute for notification	Defines whether application's start or stop notification is to be muted.	Conditional (NOTE 8)	No
Charging	*This part defines identities and instructions for charging and accounting that is required for an access point where flow based charging is configured*		
Charging key	The charging system (OCS or OFCS) uses the charging key to determine the tariff to apply to the service data flow.		yes
Service identifier	The identity of the service or service component the service data flow in a rule relates to.		yes
Sponsor Identifier	An identifier, provided from the AF which identifies the Sponsor, used for sponsored flows to correlate measurements from different users for accounting purposes.	Conditional (NOTE 6)	yes
Application Service Provider Identifier	An identifier, provided from the AF which identifies the Application Service Provider, used for sponsored flows to correlate measurements from different users for accounting purposes.	Conditional (NOTE 6)	yes
Charging method	Indicates the required charging method for the PCC rule. Values: online, offline or neither.	Conditional (NOTE 4)	no

Information name	Description	Category	PCRF permitted to modify for a dynamic PCC rule in the PCEF
Measurement method	Indicates whether the service data flow data volume, duration, combined volume/duration or event shall be measured. This is applicable to reporting, if the charging method is online or offline. Note: Event based charging is only applicable to predefined PCC rules and PCC rules used for application detection filter (i.e. with an application identifier).		yes
Application Function Record Information	An identifier, provided from the AF, correlating the measurement for the Charging key/Service identifier values in this PCC rule with application level reports.		no
Service identifier level reporting	Indicates that separate usage reports shall be generated for this Service identifier. Values: mandated or not required		Yes
Policy control	*This part defines how the PCEF shall apply policy control for the service data flow.*		
Gate status	The gate status indicates whether the service data flow, detected by the service data flow template, may pass (Gate is open) or shall be discarded (Gate is closed) at the PCEF.		Yes
QoS class identifier	Identifier for the authorized QoS parameters for the service data flow. Values: see NOTE 1.	Conditional (NOTE 2)	Yes
UL-maximum bitrate	The uplink maximum bitrate authorized for the service data flow	Conditional (NOTE 3)	Yes
DL-maximum bitrate	The downlink maximum bitrate authorized for the service data flow	Conditional (NOTE 3)	Yes
UL-guaranteed bitrate	The uplink guaranteed bitrate authorized for the service data flow		Yes
DL-guaranteed bitrate	The downlink guaranteed bitrate authorized for the service data flow		Yes
UL sharing indication	Indicates resource sharing in uplink direction with service data flows having the same value in their PCC rule		No
DL sharing indication	Indicates resource sharing in downlink direction with service data flows having the same value in their PCC rule		No

Information name	Description	Category	PCRF permitted to modify for a dynamic PCC rule in the PCEF
Redirect	Redirect state of the service data flow (enabled/disabled)	Conditional (NOTE 10)	Yes
Redirect Destination	Controlled Address to which the service data flow is redirected when redirect is enabled	Conditional (NOTE 11)	Yes
ARP	The Allocation and Retention Priority for the service data flow consisting of the priority level, the pre-emption capability and the pre-emption vulnerability	Conditional (NOTE 5)	Yes
Bind to Default Bearer	Indicates that the dynamic PCC rule shall always have its bearer binding with the default bearer.	Conditional (NOTE 15)	Yes
PS to CS session continuity	Indicates whether the service data flow is a candidate for vSRVCC.	Conditional	No
Access Network Information Reporting	This part describes access network information to be reported for the PCC rule when the corresponding bearer is established, modified or terminated.		
User Location Report	The serving cell of the UE is to be reported. When the corresponding bearer is deactivated, and if available, information on when the UE was last known to be in that location is also to be reported.		Yes
UE Timezone Report	The time zone of the UE is to be reported.		Yes
Usage Monitoring Control	*This part describes identities required for Usage Monitoring Control.*		
Monitoring key	The PCRF uses the monitoring key to group services that share a common allowed usage.		Yes
Indication of exclusion from session level monitoring	Indicates that the service data flow shall be excluded from the IP-CAN session usage monitoring		Yes
Traffic Steering Enforcement Control	This part describes identities required for Traffic Steering Enforcement Control.		
Traffic steering policy identifier(s)	Reference to a pre-configured traffic steering policy at the PCEF (NOTE 14).		Yes
NBIFOM related control Information	*This part describes PCC rule information related with NBIFOM (defined in TS 23.161 [43]. Refer also to clause 6.1.18.*		
Allowed Access Type	The access to be used for traffic identified by the PCC rule		Yes
Routing Rule Identifier	The Routing Rule identifier to be used in NBIFOM routing rule		No

Information name	Description	Category	PCRF permitted to modify for a dynamic PCC rule in the PCEF
RAN support information	*This part defines information supporting the RAN for e.g. handover threshold decision.*		
UL Maximum Packet Loss Rate	The maximum rate for lost packets that can be tolerated in the uplink direction for service data flow. *It is defined in clause 5.4.1 of TS 23.401 [17].*	Conditional (NOTE 16)	Yes
DL Maximum Packet Loss Rate	The maximum rate for lost packets that can be tolerated in the downlink direction for service data flow. *It is defined in clause 5.4.1 of TS 23.401 [17].*	Conditional (NOTE 16)	Yes

NOTE 1: The QoS class identifier is scalar and accommodates the need for differentiating QoS in all types of 3GPP IP-CAN. The value range is expandable to accommodate additional types of IP-CAN.
NOTE 2: The QoS class identifier is mandatory when the bearer binding is allocated to the PCEF.
NOTE 3: Mandatory when the QoS class identifier is of Resource Type GBR. Used to activate policy control on SDF level at the PCEF.
NOTE 4: Mandatory if there is no default charging method for the IP-CAN session.
NOTE 5: Mandatory when policy control on SDF level applies unless otherwise stated in an access-specific Annex.
NOTE 6: Applicable to sponsored data connectivity.
NOTE 7: Either service data flow filter(s) or application identifier shall be defined per each rule. application identifier can only be used for PCEF enhanced with ADC.
NOTE 8: Optional and applicable only if application identifier exists within the rule.
NOTE 9: For PCC rules based on an application detection filter, the precedence is only relevant for the enforcement, i.e. when multiple PCC rules overlap, only the enforcement, reporting of application starts and stops, monitoring, and charging actions of the PCC rule with the highest precedence shall be applied.
NOTE 10: Optional and applicable only if application identifier exists within the rule.
NOTE 11: If Redirect is enabled.
NOTE 12: YES, in case the service data flow template consists of a set of service data flow filters. NO in case the service data flow template consists of an application identifier.
NOTE 13: The Precedence is mandatory for PCC rules with SDF template containing SDF filter(s). For dynamic PCC rules with SDF template containing an application identifier, the precedence is either preconfigured in PCEF or provided in the PCC rule from PCRF.
NOTE 14: The Traffic steering policy identifier can be different for uplink and downlink direction. If two Traffic steering policy identifiers are provided, then one is for uplink direction, while the other one is for downlink direction.
NOTE 15: The presence of this attribute causes the QCI/ARP of the rule to be ignored. This attribute is defined for selected accesses as specified in the access specific Annexes.
NOTE 16: Optional and applicable only for voice service data flow in this Release.

The *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.

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 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. The same application identifier value can occur in more than one PCC rule with the following restrictions:

- 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.

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.

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.

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. For dynamic PCC rules that contain an application identifier, the Precedence shall be either 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.

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.

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).

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

NOTE 7: Assigning the same Charging key for several service data flows implies that the charging does not require the 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.

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

NOTE 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.

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

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

The *Charging method* indicates whether online charging, 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 mandatory if there is no default charging method for the IP-CAN session.

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

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.

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.

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 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.

The *Gate* indicates whether the PCEF shall let a packet identified by the PCC rule pass through (gate is open) the PCEF, or the PCEF shall discard (gate is closed) the packet.

NOTE 11: A packet, matching a PCC Rule with an open gate, may be discarded due to credit management reasons.

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.

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.

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

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

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

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

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

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.

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.

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

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

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

The *Bind to Default Bearer* indicates that the dynamic PCC rule shall be bound to the default bearer.

The *PS to CS session continuity* is present if the service data flow is a candidate for vSRVCC according to TS 23.216 [28].

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.

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

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

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.

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. The PCEF uses the *Allowed Access Type* as input for the bearer binding. When network-initiated NBIFOM mode applies, the PCEF shall also create / modify / delete a corresponding Routing Rule for such a PCC rule at the UE as described in clause 6.1.18.2. 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 default NBIFOM access.

The *Routing Rule Identifier* applies only in case of NBIFOM. The PCRF provides it to the PCEF only when network-initiated NBIFOM mode applies.

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

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

6.3.2 Policy and charging control rule operations

Policy and charging control rule operations consist of activation, modification and de-activation of PCC rules.

Activation of a dynamic PCC rule provides the PCC rule information to the PCEF via the Gx reference point.

Activation of a predefined PCC rule provides an identifier of the relevant PCC rule to the PCEF via the Gx reference point.

Activation of a predefined PCC rule, not known in the PCRF, may be done by the PCEF based on operator policy. The PCEF may only activate such predefined PCC rule if there are no UE provided traffic mapping information related to the IP-CAN bearer. Further restrictions regarding the usage of predefined PCC rules are described in clause 6.3.1.

An active PCC rule means that:

- the service data flow template shall be used for service data flow detection;
- the service data flow template shall be used for mapping of downlink packets to the IP-CAN bearer determined by the bearer binding;
- the service data flow template shall be used for service data flow detection of uplink packets on the IP-CAN bearer determined by the bearer binding;
- usage data for the service data flow shall be recorded (further details can be found in clause 6.1.2 Reporting and clause 6.1.3 Credit Management);
- policies associated with the PCC rule, if any, shall be invoked.
- for service data flow detection with an application detection filter, the start or the stop of the application traffic is reported to the PCRF, if applicable and requested by the PCRF. In that case, the notification for Start may include service data flow filters, (if possible to provide) and the application instance identifier associated with the service data flow filters.

A predefined PCC rule is known at least, within the scope of one access point.

NOTE 1: The same predefined PCC rule can be activated for multiple IP-CAN bearers in multiple IP-CAN sessions.

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 service data flow detection for the whole IP-CAN session.

The PCRF may, at any time, modify an active, dynamic PCC rule.

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.

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

A PCC rule with only a deferred activation time shall be inactive until that time. A PCC 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. An inactive PCC rule, that has not been activated yet, is still considered to be installed, and may be removed by the PCRF.

The PCRF may modify a currently installed PCC rule, including setting, modifying or clearing its deferred activation and/or deactivation time. 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.

NOTE 2: In this case, the PCRF omission of an attribute that has a prior value will erase that attribute from the rule.

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

Deferred modification of PCC rules shall not be applied for changes of the QoS or service data flow filter information of PCC rules.

6.4 IP-CAN bearer and IP-CAN session related policy information

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.

Table 6.4 lists the PCC related IP-CAN bearer and IP-CAN session related policy information.

Table 6.4: PCC related IP-CAN bearer and IP-CAN session related policy information

Attribute	Description	PCRF permitted to modify the attribute	Scope
Charging information (NOTE 2)	Defines the containing OFCS and/or OCS addresses.	No	IP-CAN session
Default charging method (NOTE 2)	Defines the default charging method for the IP-CAN session.	No	IP-CAN session
Event trigger	Defines the event(s) that shall cause a re-request of PCC rules for the IP-CAN bearer.	Yes	IP-CAN session
Authorized QoS per bearer (UE-initiated IP-CAN bearer activation/modification) (NOTE 1)	Defines the authorised QoS for the IP-CAN bearer (QCI, GBR, MBR).	Yes	IP-CAN bearer
Authorized MBR per QCI (network initiated IP-CAN bearer activation/modification) (NOTE 1) (NOTE 3)	Defines the authorised MBR per QCI.	Yes	IP-CAN session
Revalidation time limit	Defines the time period within which the PCEF shall perform a PCC rules request.	Yes	IP-CAN session
PRA Identifier(s)	Defines the Presence Reporting Area(s) to monitor for the UE with respect to entering/leaving	Yes	IP-CAN session
List(s) of Presence Reporting Area elements (NOTE 4)	Defines the elements of the Presence Reporting Area(s)	Yes	IP-CAN session
Default NBIFOM access	The access to be used for all traffic that does not match any existing Routing Rule	Yes (only at the addition of an access to the IP-CAN session)	IP-CAN session
NOTE 1: Depending on the bearer establishment mode; only one Authorized QoS information has to be used. NOTE 2: These attributes should not be provided to BBERF. NOTE 3: This attribute is only applicable when the IP-CAN supports non-GBR bearers that have a separate MBR (e.g. for GPRS). NOTE 4: The list of PRA elements shall be a short list of elements.			

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.

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.

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.

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.

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.

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.

The PCEF shall combine the requests from PCRF and the OCS.

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). The PCEF reports the PRA Identifier(s) and indication(s) whether the UE is inside or outside the Presence Reporting Area(s), and indication(s) if the corresponding Presence Reporting Area(s) is set to inactive by the serving node to the PCRF and/or the OCS.

NOTE: The serving node can activate the reporting for the PRAs which are inactive as described in the TS 23.401 [17].

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 the UE enters or leaves a Presence Reporting Area.

The PCEF stores PCRF or OCS subscription to reporting for changes of UE presence in Presence Reporting Area and forwards the PRA Identifier(s) and indication(s) whether the UE is inside or outside the Presence Reporting Area(s) received from the serving node according to the corresponding subscription.

When a PRA set identified by a PRA Identifier was subscribed to report changes of UE presence in Presence Reporting Area by the PCRF and/or OCS, the PCEF additionally receives the PRA Identifier of the PRA set from the serving node, along with the individual PRA Identifier(s) belonging to the PRA set and indication(s) of whether the UE is inside or outside the individual Presence Reporting Area(s), as described in TS 23.401 [17].

6.4a TDF session related policy information

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.

Table 6.4a lists the TDF session related policy information.

Table 6.4a: TDF session related policy information

Attribute	Description	PCRF permitted to modify the attribute
Charging Characteristics	Defines how to control TDF behaviour regarding online and offline charging.	No
Charging information	Defines the containing OFCS and/or OCS addresses.	No
Default charging method	Defines the default charging method for the TDF session.	No
Event trigger	Defines the event(s) that shall cause a re-request of ADC rules for the TDF session.	Yes
Maximum downlink bit rate	Defines the maximum downlink bit rate per TDF session.	Yes
Maximum uplink bit rate	Defines the maximum uplink bit rate per TDF session.	Yes
ADC Revalidation time limit	Defines the time period within which the TDF shall perform an ADC rules request.	Yes

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.

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 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.

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.

Upon every interaction with the TDF, the PCRF may provide Maximum downlink bit rate and/or Maximum uplink bit rate for the TDF session.

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.

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.

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.

6.4b APN related policy information

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.

Table 6.4b-1 lists the applicable PCC specific APN related policy information.

Table 6.4b-1: PCC specific APN related policy information

Attribute	Description	PCRF permitted to modify the attribute	Scope
Authorized APN-AMBR	Defines the APN-AMBR for the total bandwidth usage of non-GBR QCI traffic at the APN.	Yes	All IP-CAN sessions for the same UE within the same APN
Subsequent APN-AMBR (NOTE 1)	Defines the APN-AMBR for the total bandwidth usage of non-GBR QCI traffic at the APN to be applied by the PCEF when the APN-AMBR change time is reached.	No (NOTE 2)	All IP-CAN sessions for the same UE within the same APN
APN-AMBR change time (NOTE 1)	Defines the time at which the PCEF shall apply the Subsequent APN-AMBR for the total bandwidth usage of non-GBR QCI traffic at the APN.	No (NOTE 2)	All IP-CAN sessions for the same UE within the same APN
NOTE 1: Both parameters shall be provided together. The PCRF may provide up to four instances of them. If multiple instances are provided, the values of the APN-AMBR change time have to be different and should not be too close to each other in order to reduce the risk for signalling overload. NOTE 2: The PCRF may replace all instances that have been provided previously with a new instruction. A previously provided Subsequent APN-AMBR or APN-AMBR change time cannot be individually modified.			

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.

NOTE 1: There is always an unconditional value for the APN-AM BR 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.

NOTE 2: In order to reduce the risk for signalling overload, the PCRF should avoid simultaneous provisioning of Authorized APN-AMBR for many UEs (e.g. by spreading over time).

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.

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.

Conditional Authorized APN-AMBR(s) are not applied for a PDN connection supporting NBIFOM.

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.

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 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.

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.

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.

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.

6.5 Quality of Service Control rule

6.5.1 General

The Quality of Service control rule (QoS rule) comprises the information that is required to enable the user plane detection and the QoS control for a service data flow in the BBERF. The packets detected by applying the service data flow template of a QoS rule are designated a service data flow.

NOTE 1: The BBERF only supports service data flow templates consisting of a set of service data flow filters.

The PCRF shall ensure that each PCC rule in the PCEF has a corresponding active QoS rule in the BBERF. The QoS rule shall contain the same service data flow template, precedence and the QoS information as the corresponding PCC rule.

NOTE 2: During the course of a BBERF change procedure the BBERF might not be able to maintain the correspondence throughout the procedure. The post-condition for the procedure shall however be that corresponding PCC and QoS rules are active at the PCEF and BBERF.

There are defined procedures for activation, modification and deactivation of QoS rules (as described in clause 6.5.2). The PCRF may activate, modify and deactivate a QoS rule over the Gxx reference point.

The QoS rules are derived from the PCC rules.

Table 6.5 lists the information contained in a QoS rule, including the information name and whether the PCRF may modify this information in a QoS rule which is active in the BBERF. For the IE description, refer to clause 6.3.1. The Category field indicates if a certain piece of information is mandatory or not for the construction of a QoS rule, i.e. if it is possible to construct a QoS rule without it.

Table 6.5: The QoS rule information

Information name	Category	PCRF permitted to modify for an active QoS rule in the BBERF
Rule identifier (NOTE 1)	Mandatory	No
Service data flow detection		
Precedence	Mandatory	Yes
Service data flow template	Mandatory	Yes
QoS control		
QoS class identifier (NOTE 2)	Mandatory	Yes
UL-maximum bitrate	Conditional (NOTE 3)	Yes
DL-maximum bitrate	Conditional (NOTE 3)	Yes
UL-guaranteed bitrate	Conditional (NOTE 3)	Yes
DL-guaranteed bitrate	Conditional (NOTE 3)	Yes
UL sharing indication		No
DL sharing indication		No
ARP	Conditional (NOTE 3)	Yes
PS to CS session continuity	Conditional	No
Access Network Information Reporting		
User Location Report	Conditional	Yes
UE Timezone Report	Conditional	Yes
NOTE 1: The Rule-Identifier uniquely defines an active QoS rule for a certain BBERF within the scope of a UE. NOTE 2: The QoS class identifier is scalar and accommodates the need for differentiating QoS in all types of IP-CAN. The value range is expandable to accommodate operator specific policies. NOTE 3: If present in the corresponding PCC rule.		

6.5.2 Quality of Service control rule operations

QoS control rule operations consist of activation, modification and de-activation of QoS rules.

Activation of a dynamic QoS rule provides the QoS rule information to the BBERF via the Gxx reference point.

An active QoS rule means that:

- the service data flow template shall be used for service data flow detection;
- the service data flow template shall be used for mapping of downlink packets to the IP-CAN bearer determined by the bearer binding;
- the service data flow template shall be used for service data flow detection of uplink packets on the IP-CAN bearer determined by the bearer binding;
- QoS procedures associated with the QoS rule, if any, shall be invoked.

The PCRF may, at any time, modify an active QoS rule.

The PCRF may, at any time, deactivate an active QoS rule in the BBERF via the Gxx reference point. At IP-CAN bearer termination all active QoS rules on that bearer are deactivated without explicit instructions from the PCRF to do so.

6.6 Usage Monitoring Control specific information

6.6.1 General

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.

Table 6.6: Usage Monitoring Control related information

Information name	Description	Category	Scope
Monitoring key	The PCRF uses the monitoring key to group services that share a common allowed usage.	Mandatory	IP-CAN session, TDF session
Volume threshold (NOTE 1)	Defines the traffic volume value after which the PCEF or the TDF shall report usage to the PCRF for this monitoring key.	Optional	Monitoring key
Time threshold (NOTE 1)	Defines the resource time usage after which the PCEF or the TDF shall report usage to the PCRF.	Optional	Monitoring key
Monitoring time	Defines the time at which the PCEF or the TDF shall reapply the Volume and/or Time Threshold.	Optional	Monitoring Key
Subsequent Volume threshold	Defines the traffic volume value after which the PCEF or the TDF shall report usage to the PCRF for this Monitoring key for the period after the Monitoring time.	Optional, Conditional (NOTE 2)	Monitoring Key
Subsequent Time threshold	Defines resource time usage after which the PCEF or the TDF shall report usage to the PCRF for this Monitoring key for the period after the Monitoring time.	Optional, Conditional (NOTE 2)	Monitoring Key
Inactivity Detection Time	Defines the period of time after which the time measurement shall stop, if no packets are received.	Optional, Conditional (NOTE 3)	Monitoring Key
NOTE 1: This attribute is also used by the PCEF/TDF, e.g. during IP-CAN/TDF session termination, to inform the PCRF about the resources that have been consumed by the UE. NOTE 2: This attribute is applicable in presence of Monitoring Time only. NOTE 3: This attribute is applicable in presence of Time threshold only.			

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.

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.

The *Volume threshold* indicates the overall user traffic volume value after which the PCEF or the TDF shall report the Usage threshold reached trigger to the PCRF.

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.

The *Monitoring time* indicates the time at which the PCEF or the 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.

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.

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

6.6.2 Usage Monitoring Control operations

Usage monitoring on IP-CAN session, TDF session or monitoring key level is active in the PCEF or TDF provided that certain conditions are met. The conditions for continued monitoring on session level are:

- For IP-CAN session level monitoring at the PCEF, an IP-CAN session is active and a volume and/or time threshold value for the IP-CAN session has been provided.
- For TDF session level monitoring at the TDF, a TDF session is active and a volume and/or time threshold value has been provided.

For usage monitoring on Monitoring key level at the PCEF or the TDF the following conditions are applicable:

- A volume and/or time threshold has been provided for a Monitoring key to the PCEF and there is at least one PCC rule activated for the IP-CAN session that is associated with that Monitoring key.
- A volume and/or time threshold has been provided for a Monitoring key to the TDF and there is at least one ADC rule at the TDF activated for the TDF session that is associated with that Monitoring key.

NOTE: The PCRF is recommended to use monitoring so that the same traffic is not monitored by both PCC rules and ADC rules. This avoids double counting.

6.7 S2c based IP flow mobility Routing rule

6.7.1 General

The clause 6.7 refers to UE based IP flow mobility as described in TS 23.261 [23].

The routing rule comprises the information that is required for the PCRF to install the QoS rules for a service data flow at the right BBERF in flow mobility scenarios. The PCRF relies on the IP flow mobility routing information contained in the IP flow mobility routing rule to the applicable BBERF for each PCC/QoS rule. The IP flow mobility routing rules are provided by the PCEF to the PCRF during IP-CAN session establishment or modification.

The PCEF derives IP flow mobility routing rules based on flow binding information received from the UE as described in TS 23.261 [23].

Table 6.7 lists the information contained in a routing rule, including the information name, the description and whether the PCEF may modify this information in an updated version of the rule. The Category field indicates if a certain piece of information is mandatory or not.

Table 6.7: The routing rule information

Information name	Description	Category	PCEF permitted to modify in an update
Rule identifier	Uniquely identifies the routing rule within an IP-CAN session. It is assigned by the PCEF.	Mandatory	No
Routing information	*This clause defines the method for detecting packets belonging to a flow and the route for the flow.*		
Precedence	Determines the order, in which the routing filters are applied.	Mandatory	Yes
Packet filter	A list of packet filters for the detection of IP flows.	Mandatory	Yes
IP flow mobility Routing Address	The IP flow mobility Routing Address that the matching IP flows use.	Mandatory	Yes

The *Rule identifier* shall be unique for a routing rule within an IP-CAN session. It is assigned by the PCEF.

The *Precedence* defines in what order the routing rules is used by the PCRF to determine where to route a service data flow. The Precedence is derived from the priority included in the Binding Update as specified in TS 23.261 [23].

The *Packet filter* may comprise any number of packet filters, containing information for matching service data flows. The format of the packet filters is the same as the service data flow filter described in clause 6.2.2.2. A default packet filter can be specified by using wild card filter.

The *IP flow mobility Routing Address* identifies the IP address to be used for all service data flows matching the packet filters specified for this routing rule. The IP flow mobility Routing Address can be equal to the care-of address, or to the UE IP address (home address) in case of home link operations.

6.7.2 Routing rule operations

IP flow mobility routing rule operations consist of installation, modification and removal of routing rules.

During installation of a routing rule, the PCEF provides the routing rule information to the PCRF via the Gx reference point. The PCRF uses all the installed routing rules related to an IP-CAN Session to select BBERF for any service data flow related for that IP-CAN Session.

The PCEF may, at any time, modify or remove an installed routing rule based on updated flow binding information received from the UE as described in TS 23.261 [23].

6.8 Application Detection and Control Rule

6.8.1 General

The Application Detection and Control rule (ADC rule) comprises the information that is required in order to:

- 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.

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.

ADC rules definitions are assumed to be directly provisioned into the TDF or TSSF and referenced by the PCRF with the ADC Rule identifier.

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.

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.

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 deactivate an ADC rule at any time. The modification procedure is applicable to dynamic ADC rules only.

The operator defines the ADC rules.

Table 6.8 lists the information contained in an ADC rule that can be exchanged over the Sd and St reference point, including the information element name, the description, whether the PCRF may modify this information in a dynamic ADC rule which is active in the TDF and the applicable reference point (i.e. Sd and/or St) for the corresponding information element. The Category field indicates if a certain piece of information is mandatory or not for the construction of an ADC rule, i.e. if it is possible to construct an ADC rule without it.

Table 6.8: The Application Detection and Control rule information

Information name	Description	Category	PCRF permitted to modify for a dynamic ADC rule	Applicable reference point
ADC Rule identifier	Uniquely identifies the ADC rule within a TDF/TSSF session. It is used between PCRF and TDF/TSSF for referencing ADC rules.	Mandatory	No	Sd, St
Application detection	*This clause defines the detection and the application name.*			Sd, St
Precedence	For ADC, the precedence is only relevant for the enforcement, i.e. when multiple ADC rules overlap, only the enforcement, reporting of application starts and stops, monitoring, and charging actions of the ADC rule with the highest precedence shall be applied.	Optional	Yes	Sd, St
Application identifier (NOTE 2)	References the corresponding application detection filter for the detection of the service data flow. References the corresponding application, for which the rule applies.	Conditional (NOTE 5)	No	Sd, St
Service data flow filter list	A list of service data flow filters for the detection of the traffic.	Conditional (NOTE 5)	No	Sd, St
Mute for notification	Defines whether application's start or stop notification is to be muted.	Optional	No	Sd
Usage Monitoring Control	*This clause describes identities required for Usage Monitoring Control.*			Sd
Monitoring key	The PCRF uses the monitoring key to group applications that share a common allowed usage.	Optional	Yes	Sd
Indication of exclusion from session level monitoring	Indicates that the application shall be excluded from the TDF session usage monitoring.	Optional	Yes	Sd
Enforcement control	*This clause defines how the TDF shall apply enforcement actions for the detected application traffic.*			Sd
Gate status	The gate status indicates whether the detected application may pass (Gate is open) or shall be discarded (Gate is closed) at the TDF.	Optional	Yes	Sd
UL-maximum bit rate	The uplink maximum bit rate authorized for the application traffic	Optional	Yes	Sd
DL-maximum bit rate	The downlink maximum bit rate authorized for the application traffic	Optional	Yes	Sd
Redirect	Redirect state of detected application traffic (enabled/disabled)	Optional	Yes	Sd

Information name	Description	Category	PCRF permitted to modify for a dynamic ADC rule	Applicable reference point
Redirect Destination	Controlled Address to which detected application traffic should be redirected when redirect is enabled	Conditional (NOTE 1)	Yes	Sd
DSCP value	Downlink packets of detected application traffic shall be marked with this DSCP value.	Optional (NOTE 4)	Yes	Sd
Charging	*This clause defines identities and instructions for charging and accounting that is required for an access point where application usage charging is configured*			Sd
Charging key	The charging system (OCS or OFCS) uses the charging key to determine the tariff to apply for the application.	Optional	Yes	Sd
Service identifier	Identifies one or more applications to the charging system.	Optional	Yes	Sd
Sponsor Identifier	An identifier, provided from the AF which identifies the Sponsor, used for sponsored flows to correlate measurements from different users for accounting purposes.	Conditional (NOTE 7)	Yes	
Application Service Provider Identifier	An identifier, provided from the AF which identifies the Application Service Provider, used for sponsored flows to correlate measurements from different users for accounting purposes.	Conditional (NOTE 7)	Yes	Sd
Charging method	Indicates the required charging method for the ADC rule. Values: online, offline or neither.	Conditional (NOTE 3)	No	Sd
Measurement method	Indicates whether the application data volume, duration, combined volume/duration or event shall be measured. This is applicable for reporting, if the charging method is online or offline.	Optional	Yes	Sd
Service identifier level reporting	Indicates that separate usage reports shall be generated for this Service identifier. Values: mandated or not required.	Optional	Yes	Sd
Traffic Steering Enforcement Control	*This part describes identities required for Traffic Steering Enforcement Control.*			Sd, St

Information name	Description	Category	PCRF permitted to modify for a dynamic ADC rule	Applicable reference point
Traffic steering policy identifier(s)	Reference to a pre-configured traffic steering policy at the TDF/TSSF (NOTE 6).	Optional	Yes	Sd, St

NOTE 1: If Redirect is enabled.
NOTE 2: For every ADC rule this information is pre-configured in the TDF.
NOTE 3: Mandatory if there is no default charging method for the TDF session. It is possible to activate both online and offline charging for the same ADC Rule.
NOTE 4: See Annex U for details regarding how to apply policy and charging control for an application detected and marked by the TDF in the downlink direction (typically application with non-deducible service data flows).
NOTE 5: Either Application identifier or Service data flow filter list shall be included.
NOTE 6: The Traffic steering policy identifier can be different for uplink and downlink direction. If two Traffic steering policy identifiers are provided, then one is for uplink direction, while the other one is for downlink direction.
NOTE 7: Applicable to sponsored data connectivity.

The *ADC Rule identifier* shall be unique for an ADC rule within a TDF/TSSF session.

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.

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.

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.

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.

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.

NOTE 5: The configuration of the Application Identifier in the TDF 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.

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.

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.

The *Indication of exclusion from session level monitoring* indicates that the application shall be excluded from the TDF session usage monitoring.

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.

The *UL maximum-bitrate* indicates the authorized maximum bitrate for the uplink component of the detected application traffic.

The *DL maximum-bitrate* indicates the authorized maximum bitrate for the downlink component of the detected application traffic.

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.

The *Redirect* indicates whether the uplink part of the detected application traffic should be redirected to a controlled address.

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

The *DSCP value* indicates the value with which a TDF marks downlink application traffic identified by an ADC rule.

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.

NOTE 7: Assigning the same Charging key for several applications implies that the charging does not require the credit management to be handled separately.

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.

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.

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

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.

The *Measurement method* indicates what measurements apply for charging for ADC rule.

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.

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.

6.8.2 Application Detection and Control rule operations over Sd

Application Detection and Control rule operations apply to solicited reporting and consist of activation, modification and deactivation of ADC rules.

Activation: The PCRF provides the ADC Rule identifier to the TDF. The PCRF may provide data for usage monitoring and enforcement control for a dynamic ADC rule.

An active ADC rule means that:

- 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.

The PCRF may, at any time, modify an active, dynamic ADC rule.

The PCRF may, at any time, deactivate an active ADC rule. 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. An ADC rule may have either a single deferred activation time, or a single deferred deactivation time or both.

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. An inactive ADC rule, that has not been activated yet, is still considered to be installed, and may be removed by the PCRF.

The PCRF may modify a currently installed dynamic ADC rule, including setting, modifying or clearing its deferred activation and/or deactivation time.

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 a prior value will erase that attribute from the rule.

6.9 Policy decisions based on spending limits

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.

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.

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. The OCS may in addition provide one or more pending statuses for a requested policy counter together with the time they have to be applied. The PCRF shall immediately apply the current status of a policy counter. A pending status of a policy counter shall autonomously become the current status of a policy counter at the PCRF when the indicated corresponding time is reached. Subsequently provided information for pending statuses of a policy counter shall overwrite 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. If spending limit reporting for a policy counter is enabled, the OCS shall notify the PCRF of changes in the status of this policy counter (e.g. daily spending limit of $2 reached) and optionally pending statuses of this policy counter together with their activation time (e.g. due to a billing period that will expire at midnight). The 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.

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.

NOTE: The relationship between a policy counter identifier and the Charging Key could be 1-1. However it could also be assumed that services that share the same Charging Key can be associated with different policy counters i.e. although they are rated in the same way they are subject to different actions regarding (e.g. QoS and gating) and are therefore counted separately. Likewise services that share the same policy counters can be associated with different Charging Key.

6.11 Traffic Steering Control Information

6.11.1 General

The traffic steering control information comprises the information that is required to enable traffic steering for a detected application or service data flow. The traffic steering control information is transferred:

- From the PCRF to the PCEF within PCC rules over Gx reference point;
- From the PCRF to the TDF within ADC rules over Sd reference point;
- From the PCRF to the TSSF within ADC rules over St reference point.

NOTE 1: In this release of the specification, traffic steering control information does not contain the IP-CAN specific parameters such as e.g. RAT type, which may be needed by the (S)Gi-LAN service functions.

Table 6.11 lists the components of traffic steering control information, and their corresponding information names in PCC/ADC rule.

Table 6.11: Traffic steering control information

Component of traffic steering control information	Corresponding information name in ADC rule (NOTE 1)	Corresponding information name in PCC rule (NOTE 2)
Rule Name	ADC Rule Identifier	Rule identifier
Description of Traffic	Application Identifier or Service data flow filter list	Service Data Flow Template
Traffic steering policy identifier(s) (NOTE 3)	Traffic steering policy identifier(s) (NOTE 3)	Traffic steering policy identifier(s) (NOTE 3)
Precedence	Precedence	Precedence
NOTE 1: The information definition refers to Table 6.8. NOTE 2: The information definition refers to Table 6.3. NOTE 3: The Traffic steering policy identifier can be different for uplink and downlink direction. If two Traffic steering policy identifiers are provided, then one is for uplink direction, while the other one is for downlink direction.		

The Traffic Steering Policy Identifier is a reference to traffic steering policy locally configured at the PCEF/TDF/TSSF. The traffic steering policy identifies, explicitly or implicitly, a specific set of service functions and their order via which the traffic, identified by the description of traffic included in the traffic steering control information, needs to be steered in the (S)Gi-LAN.

For traffic steering control at the PCEF, the PCC Rule operations described in the clause 6.3.2 apply.

For traffic steering control at the TDF, the ADC Rule operations over Sd described in the clause 6.8.2 apply.

For traffic steering control at the TSSF, the Traffic Steering Control operations over St described in the clause 6.11.2 apply.

NOTE 2: In order for PCEF/TDF to measure the user plane traffic that is sent to a specific set of service functions, identified by a Traffic Steering Policy Identifier, a specific Charging Key or generic Charging Key and a specific Service Identifier is assigned to the PCC/ADC rule per each Traffic Steering Policy Identifier for which separate measurements are needed and the applicable measurement type as required. In case of Service Identifier usage, the PCC/ADC Rule also includes service identifier level reporting.

6.11.2 Traffic Steering Control Operations over St

Traffic steering control operations over St consists of provisioning, modification, and removal of traffic steering control information.

Provisioning: Provisioning of traffic steering control information to the TSSF includes the activation of traffic steering policy, so that the traffic detected by the service data flow filter list or the application identifier can be steered in the SGi-LAN according to the information associated with the traffic steering policy identifier. The PCRF provides the UE IP address and the associated APN when provisioning of traffic steering control information to the TSSF. The TSSF uses the APN to determine the PDN.

NOTE: The APN is provided from PCRF to the TSSF for the cases when the PCEF supports multiple APNs with overlapping IP addresses. In that case, the same UE IP address can be allocated to different UEs when they access different PDNs, each APN provides access to a different PDN.

When using ADC Rules, the following applies:

- For pre-defined ADC rules in TSSF, the PCRF provides the ADC Rule identifier(s) to the TSSF;
- For dynamic ADC Rules, the PCRF provides traffic steering control information within the ADC rules to the TSSF.

Modification: The PCRF may modify traffic steering control information to change the traffic steering policy identifier(s), the precedence, the service data flow filters or application identifier.

When using ADC Rules, the PCRF may modify a dynamic ADC rule.

Removal: The PCRF may, at any time, remove traffic steering control information.

When using ADC Rules, the PCRF may remove ADC Rule(s).

6.12 NBIFOM Routing rule

6.12.1 General

The NBIFOM routing rule comprises the information about the UE request to associate an access type to a service data flow filter. The NBIFOM routing rules are provided by the PCEF to the PCRF during IP-CAN session establishment or modification.

The PCEF derives NBIFOM routing rules based on the Routing Rules received from the UE (when UE-initiated NBIFOM mode applies) or based on requests from the UE to have the network create / modify / delete Routing Rules (when Network-initiated NBIFOM mode applies), as described in TS 23.161 [43].

Table 6.12 lists the information contained in an NBIFOM routing rule, including the information name, the description and whether the PCEF may modify this information in an updated version of the rule. The Category field indicates if a certain piece of information is mandatory or not.

Table 6.12: The NBIFOM routing rule information

Information name	Description	Category	PCEF permitted to modify in an update
Routing Rule identifier	Uniquely identifies the routing rule within an IP-CAN session.	Mandatory	No
Routing information	*This clause defines the method for detecting packets belonging to a flow and the route for the flow.*		
Routing Rule Priority	Determines the order, in which the routing filters are applied.	Mandatory	Yes
Routing Filter	A packet filter for the detection of IP flows.	Mandatory	Yes
Routing Access Information	The access type that the matching IP flows intend to use.	Mandatory	Yes

The *Routing Rule identifier* shall be unique for a NBIFOM routing rule within an IP-CAN session. It is set to the Routing Rule identifier assigned by the UE when UE-initiated NBIFOM mode applies as specified in TS 23.161 [43] or by the PCRF when Network-initiated NBIFOM mode applies.

The *Routing Rule Priority* defines in what order the NBIFOM routing rules are used by the PCRF to determine where to route a service data flow. The Routing Rule Priority is set according to the information provided by the UE as specified in TS 23.161 [43].

The *Routing Filter* comprises a single packet filter, containing information for matching IP flows. The format of the routing filter is the same as the service data flow filter described in clause 6.2.2.2. The Routing Filter is set according to the information provided by the UE as specified in TS 23.161 [43].

The *Routing Access Information* indicates the IP-CAN type that the IP flows matching the Routing Filter of this NBIFOM routing rule intend to use.

6.12.2 NBIFOM Routing rule operations

NBIFOM routing rule operations consist of creation, modification and removal of a NBIFOM routing rule.

At creation of a NBIFOM routing rule, the PCEF provides the NBIFOM routing rule information to the PCRF. The PCRF checks if there is a PCC Rule with a corresponding service data flow template installed in the PCEF. If it is so, the PCRF updates the Allowed Access Type in this PCC Rule according to the Routing Access Information. Otherwise a new PCC Rules is created with a service data flow filter equal to the Routing Filter, a precedence according to the Routing Rule Priority and the Allowed Access Type set to the Routing Access Information and then installed in the PCEF.

NOTE: If the Routing Filter is partially overlapping with a service data flow template of an installed PCC rule, it is up to the operator policy whether to reject the NBIFOM routing rule or whether to create a new PCC rule for this NBIFOM routing rule. In the latter case, this new PCC rule shall have the same parameters (except the rule name and the SDF template) and a higher precedence. The PCRF shall also ensure that relevant PCC rule modifications are applied for both PCC rules.

The PCRF shall store the relation between the Routing Rule identifier and the corresponding PCC rule. The PCRF may also reject a NBIFOM routing rule according to operator policy.

The modification of a NBIFOM routing rule to change the Routing Filter or the Routing Rule Priority triggers the PCRF to modify the service data flow filter or precedence in the corresponding installed PCC Rule accordingly.

The modification of a NBIFOM routing rule to change the Routing Access Information triggers the PCRF to change the Allowed Access Type in the corresponding installed PCC Rule accordingly.

The removal of a NBIFOM routing rule triggers the PCRF to remove the corresponding PCC Rule if the PCC rule creation was triggered by this NBIFOM routing rule. Otherwise, the PCRF removes only the Allowed Access Type in this PCC Rule.

7 PCC Procedures and flows

7.1 Introduction

The specification of the PCC procedures and flows is valid for the general scenario. Access specific information is included in Annex A, Annex D, Annex H and Annex P.

The description includes procedures for IP-CAN Session Establishment, Modification and Termination. The IP-CAN Session modification comprises IP-CAN bearer establishment, modification, termination, as well as unsolicited PCC decisions.

There are three distinct network scenarios for an IP-CAN Session:

Case 1: No Gateway Control Session is required, no Gateway Control Establishment occurs at all (e.g. 3GPP Access where GTP-based S5/S8 are employed, as described in TS 23.401 [17] and the IP-CAN specific Annexes, and non-3GPP accesses where GTP-based S2a or GTP-based S2b is employed, as described in TS 23.402 [18]).

Case 2: A Gateway Control Session is required. The BBERF establishes a Gateway Control Session prior to any IP-CAN session establishment. There are two sub-cases:

2a) The UE acquires a care of address (CoA) that is used for the S2c reference point. The same Gateway Control session applies for all IP-CAN sessions using that CoA.

2b) A Gateway Control Session is required, as described in TS 23.402 [18] and the IP-CAN specific Annexes, Gateway Control Session Establishment, as defined in clause 7.7.1.
Each IP-CAN session is handled in a separate Gateway Control Session.

The PCRF determines at Gx and Gxx session establishment what case applies initially as follows:

1. If the BBERF, at establishment of the Gateway Controls Session, provides an APN, then case 2b applies for the IP-CAN session.

2. If the BBERF, at establishment of the Gateway Controls Session, does not provide any APN, then case 2a applies for the UE. For this case, the PCRF expects tunnelling header information for each IP-CAN session to be provided by the applicable PCEF.

3. If there is no Gateway Control Session for the UE with the same IP-CAN type as indicated over Gx, case 1 applies.

In a handover procedure the applicable case may change for an IP-CAN session. The PCRF determines the new case in the same manner as described above. Details are defined in each such procedure.

The procedures cover non-roaming, roaming with home routed access and roaming with access to a visited PDN.

For the non-roaming case, the H-PCRF plays the full role of PCRF. The V-PCRF is not applicable in this case.

For the roaming case with home routed access, the H-PCRF interacts with the PCEF and, if the Gxx applies, the V-PCRF interacts with the BBERF.

For the roaming case with visited access (a.k.a. local breakout in TS 23.401 [17] and TS 23.402 [18]), the V-PCRF interacts with the PCEF and, if Gxx applies, the BBERF and, if Sd applies, the TDF.

NOTE: The roaming scenario (figure 5.1-4) with visited access is not applicable for traffic steering control.

Procedures defined in this clause cover the traffic cases where the TDF is located on Gi/SGi interface.

Procedures defined in clause 7 cover all the traffic cases where roaming partners both operate PCC. For limited PCC deployment scenarios, Annex K and Annex L specify the impacts to these procedures.

In the text describing the steps in each sequence diagram, the designation PCRF, without specifying V- or H-, refers to the PCRF in non-roaming case and refers to either the V-PCRF or the H-PCRF in the roaming cases. The interpretation of the text "PCRF" is thus dependent on the network scenario.

When NBIFOM (defined in TS 23.161 [43]) applies, the description of the flows in this clause 7 is complemented by the description of NBIFOM dedicated behaviours documented in clause 6.1.18.

7.2 IP-CAN Session Establishment

This clause describes the signalling flow for IP-CAN Session establishment as well as network prefix and/or IP address assignment to the UE. The AF is not involved.

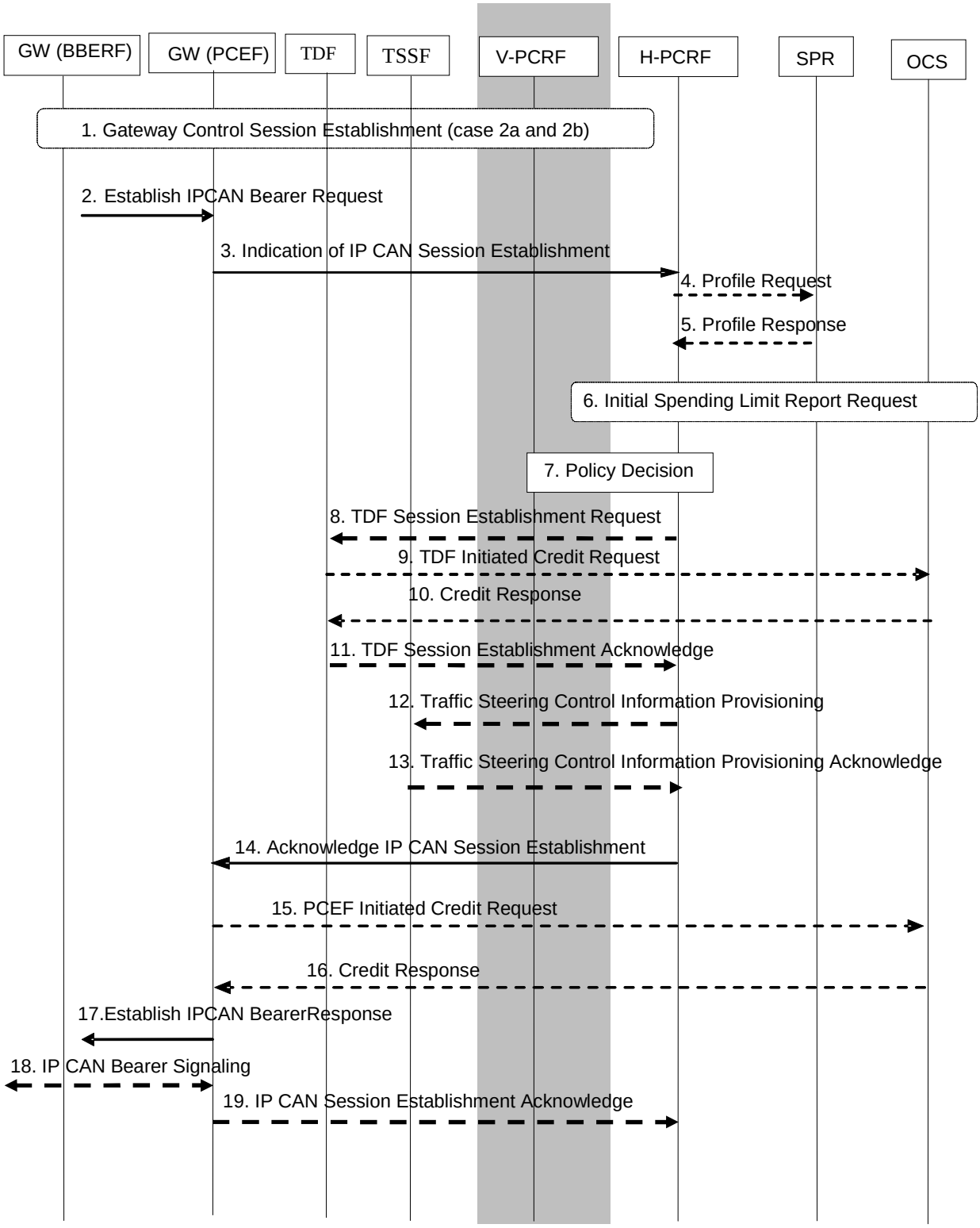

Figure 7.2-1: IP-CAN Session Establishment

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.

For the Local Breakout scenario (Figure 5.1-4) 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. 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.

In the non-roaming case (Figure 5.1-1) the V-PCRF is not involved.

1. The BBERF initiates a Gateway Control Session Establishment procedure as defined in clause 7.7.1 (applicable to case 2a during initial attach and case 2b, as defined in clause 7.1).

2. The GW (PCEF) receives a request for IP-CAN Bearer establishment. A PDN Connection Identifier may be included in the request. The GW (PCEF) accepts the request and assigns an IP address and (if requested) network prefix for the user.

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 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) where statically or dynamically allocated, and the charging identifier of the default bearer to identify different records belonging to the same PDN connection, indication on whether the charging identifier is the only one for the IP-CAN session. When the PCEF has received the IMEI(SV) in the request for IP-CAN Bearer establishment received at step 2, the PCEF shall transfer this information to the PCRF.

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.

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.

5. The PCRF stores the subscription related information containing the information about the allowed service(s) and PCC Rules information, and may 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.

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.

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/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) where 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.

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.

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.

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.

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.

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.

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.

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 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.

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 cannot be monitored at the PCEF, the PCEF shall request PCRF to arrange those to be reported by the BBERF via the PCRF.

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.

18. If network control applies the GW may initiate the establishment of additional IP--CAN bearers. See Annex A and Annex D for details.

19. If the PCRF in step 12 has 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.

7.3 IP-CAN Session Termination

7.3.1 UE initiated IP-CAN Session termination

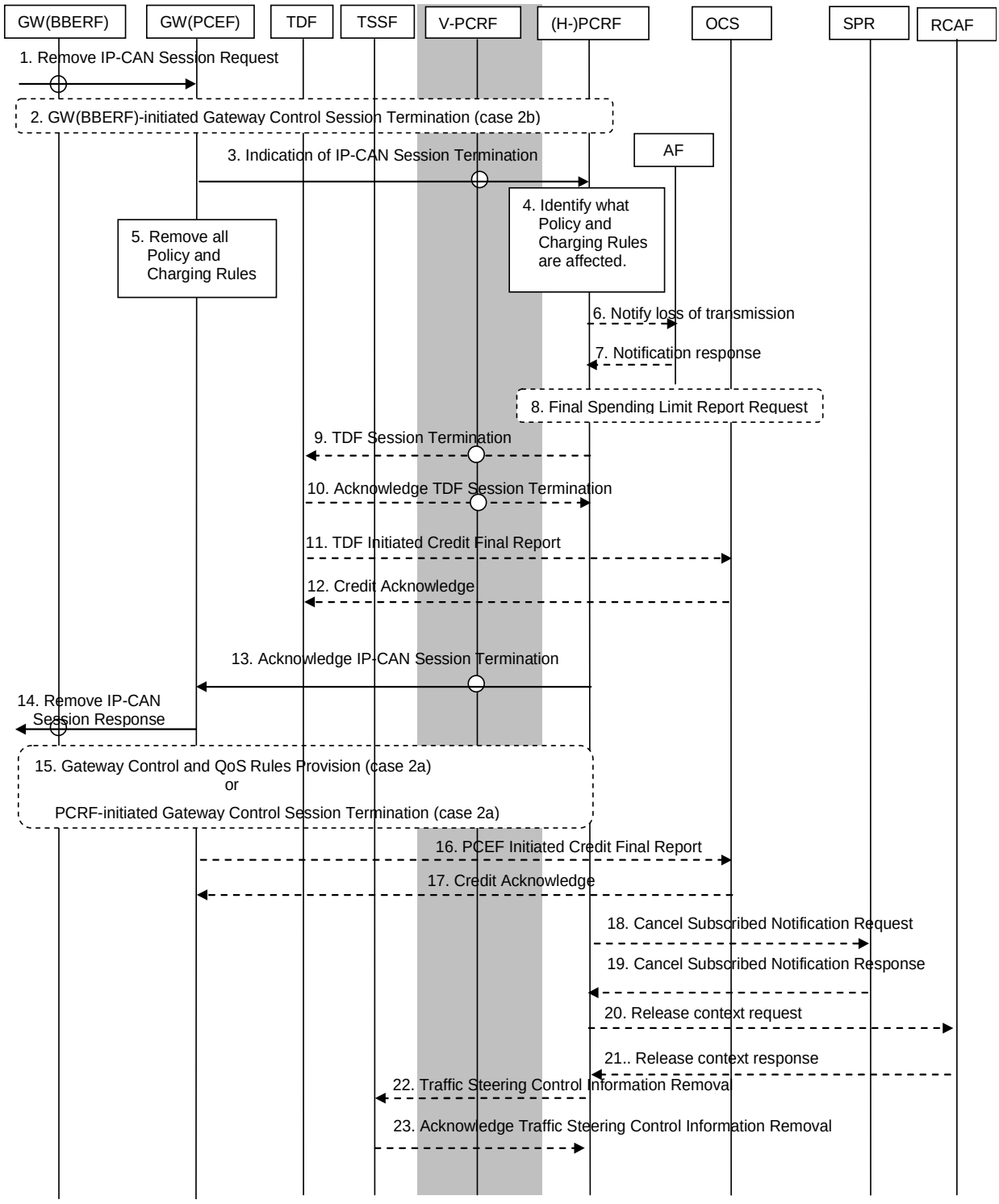

Figure 7.3.1: IP-CAN Session Termination

This procedure concerns both roaming and non-roaming scenarios. In the roaming case when home routed access is used (figure 5.1-3) or if case 2a applies (as defined in clause 7.1) for Local Breakout (figure 5.1-4), 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 5.1-4) 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 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.

In the non-roaming case (figure 5.1-1) the V-PCRF is not involved at all.

1. If case 2b applies, the GW (BBERF) receives a request to remove the IP-CAN session. In case 2a, the request goes transparently through the GW (BBERF). In all cases, the GW (PCEF) receives a request to remove the IP-CAN session.

2. If case 2b applies, the GW (BBERF)-initiated GW Control Session Termination procedure as defined in clause 7.7.2.1 is initiated.

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 11 in parallel with the indication of IP-CAN Session termination.

4. The PCRF finds the PCC Rules that require an AF to be notified and removes PCC Rules for the IP-CAN session.

5. The GW (PCEF) removes all PCC Rules associated with the IP-CAN session.

6. The PCRF notifies the AF that there are no transmission resources for the service if this is requested by the AF.

7. The AF acknowledges the notification of the loss of transmission resources.

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 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.

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.

11. If online charging is applicable for the TDF, the TDF issues the final reports and returns the remaining credit to the OCS.

12. The OCS acknowledges the credit report and terminates the online charging session with the TDF.

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.

NOTE 3: Step 13 may be initiated any time after step 7.

14. The GW (PCEF) continues the IP-CAN Session removal procedure.

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 e.g. in case the UE is detached and the CoA acquired by the UE is not used for any other IP-CAN session.

16. If online charging is applicable for the PCEF, the PCEF issues the final reports and returns the remaining credit to the OCS.

NOTE 4: Step 16 may be initiated any time after step 13.

17. The OCS acknowledges that credit report and terminates the online charging session with the PCEF.

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.

19. The SPR sends a response to the PCRF.

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.

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.

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.

23. The TSSF acknowledges the removal of the traffic steering control information.

7.3.2 GW (PCEF) initiated IP-CAN Session termination

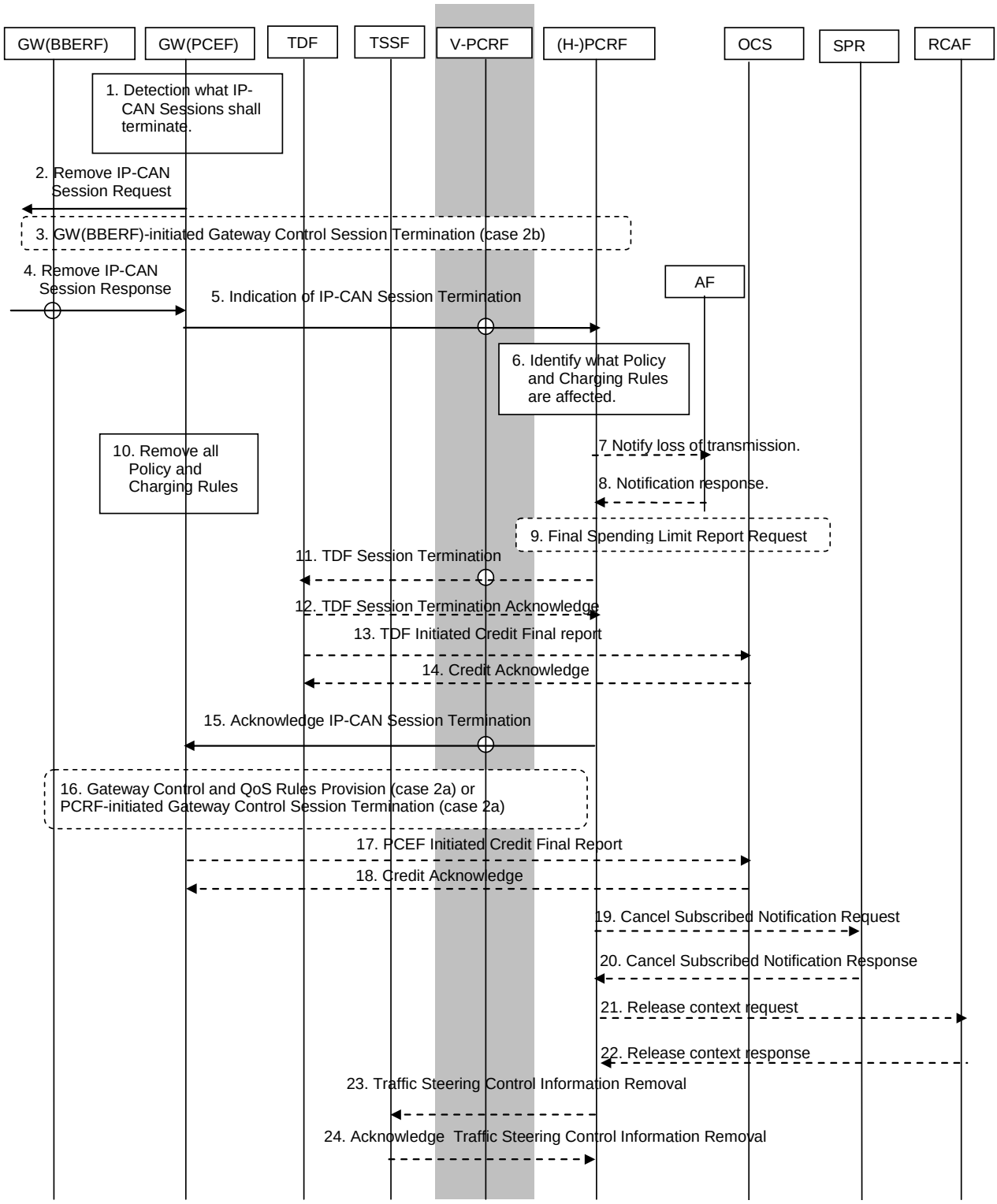

Figure 7.3.2: GW (PCEF) Initiated IP-CAN Session Termination

This procedure concerns both roaming and non-roaming scenarios. In the roaming case when home routed access is used (figure 5.1-3) or if case 2a applies (as defined in clause 7.1) for Local Breakout (figure 5.1-4), 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 5.1-4) 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.

In the non-roaming case (figure 5.1-1) the V-PCRF is not involved at all.

1. The GW (PCEF) detects that IP-CAN Session termination is required.
2. The GW (PCEF) sends a request to remove the IP-CAN session.
3. If case 2b applies, the GW (BBERF)-initiated GW Control Session Termination procedure as defined in clause 7.7.2.1 is initiated.
4. The GW (PCEF) receives the response for the IP-CAN session removal.
5. The GW (PCEF) indicates the IP-CAN Session termination and provides the relevant information to the PCRF.
6. The PCRF finds the PCC Rules that require an AF to be notified.
7. The PCRF notifies the AF that there are no transmission resources for the service if this is requested by the AF.
8. The AF acknowledges the notification on the loss of transmission resources.
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.
10. The GW (PCEF) removes all the PCC Rules associated with the IP-CAN session.
11. If there is an active Sd session between TDF and PCRF, 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.
13. If online charging is applicable for the TDF, the TDF issues the final reports and returns the remaining credit to the OCS.
14. The OCS acknowledges the credit report and terminates the online charging session with the TDF.
15. The PCRF removes the information related to the terminated IP-CAN Session (subscription information etc.), and acknowledges the IP-CAN Session termination.

NOTE 2: Step 15 may be initiated any time after step 6.

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.
17. If online charging is applicable for the PCEF, the PCEF issues final reports and returns the remaining credit to the OCS.

NOTE 3: Step 17 may be initiated any time after step 15.

18. The OCS acknowledges the credit report and terminates the online charging session.

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 4: Step 19 may be initiated any time after step 8.

20. The SPR sends a response to the PCRF.

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.

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.

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.

24. The TSSF acknowledges the removal of the traffic steering control information.

7.4 IP-CAN Session Modification

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

This clause describes the signalling flow for the IP-CAN Session modification initiated by the GW (PCEF). These modifications include IP-CAN bearer establishment and termination as well as modification if the triggering conditions given to the PCEF are fulfilled.

For the PCEF enhanced with ADC, the reason for such a modification may be that a start or stop of application traffic that matches with one of the activated PCC Rules is detected.

The AF may be involved. An example of the scenario is authorization of a session-based service for which an IP-CAN Session is also modified.

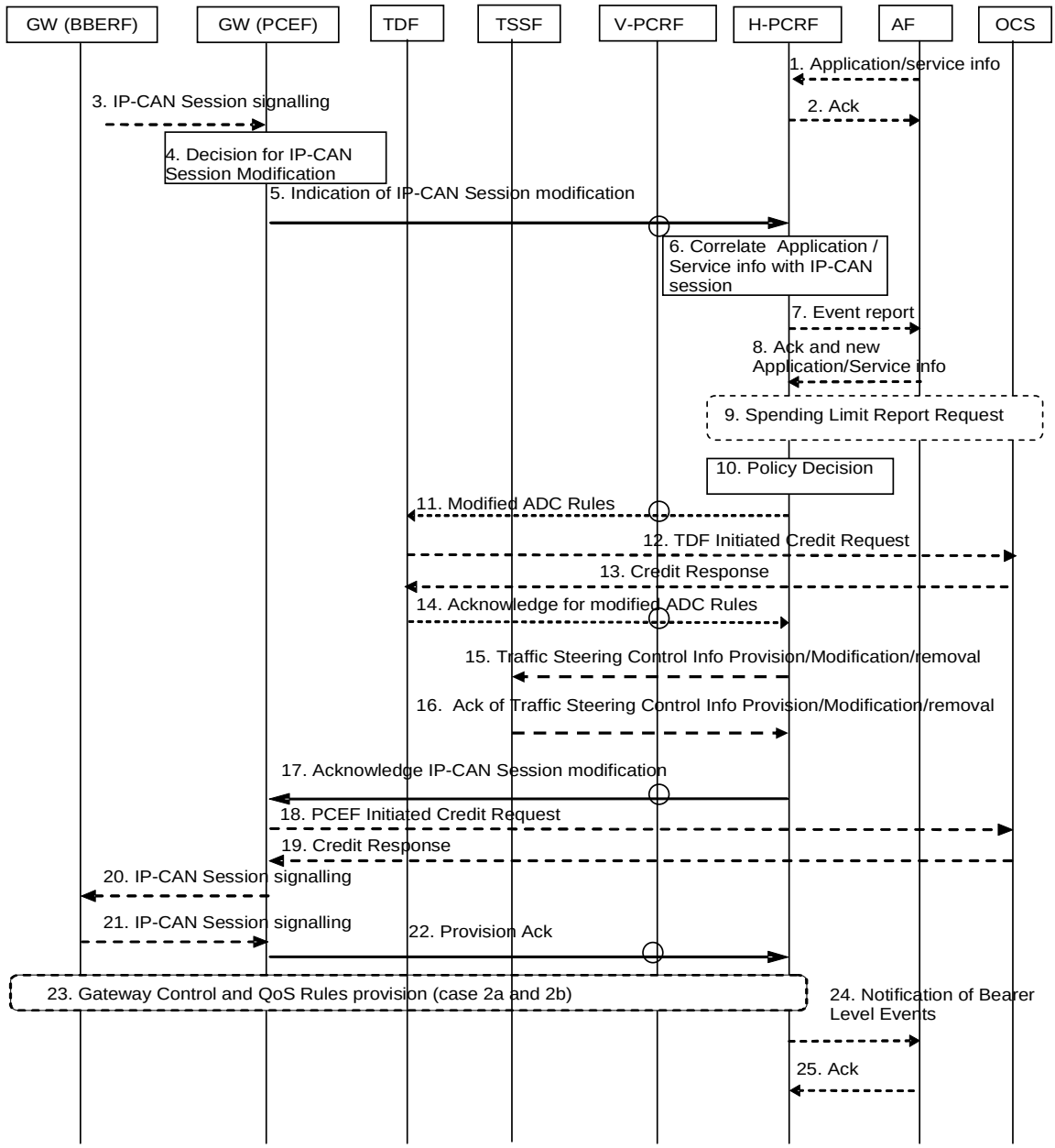

Figure 7.4: IP-CAN Session Modification; GW (PCEF) initiated

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.

1. 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.

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.

2. The PCRF stores the service information and responds with the Acknowledgement to the AF.

3. The GW (PCEF) may receive IP-CAN session signalling for IP-CAN Session modification. PDN Connection Identifier may be included in the IP-CAN session signalling.

4. The GW (PCEF) makes a decision to trigger IP-CAN Session modification either caused by the previous step or based on an internal decision or, e.g. if the GW (PCEF) enhanced with ADC, has detected the start/ stop of application traffic, requested by one of the activated PCC Rules.

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. If flow mobility applies, the GW (PCEF) may include updated IP flow mobility routing information for any IP flows; the GW (PCEF) also provides an indication if default route for the IP-CAN session is changed.

6. The PCRF correlates the request for PCC Rules with the IP-CAN session and service information available at the GW (PCEF).

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.

8. The AF acknowledges the event report and/or responds with the requested information.

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.

10. The PCRF makes the authorization and policy decision.

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.

    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.

12. If online charging is applicable for the TDF, the TDF may request credit for new charging keys from the OCS and/or may inform the OCS about re-authorization trigger if the event occurs and/or may issue final reports and return remaining credit for charging keys no longer active to the OCS.

13. If OCS was contacted by the TDF, the OCS provides the credit information to the TDF, and/or acknowledges the credit report.

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 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.

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.

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.

18. If online charging is applicable for the PCEF, the GW (PCEF) may request credit for new charging keys from the OCS and/or may inform the OCS about re-authorization trigger if the event occurs and/or may issue final reports and return remaining credit for charging keys no longer active to the OCS.

19. If OCS was contacted by the PCEF, the OCS provides the credit information to the GW (PCEF), and/or acknowledges the credit report.

20 The GW (PCEF) acknowledges or rejects any IP-CAN Session signalling received in step 3.

    An IP-CAN bearer establishment is accepted if at least one PCC rule is active for the IP-CAN bearer and in case of online charging credit was not denied by the OCS. Otherwise, the IP-CAN bearer establishment is rejected.

    An IP-CAN bearer termination is always acknowledged by the GW (PCEF).

    An IP-CAN bearer modification not upgrading the QoS and not providing traffic mapping information is always acknowledged by the GW (PCEF). An IP-CAN bearer modification is accepted if the provided traffic mapping information is accepted by the PCRF. Otherwise, the IP-CAN bearer modification is rejected.

    In case of a GW (PCEF) internal decision the GW (PCEF) initiates any additional IP-CAN Session signalling required for completion of the IP-CAN Session modification (applicable to case 1).

    In case the IP-CAN session modification is due to the BBF transitioning from a BBERF in the source access-network to the PCEF, the PCEF initiates IP-CAN bearer signalling to activate bearers in the target access network (applicable to case 1).

21. The GW (PCEF) receives the response for the IP-CAN Session signalling request (applicable to case 1).

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 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 to cases 2a and 2b, as defined in clause 7.1).

    If there are multiple BBERFs associated with the IP-CAN session, this step is performed with all the affected BBERFs.

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.

25. The AF acknowledges the notification from the PCRF.

7.4.2 IP-CAN Session Modification; PCRF initiated

This clause describes the signalling flow for the IP-CAN Session modification initiated by the PCRF. The AF or TDF or the OCS or the TSSF may be involved. An example of PCRF inputs that may trigger the procedure include:

- Initiation and authorization of a session-based service for which an IP-CAN Session is modified.
- A change in the status of a policy counter.

IP-CAN Session handling and handling of PCC rules for non-session based services, and also general handling of PCC rules that are not subject to AF-interaction or TDF-interaction is also applicable here.

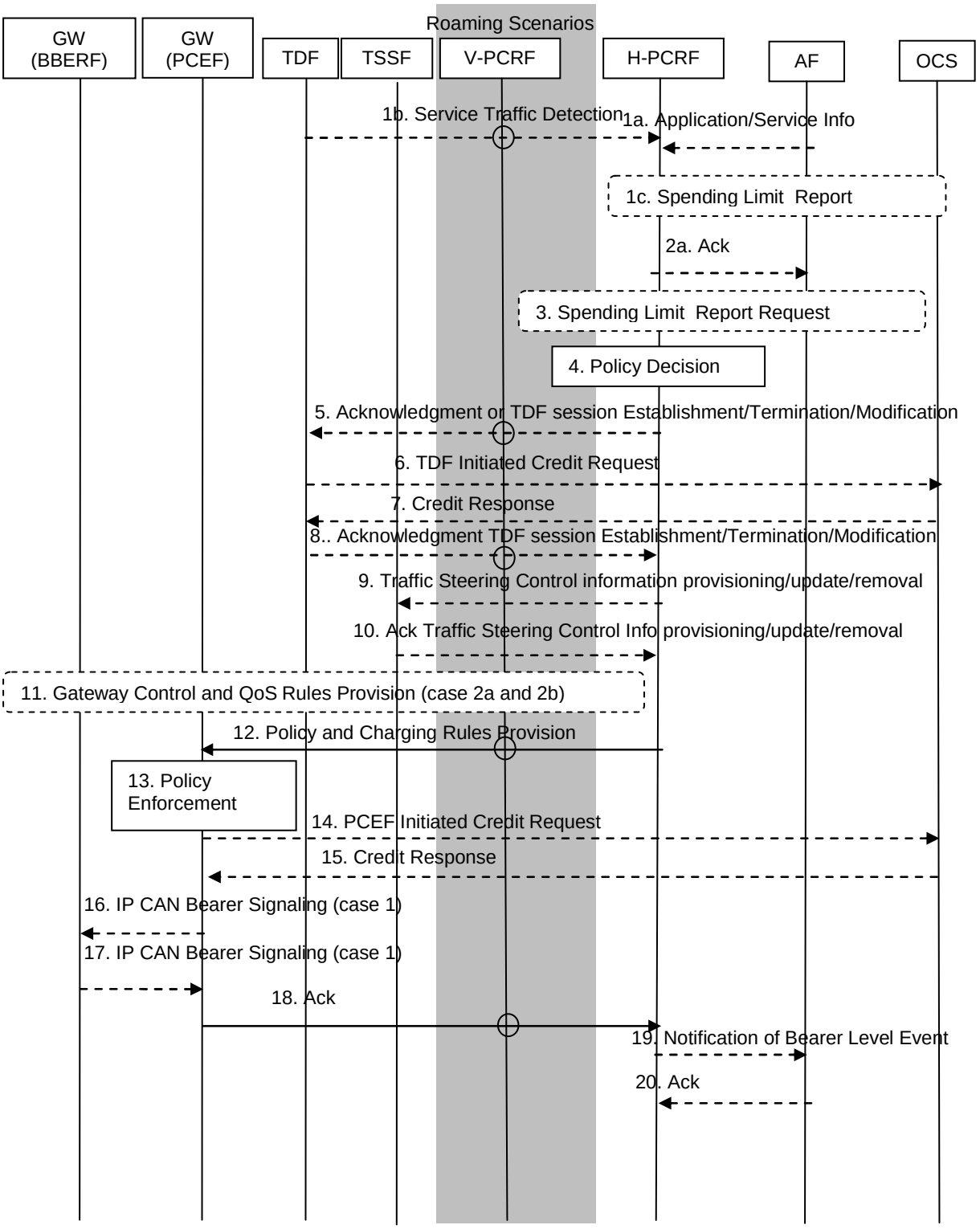

Figure 7.5: IP-CAN Session Modification; PCRF initiated

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 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 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 5.1-4) 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.

1b. Alternatively, optionally, for TDF, e.g. the TDF detects the start/stop of an application traffic that matches with one of the active ADC Rules.

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.

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.

1c. Alternatively, optionally, the OCS provides a Spending Limit Report to the PCRF as described in clause 7.9.4.

1d. Alternatively, optionally, the RCAF provides a Congestion Report to the PCRF as described in clause 7.10.1.

NOTE 3: This step is not shown on the diagram.

2a. The PCRF stores the service information if available and responds with the Acknowledgement to the AF. 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.

NOTE 5: This procedure could also be triggered by the Gateway Control and QoS Rules Request procedure as described in clause 7.7.3.

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.

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.

5. The PCRF may store the application information if provided and responds with an Acknowledgement to the TDF (for unsolicited application reporting) or a Sd 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 Sd session towards the PCRF. If there is no active Sd session yet between the TDF and the PCRF, the PCRF requests the TDF to establish the Sd 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. 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.

6. If online charging is applicable for the TDF, the TDF may request credit for new charging keys from the OCS and/or may inform the OCS about re-authorization trigger if the event occurs and/or may issue final reports and return remaining credit for charging keys no longer active to the OCS.

7. If OCS was contacted by the TDF, the OCS provides the credit information to the TDF, and/or acknowledges the credit report.

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.

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.

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.

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 to 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.

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.

12. The PCRF sends the Policy and Charging Rules Provision (PCC Rules, Event Trigger, Event Report) to the PCEF. If traffic steering control over Gx applies, the PCC Rules may contain traffic steering control information. 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.

13. The PCEF enforces the decision.

14. If online charging is applicable for the PCEF, the PCEF may request credit for new charging keys from the OCS and/or may inform the OCS about re-authorization trigger if the event occurs and/or may return the remaining credit for charging keys no longer active to the OCS.

15. If OCS was contacted by the PCEF, the OCS provides the credit information to the PCEF, and/or acknowledges the credit report.

16. The GW (PCEF) may send an IP-CAN Bearer establishment, modification or termination request (applicable to case 1, as defined in clause 7.1).

    An IP-CAN bearer modification is sent by the GW (PCEF) if the QoS of the IP-CAN bearer exceeds the authorized QoS provided by the PCRF in step 4.

    An IP-CAN bearer termination request is sent by the GW (PCEF) if all PCC rules for an IP-CAN bearer have been removed.

17. The GW (PCEF) receives the response for the IP-CAN Bearer modification or termination request (applicable to case 1).

18. The PCEF sends Acknowledge Policy and Charging Rules Provisioning (accept or reject of the PCC rule operation(s)) to the PCRF.

19. If the AF requested it, the PCRF notifies the AF related bearer level events (e.g. transmission resources are established/released/lost).

20. The AF acknowledges the notification from the PCRF.

7.4.3 Void

7.5 Update of the subscription information in the PCRF

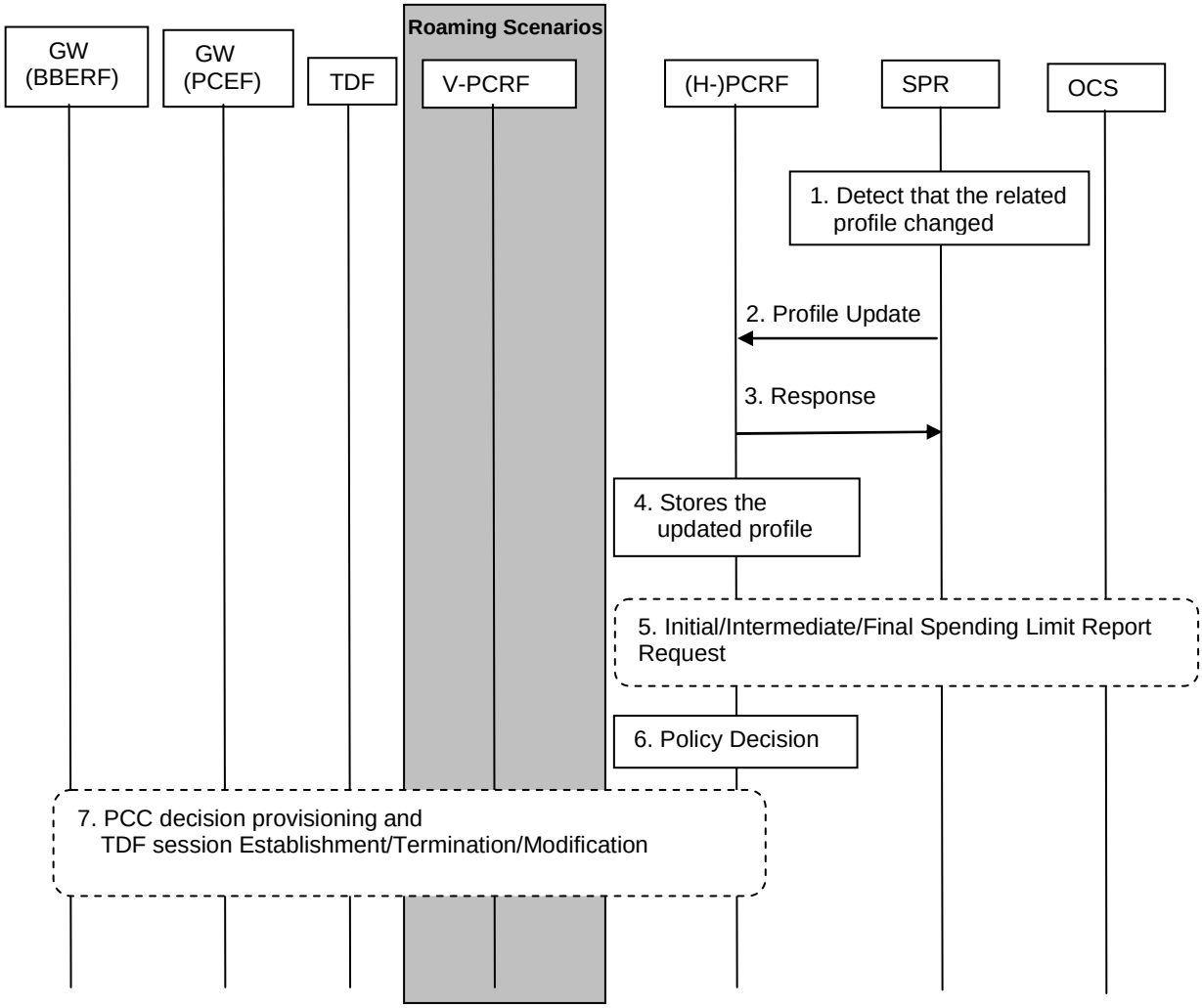

Figure-7.6: Procedure for update of the subscription information in the PCRF

1. The SPR detects that the related subscription profile of an IP-CAN session has been changed.
2. If requested by the PCRF, the SPR notifies the PCRF on the changed profile.
3. The PCRF responds to the SPR.
4. The PCRF stores the updated profile.

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 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.
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.

7.6 PCRF Discovery and Selection

7.6.1 General principles

This clause describes the underlying principles for PCRF selection and discovery:

- A single logical PCRF entity may be deployed by means of multiple and separately addressable PCRFs.
- 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).
- 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.).
- 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.

  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.
- A standardized procedure for contacting the PCRF is preferred to ensure interoperability between PCRFs from different vendors. The procedure may be specific for each reference point. The procedure shall enable the PCRF(s) to coordinate Gx, Rx and, when applicable, Gxa/Gxc, S9, Sd and Np interactions.
- It shall allow that entities contacting the PCRF may be able to provide different sets of information about the UE and PDN connections. For example:
  - The AF has information about UE IP address and PDN but may not have user identity information.
  - The PDN GW has information about user identity (UE NAI), the APN and the UE IP address(es) for a certain PDN connection.
  - For case 2b as defined in clause 7.1, the S-GW and trusted non-3GPP access has information about the user identity (UE NAI) and, the APN(s) but may not know the UE IP address(es).
  - For case 2a as defined in clause 7.1, the trusted non-3GPP access has information about the user identity (UE NAI) and the local IP address (CoA) but may not know the APN or UE IP address(es) (HoA).
  - The TDF (when the unsolicited application reporting applies) has the information about UE IP address, but may not have the UE identity.
  - The RCAF has the information about the user identity (IMSI) and the APN.
- The DRA has information about the user identity (UE NAI), the APN, the UE IP address(es) and the selected PCRF address for a certain IP-CAN Session.

  When the DRA first receives a request for a certain IP-CAN Session (e.g. from the PDN GW), the DRA selects a suitable PCRF for the IP-CAN Session and stores the PCRF address. Subsequently, the DRA can retrieve the selected PCRF address according to the information carried by the incoming requests from other entities (e.g. the AF or the BBERF).

  When the IP-CAN Session terminates, the DRA shall remove the information about the IP-CAN Session. In case of the PCRF realm change, the information about the IP-CAN session stored in the old DRA shall be removed.
- All PCRFs in a PLMN belong to one or more Diameter realms. Routing of PCC messages for a UE towards the right Diameter realm in a PLMN is based on standard Diameter routing, as specified in RFC 3588, i.e. based on UE-NAI domain part. A Diameter realm shall provide the ability of routing PCC messages for the same UE and PDN connection to the same PCRF based on the available information supplied by the entities contacting the PCRF.

- A PLMN may be separated into multiple Diameter realms based on the PDN ID information or IP address range. In this case, the relevant information (PDN ID, IP address, etc) shall be used to assist routing PCC message to the appropriate Diameter realm.

- 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).

- Standard IETF RFC 3588 mechanisms and components, e.g. Diameter agents, should be applied to deploy a network where the PCRF implementation specifics are invisible for Diameter clients. The use of Diameter agents, including Diameter redirect agents, shall be permitted, but the use of agents in a certain deployment shall be optional.

NOTE: For the use of private UE IPv4 address TS 29.213 [22] provides guidance.

7.6.2 Solution Principles

In order to ensure that all Diameter sessions for Gx, S9, Gxa/Gxc, Rx, Sd (when the unsolicited application reporting applies) and Np for a certain IP-CAN session reach the same PCRF when multiple and separately addressable PCRFs have been deployed in a Diameter realm, an optional logical "Diameter Routing Agent (DRA)" function is enabled. This resolution mechanism is not required in networks that utilise a single PCRF per Diameter realm. The DRA has the following roles:

- When deployed, DRA needs to be contacted at first interaction point for a given GW and IP-CAN session.

NOTE: How subsequent interactions work is described in TS 29.213 [22].

- When deployed, the DRA is on the Diameter routing path when initiating a session with a PCRF over Gx, Rx, Gxa/Gxc, S9 and Sd.

- The DRA is involved at IP-CAN session establishment by the PDN GW.

- The DRA selects the PCRF at initial attach (IP-CAN session or Gateway Control session establishment).

- The DRA is involved at Gateway Control session establishment by the S-GW and trusted non-3GPP access.

- The DRA selects the PCRF at unsolicited service reporting over Sd.

- After IP-CAN session or Gateway Control Session establishment, the DRA ensures that the same PCRF is contacted for Rx, Gxa/Gxc, Gx, S9, Sd and Np.

- The DRA keeps status of assigned PCRF for a certain UE and IP-CAN session.

- It is assumed that there is a single logical DRA serving a Diameter realm.

- In roaming scenarios, there is only a single VPCRF for all the PCC sessions (IP-CAN session, GW control sessions, AF session, etc.) belonging to a single PDN connection of the UE. The VPCRF shall be selected by a DRA in the visited PLMN.

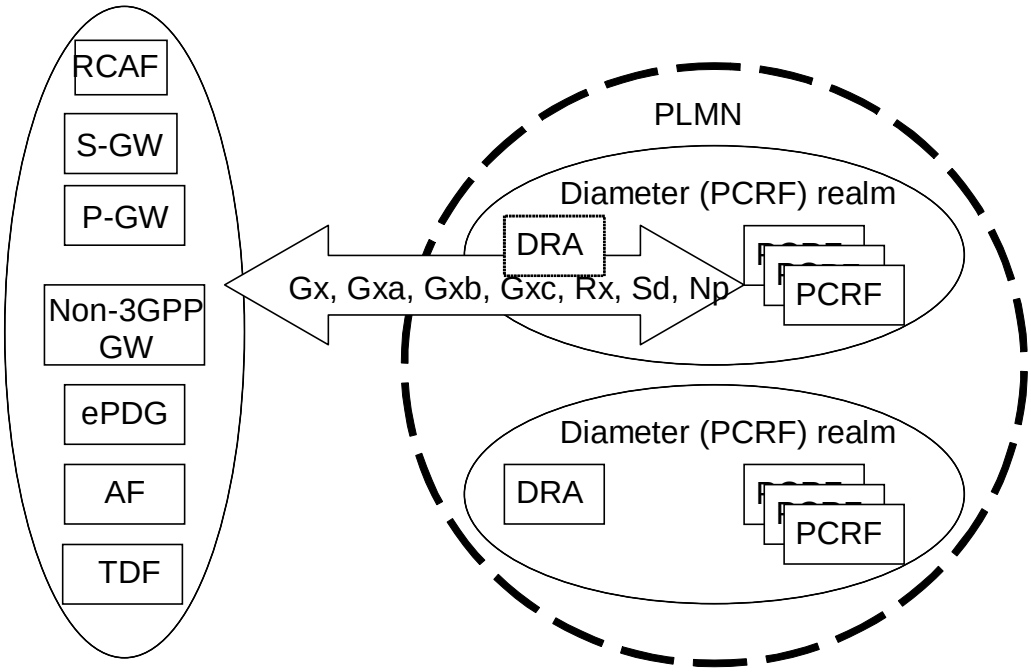

Figure 7.6-1: PCRF selection and discovery using DRA

The DRA functionality should be transparent to the Diameter applications used on the Gx, Gxa/Gxc, S9, Rx, Sd or Np reference points.

In roaming scenario, home routed or local breakout, if the DRA is deployed, the vPCRF is selected by the DRA located in the visited PLMN, and the hPCRF is selected by the DRA located in the home PLMN.

The parameters available for the DRA to be able to determine the already allocated PCRF depend on the reference point over which the DRA is contacted, as described in clause 7.6.1.

7.7 Gateway Control Session Procedures

7.7.1 Gateway Control Session Establishment

7.7.1.0 General

There are two cases considered for Gateway Control Session Establishment:

1. The PCEF establishes the IP-CAN Session during the Gateway Control session establishment. This happens when the UE attaches to the EPC for the first time and when the UE establishes a new PDN Connection.

2. There exists an established IP-CAN Session corresponding to the Gateway Control Session being established. This happens when the BBERF changes, i.e. during BBERF relocation and handovers from and to GTP based EPC.

7.7.1.1 Gateway Control Session Establishment during Attach

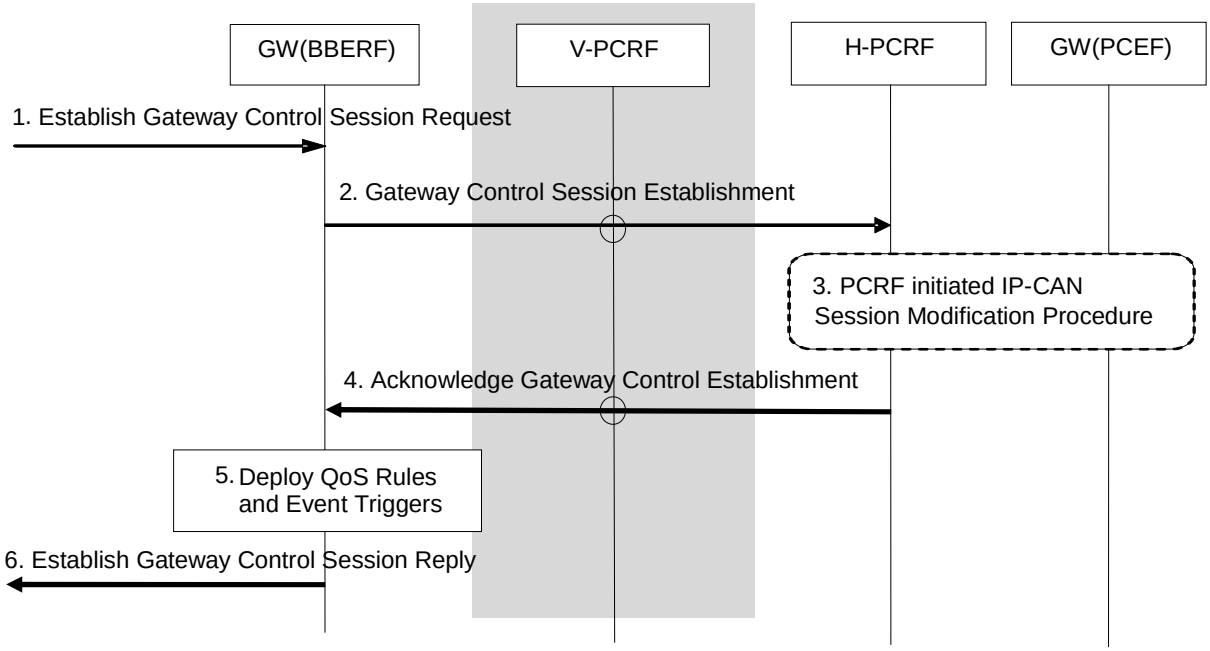

Figure 7.7.1.1-1: Gateway Control Session Establishment during Attach

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 between the BBERF in the VPLMN and the H-PCRF over S9 based on PDN-Id and roaming agreements.

In the non-roaming case (Figure 5.1-1) the V-PCRF is not involved.

1. The GW (BBERF) receives an indication that it must establish a Gateway Control Session.

2. The GW (BBERF) sends the PCRF a Gateway Control Session Establishment. The BBERF includes the following information: IP-CAN Type, UE Identity, PDN Identifier (if known), IP address(es) (if known), an indication that leg linking shall be deferred (applicable for case 2b, as defined in clause 7.1), if available, the PDN Connection Identifier and if available, the IP-CAN bearer establishment modes supported and the indication of BBERF support for the extended TFT filter format. The IP-CAN Type identifies the type of access used by the UE. The UE's identity and PDN Identifier requested are used to identify the subscriber and in PCRF selection to locate the PCRF function with the corresponding IP-CAN session established by the PDN GW. The BBERF may also include the Default Bearer QoS and APN-AMBR (applicable for case 2b, as defined in clause 7.1). An indication that leg linking shall be deferred is included to inform the PCRF that linking the Gateway Control Session to a Gx session shall occur when a matching Gx message is received as described clause 6.2.1.0. Further information is supplied on an access specific basis, as described in the IP-CAN specific Annexes.

NOTE: The BBERF support is a prerequisite for the PCRF enabling the possibility for usage of the extended TFT filter format in the IP-CAN session(s).

3. For GERAN/UTRAN accesses, if the PCRF is required to interact with the GW (PCEF), the PCRF waits until it gets informed about the establishment of the corresponding IP-CAN session (step 7 of the IP-CAN session establishment procedure) and performs a PCRF initiated IP-CAN session modification procedure with the GW (PCEF).

4. The PCRF sends an Acknowledge Gateway Control Session Establishment to the GW (BBERF). The PCRF may include the following information: the chosen IP-CAN bearer establishment mode, QoS Rules and Event Triggers. In case 2a a charging ID may be provided together with QoS rules. The QoS policy rules are employed by the GW (BBERF) to perform Bearer Binding. The Event Triggers indicate events that require the GW (BBERF) to report to the PCRF.

5. The QoS Rules and Event Triggers received by the GW (BBERF) are deployed. This will result in bearer binding being performed, according to the rules. This step may trigger IP-CAN bearer establishment procedures. The details of bearer establishment are IP-CAN specific.

6. An indication of Gateway Control Session Established is sent to the entity that triggered the initiation of the session.

7.7.1.2 Gateway Control Session Establishment during BBERF Relocation

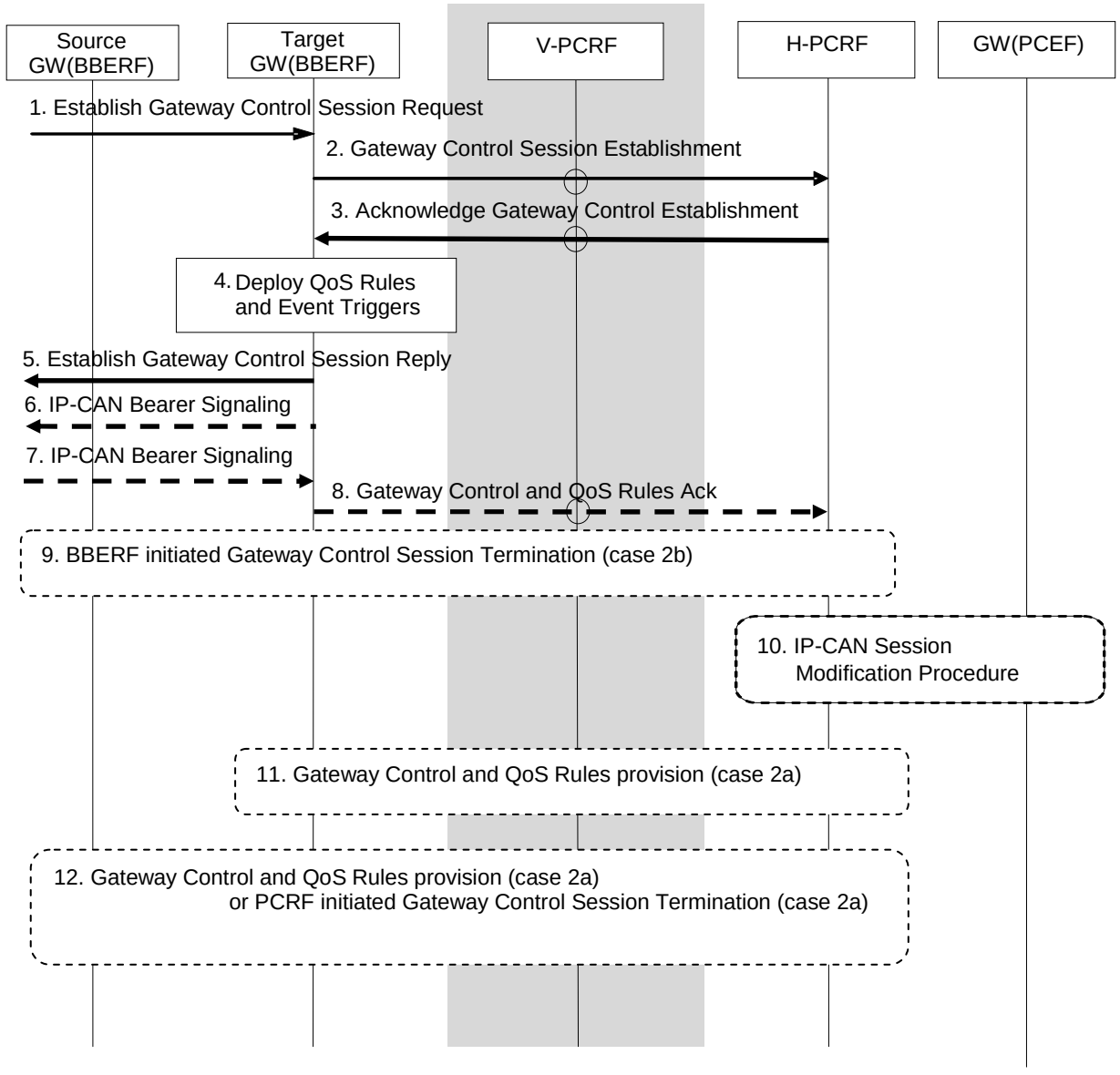

Figure 7.7.1.2-1: Gateway Control Session Establishment during BBERF Relocation

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 between the BBERF in the VPLMN and the H-PCRF over S9 based on PDN-Id and roaming agreements.

In the non-roaming case (Figure 5.1-1) the V-PCRF is not involved.

1. The target GW (BBERF) receives an indication that it must establish a Gateway Control Session.

2. The target GW (BBERF) sends the PCRF a Gateway Control Session Establishment. The BBERF includes the following information: IP-CAN Type, UE Identity, PDN Identifier (if known), IP address(es) (if known), PDN Connection Identifier if available and, if available, the IP-CAN bearer establishment modes supported. The

IP-CAN Type identifies the type of access used by the UE. The UE's identity and PDN Identifier requested are used to identify the subscriber and in PCRF selection to locate the PCRF function with the corresponding IP-CAN session established by the PDN GW. The BBERF may also include the Default Bearer QoS and APN-AMBR (applicable for case 2b, as defined in clause 7.1). If the handover state is unknown to the GW (BBERF), as described in TS 23.402 [18], the GW (BBERF) includes an indication to inform the PCRF that linking the Gateway Control Session to a Gx session shall be deferred as described clause 6.2.1.0 (applicable for case 2b, as defined in clause 7.1). Further information is supplied on an access specific basis, as described in the IP-CAN specific Annexes.

3. If case 2b of clause 7.1 applies and the PCRF correlates the Gateway Control Session with an existing IP-CAN session, it sends an Acknowledge Gateway Control Session Establishment to the target GW (BBERF). The PCRF may include the following information: QoS Rules and Event Triggers. The QoS policy rules are employed by the GW (BBERF) to perform Bearer Binding. The Event Triggers indicate events that require the GW (BBERF) to report to the PCRF. If the BBERF supports NW/UE bearer establishment mode, the PCRF provides to the new BBERF QoS rules corresponding to existing SDFs. For a change of IP-CAN type, the QoS parameters of some of the QoS rules may be changed or some QoS rules may not be provided to the new BBERF, e.g. depending of the capability of the target RAT.

   If case 2a of clause 7.1 applies, the PCRF sends an Acknowledge Gateway Control Session Establishment to the target GW (BBERF). The PCRF includes packet filters and QoS information for the CoA in order to establish the initial bearer, e.g. for the DSMIPv6 signalling. The PCRF may also include Event Triggers.

NOTE: The packet filters and QoS information provided at this step conceptually are not QoS rules as they are not associated with any IP-CAN session. However, it is a stage 3 issue if the packet filters and QoS information are communicated to the BBERF with the same information elements by which QoS rules are communicated.

4. The QoS Rules and Event Triggers received by the target GW (BBERF) are deployed. This will result in bearer binding being performed, according to the rules. This step may trigger IP-CAN bearer establishment procedures. The details of bearer establishment are IP-CAN specific.

5. An indication of Gateway Control Session Established is sent to the entity that triggered the initiation of the session.

6. The target GW (BBERF) initiates the IP-CAN Bearer signalling if required for the QoS Rules and Event Triggers deployed in step 4.

7. The target GW (BBERF) receives the response for the IP-CAN Bearer signalling.

8. The target GW (BBERF) sends the result of the QoS rule activation to the PCRF, indicating whether the resources requested have been successfully allocated.

9. If case 2b applies the source GW (BBERF) initiates the Gateway Control Session Termination procedure as defined in clause 7.7.2.1, if appropriate.

10. If the PCC rules previously provided to the GW (PCEF) need to be removed due to the result of the QoS rule activation as received in step 8, the PCRF updates the GW (PCEF). The PCRF first waits for the PCEF initiated IP-CAN session modification procedure to provide the updates. If the IP-CAN session modification procedure already occurred, the PCRF performs an IP-CAN session modification procedure with the GW (PCEF).

11. If case 2a applies the PCRF initiates a Gateway Control and QoS Rules Provision procedure towards the target GW (BBERF) as defined in clause 7.7.4, if appropriate, in order to provide any QoS Rules based on the IP-CAN session modification of step 10. In case 2a a charging ID may be provided together with QoS rules.

12. If case 2a applies the PCRF initiates a Gateway Control and QoS Rules Provision procedure towards the source GW (BBERF) as defined in clause 7.7.4, if appropriate, in order to remove any QoS Rules affected by the GW (BBERF) re-location. If there is no other IP-CAN session established at the source GW (BBERF), the PCRF instead initiates the Gateway Control Session Termination procedure as defined in clause 7.7.2.2.

7.7.2 Gateway Control Session Termination

7.7.2.1 GW (BBERF)-Initiated Gateway Control Session Termination

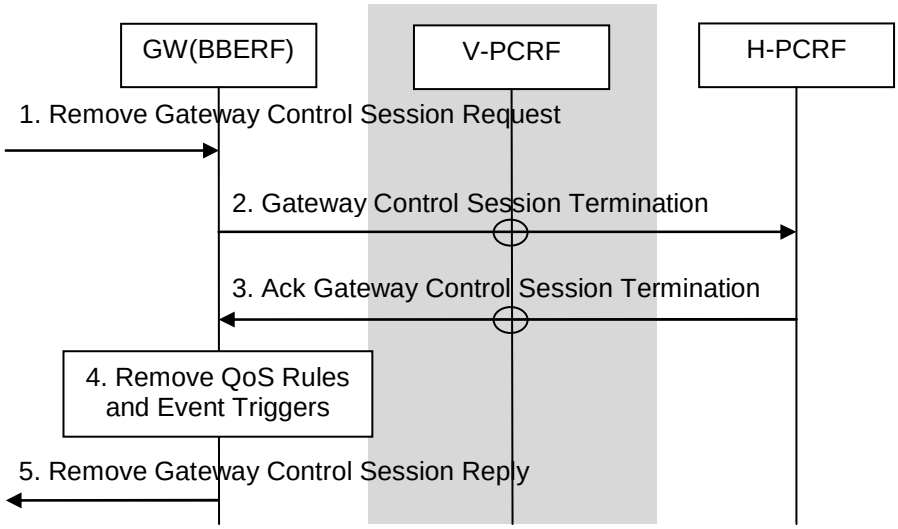

Figure 7.7.2-1: BBERF-Initiated Gateway Control Session Termination

1. The GW (BBERF) is requested to terminate its Gateway Control Session.
2. The GW (BBERF) initiates a Gateway Control Session Termination towards the H-PCRF. If the GW (BBERF) is deployed in a visited network, this procedure is initiated by the GW (BBERF) to the V-PCRF. The V-PCRF forwards the information to the H-PCRF.
3. The H-PCRF replies to the GW (BBERF) with an Ack Gateway Control Session Termination. If the GW (BBERF) is deployed in a visited network, this information is sent by the H-PCRF to the V-PCRF. The V-PCRF forwards the information to the GW (BBERF).
4. The GW (BBERF) removes the QoS rules and Event triggers associated with the Gateway Control Session. This means the GW (BBERF) ceases its bearer binding and other Gateway Control functions associated with the QoS rules and Event Triggers.
5. The GW (BBERF) has completed terminating the session and can continue with the activity that prompted this procedure.

7.7.2.2 PCRF-Initiated Gateway Control Session Termination

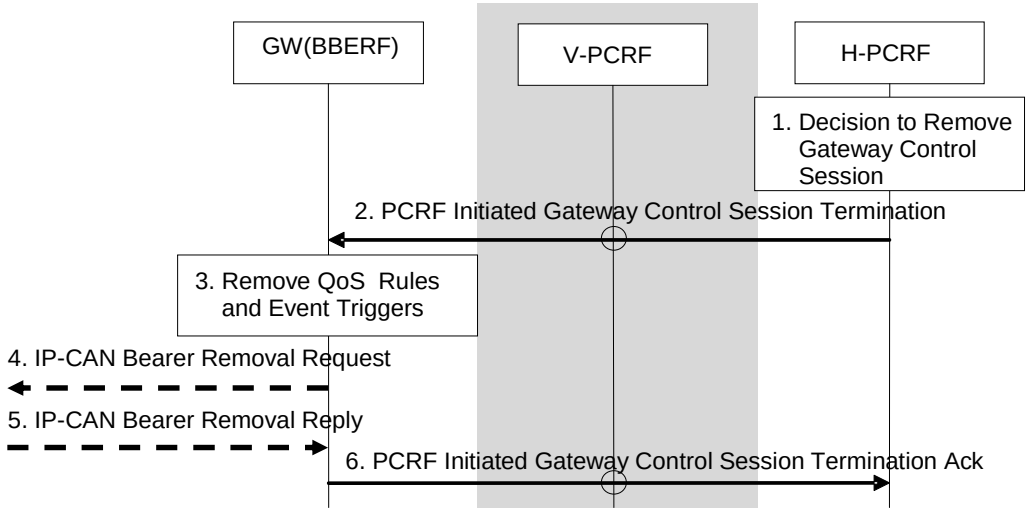

Figure 7.7.2-2: PCRF-Initiated Gateway Control Session Termination

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 Termination between the BBERF in the VPLMN and the H-PCRF over S9 based on PDN-Id and roaming agreements.

In the non-roaming case (Figure 5.1-1) the V-PCRF is not involved.

1. The PCRF is requested to terminate its Gateway Control Session.
2. The PCRF sends a PCRF-Initiated Gateway Control Session Termination to the GW (BBERF).
3. The GW (BBERF) removes the QoS rules and Event triggers associated with the Gateway Control Session. This means the GW (BBERF) ceases its bearer binding and other Gateway Control functions associated with the QoS rules and Event Triggers.
4. If the bearer(s) corresponding to the removed QoS rules are still established, the GW (BBERF) initiates an IP-CAN specific bearer removal procedure.
5. The GW (BBERF) receives the response for the IP-CAN specific bearer removal procedure.
6. The GW (BBERF) replies to the PCRF with an PCRF-Initiated Gateway Control Session Termination acknowledgement.

7.7.3 Gateway Control and QoS Rules Request

7.7.3.1 General

There are two cases considered for a Gateway Control and QoS Rules Request depending on the parameters the GW (BBERF) receives:

Case A: In case the GW (BBERF) action does not depend on the subsequent IP-CAN session modification, the GW (BBERF) can acknowledge the request after interacting with the PCRF.

NOTE 1: If QoS rules have to be updated due to the event reporting, the PCRF shall use the Gateway Control and QoS Rules Provision procedure.

Case B: The GW (BBERF) is requested to obtain QoS rules for a Gateway Control Session or to deliver IP-CAN-specific parameters or both.

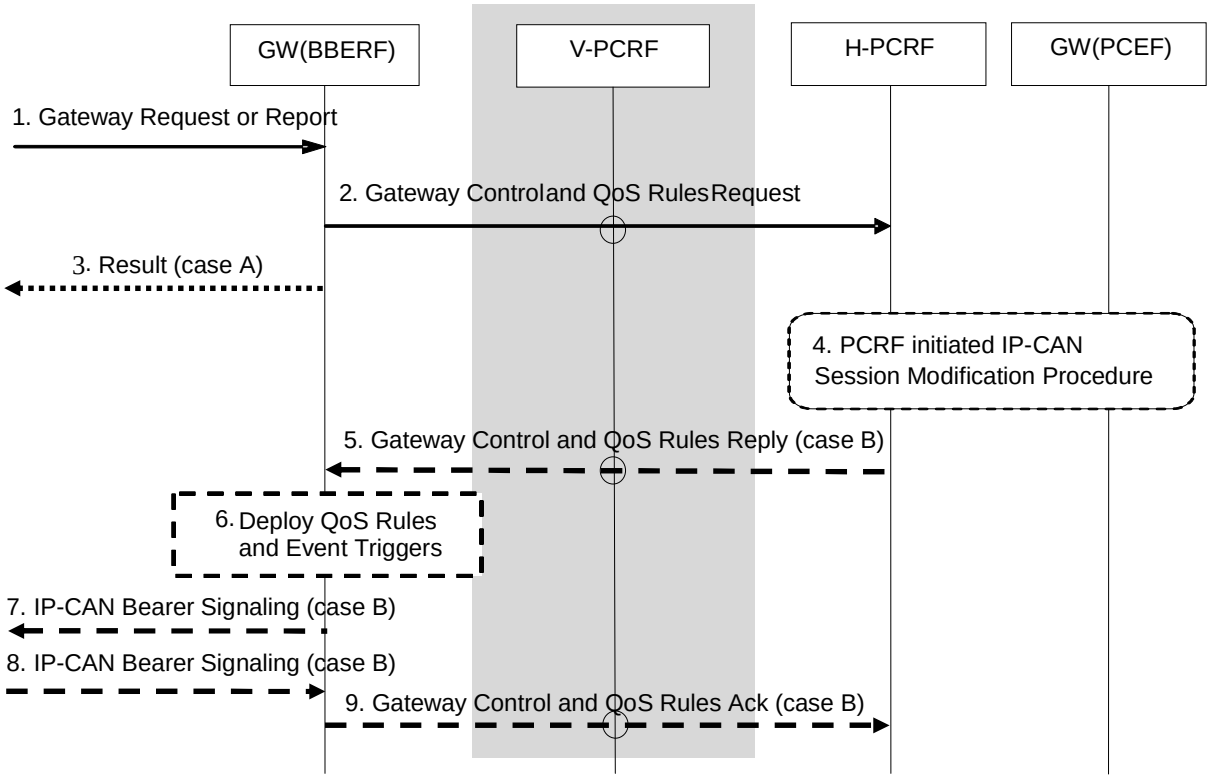

Figure 7.7.3-1: Gateway Control and QoS Rules Request

NOTE 2: If QoS rules have to be updated for case A, the PCRF shall use the Gateway Control and QoS Rules Provision procedure (clause 7.7.4).

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 and QoS Rules Request between the BBERF in the VPLMN and the H-PCRF over S9 based on PDN-Id and roaming agreements.

In the non-roaming case (Figure 5.1-1) the V-PCRF is not involved.

1. The GW (BBERF) is requested to either report an event or obtain QoS rules or both for a Gateway Control Session.

2. The GW (BBERF) sends a Gateway Control and QoS Rules Request to the PCRF and includes the new IP-CAN bearer establishment modes if changed. The information sent by the GW (BBERF) to the PCRF includes: a request for resource authorization and/or a report corresponding to a deployed Event Trigger.

3. If the GW (BBERF) is only requested to report an event, the GW (BBERF) acknowledges the step 1 by sending a result to the entity that triggered this procedure.

4. The PCRF initiated IP-CAN Session Modification Procedure may occur as the result of the Gateway Control and QoS Rules Request procedure, either to forward an Event Report to the GW (PCEF) or to issue new or revised PCC Rules and Event Triggers, or both an Event Report and a PCC Rules and Event Triggers provision.

5. If the GW (BBERF) asked for new QoS rules or IP-CAN-specific parameters need to be delivered back to the GW (BBERF) or both, the PCRF sends a Gateway Control and QoS Rules Reply to the GW (BBERF). This interaction may include QoS Rules and Event Triggers. In case 2a a charging ID may be provided together with QoS rules.

   If there are multiple BBFs associated with the IP-CAN session and the request in Step 2 is from a non-primary BBERF (see clause 6.2.1.5), only QoS rules corresponding to already activated PCC rules are included in the reply. If a request from a non-primary BBERF results in an authorization of a new QoS rule or to a modification of an existing QoS rules, the PCRF shall reject the request.

6. The QoS Rules and Event Triggers, if any, received by the GW (BBERF) are deployed. This will result in bearer binding being performed, according to the rules. This may result in the binding of additional SDFs or a change in the binding of previously bound SDFs. Subsequent events corresponding to the Event Triggers will cause an Event Report to be delivered to the PCRF by means of a Gateway Control and QoS Rules Request procedure.
7. The GW (BBERF) initiates the IP-CAN Bearer signalling if required for the QoS Rules and Event Triggers deployed in step 6.
8. The GW (BBERF) receives the response for the IP-CAN Bearer signalling.
9. If the step 5 contained new and/or modified QoS Rules, the result of the QoS rule activation is returned to the PCRF, indicating whether the resources requested have been successfully allocated.

7.7.3.2 Event reporting for PCEF in visited network and locally terminated Gxx interaction

This procedure is only used for the event reporting for a PCEF in the visited network and when the Gxx interaction is locally terminated at the V-PCRF.

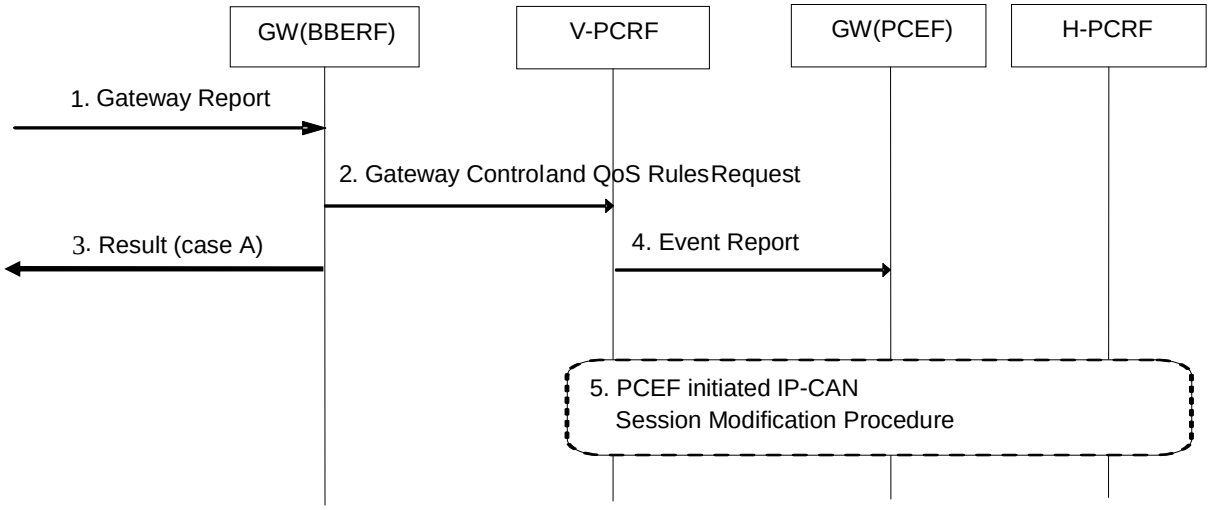

Figure 7.7.3-2: Event reporting for PCEF in visited network and locally terminated Gxx interaction

1. The GW (BBERF) is requested to report an event for a Gateway Control Session.
2. The GW (BBERF) sends a Gateway Control and QoS Rules Request to the V-PCRF and includes the new IP-CAN bearer establishment modes if changed. The information sent by the GW (BBERF) to the V-PCRF includes a report corresponding to a deployed Event Trigger.
3. Since the GW (BBERF) is only requested to report an event, the GW (BBERF) acknowledges the message received in step 1 by sending a result message to the entity that triggered this procedure.
4. The V-PCRF forwards the report corresponding to a deployed Event Trigger to the PCEF.
5. A PCEF initiated IP-CAN Session Modification Procedure may occur as the result of the received report, either to forward the report about the relevant deployed Event Trigger(s) to the H-PCRF or to request new or revised PCC Rules and Event Triggers, or both.

7.7.4 Gateway Control and QoS Rules Provision

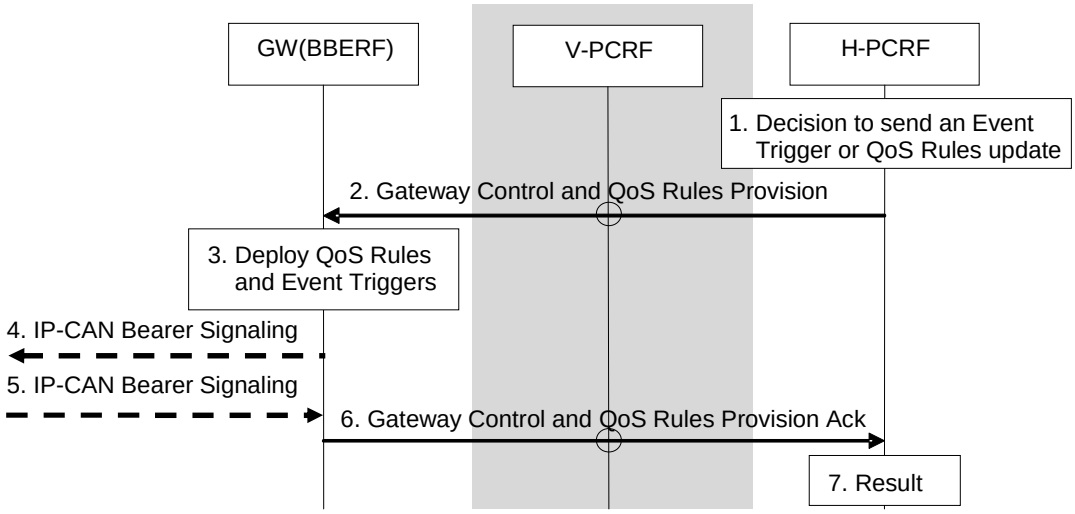

Figure 7.7.4-1: Gateway Control and QoS Rules Provision

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 and QoS Rules Provision between the BBERF in the VPLMN and the H-PCRF over S9 based on PDN-Id and roaming agreements.

In the non-roaming case (Figure 5.1-1) the V-PCRF is not involved.

1. The PCRF is requested to update the QoS Rules and Event triggers for a Gateway Control Session.

2. The PCRF sends a Gateway Control and QoS Rules Provision to the GW (BBERF). It will include QoS Rules and Event Triggers. In case 2a a charging ID may be provided together with QoS rules. If the service data flow is tunnelled at the BBERF, the information about the mobility protocol tunnelling encapsulation header may be included. It is also possible that this interaction includes an Event Report originating from the GW (PCEF) and relayed by the PCRF to the BBERF. This Event Report enables a GW (PCEF)-originating interaction to be sent by way of the PCC infrastructure to the BBERF in situations that communication is needed between the GW (PCEF) and the GW (BBERF) and no interface exists between the GWs.

3. The QoS Rules and Event Triggers received by the GW (BBERF) are deployed. This may result in bearer binding being performed, according to the rules. Subsequent events corresponding to the Event Triggers will cause an Event Report to be delivered to the PCRF by means of a Gateway Control and QoS Rules Request procedure.

4. The GW (BBERF) initiates the IP-CAN Bearer signalling if required for the QoS Rules and Event Triggers deployed in step 3.

5. The GW (BBERF) receives the response for the IP-CAN Bearer signalling.

6. The GW (BBERF) sends a Gateway Control and QoS Rules Provision Ack (Result) to the PCRF. The Result information element indicates whether the indicated QoS Rules could be implemented.

7. The PCRF has completed updating the session and can continue with the activity that prompted this procedure.

   If there are multiple BBFs associated with the IP-CAN session (see clause 6.2.1.5), then the processing of the response is as follows depending on whether the BBERF is a primary BBERF or a non-primary BBERF:

   - If a primary-BBERF reports failure to install a QoS rule in Step 4, the PCRF also removes the same QoS rule from the non-primary BBERF(s) if any. The PCRF also removes the corresponding PCC rule from the PCEF.

   - If a non-primary BBERF reports failure to install a QoS rule, the PCRF updates the enforcement status of the QoS rule for that particular BBERF in its record but does not perform any further action.

7.7.5 Void

7.8 Change in subscription for MPS priority services

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.

7.9 Procedures over Sy reference point

7.9.1 Initial Spending Limit Report Request

This clause describes the signalling flow for the H-PCRF to request the status of the policy counters available at the OCS, and to subscribe to spending limit reporting (i.e. to notifications of policy counter status changes) by the OCS. 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. 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.

The Initial Spending Limit Report Request includes all subscriber Identifiers associated with the UE available at the PCRF.

NOTE: In case the OCS returns the status of all available policy counters some of these may not be relevant for a policy decision (e.g. those used in a policy decision only when roaming).

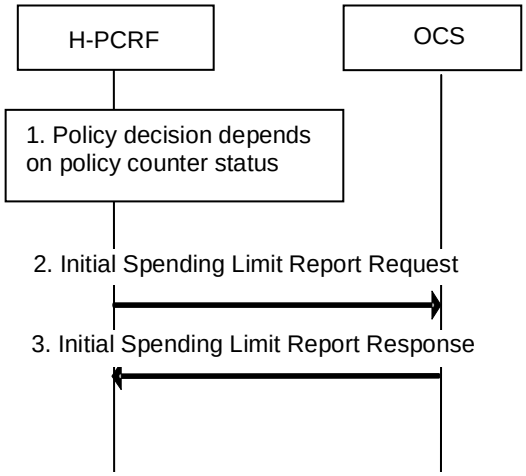

Figure 7.9.1: Initial Spending Limit Report Request

1. The H-PCRF retrieves subscription information that indicates that policy decisions 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).

3. The OCS sends an Initial Spending Limit Report Response that contains a policy counter status, and optionally pending policy counter statuses and their activation times, per required policy counter identifier and stores the H-PCRF's subscription to spending limit reports for these policy counters. If no policy counter identifier(s) was provided the OCS returns the policy counter status, optionally including pending policy counter statuses and their activation times, for all policy counter(s), which are available for this subscriber and stores the H-PCRF's subscription to spending limit reports of all policy counters provided to the H-PCRF. Otherwise, the OCS returns the policy counter status of all policy counter(s), which are available for this subscriber.

7.9.2 Intermediate Spending Limit Report Request

This clause describes the signalling flow for the H-PCRF to request the status of additional policy counters available at the OCS or to unsubscribe from spending limit reporting. 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.

NOTE: In case the OCS returns the status of all available policy counters some of these may not be relevant for a policy decision, (e.g. those used in a policy decision only when roaming).

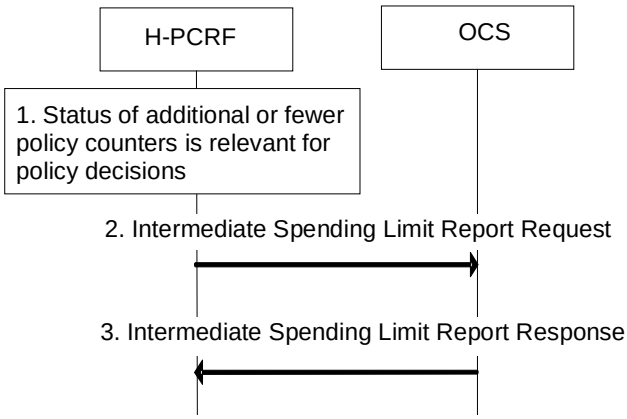

Figure 7.9.2: Intermediate Spending Limit Report Request

1. The H-PCRF determines that policy decisions depend on the status of additional policy counter(s) held at the OCS or that notifications of policy counter status changes for some policy counters are no longer required.

2. The H-PCRF sends an Intermediate Spending Limit Report Request, optionally including in the request an updated list of policy counter identifier(s).

3. The OCS sends the Intermediate Spending Limit Report Response that contains the policy counter status, and optionally pending policy counter statuses and their activation times, per required policy counter identifier, and stores or removes the H-PCRF's subscription to spending limit reporting by comparing the updated list with the existing H-PCRF subscriptions. If no policy counter identifier(s) was provided, the OCS returns the policy counter status, optionally including pending policy counter statuses and their activation times, for all policy counter(s), which are available for this subscriber and stores the H-PCRF's subscription to spending limit reports of all policy counters provided to the H-PCRF.

7.9.3 Final Spending Limit Report Request

This clause describes the signalling flow for the H-PCRF to cancel the subscriptions to status changes for the policy counters available at the OCS.

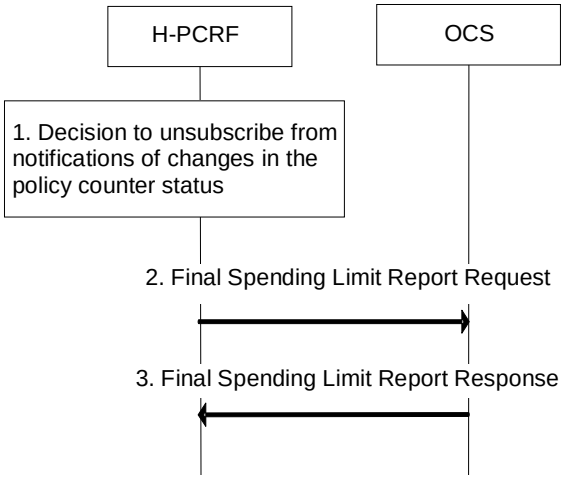

Figure 7.9.3: Final Spending Limit Report Request

1. The H-PCRF decides that notifications of policy counter status changes are no longer needed.
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.
3. The OCS removes the H-PCRF's subscription to spending limit reporting and acknowledges the request by sending the Final Spending Limit Report Response to the H-PCRF.

7.9.4 Spending Limit Report

This clause describes the signalling flow for the OCS to notify the change of the status of the subscribed policy counters available at the OCS for that subscriber. Alternatively, the signalling flow can be used by the OCS to provide one or more pending statuses for a subscribed policy counter together with the time they have to be applied.

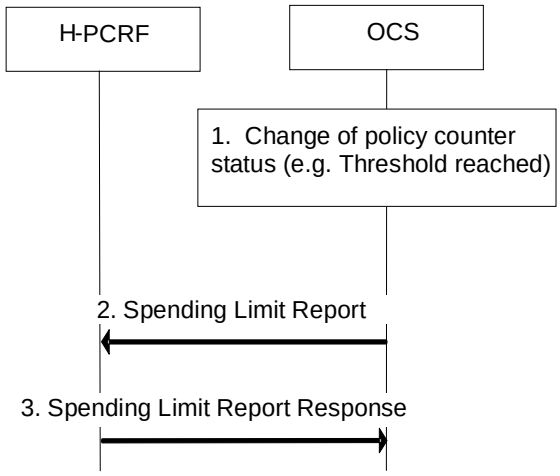

Figure 7.9.4: Spending Limit Report

1. The OCS detects that the status of a policy counter(s) has changed and the PCRF subscribed to notifications of changes in the status of this policy counter. Alternatively, the OCS may detect that a policy counter status will change at a future point in time, and decides to instruct the PCRF to apply one or more pending statuses for a requested policy counter.
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.

NOTE: The values related to the status of the subscribed counter (e.g. valid, invalid or any other status) are not specified. The interpretation and actions related to the defined values are out of scope of 3GPP.

3. The H-PCRF acknowledges the Spending Limit Report and takes that information into account as input for a policy decision.

7.9.5 Sy Session Termination

This clause describes the signalling flow for the OCS to terminate the Sy session of a subscriber. This feature is optional.

NOTE 1: When the PCRF supports this procedure and a subscriber is removed from an OCS system, the existing Sy session of the subscriber can be terminated by this procedure.

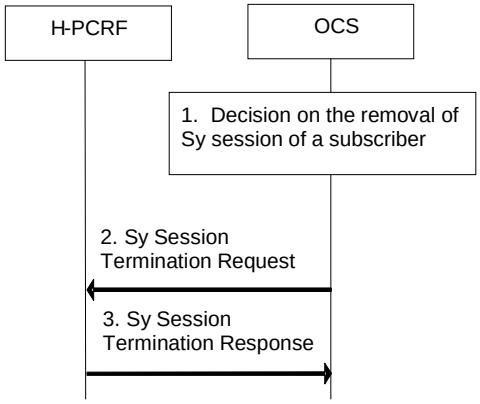

Figure 7.9.5: Sy Session Termination

1. The OCS decides that the Sy session for a subscriber needs to be terminated.

2. The OCS sends the Sy Session Termination Request to H-PCRF to terminate the Sy session. The H-PCRF removes the Sy session context of the subscriber.

NOTE 2: The termination of the Sy session causes the H-PCRF to make the applicable policy decision and act accordingly, i.e. sessions on other interfaces such as the Rx or Gx interface will remain established, unless the policy decision causes their termination.

3. The H-PCRF acknowledges the termination of the Sy session of the subscriber by sending the Sy Session Termination Response.

7.10 Procedures over Np reference point

7.10.1 Report RAN user plane congestion information to PCRF

This clause describes the signalling flow for reporting RUCI (RAN User Plane Congestion Information) from the RCAF to the PCRF. Any RUCI changes shall be reported by RCAF unless reporting restrictions apply.

Two types of messages are used on Np for transfer of congestion information from RCAF to PCRF:

- Non-aggregated RUCI report messages, which are sent on a per UE per APN basis using DRA routing. The IMSI and the APN can be used to route messages.

- Aggregated RUCI report messages, which are sent between an RCAF and PCRF and contain congestion information for multiple UEs. A logical PCRF id is allocated for these aggregate messages which determine the destination of the message.

The congestion reporting takes place as shown in Figure 7.10.1 below.

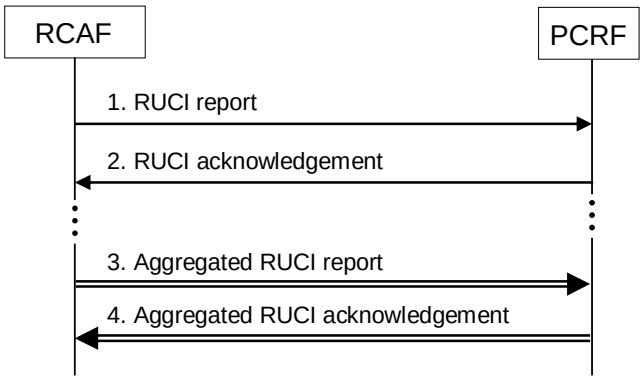

Figure 7.10.1: RUCI reporting from RCAF to PCRF

1. RCAF indicates congestion information for a given UE and APN in a RUCI report message. This message is routed by DRA to the appropriate PCRF based on IMSI and APN.

   The RUCI report message includes the RUCI which is defined in clause 6.1.15.1.

   Upon receiving the RUCI the PCRF stores the identity of the RCAF for the given UE if the RUCI indicates congestion. The PCRF makes a policy decision.

2. The PCRF allocates a logical PCRF id to identify the PCRF that is the Np destination for the given UE and APN for the RCAF when sending aggregate messages, and reports the logical PCRF id in the RUCI acknowledgement.

   The RCAF stores the logical PCRF id in the UE context for the given IMSI, APN combination.

3. Subsequent congestion information for the given UE can be sent as part of an Aggregated RUCI report message. Such a message can contain the congestion information for multiple UEs. These UEs can have different congestion levels associated with different eNB identifier or ECGI or SAI, which are indicated in the message. An aggregated RUCI report message is always destined to a single PCRF only, and can be routed directly to that PCRF or via the DRA.

NOTE: How the RCAF decides about which information should be contained in a single aggregated RUCI report message out of the UEs with a given logical PCRF id is out of the scope of 3GPP specifications. e.g. the RCAF may aggregate information only for a given cell or eNB into a single message. Alternatively, the RCAF may wait for a configurable period of time to aggregate information from multiple cells or eNBs into a single message. The amount of RUCI updates may be limited by configuring a minimum time between RUCI updates in the RCAF (e.g. when only the identifier of the congested cell serving the UE has changed). This configuration is expected to take both the required accuracy as well as the acceptable signalling amount into account.

4. The Aggregated RUCI is acknowledged.

7.10.2 PCRF provided reporting restrictions

This clause describes the signalling flow for adding, updating or removing reporting restrictions for a given UE and APN. A pre-condition for this procedure is that the RCAF has already performed RUCI reporting for the given UE and APN. The PCRF stores the RCAF identity for the given UE when the RCAF performs RUCI reporting indicating congestion

This procedure may be triggered by the initial RUCI report message for the given UE at an RCAF, or by other events, e.g., change in the subscription. The procedure is shown in Figure 7.10.2 below.

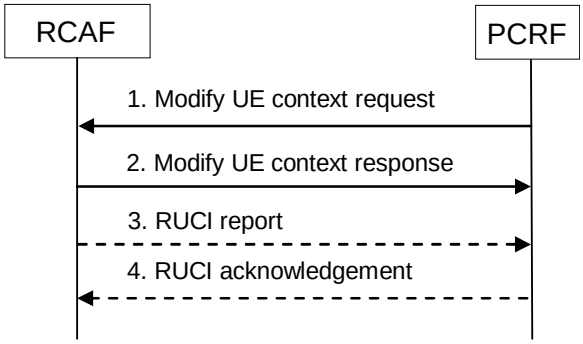

Figure 7.10.2: PCRF provided reporting restrictions

1. PCRF sends a Modify UE context request to the RCAF of the given UE and APN using the stored identity of the RCAF, specifying the new reporting restrictions or the removal of the reporting restrictions. The RCAF stores the new reporting restrictions or removes the reporting restrictions accordingly.
2. The RCAF sends a Modify UE context response back to the PCRF to notify the PCRF about the success of the change in the reporting restrictions.
3. In case the RCAF already had reporting restrictions for the UE and the APN which are changed in step 2, this may trigger RUCI reporting as specified in clause 7.10.1. This occurs in case of a change from disabled reporting to enabled reporting, or if some reporting restrictions are lifted. The RCAF uses the RUCI report message to report congestion information to the PCRF if it is allowed by the change in the reporting restrictions.
4. The RUCI is acknowledged.

7.10.3 UE mobility between RCAFs

This clause describes the handling mobility of a UE from one RCAF to a different RCAF. The PCRF applies the rules described in clause 6.1.15.3.

The process is shown in Figure 7.10.3 below for the case when the UE is affected by congestion at RCAF2 after the UE was earlier affected by congestion at RCAF1.

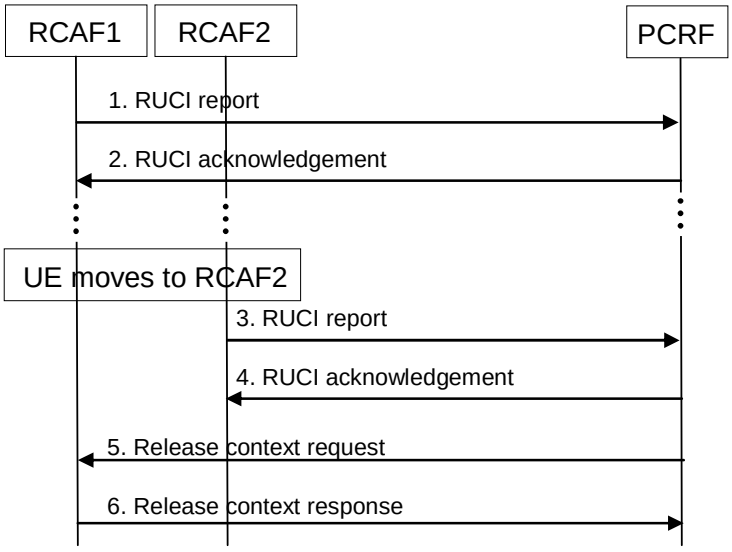

Figure 7.10.3: UE mobility from RCAF1 to RCAF2 in case UE is affected by congestion at RCAF2 after the UE was earlier affected by congestion at RCAF1

1. RCAF1 reports RAN user plane congestion information (RUCI). The PCRF stores the identity of the current RCAF1 for a given UE when it receives the congestion information over Np that is different from no congestion.

2. The RUCI is acknowledged.

3. The UE moves to RCAF2 where it is affected by congestion. RCAF2 reports RAN user plane congestion information (RUCI). The PCRF stores the identity of the current RCAF2 for the given UE when it receives the congestion information over Np that is different from no congestion.

4. The RUCI is acknowledged.

5. Using on the previously stored identity of the old RCAF, the PCRF sends a Release context request message to RCAF1.

6. RCAF1 acknowledges this by sending the Release context response message to the PCRF. The RCAF releases the context corresponding to the given UE and 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 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.

7.11 Procedures over Nt reference point

7.11.1 Negotiation for future background data transfer

This procedure enables the negotiation between the SCEF and the H-PCRF about the time window and the related conditions for future background data transfer (as described in clause 6.1.16). The interaction between the SCEF and the H-PCRF is not related to an IP-CAN session and the H-PCRF associates the information provided by the SCEF to the policies belonging to the ASP and stored in the SPR.

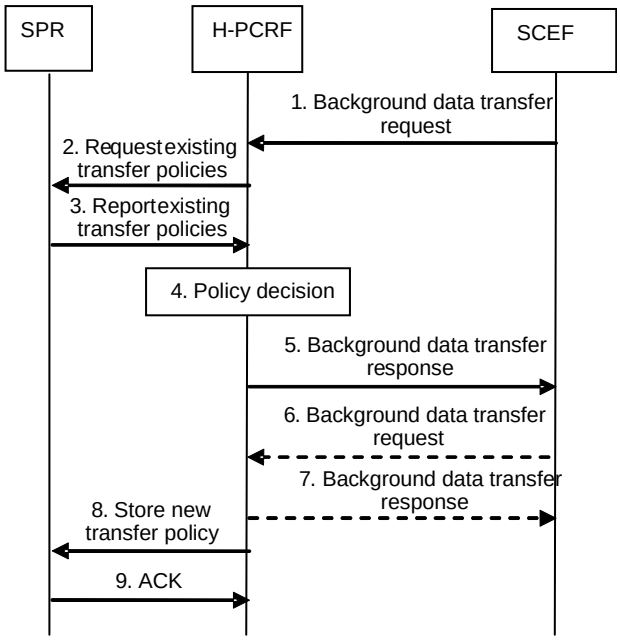

Figure 7.11.1-1: Negotiation for future background data transfer

1. Based on an AF request, the SCEF sends a Background data transfer request to the H-PCRF. The background data transfer request contains ASP identifier, the volume of data to be transferred per UE, the expected amount of UEs, the desired time window and optionally, network area information (e.g. list of cell ids, TAs/RAs).

NOTE 1: The SCEF does not provide any information about the identity of the UEs potentially involved in the future background data transfer.

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

2. The H-PCRF requests from the SPR all existing transfer policies.

3. The SPR provides all existing transfer policies and corresponding network area information to the H-PCRF.

4. The H-PCRF determines, based on information provided by the AF and other available information (see clause 6.1.16) one or more transfer policies. A transfer policy consists of a recommended time window for the background data transfer, a reference to a charging rate for this time window and optionally a maximum aggregated bitrate.

NOTE 3: The maximum aggregated bitrate is not enforced in the network.

5. The H-PCRF sends a Background data transfer response to the SCEF with the possible transfer policies and a reference ID.

NOTE 4: The SCEF forwards the information to the AF. The AF stores the reference ID for the future transfer of AF session information related to this background data transfer via the Rx interface.

6.-7. If the SCEF receives more than one transfer policy, the AF selects one of them and send another Background data transfer request to inform the H-PCRF about the selected transfer policy. The H-PCRF sends a Background data transfer response to the SCEF to acknowledge the selection.

NOTE 5: If the SCEF receives only one transfer policy, the AF is not required to confirm.

8. The H-PCRF stores the reference ID together with the new transfer policy and the corresponding network area information in the SPR.

9. The SPR sends an acknowledgement to the H-PCRF.

7.12 Procedures for management of PFDs

7.12.1 PFD Retrieval by the PCEF/TDF ("Pull mode")

This procedure enables the PCEF/TDF to retrieve PFDs for an Application Identifier from the PFDF when a PCC/ADC Rule with an Application Identifier is provisioned/activated and PFDs provisioned by the PFDF are not available at the PCEF/TDF.

In addition, this procedure enables the PCEF/TDF to retrieve PFDs from the PFDF when the caching timer for an Application Identifier elapses and a PCC/ADC Rule for this Application Identifier is still active.

The PCEF/TDF may retrieve PFDs for one or more Application Identifiers in the same Request. All PFDs related to an Application Identifier is provided in the response from the PFDF. The signalling flow of PFD Retrieval is depicted in Figure 7.12.1-1 as below.

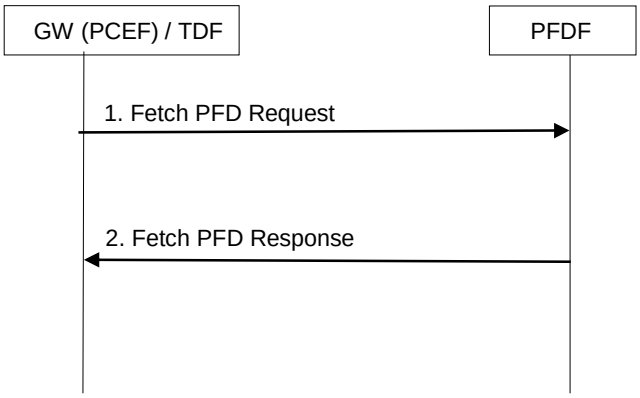

Figure 7.12.1-1 PFD Retrieval by the PCEF/TDF

1. When one of the above mentioned conditions is met, PCEF/TDF shall fetch from the PFDF the PFDs for the Application Identifier(s) by sending Fetch PFD Request, in which the Application Identifier(s) is included.

2. The PFDF shall response with the list of Application Identifier and all associated PFDs in the Fetch PFD Response message. The PCEF/TDF shall bind the PFDs received from the PFDF to the respective Application Identifier.

7.12.2 Management of PFDs in the PCEF/TDF ("push mode")

This procedure enables the provisioning, modification or removal of PFDs associated with an application identifier in the PCEF/TDF via PFDF. Either the complete list of all PFDs of all application identifiers, the complete list of all PFDs of one or more application identifiers or a subset of PFDs for individual application identifiers may be managed.

Each PFD of an application identifier is associated with a PFD id in case a subset of the PFD(s) associated with an application identifier can be provisioned, updated or removed. In case always the full set of PFD(s) for an application identifier is managed in each transaction, PFD ids do not need to be provided.

NOTE 1: The prerequisite to provision or update PFDs is that the application identifier which the external entity provided is mapped into the application identifier that is included in the PCC/ADC Rule as described in TS 23.682 [42].

The interaction between the PFDF and the PCEF/TDF is not related to an IP-CAN session.

The PFDF may decide to delay the distribution of PFDs to PCEFs/TDFs for some time to optimize the signalling load over the Gw/Gwn interface. If the PFDF received an Allowed Delay for a PFD, the PFDF shall distribute this PFD within the indicated time interval.

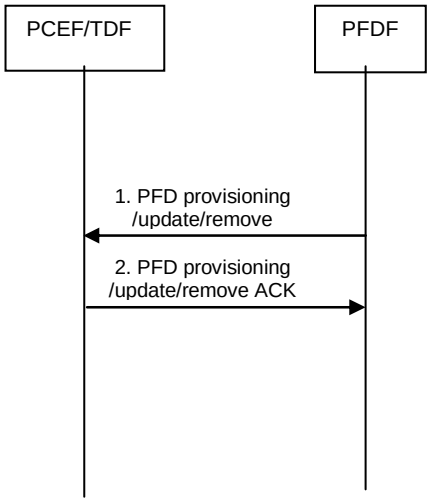

Figure 7.12.2-1: Provisioning/update/removal of PFDs in the PCEF/TDF

1. The PFDF may provision, update or remove one, multiple, or all PFDs associated with an application identifier. The PFDF may manage PFDs for more than one application identifier at the same time. Alternatively, the PFDF may provision or remove the list of all PFDs associated with all application identifiers.

2. The PCEF/TDF binds (for provision or update) or unbinds (for removal) the PFDs to the application identifier received from the PFDF. The provisioning of PFDs associates new PFDs to an application identifier. The PFDF may also provide a PFD id for each PFD provided. The update of PFDs modifies existing PFDs associated to an application identifier. Either all PFDs of an application identifier are replaced, or a subset of the PFDs are replaced, where each PFD is identified by a PFD id. Partial modification of a PDF is not supported. The removal of PFDs removes some or all existing PFDs associated to an application identifier. In the case of removal of a subset of the PFD(s), each PFD is identified by a PFD id. The PCEF/TDF acknowledges the reception of the PFDs to the PFDF.

Annex A (normative): Access specific aspects (3GPP)

A.1 GPRS

A.1.0 General

The GPRS IP-CAN employs, for an IP-CAN session, the concept of PDP contexts in order to provide an information transmission path of defined capacity (QoS). For GPRS, the IP-CAN bearer is the PDP context.

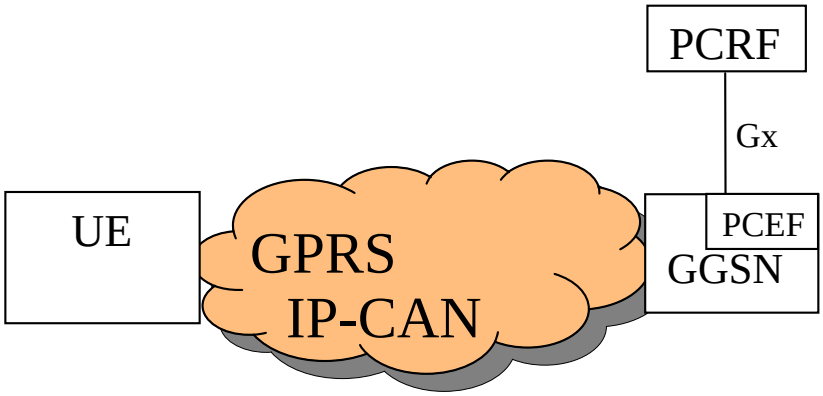

Figure A.1: The GPRS IP-CAN

A.1.1 High level requirements

A.1.1.1 General

A.1.1.2 Charging related requirements

It shall be possible for the charging system to select the applicable rate based on:

- SGSN IP address that is used by the GTP control plane for the handling of control messages.
- location with the granularity as specified for the credit re-authorization trigger Location change in clause A.1.3.1.3;
- User CSG Information, including CSG ID, access mode and CSG membership indication;
- RAT type.

A.1.1.3 Policy control requirements

IP-CAN Bearer QoS control allows the PCC architecture to control the "Authorized QoS" of a PDP context. Criteria such as the QoS subscription information may be used together with service-based, subscription-based, or a predefined PCRF internal policies to derive the "Authorized QoS" of a PDP context.

NOTE: 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 takes place first.

A.1.1.4 QoS control

For GPRS IP-CANs it shall be possible to apply QoS control at APN-level.

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 QCIs at the PCEF within the same APN.

NOTE: 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.

A.1.2 Architecture model and reference points

A.1.2.1 Reference points

A.1.2.1.1 Gx reference point

The Gx reference point enables the signalling of PCC rules, which govern the PCC behaviour, and it supports the following GPRS-specific functions:

- Indication of PDP context activation, modification and deactivation.

A.1.2.2 Reference architecture

In the GPRS IP-CAN, the Bearer Binding and Event Reporting Function (BBERF) does not apply.

A.1.3 Functional description

A.1.3.1 Overall description

A.1.3.1.1 Binding mechanism

A.1.3.1.1.0 General

As explained in clause 6.1.1, the binding mechanism is performed in three different steps: session binding, PCC rule authorization and bearer binding. Session binding has no GPRS specifics.

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.

NOTE: For the authorization of PCC Rules with the same QCI the PCRF may also check that aggregated GBR is within the limits supported by the serving network to minimize the risk of rejection of the bearer by the serving network.

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.

The bearer binding performed by the PCRF shall bind a PCC rule that is authorized for a TFT packet filter to the PDP context 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).

The bearer binding performed by the PCEF shall compare the PCC rule QoS parameters with the PDP context QoS parameters and bind a PCC rule:

- to a candidate PDP context with a matching QoS class and Evolved ARP (if this is supported by the SGSN);
- to a candidate PDP context with a matching QoS class and Evolved ARP (if this is supported by the SGSN) that, after modification of the bitrates, fulfils the PCC rule QoS demands;
- to a new PDP context with a matching QoS class and Evolved ARP (if this is supported by the SGSN), if there is no suitable candidate PDP context present.

The bearer binding mechanism associates the PCC rule with the PDP context to carry the service data flow. The association shall:

- cause the downlink part of the service data flow to be directed to the PDP context in the association, and
- assume that the UE directs the uplink part of the service data flow to the PDP context in the association.

Thus, the detection of the uplink part of a service data flow shall be active on the PDP context, which the downlink packets of the same service data flow is directed to. The detection of the uplink part of the service data flow may be active, in parallel, on any number of additional PDP contexts.

A.1.3.1.1.1 Bearer binding mechanism allocated to the PCEF

When the bearer binding mechanism is allocated to the PCEF, no per bearer information is required to be communicated over the Gx reference point.

Once the PCRF has provided the PCC rule decisions at the IP-CAN session establishment procedure, the PCRF shall provide further PCC rule decisions

- using the PCRF initiated IP-CAN Session Modification procedure; or
- in response to an event report from the PCEF (the GW (PCEF) initiated IP-CAN Session Modification).

The bearer binding function shall not combine PCC rules with different ARP values onto the same PDP context.

NOTE: If Evolved ARP is not supported by the SGSN then this enables a modification of the PDP context ARP without impacting the bearer binding after relocation to a SGSN that supports Evolved ARP.

A.1.3.1.1.2 Bearer binding mechanism allocated to the PCRF

If a PDP context is established/modified in order to successfully perform the bearer binding the PCRF will set the PCC rule as binding-pending status until the PCEF reports the establishment or modification of a PDP context that fulfils the PCC rule demands or the PCC rule is removed.

The following particularities apply when the bearer binding mechanism is allocated to the PCRF:

- The PCEF
  - shall include a bearer reference in all requests for PCC decisions;
  - shall report bearer QoS class identifier and the associated bitrates for new/modified PDP contexts;
  - shall report the TFT filter status for new PDP contexts and for modified TFTs;
  - shall report the deactivation of a PDP context
- The PCRF
  - shall provide the bearer reference for the binding result when activating a PCC rule;
  - shall arm the GPRS-specific IP-CAN event trigger "PDP context activity".
- shall arm the event trigger "traffic mapping information change".

NOTE: For the above case, the allocation of the bearer binding mechanism to the PCRF facilitates the migration from Rel-6 products to Rel-7 products. The allocation of the binding mechanism may be re-evaluated in future releases.

When the PCRF performs the bearer binding the ARP information in the PCC rule shall be ignored unless the SGSN has indicated support for Evolved ARP.

A.1.3.1.2 Reporting

A container may be closed and a new container opened by the triggering of event triggers.

A.1.3.1.3 Credit management

For GPRS the PCEF shall initiate one credit management session for each PDP context.

For GPRS the credit re-authorisation triggers in table A.1-1 shall apply in addition to the ones in table 6.1. They are applicable both in case of PCEF and in case of TDF.

Table A.1-1: GPRS specific credit re-authorization triggers

Credit re-authorization trigger	Description
SGSN change	The UE has moved to a new SGSN.
RAT type change.	The characteristics of the air interface, communicated as the radio access type, have changed.
Location change (routeing area)	The routeing area of the UE has changed.
Location change (CGI/SAI)	The CGI/SAI of the UE has changed.
User CSG Information change in CSG cell	User CSG Information has changed when the UE enters/leaves/accesses via a CSG cell
User CSG Information change in subscribed hybrid cell	User CSG Information has changed when the UE enters/leaves/accesses via a hybrid cell in which the subscriber is a CSG member
User CSG Information change in un-subscribed hybrid cell (see note)	User CSG Information has changed when the UE enters/leaves/accesses via a hybrid cell in which the subscriber is not a CSG member
NOTE: Due to the increased signalling load, such reporting should be applied for a limited number of subscribers only.	

If the Location change trigger for CGI / SAI or RAI is armed, the GGSN should request the SGSN to report any changes in location to the level indicated by the trigger according to the procedures described in TS 23.060 [12]. If credit re-authorization triggers and event triggers require different levels of reporting of location change for different PDP contexts for a single IP-CAN session, the SGSN reports location changes to the highest level of detail required. However, the GGSN should not trigger a credit re-authorization if the report received is more detailed than requested by the OCS.

If the User CSG Information change in CSG cell trigger is armed, the GGSN should request the SGSN to report any changes in user CSG information when the UE enters/leaves/accesses via a CSG cell.

If the User CSG Information change in subscribed hybrid cell trigger is armed, the GGSN should request the SGSN to report any changes in user CSG information when the UE enters/leaves/accesses via a hybrid cell in which the subscriber is a CSG member.

If the User CSG Information change in un-subscribed hybrid cell trigger is armed, the GGSN should request the SGSN to report any changes in user CSG information when the UE enters/leaves/accesses via a hybrid cell in which the subscriber is not a CSG member.

If credit re-authorization triggers, event triggers and IP-CAN session related policy information require different levels of reporting of User CSG information for a single IP-CAN session, then the User CSG information to be requested from the SGSN should be changed to the highest level of detail required.

Change of UE presence in Presence Reporting Area is not applicable for GPRS IP-CAN.

A.1.3.1.4 Event Triggers

For GPRS the event triggers in table A.2 shall apply in addition to the ones in table 6.2 at the PCEF upon the request of the PCRF.

NOTE: The request from the PCRF can be triggered by configured policy, or a request received from the TDF. In case of TDF, this may be a result of credit re-authorization trigger received by the TDF from the OCS.

Table A.2: GPRS specific event triggers

Event trigger	Description
SGSN change	The UE has moved to a new SGSN.
RAT type change.	The characteristics of the air interface, communicated as the radio access type, have changed.
PDP Context Activity	The GGSN has received a request for a PDP context activation, modification or deactivation. Note 1.
Location change (routeing area)	The routeing area of the UE has changed.
Location change (CGI/SAI)	The CGI/SAI of the UE has changed.
Subscribed APN-AMBR change	The subscribed APN-AMBR has changed.
User CSG Information change in CSG cell	User CSG Information has changed when the UE enters/leaves/accesses via a CSG cell. (Note 2)
User CSG Information change in subscribed hybrid cell	User CSG Information has changed when the UE enters/leaves/accesses via a hybrid cell in which the subscriber is a CSG member. (Note 2)
User CSG Information change in un-subscribed hybrid cell (see note)	User CSG Information has changed when the UE enters/leaves/accesses via a hybrid cell in which the subscriber is not a CSG member. (Note 2)
3GPP PS Data Off status change	The PCEF reports when the 3GPP PS Data Off status changes.
NOTE 1: Available only when the bearer binding mechanism is allocated to the PCRF. NOTE 2: Due to the increased signalling load, such reporting should be applied to a limited number of subscribers only.	

If the Location change trigger is armed, the GGSN should request the SGSN to report any changes in location to the level indicated by the trigger according to the procedures described in TS 23.060 [12]. If credit-authorization triggers and event triggers require different levels of reporting of location change for different PDP contexts for a single UE, the SGSN reports location changes to the highest level of detail required. However, the GGSN should not trigger a request for PCC rules if the report received is more detailed than requested by the PCRF.

For GPRS, the traffic mapping information is represented by the TFT information.

For GPRS, the loss/recovery of transmission resources is indicated by a PDP context modification changing the 'Maximum bitrate' UMTS QoS parameter to/from 0 kbit/s (as described in the PDP context preservation procedure in TS 23.060 [12]).

The User Location Report in the Access Network Information Reporting contains the CGI/SAI and when the PDP context is deactivated, information on when the UE was last known to be in that location.

If the User CSG Information change in CSG cell was provided as event trigger, the GGSN should request the SGSN to report any changes in user CSG information when the UE enters/leaves/accesses via a CSG cell.

If the User CSG Information change in subscribed hybrid cell was provided as event trigger, the GGSN should request the SGSN to report any changes in user CSG information when the UE enters/leaves/accesses via a hybrid cell in which the subscriber is a CSG member.

If the User CSG Information change in un-subscribed hybrid cell was provided as event trigger, the GGSN should request the SGSN to report any changes in user CSG information when the UE enters/leaves/accesses via a hybrid cell in which the subscriber is not a CSG member.

If credit re-authorization triggers, event triggers and IP-CAN session related policy information require different levels of reporting of User CSG information for a single IP-CAN session, then the User CSG information to be requested from the SGSN should be changed to the highest level of detail required.

Change of UE presence in Presence Reporting Area is not applicable for GPRS IP-CAN.

A.1.3.1.5 Policy Control

For GPRS the AF instruction to report changes of the IP-CAN bearer level information Type of IP-CAN shall also result in a reporting of RAT type changes, even if the IP-CAN type is unchanged.

A.1.3.2 Functional entities

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

A.1.3.2.1.0 General

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.

A.1.3.2.1.1 Input for PCC decisions

The PCRF shall accept any of the following input which the PCEF may provide, specific for GPRS, as a basis for decisions on PCC rule operations.

The following information represents GPRS specific values of the ones listed in clause 6.2.1.1:

- Subscriber Identifier in the form of IMSI, MSISDN;
- A PDN identifier in the form of APN;
- A PLMN identifier in the form of SGSN Mobile Country Code and Mobile Network Code;
- Type of IP-CAN set to GPRS;
- IP-CAN bearer attributes in the form of:
  - Requested QoS, for a PDP context;
  - TFT, to enable the identification of the corresponding PDP Context;
- Location of the subscriber in the form of CGI/SAI or RAI.

The following information is in addition to the ones listed in clause 6.2.1.1:

- RAT type.
- Subscribed APN-AMBR.

The SPR may provide the following information for a subscriber (in addition to the information in clause 6.2.1.1) connecting to a specific PDN:

- Authorized APN-AMBR.

The Authorized APN-AMBR is derived by the PCRF from SPR interaction, according to operator policy.

A.1.3.2.2 Policy and Charging Enforcement Function (PCEF)

A.1.3.2.2.1 General

This functional entity is located in the GGSN. The GGSN provides the GPRS-specific bearer QoS handling.

The PCEF shall contact the PCRF based on PCRF address information that shall be configured for the access point name (APN) together with the IMSI or MSISDN (if needed).

The PCEF shall maintain a 1:1 mapping from the GPRS QoS Class Identifier to a UMTS QoS profile and vice versa. Each GPRS QoS Class Identifier (QCI) parameter value has a 1:1 mapping to a set of QoS parameters defined for GPRS, TS 23.107 [14]. A recommended mapping is listed in table A.3.

Table A.3: Recommended mapping for GPRS QoS Class Identifier to/from Release 99 UMTS QoS parameters

GPRS QoS Class Identifier value	UMTS QoS parameters			
	Traffic Class	THP	Signalling Indication	Source Statistics Descriptor
1	Conversational	n/a	n/a	speech (NOTE 1)
2	Conversational	n/a	n/a	unknown
3	Streaming	n/a	n/a	speech (NOTE 1)
4	Streaming	n/a	n/a	unknown
5	Interactive	1	Yes	n/a
6	Interactive	1	No	n/a
7	Interactive	2	No	n/a
8	Interactive	3	No	n/a
9	Background	n/a	n/a	n/a
NOTE 1: The operator's configuration should reserve QCI values that map to "speech" for service data flows consisting of speech (and the associated RTCP) only.				

NOTE 2: This table defines the mapping for GPRS QCI to/from UMTS QoS parameters for pre-Release 8 GPRS. The characteristics of GPRS QCIs are independent from the standardized QCI characteristics for EPS.

The PCEF determines Release 97/Release 98 attributes from Release 99 attributes according to TS 23.107 [14].

The remaining UMTS QoS parameters are subject to operator's policies and either provisioned in the Create PDP Context Request or locally defined in GGSN.

NOTE 3: Any change of the ARP parameter by the PCEF may get overwritten by the SGSN due to subscription enforcement unless the SGSN has indicated support for Evolved ARP.

For each PDP context, the PCEF shall accept information during bearer establishment and modification relating to:

- The user and terminal (e.g. MSISDN, IMEISV);
- Bearer characteristics (e.g. QoS negotiated, APN, IM CN Subsystem signalling flag);
- Network related information (e.g. MCC and MNC).

The PCEF shall use this information in the OCS request/reporting or request for PCC rules.

A GGSN may provide more than one APN for access to the same PDN. It should be possible to enable or disable PCC functionality for each APN, independent from the other APNs for access to the same PDN. Once the PCC functionality is disabled, regular GPRS charging and policy methods would be applied, i.e. no PCRF interaction would occur.

For each PDP context, there shall be a separate OCS request/OFCS reporting, so this allows the OCS and offline charging system to apply different rating depending on the PDP context.

The GGSN shall report the service data flow based charging data on a per PDP context basis.

The GGSN shall be able to request the SGSN to provide reports of changes in CGI/SAI/RAI of a UE as directed by the credit re-authorization triggers and/or event triggers.

The PCEF enforces QoS Policies as indicated by the PCRF in accordance to what is stated in clause 6.2.2.1 with the following additions:

- Authorized APN-AMBR enforcement. The PCEF shall enforce the authorized APN-AMBR received via the Gx interface for the total bandwidth usage of non-GBR QCI for the APN.

Only the GBR per bearer is used for resource reservation (e.g. admission control in the RAN).

The MBR (per PCC rule / per bearer) and the authorized APN-AMBR are used for rate policing.

When the GGSN is connected to a SGSN that does not support the Evolved ARP, the GGSN shall map the Evolved ARP to Rel-99 ARP parameter value as specified in Annex E of TS 23.401 [17].

A.1.3.2.2.2 Service data flow detection

For uplink traffic, in the case of GPRS, all the uplink parts of service data flows templates, which are associated with the PDP context are candidates for matching in the detection process.

NOTE: Service data flow templates, which are not associated with the PDP context the packet was received, are not candidates for matching (dashed in the figure).

A.1.3.2.2.3 Packet Routeing and Transfer Function

The PCEF performs the packet routeing and transfer functions as specified in TS 23.060 [12], with the differences specified in this clause.

For the PDP address of an UE, the PCEF routes downlink packets to the different PDP contexts based on the downlink parts of the service data flow templates, in the active PCC rules and their routeing associations to the PDP contexts. The association between an active PCC rule and a PDP context shall correspond to the downlink TFT received from the UE. Each active PCC rule shall have a single routeing association to a PDP context. Upon reception of a packet, the PCEF evaluates the downlink part of the service data flow templates of the PCC rules activated for the PDP address in order of precedence to find a match. When the first match is found, the packet is tunnelled to the SGSN via the PDP context, for which the PCC rule has the routeing association. If no match is found, the PCEF shall silently discard the packet.

The UE shall define TFTs that enable successful binding at the PCRF for service data flows requiring a binding to occur.

For each uplink packet, the UE should choose the PDP context that is used for the downlink direction of the same service data flow, as declared in the TFT information. The PCEF shall only apply the uplink parts of the service data flow templates of the PCC rules, which are associated with the same PDP context as the uplink packet arrived on.

The packet filters, to be applied on dedicated signalling PDP contexts, shall form PCC rules, which shall be granted higher precedence than any other PCC rule and be active on the dedicated signalling context.

A.1.3.2.2.4 Measurement

The details of measurement are specified in TS 32.251 [9].

A.1.3.2.3 Application Function (AF)

For GPRS the AF instruction to report changes of the IP-CAN bearer level information Type of IP-CAN will also result in a reporting of RAT type changes, even if the IP-CAN type is unchanged.

The AF instructions to report loss of transmission resources will result in a notification from the PCRF that may include an indication that the transmission resources are lost due to PS to CS handover.

NOTE: The AF action up to notification of termination of transmission resources due to PS to CS handover is application specific. IMS interprets that the PS to CS handover notification as SRVCC.

A.1.3.3 Policy and charging control rule

A.1.3.3.1 General

Void.

A.1.3.3.2 Policy and charging control rule operations

The PCRF associates, at activation, a PCC rule with a PDP context at the PCEF.

A.1.3.4 IP-CAN bearer and IP-CAN session related policy information

For GPRS the IP-CAN bearer and IP-CAN session related policy information in table A.4 shall apply in addition to the ones in table 6.4.

Table A.4: PCC related IP-CAN bearer and IP-CAN session related policy information

Attribute	Description	PCRF permitted to modify the attribute	Scope
User CSG Information change in CSG cell	Defines whether to report User CSG Information change when the UE enters/leaves/accesses via a CSG cell.	Yes	IP-CAN session
User CSG Information change in subscribed hybrid cell	Defines whether to report User CSG Information change when the UE enters/leaves/accesses via a hybrid cell in which the subscriber is a CSG member.	Yes	IP-CAN session
User CSG Information change in un-subscribed hybrid cell (see note)	Defines whether to report User CSG Information change when the UE enters/leaves/accesses via a hybrid cell in which the subscriber is not a CSG member.	Yes	IP-CAN session
NOTE: Due to the increased signalling load, such reporting should be applied for a limited number of subscribers only.			

If the User CSG Information change in CSG cell was provided under IP-CAN session related policy information, the GGSN should request the Serving Node to report any changes in user CSG information when the UE enters/leaves/accesses via a CSG cell.

If the User CSG Information change in subscribed hybrid cell was provided under IP-CAN session related policy information, the GGSN should request the Serving Node to report any changes in user CSG information when the UE enters/leaves/accesses via a hybrid cell in which the subscriber is a CSG member.

If the User CSG Information change in un-subscribed hybrid cell was provided under IP-CAN session related policy information, the GGSN should request the Serving Node to report any changes in user CSG information when the UE enters/leaves/accesses via a hybrid cell in which the subscriber is not a CSG member.

If credit re-authorization triggers, event triggers and IP-CAN session related policy information require different levels of reporting of User CSG information for a single IP-CAN session, then the User CSG information to be requested from the Serving Node should be changed to the highest level of detail required.

The reporting of User CSG information to the OFCS shall be done on the level of detail as requested by the PCRF within IP-CAN session related policy information and the reporting of User CSG information to the OCS shall be done on the level of detail as requested by the OCS re-authorization triggers.

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) shall be mapped by the PCEF to the GBR and MBR of the PDP context as described in clause 6.2.2.4. The mapping of the QCI to the UMTS QoS profile parameters is defined in clause A.1.3.2.2.1.

A.1.3.4a TDF session related policy information

For TDF session related policy information in table A.4a shall apply in addition to the ones in table 6.4a.

Table A.4a: TDF session related policy information

Attribute	Description	PCRF permitted to modify the attribute	Scope
User CSG Information change in CSG cell	Defines whether to report User CSG Information change when the UE enters/leaves/accesses via a CSG cell.	Yes	TDF session
User CSG Information change in subscribed hybrid cell	Defines whether to report User CSG Information change when the UE enters/leaves/accesses via a hybrid cell in which the subscriber is a CSG member.	Yes	TDF session
User CSG Information change in un-subscribed hybrid cell (see note)	Defines whether to report User CSG Information change when the UE enters/leaves/accesses via a hybrid cell in which the subscriber is not a CSG member.	Yes	TDF session
NOTE: Due to the increased signalling load, such reporting should be applied for a limited number of subscribers only.			

The reporting of User CSG information to the OFCS shall be done on the level of detail as requested by the PCRF within TDF session related policy information and the reporting of User CSG information to the OCS shall be done on the level of detail as requested by the OCS re-authorization triggers.

NOTE: PCRF is responsible for setting the event triggers to the highest level of detail required in case different levels of User CSG information reporting to the charging domain are required for a single TDF session.

A.1.3.5 Void

A.1.4 PCC Procedures and flows

A.1.4.1 Introduction

For GPRS, the GW (PCEF) is the GGSN. The IP-CAN bearer is the PDP context and the IP-CAN Session is established by the Create PDP Context message. The IP-CAN Session is terminated when the last PDP Context of the specific IP address is deleted and the IP Address is released.

A.1.4.2 IP-CAN Session Establishment

The IP-CAN session establishment procedure (described in clause 7.2) is triggered at the GGSN by receiving a Create PDP Context Request message for the first PDP Context that is created for a new IP Address. The successful procedure results in an establishment of a UE IP Address and a PDP Context for the UE. The Create PDP Context Response message, indicating that a new PDP context is created, is sent to the SGSN. The response may include any changes in QoS according to bearer binding and policy enforcement.

During the PDP context activation procedure, it shall be possible to forward the network capability of reporting of changes in CGI/SAI/RAI to the PCRF.

The PCRF also includes the Authorized APN-AMBR in the IP-CAN Session Establishment Ack.

A.1.4.3 IP-CAN Session Termination

A.1.4.3.1 UE initiated IP-CAN Session termination

The UE initiated IP-CAN Session termination procedure (described in clause 7.3.1) is triggered at the GGSN by receiving a Delete PDP Context request message if this is the deletion of the last PDP Context for the IP Address or the Teardown Indicator in the Delete PDP Context Request indicates that all PDP contexts that share the same IP address should be deactivated. All PDP Contexts in the IP-CAN Session are deleted in the GGSN. The IP Address of the UE is released. The Delete PDP Context Response message, indicating that the PDP context(s) is deleted, is sent to the SGSN.

A.1.4.3.2 GW initiated IP-CAN Session termination

The GW initiated IP-CAN Session termination procedure (described in clause 7.3.2) is triggered if the GGSN detects that the IP-CAN Session shall be terminated. The Delete PDP Context request message is sent by the GGSN to the SGSN.

This may be the deletion of the last PDP Context for the IP Address. If not, the GGSN shall set the Teardown Indicator in the Delete PDP Context Request message to indicate that all PDP contexts that share that same IP address shall also be deactivated. All PDP Contexts in the IP-CAN Session are deleted. The IP Address of the UE is released. The Delete PDP Context Response, indicating that the PDP context(s) is deleted, is received from the SGSN.

A.1.4.4 IP-CAN Session Modification

A.1.4.4.1 IP-CAN Session Modification; GW (PCEF) initiated

The GW (PCEF) initiated IP-CAN Session modification procedure (described in clause 7.4.1) is triggered at the GGSN by receiving one of the following messages:

- Create PDP Context Request message;
- Update PDP Context Request message;
- Delete PDP Context Request message;
- a Change Notification message (indicating the new CGI, SAI or RAI) – see TS 23.060 [12].

In case of a Create PDP Context Request message, the modification of the IP-CAN Session is the addition of a new PDP Context to the IP-CAN Session. The new PDP Context is added with specific QoS requirements and traffic mapping information (TFT). A Create PDP Context Response message, indicating that a new PDP context is created, is sent to the SGSN. The response may include any changes in QoS according to bearer binding and policy enforcement.

In case of an Update PDP Context Request, a PDP Context in the IP-CAN Session is modified. The modification may include modifying the QoS and/or the traffic mapping information. The Update PDP Context Response message, indicating that a PDP context is modified, is sent to the SGSN. The response may include any changes in QoS according to bearer binding and policy enforcement.

In case of a Delete PDP Context Request message, a PDP Context in the IP-CAN Session is deleted. The Delete PDP Context Response message, indicating that a PDP context is deleted, is sent to the SGSN. .If the PS to CS handover indicator is set in a Delete PDP context request message , the PCEF reports termination of transmission resources for associated PCC Rules due to PS to CS handover.

A Change Notification message indicating a change in CGI / SAI or RAI information is received when there are only changes regarding the current location of the UE. A change in CGI / SAI or RAI may also be notified within other session management messages.

The PCRF may provide the Authorized APN-AMBR in the Acknowledgement of the IP-CAN Session Modification to the GW (in addition to the parameters in clause 7.4.1).

Based on operator policy the PCRF may re-authorize MBR/APN-AMBR.

A.1.4.4.2 IP-CAN Session Modification; PCRF initiated

The PCRF initiated IP-CAN Session modification procedure (described in clause 7.4.2) may result in a GGSN initiated PDP Context Modification or Deactivation or a Network Requested secondary PDP Context Activation.

If a PDP Context in the IP-CAN Session needs to be modified, the GGSN sends an Update PDP Context Request message. The modification may include modifying the QoS negotiated, negotiated Evolved ARP or the required CGI/SAI/RAI change reporting. The Update PDP Context Response message, indicating that a PDP context is modified, will be received from the SGSN.

If a PDP Context in the IP-CAN Session needs to be deleted, the GGSN sends a Delete PDP Context Request message. The Delete PDP Context Response message will be received from the SGSN.

If the PCEF bearer binding yields that a new PDP context is required, the PCEF shall initiate the Network Requested secondary PDP Context Activation procedure.

NOTE: If online charging is applicable, with PCEF bearer binding and a new PDP Context is required, the PCEF may not have all the information (e.g. NSAPI and negotiated QoS) associated with that PDP context for the credit authorisation until the activation procedure is complete and therefore a second credit authorisation may be necessary to provide the remaining information.

The PCRF may provide the Authorized APN-AMBR in the Policy and Charging Rule Provision to the GW (in addition to the parameters in clause 7.4.2).

A.2 Void

A.3 Void

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

A.4.0 General

For 3GPP Access (GTP-based), architecture details are described in TS 23.401 [17] and in TS 23.060 [12].

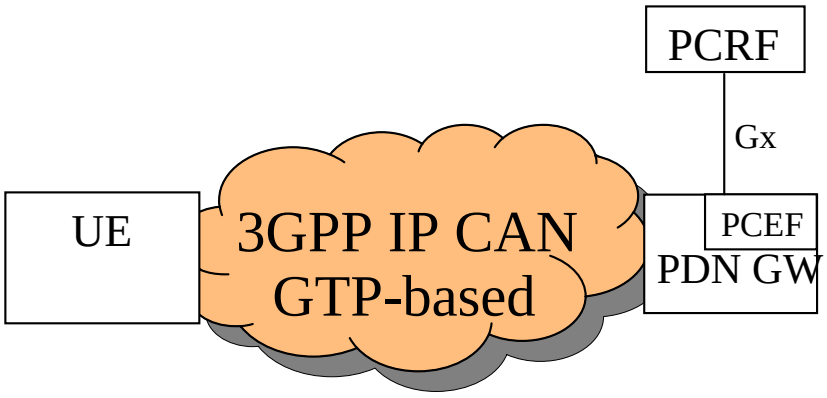

Figure A.1: The 3GPP EPS IP-CAN (GTP-based)

A.4.1 High Level Requirements

A.4.1.1 Charging related requirements

It shall be possible for the charging system to select the applicable rate based on:

- Location with the granularity as specified for the credit re-authorization trigger Location change in clause A.4.3.1.1;
- User CSG Information, including CSG ID, access mode and CSG membership indication;
- RAT type.

A.4.1.2 QoS control

For 3GPP Access (GTP based) it shall be possible to apply QoS control at APN-level.

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 QCIs 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.

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'. 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.

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.

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.

A.4.2 Architectural Model and Reference Points

A.4.2.1 Reference architecture

In the 3GPP Access (GTP-based) architecture, see TS 23.401 [17] and in TS 23.060 [12],

- the Policy and Charging Enforcement Function (PCEF) is allocated to the PDN GW;
- the Bearer Binding and Event Reporting Function (BBERF) does not apply.

A.4.3 Functional Description

A.4.3.1 Overall description

A.4.3.1.1 Credit management

For EPS the credit re-authorisation triggers in table A.4.3-1 shall apply in addition to the ones in table 6.1. They are applicable both in case of PCEF and in case of TDF.

Table A.4.3-1: EPS specific credit re-authorization triggers

Credit re-authorization trigger	Description
SGSN change	The UE has moved to a new SGSN. (Note 2)
Serving GW change	The UE has moved to a new Serving GW. (Note 1) (Note 2)
RAT type change.	The characteristics of the air interface, communicated as the radio access type, have changed.
Location change (routeing area)	The routeing area of the UE has changed. (Note 2)
Location change (tracking area)	The tracking area of the UE has changed. (Note 1)
Location change (ECGI)	The ECGI of the UE has changed.(Note 1)
Location change (CGI/SAI)	The CGI/SAI of the UE has changed.(Note 2)
Location change (eNodeB ID)	The eNodeB ID of the UE has changed. (Note 1)
Change of UE presence in Presence Reporting Area	The UE is entering/leaving a Presence Reporting Area
User CSG Information change in CSG cell	User CSG Information has changed when the UE enters/leaves/accesses via a CSG cell
User CSG Information change in subscribed hybrid cell	User CSG Information has changed when the UE enters/leaves/accesses via a hybrid cell in which the subscriber is a CSG member
User CSG Information change in un-subscribed hybrid cell (see NOTE 3)	User CSG Information has changed when the UE enters/leaves/accesses via a hybrid cell in which the subscriber is not a CSG member
NOTE 1: These triggers are used for E-UTRAN access. NOTE 2: These triggers are used for GERAN/UTRAN accesses. NOTE 3: Due to the increased signalling load, such reporting should be applied to a limited number of subscribers only.	

If the Location change trigger for GERAN/UTRAN or E-UTRAN is armed, the PDN GW should request the Serving Nodes (then SGSN or MME specifically) to report any changes in location to the level indicated by the trigger according to the procedures described in TS 23.060 [12] or TS 23.401 [17].

The OCS determines at credit management 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 OCS may subscribe to Change of UE presence in Presence Reporting Area at any time during the life time of the credit management session.

If the Change of UE Presence in Presence Reporting Area trigger is armed, the PDN GW should request the Serving Nodes (the SGSN or MME) to report any changes in the UE presence in Presence Reporting Area according to the procedures described in TS 23.060 [12] or TS 23.401 [17].

If the User CSG Information change in CSG cell trigger is armed, the PDN GW should request the Serving Nodes (then SGSN or MME specifically) to report any changes in user CSG information when the UE enters/leaves/accesses via a CSG cell.

If the User CSG Information change in subscribed hybrid cell trigger is armed, the PDN GW should request the Serving Nodes (then SGSN or MME specifically) to report any changes in user CSG information when the UE enters/leaves/accesses via a hybrid cell in which the subscriber is a CSG member.

If the User CSG Information change in un-subscribed hybrid cell trigger is armed, the PDN GW should request the Serving Nodes (then SGSN or MME specifically) to report any changes in user CSG information when the UE enters/leaves/accesses via a hybrid cell in which the subscriber is not a CSG member.

If credit re-authorization triggers, event triggers and IP-CAN session related policy information require different levels of reporting of User CSG information for a single IP-CAN session, then the User CSG information to be requested from the Serving Nodes should be changed to the highest level of detail required.

A.4.3.1.2 Event Triggers

For EPS the event triggers in table A.4.3-2 shall apply in addition to the ones in table 6.2 at the PCEF upon the request of the PCRF.

NOTE: The request from the PCRF can be triggered by configured policy, or a request received from the TDF. In case of TDF, this may be a result of credit re-authorization trigger received by the TDF from the OCS.

Table A.4.3-2: EPS specific event triggers

Event trigger	Description	Reported from	Condition for reporting
SGSN change	The UE has moved to a new SGSN. (Note 2)	PCEF	PCRF
Serving GW change	The UE has moved to a new Serving GW. (Note 1) (Note 2)	PCEF	PCRF
RAT type change.	The characteristics of the air interface, communicated as the radio access type, have changed.	PCEF	PCRF
Location change (routeing area)	The routeing area of the UE has changed.	PCEF	PCRF
Location change (tracking area)	The tracking area of the UE has changed. (Note 1)	PCEF	PCRF
Location change (ECGI)	The ECGI of the UE has changed.(Note 1)	PCEF	PCRF
Location change (CGI/SAI)	The CGI/SAI of the UE has changed.(Note 2)	PCEF	PCRF
Location change (eNodeB ID)	The eNodeB ID of the UE has changed. (Note 1)	PCEF	PCRF
Change of UE presence in Presence Reporting Area	The UE is entering/leaving a Presence Reporting Area	PCEF	PCRF
Subscribed APN-AMBR change	The subscribed APN-AMBR has changed	PCEF	Always set
EPS Subscribed QoS change	The QoS of the default EPS bearer has changed.	PCEF	Always set
User CSG Information change in CSG cell	User CSG Information has changed when the UE enters/leaves/accesses via a CSG cell. (Note 3)	PCEF	PCRF
User CSG Information change in subscribed hybrid cell	User CSG Information has changed when the UE enters/leaves/accesses via a hybrid cell in which the subscriber is a CSG member. (Note 3)	PCEF	PCRF
User CSG Information change in un-subscribed hybrid cell (see note)	User CSG Information has changed when the UE enters/leaves/accesses via a hybrid cell in which the subscriber is not a CSG member. (Note 3)	PCEF	PCRF
3GPP PS Data Off status change	The PCEF reports when the 3GPP PS Data Off status changes	PCEF	Always set
NOTE 1: These triggers are used for E-UTRAN access. NOTE 2: These triggers are used for GERAN/UTRAN accesses. NOTE 3: Due to the increased signalling load, such reporting should be applied to a limited number of subscribers only.			

If the Location change trigger is armed, the PDN GW should request the Serving Nodes (then SGSN or MME specifically) to report any changes in location to the level indicated by the trigger according to the procedures described in TS 23.060 [12] or TS 23.401 [17].

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.

If the Change of UE Presence in Presence Reporting Area trigger is armed, the PDN GW should request the Serving Nodes (SGSN or MME) to report any changes in the UE presence in Presence Reporting Area according to the procedures described in TS 23.060 [12] or TS 23.401 [17].

The User Location Report in the Access Network Information Reporting contains the ECGI and when the bearer is deactivated, information on when the UE was last known to be in that location.

If the User CSG Information change in CSG cell was provided as event trigger, the PDN GW should request the Serving Nodes to report any changes in user CSG information when the UE enters/leaves/accesses via a CSG cell.

If the User CSG Information change in subscribed hybrid cell was provided as event trigger, the PDN GW should request the Serving Nodes to report any changes in user CSG information when the UE enters/leaves/accesses via a hybrid cell in which the subscriber is a CSG member.

If the User CSG Information change in un-subscribed hybrid cell was provided as event trigger, the PDN GW should request the Serving Nodes to report any changes in user CSG information when the UE enters/leaves/accesses via a hybrid cell in which the subscriber is not a CSG member.

If credit re-authorization triggers, event triggers and IP-CAN session related policy information require different levels of reporting of User CSG information for a single IP-CAN session, then the User CSG information to be requested from the Serving Nodes should be changed to the highest level of detail required.

A.4.3.1.3 Binding mechanism

As explained in clause 6.1.1, the binding mechanism is performed in three steps: Session Binding, PCC Rule authorization and Bearer Binding.

Session Binding has no 3GPP Access (GTP-based) specifics.

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.

NOTE 1: For the authorization of PCC Rules with the same QCI the PCRF may also check that aggregated GBR is within the limits supported by the serving network to minimize the risk of rejection of the bearer by the serving network.

For the 3GPP Access (GTP-based) the Bearer Binding is performed by the PCEF. For GERAN/UTRAN in UE-only mode the Bearer Binding mechanism is restricted by the UE provided binding between a SDF and a bearer for UE initiated resource requests.

A PCEF supporting the Bind to Default Bearer PCC rule attribute shall bind a dynamic PCC rule with this attribute to the default bearer instead of using the bearer binding mechanism defined in clause 6.1.1.4 and keep the binding as long as this attribute remains set. When the PCRF removes the Bind to Default Bearer PCC rule attribute, the bearer binding mechanism as defined in clause 6.1.1.4 shall be applied by using the QoS Class Identifier and ARP values of the dynamic PCC rule. The PCEF support for the Bind to Default Bearer PCC rule attribute is optional, and shall be indicated to the PCRF.

The bearer binding mechanism associates the PCC Rule with the EPS bearer to carry the service data flow. The association shall:

- cause the downlink part of the service data flow to be directed to the EPS bearer in the association; and
- assume that the UE directs the uplink part of the service data flow to the EPS bearer in the association.

Thus, the detection of the uplink part of a service data flow shall be performed on the EPS bearer over which the downlink packets of the same service data flow is directed to.

NOTE 2: For GERAN/UTRAN in UE-only mode the detection of the uplink part of the service data flow may be active, in parallel, on any number of EPS bearers.

When the PDN GW is connected to an SGSN via Gn/Gp (and thus a handover from UTRAN/GERAN to E-UTRAN is possible), the bearer binding in the PCEF shall not combine PCC rules with different ARP values onto the same PDP context. For the UE-only mode (which is based on a UE provided binding) PCC rules with different ARP values shall not be authorized for the same PDP context.

NOTE 3: If Evolved ARP is not supported by the SGSN then this enables a modification of the EPS bearer ARP without impacting the service assignment after a handover to E-UTRAN or after relocation to a S4-SGSN or a Gn/Gp SGSN that supports Evolved ARP.

A.4.3.1.4 Policy Control

For 3GPP Access (GTP based) the policy control functionalities should include the following functionality for QoS control (in addition to the functionalities listed in clause 6.1.5):

- Authorization and enforcement of the maximum QoS that is authorized for the total bandwidth usage of non-GBR QCIs at an APN.
- Authorization and enforcement of the maximum QoS allocated to the Default EPS bearer. The Default EPS bearer shall have a non-GBR QCI as defined in clause 4.7.2.1 of TS 23.401 [17].

A.4.3.2 Functional Entities

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

The following information represents 3GPP EPS specific values of the ones listed in clause 6.2.1.1:

- Subscriber Identifier in the form of IMSI, MSISDN;
- Type of IP-CAN is set to 3GPP-EPS.

The PCEF may provide the following information (in addition to the information in clause 6.2.1.1):

- Subscribed APN-AMBR;
- Default EPS Bearer QoS.

The SPR may provide the following information for a subscriber (in addition to the 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.

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.

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.

The PCRF shall provide SDF filters in the PCC rule as received in the packet filter information from the PCEF.

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 to fail, since the PCEF cannot map the new SDFs to another bearer.

A.4.3.2.2 Policy and Charging Enforcement Function (PCEF)

In the 3GPP Access (GTP-based) architecture the PCEF enforce QoS Policies as indicated by the PCRF in accordance to what is stated in clause 6.2.2.1 with the following additions:

- Authorized APN-AMBR enforcement. The PCEF shall enforce the authorized APN-AMBR received via the Gx interface for the total bandwidth usage of non-GBR QCI for the APN.

- Authorized Default EPS Bearer QoS Enforcement. The PCEF receives the authorized QoS for the default bearer over Gx interface. The PCEF enforces it which may lead to the upgrade or downgrade of the default EPS Bearer QoS. The PCEF shall re-evaluate the bearer binding (as defined in clause 6.1.1.4) taking into account the default bearer QoS change and any PCC Rule operation requested by the PCRF.

When the PDN GW is connected via Gn/Gp (and thus handover from UTRAN/GERAN to E-UTRAN is possible), the PDN-GW shall map QoS parameters of EPS bearers and APN-AMBR (if not received via Gn/Gp) to/from Release 99 and Release 97/Release 98 QoS parameter values of PDP-contexts as specified in Annex E of TS 23.401 [17]. The PDN GW shall mediate Gn/Gp procedures so that PCRF experiences no difference compared to S5/S8 procedures.

Only the GBR per bearer is used for resource reservation (e.g. admission control in the RAN).

The MBR (per PCC rule / per bearer) and the authorized APN-AMBR are used for rate policing.

A.4.3.2.3 Application Function (AF)

The AF instructions to report loss of transmission resources will result in a notification from the PCRF that may include an indication that the transmission resources are lost due to PS to CS handover.

NOTE: The AF action up to notification of termination of transmission resources due to PS to CS handover is application specific. IMS interprets that the PS to CS handover notification as SRVCC.

A.4.3.3 Void

A.4.3.4 IP-CAN bearer and IP-CAN session related policy information

For EPS the IP-CAN bearer and IP-CAN session related policy information in table A.4.3.4-1 shall apply in addition to the ones in table 6.4 and table A.4.

A Presence Reporting Area may be defined as a short list of TAs or eNBs and/or ECGI for E-UTRAN, a short list of RAs or SAIs or CGIs for UTRAN, and a short list of RAs or CGIs for GERAN.

Table A.4.3.4-1: PCC related IP-CAN bearer and IP-CAN session related policy information

Attribute	Description	PCRF permitted to modify the attribute	Scope
Authorized default EPS bearer QoS	Defines the QCI and ARP of the default EPS bearer.	Yes	IP-CAN session
Subsequent default EPS bearer QoS (NOTE 1)	Defines the QCI and ARP of the default EPS bearer to be applied by the PCEF when the default EPS bearer QoS change time is reached.	No (NOTE 2)	IP-CAN session
Default EPS Bearer QoS change time (NOTE 1)	Defines the time at which the PCEF shall apply the subsequent default EPS bearer QoS.	No (NOTE 2)	IP-CAN session
NOTE 1: Both parameters shall be provided together. The PCRF may provide up to four instances of them. NOTE 2: The PCRF may replace all instances of Subsequent default EPS bearer QoS that have been provided previously with a new instruction. There is no operation to modify a previously provided instance of Subsequent default EPS bearer QoS and/or Default EPS Bearer QoS change time.			

The purpose of the default EPS bearer related policy information in table A.4.3.4-1 is to provide QCI and ARP that is applicable to the default bearer of an IP-CAN session. The PCRF may provide the authorized default EPS bearer QoS in every interaction with the PCEF. The PCEF shall apply the authorized default EPS bearer QoS for the IP-CAN session, including the necessary bearer binding actions.

If dynamic PCC rules are used and the PCEF has indicated that it supports the PCC rule attribute Bind to Default Bearer, the PCRF may provide a subsequent default EPS bearer QoS together with a default EPS bearer QoS change time. When the default EPS bearer QoS change time is reached, the PCEF shall apply the corresponding subsequent default EPS bearer QoS as the new authorized default EPS bearer QoS for the IP-CAN session and perform the necessary bearer binding actions for all of the respective dynamic PCC rules. To keep dynamic PCC rules bound to the default bearer, the PCRF shall include the attribute Bind to Default Bearer in every dynamic PCC rule intended to remain bound to the default bearer.

The PCRF may provide up to four instances of subsequent default EPS bearer QoS.

NOTE 1: In order to reduce the risk for signalling overload, the PCRF can spread the provisioning of subsequent default EPS bearer QoS for many UEs over time.

NOTE 2: The bearer modification is made in the same way as if the PCRF had modified the authorized default EPS bearer QoS at that point in time.

The PCEF shall discard any previously received subsequent default EPS bearer QoS instances on explicit instruction as well as whenever the PCRF provides a new instruction for one or more subsequent changes to the default EPS bearer QoS or any other subsequent parameter.

NOTE 3: In order to provide further subsequent default EPS bearer QoS 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.

NOTE 4: For services that depend on specific APN-AMBR and/or QoS for the default EPS bearer (e.g. MPS session) the PCRF is responsible to ensure that no subsequent APN-AMBR or default EPS bearer QoS interfere with the service, e.g. by removing the subsequent APN-AMBR or default EPS bearer QoS before the respective change time is reached.

A.4.3.5 TDF session related policy information

For EPS the TDF session related policy information in table A.4a shall apply in addition to the ones in table 6.4a.

A.4.4 PCC Procedures and Flows

A.4.4.1 Introduction

For the 3GPP Access (GTP-based), an IP-CAN session is established by the Create Default Bearer message. The IP-CAN session is terminated when the last EPS bearer of the IP-CAN session is disconnected.

From the network scenarios listed in clause 7.1, the Case 1 (no Gateway Control Session) applies.

A.4.4.2 IP-CAN Session Establishment

In the case of IP-CAN Session Establishment (described in clause 7.2), the PCEF provides to PCRF (in addition to the parameters described in clause 7.2): the User Location Information, Serving Network, Serving-GW address and RAT type.

The PCEF shall also forward the network capability of reporting of changes in CGI/SAI/RAI to the PCRF.

The PCRF includes, in the IP-CAN Session Establishment Ack, PCC Rules with QCI and ARP matching the Authorized Default EPS Bearer QoS, Authorized APN-AMBR and Authorized Default EPS Bearer QoS. If bearer establishment mode is UE/NW, the PCRF may also include PCC Rules requiring a QCI and ARP different from the Default Bearer QoS and for which NW mode applies.

A.4.4.3 GW (PCEF) initiated IP-CAN Session termination

The GW (PCEF) initiated IP-CAN Session termination procedure (described in clause 7.3.2) has no 3GPP specific information.

A.4.4.4 IP-CAN Session Modification

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

For IP-CAN session modification (described in clause 7.4.1) the PCEF includes the modification of any of the 3GPP specific information listed in clause A.4.4.2.

If the PS to CS handover indicator is set for an IP-CAN bearer that is deleted, the PCEF reports termination of transmission resources for associated PCC Rules due to PS to CS handover.

The PCRF may provide the following parameters in the Acknowledgement of the IP-CAN Session Modification to the PDN GW (in addition to the parameters in clause 7.4.1): Authorized APN-AMBR, Authorized Default EPS Bearer QoS.

A.4.4.4.2 IP-CAN Session Modification; PCRF initiated

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.

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.

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.

NOTE: The network configuration can ensure that at least one PCC Rule is bound to the default bearer by applying, either operator policies in the PCRF ensuring that a PCC Rule with matching QoS will be active or in the PCEF ensuring that a predefined PCC Rule not known to the PCRF is bound to the default bearer.

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

A.5.0 General

For 3GPP Access (PMIP-based), architecture details are described in TS 23.402 [18].

When PMIP-based S5/S8 has been deployed, the IP-CAN-specific parameter exchange occurs by means of IP-CAN Session Modification messages including the necessary information.

A.5.1 High Level Requirements

A.5.1.0 General

The same requirements as in clause A.4.1 apply for 3GPP Access (PMIP-based).

A.5.1.1 QoS control

For 3GPP Access (PMIP based) the same requirements as defined in clause A.4.1.2 apply.

A.5.2 Architectural Model and Reference Points

A.5.2.1 Reference architecture

In the 3GPP Access (PMIP-based) architecture, see TS 23.402 [18],

- the Policy and Charging Enforcement Function is allocated to the PDN GW;
- the Bearer Binding and Event Reporting Function (BBERF) is allocated to the Serving GW.

The Gxx applies and corresponds to the Gxc, as defined in TS 23.402 [18]. One Gateway Control Session corresponds to one IP-CAN session.

A.5.3 Functional Description

A.5.3.1 Overall Description

A.5.3.1.1 Binding mechanism

The same considerations as in clause A.4.3.1.3 apply with the following modifications:

- For the 3GPP Access (PMIP-based) the Bearer binding is performed by the BBERF.

A.5.3.1.2 Credit management

For 3GPP Access (PMIP-based EPC) the same credit re-authorisation triggers as defined in table A.4.3-1 apply.

A.5.3.1.3 Event triggers

For 3GPP Access (PMIP-based EPC) the same event triggers as defined in table A.4.3-2 apply. However, they apply at the BBERF (and not at the PCEF) upon the request from the PCRF.

NOTE: The request from the PCRF can be triggered by configured policy, a request received from the PCEF or request received from the TDF. For a PCEF or TDF based request, this may be a result of credit re-authorization trigger received by the PCEF or by the TDF from the OCS.

A.5.3.2 Functional Entities

A.5.3.2.1 Policy Control and Charging Rules Function (PCRF)

For 3GPP Access (PMIP based) the same requirements as defined in clause A.4.3.2.1 apply with the following modification:

- Default EPS Bearer QoS and Subscribed APN-AMBR are provided by the BBERF.

For 3GPP Access (PMIP based), the PCRF receives information about supported bearer establishment modes from the PCEF and provides the bearer establishment mode to be used to the PCEF, i.e. in the same way as for 3GPP Access (GTP based).

A.5.3.2.2 Policy and Charging Enforcement Function (PCEF)

For 3GPP Access (PMIP based) the same requirements as defined in clause A.4.3.2.2 apply with the following modification:

- For the 3GPP Access (PMIP-based) the enforcement of the Authorized Default EPS Bearer QoS is not performed by the PCEF.

A.5.3.2.3 Bearer Binding and Event Reporting Function (BBERF)

In the 3GPP Access (PMIP-based) the BBERF enforces QoS Policies as indicated by the PCRF in accordance to what is stated in clause 6.2.7.3 with the following additions:

- Authorized Default EPS Bearer QoS Enforcement. The BBERF receives the authorized QoS for the default bearer over Gxx interface. The BBERF enforces it which may lead to the upgrade or downgrade of the default EPS Bearer QoS. The BBERF shall re-evaluate the bearer binding (as defined in clause 6.1.1.4) taking into account the default bearer QoS change and any QoS Rule operation requested by the PCRF.

A.5.3.3 Void

A.5.3.4 Void

A.5.3.5 IP-CAN bearer and IP-CAN session related policy information

For 3GPP Access (PMIP based) the same requirements as defined in clause A.4.3.4 apply.

A.5.3.6 TDF session related policy information

For 3GPP Access (PMIP based) the same requirements as defined in clause A.4.3.5 apply.

A.5.4 PCC Procedures and Flows

A.5.4.1 Introduction

For the 3GPP Access (PMIP-based), the IP-CAN session is established by the Proxy Binding Update message to the PDN-GW. The IP-CAN session is terminated when the PMIP session is terminated.

From the network scenarios listed in clause 7.1, the Case 2b applies.

A.5.4.2 Gateway Control Session Establishment

For the Gateway Control Session Establishment Procedure (see clause 7.7.1), the Serving GW includes the following additional information in the Gateway Control Session Establishment message (in addition to the parameters described in clause 7.7.1): User Location Information, user GSG information, (if received from the MME), Serving-GW address, Serving Network, RAT Type, Default EPS Bearer QoS and if available the APN-AMBR are provided to the PCRF.

The PCRF includes, in the Acknowledge Gateway Control Session Establishment (in addition to the parameters described in clause 7.7.1): QoS Rules with QCI and ARP matching the Default EPS Bearer QoS. If the bearer establishment mode is UE/NW, the PCRF may also include QoS Rules requiring a QCI and ARP different from the Default EPS Bearer QoS and for which NW mode applies.

In support of PDP Context Activation procedures over S4, the BBERF must indicate various session parameters, e.g. the RAT type, to the PCRF.

The PCRF may provide the following parameters in the Acknowledgement of the Gateway Control Session Establishment to the Serving GW (in addition to the parameters described in clause 7.7.1): Authorized APN-AMBR, Authorized Default EPS Bearer QoS.

If the PS to CS handover indicator is set for an IP-CAN bearer that is deleted, the BBERF reports termination of transmission resources for associated QoS Rules due to PS to CS handover.

A.5.4.3 Gateway Control and QoS Rules Request

In the case of Gateway Control and QoS Rules Request (described in clause 7.7.3) the BBERF includes the addition/modification/removal of any the 3GPP specific information listed in clause A.5.4.2.

When a change of RAT without S-GW relocation occurs, the BBERF signals the RAT type change as a parameter in an event report sent from the BBERF to the PCRF. An event report is the then sent, indicating the RAT type change, from the PCRF to the PCEF.

When Secondary PDP Context Activation occurs, the S4 SGSN performs a Request Bearer Resource Allocation procedure with the Serving GW. The Serving GW supplies the parameters required by the PCEF to properly handle the allocation of resources. These parameters are sent from the BBERF (Serving GW) to the PCRF for further processing when a PMIP-based S5/S8 is deployed.

The PCRF may provide the following parameters in the Acknowledgement of the Gateway Control and QoS Rules Request to the Serving GW (in addition to the parameters described in clause 7.7.3): Authorized APN-AMBR, Authorized Default EPS Bearer QoS.

For the purpose of event reporting to the PCEF the BBERF may generate Event Reports to the PCRF if this has been requested by the PCRF.

A.5.4.4 Gateway Control and QoS Rules Provisioning

In the case of Gateway Control and QoS Rules Provisioning (described in clause 7.7.4) the PCRF may provide the following parameters (in addition to the parameters described in clause 7.7.4) to the Serving GW: Authorized APN-AMBR, Authorized Default EPS Bearer QoS.

Whenever the PCRF modifies the Authorized Default EPS Bearer QoS, the PCRF shall simultaneously modify the QCI and ARP of all QoS Rules that, according to the operator policy, shall have the same QoS as the default bearer.

A modification of the Authorized Default EPS Bearer QoS requires that at least one QoS Rule with a matching QoS can be bound to the default bearer as defined in clause 6.1.1.4.

NOTE: The network configuration can ensure that at least one QoS Rule is bound to the default bearer by applying operator policies in the PCRF ensuring that a QoS Rule with matching QoS will be active.

For the purpose of event reporting to the PCEF the PCRF may request Event Reports from the BBERF. In response to such request the BBERF shall provide the present value(s) of the event parameters.

A.5.4.5 IP-CAN Session Establishment

The PCRF may provide the following parameters in the Acknowledgement of the IP-CAN Session Establishment to the PDN GW (in addition to the parameters in clause 7.2): Authorized APN-AMBR, User Location Information, user GSG information (if received from the BBERF).

A.5.4.6 IP-CAN Session Modification

A.5.4.6.1 IP-CAN Session Modification; GW (PCEF) initiated

The PCRF may provide the following parameters in the Acknowledgement of the IP-CAN Session Modification to the PDN GW (in addition to the parameters in clause 7.4.1): Authorized APN-AMBR.

A.5.4.6.2 IP-CAN Session Modification; PCRF initiated

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, User Location Information (if received from the BBERF), user GSG information (if received from the BBERF).

A.5.4.6.3 Void

Annex B (informative): Void

Annex C (informative):
Void

Annex D (informative): Access specific aspects (Non-3GPP)

D.1 DOCSIS IP-CAN

D.1.1 General

In the DOCSIS IP-CAN, each UE is connected to the network via a Cable Modem (CM) which is connected through a Hybrid Fibre Coax (HFC) access network to a Cable Modem Termination System (CMTS). Though the UE and CM may or may not be embedded within the same physical package, they remain separate logical devices. One or more UEs may subtend a single CM. Because the CMTS provides the IP connectivity and traffic scheduling and manages quality of service for the CM and the UEs which subtend it, the CMTS fulfils the role of PCEF for the DOCSIS IP-CAN. In the DOCSIS IP-CAN, the Application Manager (AM) and the Policy Server (PS) fulfil the role of the PCRF.

When accessing resources via a DOCSIS IP-CAN, the Rx interface can be used to request resources. The communication between the AM and PS and the PS and CMTS uses the PKT-MM-2 interface which is based on COPS and defined in J.179. The remainder of this clause documents the mapping of PCC terminology to the DOCSIS IP-CAN and how the DOCSIS IP-CAN realizes the defined PCC functionality. This clause also establishes the requirements of the Rx interface as it is used for the DOCSIS IP-CAN.

The PKT-MM-2 interface is shown here for information to illustrate the organization of the DOCSIS IP-CAN. References that specify the PKT-MM-2 interface do not constitute normative requirements for the 3GPP architecture. The DOCSIS IP-CAN does not intend to pose any new normative requirements for the Gx interface.

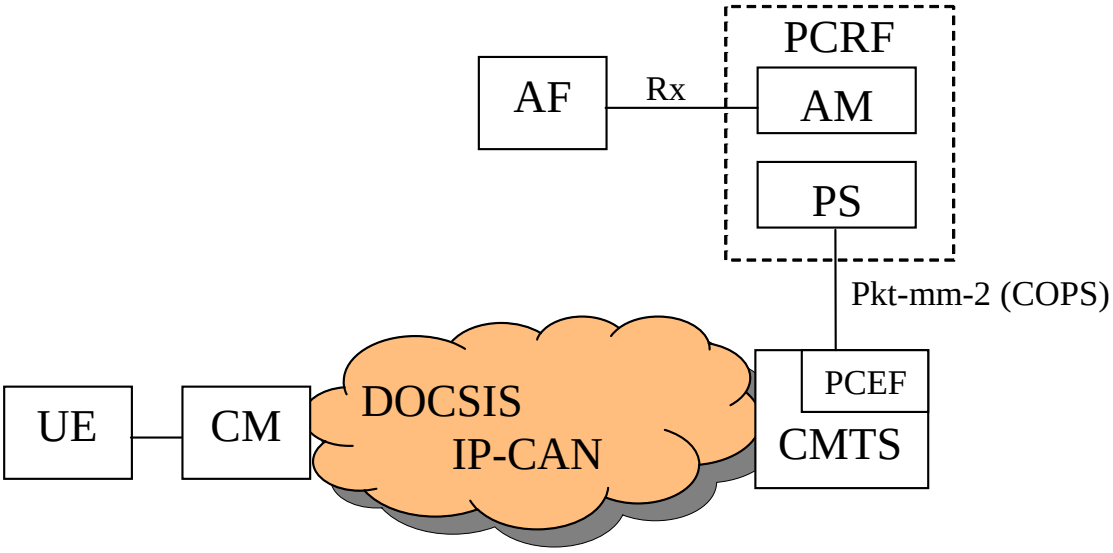

Figure D.1.1: DOCSIS IP-CAN

D.1.1 High level requirements

D.1.1.1 General

The DOCSIS IP-CAN employs for an IP-CAN session, the concept of a DOCSIS registration.

The DOCSIS IP-CAN employs for an IP-CAN bearer, the concept of a DOCSIS service flow in order to provide an information path between the UE and the CMTS. Note that DOCSIS service flows are unidirectional, either upstream (toward the CMTS) or downstream (toward the CM). When a CM is registered in the DOCSIS IP-CAN, it is assigned a unique IP Address and separate primary service flows are created for both the upstream and downstream direction These primary service flows are typically given best effort scheduling and are used to carry all IP traffic through the

CM for which a more specific service flow has not been created. When a UE is registered in the DOCSIS IP-CAN, it is assigned its own IP Address and is identified by its MAC address. A UE does not have a service flow assigned to it as a result of registration; rather it is associated with the primary service flows of the CM through which it is attached to the network. Additional bearers for the UE are created dynamically as required to provide appropriate QoS for service flows.

Bearer creation is triggered when media descriptors (Media Type and Format) for the SIP session are sent from the AF to the AM over the Rx interface. The AM translates the media descriptors into a QoS request for a DOCSIS service flow. The AM then forwards the QoS request towards the bearer enforcement point using the PKT-MM-2 interface. The PKT-MM-2 interface is not a 3GPP reference point, Specifications that detail the PKT-MM-2 interface do not impose normative requirements on the 3GPP architecture.

The following figure provides a graphical representation of the DOCSIS IP-CAN and how it maps into the generic PCC terminology.

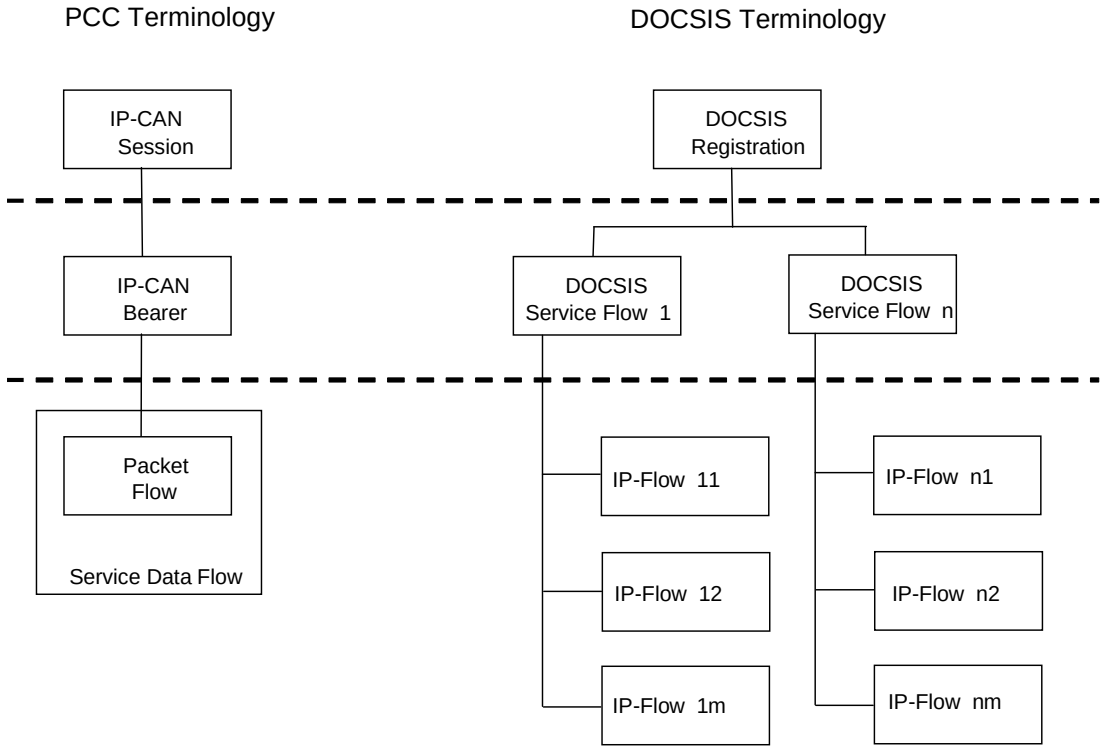

Figure D.1.2: PCC to DOCSIS terminology mapping

The DOCSIS IP-CAN defines an IP-Flow to be a unidirectional sequence of packets identified by OSI Layer 3 and Layer 4 header information. This information includes source/destination IP addresses, source/destination port numbers, protocol ID. Multiple Multimedia streams may be carried in a single IP Flow.

In a DOCSIS IP-CAN, there is no equivalent concept as a service data flow. Further a DOCSIS service flow is uni-directional and each service flow is an aggregation of the QoS needs for all the IP-Flows which make up the service flow. As such, the QoS enforcement is done at the service flow level not at the IP-Flow level.

D.1.1.2 Charging related requirements

D.1.1.3 Policy control requirements

D.1.2 Architecture model and reference points

D.1.2.1 Reference points

D.1.2.1.1 Rx reference point

D.1.2.1.2 Gx reference point

D.1.2.1.3 Void

D.1.3 Functional description

D.1.3.1 Overall description

The DOSCIS IP-CAN employs for an IP-CAN bearer, the concept of a DOCSIS service flow in order to provide an information path between the UE and the CMTS. When a Cable Modem is registered in the DOCSIS IP-CAN, primary upstream and downstream service flows are created.

When a UE is registered in the DOCSIS IP-CAN it is associated with the primary service flows of the cable modem through which it is attached to the network. Based on session information provided by the AF using the Rx reference point, the Application Manager will determine QoS requirements for each IP flow. IP flows which do not require special quality of service treatment may be carried over the primary service flows. For other IP flows which require specific QoS treatment, the Policy Server requests the CMTS to admit the flows using the pkt-mm-2 interface providing detailed information of the QoS requirements. Provided that resources are available, the CMTS will create additional bearers dynamically and push the appropriate traffic filters to the cable modem.

D.1.3.1.1 Binding mechanism

In the DOCSIS IP-CAN, the binding mechanism is achieved through the use of traffic Classifiers. These Classifiers filter traffic destined to a UE behind a Cable Modem or sourced from a UE behind a Cable Modem, to a particular DOCSIS service flow. DOCSIS Classifiers contain the following attributes which can be used to filter IP traffic:

- IP Type of Service – Range and Mask;
- IP Protocol;
- IP Source Address;
- IP Source Mask;
- IP Destination Address;
- IP Destination Mask;
- TCP/UDP Source Port Start;
- TCP/UDP Source Port End;
- TCP/UDP Destination Port Start;
- TCP/UDP Destination Port End.

The Classifier(s) which are used for a particular DOCSIS service flow are communicated to the CMTS by the Policy Server (on behalf of the Application Manager) via the pkt-mm-2 interface. The Application Manager will specify the

QoS requirements for the IP flow, the direction of the IP flow, and the Classifier(s) which are to be used for the DOCSIS service flow serving the IP flow.

When a session is no longer in use, the Application Manager communicates to the CMTS to tear down the resources associated with the session. Based on this communication, the CMTS will remove the DOCSIS service flow(s) and any Classifier(s) associated with the service flow(s), and inform the Cable Modem of the removal. Traffic which previously matched the removed Classifier(s) will now be placed on either the upstream or downstream primary DOCSIS service flow, depending on the direction of the traffic.

D.1.3.2 Functional entities

D.1.3.2.1 Policy Control and Charging Rules Function (PCRF)

In the DOCSIS IP-CAN, the Application Manager (AM) and the Policy Server (PS) fulfil the role of the PCRF.

The AM receives media descriptors (Media Type and Format) from the AF for SIP sessions and maps the QoS needs of the session to a FlowSpec, The FlowSpec is a layer 2 independent representation of the bandwidth and QoS requirements for the flow derived from the media descriptors using a well defined algorithm. The AM and PS provide network resource control in the DOCSIS IP-CAN by managing the CMTS using the PacketCable Multimedia interface pkt-mm-2.

The AM and PS map IP flows to DOCSIS service flows in accordance with the operator's policies and based on the media format information provided by the AF.

D.1.3.2.1.1 Input for PCC decisions

The AM accepts any of the following input as a basis for decisions on PCC rule operations:

- Per IP-CAN session (e.g.: UE IP address);
- Requested QoS, media format, priority indicator.

The SPR may provide the following information:

- Subscribers maximum allowed QoS resources.

Subscriber's maximum allowed bit rate for upstream and downstream.

D.1.3.2.2 Policy and Charging Enforcement Function (PCEF)

The CMTS provides PCEF equivalent functionality within the DOCSIS IP-CAN. The CMTS creates, modifies, and deletes DOCSIS service flows upon request of the Policy Server. The CMTS receives requests from the Policy Server over the pkt-mm-2 interface.

D.1.3.2.3 Application Function (AF)

D.1.3.3 Policy and charging control rule

D.1.3.3.1 General

D.1.3.3.2 Policy and charging control rule operations

D.2 WiMAX IP-CAN

In the WiMAX IP-CAN, the UE (also referenced as Mobile Station or MS in IEEE 802.16 standards) connects to the WiMAX Access Service Network (ASN). The ASN logically communicates with a Connectivity Service Network (CSN) which is a collection of core networking functions (e.g. Mobile IP HA, AAA Server, DHCP, DNS etc.). The ASN manages traffic admission and scheduling, enforces QoS for an authorized UE and performs accounting functions for the UE (per session, flow, or UE). WiMAX PCEF is part of WiMAX IP-CAN and is to be defined by WiMAX Forum [15]. WiMAX PCEF terminates the Gx reference point from the PCRF and may be a distributed enforcement architecture.

The PCC functional mapping to WiMAX IP-CAN is shown in the following figure where PCC Gx and Rx are applied.

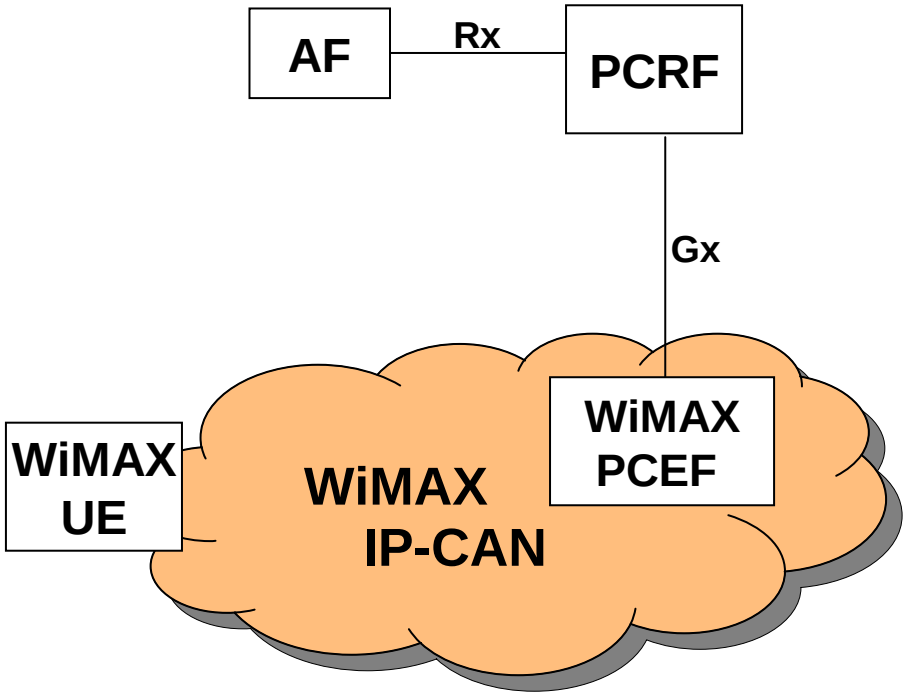

Figure D.2.1: WiMAX IP-CAN and 3GPP PCC

D.2.1 High level requirements

D.2.1.1 General

No new requirements have been identified.

D.2.1.2 Charging related requirements

No new requirements have been identified.

D.2.1.3 Policy control requirements

No new requirements have been identified.

D.2.2 Architecture model and reference points

D.2.2.1 Reference points

D.2.2.1.1 Rx reference point

WiMAX IP-CAN imposes no new requirements to the Rx reference point.

D.2.2.1.2 Gx reference point

WiMAX IP-CAN imposes no new requirements to the Gx reference point other than WiMAX specific values for existing Gx parameters (e.g. RAT type) as described in [15].

D.2.2.1.3 Sp reference point

WiMAX IP-CAN imposes no new requirements to the Sp reference point.

D.2.3 Functional description

D.2.3.1 Overall description

The WiMAX IP-CAN employs for an IP-CAN bearer, the concept of a WiMAX service flow, in order to provide a data path between the UE and the WiMAX CSN via the ASN. When a UE is registered in the WiMAX IP-CAN, it is associated with one or more WiMAX service flows. Based on session information provided by the AF via the Rx reference point, the PCRF determines the QoS requirements for each service by constructing PCC rules. The PCRF requests the WiMAX IP-CAN via Gx interface to enforce the authorized PCC rules on the WiMAX service flows. The PCEF function in the WiMAX IP-CAN enforces the PCC rules received from the PCRF. Provided that resources are available, the ASN creates and configures logical bearers and enforces creation of appropriate traffic classes associated with service flows compliant with IEEE 802.16 standards for the air interface and IP-CAN bearer capabilities in the ASN (e.g. DiffServ).

D.2.3.1.1 Binding mechanism

D.2.3.1.2 Credit management

D.2.3.1.3 Event triggers

D.2.3.2 Functional entities

D.2.3.2.1 Policy Control and Charging Rules Function (PCRF)

The 3GPP PCRF is used for the WiMAX IP-CAN. The PCRF interacts with WiMAX IP-CAN using 3GPP Gx reference point.

D.2.3.2.2 Policy and Charging Enforcement Function (PCEF)

For WiMAX IP-CAN, PCEF functions may be distributed. It additionally:

- Terminates the Gx reference point from PCRF and may act as a proxy for the PCRF.
- Handles the enforcement function relocation in WiMAX IP-CAN in a way that is transparent to the PCRF.

D.2.3.2.3 Application Function (AF)

WiMAX IP-CAN imposes no requirements to the AF functionalities.

D.2.3.3 Policy and charging control rule

D.2.3.3.1 General

D.2.3.3.1 Policy and charging control rule operations

Annex E (informative): Void

Annex F (informative):
Void

Annex G (informative): PCC rule precedence configuration

The precedence information is part of the PCC rule (see clause 6.3.1) and instructs the PCEF in which order the service data flow templates of the active PCC rules needs to be analyzed when an IP packet arrives. This mechanism ensures that the service data flows can be correctly identified even if the service data flow templates contain overlapping service data flow filters.

For PCC rules that contain an application identifier (i.e. that refer to an application detection filter), the order and the details of the detection are implementation specific. Once an application has been detected, enforcement and charging shall however be applied under consideration of the PCC rule precedence, i.e. when multiple PCC rules overlap, only the enforcement and charging actions of the PCC rule with the highest precedence shall be applied.

NOTE: This ensures that traffic described by service data flow filters can be precluded from the enforcement of application detection filter based PCC rules if this is necessary (e.g. for sponsored data connectivity).

Within the PCC framework it is possible to use different types of PCC rules for which the service data flow templates may not always be known by the PCRF. Therefore, the PCC rule precedence information needs to be carefully configured to avoid certain situations e.g. a dynamic PCC rule cannot be applied for service data flow detection due to a predefined PCC rule not known to the PCRF with overlapping filter information and a higher precedence.

For example, an operator could structure the value range of the precedence information into separate value ranges (in decreasing order) for the different types of PCC rules as follows:

- dynamic PCC rules;
- predefined PCC rules known to the PCRF;
- predefined PCC rules not known to the PCRF;
- dynamic PCC rules for non-operator controlled services, i.e. those which are generated by the PCRF based on the UE provided traffic mapping information (and which take over the UE provided precedence information).

Annex H (normative): Access specific aspects (EPC-based Non-3GPP)

H.1 General

An EPC-based non-3GPP IP-CAN (TS 23.402 [18]), which requires the Gxa for dynamic QoS control, shall include the BBERF. The allocation of a BBERF to a node within the non-3GPP IP-CAN is out of 3GPP scope, unless otherwise specified in this Annex.

H.2 EPC-based cdma2000 HRPD Access

In case of EPC-based cdma2000 HRPD access the BBERF is located in the HRPD Serving Gateway (HSGW) defined in 3GPP2 X.S0057 [20].

The HSGW of an EPC-based cdma2000 HRPD access that supports a Gxa interface shall support all the Gxa procedures defined in this specification.

NOTE 1: If the HSGW does not support the Gxa interface, the HSGW performs QoS enforcement in the HRPD access based on subscription-based QoS policies provided by the 3GPP AAA Server/Proxy during access authentication and/or static QoS policies configured in the HSGW. However, this is out of the scope of this specification.

The operator may configure an indicator in HSS which is delivered to the BBERF in HSGW within the Charging Characteristics and used by the BBERF to not establish the Gateway Control Session during the IP-CAN session establishment procedure.

NOTE 2: The decision to not establish the Gateway Control Session applies for the life time of the IP-CAN session.

NOTE 3: The indicator in the HSS is operator specific, therefore it can only be used in non-roaming cases.

During the pre-registration phase in case of optimised EUTRAN-to-HRPD handovers, the Serving GW and the HSGW are associated with the IP-CAN session(s) of the UE in the PCRF. The HSGW is the non-primary BBERF. For each PDN connection, if the UE has acquired an IPv6 prefix via the 3GPP access, the PCRF (H-PCRF in the home-routed case, V-PCRF in the local-breakout case) shall provide the IPv6 prefix of UE to the HSGW during the Gateway Control Session establishment procedure. In order to allow PCRF to link the new Gateway Control session to a Gx session based on the information received in the Gateway Control session establishment message, it is assumed that there is only a single IP-CAN session per PDN ID and IMSI.

NOTE 4: The HSGW performs QoS mapping between the QoS parameters exchanged across Gxa interface and the cdma2000 HRPD QoS parameters used within the HRPD access. However, this is out of the scope of this specification.

For EPC based cdma2000 HRPD access, the IP-CAN bearer establishment mode for all of the simultaneous IP-CAN sessions between a UE and a PDN shall have the same value.

NOTE 5: The UE is supposed to assign the same BCM value and the PCRF is supposed to keep the value assigned by the UE.

H.3 EPC-based Trusted WLAN Access with S2a

In an EPC-based trusted WLAN Access with S2a, the PCEF is located in the PDN-GW and the BBERF does not apply.

NOTE: Gxa interface is not used for S2a-PMIP in Trusted WLAN within this Release of the specification.

From the network scenarios listed in clause 7.1, the Case 1 (no Gateway Control Session) applies.

Specific event triggers applicable are listed in table H.3.

Table H.3: TWAN access specific event/credit reauthorization triggers

Event/Credit reauthorization trigger	Description	Reported from	Condition for reporting
RAT type change.	The characteristics of the air interface, communicated as the radio access type, have changed.	PCEF	PCRF/OCS

For an IP-CAN session set-up over a Trusted WLAN Access with S2a:

- at IP-CAN Session Establishment the PCEF provides TWAN location information (TWAN ID and/or UE Time Zone as described in clause 16 of TS 23.402 [18]), IP-CAN type , RAT Type, PLMN identifier and an indication that access is trusted to the PCRF (over Gx). The TWAN ID may include the identifier of the operator of the TWAN as defined in clause 16 of TS 23.402 [18]. This occurs at step 3 of Figure 7.2-1 (IP-CAN Session Establishment). This information is also provided by the PCEF to the charging entities as described in TS 32.251 [9].

- The Access Network Information Report event trigger defined in clause 6.1.4 applies. The user location information within the Access Network Information reporting contains the TWAN ID and/or UE Time Zone as described in clause 16 of TS 23.402 [18]. This information is sent when a bearer over Trusted WLAN access is activated or modified or deactivated and when the IP-CAN session is terminated. When the bearer over Trusted WLAN access is deactivated or the IP-CAN session is terminated the user location information corresponds to the last known UE location. When the IP-CAN session is terminated a TWAN Release Cause (if available) is also provided to the PCRF.

The IP-CAN type change, the PLMN change event triggers defined in clause 6.1.4 and RAT type event trigger applies. The PCEF reports to the PCRF when a Create Session Request is received including information that the UE moved to a trusted WLAN access. This information is also provided by the PCEF to the charging entities as described in TS 32.251 [9].

When the PCRF subscribes to any of the listed above event triggers using the Provision of PCC Rules procedure, the PCEF provides the parameter values in the response back to the PCRF, as defined in clause 6.1.4.

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 or at a specific point in time by providing the default EPS bearer related policy information as defined in clause A.4.3.4.

H.4 EPC-based untrusted non-3GPP Access

In an EPC-based untrusted non 3GPP Access, the BBERF does not apply.

Specific event triggers and credit reauthorization triggers are listed in table H.4.

Table H.4: Untrusted non-3GPP access specific event/credit reauthorization triggers

Event/Credit reauthorization trigger	Description	Reported from	Condition for reporting
RAT type change.	The characteristics of the air interface, communicated as the radio access type, have changed.	PCEF	PCRF/OCS

For an IP-CAN session set-up over an untrusted non-3GPP access over S2b:

- At IP-CAN Session Establishment the PCEF provides IP-CAN type, indication that it is untrusted RAT type, ePDG IP address and the Serving Network Identifier to the PCRF. This occurs at step 3 of Figure 7.2-1 (IP-CAN Session Establishment). This information is also provided by the PCEF to the charging entities as described in TS 32.251 [9]. The PCEF provides also the PCRF with User location information it may have received from the ePDG. As defined in TS 23.402 [18], this User location information may contain: ePDG IP address used in IKEv2 tunnel procedures. 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. The TWAN ID within the WLAN location Information includes the identifier of the operator of the TWAN as defined in clause 16 of TS 23.402 [18].

- The IP-CAN type changes, the PLMN change event trigger defined in clause 6.1.4 and RAT type changes event trigger applies. The PCEF reports to PCRF when a Create Session Request is received including information that the UE moved to an untrusted WLAN access. This information is also provided by the PCEF to the charging entities as described in TS 32.251 [9]. As described for the case of an IP-CAN Session Establishment, the PCEF provides also the PCRF with location information it may have received from the ePDG and the ePDG IP address used in IKEv2 tunnel procedures.

- When the PCRF subscribes to any of the listed above event triggers using the Provision of PCC Rules procedure, the PCEF provides the parameter values in the response back to the PCRF, as defined in clause 6.1.4.

- The Access Network Information Report event trigger defined in clause 6.1.4 applies. As defined in TS 23.402 [18], the user location information within the Access Network Information reporting may contain:

  - 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.

  When the Access Network Information reported by the PCRF to the AF corresponds to the local IP address used by the UE to reach the ePDG, this information cannot be considered as reliable.

  NOTE 1: This is because the UE can spoof its IP address.

- When the IP-CAN session is terminated a UWAN Release Cause (if available) is provided to the PCRF. As defined in TS 23.402 [18], the User Location Information within the Access Network Information reporting may contain:

  - 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 defined in TS 23.402 [18]

When the PCEF receives no user location information from the ePDG, it provides at least information on the Serving Network of the ePDG.

The PCRF reports the ePDG IP address used in IKEv2 tunnel procedures to the AF (i.e. P-CSCF) at the time the AF 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.

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.

NOTE 2: In order to provide more detailed information to the AF about the characteristics of the access when the RAT type is unknown, the information on whether the access is untrusted is provided.

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 or at a specific point in time by providing the default EPS bearer related policy information as defined in clause A.4.3.4.

Annex I (informative):
Void

Annex J (informative): Standardized QCI characteristics - rationale and principles

The following bullets capture design rationale and principles with respect to standardized QCI characteristics:

- A key advantage of only signalling a single scalar parameter, the QCI, as a "pointer" to standardized characteristics - as opposed to signalling separate parameters for resource type, priority, delay, and loss – is that this simplifies a node implementation.

NOTE 1: TS 23.107 [14] permits the definition of more than 1600 valid GPRS QoS profiles (without considering GBR, MBR, ARP, and Transfer Delay) and this adds unnecessary complexity.

- In general, the rate of congestion related packet drops can not be controlled precisely for Non-GBR traffic. This rate is mainly determined by the current Non-GBR traffic load, the UE's current radio channel quality, and the configuration of user plane packet processing functions (e.g. scheduling, queue management, and rate shaping). That is the reason why services using a Non-GBR QCI should be prepared to experience congestion related packet drops and/or per packet delays that may exceed a given PDB. The discarding (dropping) of packets is expected to be controlled by a queue management function, e.g. based on pre-configured dropping thresholds, and is relevant mainly for Non-GBR QCIs. The discarding (dropping) of packets of an SDF aggregate mapped to a GBR QCI should be considered to be an exception as long as the source sends at a rate smaller than or equal to the SDF aggregate's GBR. Under these exceptional conditions, when required by operator policy, the eNodeB can be configured to also use the bearer's ARP priority level to assess the relative priority of packets belonging to different SDFs in determining whether to discard a packet or not.

- An operator would choose GBR QCIs for services where the preferred user experience is "service blocking over service dropping", i.e. rather block a service request than risk degraded performance of an already admitted service request. This may be relevant in scenarios where it may not be possible to meet the demand for those services with the dimensioned capacity (e.g. on "new year's eve"). Whether a service is realized based on GBR QCIs or Non-GBR QCIs is therefore an operator policy decision that to a large extent depends on expected traffic load vs. dimensioned capacity. Assuming sufficiently dimensioned capacity any service, both Real Time (RT) and Non Real Time (NRT), can be realized based only on Non-GBR QCIs.

NOTE 2: The TCP's congestion control algorithm becomes increasingly sensitive to non congestion related packet losses (that occur in addition to congestion related packet drops) as the end-to-end bit rate increases. To fully utilise "EUTRA bit rates" TCP bulk data transfers will require a PLR of less than 10^{-6}.

Annex K (informative): Limited PCC Deployment

Limited support for policy provisioning occurs in certain deployment scenarios.

If PCC is deployed in the HPLMN but not the VPLMN, dynamic policy provisioning only occurs in the home routed roaming cases if no BBERF is employed, or in the non-roaming scenarios.

In roaming scenarios in which the PCC is deployed in the HPLMN but not the VPLMN, and a GW (BBERF) is used:

- limited policy control is possible when the UE moves from the HPLMN to the VPLMN. In the VPLMN, the UE receives only service according to static policies or according to static subscriber policies, defined outside the PCC framework delivered as described in TS 23.402 [18]; the dynamically allocated resources associated with specific EPS Bearers no longer apply after this transition.
- If a UE moves from the VPLMN to the HPLMN, dedicated resource establishment procedures are used to dynamically allocate the appropriate resources in the HPLMN for EPS bearers.
- PCC may still be employed to provision rules to the PCEF/TDF for the purpose of charging on the basis of the IP-CAN session.

When PCC is supported in the VPLMN and not in the HPLMN, dynamic policy may only be provided for the LBO case. As the VPCRF has no access to subscriber policy information from the HPLMN, only static policy will apply. The VPCRF may however interact with the AF in the VPLMN in order to determine dynamic policy operating entirely in the VPLMN. This policy will be enforced either in the PCEF or the BBERF or the TDF to be enforced entirely in the VPLMN. Bearer binding will occur under control of the VPLMN, either in the GW (BBERF) or in the GW (PCEF) (in the case of GTP-based S5/S8 for 3GPP access).

Annex L (normative): Limited PCC Deployment

In roaming scenarios in which the PCC is deployed in the HPLMN but not the VPLMN, and a GW (BBERF) is used:

- HPCRF and OCS shall detect based on local configuration according to roaming agreements that the event reporting is restricted. The OCS shall not set re/authorization triggers which would require event reporting that can not be generated.
- The H-PCRF shall inform the AF of event triggers that cannot be reported. The H-PCRF shall inform the AF of events that cannot be reported when AF registers event trigger to the H-PCRF. When the H-PCRF detects limited PCC deployment, some event triggers which are dependent upon reporting from the BBERF cannot be reported. The H-PCRF shall inform the AF of events that cannot be reported when the UE is in or after the UE has handed over to an Access Gateway where the BBERF functionality is not deployed.

Annex M (informative): Handling of UE or network responsibility for the resource management of services

For access networks supporting network initiated resource signalling, the network can take over the responsibility for the resource management for a service. This means the network triggers the request for resources when the service is started or modified and triggers the release of the resources when the service is terminated. The UE remains responsible for starting the service or reacting to an incoming service signalling and needs to decide about how to proceed with the service if the desired resources are not available.

As the network initiated resource signalling cannot always be used due to UE, access network, roaming or other restrictions, the default responsibility for the resource management for a service is given to the UE. However, the UE and the PCRF may be configured on a per service basis to make use of the network responsibility for resource management if the current access network allows this, i.e. if network initiated resource signalling is possible. The UE configuration regarding the responsibility for the resource management of a service might be updated by device management.

Regarding the PCC functionality, the main difference between the UE and the network responsibility for resource management is in the PCRF behaviour. When the UE is responsible, the PCRF waits with the authorization and installation of PCC rules until an appropriate resource request arrives. The main criteria for authorizing a PCC rule is a match of the service data flow filter information with the UE provided traffic mapping information, i.e. the UE desire to run this service on the requested resource. The QoS requested by the UE is then aligned with the authorized QoS for the PCC rules that are associated with the resource request by the PCRF.

When the network is responsible for the resource management, the PCRF authorizes PCC rules immediately, i.e. when the IP-CAN session is established and when new service information is received from the AF. The authorized PCC rules are installed afterwards.

Annex N (informative): PCC usage for sponsored data connectivity

N.1 General

With sponsored data connectivity, the Sponsor has a business relationship with the operator and the Sponsor reimburses the operator for the user's data connectivity in order to allow the user access to an associated Application Service Provider's (ASP) services. Alternatively, the user pays for the connectivity with a transaction which is separate from the subscriber's charging. It is assumed the user already has a subscription with the operator.

A possible deployment configuration for sponsored data connectivity in the non roaming case is illustrated in Figure N.1-1. In the roaming case a S9 reference point is present between the H-PCRF and the V-PCRF.

NOTE 1: Sponsored data connectivity is not supported in the roaming with visited access scenario in this Release.

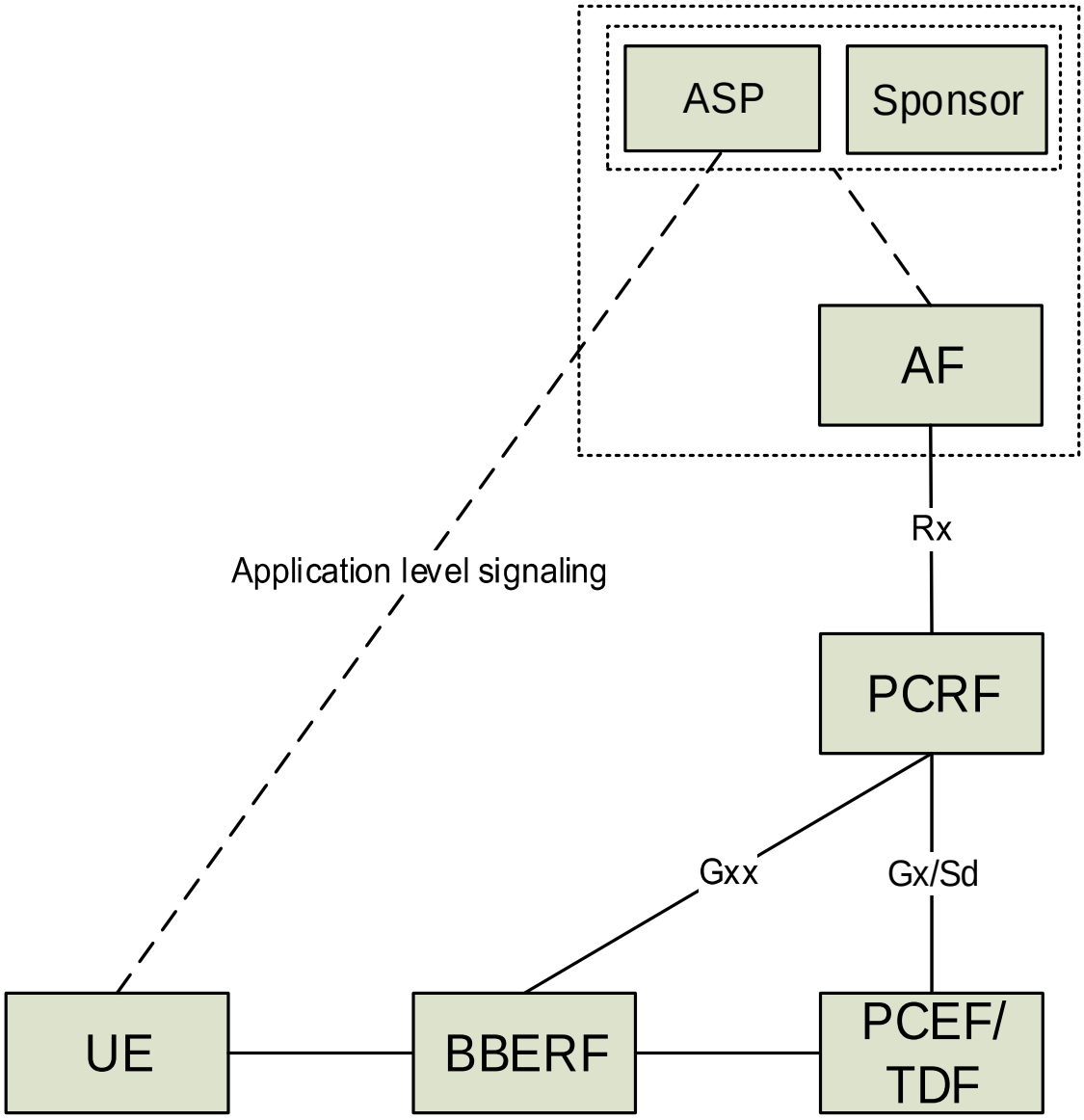

Figure N.1-1: Deployment for sponsored data connectivity

The relationship between the AF and Sponsor and between the Sponsor and ASP is out of scope of this specification. A single AF can serve multiple ASPs and multiple sponsors.

NOTE 2: An ASP can also be a sponsor.

The sponsor may choose to supply the PCRF (via the AF) with the usage thresholds that it expects the PCEF/TDF to enforce. Alternatively, the Sponsor can allow the ASP to enforce such control over the sponsored data connectivity.

The information required for the detection of sponsored HTTP traffic (i.e. server host name) can be verified with the corresponding server IP address/prefix of the IP packets by the PCEF/TDF. The PCEF/TDF uses implementation specific logic to perform this verification.

N.2 Reporting for sponsored data connectivity

There are two deployment scenarios for usage reporting for sponsored data connectivity. The Sponsor Identifier and Application Service Provider Identifier are provided for sponsored services to the PCRF from the AF over the Rx interface.

In the first scenario the PCRF assigns a service specific Charging Key for a sponsored IP flow. The Charging key is used by the PCEF/TDF to generate separate accounting records for offline charging and and/or usage data records for online charging for the sponsored flows. Correlation of accounting records and usage data records from multiple users per sponsor and/or application service provider is then performed using the charging key.

In a second scenario the Sponsor Identifier and Application Service Provider Identity is included in PCC/ADC rules from the PCRF to the PCEF/TDF as defined in clause 6.3.1. For this scenario the same Charging Key may be used both for IP flows that are sponsored and for flows that are not sponsored. Accounting records generated by the PCEF/TDF for offline charging include the Sponsor Identity and the Application Service Provider Identity. Correlation of accounting records from multiple users per sponsor and/or application service provider can then be based on Sponsor Identity and Application Service Provider Identity instead of the Charging Key. Usage reporting for online charging including Sponsor Identity and Application Service Provider Identity has not been specified in this release of the specification. PCC/ADC rules that include a Sponsor Identity and an Application Service Provider Identity should include a Charging Method that indicates offline charging.

Annex P (normative): Fixed Broadband Access Interworking with EPC

This annex specifies the enhancement to PCC framework for supporting dynamic QoS interworking with Policy Framework defined by Broadband Forum.

P.1 Definitions

UE local IP address is defined as: either the public IPv4 address and/or IPv6 address/IPv6 network prefix assigned to the UE by the BBF domain in the no-NAT case, or the public IPv4 address assigned by the BBF domain to the NATed RG that is used for this UE.

H(e)NB local IP address is defined as: either the public IPv4 address and/or IPv6 address/IPv6 network prefix assigned to the H(e)NB by the BBF domain in the no-NAT case, or the public IPv4 address assigned by the BBF domain to the NATed RG that is used for this H(e)NB.

Non-seamless WLAN offload (NSWO) is a capability of routing specific IP flows over the WLAN access without traversing the EPC as defined in clause 4.1.5 of TS 23.402 [18].

EPC-routed: User plane traffic that is routed via a PDN GW in EPC as part of a PDN Connection. EPC-routed applies to non-roaming, roaming with traffic home-routed and roaming with traffic local break-out cases.

P.2 Abbreviations

The following abbreviations are relevant for this annex only:

BBF	Broadband Forum
BPCF	Broadband Policy Control Function
NSWO	Non-Seamless WLAN offload
NSWO-APN	Non-Seamless WLAN offload APN

P.3 High Level Requirements

The same requirements as defined in clause 4 applies with the following exceptions:

- no UE initiated resource reservation procedures are supported for EPC-based Fixed Broadband Access.
- The support of traffic steering control for the traffic in the (S)Gi-LAN is only applicable to the EPC-routed traffic of Home-routed scenario.

In addition, it shall be possible to.

- perform resource reservation (e.g. admission control request to the Fixed Broadband Network) based on the bandwidth requirements and the QoS attributes of a service request for EPC-routed traffic in the Fixed Broadband network;
- provide information to identify a 3GPP UE in the Fixed Broadband Network.
- perform resource reservation (e.g. admission control request to the Fixed Broadband Network) based on the bandwidth requirements and the QoS attributes of a service request for non-seamless WLAN offloaded traffic in the Fixed Broadband network. In this case the non-seamless WLAN offloaded traffic shall be managed by PCRF as an IP-CAN session identified by one IPv4 and/or an IPv6 prefix together with UE identity information and Non-seamless WLAN offload APN. The IP-CAN session for NSWO exists as long as UE Local IP addresses/prefix is announced to the IP network and authorized by EPC. The NSWO-APN is an APN allowing the BPCF to indicate to PCRF that for subscribers of a certain HPLMN the IP-CAN session is related to NSWO traffic.

NOTE 1: The NSWO-APN is not used for the selection of a PDN GW.

NOTE 2: Dynamic provisioning from the HPLMN of NSWO-APN to BPCF is out of the scope of this Release.

NOTE 3: The naming convention of NSWO-APN is left to operator's implementation decision.

P.4 Architecture model and reference points

P.4.1 Reference points

P.4.1.1 S9a Reference point

The S9a reference point resides between:

- the PCRF in the PLMN and the BPCF in the Fixed Broadband Access Network (BPCF);
- the PCRF in the VPLMN (V PCRF) and the BPCF in the Fixed Broadband Access Network (BPCF).

The S9a reference point enables transfer of dynamic QoS control policies from the (V-)PCRF to the BPCF for the purpose of allocation of QoS resources in the Fixed Broadband Access Network for non-seamless WLAN offloaded traffic and for EPC-routed traffic.

For scenarios where the traffic is non-seamless WLAN offloaded in the Fixed Broadband Access Network, based on Rx authorizations and event subscriptions, or equivalent information, received by the BPCF from an AF in the Fixed Broadband Access Network, the S9a reference point enables the BPCF to send Rx authorizations and event subscriptions to the PCRF.

NOTE: The AF in the Fixed Broadband Access Network and the reference point between the AF in the Fixed Broadband Access Network and the BPCF are out of scope for this specification.

P.4.1.2 S15 Reference Point

The S15 reference point between the HNB GW and the PCRF and between the HNB GW and the V-PCRF. It enables the transfer of dynamic QoS control policies from the (V-)PCRF to the BPCF for the purpose of allocation of QoS resources in the Fixed Broadband Access Network for HNB CS calls.

P.4.1.3 Gxx reference point

When this reference point corresponds to the Gxb*, it transports access information for WLAN UEs such as the UE local IP address and the UDP port number. It is used scenarios in which the ePDG provides the access information via Gxb* to trigger the PCRF to initiate the S9a session i.e. S2b-PMIP and untrusted S2c.

For the case of H(e)NB with S5/S8 PMIP, this reference point corresponds to Gxc and the requirements in clause 5.2.7 applies. In addition for the purpose of fixed broadband access interworking, Gxc transports the H(e)NB Local IP address and the UDP source port, if available, in the fixed broadband access network where the H(e)NB connects to.

P.4.1.4 S9 reference point

In addition to the specification of the S9 reference point defined in clause 5.2.6, this reference point is used to trigger the V-PCRF to initiate the Gateway Control Session establishment over S9a. The S9 interface is enhanced to carry from the H-PCRF to the V-PCRF the UE local IP address, the UDP port number, if available, the H(e)NB local IP address and UDP port, if available, and the ePDG IP address (for S2b and untrusted S2c access) or the PDN GW IP address (for trusted S2c access), if available.

P.4.1.5 Gx reference point

In addition to the specification of the Gx reference point defined in clause 5.2.2, this reference point is enhanced as described in the following. The IP-CAN establishment/modification request message, send from PCEF to PCRF, should include:

- the UE local IP address and the UDP port number, if available, when WLAN access and GTP is used.
- the UE local IP address and the UDP port number, if available, when trusted S2c is used.
- the H(e)NB local IP address and the UDP port number, if available, when UE accesses from H(e)NB and GTP S5/S8 is used.

P.4.2 Reference architecture

P.4.2.0 General

The reference architecture described in clause 5.1 is:

- extended to include S9a reference point to support fixed broadband access interworking to EPC for the following scenarios:
  - S9a reference point between PCRF and BPCF in the non-roaming case for traffic that is routed via EPC and for traffic that is non-seamless WLAN offloaded in the fixed broadband access network; and
  - S9a reference point between the V-PCRF and BPCF for roaming cases with visited access and home routed for traffic that is routed via EPC; and for traffic that is non-seamless WLAN offloaded in the fixed broadband access network;
- extended to include the S15 reference point as defined in clause P.4.1.2;
- PCEF resides in the PDN GW;
- for WLAN access: BBERF resides in the ePDG. The BBERF only applies for cases 2b (i.e. S2b-PMIP, S2c-untrusted);
- for H(e)NB access with S5/S8 PMIP: BBERF resides in the Serving GW.

The UE may or may not be behind a NAT. The NAT may reside in the BBF access network or in the customer premises network. Policy interworking via S9a for non-seamless WLAN offloaded traffic in this release is supported for scenarios without NAT in the BBF domain.

P.4.2.1 Reference architecture – Non-Roaming

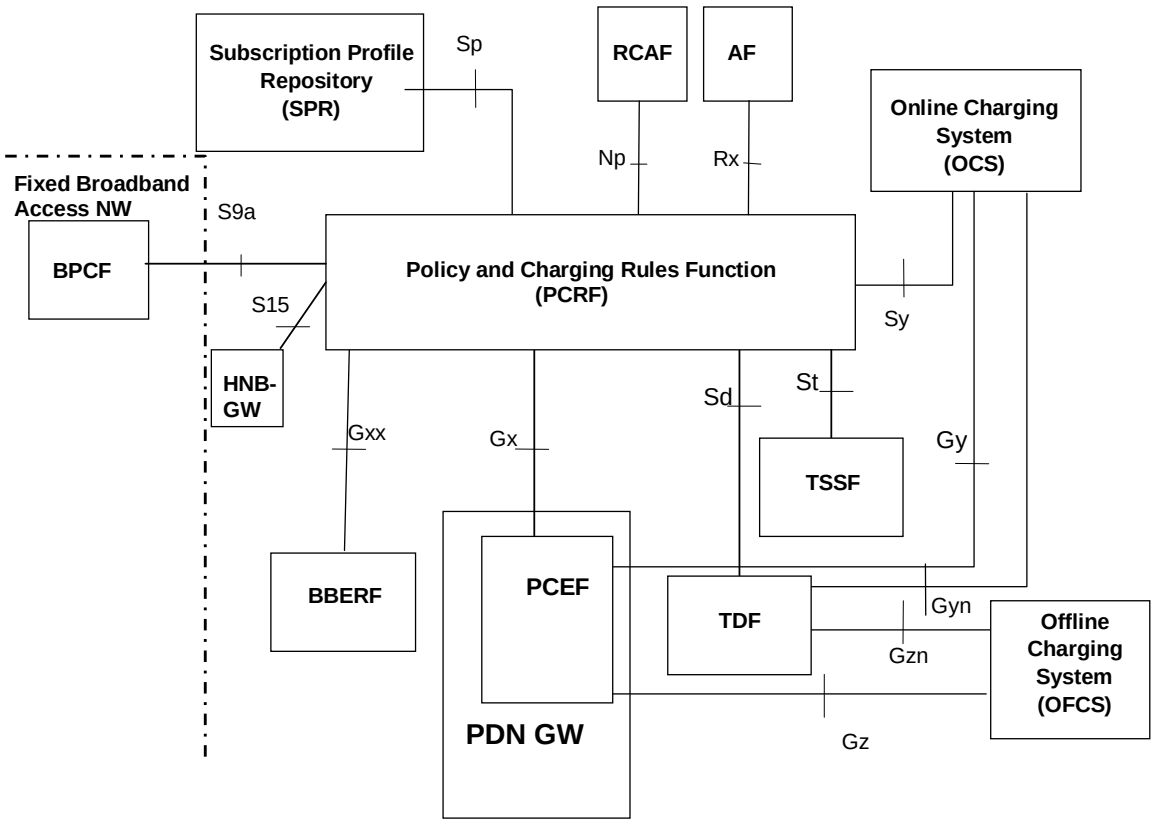

Figure P.4.2.1-1: PCC Reference architecture for Fixed Broadband Access Interworking

P.4.2.2 Reference architecture – Home Routed

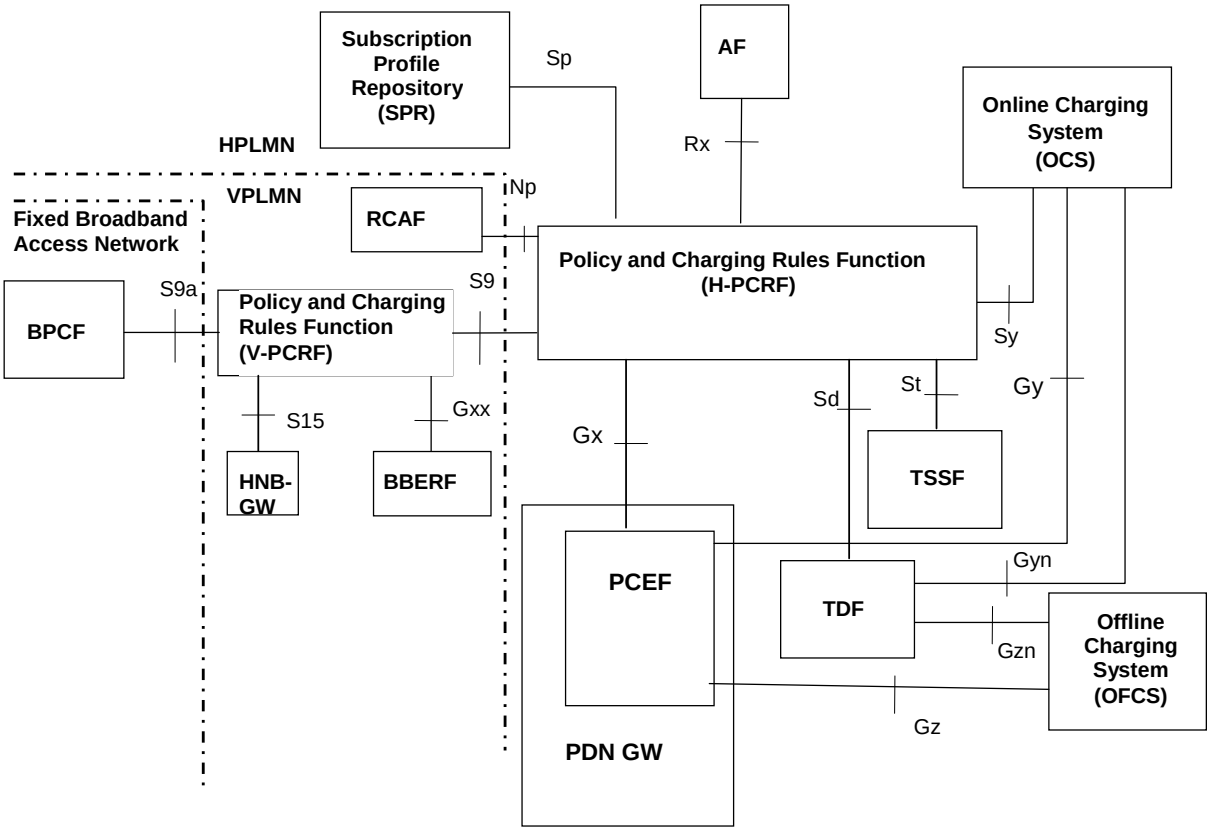

Figure P.4.2.2-1: PCC Reference architecture for Fixed Broadband Access Interworking (home routed)

P.4.2.3 Reference architecture – Visited Access

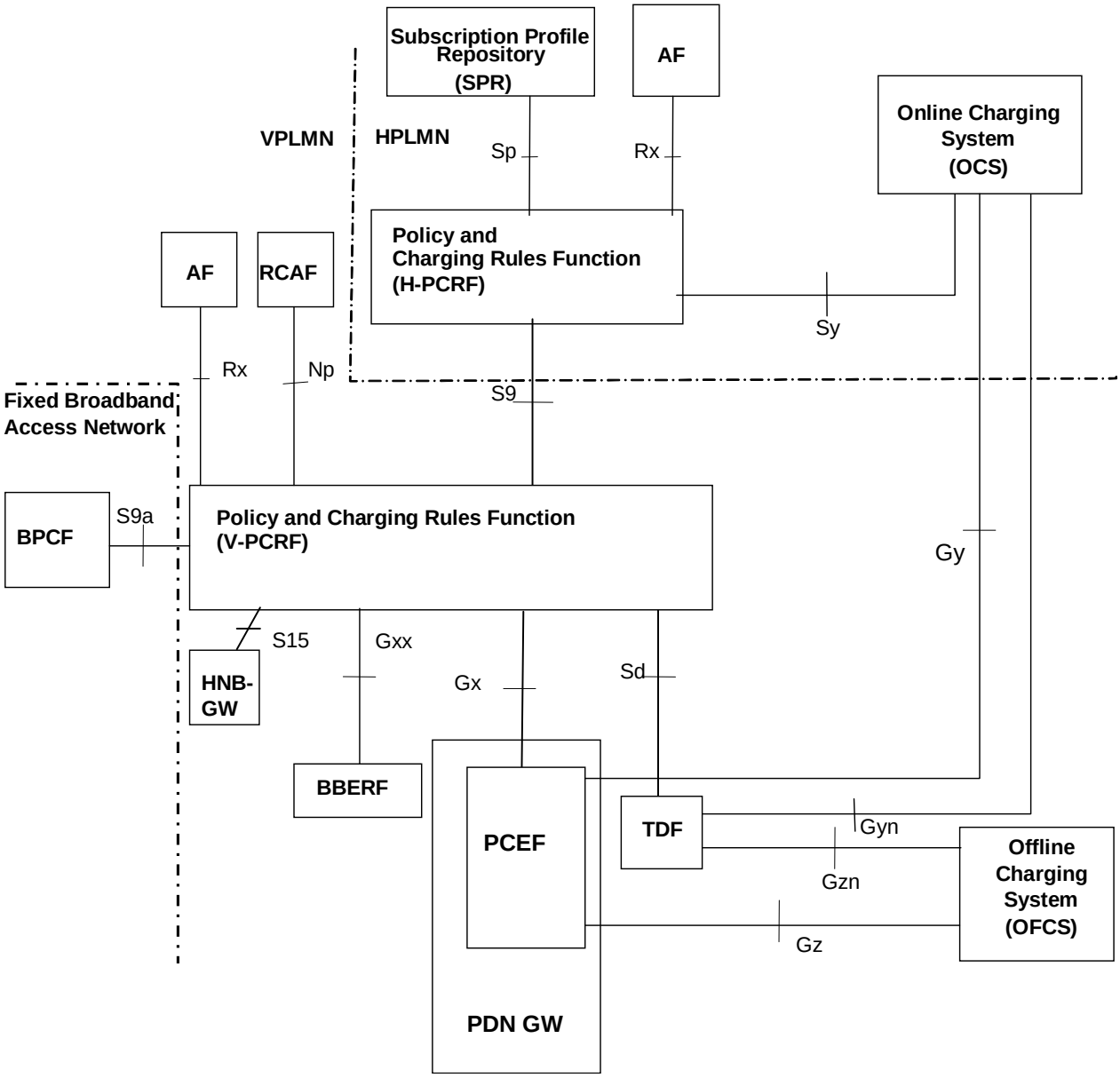

Figure P.4.2.3-1: PCC Reference architecture for Fixed Broadband Access Interworking (visited access)

P.4.2.4 Reference architecture - Non-Roaming with non-seamless WLAN offload in Fixed Broadband Access Network; scenario with AF

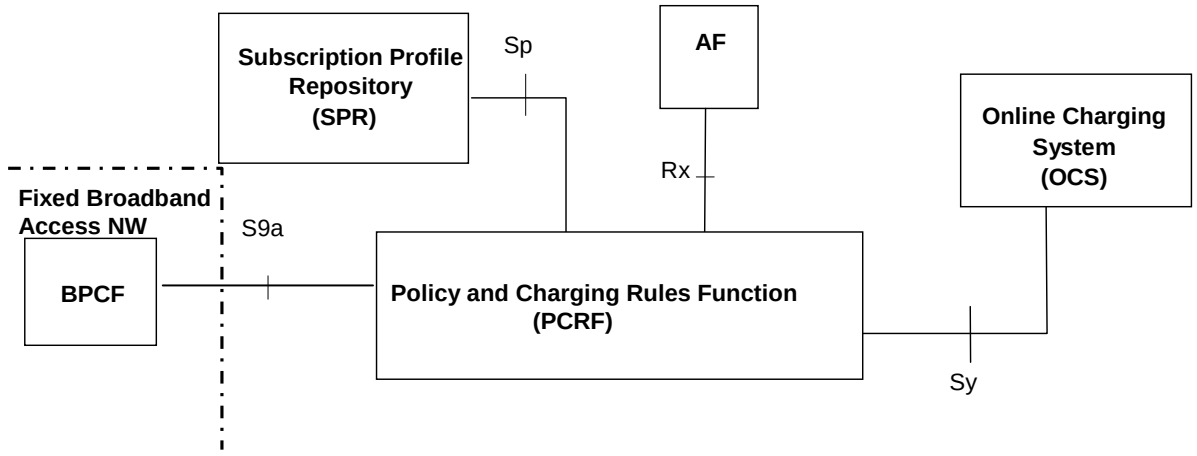

Figure P.4.2.4-1: PCC Reference architecture for Fixed Broadband Access Interworking (non-roaming with non-seamless WLAN offload in Fixed Broadband Access Network)

NOTE 1: The architecture also supports scenarios where there is an Application Function in the Fixed Broadband Access Network. The AF in the Fixed Broadband Access Network and the reference point between the AF in the Fixed Broadband Access Network and the BPCF are out of scope for this specification.

NOTE 2: The AF in this architecture is used with traffic that is non-seamless WLAN offloaded in the Fixed Broadband Access Network.

P.4.2.5 Reference architecture - Roaming with non-seamless WLAN offload in Fixed Broadband Access Network: scenario with AF

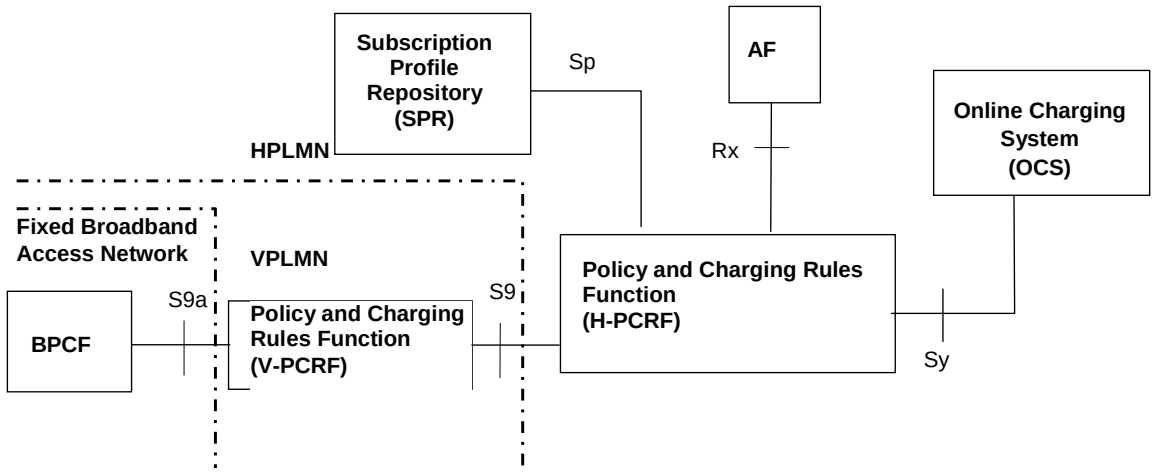

Figure P.4.2.5-1: PCC Reference architecture for Fixed Broadband Access Interworking (roaming with non-seamless WLAN offload in Fixed Broadband Access Network)

NOTE 1: The architecture also supports scenarios where there is an Application Function in the Fixed Broadband Access Network. The AF in the Fixed Broadband Access Network and the reference point between the AF in the Fixed Broadband Access Network and the BPCF are out of scope for this specification.

NOTE 2: The AF in this architecture is used with traffic that is non-seamless WLAN offloaded in the Fixed Broadband Access Network.

P.4.2.6 Reference architecture - Non-Roaming with non-seamless WLAN offload in Fixed Broadband Access Network: scenario with TDF

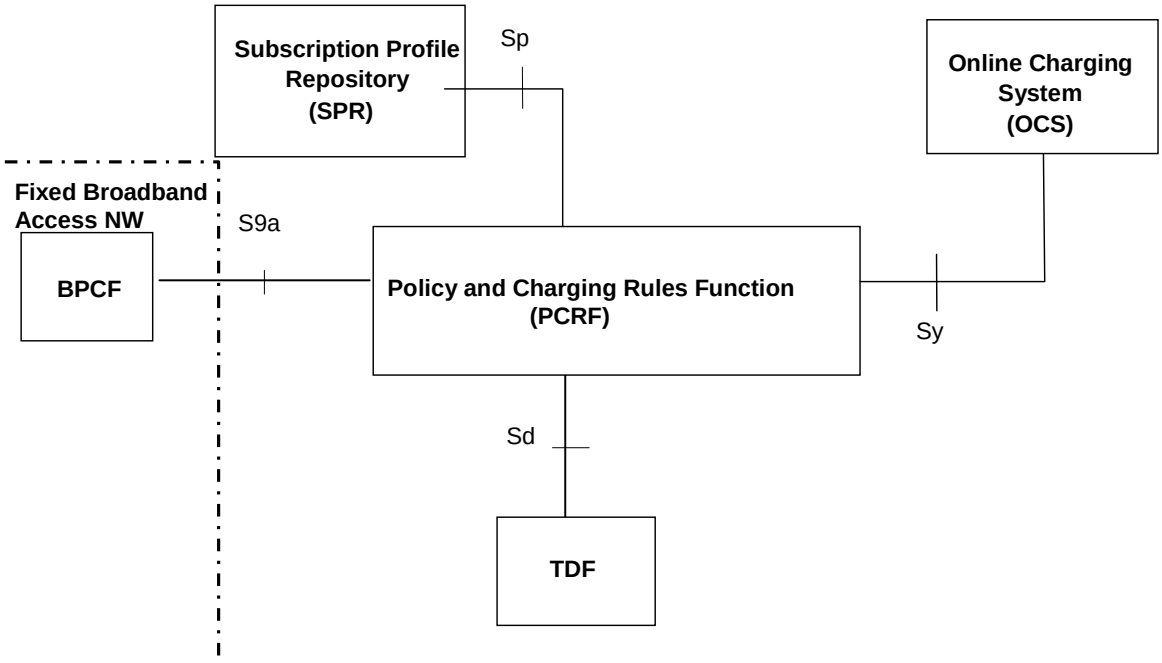

Figure P.4.2.6-1: PCC Reference architecture for Fixed Broadband Access Interworking (non-roaming with non-seamless WLAN offload in Fixed Broadband Access Network)

NOTE 1: The TDF in this architecture is used with traffic that is non-seamless WLAN offloaded in the Fixed Broadband Access Network.

NOTE 2: Sd is an intra-operator interface. Scenarios where non-seamless WLAN offloaded traffic is routed via the TDF are therefore limited to the case where the Fixed Broadband Access Network and the PLMN are owned by the same operator.

P.4.2.7 Reference architecture - Roaming with non-seamless WLAN offload in Fixed Broadband Access Network: scenario with TDF

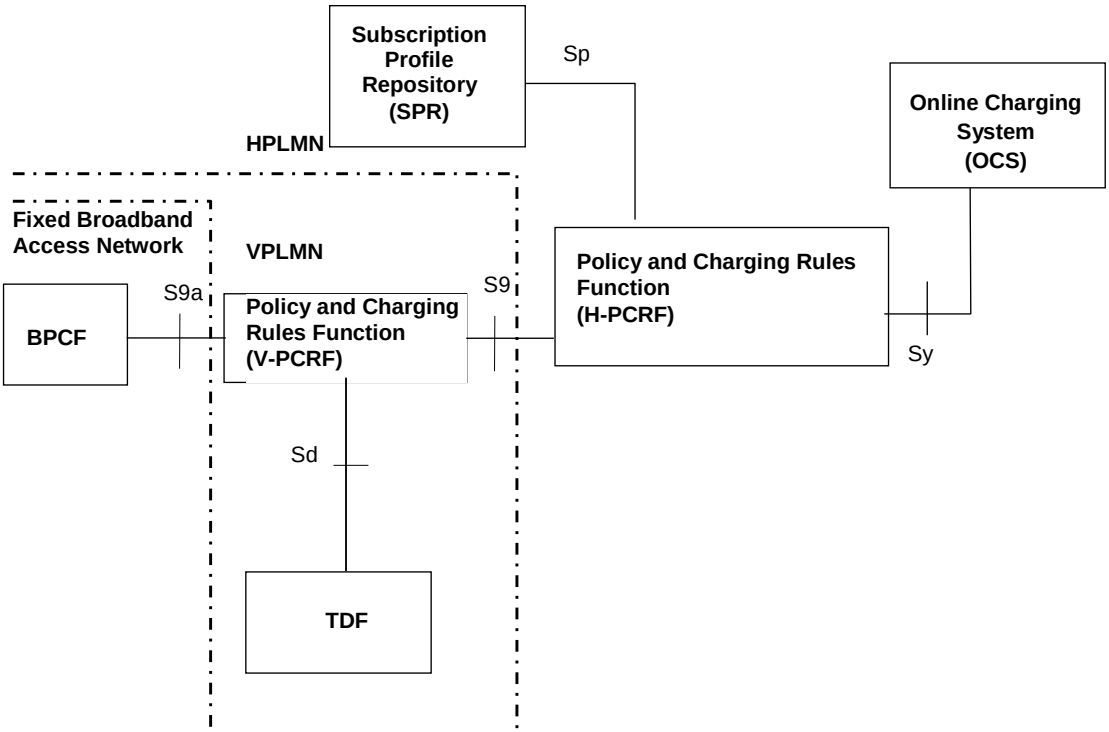

Figure P.4.2.7-1: PCC Reference architecture for Fixed Broadband Access Interworking (roaming with non-seamless WLAN offload in Fixed Broadband Access Network)

NOTE 1: The TDF in this architecture is used with traffic that is non-seamless WLAN offloaded in the Fixed Broadband Access Network.

NOTE 2: Sd is an intra-operator interface. Scenarios where non-seamless WLAN offloaded traffic is routed via the TDF are therefore limited to the case where the Fixed Broadband Access Network and the VPLMN are owned by the same operator.

P.5 Functional description

P.5.1 Overall description

For EPC based Fixed Broadband Access Interworking with EPC-routed traffic the credit management, reporting, usage monitoring, termination actions, service data flow prioritization and standardized QoS characteristics as defined in clause 6.1 shall apply.

For non-seamless WLAN offloaded traffic service data flow prioritization as defined in clause 6.1 applies. For scenario with TDF, usage monitoring as defined in clause 6.1 applies. For NSWO traffic in other scenarios, without TDF, usage monitoring is out of scope of this specification. For all scenarios, credit management, termination actions and reporting for NSWO traffic are out of scope of this specification.

The purpose of policy interworking via S9a for non-seamless WLAN offloaded traffic (PCC Rules provisioned for the UE local IP address) is to enable policy control in the BBF domain in two different ways:

- Gate enforcement. The BPCF is expected to provide information over R interface to control whether a service data flow, which is subject to policy control, pass through the BNG if and only if the corresponding gate is open.

- QoS enforcement: The BPCF is expected to provide information over R interface to control the authorized QoS of a service data flow according to the QoS information received over S9a interface.

The complete specification of the BPCF is defined in BBF TR-134 [31] and BBF TR-203 [30] and BBF TR-291 [33] and it is out of the scope of 3GPP.

The information contained in a PCC Rule generated by the PCRF for NSWO traffic includes Service Data Flow Detection and Policy Control information elements specified in table 6.3. The PCC rules for NSWO traffic do not include the Charging and Usage Monitoring Control elements specified in table 6.3.

For Fixed Broadband Access the event triggers in table P.5.1-1 shall apply in addition to the ones in table 6.2.

Table P.5.1-1: Fixed Broadband specific event triggers

Event trigger	Description	Reported from	Conditions for reporting
UE local IP address change	Either the UE local IP address or the UDP port number or both assigned by Fixed Broadband Access have changed	PCEF, BBERF	Always set
H(e)NB local IP address change	Either the H(e)NB IP address or the UDP port number or both assigned by Fixed Broadband Access have changed	PCEF, BBERF	PCRF

P.5.1.1 Binding Mechanism

P.5.1.1.1 EPC-routed traffic

For EPC routed traffic, binding mechanisms apply as defined in clause 6.1.1 by PCRF, PCEF and BBERF. In addition, the PCC and QoS Rule generation is performed by PCRF as specified in clause 6.1.1, in addition when:

- Both a Gx and associated Gateway Control Session exist for the same IP-CAN session; the PCRF shall generate QoS Rules for all the authorized PCC rules in this step.

P.5.1.1.2 Non-seamless WLAN offloaded traffic

The binding mechanism includes two steps for the non-seamless WLAN offloaded traffic:

1. Session binding.
2. PCC rule authorization.

For NSWO traffic, session binding of AF session and TDF session (in unsolicited mode) to an IP-CAN session is performed by the PCRF, as defined in clause 6.1.1, for the purpose of policy control in the BBF domain.

The PCRF derives and authorises PCC rules as described in clause 6.1.1.

P.5.1.2 S9a, Gx and S15 Session Linking

For WLAN, PCRF and BPCF both need to support session linking function. Depending on the deployment there may be one or multiple PCRF that have a Gateway Control Session on S9a for a given UE. The PCRF shall be able to perform the linking between IP-CAN sessions on Gx and the Gateway Control Session on S9a for the same UE based on IMSI and UE local IP address.

For H(e)NB scenarios a Gateway Control Session on S9a may be linked to:

- IP-CAN Sessions on Gx for all UEs connected to the H(e)NB;
- Gateway Control Sessions on S9 and/or IP-CAN Sessions on S9 (in roaming cases);
- S15 Session;

NOTE 1: There is a single S15 session per HNB for CS calls for all UEs connected to the HNB in order to improve performance. In addition, for CS calls there are no UE specific policies and therefore a single PCRF can handle CS calls for all UEs.

When the Gateway Control Session on S9a is initiated by PCRF, BPCF is expected to associate the session on R with the Gateway Control Session on S9a.

NOTE 2: How the BPCF performs the association of a Gateway Control Session on S9a and R session is out of the scope of 3GPP.

P.6 Functional Entities

P.6.1 Policy Control and Charging Rules Function (PCRF)

P.6.1.1 General

The PCRF functionality defined in clause 6.2.1.0 shall apply. In addition, to support interworking with Fixed Broadband networks, the PCRF shall:

- Send the QoS rules to the BPCF over S9a to request admission control in the fixed access.
- Send to the BPCF the UE local IP address and UDP port number for the WLAN scenario to allow the Fixed Broadband Access to identify UE traffic.
- Send to the BPCF the HeNB Local IP address and UDP port number for the Femto scenario. This allows the Fixed Broadband Access to identify IP flows corresponding to the IPSec tunnel from the HeNB GW to the SeGW which transports H(e)NB UE traffic.
- Be able to be configured with the relation of IP address ranges to Fixed Broadband Access, to allow BPCF discovery.
- Be able to receive from PDN GW the H(e)NB Local IP address and the UDP source port, if available, in the Fixed Broadband access network at which the H(e)NB is connected.
- Be able to receive the UE local IP address and UDP source port from the ePDG (case 2a and case 2b) and PDN GW (case 1).
- Be able to receive the HNB local IP address and UDP source port from HNB GW (case 1) for the HNB CS scenario.

When PCRF receives the IP-CAN session establishment indication for a PDN connection initiated for a UE connected via Fixed network access, the PCRF determines if a Gateway control session is already present for this IP-CAN session. If Gateway control session is not already established, the PCRF shall trigger Gateway control session establishment procedure from the BPCF.

When the UE is connecting via Fixed Broadband access network, no QoS Rules should be sent to the ePDG. The PCRF identifies when the UE is connecting via Fixed Broadband access network from the IP-CAN type.

For the purpose of the policy control in the Fixed Broadband Access network for the non-seamless WLAN offloaded traffic, the PCRF shall:

- Handle incoming request of IP-CAN session establishment received over S9a.
- Perform session binding of the AF session information received via Rx or via S9a with an existing IP-CAN session using the UE local IP address and the IMSI (if available).
- Initiate IP-CAN Session Modification and also QoS information provision for Non-seamless WLAN offloaded traffic.
- Establish an Sd session with the TDF when an indication of IP-CAN session establishment is received over S9a for the UE local IP address in case of architecture variant C the solicited mode.

P.6.1.2 V-PCRF

The V-PCRF functionality defined in clause 6.2.1.3 shall apply. For the purpose of Fixed Access interworking the V-PCRF functionalities for EPC routed traffic, the following are applicable:

- If a BPCF-Initiated Gateway Control Session termination is received over S9a, then the V-PCRF shall terminate a Gateway Control session over S9 with the H-PCRF.

- For home routed roaming case, in case 1:

  - If a Gateway Control Session termination indication is received over S9 from the H-PCRF, then the V-PCRF shall trigger a Gateway Control Session termination to the BPCF.

  - If a Gateway Control and QoS Rules Request is received over S9 from the H-PCRF, then the V-PCRF shall trigger a Gateway Control and QoS Rules Request to the BPCF.

- For both home routed and visited access roaming cases, in case 2b:

  - If a Gateway Control Session establishment from the BBERF (ePDG) occurs, then the V-PCRF shall establish a Gateway Control Session with the BPCF over S9a and with the H-PCRF over S9.

  - If the last Gateway Control Session from the BBERF (ePDG) is terminated, then the V-PCRF shall terminate the Gateway Control Session with the BPCF over S9a and with the H-PCRF over S9.

- When the last PDN connection over the HNB has been terminated the V-PCRF initiates the GW Control Session Termination to the BPCF if there is no S15 session bound to the Gateway control session over S9a interface session. Otherwise, if there is a S15 session bound to the Gateway control session over S9a interface session the V-PCRF initiates the GW Control QoS rule Provision procedure to the BPCF to release the resources in the fixed broadband network.

When the V-PCRF receives the Gateway Control Session establishment indication for a PDN connection initiated for a UE connected via Fixed network access, the V-PCRF determines if a Gateway Control Session is already present for this IP-CAN session. If a Gateway Control Session is not already established, the V-PCRF shall trigger a Gateway Control Session establishment procedure from the BPCF.

For the purpose of BBF interworking for NSWO traffic, the V-PCRF functionalities described in the following are applicable:

- For roaming scenario, V-PCRF shall handle incoming request of IP-CAN session establishment received over S9a.

- If an IP-CAN session establishment request is received for a roaming user over the S9a reference point, then the V PCRF shall conclude that the IP-CAN session is used for NSWO and acts as visited access network as described in clause 6.2.1.3.3.

P.6.1.3 H-PCRF

The H-PCRF functionality defined in clause 6.2.1.4 shall apply. For the purpose of Fixed Access interworking, the H-PCRF functionalities defined in the following are applicable to the home routed scenario:

- For case 1, if an IP-CAN Session Establishment indication is received over Gx, then if this is the first IP-CAN session for this UE the H-PCRF shall establish a Gateway Control Session to the V-PCRF over S9.

- For case 1, if an IP-CAN Session Termination indication is received over Gx then if this is the last IP-CAN session for this UE, the H-PCRF shall terminate the Gateway Control session to the V-PCRF over S9.

- If a PCC Rule is generated, the H-PCRF shall send QoS rules to the V-PCRF to request admission control over S9.

- If a PCEF-Initiated IP-CAN Session Modification Procedure occurs over Gx to update, for WLAN scenario, the UE local IP Address and UDP port number, or, for the HeNB scenario, the HeNB local IP Address and UDP port number, then the H-PCRF shall send them to the V-PCRF.

- For the purpose of BBF interworking for NSWO traffic, in case of roaming, the H-PCRF shall determine PCC rules based on home operator policy for the specific UE when it receives the IP-CAN session establishment request from V-PCRF.

P.6.2 Broadband Policy Control Function (BPCF)

The BPCF is the policy Control entity in the Fixed Broadband Access network. The complete specification of the BPCF is defined in BBF TR-134 [31] and BBF TR-203 [30] and it is out of the scope of the 3GPP.

For the purpose of interworking with 3GPP network the BPCF is expected to:

- Perform admission control in fixed access or delegates admission control decision to other BBF nodes. Based on the admission control, the BPCF accepts or rejects the request received from PCRF over S9a. As with current S9, the BPCF may include the acceptable QoS in the reply if the request is rejected.
- Translate the 3GPP QoS rule as received from PCRF over S9a interface into access specific QoS parameters applicable in the Fixed Broadband access network.
- Support PCRF-triggered Gateway Control session establishment procedure over S9a.
- Support Gateway Control session modification and termination procedures over S9a.

The functionality of the BPCF in a roaming scenario is the same as in a non-roaming scenario.

For the purpose of the policy control in the BBF domain for the Non-Seamless WLAN offloaded, the BPCF shall:

- Support BPCF-initiated IP-CAN Session Establishment procedure over S9a only after successfully checking the local policies indicating that policy control for NSWO is provided.
- Support IP-CAN Session Modification procedure over S9a.
- Support IP-CAN Session Termination procedure over S9a.
- Bind the request received on E/G from AF in the Fixed Broadband access network with an existing IP-CAN session on S9a using the UE local IP address and the IMSI (if available).

P.6.3 Bearer Binding and Event Reporting Function (BBERF)

For case 2a and case 2b, the BBERF in the ePDG supports only reporting of the UE's Local IP address and UDP port number to the PCRF. Bearer binding, uplink bearer binding verification functions are not supported.

For case 2b, the BBERF in the Serving GW supports those functions specified in clause 6.2.7.1

NOTE: The IP-CAN-specific parameters provided by BBERF in Serving GW to PCRF includes the H(e)NB's Local IP address and UDP port number.

P.6.4 Policy and Charging Enforcement Function (PCEF)

PCEF supports those functions specified in clause 6.2.2.1. Case 1 additionally supports the reporting of the UE / H(e)NB Local IP address and the UDP port number, if available, in the Fixed Broadband Access at which the H(e)NB is connected to the PCRF.

P.7 PCC Procedures and Flows

P.7.1 Introduction

From the network scenarios listed in clause 7.1, the Case 1 (no Gateway Control Session over Gxx interface) applies for Fixed Broadband Access for S2a-GTP, S2b-GTP, trusted S2c and H(e)NB scenarios, the Case 2b (a Gateway Control Session over Gxx interface per IP-CAN Session) applies for S2b-PMIP and case 2a (the same Gateway Control Session over Gxx interface for all IP-CAN Sessions) applies for untrusted S2c.

In all information flows, the ePDG is present only in untrusted scenario case 2a and case 2b.

NOTE: No policy interworking solution based on S9a is defined for Fixed Broadband access interworking via S2a within this release of the specification.

P.7.2 IP-CAN Session Establishment

P.7.2.0 General

This procedure is applicable for WLAN and H(e)NB scenarios for EPC routed traffic and for NSWO traffic. This procedure is the same as described in clause 7.2 with the exceptions described in this clause.

NOTE 1: When PCRF receives the IP-CAN session establishment indication over Gx interface, PCRF determines if a Gateway Control session is already present for this IP-CAN session. If a Gateway Control session is not already established, the PCRF shall trigger a Gateway Control session establishment procedure from the BPCF.

P.7.2.1 IP-CAN Session Establishment

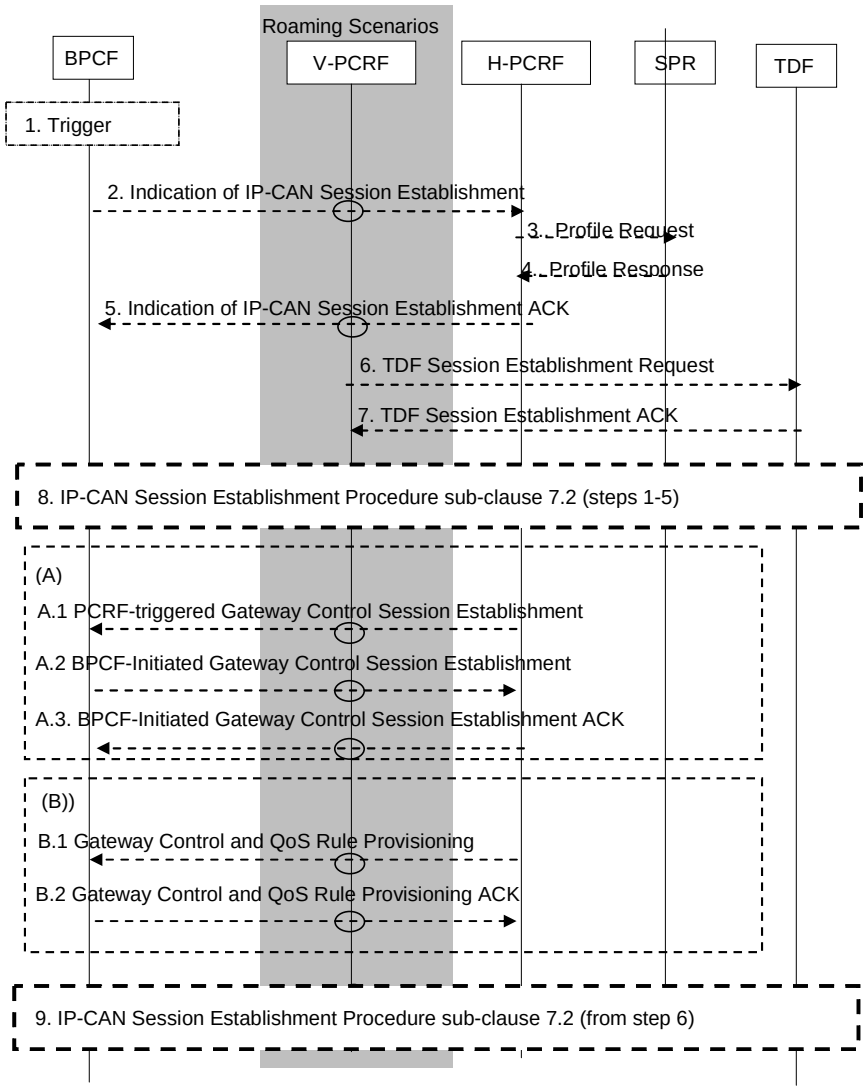

Figure P.7.2.1: IP-CAN Session Establishment for both EPC routed and NSWO traffic

This procedure is the same as described in clause 7.2 with the additions described below:

1. The BBF access network may become aware of the IMSI of the 3GPP UE if 3GPP-based access authentication (EAP-AKA/AKA') is performed. The BPCF also becomes aware of the UE local IP address.

The steps from 2 to 7 show PCC signalling to provision PCC rules and ADC rules for NSWO traffic.

2. The BPCF Initiates a IP-CAN session establishment over S9a to the PCRF for non-roaming and to the V-PCRF for roaming cases, the information contained in the request message includes IMSI, IP-CAN type, local UE IP address and the NSWO-APN. Triggered by the IP-CAN session establishment over S9 the V-PCRF triggers the S9 session establishment to the H-PCRF.

3-4. The PCRF retrieves user profile from SPR as described in clause 7.2. As part of the user profile, the PCRF may receive an indication on whether policy control for NSWO traffic should be performed for that UE.

5. The PCRF enables policy control for NSWO traffic for that UE based on operator policies and user profile information that may depend on e.g. network where the UE is offloading. The PCRF sends a reply message containing PCC Rules if policy control is enabled .

6. Triggered by the successful establishment of the IP-CAN session for the UE local IP address in step 3, the V-PCRF (roaming) and the PCRF (non-roaming) may establish a session with the TDF to provision ADC Rules for that UE local IP address (if applicable, when solicited application reporting applies and when policy control for offloaded traffic is to be performed). The PCRF provides the TDF with the UE local IP address, the IMSI, the IP-CAN type and the NSWO-APN.

7. The TDF replies as described in the clause 7.2.

The steps from 6 to 10 show PCC signalling to provision policies for EPC routed traffic.

8. IP-CAN session establishment as specified in clause 7.2 is performed, including the establishment of a Gateway Control session (if applicable), as specified below with the following additional information:

   In case 2a and case 2b, the ePDG (BBERF) initiates a Gateway Control Session Establishment procedure to provide the UE local IP address and UDP port (if available) as defined in clause P.7.5.1.

   For case 1, step 3 of clause 7.2 for WLAN scenario the PCEF includes the UE local IP address and the UDP port number (if available), while for the H(e)NB scenario the PCEF includes the H(e)NB Local IP address and the UDP port number (if available) in the Fixed Broadband Access at which the H(e)NB is connected to.

   In case 2b, S-GW (BBERF) initiates a Gateway Control Session Establishment procedure to request QoS Rules for the H(e)NB local IP address as defined in clause P.7.5.1.

   The PCRF determines, based on information (UE local IP address information or H(e)NB local IP address information) provided in the IP-CAN session establishment indication or Gateway Control Session establishment indication (if applicable), whether or not the user is connecting via a Fixed Broadband Access Network.

The steps in (A) show PCC signalling to establish a Gateway Control Session over S9a for EPC routed traffic.

A.1. Triggered by the IP-CAN session establishment indication, or triggered by Gateway control session establishment over Gxb*, the PCRF (non-roaming case) or the V-PCRF (visited access roaming case) initiates Gateway Control Session establishment with the BPCF over S9a, if no Gateway Control Session exists for the same IMSI for WLAN scenario. The PCRF includes in the request message to BPCF the IMSI, the UE local IP address and the UDP port number (if available), QoS Rules, and the ePDG IP address (for S2b-GTP access) or PDN GW IP address (for trusted S2c access), while for the H(e)NB scenario, the PCRF (Non-roaming case) or the V-PCRF (visited access roaming case) initiates Gateway Control Session establishment with the BPCF over S9a, if no Gateway Control Session exists for the same H(e)NB including the IMSI, H(e)NB Local IP address, the UDP port number (if available) and QoS Rules. For home routed, the H-PCRF initiates a Gateway Control Session over S9 to trigger the V-PCRF to establish a Gateway Control Session over S9a, for visited access, the V-PCRF initiates a Gateway Control Session over S9 to H-PCRF and the Gateway Control Session over S9a to BPCF.

A.2. For WLAN scenario the BPCF Initiates the Gateway Control session establishment on S9a including in the request message the IMSI, UE Local IP address and the UDP port (if available), while for the H(e)NB scenario it includes the IMSI, H(e)NB Local IP address and the UDP port number (if available) to the PCRF.

A.3. The PCRF reply message contains the result code.

The steps in (B) show PCC signalling to provision QoS Rules over S9a for EPC routed traffic.

B.1. Triggered by the IP-CAN session establishment indication, or triggered by Gateway control session establishment over Gxb*, the PCRF (non-roaming case) or the V-PCRF (visited access roaming case) initiates Gateway Control and QoS Rule provisioning including QoS Rules and the PDN GW IP address (for trusted S2c access and if this PDN GW IP address has not been provided before), if a Gateway Control Session exists for the same IMSI for WLAN scenario while for the H(e)NB scenario the PCRF (Non-roaming case) or the V-PCRF (visited access roaming case) initiates Gateway Control and QoS Rule provisioning, if Gateway Control Session exists for the same H(e)NB including QoS Rules.

B.2. The PCRF reply message contains the result code.

9. Remaining steps of IP-CAN session establishment procedure as defined in clause 7.2 from step 6 onwards.

P.7.2.2 Void

P.7.3 IP-CAN Session Termination

P.7.3.1 Void

P.7.3.2 IP-CAN Session Termination

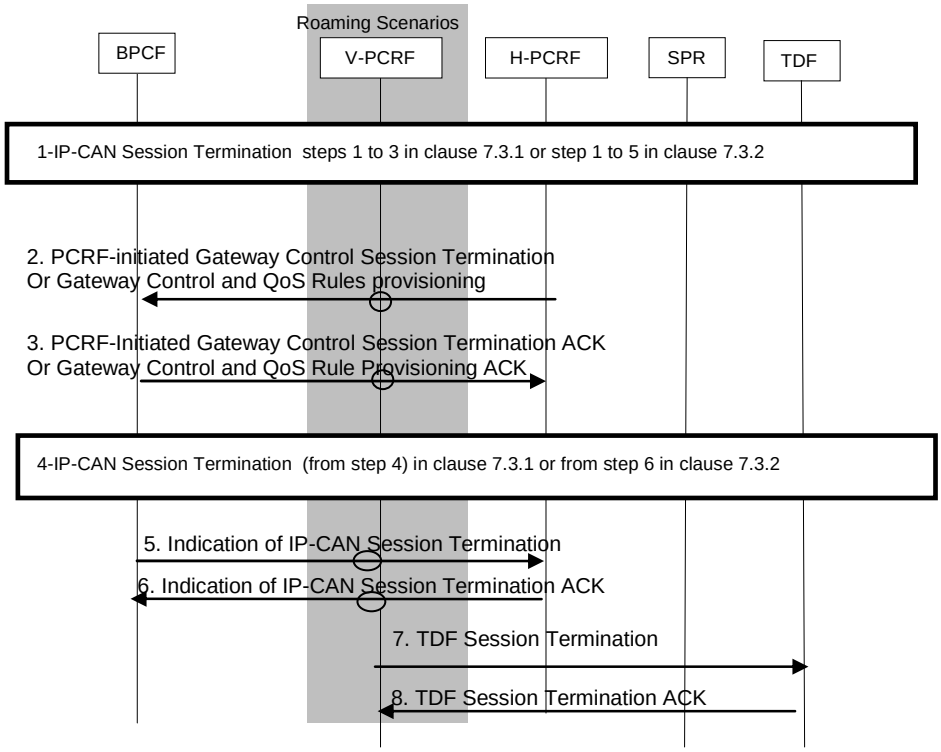

Figure P.7.3.2: IP-CAN Session Termination for either EPC routed or NSWO traffic

This procedure is applicable for both WLAN and H(e)NB scenario.

For WLAN scenarios, this procedure is performed when the PCRF knows that the 3GPP UE released a PDN connection and request the BPCF to remove the PCC/QoS Rules associated to the terminated IP-CAN session or when the last PDN connection for that 3GPP UE is released to terminate the Gateway Control Session over S9a.

For H(e)NB scenarios, this procedure is performed when the PCRF knows that the last 3GPP UE connecting to the H(e)NB released its last PDN connection and request the BPCF to release the Gateway Control session over S9a or

when a PDN connection is released to request the BPCF to remove the QoS Rules associated with the terminated IP-CAN session.

This procedure is the same as described in clauses 7.3.1 and 7.3.2, with the new steps described below:

1. The PCEF initiates the IP-CAN session termination over Gx, as defined in the clauses 7.3.1 and 7.3.2.

2. This step is triggered by the IP-CAN session termination indication in step 3 in clauses 7.3.1 and 7.3.2, the PCRF (non-roaming case) or the H-PCRF (roaming case) initiates Gateway Control Session Termination over S9a with the BPCF if this is the last IP-CAN session corresponding to this Gateway Control Session over S9a, or initiates Gateway Control and QoS Rule Provisioning over S9a to remove QoS Rules for the purpose to release resources in the Fixed Broadband Access.

NOTE: For case 2b, the description of the Gateway Control Session Termination procedure over Gxb* when triggered by the ePDG (BBERF) is described in clause P.7.5.2 and the description of the Gateway Control and QoS Rule request procedure when triggered by the ePDG (BBERF) is described in clause P.7.5.3.

For case 2a, the description of the Gateway Control Session Termination procedure over Gxb* when triggered by the PCRF is described in clause P.7.5.4.

3. The BPCF reply message contains the result code.

4. Remaining steps of IP-CAN session termination as described in clause 7.3 from step 4 onwards, with the additions that in .case 2a and roaming scenario, triggered by step2, the vPCRF initiates the Gateway control session termination with the ePDG over Gxb* if the Gateway control session over S9a bound to that IMSI has been terminated.

Steps 5, 6, 7 and 8 are triggered when the BBF access is aware that the UE is detached from BBF access. These steps are not necessarily performed at termination of the IP-CAN session but may occur at a later time.

5. If the BBF access network is aware of the UE is detached from the BBF access network, the BPCF Initiates IP-CAN session termination to the PCRF (non-roaming) and the V-PCRF (for roaming cases). Triggered by the IP-CAN session termination over S9a, the V-PCRF triggers the IP-CAN session termination over S9.

6. The PCRF reply message contains the result code for the IP-CAN session terminated.

7. Triggered by step 6, the PCRF (for non-roaming case) and the V-PCRF (for roaming cases) terminates the TDF session, if exists for the UE local IP address as described in the clause 7.3.

8. The TDF replies as described in the clause 7.3.

P.7.4 IP-CAN Session Modification

Both the PCRF-initiated IP-CAN Session Modification Procedure and the PCEF-initiated IP-CAN Session Modification Procedures as described in clause 7.4 are applicable for a 3GPP UE that attaches via a Fixed Broadband Access.

P.7.4.1 PCEF-Initiated IP-CAN Session Modification

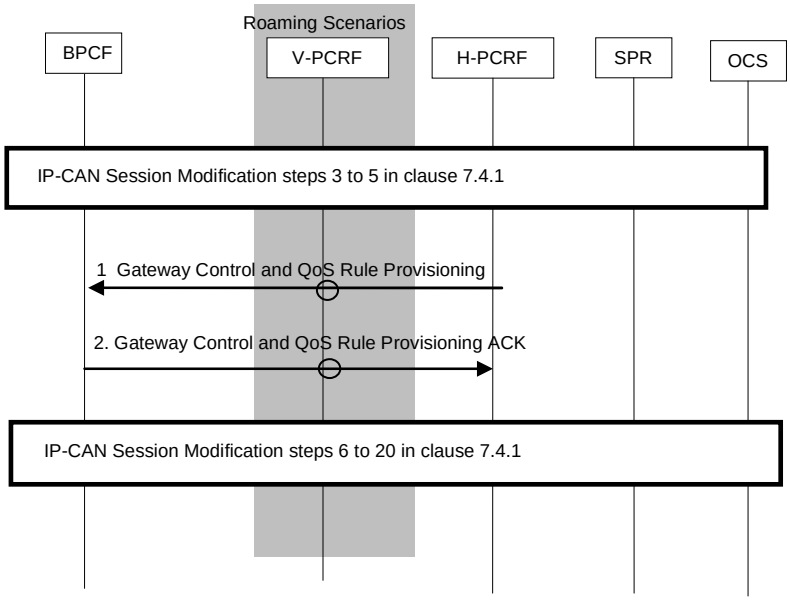

Figure P.7.4.1: PCEF-initiated IP-CAN Session Modification

This procedure is applicable for WLAN and H(e)NB scenario. This procedure is performed when the UE Local IP address, H(e)NB Local IP address or the UDP port number is changed and/or when a request for PCC Rules is received from the PCEF. This procedure is the same as described in clause 7.4.1 with the additions described below:

Step 3 in case 1, the PCEF provides the updated UE local IP address, the updated H(e)NB IP address and/or UDP port number to the PCRF.

1. The PCRF (non-roaming case) initiates Gateway Control and QoS Rule Provisioning with the BPCF to provide either:

   a. QoS-Rule with the QoS control information (i.e. QCI, GBR, MBR, ARP) and SDF information; and/or

   b UE local IP address and/or the UDP port number, the H(e)NB Local IP address may be provided in the request;

   c. Information (e.g. Session ID) that allows the BPCF to associate the request with the existing Gateway Control Session on S9a so that the fixed access can identify the traffic plane resources that are affected.

   The H-PCRF (home routed roaming case) provisions for WLAN case the UE local IP address and UDP port number (if available) and for H(e)NB case the H(e)NB local IP address and UDP port number (if available) to the V-PCRF to trigger the provisioning over S9a.

2. The BPCF translates the QoS rule as received of the S9a interface (i.e. SDF information, QCI, GBR, MBR and ARP) into access specific QoS parameters applicable in the BBF domain (the details of the mapping from 3GPP QoS parameters on S9a to QoS parameters applicable in the BBF domain is out of 3GPP scope). The BPCF may respond with a "counter-offer" in form of acceptable bandwidth and/or QoS for one or more SDFs if it cannot provide the requested QoS from the PCRF. The BPCF provides the acceptable QoS in the BBF access using 3GPP QoS parameters (i.e. QCI, GBR, MBR and ARP) and SDF information on S9a interface in the reply if the QoS validation for admission control fails. The PCRF may make a new policy decision, e.g. decide to modify or remove the affected QoS rules.

NOTE: For H(e)NB PMIP scenario, Gateway Control and QoS Rule Provisioning to the BBERF may be performed as described in clause 7.4.1.

P.7.4.2 PCRF-Initiated IP-CAN Session Modification

This procedure is initiated by the PCRF (non-roaming) or by the V-PCRF (roaming). The (V-)PCRF requests the BPCF to perform admission control. Steps (A) show how to provision QoS Rules for the UE IP address(es) allocated by EPC

and received over Gx and Steps (B) show how to provision PCC Rules to request admission control for the IP-CAN session for the UE local IP address received over S9a. Note that the TDF that is selected for EPC routed and NSWO traffic may or may not be the same TDF.

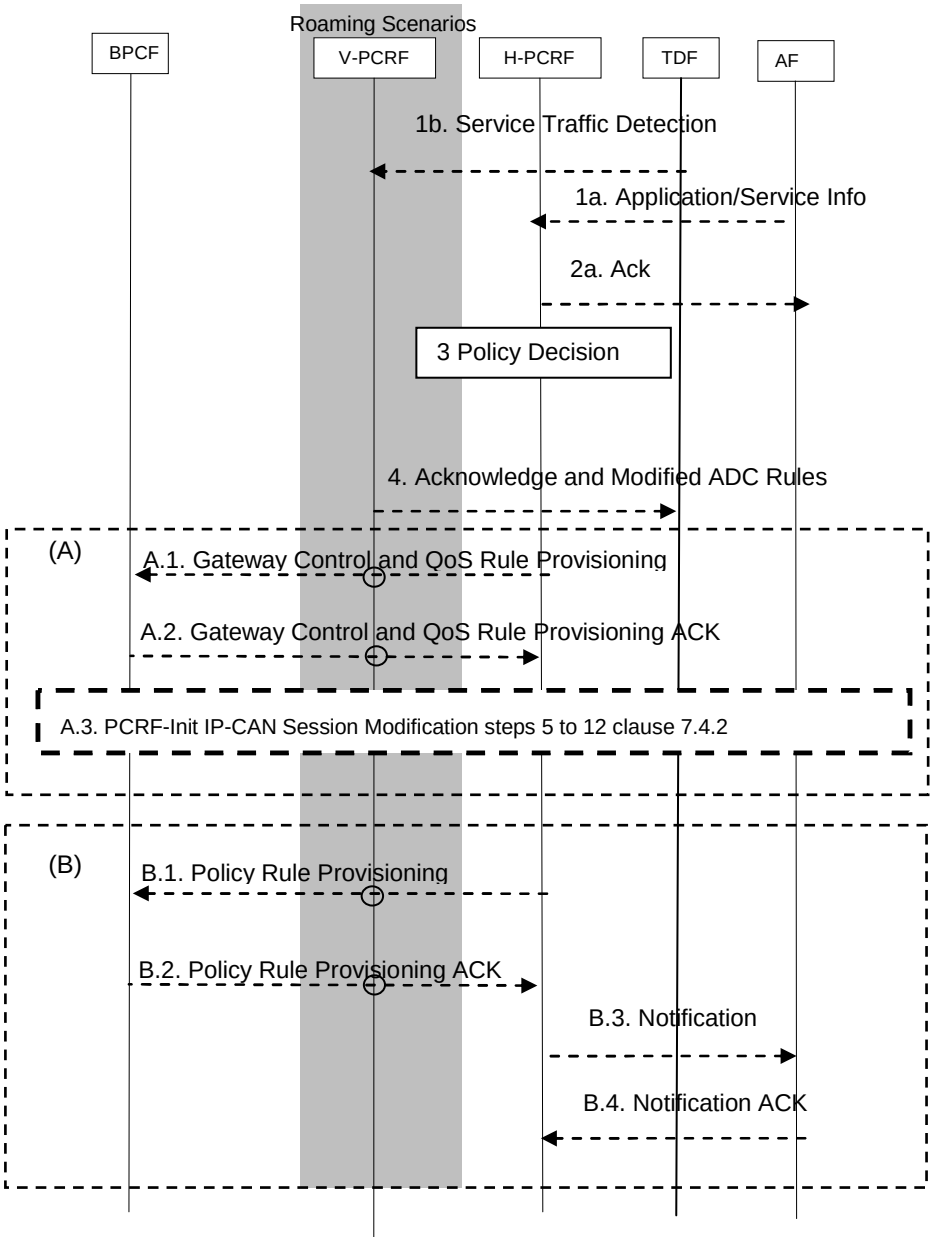

Figure P.7.4.2: PCRF-Initiated IP-CAN Session Modification

This procedure is applicable for WLAN and H(e)NB scenario. This procedure is the same as described in clause 7.4.2 with the additions described below:

1a, 2a. 1b. The AF or the TDF provides/revokes service information to the PCRF and detected event triggers if applicable as described in steps 1a, 2a and 1b in clause 7.4.2. For roaming case and for NS-WLAN offloaded traffic, the TDF provides service information and event triggers detected to the V-PCRF.

3. The PCRF for non-roaming cases or the H-PCRF for roaming cases, makes the authorization and policy decision.

4. The PCRF acknowledges to the TDF as described in clause 7.4.2.

A: The steps in (A) show PCC signalling to provision QoS Rules for EPC routed traffic.

A.1. Triggered by the step 1, the PCRF (non-roaming case) or the v-PCRF (roaming case) initiates Gateway Control and QoS Rule Provisioning to provide:

a. QoS-Rule with the QoS control information (QCI, GBR, MBR, ARP) and SDF information.

b. Information (e.g. Session ID) that allows the BPCF to associate the request with the existing Gateway Control Session on S9a so that the fixed access can identify the traffic plane resources that are affected.

A.2. The BPCF translates the QoS rule as received of the S9a interface (i.e. QCI, MBR, GBR and ARP) into access specific QoS parameters applicable in the BBF domain (the details of the mapping from 3GPP QoS parameters on S9a to QoS parameters applicable in the BBF domain is out of 3GPP scope). The BPCF may respond with a "counter-offer" in form of acceptable bandwidth and/or QoS for one or more SDFs if it cannot provide the requested QoS from the PCRF. The BPCF provides the acceptable QoS in the BBF access using 3GPP QoS parameters on S9a interface (i.e. QCI, GBR) in the reply if the QoS validation for admission control fails. The PCRF may make a new policy decision, e.g. decide to modify or remove the affected QoS rules.

A.3. PCC Rules are installed in the PCEF as described in clause 7.4.2 and AF is notified if subscribed to the notification of the resource allocation request/modification.

B: The steps in (B) show PCC signalling to provision PCC Rules for NS-WLAN offloaded traffic.

B.1. Triggered by the step 3, the PCRF (non-roaming case) or the H-PCRF (roaming case) initiates Policy Rule Provisioning towards the BPCF to provide QoS-Rules for the UE local IP address.

B.2. The BPCF translates the PCC rules as received of the S9a interface (i.e. SDF information, QCI, MBR, GBR and ARP) into access specific QoS parameters applicable in the BBF domain as described in A.2.

B.3. If the AF requested it, the PCRF notifies the AF (e.g. transmission resources are established/released/lost).

B.4. The AF acknowledges the notification from the PCRF.

P.7.4.3 BPCF-Initiated IP-CAN Session Modification

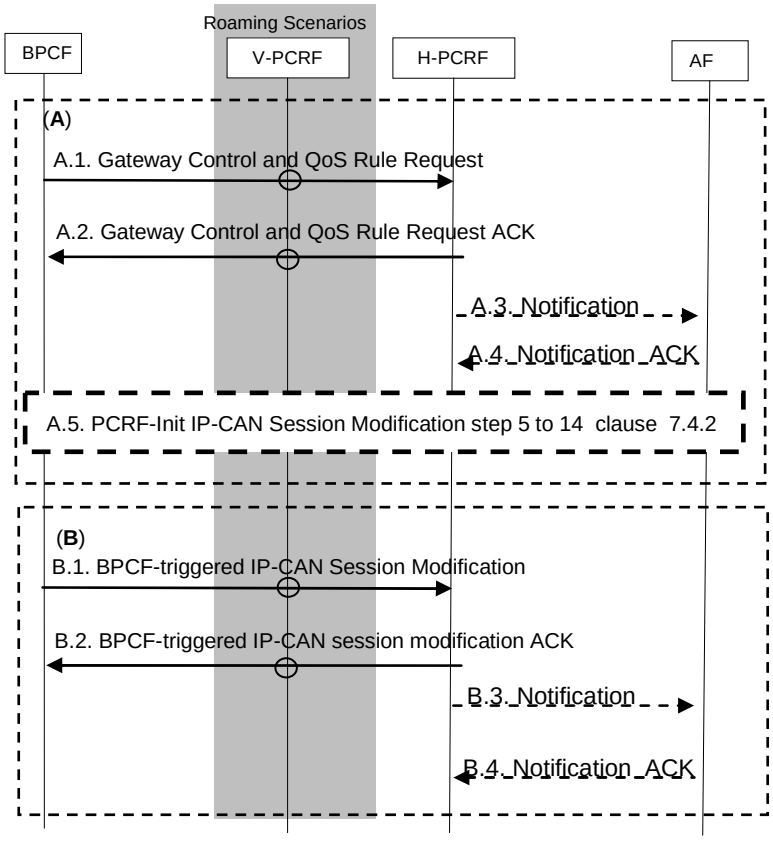

Figure P.7.4.3: BPCF-Initiated IP-CAN Session Modification

The trigger for this procedure is that the BPCF has pre-empted some resources and wants to report a QoS rule failure to the PCRF, or when the BBF network cannot sustain the Bandwidth allocated to a particular traffic class/DSCP aggregate.

This procedure is applicable for both WLAN and H(e)NB scenarios.

NOTE: Whether additional condition and criteria specific for BBF network and defined by BBF forum are applicable for trigger BPCF-Initiated IP-CAN session modification is out of the scope of 3GPP definition.

A: The steps in (A) show PCC signalling to report QoS Rule failure to PCRF for the EPC routed traffic.

A.1. The BPCF initiates Gateway Control and QoS Rule Request to report QoS Rule failure to PCRF. The request includes a report identifying the QoS Rules that failed and a reason.

A.2. The PCRF acknowledge the request and may initiate PCRF-initiated IP-CAN session modification.

Step 5 to 14 is the same as described in clause 7.4.2.

A.3. If the AF requested it, the PCRF notifies the AF (e.g. transmission resources are released).

A.4. The AF acknowledges the notification from the PCRF.

A.5. The PCRF-initiated IP-CAN session modification as described in clause P.7.4.2 may take place.

B: The steps in (B) show PCC signalling to report PCC Rule failure to PCRF for NSWO traffic.

B.1. The BPCF initiates IP-CAN session modification to report PCC Rule failure to PCRF.

A.2. The PCRF acknowledges the request.

A.3. If the AF requested it, the PCRF notifies the AF (e.g. transmission resources are released).

A.4. The AF acknowledges the notification from the PCRF.

P.7.5 Gateway Control Session Procedures

P.7.5.1 BBERF-Initiated Gateway Control Session Establishment

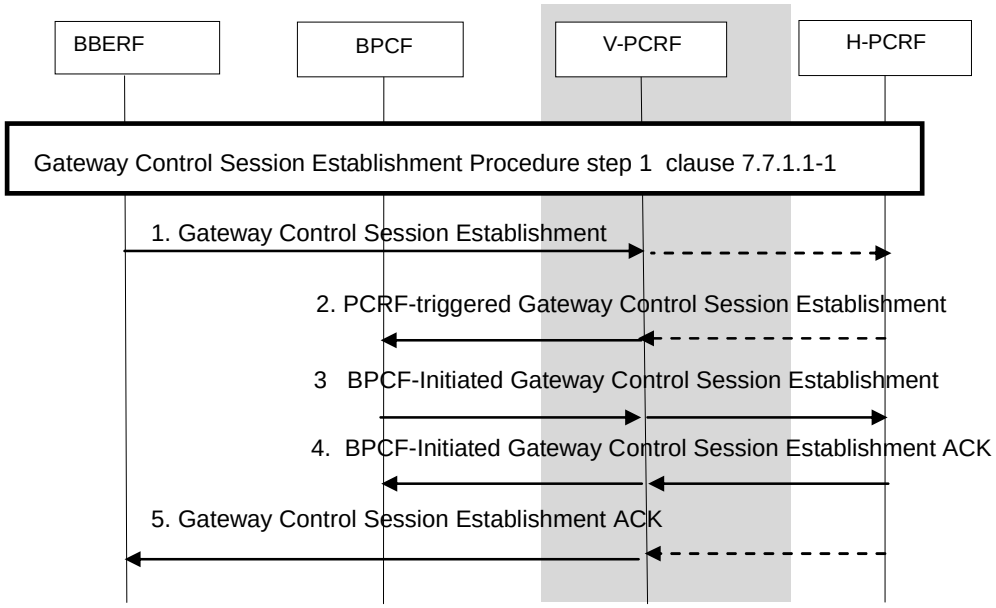

Figure P.7.5.1: PCRF-triggered Gateway Control Session Establishment for EPC routed traffic

This procedure is applicable for both WLAN and H(e)NB PMIP. This procedure is the same as described in clause 7.7.1.1 with the additions described below:

1. For the WLAN case, the ePDG (BBERF) initiates a Gateway Control Session Establishment as defined in clause 7.7.1 with the PCRF (for non-roaming) and with the V-PCRF (for home routed and visited access roaming cases) including the IMSI, APN (if available), the UE Local IP address, the UDP port number if available, while for H(e)NB case the SGW (BBERF) initiates a Gateway Control Session Establishment as defined in clause 7.7.1 with the PCRF (for non-roaming) and with V-PCRF (for home routed and visited access roaming case) including the H(e)NB local IP address and the UDP port number (if available) in the Fixed Broadband Access at which the H(e)NB is connected to.

2. For WLAN case, the PCRF (non-roaming case) or the V-PCRF (home routed and visited access roaming cases) triggers Gateway Control Session establishment with the BPCF over S9a, if this is the first Gateway Control Session for the same IMSI, the PCRF includes in the request message to BPCF the IMSI, the UE local IP address and the UDP port number (if available) and the ePDG IP address (for S2b-PMIP and untrusted S2c access).

   For the H(e)NB case, the PCRF (non-roaming case) or the V-PCRF (home routed and visited access roaming cases) triggers Gateway Control Session establishment with the BPCF over S9a, if this is the first Gateway Control Session for the same H(e)NB, the PCRF includes in the request message to BPCF the IMSI, the H(e)NB IP address and the UDP port number (if available).

3. The BPCF Initiates the Gateway Control session establishment to the PCRF (for non-roaming case), to the V-PCRF (for visited access and home routed roaming case) including in the request message the IMSI. Triggered by the BPCF-initiated Gateway Control Session establishment over S9a the V-PCRF sends the Gateway Control Session Establishment over S9.

4. The PCRF in non-roaming and the V-PCRF for roaming cases reply message contains the result code.

5. For H(e)NB case, the PCRF provisions QoS Rules to the BBERF, while for the WLAN case, the PCRF sends a result code in the reply message.

   No QoS Rules and no event triggers are provided to the BBERF for WLAN scenarios.

P.7.5.2 GW (BBERF)-Initiated Gateway Control Session Termination

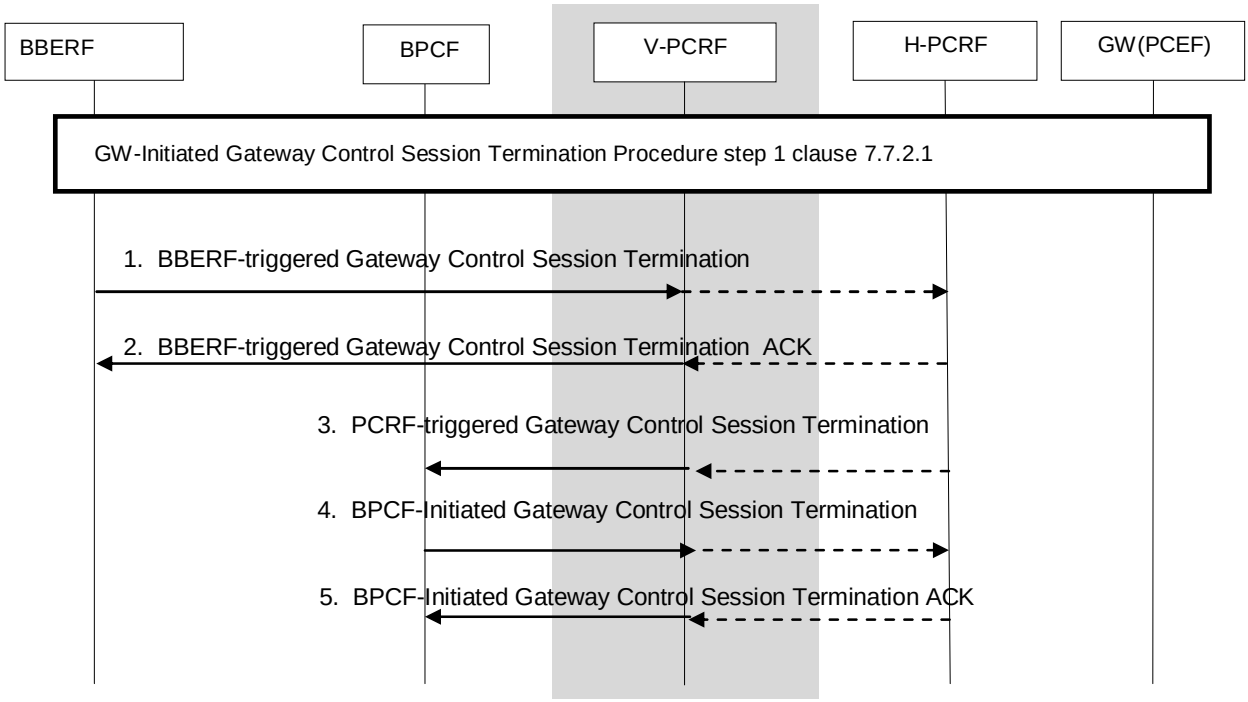

Figure P.7.5.2: Gateway Control Session Termination over S9a

This procedure is applicable for both WLAN and H(e)NB scenarios. This procedure is the same as described in clause 7.7.2.1 with the additions described below:

1. For WLAN scenarios, the ePDG (BBERF) initiates a Gateway Control Session Termination with the PCRF (for non-roaming) and with the V-PCRF (for home routed and visited access roaming cases).

For H(e)NB scenarios, the SGW (BBERF) initiates a Gateway Control Session Termination as defined with the PCRF (for non-roaming) and with the V-PCRF (for home routed and visited access roaming cases).

2. The PCRF sends a response code.
3. The PCRF (non-roaming case) or the V-PCRF (roaming case) initiates a Gateway Control Session Termination over S9a with the BPCF to terminate the Gateway Control Session with the BPCF if this is the last Gateway Control Session bound to the Gateway Control session over S9a.
4. The BPCF terminates the Gateway Control Session over S9a to the PCRF. In the roaming scenario, V-PCRF (for both home routed and visited access) sends a Gateway Control Session Termination over S9 to the PCRF.
5. The PCRF sends a response code.

P.7.5.3 Gateway Control and QoS Rule Request from ePDG/Serving GW

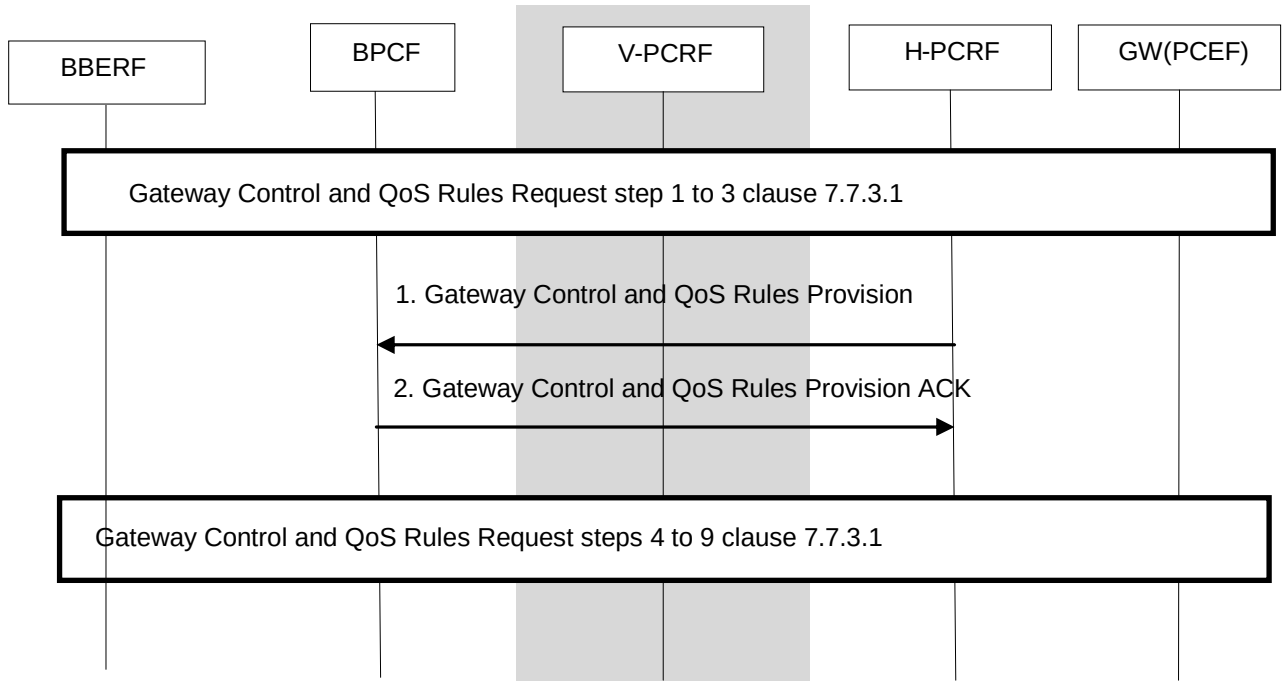

Figure P.7.5.3: Gateway Control and QoS Rule Request for EPC Routed Traffic

This procedure is applicable for both WLAN and H(e)NB PMIP. This procedure is the same as described in clause 7.7.3.1 with the exceptions described below:

In case 2b and case 2a for WLAN scenario, the ePDG (BBERF) may initiate a Gateway Control and QoS Rules Request Procedure to provide the updated UE local IP address and the UDP port number, if available, while for H(e)NB scenario the SGW (BBERF) may initiate a Gateway Control and QoS Rule Procedure to provide the updated H(e)NB local IP address and the UDP port number (if available) in the Fixed Broadband Access at which the H(e)NB is connected to.

1. For the WLAN scenario, triggered by the Gateway Control and QoS Rules Request Procedure in step 2 of clause 7.7.3.1, the PCRF (non-roaming case) or the v-PCRF (roaming case) initiates Gateway Control and QoS Rules Provision Procedure. The updated UE local IP address and/or the UDP port number are provided in the procedure if available, while for H(e)NB scenario the PCRF (non-roaming) or the H-PCRF (for visited access and home routed) may initiate a Gateway Control and QoS Rule Procedure to provide the updated H(e)NB local IP address and the UDP port number (if available) in the Fixed Broadband Access at which the H(e)NB is connected to.

   For H(e)NB PMIP scenario, the PCRF may provide:

   a. QoS-Rule with the QoS control information (i.e. QCI, GBR, MBR, ARP) and SDF information.

b. Information (e.g. Session ID) that allows the BPCF to associate the request with the existing Gateway Control Session on S9a so that the fixed access can identify the traffic plane resources that are affected.

2. The BPCF replies with a response code, when QoS Rules were provided by the PCRF, the BPCF translates the QoS rule as received of the S9a interface into access specific QoS parameters applicable in the BBF domain . The BPCF may respond with a "counter-offer" in form of acceptable bandwidth and/or QoS for one or more SDFs if it cannot provide the requested QoS from the PCRF. The BPCF provides the acceptable QoS in the BBF access using 3GPP QoS parameters on S9a interface (i.e. QCI, GBR) in the reply if the QoS validation for admission control fails. The PCRF may make a new policy decision, e.g. decide to modify or remove the affected QoS rules.

NOTE: For H(e)NB PMIP scenario, Gateway Control and QoS Rule Provisioning to the BBERF may be performed as described in clause 7.4.1.

P.7.5.4 PCRF-Initiated Gateway Control Session Termination

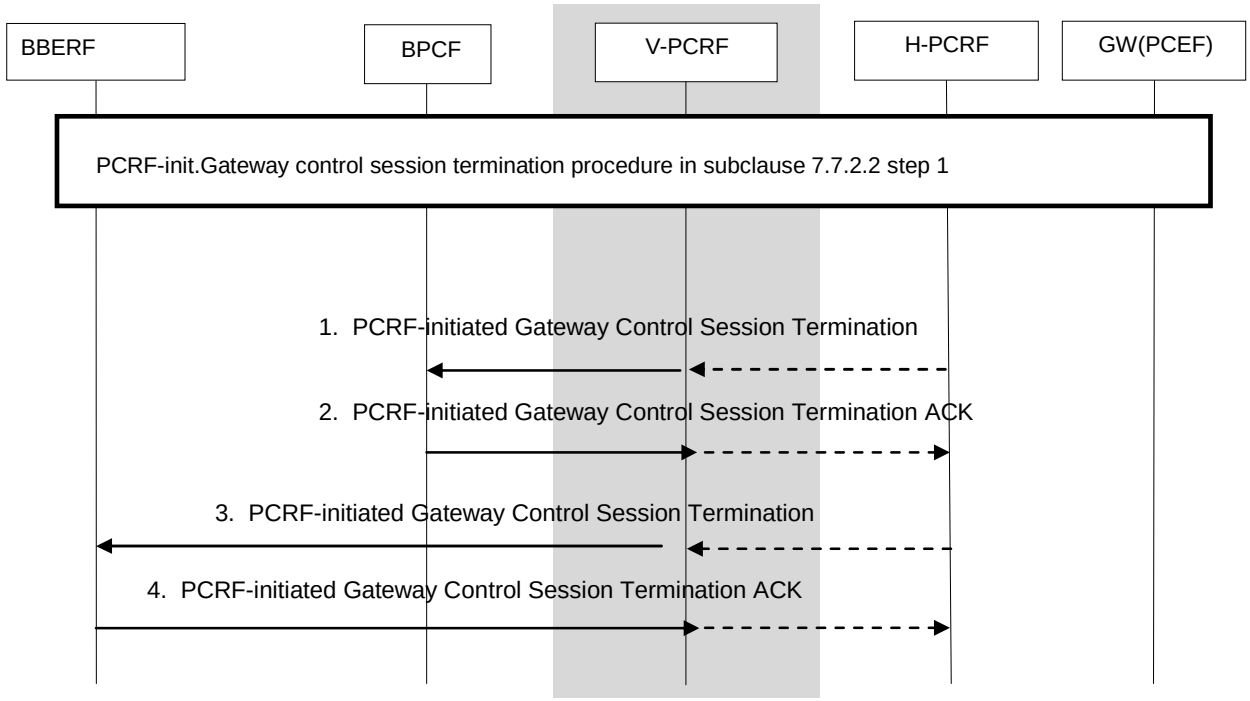

Figure P.7.5.4: PCRF-Initiated Gateway Control Session Termination

This procedure is applicable for WLAN scenario. This procedure is the same as described in clause 7.7.2.2 steps 1 with the additions described below:

1. For the non-roaming and roaming home routed cases, triggered by step 1 in clause 7.7.2.2, the (h)PCRF sends a PCRF-initiated Gateway Control Session termination procedure with BPCF over S9a. For the roaming LBO case, triggered by step 1 in clause 7.7.2.2, the (v)PCRF sends a PCRF-Initiated Gateway control session termination procedure with BPCF over S9a.

2. The BPCF sends PCRF-Initiated Gateway Control Session Termination acknowledgement.

3. Triggered by step 1 in clause 7.7.2.2, the (h)PCRF (for non-roaming case and home routed roaming case) sends a PCRF-initiated Gateway Control Session Termination over Gxb* with the ePDG (BBERF). Triggered by the Gateway Control Session Termination over S9a and S9 with the BPCF, the V-PCRF (roaming LBO case) sends a PCRF-initiated Gateway Control Session Termination over Gxb* with the ePDG (BBERF).

4. The ePDG (BBERF) sends a sends PCRF-Initiated Gateway Control Session Termination acknowledgement.

P.7.6 PCRF Discovery and Selection

P.7.6.1 PCRF Discovery and Selection by BPCF

When the BPCF knows that a 3GPP UE attached via a Fixed Broadband access network and learns the IMSI and the NSWO-APN, the BPCF initiates the IP-CAN session establishment for NSWO offloaded traffic, the BPCF finds the PCRF using the DRA as described in clause 7.6.1.

When the BPCF is requested to establish a Gateway Control Session over S9a by PCRF, the BPCF uses the PCRF address provided in the request to establish the Gateway Control Session over S9a.

In roaming scenarios, the selected V-PCRF shall belong to the same V-PLMN selected during the 3GPP access authentication procedure. The BPCF uses the VPLMN id to find the V-DRA in the VPLMN. The V-PCRF finds the DRA in the HPLMN based on the IMSI and the APN if available as described in clause 7.6.1.

P.7.6.2 PCRF Discovery and Selection by AF/TDF unsolicited application reporting for NS-WLAN offloaded traffic

For PCRF discovery and selection by AF/TDF unsolicited application reporting for NS-WLAN offloaded traffic the procedure described in clause 7.6.1 applies.

P.7.6.3 PCRF Discovery and Selection by HNB GW

When the DRA receives a request for a certain S15 Session establishment from the HNB GW, the DRA selects a suitable PCRF for the S15 Session based on HNB local IP address. When the S15 Session terminates, the DRA shall remove the information about the S15 Session.

P.7.7 BPCF Discovery and Selection

For PCRF-triggered Gateway Control Session establishment, the PCRF (for non-roaming case) and the V-PCRF (for home routed and visited access roaming cases) is configured with IP address range mappings { (IPx..IPy) -> BBF network entry point}. The PCRF (for non-roaming) and the V-PCRF (for roaming cases) selects the correct BBF network entry point based on UE Local IP address for WLAN access and based on H(e)NB Local IP address received from the PCEF/BBERF for H(e)NB case. The implementation of a BBF network entry point is out-of-scope for 3GPP e.g. be a BPCF or a DRA. The H-PCRF sends the H(e)NB/UE local IP address to the V-PCRF over the S9 interface.

For WLAN and H(e)NB in Home Routed roaming case, for PCRF-triggered Gateway Control Session establishment, H-PCRF finds V-DRA according to the VPLMN ID if received via Gx session, and then discovers V-PCRF by V-DRA. V-PCRF selects the correct BBF network entry point with the given UE local IP address and the H(e)NB Local IP address in the BBF access network at which the H(e)NB is connected to respectively.

NOTE: Mobility procedures that implies selection of a new BPCF are not supported in this Release.

P.7.8 TDF Discovery and Selection for NS-WLAN offloaded traffic

For the solicited application reporting, the TDF address may be preconfigured in the PCRF. Alternatively, the PCRF may receive the TDF address as a part of IP-CAN session signalling for NS-WLAN offloaded traffic over S9a.

NOTE: It is assumed that UL and DL traffic are routed via the same TDF.

P.8 3GPP HNB Procedures – CS Support

P.8.1 S9a CS Session Establishment

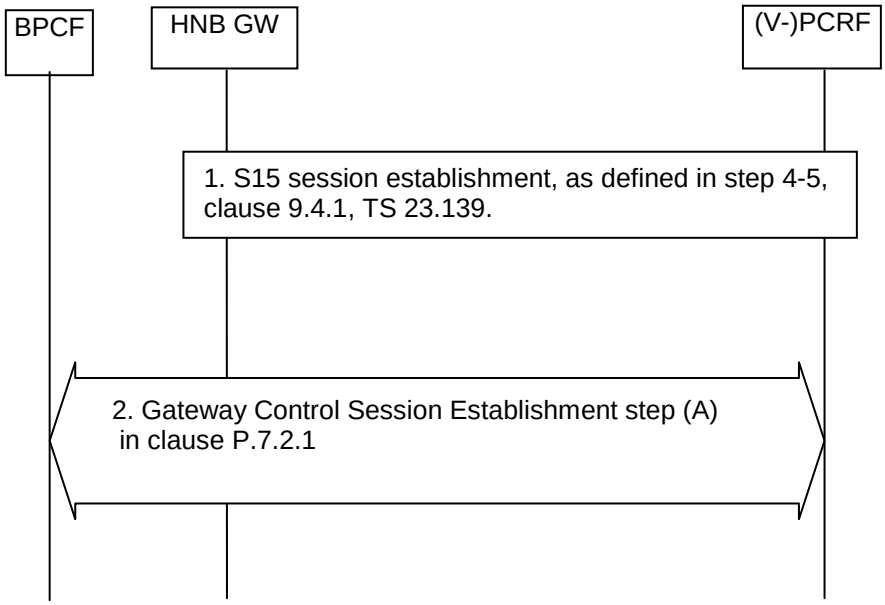

Figure P.8.1-1: S9a CS Session Establishment

This procedure is applicable to HNB for QoS enforcement for CS services.

1) S15 session establishment procedure is performed, which can be referred to step 4-5, clause 9.4.1, TS 23.139 [29].

2) The (v-)PCRF initiates Gateway Control Session Establishment procedure with BPCF. The description of this step is the same as steps (A) in clause P.7.2.1.

P.8.2 PCRF initiated S9a CS Session Modification

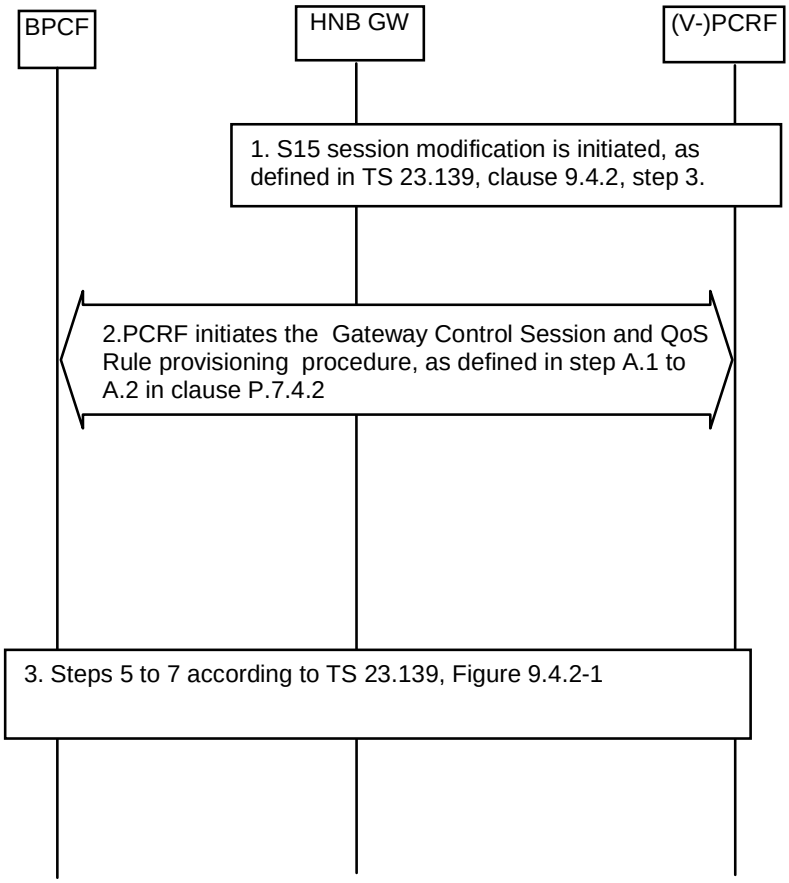

Figure P.8.2-1: PCRF initiated S9a CS Session Modification

This procedure is performed when the first UE or a subsequent UE connected to a HNB requesting a CS call.

1) The HNB GW sends the S15 session modification message to the PCRF, which can be referred to clause 9.4.2, step3 of TS 23.139 [29].

2) The PCRF (V-PCRF) initiates the Gateway Control and QoS Rules Provisioning procedure to the BPCF as described in step from A.1 to A.2 in clause P.7.4.2.

3) The remaining steps are the same as for clause 9.4.2, steps 5-7 of TS 23.139 [29].

P.8.2A BPCF initiated S9a CS Session Modification

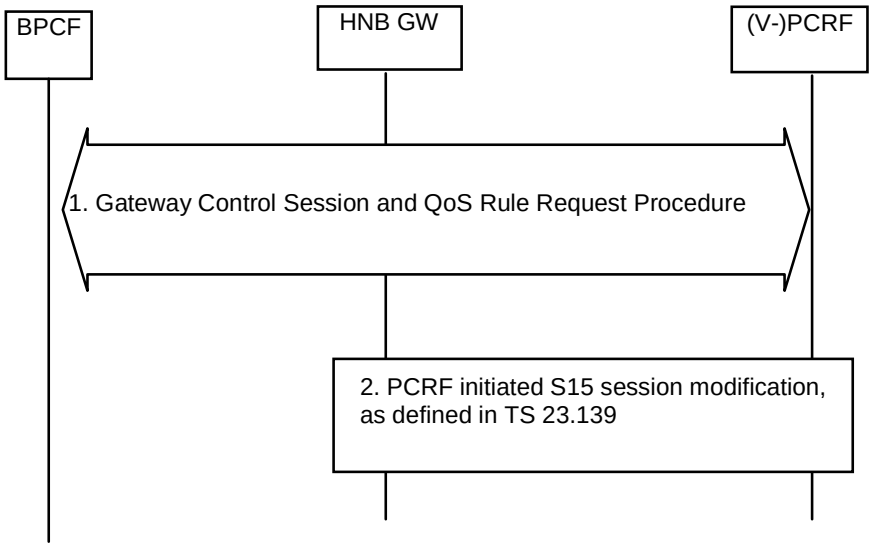

Figure P.8.2A-1: BPCF initiated S9a CS Session Modification

1) This step shows PCC signalling to report QoS Rule failure to (v)PCRF for the CS traffic.

NOTE: Whether additional condition and criteria specific for BBF network and defined by BBF forum are applicable for trigger BPCF-Initiated S9a CS Session Modification is out of the scope of 3GPP definition.

The BPCF initiates Gateway Control and QoS Rule Request to report QoS Rule failure to (v)PCRF. The request includes a report identifying the QoS Rules that failed and a reason. The (v)PCRF acknowledges the request.

2) The (v)PCRF sends the S15 session modification request message to the HNB GW. The (v)PCRF includes the report identifying the QoS Rules that failed and a reason derived from the BPCF. The BPCF response the S15 session modification to the (v)PCRF, which is according to TS 23.139 [29].

P.8.3 S9a CS Session Termination

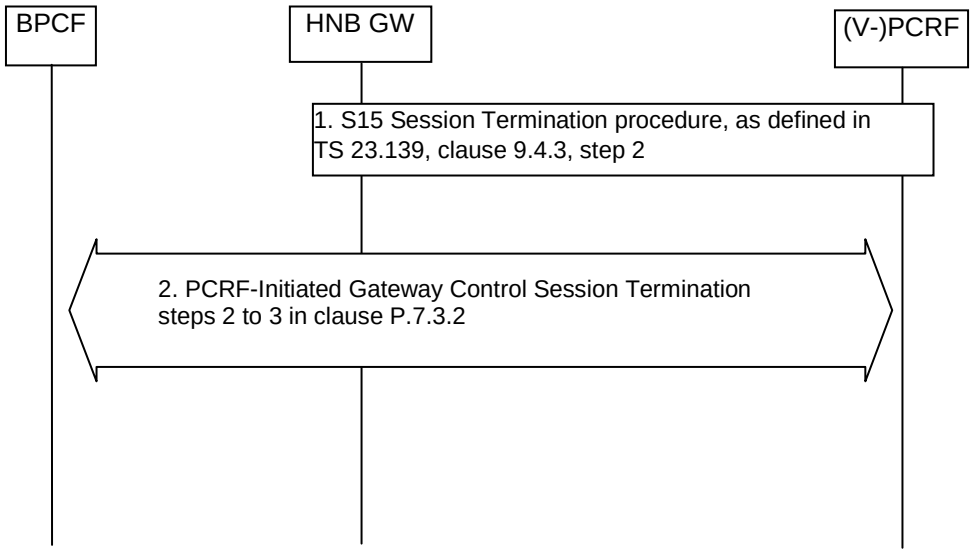

Figure P.8.3-1: S9a CS Session Termination

1) The HNB GW sends a S15 session termination request to the to (v-)PCRF and then the (v-)PCRF acknowledges the request. This can be referred to clause 9.4.3, step 2 of TS 23.139 [29].

2) The PCRF (V-PCRF) initiated the GW control session termination as defined in steps 2 and 3 in clause P.7.3.2.

Annex Q (informative): How to achieve Usage Monitoring via the OCS

An alternative to providing the usage monitoring feature described in this technical specification is to re-use the capabilities defined in 3GPP Release 11 for implementation of Policy Control based on Subscriber Spending Limits when online charging is also performed.

There are two ways defined in this Annex to achieve usage monitoring via OCS:

If PCC/ADC rules that are subject to usage monitoring share the same charging key, the same measurement methods then the Usage Reports over Gy are used for both charging and usage monitoring, and in addition:

- Policy Counter Status values are associated with the quota allocated with Charging Keys are configured in the OCS. Policy Counter Status (INQUOTA, OUTQUOTA) changes trigger notifications over Sy.
- The PCRF is configured with operator policies that associate the policy counter status to a policy decision e.g. block or allow a service to a QoS.

If PCC/ADC rules that are subject to usage monitoring have different charging keys and/or different measurement methods then to achieve a common usage report over Gy then:

- A common Charging Key is used for all services that are subject to usage monitoring. The charging control information of the PCC/ADC rules includes that online charging applies, the common charging key for the service and service level reporting is activated. In addition, the measurement method is to be set to time/volume.
- Policy Counter Status values associated with the quota allocated with Service identifier is configured in the OCS. Policy Counter Status (INQUOTA, OUTQUOTA) changes trigger notifications over Sy.
- The PCRF is configured with operator policies that associate the policy counter status to a policy decision e.g. block or allow a service to a QoS.

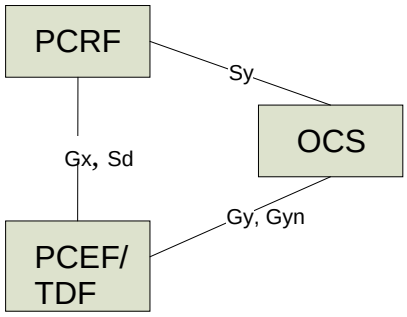

Figure Q.1-1: Deployment for Usage Monitoring via Online Charging System

Annex R (informative): Disabling/re-enabling Usage Monitoring for a PCC/ADC rule

If usage monitoring for a PCC/ADC rule (belonging to a usage monitoring group) needs to be disabled, one of the two ways below can be chosen to realize this feature:

- The PCRF generates a new PCC/ADC rule with the same information (apart from the PCC/ADC Rule identifier) as the existing PCC/ADC rule used to control the same traffic but without the monitoring key. The PCRF provides the new PCC/ADC rule to the PCEF/TDF and removes the existing PCC/ADC rule.

NOTE 1: It is assumed that the activation of the new PCC/ADC rule takes place at the same time as the removal of the existing PCC/ADC rule and that no other actions are triggered (e.g. with respect to charging and bearer management) beside the ones related to the disabling of usage monitoring.

- The operator selects a specific monitoring key value to be used for all PCC/ADC rules for which usage monitoring is disabled. The PCRF modifies the monitoring key of the corresponding PCC/ADC rule to this specific value. Following the PCRF instruction, the PCEF or TDF updates the monitoring key in the modified PCC/ADC rule and collects the usage information for the specific monitoring key value. The PCEF/TDF usage reports would still be received by the PCRF but could be ignored.

NOTE 2: The operator should configure the usage threshold to a sufficiently high value so that frequent usage reports are avoided.

If usage monitoring needs to be re-enabled for a PCC/ADC rule (i.e. usage monitoring has been disabled for this PCC/ADC rule before), one of the two ways below can be chosen to realize this feature:

- The PCRF generates a new PCC/ADC rule with the same information (apart from the PCC/ADC Rule identifier) as the existing PCC/ADC rule used to control the same traffic and adds the required monitoring key. The PCRF provides the new PCC/ADC rule to the PCEF/TDF and removes the existing PCC/ADC rule without monitoring key. The PCEF/TDF executes the operations in the same way it is described above in Note 1.

- The PCRF modifies the monitoring key of the corresponding PCC/ADC rule to the value of the required usage monitoring group (e.g. back to its original value).

Annex S (normative): Fixed Broadband Access

S.1 General

This annex specifies the enhancement to PCC framework for supporting policy and charging control in the fixed broadband access network in the convergent scenario where a single operator is deploying both the fixed broadband access network and the Evolved Packet Core (EPC).

The scope of this Annex is to define requirements for the convergent scenario where the PCRF controls directly the network element(s) in the fixed broadband access without the mediation of a different policy server, such as the BPCF defined in Annex P.

Policy and charging control is provided for both Non-seamless WLAN offload traffic from a 3GPP UE and fixed devices.

The work in this annex takes the fixed broadband accesses as specified by BroadBand Forum in TR-300 [37] as a reference.

NOTE 1: This does not preclude the applicability of the solutions described in this Annex to fixed broadband accesses not defined by Broadband Forum.

This annex is a realization of the main specification body for the Fixed Broadband Access IP-CAN. It describes only the exceptions and additions in respect to the main specification body, therefore, if not explicitly mentioned, the main specification body is applicable.

NOTE 2: Support for MPS Services and IMS Emergency is not specified in this Release.

S.2 Definitions

The definitions in the following are relevant for this annex only.

UE local IP address: Defined as either the public IP address assigned to the UE by the Broadband Forum domain in the no-NAT case, or the public IP address assigned by the Broadband Forum domain to the NATed RG.

IP-CAN session: For fixed broadband access, the IP-CAN session can also be identified primarily by an IP address(es). The term UE corresponds to the device that access the services provided by the network (i.e. either RG, or 3GPP UE or fixed end-device), the PDN identifies the IP network where the device gets IP connectivity and the UE identity information may be the IMSI, the user-name or the access line identifier (if available). In a Fixed Broadband Access an IP-CAN session corresponds to a Subscriber IP Session defined in TR-146 [36].

NOTE: The PDN connection concept and APN are not applicable to Subscriber IP session for fixed device.

S.3 High Level Requirements

S.3.0 General

The same requirements as defined in clause 4 4 to support usage monitoring and clause 4.5 to support application detection and control applies.

S.3.1 General Requirements

The same requirements as defined in clause 4 applies with the following exception and addition:

- For Fixed devices the policy and charging control shall be possible only in non- roaming scenario.

- For Fixed Broadband Access, PCC decisions shall be based on subscription information for both fixed device and/or fixed access line.

- PCRF shall control directly the PCEF in the IP-Edge in the fixed broadband access without the mediation of the BPCF defined in TS 23.139 [29].

NOTE 1: In this Release of the specification, Policy and charging control for layer 2 sessions are out of the scope.

- An IP-CAN session shall be established on the IP-Edge per IPv4 address and/or IPv6 address or IPv6 prefix known in the IP-Edge.

  PCC shall be supported for both the IP-CAN session established for the RG and for each IP-CAN session created for every device (i.e. fixed device or 3GPP UE) behind the RG that is visible in the IP-Edge/PCEF.

NOTE 2. In this Release the identification of end-user devices behind a RG configured in routed mode is not supported.

NOTE 3: In this Release of the specification, there is no support for IMS-based emergency services.

NOTE 4: In this Release of the specification, there is no support for traffic steering control.

S.3.2 Charging Related Requirements

The same requirements as defined in clauses 4.2.1, 4.2.2 and 4.2.2.a apply, with the exception and addition listed in the following:

- The architecture shall provide charging for traffic exchanged by fixed devices and NSWO traffic to/from 3GPP UEs in the following scenarios:

  - 3GPP IP-Edge based charging with PCEF located in the fixed broadband access network;

  - Traffic Detection Function (TDF)-based charging;

  - AAA-based charging,

- The requirements for the AAA-based charging solution are described in clause S.8.

NOTE 1: The selection of which accounting methods enabled is based on deployment option and there is no dynamic capability negotiation.

NOTE 2: The same accounting method is applicable to all devices connected to the same fixed broadband access network.

Charging interaction per device (i.e. fixed device or 3GPP UE) is possible only when an IP-CAN session exists for the 3GPP UE or fixed device connected behind a RG.

NOTE 3: For a 3GPP UE or a fixed device behind a NATed RG it is not possible to perform charging for that specific device.

Inter operator settlements are assumed to ensure support of the case of an UE receiving NSWO over a Fixed Broadband Access (FBA), when the HPLMN and the FBA Service Provider support different charging options.

It shall be possible for the charging system to select the applicable rate based on:

- home/visited IP-CAN;

- QoS provided for the service;

- Time of day;

- Location of the subscriber.

- Subscriber identifier.

Home/visited IP-CAN is not applicable for charging of fixed devices.

S.3.3 Policy Control Requirements

The same requirements as defined in clause 4.3 applies with the exception and addition listed below:

- The PCEF in the IP-Edge shall be able to enforce policies and to perform the appropriate mapping from QoS parameters it receives from the PCRF to Broadband Forum specific parameters.

NOTE: How the IP-Edge performs such mapping is out of 3GPP scope.

- PCC shall provide QoS control on a service data flow/detected application traffic basis, for IP traffic exchanged by fixed devices and for NSWO traffic exchange by 3GPP UEs in the fixed broadband access.
- Requirements for QoS control at IP-CAN bearer level defined in clause 4.3.3.2 are not applicable for Fixed Broadband Access.

S.4 Architecture model and reference points

S.4.1 Reference architecture

S.4.1.1 General

The reference architecture described in clause 5.1 and shown in figures S.4.1.2-1 and S.4.1.3-1 applies with the exception and addition listed in the following:

- PCEF resides in the IP-Edge in the Broadband Forum access network;
- Gxx reference point is not used.

NOTE 1: Either SPR or UDR is used in this architecture.

NOTE 2: The roaming scenario is not applicable to fixed device and RG.

S.4.1.2 Reference architecture - Non-Roaming

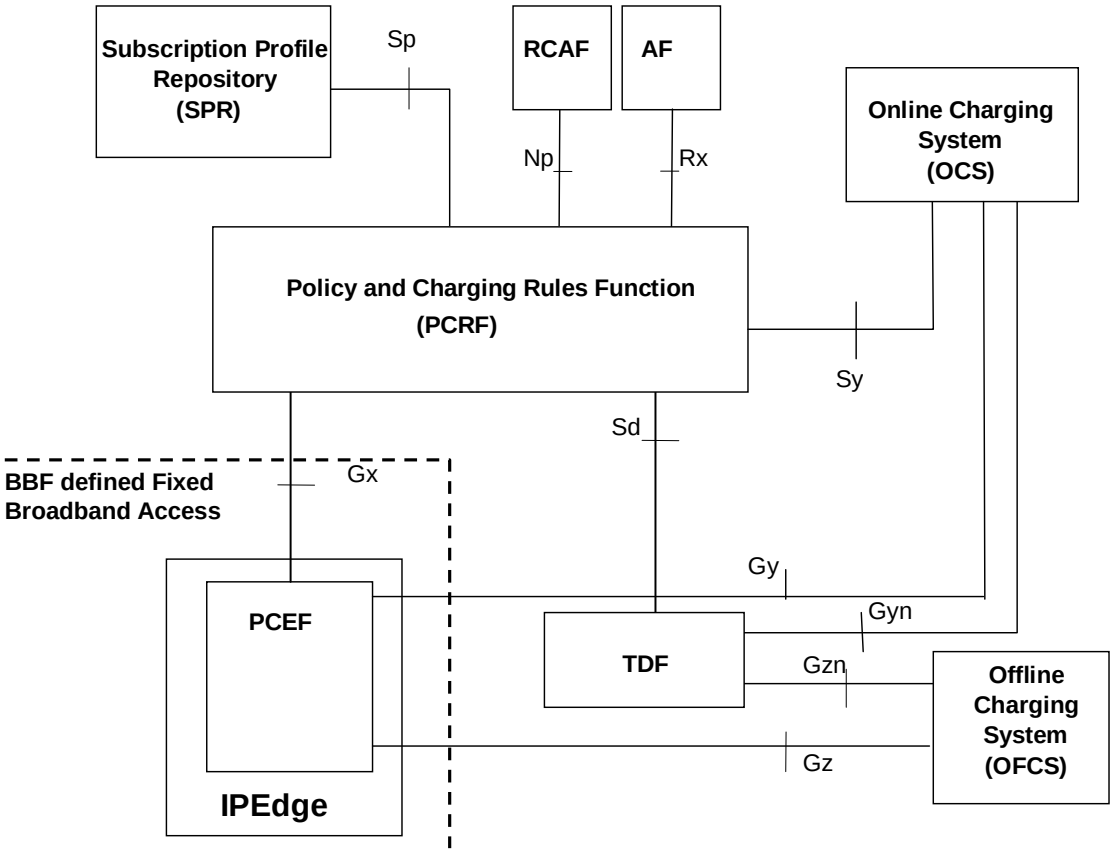

Figure S.4.1.2-1: PCC Reference architecture for Fixed Broadband Access convergence when SPR is used

S.4.1.3 Reference architecture - Roaming

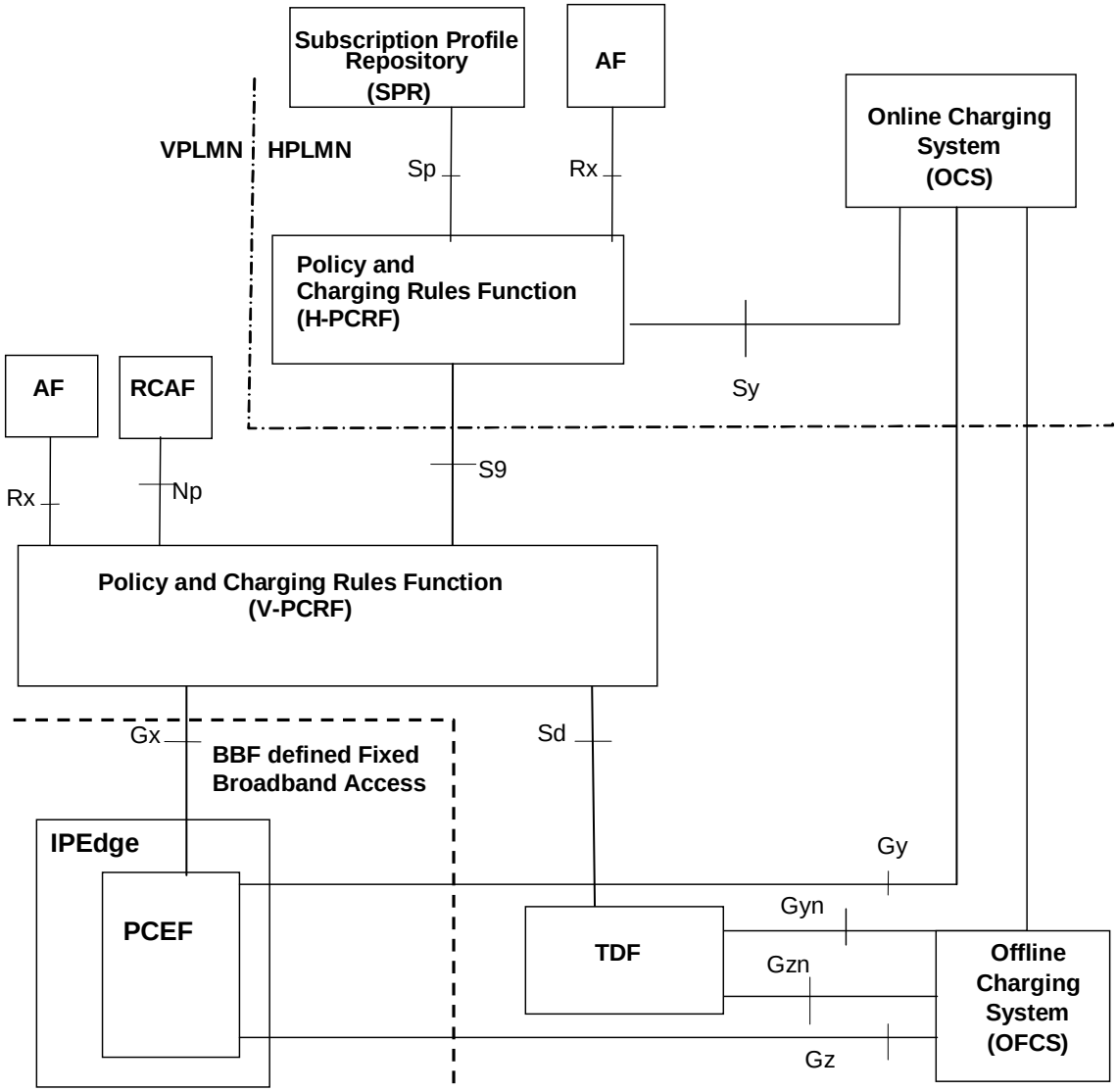

Figure S.4.1.3-1: PCC Reference architecture for Fixed Broadband Access convergence (roaming) when SPR is used

S.4.2 Reference points

S.4.2.1 Gx Reference Point

This reference point corresponds to the Gx which resides between the PCEF in the IP-Edge and the PCRF.

The same functionality as defined in clause 5.2.2 with the following exceptions:

- No provisioning of IP flow mobility routing information from PCEF to PCRF is performed.
- Negotiation of IP-CAN bearer establishment mode (UE-only or UE/NW) does not apply.

In addition, for the purpose of convergence between 3GPP access and Broadband Forum access network, the Gx reference point enables the transfer of PCC rules for an IP-CAN session that exists in the PCEF for a fixed device or for a 3GPP UE.

S.4.2.2 Sp Reference Point

For the purpose of policy and charging control convergence between 3GPP and Broadband Forum access network, the Sp reference point allows the PCRF to request subscription information from the SPR based on a subscriber ID that is defined in clause S.5.2.1. When the subscriber Id is an IMSI, the PDN identifier is the NSWO-APN. When the subscriber Id is used to identify a fixed device no PDN identifier is applicable.

NOTE 1: The naming convention of NSWO-APN is left to operator's implementation decision.

S.4.2.3 Ud Reference Point

For the purpose of convergence between 3GPP access and Broadband Forum access network, the Ud reference point provides the same functionality as the Sp reference point described in clause S.4.2.2.

S.4.2.4 Gy/Gz Reference Point

These reference points provide the same functionality as defined in the clauses 5.2.4 and 5.2.5 respectively.

For the purpose of convergence between 3GPP access and BBF access network, the functions of credit management and reporting is defined in clause S.5.1.6.

The Gz and Gy interfaces are specified in TS 32.240 [3] and the functionalities required across the Gz and Gy reference point are defined in TS 32.251 [9].

S.4.2.5 Gyn/Gzn Reference Point

These reference points provide the same functionality as defined in the clause 5.2.10 and 5.2.11 respectively.

In addition for the purpose of convergence between 3GPP and BBF access network, the functions of credit management and reporting are defined in clause S.5.1.6.

The Gzn and Gyn interfaces are specified in TS 32.240 [3] and the functionalities required across the Gzn and Gyn reference point are defined in TS 32.251 [9].

S.4.2.6 Sd Reference Point

For the purpose of convergence between 3GPP and Broadband Forum access network, the Sd reference point allows PCRF to have dynamic control over the application detection and control behaviour at a TDF for a fixed device or for a 3GPP UE. The Sd reference point enables the signalling of ADC decision, which governs the ADC behaviour. The Sd reference point provides the same functionality as the Sd described in clause 5.2.8.

S.5 Functional description

S.5.1 Overall description

The purpose of PCC convergence is to enable the policy and charging control for NSWO traffic from 3GPP UE connected to the fixed broadband access network and for the traffic from fixed devices with where the PCRF controls directly the network element(s) in the fixed broadband access without the mediation of a different policy server, such as the BPCF defined in TS 23.139 [29]. In this release, EPC-routed traffic from 3GPP UE connected to connected fixed broadband access network is considered outside the scope.

The binding mechanism, credit management, reporting, usage monitoring, termination actions, service data flow prioritization, ADC Rule definition and operations, PCC Rule definition and operations and standardized QoS characteristics as defined in clause 6.1 shall apply.

Handling of packet filters provided to the UE by the PCEF as defined in clause 6.1.9 is not applicable for Fixed Broadband Access.

S.5.1.1 IP-CAN Session

For routed mode RG with NAT, one IP-CAN session shall be established for each corresponding Subscriber IP session on the IP-Edge for the IPv4 address and/or IPv6 address or IPv6 prefix assigned to the RG.

In case of routed mode RG when the PPP pass-through feature is enabled (see requirement R-10 in TR-124 Issue 3 [34b]) an IP-CAN session shall be established for the each single fixed device starting the PPP session. In this case the 3GPP UE does not have Subscriber IP session in IP-Edge.

For bridged mode RG, one IP-CAN session shall be established for each corresponding Subscriber IP session on the IP-Edge for each IPv4 address and/or IPv6 address or IPv6 prefix assigned to the fixed device or 3GPP UE which established a Subscriber IP session in fixed broadband network.

For routed mode RG with IPv6 when stateless IPv6 address autoconfiguration is used by the end-device behind the RG, one IP-CAN session shall be established for each corresponding Subscriber IP session on the IP-Edge for the IPv6 prefix assigned to the RG. When stateful IPv6 address configuration is used by the end-devices, one IP-CAN session may be established for each end-device.

For routed mode RG, the successful completion of 3GPP-based access authentication and assignment of IP address to the 3GPP UE shall not result in any IP-CAN session establishment if the IP address assignment does not result in a new Subscriber IP Session in the IP-Edge. In this case the pre-existent IP-CAN session for the RG is used.

A device connected to the RG (e.g. VoIP phones) may also initiate a Subscriber IP session when the RG is configured in bridge mode or when the PPP pass-through feature is enabled on the Routing RG (see requirement R-10 in TR-124 Issue 3 [34b]).

S.5.1.2 Subscriber Identifier

The Subscriber ID represents the identity of the User.

For the 3GPP UE the Subscriber ID is the IMSI.

The Subscriber ID used by fixed device at establishment of Subscriber IP session in fixed broadband access network can be the Access Line Identifier (physical and logical circuit ID) or the username, for example when the Subscriber IP session is a PPP Session. For the RG and fixed device based on Broadband Forum specification, the Subscriber ID is defined in Broadband Forum WT 134 [31] specification.

S.5.1.3 Event triggers

The fixed broadband access network in the convergent scenario supports the Event triggering mechanisms described in clause 6.1.4. The event triggers applicable are listed in the following:

Table S.5.1.3-1: Event triggers

Event trigger	Description	Reported from	Condition for reporting
QoS change	The QoS of the Default Access Profile in AAA has changed	PCEF	PCRF
Out of credit (see note 1)	Credit is no longer available.	PCEF, TDF	PCRF
Enforced ADC rule request	TDF is performing an ADC rules request as instructed by the PCRF.	TDF	PCRF
Usage report	The IP-CAN/TDF session or the Monitoring key specific resources consumed by a UE either reached the threshold or needs to be reported for other reasons.	PCEF, TDF	PCRF
Start of application traffic detection and Stop of application traffic detection (see note 2)	The start or the stop of application traffic has been detected.	PCEF, TDF	PCRF
Credit management session failure (see note 1)	Transient/Permanent Failure as specified by the OCS	PCEF, TDF	Always set
NOTE 1: This event may apply only when Gy and/or Gyn are deployed. NOTE 2: This event may only be triggered by a PCEF enhanced with ADC.			

S.5.1.4 Void

S.5.1.5 Void

S.5.1.6 Credit management

For the purpose of credit management of an IP-CAN session for a fixed devices or a 3GPP UE using NSWO, the description in clause 6.1.3 applies with the following exceptions: the subscription identity is provided by PCEF or TDF to the OCS as defined in S.5.1.2 and the applicable credit-reauthorization triggers are defined in the table S.5.1.6-1:

Table S.5.1.6-1: Credit re-authorization triggers

Credit re-authorization trigger	Description	Applicable for
Credit authorisation lifetime expiry (see note 1)	The OCS has limited the validity of the credit to expire at a certain time.	PCEF, TDF
Idle timeout (see note 1)	The service data flow identified by a PCC Rules or the application identified by an ADC Rule has been empty for a certain time.	PCEF, TDF
QoS changes	The QoS of the access network profile has changed.	PCEF
NOTE 1: This credit reauthorization triggers apply only when Gy and/or Gyn are deployed.		

S.5.2 Policy and charging Control

S.5.2.1 Policy and charging control rule

The definition of PCC rule and PCC Rule operations in clauses 6.3.1 and 6.3.2 are applicable, except:

- PS to CS session continuity;

- User Location Report.

NOTE: The procedure for provisioning predefined PCC rules at the IP-Edge is out of 3GPP scope.

S.5.2.1a IP-CAN session related policy information

Table 6.4 applies with the following exceptions:

- Authorized QoS per bearer and authorized MBR per QCI are not applicable for Fixed Broadband Access.
- Charging characteristics profile for 3GPP UE is not available at the PCEF/IP-Edge.
- No Charging Characteristics profile is defined for fixed devices.

S.5.2.2 Void

S.5.3 Void

S.5.4 Reflective QoS

The Fixed Broadband Network received the PCC rules from Gx reference point and as described in clauses S.3.3 and S.6.1.2 performs the appropriated mapping to Fixed Broadband access parameters. The mapping is outside the scope of 3GPP network and defined in TR-300 [37]. Fixed Broadband Access network currently supports the DSCP marking as specified in BBF TR-092 [40] for BRAS, in BBF TR-101 [35] for Access Nodes and Aggregation Nodes and in BBF TR-124 Issue 3 [34b] for the RG.

The solution is based on DSCP marking of packets traversing the Fixed Broadband Access network. The solution assumes functionality in the BBF domain, all these functions are out-of-scope for 3GPP; also, these functions may or may not be implemented depending on the agreement between 3GPP and Fixed Broadband Access operator, these functions are described for information only.

The downlink QoS treatment of the traffic in the PCEF is defined in clause S.6.1.2 and in TR-300 [37].

For the QoS treatment of the IP flow traffic from the UE to the IP-Edge, DSCP marking may be performed by the 3GPP UE by means of reflective QoS as defined in TS 23.139 [29], in particular:

- How to inform the UE, as part of 3GPP access authentication signalling, that reflective QoS shall be applied on all the traffic in the attached network as defined in clause 6.3.1 of TS 23.139 [29].
- How the UE creates a 5-tuple rule for uplink traffic as defined in clause 6.3.3 of TS 23.139 [29]. How the RG or the IP-Edge may implement protective measurements (e.g. per UE-bandwidth limitations in the RG or in the IP-Edge) as defined in clause 6.3.1 of TS 23.139 [29].

NOTE: The UE supporting reflective QoS always send this indication during the Access authentication procedure.

S.5.5 Policy Control

Policy control functionalities listed in clause 6.1.5: binding, gating control, event reporting, QoS control and Redirection are applicable for Fixed Broadband Access. There is no support for NW initiated or UE initiated bearer establishment procedures; policy control is performed locally at the PCEF or at the TDF.

If the PCRF provides authorized QoS for both, the IP-CAN session and PCC rule(s), the enforcement of authorized QoS of the individual PCC rules shall take place first.

S.5.5.1 Default QoS Control

The BBF AAA may provide a default Access Profile QoS for the IP-CAN session that may contain QoS information.

The PCRF may provide dynamically the default QoS for the IP-CAN session to the PCEF over Gx or alternatively may provide a default QoS profile name for those cases when the default QoS profile is provisioned in the IP-Edge/PCEF. The PCEF enforces the default QoS or the default QoS profile for the IP-CAN session provisions over Gx. The PCEF does not enforce the default Access Profile QoS provided by BBF AAA for the IP-CAN session if PCRF is deployed.

The default QoS consists of a QCI and MBR.

The IP-Edge/PCEF shall be able to convert default QoS into Fixed Broadband Access QoS attribute values. In the IP-Edge, the QCI and optionally the ARP priority level is used to determine the DSCP code value or other transport specific information element and the MBR is used for bandwidth limitation for the DSCP code value. The PCEF/IP-Edge shall enforce first the QoS for the packets that matches a service data flow template in an installed PCC Rule for which specific QoS enforcement actions are provided then the IP-Edge/PCEF shall enforce the default QoS for all downlink and uplink traffic for the IP-CAN session.

S.6 Functional Entities

The functional entities listed in clause 6.2 apply, except BBERF. Those functional entities that have specific values or specific functionality for Fixed Broadband Access are described in this clause.

NOTE: Support for MPS Services and IMS Emergency is not specified in this Release.

S.6.1 Policy Control and Charging Rules Function (PCRF)

S.6.1.1 General

The PCRF functionality defined in clause 6.2.1.0 shall apply, with the following exceptions:

- No negotiation of IP-CAN bearer establishment mode applies.
- No subscription to changes of IP-CAN type, RAT type or Access Network Information applies to the PCEF.
- No event triggers that the TDF can subscribe to need to be monitored by the PCRF.
- Usage Monitoring Control as defined in clause 6.6 applies with the following exceptions:
  - In the routed RG with NAT mode, the IP-CAN session is per RG in the PCEF/IP-Edge, the PCRF retrieves the usage monitoring related information from the SPR using the subscriber-id provided over Gx. The PCRF decides how to allocate a usage threshold to each existing IP-CAN session and/or MK.
  - In the bridge RG mode and in routed RG mode without NAT there may be a separate fixed subscriber session (i.e. IP-CAN session) for the each device behind the RG. The PCRF retrieves usage monitoring related information from the SPR using the subscriber-id and, if the request is for a 3GPP UE, the NSWO APN provided over Gx. The PCRF decides how to allocate a usage threshold to each existing IP-CAN session and/or Monitoring Key.

S.6.1.1.1 Input for PCC decisions

The PCEF may provide a subset of the information listed in clause 6.2.1.1 with the following fixed broadband specific values:

- Subscriber Identifier in the form of an IMSI, MSISDN for a 3GPP UE or in the form of a user-name or Access Line Identifier (physical and logical circuit ID) for fixed device or RG;
- Location of the subscriber; that may include Access line id (physical and logical circuit ID), SSID of the AP, BSSID of the AP;

NOTE: How the location information becomes available to the PCEF/IPEdge is out of the scope of 3GPP.

- PLMN id of the PCEF located in the IPEdge, if available;
- IPv4/IPv6 address or IPv6 prefix of the UE;
- Type of IP-CAN (i.e. Fixed Broadband Access);
- A PDN ID in the form of the NSWO-APN for a 3GPP UE.

The SPR may provide the information listed in clause 6.2.1.1 for a UE and optionally for NSWO-APN.

The OCS may provide the information listed in clause 6.2.1.1 for a UE.

The TDF may provide the information listed in clause 6.2.1.1 for a UE and optionally for NSWO-APN.

The AF, if involved, may provide the information listed in clause 6.2.1.1 with the following Fixed Broadband Access Specific values:

- Subscriber Identifier;
- IPv4/IPv6 address or IPv6 prefix of the UE.

S.6.1.2 Policy and Charging Enforcement Function (PCEF)

The PCC requirements for the PCEF is located in the Fixed Broadband Access are defined in TR-300 [37]. The PCEF performs the following Fixed Broadband specific functions:

QoS enforcement:

- The PCEF shall be able to convert a QoS parameters sent from PCRF to Fixed Broadband Access to specific QoS attribute and determine the QoS parameters sent to PCRF from the PCEF from a set of Fixed Broadband Access specific QoS attribute.

Application Detection:

- The support of Application Detection functionality is considered a network operator choice in Fixed Broadband Access. If supported, the functionality defined in clause 6.2.2.5 applies.

In addition, the following functions are not supported:

- No UE and/or NW initiated bearer procedures and no enforcement of the authorized QoS for an IP-CAN bearer is supported for Fixed Broadband Access.

S.6.1.3 Application Function (AF)

The AF functionality defined in clause 6.2.3 shall apply, except for the following functionality:

- No subscription to changes of IP-CAN type, RAT type or Access Network Information applies.

S.6.1.4 Subscriber Profile Repository (SPR)

The SPR functionality defined in clause 6.2.4 shall apply. For Fixed Broadband Access the SPR may provide the subscription profile information per subscriber and PDN in case of a 3GPP UE or per subscriber in case of a fixed device or RG:

- Subscriber Identifier in the form of an IMSI, MSISDN for a 3GPP UE or in the form of a user-name or Access Line Identifier (physical and logical circuit ID) for fixed device or RG;
- A PDN ID in the form of the NSWO-APN.

S.6.1.5 Online Charging System (OCS)

The OCS functionality defined in clause 6.2.5 shall apply.

For Fixed Broadband Access the PCEF provides the Subscriber Identifier that may be e.g. IMSI for a 3GPP UE or a user name or Access line identifier for a fixed devices or RG to the OCS. The PCEF or TDF also sends Access line id (physical and logical circuit ID) to the OCS when the subscriber ID identifies a 3GPP UE or a fixed device behind the RG.

NOTE: 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.

S.6.1.6 Offline Charging System (OFCS)

The OCS functionality defined in clause 6.2.6 shall apply.

For Fixed Broadband Access the PCEF provides the Subscriber Identifier that may be e.g. IMSI for a 3GPP UE or a user name or Access line identifier for a fixed devices or RG to the OFCS. The PCEF or TDF also sends Access line id (physical and logical circuit ID) to the OFCS when the subscriber ID identifies a 3GPP UE or a fixed device behind the RG.

NOTE: 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.

S.6.1.7 User Data Repository (UDR)

The SPR data listed in clause 6.2.3 are stored in the UDR, the subscriber identifier and the PDN ID defined in S.6.1.4 applies.

S.6.1.8 Traffic Detection Function (TDF)

The TDF functionality defined in clause 6.2.9 shall apply. For Fixed Broadband Access, the TDF does not subscribe to event triggers indication from the PCRF at any IP-CAN session procedure.

S.7 PCC Procedures and Flows

S.7.1 Introduction

A "Fixed Broadband Access IP-CAN" is a fixed access broadband network that provides IP connectivity to a UE. The Fixed Broadband Access IP-CAN reuses the definition of an IP-CAN session in this specification.

The AF can provide the NATed IP address and ports used by the UE (for IMS, according to TS 23.228 [39]).

NOTE: When the above condition is not met, there are no standardized means as for now to identify a UE behind a NATed-RG.

The Fixed Broadband Access network does not support the concept of a bearer and multiple bearers as defined in TS 23.401 [17]. However, DSCP marking provides QoS support on transport network layer so that QoS and charging policies can be applied per SDF.

Case 1, no Gateway Control Session applies for Fixed Broadband Access.

The procedures cover both non-roaming and roaming with access to NSWO APN for a 3GPP UE. For the roaming case with access to NSWO APN, the V PCRF interacts with the IP-Edge PCEF and, if Sd applies, with the TDF.

S.7.2 IP-CAN Session Establishment

The PCEF located in the IP-Edge initiates the Gx IP-CAN Session establishment as defined in clause 7.2. The session is initiated after that the IP-Edge becomes aware of an IPv4 address and/or an IPv6 prefix has been assigned to the fixed device and/or 3GPP UE.

In route mode configuration with NATed RG, the session is initiated after the RG has been connected to the network and has been assigned an IPv4 address and/or IPv6 Prefix. The IPv4 address and/or IPv6 Prefix are assigned as per Broadband Forum specifications and it is out of scope of 3GPP.

In bridge mode, the session is initiated after the device has been authenticated has been assigned an IPv4 address and/or IPv6 address or IPv6 Prefix by the Fixed Broadband access.

Operator policies in the PCEF indicate if dynamic policy control is provided. In addition, the NSWO-APN is also configured for subscribers on a PLMN basis.

The PCEF located in the IP-Edge includes in the IP-CAN Session establishment message the Subscriber-Id, NSWO-APN if available, IP-CAN type, the Default QoS if available, the PLMN id if available and the location information as defined in S.6.1.1.1.

The IP-Edge maps the Default-Access-Profile QoS to Default-QoS as defined in clause S.5.5.1.

The PCRF may provision a Default QoS or a Default QoS profile, PCC Rules to activate and Events Triggers to report.

S.7.3 IP-CAN Session Termination

This procedure is in accordance with clause 7.3.2 with the exceptions listed in this Annex. The UE-initiated IP-CAN session termination is not to applicable to Fixed Broadband Access.

The IP-CAN session termination is triggered by PCEF when Subscriber IP session is terminated. The trigger to terminate the Subscriber IP session may be HSS/AAA request to detach the UE or may be Broadband Forum specific (e.g. RG switch off, loss of transmission, IP address lease expiration PPPoE session termination, etc) and out of the scope of 3GPP.

In routed mode configuration with NAT this procedure is applicable only when IP session from RG is terminated, e.g. when RG switches off or when public IP address assigned to the RG is released, etc.

NOTE: In routed mode with NAT, the termination of connection from a device in LAN, e.g. when device releases the local IP address or it disconnects from WLAN does not trigger the IP-CAN session termination for IP session from RG.

S.7.4 IP-CAN Session Modification

S.7.4.1 PCEF-Initiated IP-CAN Session Modification

This clause is related to IP-CAN session modification initiated by IP-Edge/PCEF for IP session. This procedure is in accordance with clause 7.4.1 with the exceptions listed in this Annex.

In routed mode with NAT, this procedure can be triggered when new device connects to the RG, for example when UE requests a local IP address to the RG or when a UE disconnects from WLAN.

The IP-Edge reports that an Event was met, including the Event Trigger and the affected PCC Rule. If TDF applies, the PCRF may provide ADC Rules and Event Triggers to the TDF and may provide PCC Rule, Event Triggers and a Default QoS or a Default QoS profile to PCEF.

S.7.4.2 PCRF-Initiated IP-CAN Session Modification

This procedure is in accordance with clause 7.4.2 with the exceptions listed in this Annex.

The PCRF may also provide a Default QoS or a Default QoS profile to PCEF.

S.7.5 Update of the subscription information in the PCRF

This procedure is in accordance with clause 7.5.when the UE's (i.e. RG, fixed device or 3GPP UE) profile changes.

S.7.6 PCRF Discovery and selection

PCRF discovery and selection follows the principles defined in clause 7.6 with the following modification:

- The Subscriber ID specified in clause S.5.1.2 is used as user identity.
- For a 3GPP UE, the NSWO-APN is also available.
- The IPv6 address may be included in the IP-CAN session establishment in the case of bridge-mode RG.

S.8 Charging using AAA signalling

The architecture shall provide charging for traffic exchanged by fixed devices and NSWO traffic to/from 3GPP UEs using AAA signalling.

In this release in case of AAA-based charging the BBF AAA server is used for performing accounting of fixed device as defined by BBF specifications TR-101 [35] and TR-146 [36].

NOTE: The AAA-based accounting for fixed device is not applicable in roaming scenario.

For the charging session over Gya and Gza, the user identifier is the same that is issued over the Gx session

S.8.1 Reference architecture - Non-Roaming

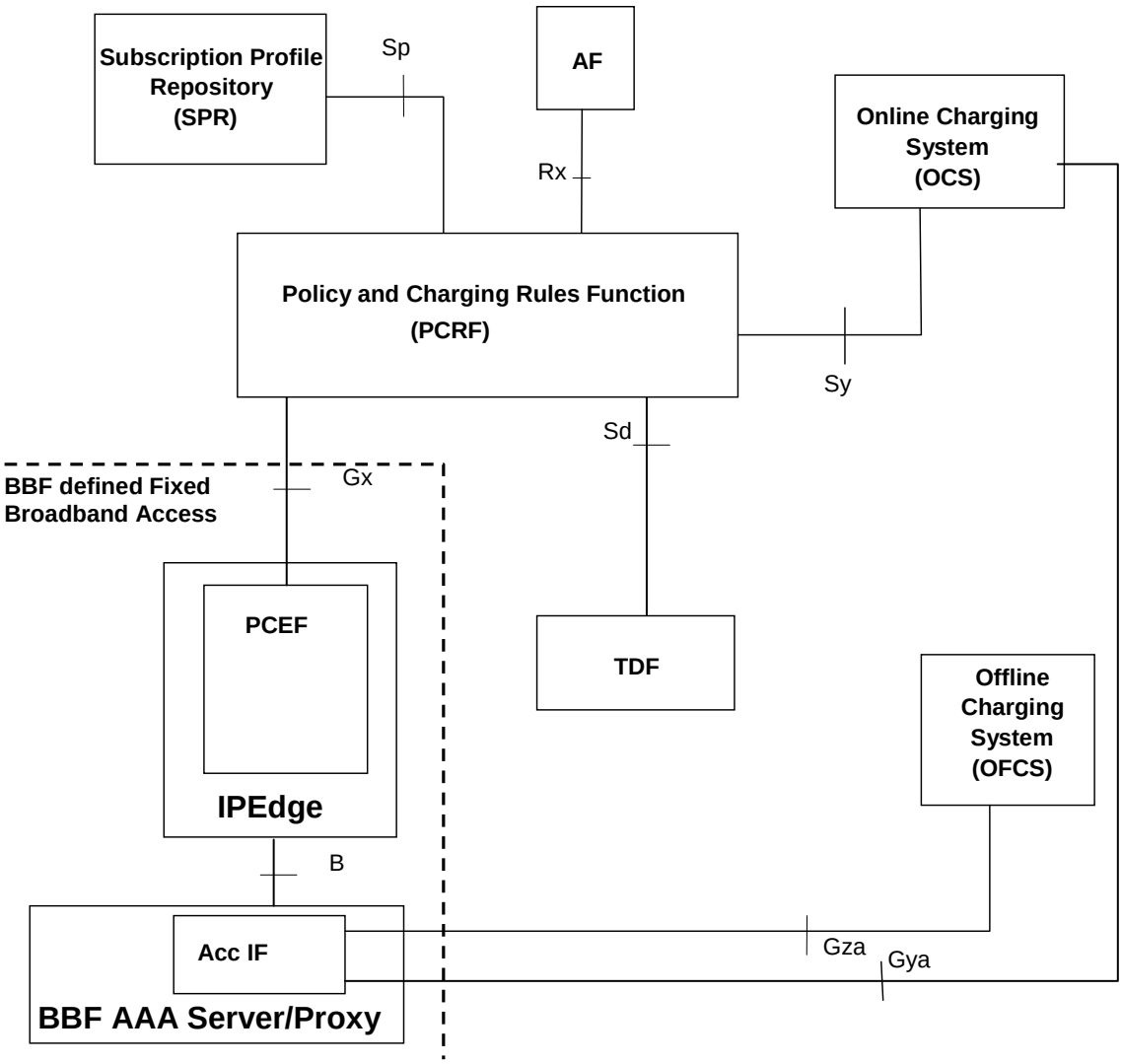

Figure S.8.1: PCC Reference architecture for Fixed Broadband Access convergence when AAA-based accounting is used

S.8.2 Reference architecture - Roaming

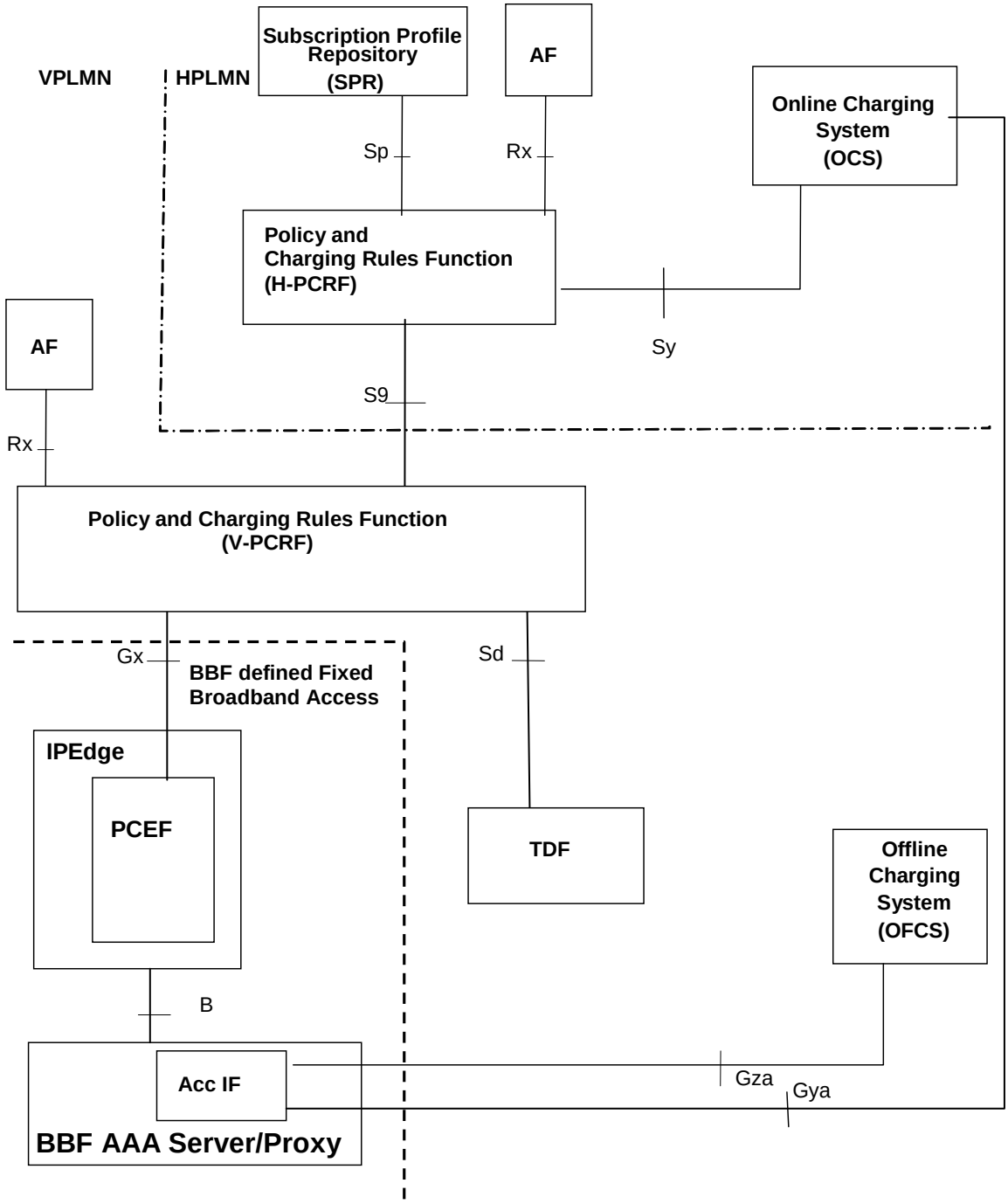

Figure S.8.2: PCC Reference architecture for Fixed Broadband Access convergence (roaming) when AAA-based accounting is used

S.8.3 Gza Reference Point

To transport charging information about 3GPP UE, the Gza reference point is located between Accounting Interworking function in the BBF defined network and the 3GPP offline charging system OFCS located in the VPLMN (roaming scenario) or in the HPLMN (non-roaming scenario).

To transport charging information about fixed devices, the Gza reference point is located between the Accounting Interworking function in the BBF defined network and the 3GPP offline charging system located in the HPLMN (only non-roaming scenario).

NOTE: The detailed definition of Gza reference point and diagram flows for supporting AAA-based charging is outside the scope of this specification. See SA WG5 specifications for further details.

S.8.4 Gya Reference Point

The Gya reference point is located between the Accounting Interworking function in the BBF defined Access Network and the 3GPP online charging system OCS located in the HPLMN and it transports charging information for 3GPP UE.

The Gya reference point is located between the Accounting Interworking function in the BBF defined Access Network and the 3GPP online charging system located in the HPLMN and it transports charging information for fixed device.

NOTE: The definition of Gya reference point and diagram flows for supporting AAA-based charging is outside the scope of this specification. See SA WG5 specifications for further details.

S.8.5 B Reference Point

This reference point is defined in BBF TR-300 [37].

NOTE: The definition of this reference point is out of the scope of 3GPP.

S.8.6 AAA based charging

The charging support for NSWO traffic for 3GPP UE and fixed devices can be provided when the BBF network reports per-user accounting data via B and Gya/Gza reference points.

Offline and online charging may be supported by the 3GPP and BBF domain. In this Release, in case of AAA-based charging, the Online charging is supported based on existing capability supported by B reference point and IP-Edge with limitation based on AAA RADIUS/Diameter accounting in the BBF network (e.g. BNG capability, usage of RADIUS over B reference point).

For RG in routed mode configuration with NAT, the single devices (i.e. fixed device and 3GPP UE) connected behind a RG can not be recognised, so the accounting is performed only for the RG.

In case of RG bridge mode configuration and in routed mode configuration without NAT the AAA based charging is performed per single devices having a Subscriber IP session.

In order to allow performing charging for fixed devices, the following assumptions are made about functionality in the Fixed Broadband Network:

- The BBF network is able to collect per user accounting data for fixed devices and periodically report this data via the B reference point.

S.8.7 Accounting Interworking Function

The Accounting Interworking Function that performs translation of the accounting signalling and parameters that are understood by the IP-Edge into the credit management signalling and parameters that are understood by the OCS and the OFCS is defined in BBF TR-300 [37].

S.8.8 Procedures AAA based charging using accounting signalling

S.8.8.0 General

This clause describes the AAA-based charging. The basic assumption is that B interface is not modified.

S.8.8.1 Charging Session Initiation

This procedure is performed for initiation of charging session

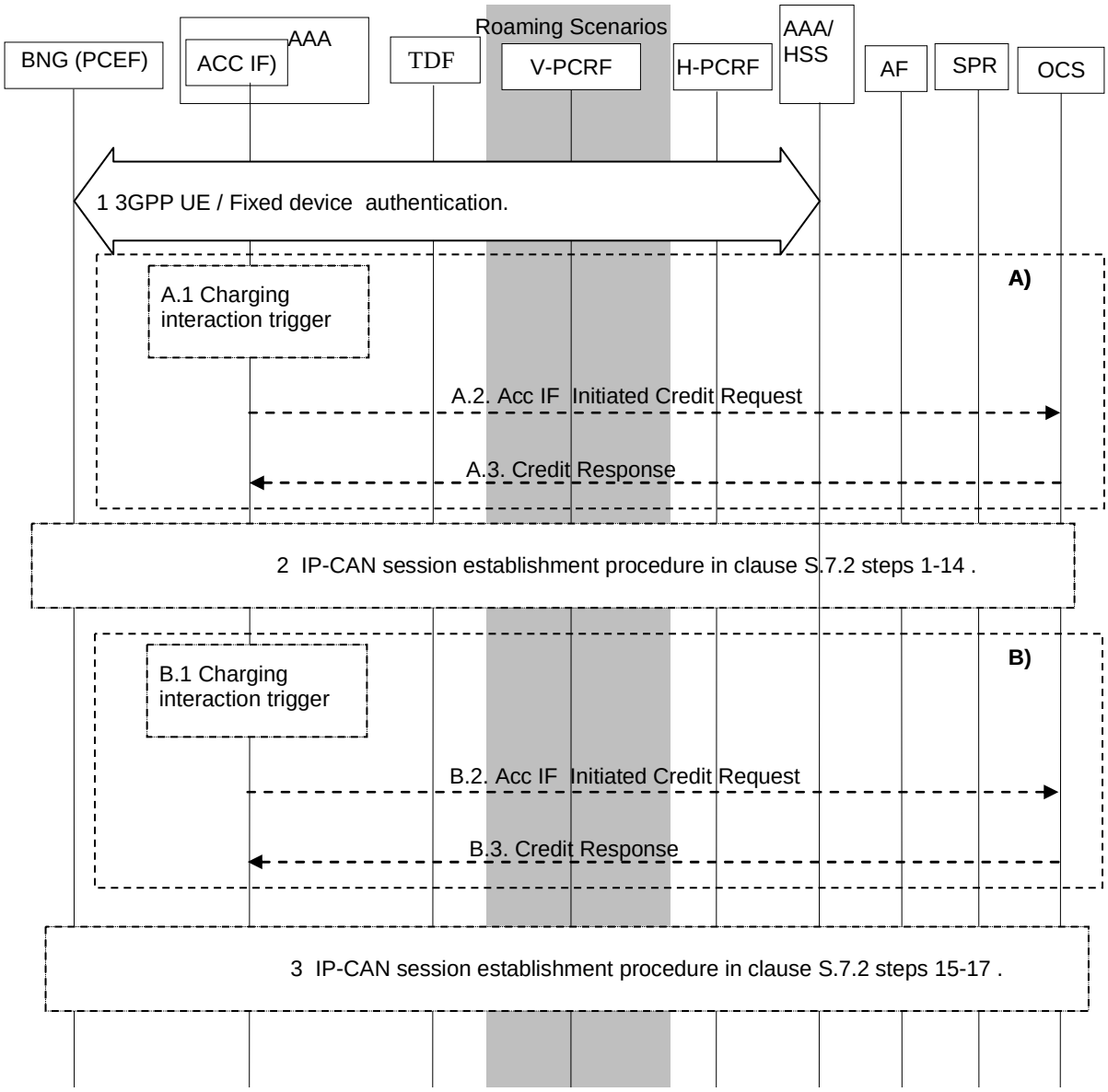

Figure S.8.8.1: AAA-based Charging Session Initiation

The steps included in Block A and B are mutually exclusive.

1. The 3GPP UE EAP-based authentication or BBF Fixed device authentication is performed.

NOTE 1: Authentication for fixed device is out of the scope of 3GPP specifications.

A.1 If AAA-based accounting applies, the 3GPP UE/BBF device is successfully authenticated and this triggers the interaction with the OCS system. This step is outside the 3GPP scope.

A.2. The Accounting Interworking Function that will activate the online-charging session, and provide relevant input information for the OCS decision. i.e. subscriber identifier and charging keys obtained in step A.1.

A.3. If online charging is applicable, the OCS provides the possible credit information to the Accounting Interworking Function and may provide re-authorisation triggers for each of the credits.

NOTE 2: The Only Credit Reauthorization triggers that can be reported are "Credit Reauthorization time expired".

2. If PCC is supported, the IP-CAN session establishment procedure may be established as define in clause S.7.2. The steps from 1 to 14 defined in clause 7.2 are performed with the following exception:

   - Steps 9 - 10 are performed only if TDF based accounting is supported and AAA-based accounting is not supported.

   - Steps 13 - 14 are performed only if PCEF accounting is supported and AAA-based accounting is not supported.

B.1. If AAA-based accounting applies, the start of accounting session is triggered in BBF AAA. This step is out of the scope of 3GPP specifications.

NOTE 3: This step may occur anytime in parallel to steps from 1 to 14 of clause 7.2

B.2. The same step as step A.1

B.3. The same step as step A.2

3 The IP-CAN session establishment as defined in clause 7.2 steps from 15 to 17 are performed.

S.8.8.2 Charging Session Modification

This procedure is performed for updating the charging information, such as the available quota.

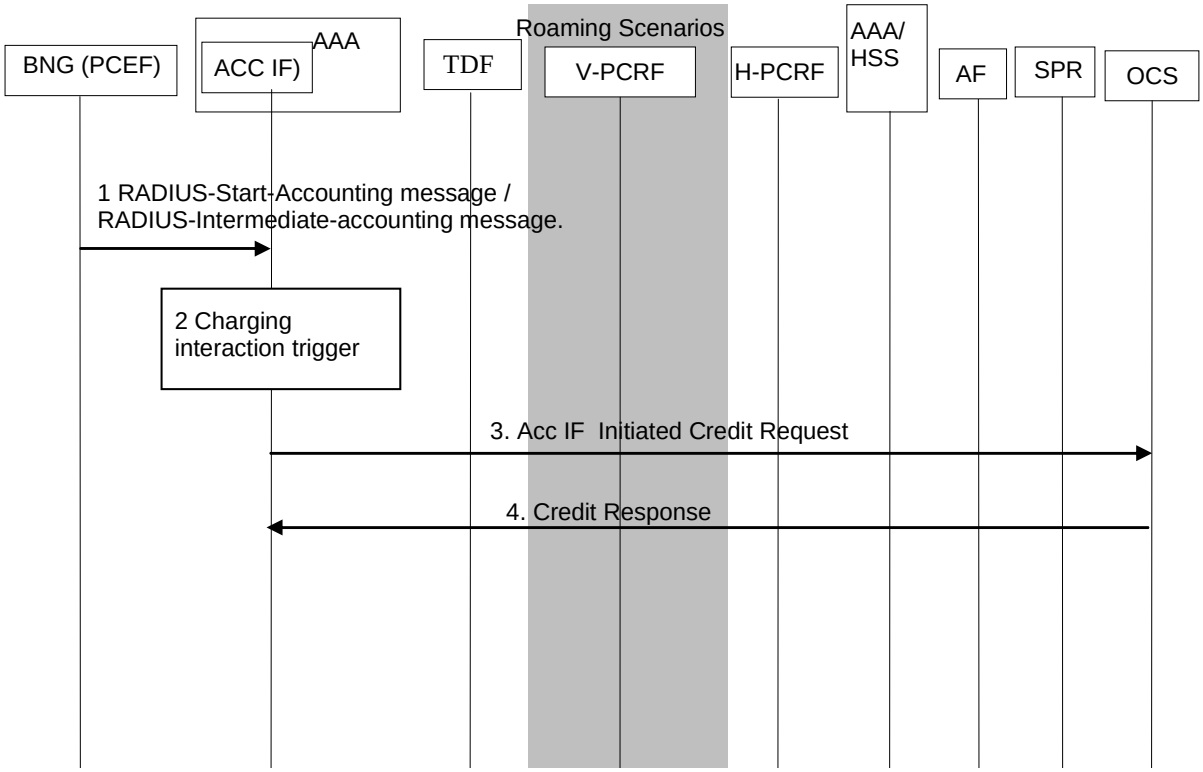

Figure S.8.8.2: AAA-based Charging Session modification

1. The BNG can sent a RADIUS-Start accounting message or a RADIUS-Intermediate-Accounting message.

2 When the Accounting Interworking Function receives the message, it determines if it is required to update the accounting information which triggers an interaction with the OCS.

3. The Accounting Interworking Function may contact the OCS to request credit for new charging keys and/or to issue final report and return remaining credit for charging keys no longer active, i.e. when the accounting session is terminated.

4. The OCS may instruct the Accounting Interworking Function on the further handling of the session (terminate, continue, etc), provide credit information (possibly with re-authorisation trigger), and/or acknowledge the credit report.

S.8.8.3 Charging Session Termination

S.8.8.3.1 Charging Session Termination BNG-initiated

This procedure is performed when BNG send a stop accounting message to the Accounting Interworking Function, for example the IP-CAN session termination procedure is initiated by PCRF or when Subscriber IP session terminated (for example when the 3GPP UE disassociates from the fixed broadband network, the RG is switched off, etc.).

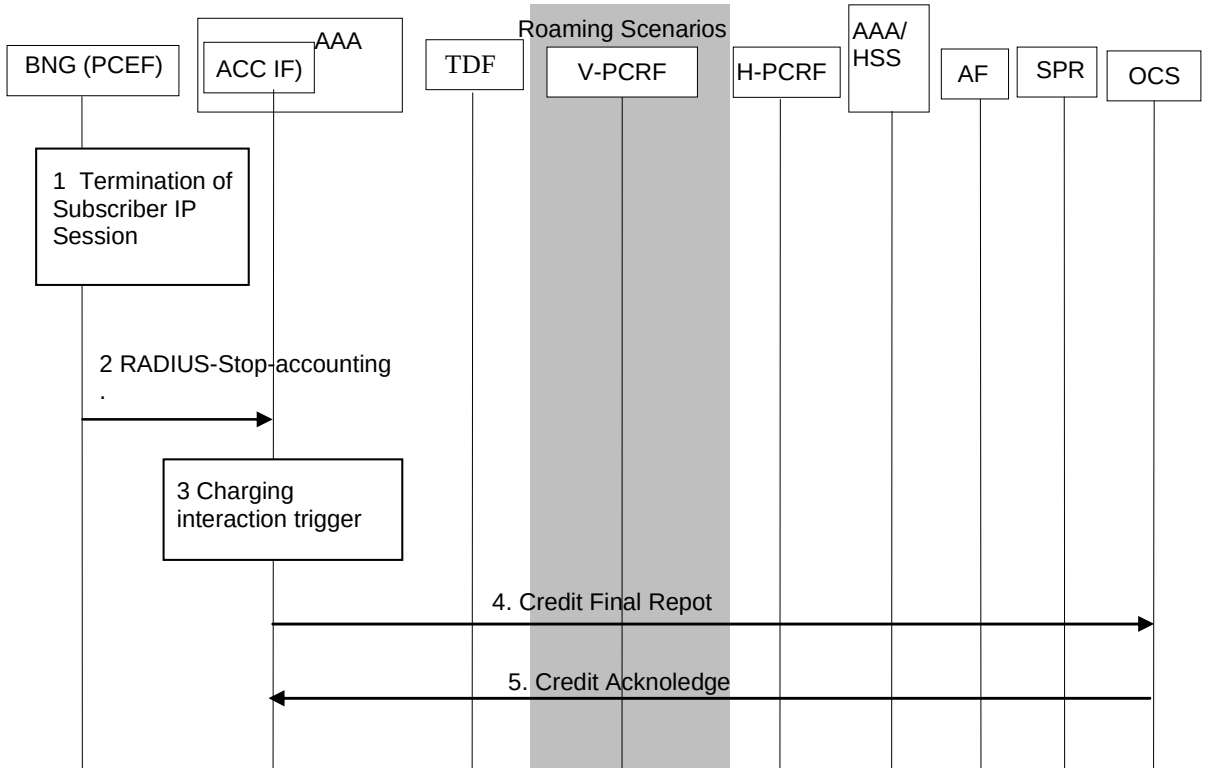

Figure S.8.8.3.1-1: AAA-based Charging Session Termination

1. The BNG determines that the Subscriber IP session is terminated (e.g. the device has left the fixed broadband network) and consequently a PCEF-Initiated IP-CAN session termination is initiated or it shall be terminated, when PCRF-Initiated IP-CAN session termination procedure is performed.

2. The BNG send a RADIUS-Stop-accounting message to the ACC_If. This step is outside the scope of 3GPP specifications.

3 The Accounting Interworking Function determines that the Accounting Session shall be terminated.

4. The Accounting Interworking Function shall issue the final reports and return the remaining credit to the OCS.

5. The OCS acknowledges the credit report and terminates the online charging session.

Annex T (informative): How to accumulate PCC/ADC Rule usage in multiple monitoring groups

If usage for a PCC/ADC rule is accumulated in multiple Monitoring Groups, the following solution re-uses the capabilities defined in the main body of this specification, the steps are described below:

1. The PCRF retrieves the total group allowance for the Monitoring Group and the set of services belonging to the Monitoring Group from the SPR.

2. For dynamic PCC/ADC Rules, the PCRF selects a Monitoring Key for those services that belongs to more than one Monitoring Group but does not have an individual Monitoring Key assigned.

3. For pre-configured PCC/ADC Rules the PCRF selects the PCC/ADC Rules for each of the services that belong to the monitoring group. For pre-configured PCC/ADC Rules, the PCEF is configured with an individual Monitoring Key that monitors the usage.

4. The PCRF calculates a usage threshold for each of these Monitoring Keys taking into account the minimum of the individual service allowance and the monitoring group allowance(s) the service belongs to.

5. The PCRF installs or activates the PCC/ADC Rule. The PCRF provides a usage threshold for each Monitoring Key.

6. When the PCRF receives a usage report for a Monitoring Key from the requested node (PCEF or TDF), the PCRF shall deduct the value from the corresponding group allowances and from the individual allowance if needed.

7. As long as all group usage allowances are not reached, the PCRF calculates a new usage threshold for the Monitoring Key based on the corresponding group allowances the service belongs to.

Annex U (normative): Policy and charging control in the downlink direction for traffic marked with DSCP by the TDF

In order to provide policy and charging control (e.g. QoS enforcement) in the downlink direction for applications with non-deducible service data flows detected by the TDF, in addition to the solution described in clause 4.5, the following solution is defined:

The TDF shall be able to mark detected downlink application traffic with a DSCP value received within an installed ADC Rule matching this traffic.

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.

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.

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.

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 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.

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.

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 -deducible 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.

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.

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

With the Proximity-based services, in accordance with TS 23.303 [44], a UE acting as a Remote UE can connect to a PDN via a ProSe UE-to-Network Relay UE, using an IP-CAN session that the Relay UE has established.

The Relay UE is assigned an IPv6 prefix that is shorter than /64.

The PCRF does not get any Remote UE identity and is not required to be aware of the Remote UE but is expected to validate Remote UE related service information from the AF and generate any necessary PCC rules according to standard procedures already defined. PCC rule authorizations may be static (e.g. predefined PCC rules) or rely on AF provided service information.

An AF serving a remote UE reaches the appropriate PCRF based on the IPv6 prefix that the UE-to-Network Relay UE has assigned to the remote UE. The AF reaches the appropriate PCRF by performing a PLMN lookup for the IPv6 prefix and using the Network Realm/Domain, as defined in TS 23.003 [16], associated with the PLMN.

In order to make a PCC rule specific for a certain Remote UE, the SDF filters used for traffic detection need to include the attribute Local Address and Mask with a value that corresponds to the Remote UE only. The value is normally an IPv6 prefix that is longer than the prefix assigned for the IP-CAN session (i.e. for the ProSe UE-to-Network Relay UE).

Annex W (informative): Void

Annex X (informative): Encrypted traffic detection by using domain name matching

For the cases when it is required to detect and enforce/charge sponsored services within encrypted traffic, and those sponsored services are uniquely identifiable by a list of {IP address ranges, domain name matching strings, match type (absolute/suffix)} set, while either element in the pair of {IP address ranges, domain name matching strings} can be "any", as applicable, but not both elements simultaneously, the domain name matching solution described below may be used.

NOTE 1: L3 information (IP address ranges) is visible even if traffic is encrypted.

The following assumptions apply for the solution:

- There exists an agreement between the operator and sponsored data connectivity content provider.
- Content provider uses HTTPS as a transport mechanism, using Web Public Key Infrastructure (PKI).

The set of information {IP address ranges, domain name matching strings, match type (absolute/suffix)} required to identify encrypted traffic is defined in the PCEF/TDF either by using pre-defined PCC/ADC Rules or by using dynamic PCC/ADC Rules that include Application Identifiers, as applicable. The detection logic to which Application Identifier in the PCEF/TDF refers to, is extended to cover ({IP address ranges, domain name matching strings, match type (absolute/suffix)} information. If such a pre-defined or dynamic PCC/ADC Rule is active for an IP-CAN/TDF session, the PCEF/TDF shall check IP address ranges, and, in case of compliancy with the received/preconfigured value (see note 2), match domain name strings, either absolutely or by suffix, against the following fields in the initial HTTPS handshake:

- TLS Server Name Indication (SNI) extension, when available (see [47]); or, if not available.
- Server certificate's Subject Alternative Name x.509 extension DNS name, when available. All relevant values shall be examined for matching; or if not available or no match was found.
- Server certificate's Subject Common Name (CN).

NOTE 2: If the IP address ranges equals "Any", then any traffic is said to be compliant.

The information required for the detection of sponsored HTTPS (i.e. defined in Annex X to be pre-configured in the PCEF/TDF and either the TLS SNI extension or the Server certificate´s Subject Alternative Name x.509 DNS name or Server certificate´s Subject CN) is verified with the corresponding server IP address/prefix of the IP packets by the PCEF/TDF. The PCEF/TDF uses implementation specific logic to perform this verification.

Annex Y (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2014-06	SP-64	SP-140273	0885	5	B	PCC Rules sharing resources	**13.0.0**
2014-06	SP-64	SP-140383	0885	6	B	PCC Rules sharing resources MCC Update to use correct approved revision of the Rel-13 CR.	**13.0.1**
2014-09	SP-65	SP-140428	0896	2	B	Addition of RAN user plane congestion handling feature into the specification	13.1.0
2014-09	SP-65	SP-140428	0897	2	B	Np reporting restrictions	13.1.0
2014-09	SP-65	SP-140428	0899	2	B	Aggregation of Np messages	13.1.0
2014-09	SP-65	SP-140421	0907	2	A	Clarifications for PRA reporting	13.1.0
2014-09	SP-65	SP-140431	0908	2	F	Clarification of resource sharing for different Rx sessions	13.1.0
2014-09	SP-65	SP-140441	0914	-	A	QCI values for Public Safety services	13.1.0
2014-12	SP-66	SP-140674	0904	3	A	Clarifications for TFT handling	13.2.0
2014-12	SP-66	SP-140689	0915	-	C	Applicability of congestion information reporting for certain APNs only	13.2.0
2014-12	SP-66	SP-140689	0916	2	F	Clarifying details of deferred services	13.2.0
2014-12	SP-66	SP-140671	0920	2	A	Support for IPv6 prefix retrieve by the HSGW during the eHRPD pre-registration procedure	13.2.0
2014-12	SP-66	SP-140694	0921	3	B	Introducing the feature of excluding Usage of a Service/Application from IP-CAN session/TDF session Usage into the specification	13.2.0
2014-12	SP-66	SP-140690	0922	2	B	Indication to share resources in the UL or DL or both directions	13.2.0
2014-12	SP-66	SP-140685	0924	4	A	Charging correlation identifier for the IP-CAN session	13.2.0
2014-12	SP-66	SP-140694	0925	1	D	New Annex: Monitor service usage in multiple groups	13.2.0
2014-12	SP-66	SP-140689	0926	3	C	Np mobility handling	13.2.0
2014-12	SP-66	SP-140689	0927	-	C	Resolution of Editor's note on bandwidth limitation.	13.2.0
2014-12	SP-66	SP-140678	0930	2	A	QoS handling at inter-RAT mobility	13.2.0
2014-12	SP-66	SP-140668	0939	1	A	Correct Reference to 3GPP2 X.S0057	13.2.0
2014-12	SP-66	SP-140678	0946	2	A	Correction to Delay Budget for first packets in a data burst	13.2.0
2014-12	SP-66	SP-140689	0950	2	F	Transfer of location information on Np	13.2.0
2014-12	SP-66	SP-140689	0952	-	F	Removal of Editor Note on logical PCRF id	13.2.0
2014-12	SP-66	SP-140693	0953	3	C	TDF support for downlink's bearer selection and bearer binding procedures	13.2.0
2014-12	SP-66	SP-140686	0955	2	A	Proposal to solve the discussion on how QoS change of default bearer affects PCC Rules bound to the default bearer	13.2.0
2014-12	SP-66	SP-140693	0958	3	B	Activate PCC function per UE based on subscription information	13.2.0
2014-12	SP-66	SP-140689	0961	2	F	Clarifying reporting of no congestion state	13.2.0
2014-12	SP-66	SP-140693	0963	2	B	TWAN release cause for Trusted WLAN	13.2.0
2014-12	SP-66	SP-140679	0964	-	F	Stage 3 alignment for Fixed Broadband Access	13.2.0
2015-03	SP-67	SP-150027	0966	3	B	Removing restrictions to report RAT type to the AF	13.3.0
2015-03	SP-67	SP-150027	0968	1	B	Activate PCC function per UE based on subscription information when BBERF is deployed	13.3.0
2015-03	SP-67	SP-150109	0971	1	A	Correction to support of I-WLAN in TS 23.203	13.3.0
2015-06	SP-68	SP-150230	0905	6	A	Priority of Default Bearer	13.4.0
2015-06	SP-68	SP-150230	0941	5	A	Clarifications for QoS change of default bearer	13.4.0
2015-06	SP-68	SP-150235	0975	2	B	Resource management for background data transfer via Rx	13.4.0
2015-06	SP-68	SP-150232	0976	3	F	Configuring AF application identifier value in PCRF to avoid SRVCC	13.4.0
2015-06	SP-68	SP-150239	0977	1	F	Session/bearer release cause over S2b	13.4.0
2015-06	SP-68	SP-150231	0978	2	F	Alignment of RUCI reporting restrictions' basis for UPCON	13.4.0
2015-09	SP-69	SP-150492	0980	3	B	Introduction of Flexible Mobile Service Steering feature into PCC architecture	13.5.0
2015-09	SP-69	SP-150498	0981	1	F	Adding Nt reference point to architecture	13.5.0
2015-09	SP-69	SP-150503	0985	2	B	Location to Support Emergency services over WLAN access to EPC	13.5.0
2015-09	SP-69	SP-150497	0986	3	B	PCC Support of NBIFOM	13.5.0
2015-09	SP-69	SP-150491	0988	1	A	Clarifications for PCC rule actions	13.5.0
2015-09	SP-69	SP-150492	0989	3	B	Update the architecture to support the FMSS for EPC-routed scenario	13.5.0
2015-09	SP-69	SP-150492	0990	4	B	Definition of Traffic Steering Control Information	13.5.0
2015-09	SP-69	SP-150505	0991	2	F	Removal of OCS proxy in LBO roaming scenario	13.5.0
2015-09	SP-69	SP-150492	0992	3	B	High level requirement and function description of FMSS	13.5.0
2015-09	SP-69	SP-150500	0994	1	F	Addition of resource sharing indication	13.5.0
2015-09	SP-69	SP-150492	0995	3	B	PCC architecture enhancement for traffic steering using St and TSSF	13.5.0
2015-09	SP-69	SP-150550	0983	4	B	PCC Procedures and Flows including Traffic Steering	13.5.0
2015-09	-	-	-	-	-	MCC correction to implementation of CR0986R3	13.5.1
2015-12	SP-70	SP-150604	1000	3	B	Policy Control for remote UE behind relay UE	13.6.0
2015-12	SP-70	SP-150607	1002	3	F	Bearer binding, usage monitoring and other impacts due to NBIFOM	13.6.0
2015-12	SP-70	SP-150608	1004	1	F	Clarify Nt Reference Point	13.6.0
2015-12	SP-70	SP-150614	1006	1	F	Update of the PCC rules during the addition of an access procedure	13.6.0
2015-12	SP-70	SP-150617	1007	1	F	Conveying to the EPC the IMEI of devices accessing a trusted or untrusted WLAN	13.6.0

2015-12	SP-70	SP-150613	1008	1	F	Transfer of User Location Information at Create Session Request over S2b	13.6.0
2015-12	SP-70	SP-150600	1012	-	A	Correction of definition of QCI 65, 66, 69 and 70	13.6.0
2016-03	SP-71	SP-160162	1009	7	B	APN AMBR change at a certain time on Gx	13.7.0
2016-03	SP-71	SP-160162	1018	2	F	Bitrate variations	13.7.0
2016-06	SP-72	SP-160298	1013	7	C	Priority sharing for concurrent sessions	13.8.0
2016-06	SP-72	SP-160294	1021	1	F	Clarification of the decision of NBIFOM mode	13.8.0
2016-06	SP-72	SP-160291	1023	1	F	Transfer of traffic steering policy control information for TSSF	13.8.0
2016-06	SP-72	SP-160291	1026	-	F	Corrections to FMSS related descriptions	13.8.0
2016-06	SP-72	SP-160287	1029	2	B	Update of 23.203 for CIoT	13.8.0
2016-06	SP-72	SP-160294	1030	2	F	Clarifications and Corrections for NBIFOM	13.8.0
2016-06	SP-72	SP-160304	1022	2	B	Subscription to notification of PLMN id change over Rx	**14.0.0**
2016-09	SP-73	SP-160653	1025	3	B	Reporting entering or leaving a set of PRAs	14.1.0
2016-09	SP-73	SP-160653	1031	9	B	Support of Multiple PRAs	14.1.0
2016-09	SP-73	SP-160655	1032	-	C	Support of sponsored data connectivity for TDF	14.1.0
2016-09	SP-73	SP-160655	1033	5	B	Encrypted traffic detection by using domain name matching	14.1.0
2016-09	SP-73	SP-160645	1034	4	C	Support of traffic steering control for 3rd party service function	14.1.0
2016-09	SP-73	SP-160651	1035	3	B	Provision of EPC-level identities for IMS emergency sessions over Rx	14.1.0
2016-09	SP-73	SP-160655	1036	7	B	Management of PFDs to PCEF/TDF	14.1.0
2016-09	SP-73	SP-160644	1037	1	A	Provisioning of the Source port and ePDG IP address	14.1.0
2016-09	SP-73	SP-160641	1039	1	A	Setting the RR identifier alignment with stage 3	14.1.0
2016-09	SP-73	SP-160655	1041	3	B	Architecture enhancement to support SDCI	14.1.0
2016-09	SP-73	SP-160655	1043	6	B	PFD retrieval and the procedures for sponsored data connectivity enhancement	14.1.0
2016-09	SP-73	SP-160641	1045	3	A	Details of PCEF Routing Rule operations	14.1.0
2016-09	SP-73	SP-160638	1050	2	A	Extending the IE for application detection within the ADC Rules	14.1.0
2016-09	SP-73	SP-160655	1051	3	B	Sponsored HTTP traffic detection by using domain name matching	14.1.0
2016-09	SP-73	SP-160658	1052	1	B	Adding ENODEB_CHANGE event trigger	14.1.0
2016-09	SP-73	SP-160655	1053	3	B	Rx enhancement for SDCI	14.1.0
2016-09	SP-73	SP-160646	1058	2	B	New QCI values for V2X services	14.1.0
2016-09	SP-73	SP-160658	1060	2	B	Predictable pre-emption of media flows	14.1.0
2016-09	SP-73	SP-160638	1066	2	A	Overlapping IP Addresses with FMSS	14.1.0
2016-12	SP-74	SP-160812	1070	1	A	Remove "same media type" requirement for Priority Sharing	14.2.0
2016-12	SP-74	SP-160818	1071	3	F	Modification of PRA information over Gx reference point	14.2.0
2016-12	SP-74	SP-160826	1076	4	B	Introduction of 3GPP PS Data Off	14.2.0
2016-12	SP-74	SP-160818	1077	3	F	Corrections on the usage of set of PRA	14.2.0
2016-12	SP-74	SP-160818	1079	1	F	Configuration of multiple PRAs	14.2.0
2016-12	SP-74	SP-160908	1073	3	C	Service input for the setting of the ARP-PCI and ARP-PVI	14.2.0
2016-12	SP-74	SP-160921	1068	5	C	Deferred default EPS bearer QCI and ARP change	14.2.0
2017-03	SP-75	SP-170052	1081	1	C	TS 23.203 support for transport level packet marking	14.3.0
2017-06	SP-76	SP-170370	1082	3	F	Updating the description of 3GPP PS Data Off feature	14.4.0
2017-06	SP-76	SP-170368	1086	7	F	Clarification of caching time	14.4.0
2017-06	SP-76	SP-170368	1090	2	F	Corrections to handling of partial and full updates	14.4.0
2017-09	SP-77	SP-170719	1093	1	F	Correction to event trigger Data Off Change	14.5.0
2017-09	SP-77	SP-170720	1094	2	F	Corrections to PFD removal	14.5.0
2017-09	SP-77	SP-170732	1092	2	C	Enhancement on Sy reference point	**15.0.0**
2017-09	SP-77	SP-170729	1099	2	C	23.203 PCEF Support for Data Off phase 2	**15.0.0**
2017-12	SP-78	SP-170921	1106	3	C	Support for Unsynchronized lists	15.1.0
2017-12	SP-78	SP-170926	1107	5	B	Enhanced VoLTE performance CR for TS 23.203	15.1.0
2017-12	SP-78	SP-170924	1110	3	C	Use of ARP priority level in addition to QCI for packet handling	15.1.0
2017-12	SP-78	SP-170929	1111	2	C	Extension on QCI for MC Video	15.1.0
2017-12	SP-78	SP-170920	1112	4	B	Introduction of new QCIs for low latency with normal reliability requirements	15.1.0
2017-12	SP-78	SP-170924	1113	2	F	Clarify MBMS and other use of PCC/QoS specification	15.1.0
2018-03	SP-79	SP-180110	1116	1	C	QCIs for URLLC	15.2.0
2018-06	SP-80	SP-180472	1119	4	A	Application detection report when the PFDs are removed	15.3.0
2018-06	SP-80	SP-180496	1120	5	F	Policy update when UE is suspended	15.3.0
2018-06	SP-80	SP-180494	1121	-	F	Updates to URLLC QCIs to align with SA1's updated requirements	15.3.0
2018-09	SP-81	SP-180726	1122	1	F	Corrections for low latency QCIs	15.4.0
2018-09	SP-81	SP-180729	1123	1	F	Removal of incorrect definition of WB-E-UTRAN	15.4.0
2019-03	SP-83	SP-190175	1124	3	C	New QCIs for Enhanced Framework for Uplink Streaming	**16.0.0**
2019-03	SP-83	SP-190163	1125	2	B	Support for Restricted Local Operator Services in 23.203	16.0.0
2019-06	SP-84	SP-190404	1127	2	A	Multiple PFD filters, alignment with stage 3	16.1.0
2019-12	SP-86	SP-191089	1130	1	F	Aligning TS 23.203 with the CHEM feature of SA4	16.2.0
2021-03	SP-91E	SP-210085	1133	1	B	Multimedia Priority Service (MPS) Phase 2 support for Data Transport Service	**17.0.0**
2021-06	SP-92E	SP-210361	1134	1	F	Multimedia Priority Service (MPS) Phase 2 support for Data Transport Service	17.1.0
2021-06	SP-92E	SP-210361	1135	1	B	Additional authorization functionality in support of MPS for Data Transport Service	17.1.0
2021-12	SP-94E	SP-211284	1136	2	B	Support policy and QoS control for satellite access	17.2.0

2021-12	SP-94E	SP-211279	1138	1	A	Access network information request without PCC rules	17.2.0
2024-03	-	-	-	-	-	Update to Rel-18 version (MCC)	**18.0.0**

History

Document history		
V18.0.0	April 2024	Publication