3GPP TS 23.203 V8.1.1 (2008-03)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Policy and charging control architecture
(Release 8)

Keywords
UMTS, GSM, Charging, Performance

3GPP

Postal address

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

Internet
http://www.3gpp.org

Contents

Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

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

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

Introduction

Editor's Note: The content of this specification has been copied from TS 23.203 v.7.4.0 and thus is not fully updated according to current Rel-8 TS 23.401 and TS 23.402 versions. Thus, it is expected further contributions in order to make this specification compliant with Rel-8 requirements.

Policy and Charging Control functionality encompasses two main functions:

- Flow Based Charging, including charging control and online credit control;
- 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, I-WLAN, Fixed Broadband, etc.):

- Flow Based Charging, including charging control and online credit control;
- 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 for the present release of this document.

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] 3GPP TS 23.234: "3GPP system to Wireless Local Area Network (WLAN) interworking; System description".

[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: "GPRS enhancements for E-UTRAN access".

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

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].

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.

dynamic PCC Rule: a PCC rule for which the definition is provided into 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. Also, a trigger for credit management events. The event trigger criteria are supplied to the PCEF or BBERF by the PCRF.

gating control: The process of blocking or allowing packets, belonging to a service data flow, to pass through to the desired endpoint.

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 TS 21.905 [8] for the definition of bearer.

IP-CAN session: The association between a UE represented by an IPv4 and/or an IPv6 address, and 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 are established and announced to the IP network.

I-WLAN IP-CAN: This IP-CAN incorporates 3GPP IP access of I-WLAN, see TS 23.234 [13].

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

packet flow: A specific user data flow carried through the PCEF. A packet flow can be an IP flow.

PCC decision: A decision consists of PCC rules and IP-CAN bearer attributes, which is provided by the PCRF to the PCEF for policy and charging 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.

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.

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

QoS class identifier: An identifier representing QoS parameters, excluding the bitrates, of the IP-CAN. A network may be configured to provide corresponding QoS, given the same QoS class identifier value, in multiple IP-CAN types.

QoS rules: A set of information enabling the detection of a service data flow and for performing bearer binding and uplink bearer binding verification. The QoS rules contain QoS parameters.

service data flow: An aggregate set of packet flows that matches a service data flow template.

service data flow filter: A set of IP header parameter values/ranges used to identify one or more of the packet flows constituting a service data flow. A service data flow filter of a PCC rule that is predefined in the PCEF may use parameters that extend the packet inspection beyond the IP 5 tuple.

service data flow template: The set of service data flow filters in a PCC rule, 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.

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

3.3 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].

AF	Application Function
H-PCEF	A PCEF in the HPLMN
IP-CAN	IP Connectivity Access Network
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
SPR	Subscription Profile Repository
V-PCEF	A PCEF in the VPLMN

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, I-WLAN, 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 filter 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 filter of any other active PCC rules.

The PCC architecture shall allow the charging control to be applied on a per service data flow 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 template shall suffice, to detect a service data flow, 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. This requires a single optimized interface between the PCC nodes.

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.

NOTE: The usage of home network control of PCC in the visited network (as being developed in Annex B) is not specified in this Release.

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.

4.2 Charging related requirements

4.2.1 General

In order to allow for charging control, 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.

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:

- 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.

4.2.2a Charging requirements

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 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 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 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 for monitoring. In case the PCEF detects that any of the time based or volume based credit falls below the threshold, the PCEF 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;
- IP-CAN bearer characteristics (e.g. QoS);
- QoS provided for the service;
- time of day;
- IP-CAN specific parameters according to Annex A.

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 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 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 may change as a result of having used the service data flow for a certain amount of time and/or volume.

In the case of online charging, it shall be possible to apply an online charging action upon PCEF events (e.g. re-authorization upon QoS change).

It shall be possible to indicate to the PCEF that interactions with the charging systems are not required for a PCC rule, i.e. to perform neither accounting nor credit control for this service data flow, and then no offline charging information is generated.

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 reference point.

4.3.2 Gating control

Gating control shall be applied 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.

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 pre-defined 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. It shall be possible to determine the QoS to be applied in QoS reservation procedures (QoS control) based on the authorised QoS of the service data flows that are applicable to the IP-CAN bearer and on criteria such as the QoS subscription information, service based policies, and/or pre-defined PCRF internal policies. Details of QoS reservation procedures are IP-CAN specific and therefore, the control of these procedures is described in Annex A and Annex D.

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 when the authorized bandwidth associated with multiple PCC rules exceeds the Subscribed Guaranteed bandwidth QoS.

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, the Bearer Binding and Event Reporting Function (BBERF), the Policy and Charging Rules Function, the Application Function, the Online Charging System, the Offline Charging System and the Subscription Profile Repository.

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.

Editor's note: Each IP-CAN type specific Annex shall indicate whether the BBERF is applicable and its potential allocation.

Editor's note: Whether any CAMEL SCP need to be included in the architecture is FFS.

Editor's note: Whether the roaming case for Gy requires an OCS proxy is FFS.

Editor's note: Whether the roles of AF in HPLMN and VPLMN in Figure 5.1.3 need any clarifications in this clause or any difference can be accommodated in the AF and/or PCRF clauses is FFS.

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

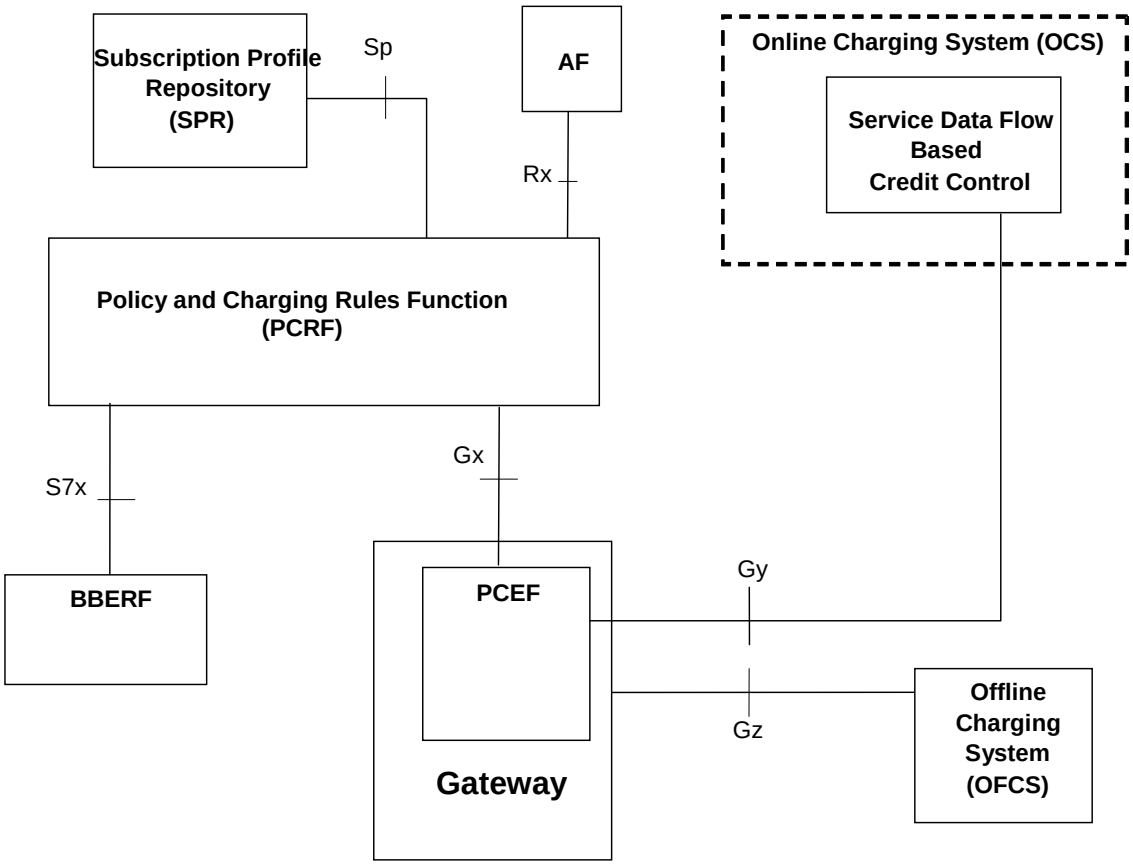

Figure 5.1.1: Overall PCC logical architecture (non-roaming)

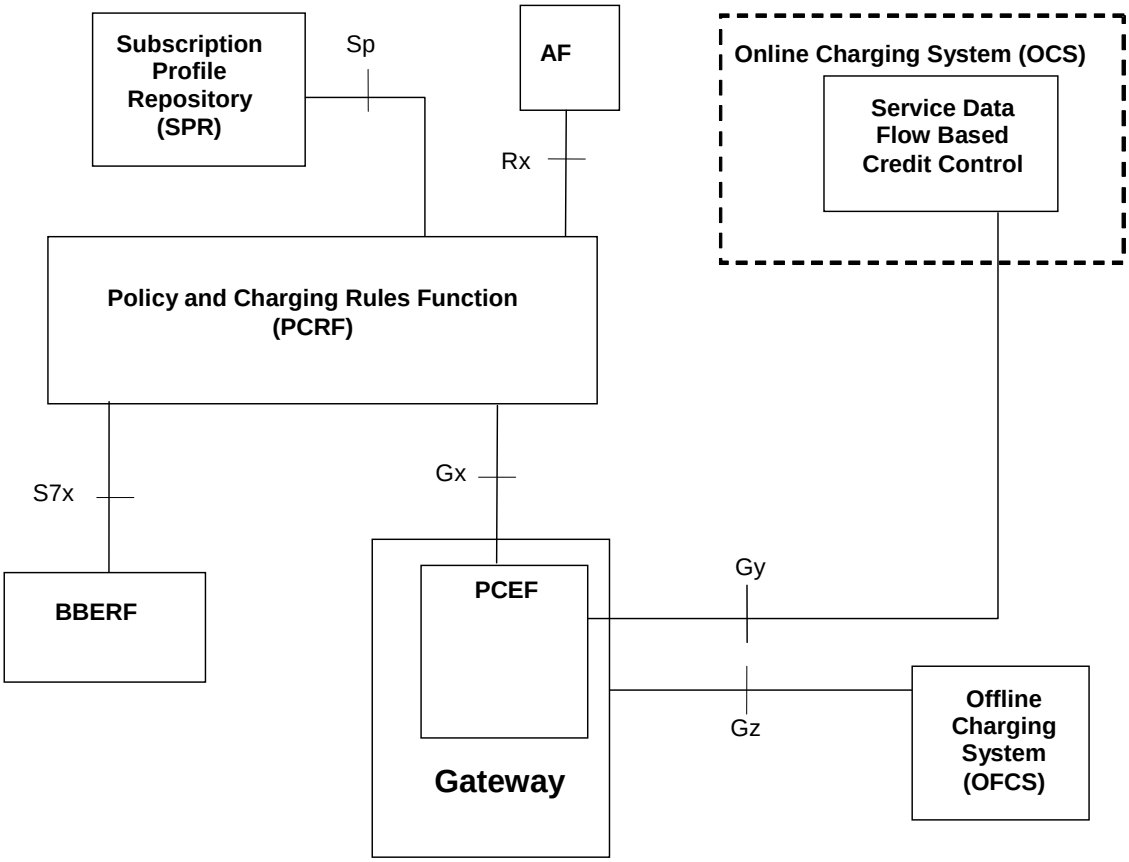

Figure 5.1.2: Overall PCC architecture (roaming with home routed access)

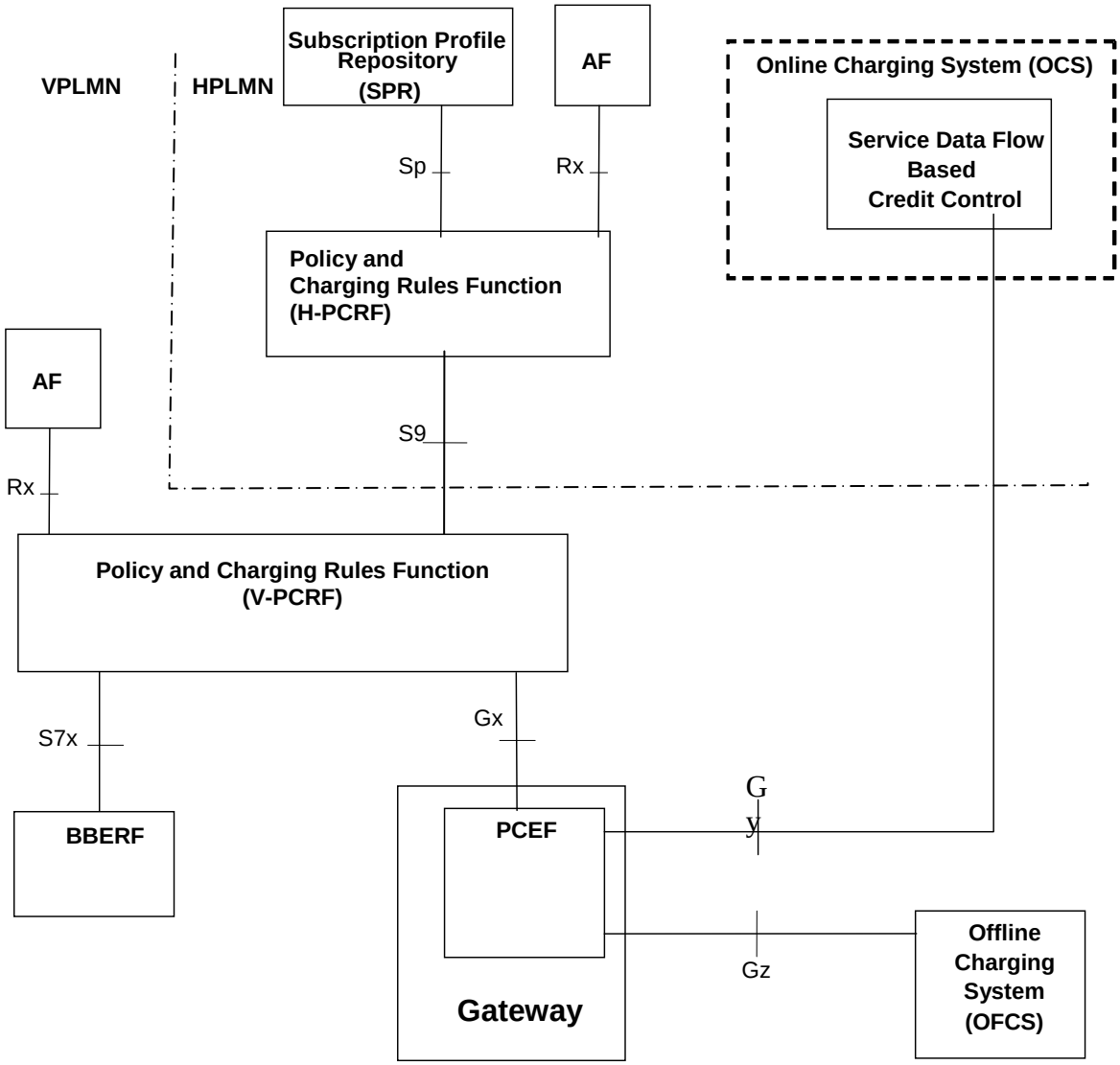

Figure 5.1.3: Overall PCC architecture for roaming with PCEF in visited network (local breakout)

5.2 Reference points

5.2.1 Rx reference point

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

NOTE: 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.

The Rx reference point enables the AF subscription to notifications on signalling path status of AF session in the IP-CAN.

5.2.2 Gx reference point

Editor's note: The Gx reference point coincides with S7 reference point of TS 23.401 and TS 23.402. Whether the same designation can be used for Gx and S7 in all the specifications is FFS.

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

The Gx reference point enables a 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:

- Request for PCC decision from PCEF to PCRF;
- Provision of PCC decision from PCRF to PCEF;
- Negotiation of IP-CAN bearer establishment mode (UE-only, UE/NW or NW-only);
- Termination of Gx session (corresponding to an IP-CAN session) by PCEF or PCRF.

NOTE: The PCRF decision to termination an 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.

A PCC decision consists of zero or more PCC rule(s) and IP-CAN attributes. The information contained in a PCC rule is defined in clause 6.3.

5.2.3 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.

5.2.4 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 use existing functionalities and mechanisms, 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 PCEF in visited network, the S9 reference point enables the Home PCRF to have dynamic control, via the V-PCRF, over the PCC behaviour at a PCEF in the VPLMN.

In all roaming scenarios, S9 has functionality to provide dynamic QoS control policies from the HPLMN, via a V-PCRF, to a BBERF in the VPLMN.

Editor's note: The designation of this reference points shall be aligned with the final choice in the TS 23.402. The definition of this reference point remains to be completed.

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

The binding mechanism is the procedure that associates a service data flow (defined in a PCC rule by means of the SDF template), to the IP-CAN bearer deemed to transport the service data flow. Thus, the binding mechanism shall associate the AF session information with the IP-CAN bearer that is intended to carry the service data flow.

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

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, i.e. the association of the AF session information and applicable PCC rules to an IP-CAN session.

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

   a) The UE IP address;

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

NOTE 2: 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.

NOTE 3: Only a 1:1 mapping between the Rx session and IP-CAN session is supported in Release 7.

2. PCC Rule authorization, i.e. the selection of the QoS parameters (QCI, GBR, MBR, etc.) for the PCC rule.

   The PCRF shall perform the PCC rule authorization for the dynamic PCC rules that have been selected in step 1, taking 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.

3. Bearer binding, i.e. the association of the PCC rule to an IP-CAN bearer within that IP-CAN session.

   The PCEF performs the bearer binding, unless specified differently in Annex A and Annex D (e.g. for GPRS running UE only IP-CAN bearer establishment mode).

NOTE 4: 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 following parameters to create the bearer binding for a service data flow:

a) The session binding result;

b) The QoS parameters of the IP-CAN bearer, if available;

c) The traffic mapping information, if available.

The bearer binding mechanism works in the following way:

- If the PCEF performs the bearer binding, then the set of QoS parameters assigned in step 2 above to the service data flow is the main input for this mapping. The PCEF shall evaluate whether it is possible to use one of the existing bearers or not. If none of the existing bearers are possible to use, the PCEF should initiate the establishment of a suitable bearer. The binding is created between service data flow(s) and the IP-CAN bearer which have the same QoS class identifier.

NOTE 5: The handling of a PCC 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).

- If the PCRF performs the bearer binding, then the binding mechanism shall associate the PCC rule with the IP-CAN bearer that is intended to carry the service data flow, as indicated by the traffic mapping information synchronized between the PCEF and UE. The PCRF shall compare the available traffic mapping information of all IP-CAN bearers, for the same IP-CAN session, with the existing service data flow filter information. Each part of the traffic mapping information shall be evaluated separately in the order of their related precedence. Any matching service data flow filter creates the binding of its corresponding service data flow with the IP-CAN bearer to which the traffic mapping information belongs. 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 bound to a single IP-CAN bearer, i.e. the same PCC rule may not be established on multiple IP-CAN bearers.

NOTE 6: For example, a PCC rule containing multiple service data flow filters that match traffic mapping information of more than one IP-CAN bearer could be segmented by the PCRF according to the different matching traffic mapping information. Afterwards, the PCRF can bind the generated PCC rules individually.

Requirements, specific for each type of IP-CAN, are defined in Annex A and described in Annex D.

For an IP-CAN, where the PCEF gains no information on what IP-CAN bearer the UE selects to send an uplink IP flow, the binding mechanism shall assume that, for bi-directional service data flows, both downlink and uplink packets travel on the same IP-CAN bearer.

PCC shall re-evaluate existing bindings, i.e. perform the binding mechanism, whenever the service data flow template, the QoS authorization or the negotiated traffic mapping information changes. The re-evaluation may, for a service data flow, require a new binding with another IP-CAN bearer.

6.1.2 Reporting

Reporting refers to the differentiated IP-CAN bearer usage information (measured at the PCEF) 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 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 shall report usage information for online and offline charging.

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

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

NOTE 2: For reporting purposes 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.

Charging information shall be reported based on the result from the service data flow detection and measurement on a per IP-CAN bearer basis.

A report may contain multiple containers, each container associated with a charging key 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 shall support credit management on a per IP-CAN bearer basis.

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

The PCEF shall request a credit for each charging key occurring in a PCC rule. It shall be up to operator configuration whether the PCEF shall request credit in conjunction with the PCC rule being activated or when the first packet corresponding to the service data flow 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 policy enforcement (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, e.g. with the objective of avoiding credit fragmentation. Multiple pools of credit shall be allowed per IP-CAN bearer. 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. 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 charged at different rates or in different units (e.g. time/volume/event) into the same pool.

For each charging key, the PCEF may receive credit re-authorisation trigger information from the OCS, which shall cause the PCEF to perform a credit re-authorisation when the event occurs. The credit re-authorisation trigger detection shall cause the PCEF to request re-authorisation of the credit in the OCS. It shall be possible for the OCS to instruct the PCEF 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
Credit authorisation lifetime expiry	The OCS has limited the validity of the credit to expire at a certain time.
Idle timeout	The service data flow has been empty for a certain time.
PLMN change	The UE has moved to another operators' domain.
QoS changes	The QoS of the IP-CAN bearer has changed.

NOTE: This list is not exhaustive. Events specific for each IP-CAN are specified in clause A, and the protocol description may support additional events.

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.

6.1.4 Event Triggers

The PCEF shall receive information from the PCRF that define the conditions when the PCEF shall interact again with PCRF after an IP-CAN session establishment.

The event triggers are provided by the PCRF to the PCEF using the Provision of PCC Rules procedure. Event triggers are associated with all PCC rules of an IP-CAN session. Event triggers determine when the PCEF shall signal to the PCRF that an IP-CAN bearer has been modified. It shall be possible for the PCRF to instruct the PCEF to react on the event triggers listed in table 6.2.

Table 6.2: Event triggers

Event trigger	Description
PLMN change	The UE has moved to another operators' domain.
QoS change	The QoS of the IP-CAN bearer has changed.
QoS change exceeding authorization	The QoS of the IP-CAN bearer has changed and exceeds the authorized QoS (note 3).
Traffic mapping information change	The traffic mapping information of the IP-CAN bearer has changed (note 3).
Change in type of IP-CAN (see note 1)	The access type of the IP-CAN bearer has changed.
Loss/recovery of transmission resources	The IP-CAN transmission resources are no longer usable/again usable.

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.

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 PCEF shall check the QoS class identifier and the bandwidth.

6.1.5 Policy Control

Policy control comprises functionalities for:

- Gating control, i.e. the blocking or allowing of packets, belonging to a service data flow, to pass through to the desired endpoint;
- Event reporting, i.e. the notification of and reaction to application events to trigger new behaviour in the user plane as well as the reporting of events related to the resources in the GW(PCEF);
- QoS control, i.e. the authorisation and enforcement of the maximum QoS that is authorised for a service data flow or an IP-CAN bearer.
- 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 it can be a pre-defined PCC rule in the PCEF. In case the PCRF provides PCC rules dynamically, authorised QoS information for the IP-CAN bearer (combined QoS) may be provided. For a predefined PCC rules within the PCEF the authorized QoS information shall take affect when the PCC rule is activated. The PCEF shall combine the different sets of authorized QoS information, i.e. the information 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 IP-CAN session modification;
- 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 events.

Editor's note: It is FFS how to control whether a service may start on any bearer that could transfer the traffic or whether a bearer dedicated for this traffic is required.

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.

6.2 Functional entities

6.2.1 Policy Control and Charging Rules Function (PCRF)

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

Editor's note: The definition of the H-PCRF and V-PCRF is FFS.

The PCRF provides network control regarding the service data flow detection, gating, QoS and flow based charging (except credit management) towards the PCEF.

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

The PCRF shall decide how a certain service data flow shall be treated in the PCEF, 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.

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.

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

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.

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.

To support the different IP-CAN bearer establishment modes (UE-only, UE/NW or NW-only) the PCRF shall:

- set the IP-CAN bearer establishment mode for the IP-CAN session based on operator configuration, network capabilities and UE preferred bearer establishment mode;
- if the bearer establishment mode is UE/NW, decide what mode (UE or NW) shall apply for a PCC rule;
- guarantee the precedence of dynamic PCC rules for network controlled services in the service data flow detection process at the PCEF by setting the PCC rule precedence information to appropriate values.

6.2.1.1 Input for PCC decisions

The PCRF shall accept input for PCC decision-making from the PCEF, SPR and if the AF is involved, from the AF, as well as the PCRF may use its own pre-defined 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 may provide the following information:

- Subscriber Identifier;
- IP address(es) of the UE;
- IP-CAN bearer attributes;
- Request type (initial, modification, etc.);
- Type of IP-CAN (e.g. GPRS, I-WLAN, etc.);

NOTE 1: The Type of IP-CAN parameter should allow extension to include new types of accesses.

- Location of the subscriber;
- A PDN ID;
- A PLMN identifier;
- IP-CAN bearer establishment mode.

NOTE 2: 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.

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;
- Subscriber category.

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;
- 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;
- Emergency indicator.

In addition, the pre-defined 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.

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. The PCRF should specify the subscriber ID and 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.

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 by providing the new PCC 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).

6.2.1.3.2 V-PCRF and Home Routed Access

The V-PCRF provides functions to forward S7x interactions between the BBERF and the H-PCRF as follows:

- Gateway Control Session establishment and termination messages;

- Gateway Control and QoS Policy Rules Provision messages;
- Gateway Control and QoS Rule Request messages.

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 for a certain service 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.

Editor's note: It is FFS whether the V-PCRF should provide functionality to add local (pre-configured) PCC rules to an IP-CAN session and/or QoS rules to a Gateway Control Session.

When Gx interactions are forwarded between the PCEF and the H-PCRF, the V-PCRF forwards:

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

Editor's note: It is FFS if the Gateway Control Signalling is forwarded over S9 of if the V-PCRF "hides" the S7x from the roaming interface. It is FFS if there is a single S9 interface independent of whether the VPLMN deploys "off-path" or "on-path" PCC or if the S9 is different depending on the VPLMN PCC architecture.

Editor's note: It is FFS whether there is a scenario where Gx and S7x interactions are handled locally in the V-PCRF without using S9 and without taking per user subscription into account.

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

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 policy enforcement or flow based charging, is neither reported for offline charging nor cause credit consumption for online charging.

NOTE: 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.

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 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. 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 for 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.

NOTE: 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 uplink traffic mapping information. See 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, UE/NW or NW-only) the PCEF shall:

- forward the network capabilities and UE preferred bearer establishment mode 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.

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;
- Each service data flow template may contain any number of service data flow filters;
- Service data flow filters are unidirectional, so that the detection is applied independently for the downlink and uplink directions.

NOTE 1: A service data flow template may include service data flow filters for one direction, or for both directions.

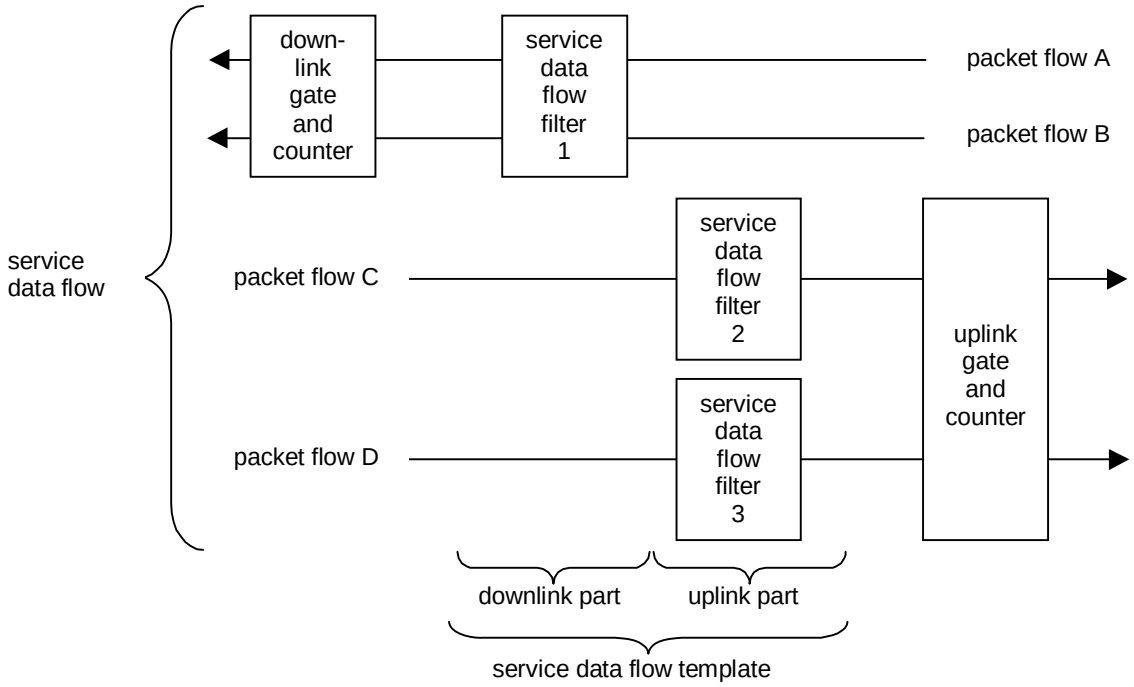

Figure 6.3: Relationship of service data flow, packet flow, service data flow template and service data flow filter

Service data flow filters identifying the service data flow may:

- be a pattern for matching the IP 5 tuple (source IP address, destination IP address, 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.
- extend the packet inspection beyond the IP 5 tuple 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 2: 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.

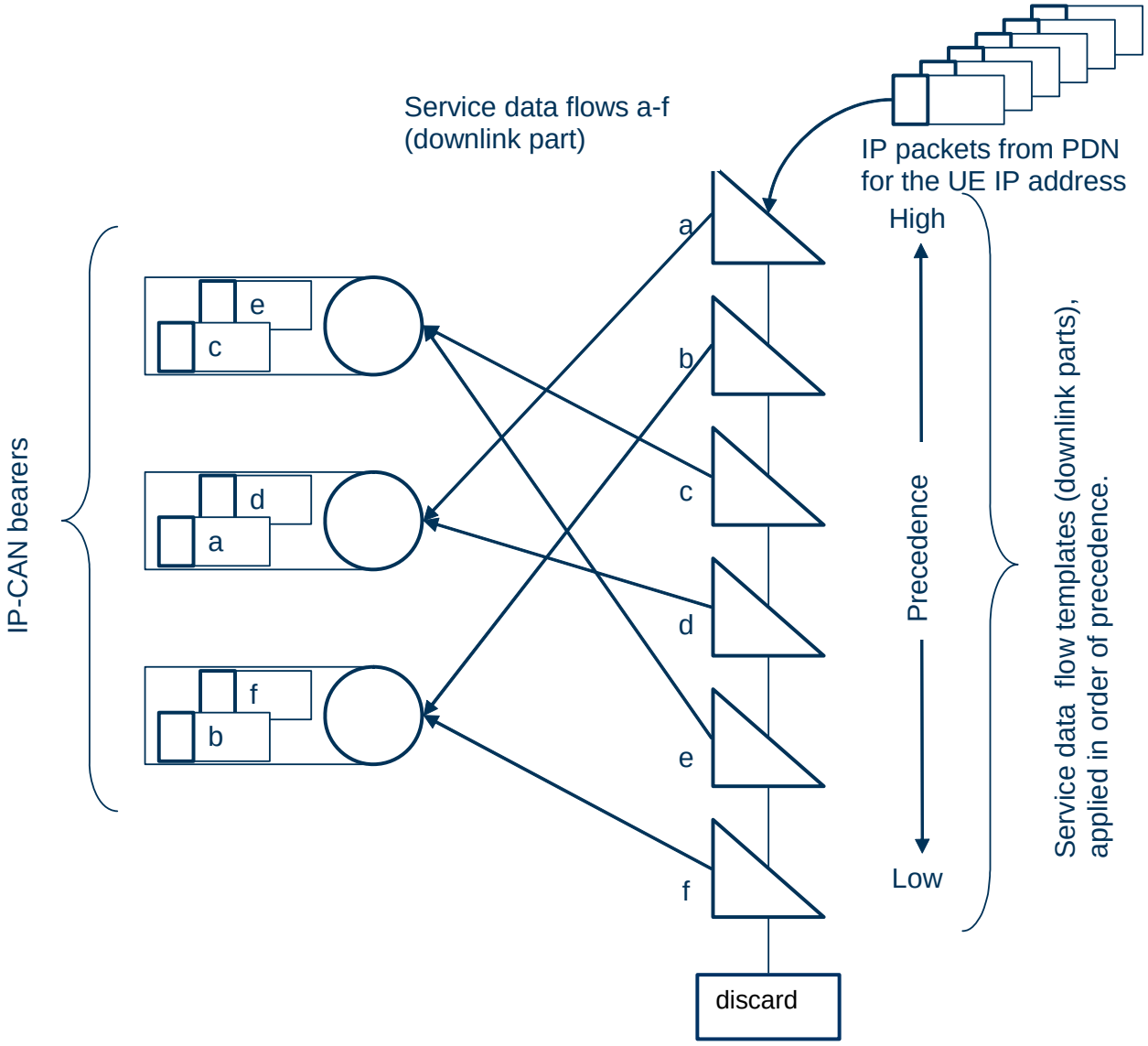

Figure 6.4: The service data flow template role in detecting the downlink part of a service data flow and mapping to IP-CAN bearers

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.

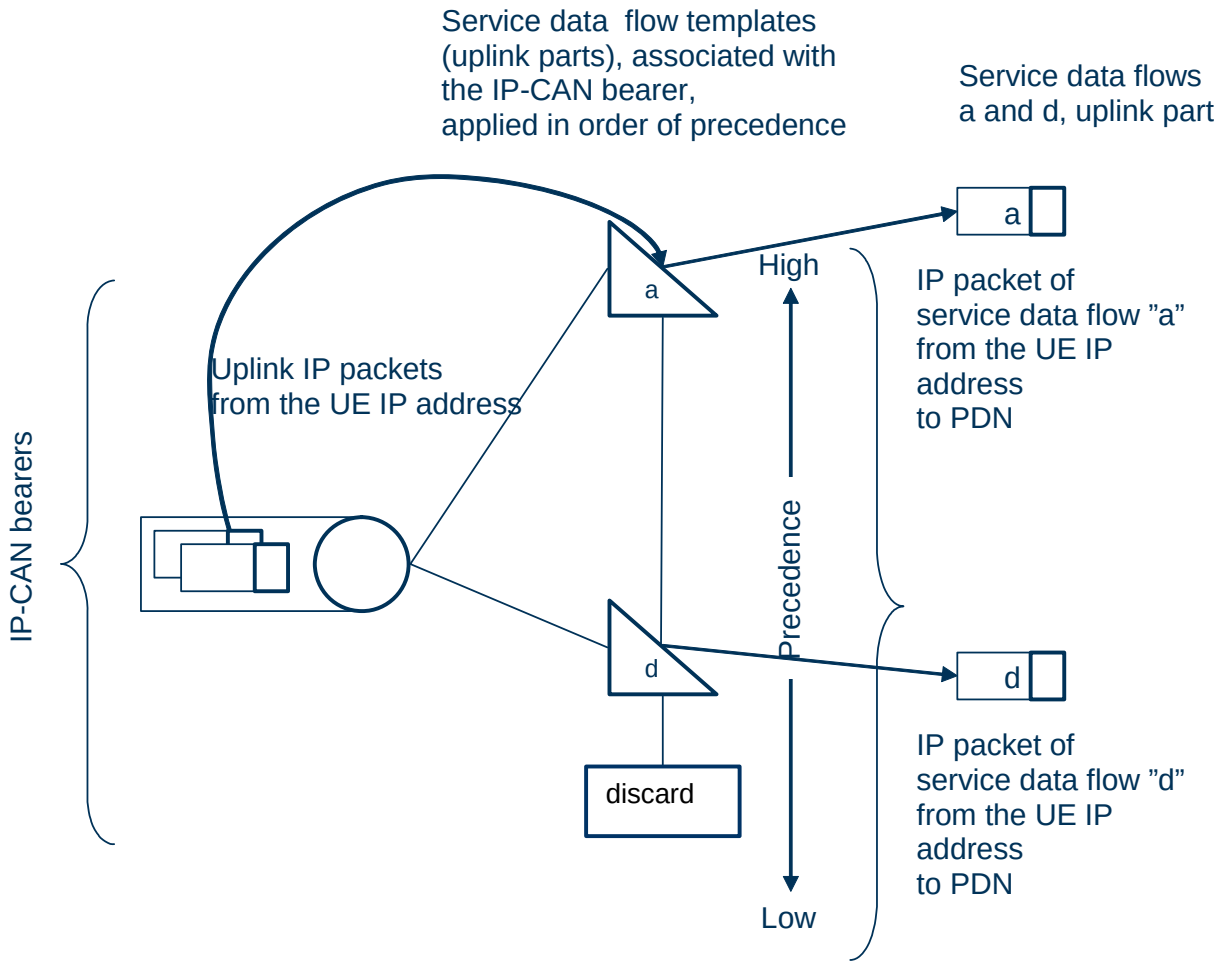

Figure 6.5: The service data flow template role in detecting the uplink part of a service data flow

The PCEF shall discard a packet in case there is no service data flow filter 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 3: 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 filters 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. The Measurement method indicates what measurement type is applicable for the PCC rule.

NOTE: Event based charging is only applicable to pre-defined PCC rules.

The PCC 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: In addition, the GW may maintain IP-CAN bearer level measurement if required by the operator.

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, 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.

For a network initiated IP-CAN bearer establishment or modification the PCEF receives the authorized QoS per PCC rule (QCI, 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. 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. 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: 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.

6.2.3 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: 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.

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 request the PCRF to report on the signalling path status for the AF session. The AF shall cancel the request when the AF ceases handling the user.

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: 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 category.

6.2.5 Service Data Flow Based Credit Control Function

The Service Data Flow Based Credit Control Function performs online credit control functions. It is a functional entity within the Online Charging System.

The Online Charging System is specified in TS 32.240 [3].

The OCS may trigger the PCEF to initiate a 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 data flow), it is recommended to use different charging keys for any service data flows 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. OCS addresses may also be passed once per IP-CAN session from the PCRF to the PCEF. 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. OFCS addresses may also be passed once per IP-CAN session from the PCRF to the PCEF. 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)

The BBERF includes the following functionalities:

- Bearer binding;
- Uplink bearer binding verification.

Editor's Note: The detailed definition of 'Uplink bearer binding verification' is FFS. The purpose is to discard traffic that does not comply with the present bearer binding.

- Event reporting to the PCRF.

Editor's note: This functional entity is, when Gxc applies, located at the Serving Gateway and, when Gxa applies, located in a trusted non-3GPP access.

Editor's note: The remaining part of this clause remains to be completed.

6.2.8 Bearer Binding and Event Reporting Function (BBERF)

6.2.8.1 General

The BBERF includes the following functionalities:

- Bearer binding.
- Uplink bearer binding verification.

Editor's Note: The detailed definition of 'Uplink bearer binding verification' is FFS. The purpose is to discard traffic that does not comply with the present bearer binding.

- Event reporting to the PCRF.

Editor's Note: This functional entity is, when Gxc applies, located at the Serving Gateway and, when Gxa applies, located in a trusted non-3GPP access.

Editor's Note: The remaining part of this clause remains to be completed.

6.2.8.2 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.

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 are designated 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.

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

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, i.e. PCC rules containing completely identical information shall receive different PCC rule identifiers (an exception are predefined PCC rules that contain only uplink service data flow filters and which are known to the PCRF, 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 section 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.	Mandatory	yes
Service data flow template	A list of service data flow filters for the detection of the service data flow.	Mandatory	yes
Charging	*This section 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 for 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
Charging method	Indicates the required charging method for the PCC rule. Values: online, offline or neither.	Conditional (NOTE 4)	no
Measurement method	Indicates whether the service data flow data volume, duration, combined volume/duration or event shall be measured. This is applicable for reporting, if the charging method is online or offline. Note: Event based charging is only applicable to pre-defined PCC rules.		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

Information name	Description	Category	PCRF permitted to modify for a dynamic PCC rule in the PCEF
Policy control	*This section defines how the PCEF shall appy 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

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 policy control on SDF level applies.
NOTE 4: Mandatory if there is no default charging method for the IP-CAN session.

The *PCC Rule identifier* shall be unique for a PCC rule within an IP-CAN session. A dynamically provided PCC rule that has the same Rule identifier value as a predefined PCC rule shall replace the predefined rule within the same IP-CAN session.

The *PCC 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 for matching against the IP 5-tuple. 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.

The *PCC 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.

NOTE 4: 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.

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.

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

NOTE 5: Assigning the same Charging key for several service data flows implies that the charging does not require the credit management to be handled separately.

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

NOTE 6: The PCC service identifier need not have any relationship to service identifiers used on the AF level, i.e. is an operator policy option.

The PCC *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 PCC charging method identifies that the service data flow is not subject to any end user charging, a PCC Charging key shall not be included in the PCC rule for that service data flow, along with other charging related parameters. If the PCC charging method is omitted the PCEF shall apply the default charging method as determined at IP-CAN session establishment (see clause 6.4). The PCC Charging method is mandatory if there is no default charging method for the IP-CAN session.

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

The PCC 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 PCC *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 7: 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 PCC *Gate* indicates whether the PCEF shall let a packet matching the PCC Service data flow template, pass through (gate is open) the PCEF or the PCEF shall discard (gate is closed) the packet.

NOTE 8: 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.

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.

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.

A predefined PCC rule is known at least, within the scope of one access point.

NOTE: The same predefined PCC rule can be activated for multiple IP-CAN bearers in multiple IP-CAN sessions.

A predefined PCC rule that contains downlink service data flow filters can only be activated once per IP-CAN session. A predefined PCC rule that contains only uplink service data flow filters can be activated for multiple IP-CAN bearers of the same IP-CAN session (deactivation of such a predefined PCC rule would remove this PCC rule from every IP-CAN bearer).

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.

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 using the PCC rule provision procedure. The IP-CAN bearer related policy information may be provided together with PCC 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	Defines the containing OFCS and/or OCS addresses.	No	IP-CAN session
Default charging method	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)	Defines the authorised MBR per QCI.	Yes	IP-CAN session

NOTE 1: Depending on the bearer establishment mode only one Authorized QoS information has to be used.

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.

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.

Upon every interaction with the PCEF, the PCRF may provide event triggers for the IP-CAN session. Event triggers are used to determine which IP-CAN bearer modification causes the PCEF 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.

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 and Annex D.

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.

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.

Procedures defined in clause 7 cover all the traffic cases where roaming partners both operate PCC.

Editor's Note: It is FFS if the procedures defined in clause 7 also cover the case of visited operator only using PCC. In this case, the V-PCRF acts as for the visited access case, but without any interaction with the H-PCRF. As a consequence, the SPR is not accessible.

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.

7.2 IP-CAN Session Establishment

This clause describes the signalling flow for IP-CAN Session establishment and IP address assignment to the UE. The AF is not involved.

There are three cases considered for IP-CAN Session Establishment.

1. In cases where 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).

2. In cases where a Gateway Control Session is required there are two sub-cases:

a) In cases where the UE acquires a care of address (CoA) that is used for S2c, the BBERF establishes a Gateway Control session prior to any IP-CAN session establishment. This interaction, as defined in clause 7.7.1 will precede the rest of the procedure.

b) In other cases where 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 proceeds after the IP CAN Session Establishment.

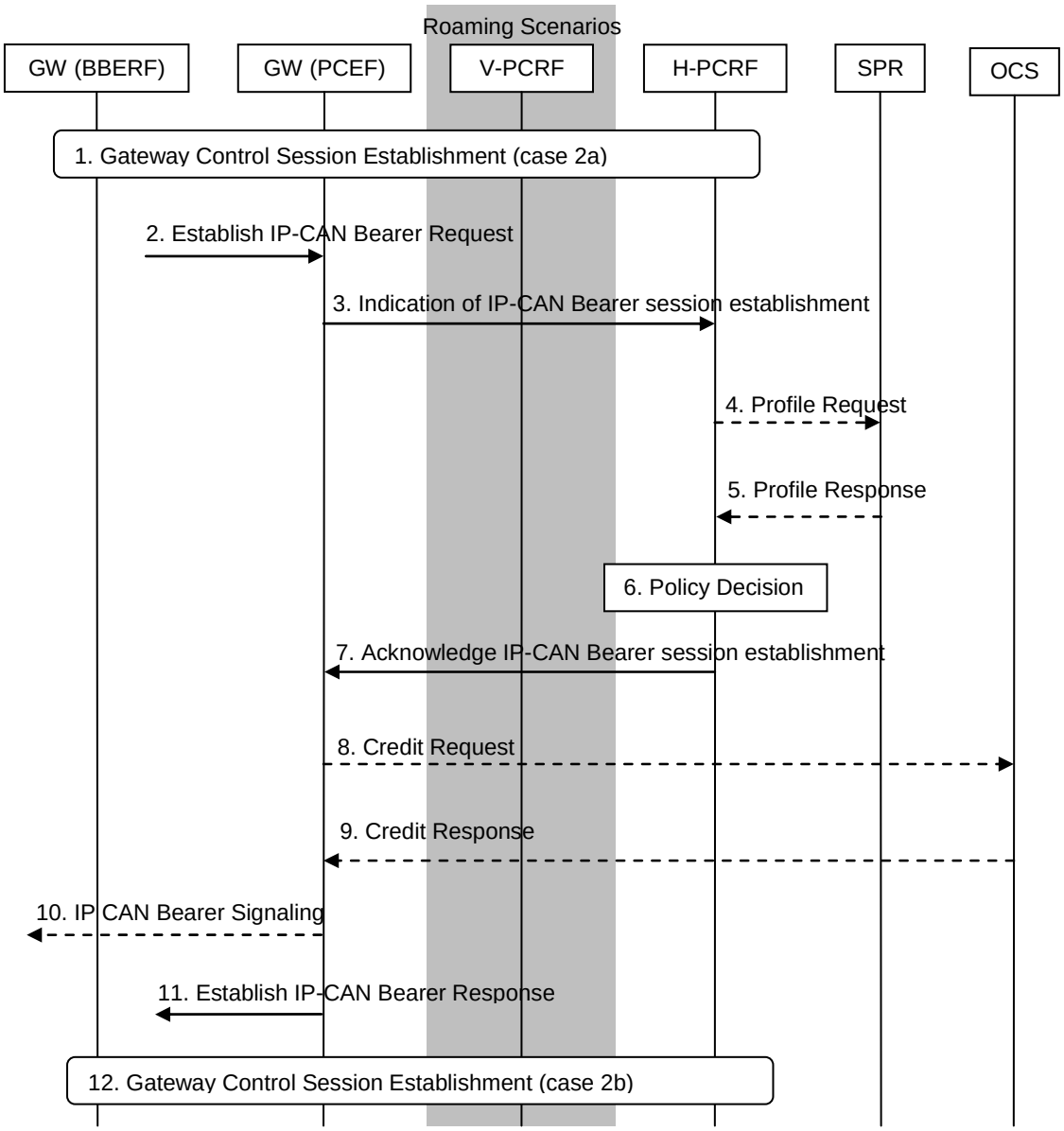

Figure 7.2-1: IP-CAN Session Establishment

1. Initiate the Gateway Control Session Establishment procedure as defined in clause 7.7.1, if appropriate.

2. The GW(PCEF) receives a request for IP-CAN Bearer establishment. The GW(PCEF) accepts the request and assigns an IP address for the user. In case the data flow is tunnelled at the BBERF the PCEF shall provide information about the mobility protocol tunnelling encapsulation header in the message.

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; IP-CAN type and, if available, the default charging method and the IP-CAN bearer establishment modes supported.

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.

6. The PCRF makes the authorization and policy decision.

7. The PCRF sends the decision(s) , including the chosen IP-CAN bearer establishment mode, to the PCEF. The GW(PCEF) enforces the decision. The PCRF may provide the default charging method.

8. If online charging is applicable, and at least one PCC rule was activated, the PCEF shall activate the online charging session, and provide relevant input information for the OCS decision. Depending on operator configuration PCEF may request credit from OCS for each charging key of the activated PCC rules.

9. 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.

10. If network control applies the GW may initiate the establishment of additional IP-CAN bearers. See Annex A and Annex D for details.

    Step 10, which establishes dedicated bearers, does not apply when step 12 is performed.

11. If at least one PCC rule was successfully activated and if online charging is applicable credit was not denied by the OCS, the GW(PCEF) acknowledges the IP-CAN Bearer Establishment Request.

12. Proceed with the Gateway Control Session Establishment procedure defined in 7.7.1, if appropriate. If network control applies, the GW may initiate the allocation of initial and additional resources.

7.3 IP-CAN Session Termination

7.3.1 UE initiated IP-CAN Session termination

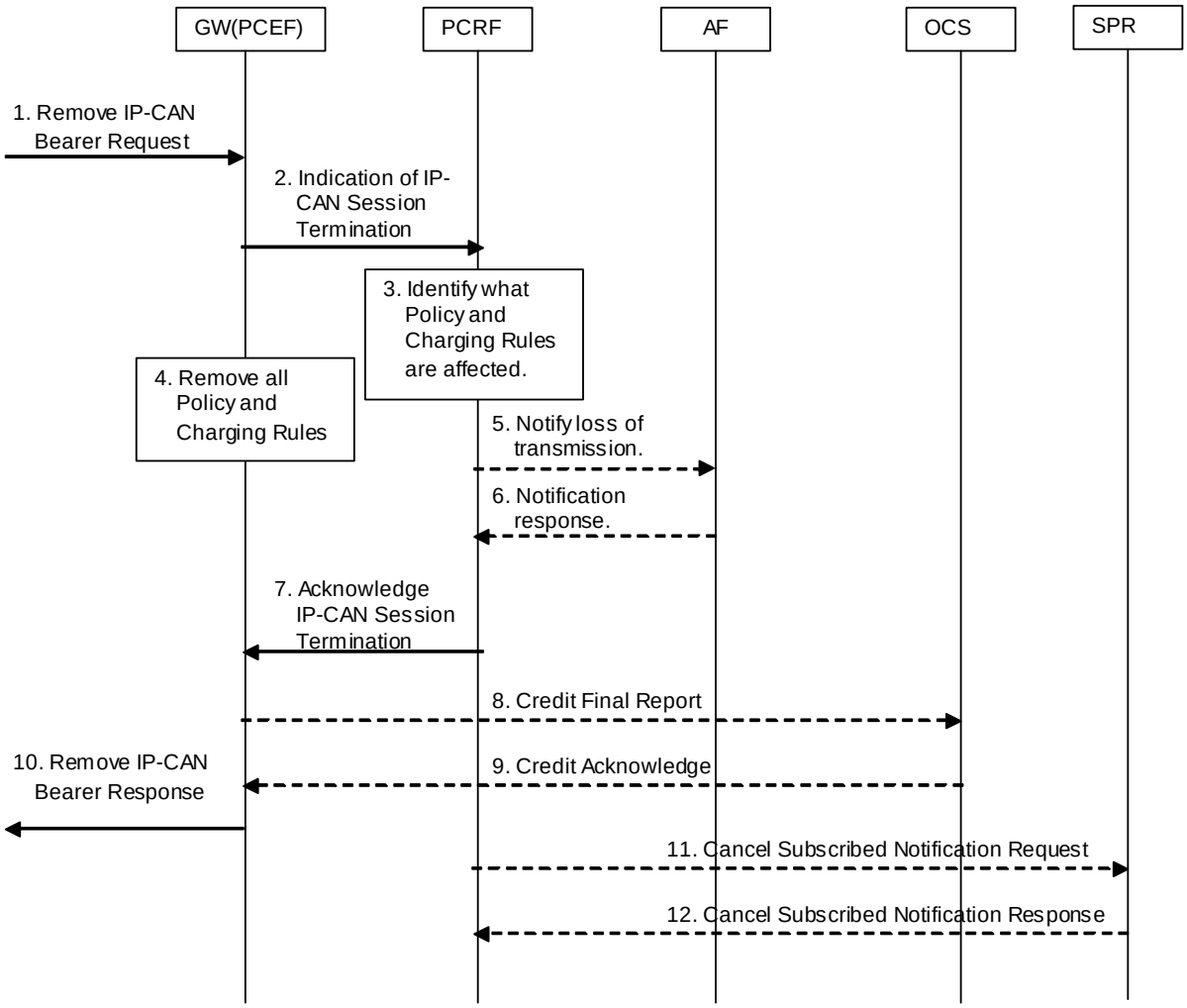

Figure 7.2: IP-CAN Session Termination

1. The GW(PCEF) receives a request to remove the last IP-CAN bearer associated to this IP-CAN session.
2. The PCEF indicates that the IP-CAN Session is being removed and provides relevant information to the PCRF.
3. The PCRF finds the PCC Rules that require an AF to be notified.
4. The PCEF removes all PCC Rules associated with the IP-CAN session.
5. The PCRF notifies the AF that there are no transmission resources for the service if this is requested by the AF.
6. The AF acknowledges the notification of the loss of transmission resources.
7. The PCRF removes the information related to the terminated IP-CAN Session (subscription information etc.), and acknowledges to the PCEF that the PCRF handling of the IP-CAN session has terminated. This message is flagged as the response to the PCEF request.
8. If online charging is applicable, the PCEF issues final reports and returns the remaining credit to the OCS.
9. If online charging is applicable the OCS acknowledges that credit report.
10. The GW(PCEF) continues the IP-CAN Bearer removal procedure.
11. The PCRF sends a cancellation notification request to the SPR if it has subscribed such notification.
12. The SPR sends a response to the PCRF.

NOTE: The IP-CAN Session removal procedure may proceed in parallel with the indication of IP-CAN Session termination.

7.3.2 GW(PCEF) initiated IP-CAN Session termination

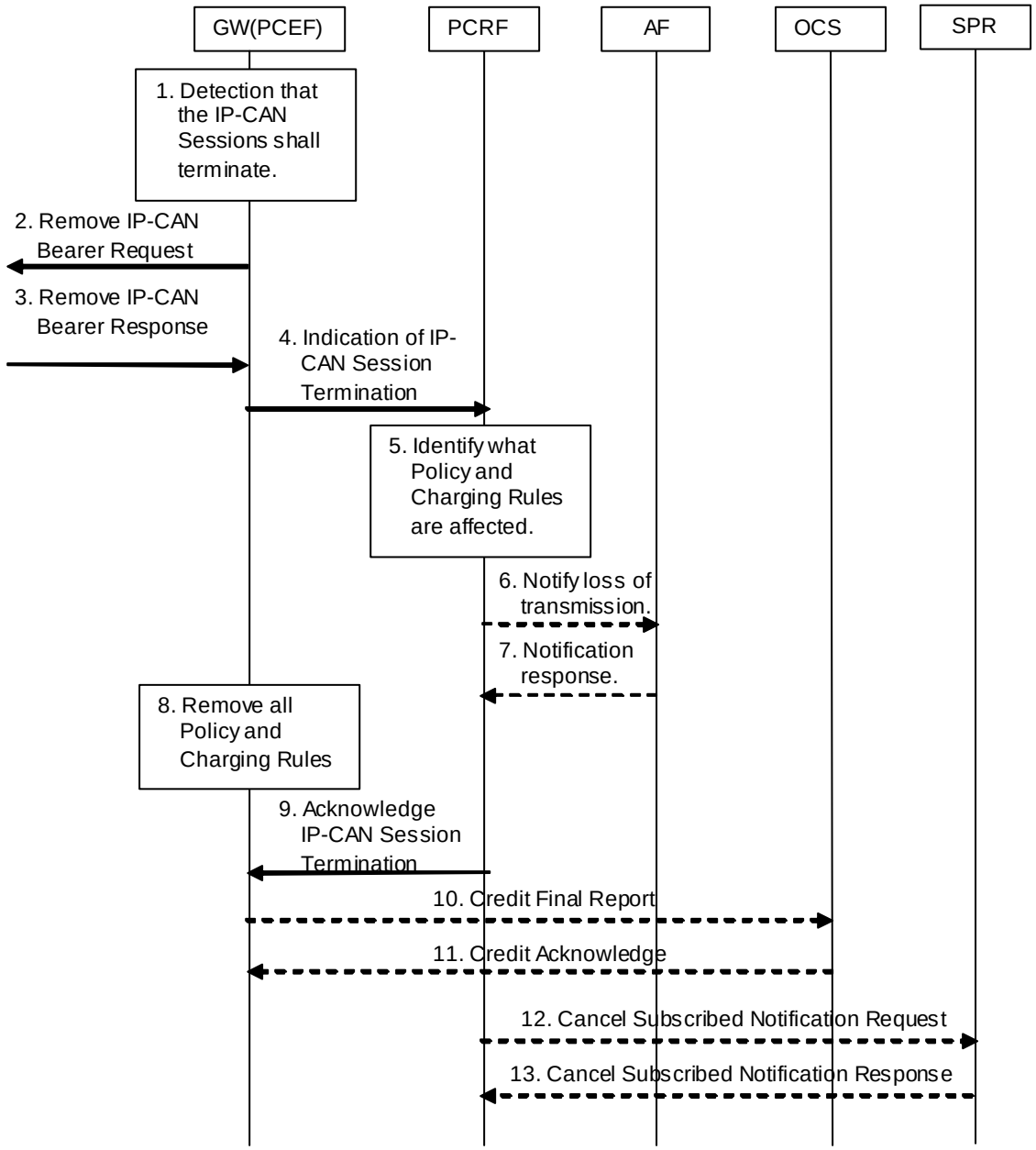

Figure 7.3: GW(PCEF) Initiated IP-CAN Session Termination

1. The GW(PCEF) detects that IP-CAN Session termination is required.
2. The GW(PCEF) sends a request to remove the IP-CAN bearer. For IP-CAN with multiple IP-CAN bearers this applies for each IP-CAN bearer associated to this IP-CAN session.
3. The GW(PCEF) receives the response for the IP-CAN bearer removal.
4. The PCEF indicates the IP-CAN Session termination and provides the relevant information to the PCRF.
5. The PCRF finds the PCC Rules that require an AF to be notified.
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 on the loss of transmission resources.
8. The PCEF removes all the PCC Rules associated with the IP-CAN session.

9. The PCRF removes the information related to the terminated IP-CAN Session (subscription information etc.), and acknowledges the IP-CAN Session termination.
10. If online charging is applicable, the GW issues final reports and returns the remaining credit to the OCS.
11. If online charging is applicable the OCS acknowledges the credit report.
12. The PCRF sends a cancellation notification request to the SPR if it has subscribed such notification.
13. The SPR sends a response to the PCRF.

7.4 IP-CAN Session Modification

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

This sub-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. 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.

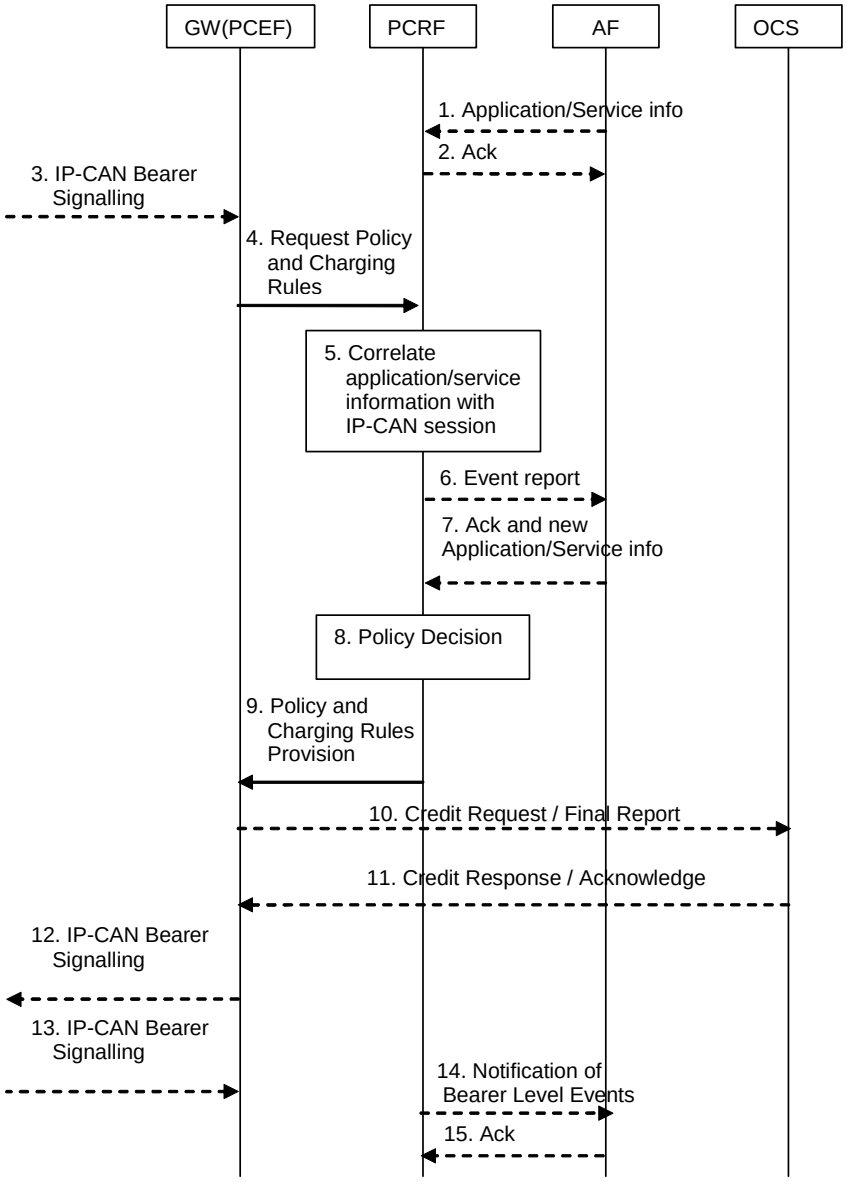

Figure 7.4: IP-CAN Session Modification; GW(PCEF) initiated

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: 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) makes an internal decision or receives a request for IP-CAN Bearer establishment, modification or termination.

4. The PCEF determines that the PCC interaction is required and sends the PCC Rules request to the PCRF. If there is a limitation or termination of the transmission resources for a PCC Rule, the PCEF reports this to the PCRF.

5. The PCRF correlates the request for PCC Rules with the IP-CAN session and service information available at the PCEF.

6. The PCRF may need to report to the AF an event related to the transmission resources and/or if the AF requested it at initial authorisation or if the PCRF requires more information from the AF before authorising the network resources modification..

7. The AF acknowledges the event report and/or responds with the requested information.

8. The PCRF makes the authorization and policy decision.

9. The PCRF sends the decision(s) to the PCEF. The GW(PCEF) enforces the decision.

10. If online charging is applicable, the PCEF may request credit for new charging keys from and/or shall issue final reports and return remaining credit for charging keys no longer active to the OCS.

11. If OCS was contacted, the OCS provides the credit information to the PCEF, and/or acknowledges the credit report.

12 The GW(PCEF) acknowledges or rejects any IP-CAN bearer signalling received in step 3.

The IP-CAN bearer establishment or modification 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 or modification 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).

13. In case of a GW(PCEF) internal decision the GW(PCEF) initiates any IP-CAN bearer signalling required for completion of the IP-CAN Session modification.

14. If the AF requested it, the PCRF notifies the AF related bearer level events (e.g. transmission resources are established/released/lost).

15. 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 may be involved. An example of the scenario is initiation and authorization of a session-based service for which an IP-CAN Session is modified. 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 is also applicable here.

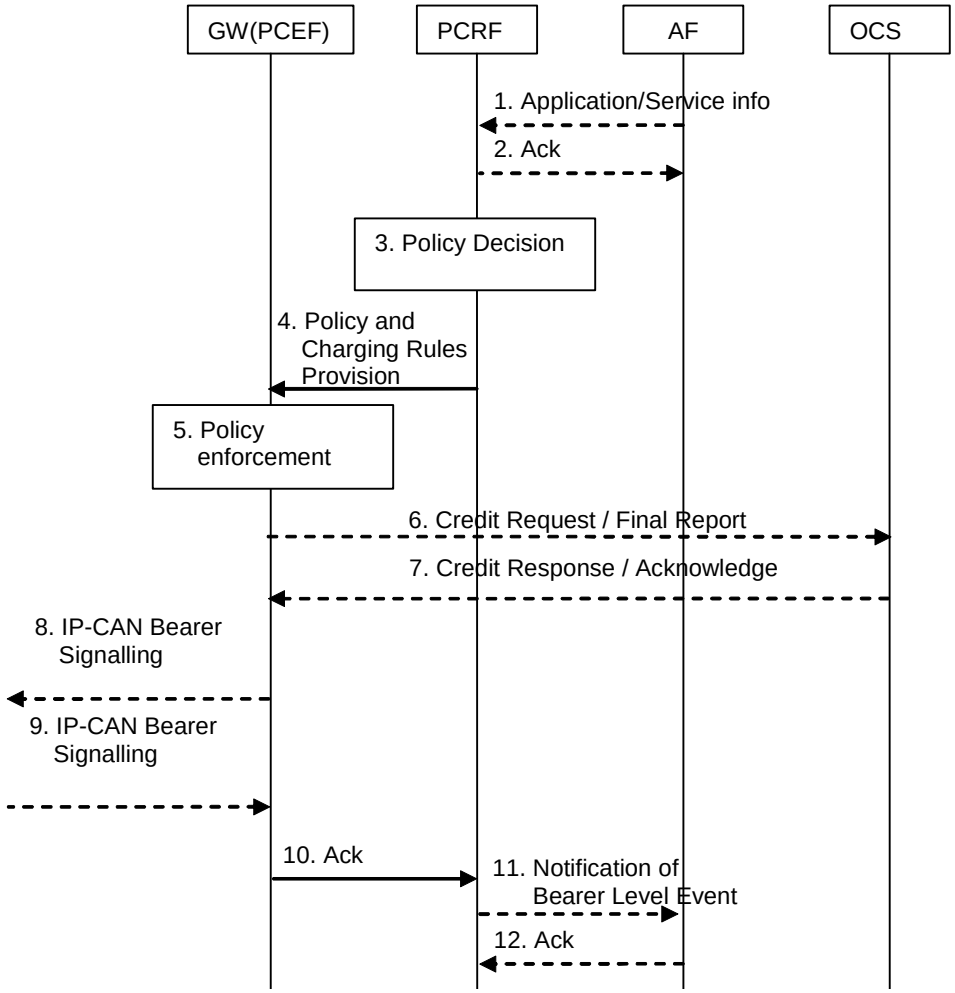

Figure 7.5: IP-CAN Session Modification; PCRF initiated

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 1: 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 if available and responds with the Acknowledgement to the AF.

NOTE 2: Without AF interaction, a trigger event in the PCRF may cause the PCRF to determine that the PCC rules require updating at the PCEF, e.g. change to configured policy.

3. The PCRF makes the authorization and policy decision.

4. The PCRF sends the decision(s) to the PCEF.

5. The PCEF enforces the decision.

6. If online charging is applicable, the PCEF may request credit for new charging keys from and/or shall return the remaining credit for charging keys no longer active to the OCS.

7. If OCS was involved, the OCS provides the credit information to the PCEF, and/or acknowledges the credit report

8. The GW(PCEF) may send an IP-CAN Bearer establishment, modification or termination request.
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 3.

An IP-CAN bearer termination request is sent by the GW(PCEF) if all PCC rules for an IP-CAN bearer have been removed.

9. The GW(PCEF) receives the response for the IP-CAN Bearer modification or termination request.
10. The PCEF sends ACK (accept or reject of the PCC rule operation(s)) to the PCRF.
11. If the AF requested it, the PCRF notifies the AF related bearer level events (e.g. transmission resources are established/released/lost).
12. The AF acknowledges the notification from the PCRF.

7.5 Update of the subscription information in the PCRF

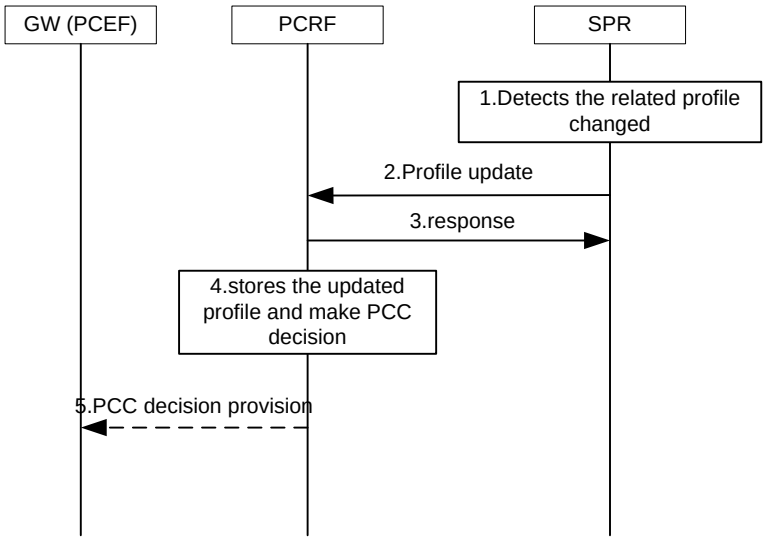

Figure-7.6: Procedure for update of the subscription information in the PCRF

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 and makes resulting PCC decisions.
5. The PCRF provides all new PCC decisions to the PCEF, using the PCRF initiated IP-CAN session modification procedure in clause 7.4.2.

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 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, S9, Gxa/Gxc), 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.).

Editor's note: What type of linking between different sessions (Rx, Gx, S9, Gxa, Gxc) that is performed by the V-PCRF and the H-PCRF respectively in the different roaming scenarios is FFS.

- 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.

  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 interactions, as well as S9, when applicable.

- 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 network based mobility, 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 host based mobility using S2c, 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).

Editor's note: The IP-CAN specific information above should eventually be described in the IP-CAN specific annexes.

- 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).

Editor's note: It is FFS if the possibility for a UE to have multiple PDN connections to the same APN will require additional information to uniquely identify an IP-CAN session.

- 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.

7.6.2 Solution Principles

Editor's note: The content of this clause represents the working assumptions made by SA2. Protocol aspects shall be handled by stage 3 work. It is FFS whether the content of this section, or parts of the content, belongs in this specification or should be covered by stage 3 specifications.

In order to ensure that all Diameter sessions for Gx, S9, Gxa/Gxc and Rx 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.

Editor's note: It is FFS whether DRA involvement in, subsequent interactions is needed.

Editor's note: It is FFS whether there is one Gxa/Gxc instance per IP-CAN session or one Gxa/Gxc instance for all IP-CAN sessions.

- When deployed, the DRA is on the Diameter routing path when initiating a session with a PCRF over Gx, Rx, Gxa/Gxc, and S9.
- 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
- After IP-CAN session or Gateway Control Session establishment, the DRA ensures that the same PCRF is contacted for Rx, Gxa/Gxc, Gx and S9.
- The DRA keeps status of assigned PCRF for a certain UE and IP-CAN session.

Editor's note: It is FFS how the status information is released when related sessions are terminated.

- 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.

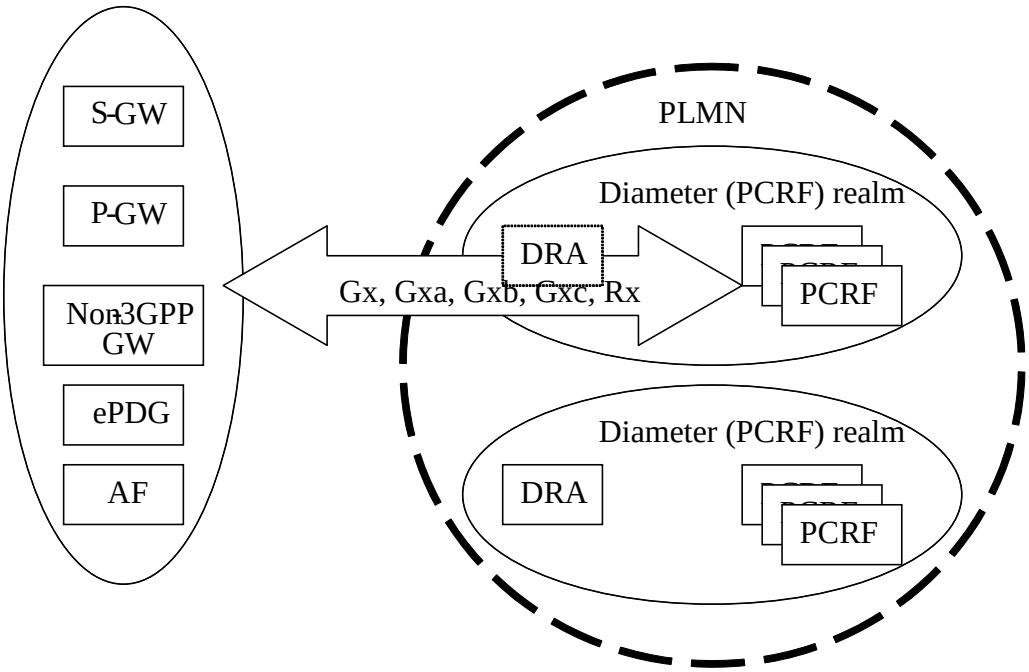

Figure 7.6-1: PCRF selection and discovery using DRA

The DRA functionality should be transparent to the Diameter applications used on the Gx, Gxa/Gxc, S9 or Rx 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

There are two cases considered for Gateway Control Session Establishment:

1. There exists an established IP CAN Session corresponding to the Gateway Control Session being established.
2. The PCEF establishes the IP CAN Session subsequent to the Gateway Control session establishment.

In the first case, the Gateway Control Session establishment may result in a change in the IP CAN session, as is shown by the optional step 3 in the figure below.

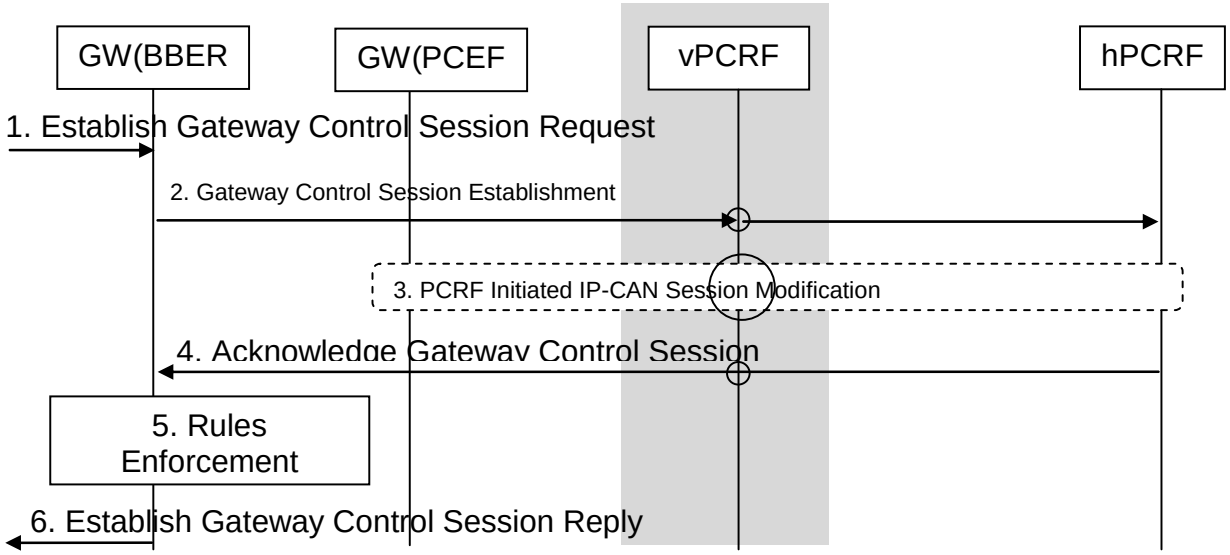

Figure 7.7.1-1: Gateway Control Session Establishment

1. The GW(BBERF) receives a message or indication that it must establish a Gateway Control Session.
2. The GW(BBERF) sends the H-PCRF a Gateway Control Session Establishment message. This will include information required to associate this session with a pre-existing IP-CAN Session, or if a IP-CAN session has not been established the information will be sufficient to select a PCRF and correlate a future IP-CAN session establishment with this session. In roaming scenarios, the Gateway Control Session Establishment message is sent to the vPCRF. The vPCRF may forwards the message to the HPCRF.

Editor's Note: It is FFS if the vPCRF if the vPCRF may hide the interaction from the hPCRF, for example in case the hPLMN supports on-path PCC model.

3. In case an IP-CAN session has already been established, the hPCRF correlates the Gateway Control Session with the IP-CAN session and performs an IP-CAN session modification procedure with the PCEF, if the PCC rules previously provided to the PCEF need to be updated.
4. The H-PCRF sends an Acknowledge Gateway Control Session Establishment to the GW(BBERF). This includes QoS Rules and Event Trigger information elements. In case of roaming scenario, this message goes through the vPCRF.

Editor's Note: It is FFS whether the V-PCRF may save information or other resources associated with Gateway Control Session.

Editor's Note: Bearer establishment may result from Step 4, though this is not yet shown in the figure.

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.

6. An indication of Gateway Control Session Established is sent to the entity that triggered the initiation of the session.

7.7.2 Gateway Control Session Termination

7.7.2.1 GW(BBERF)-Initiated Gateway Control Session Termination

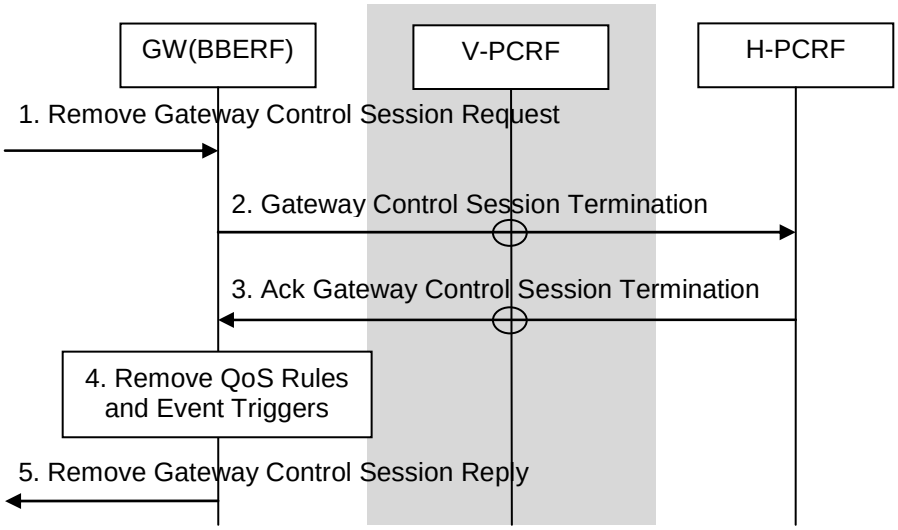

Figure 7.7.2-1: BBERF-Initiated Gateway Control Session Termination

1. The GW(BBERF) is requested to terminate its Gateway Control Session.

2. The GW(BBERF) sends a Gateway Control Session Termination message to the H-PCRF. If the GW(BBERF) is deployed in a visited network, this message is sent by the GW(BBERF) to the V-PCRF. The V-PCRF forwards the message to the H-PCRF.

Editor's Note: As a result of step 2, in the case where relocation is not being performed, there will be an IP CAN session termination procedure at this point.

3. The H-PCRF replies to the GW(BBERF) with an Ack Gateway Control Session Termination message. If the GW(BBERF) is deployed in a visited network, this message is sent by the H-PCRF to the V-PCRF. The V-PCRF forwards the message to the GW(BBERF).

Editor's Note: It is FFS whether the V-PCRF may release information or other resources associated with Gateway Control Session.

Editor's Note: It is FFS if the vPCRF if the vPCRF may hide the BBEF interaction from the hPCRF, for example in case the hPLMN supports on-path PCC model.

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

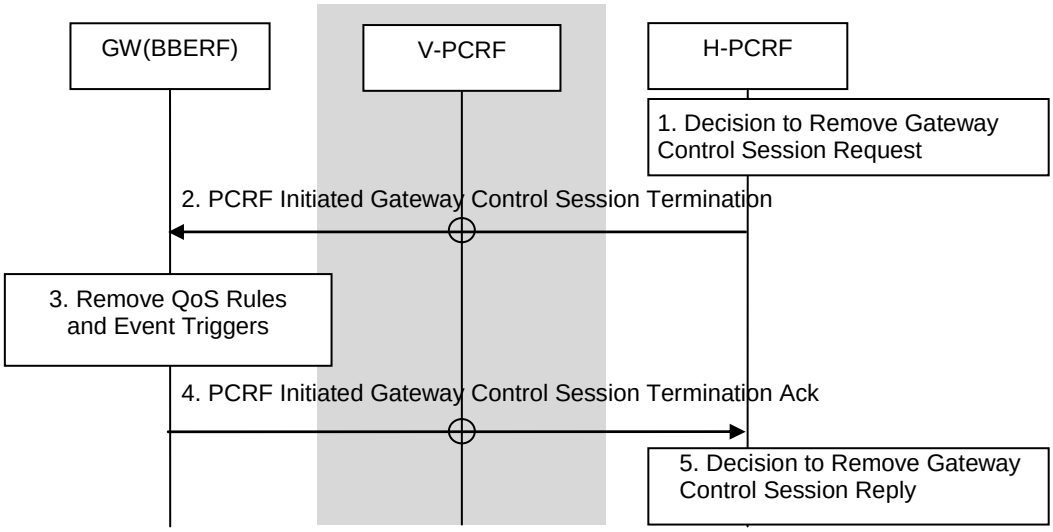

Figure 7.7.2-2: PCRF-Initiated Gateway Control Session Termination

1. The H-PCRF is requested to terminate its Gateway Control Session.
2. The H-PCRF sends a PCRF-Initiated Gateway Control Session Termination message to the GW (BBERF). If the GW (BBERF) is deployed in a visited network, this message is sent by the PCRF to the V-PCRF. The V-PCRF forwards the message to the GW (BBERF).

Editor's Note: It is FFS whether the V-PCRF may release information or other resources associated with Gateway Control Session.

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. The GW (BBERF) replies to the H-PCRF with an PCRF-Initiated Gateway Control Session Termination message. If the GW (BBERF) is deployed in a visited network, this message is sent by the GW (BBERF) to the V-PCRF. The V-PCRF forwards the message to the H-PCRF.
5. H-PCRF has completed terminating the session and can continue with the activity that prompted this procedure.

7.7.3 Gateway Control and QoS Rules Request

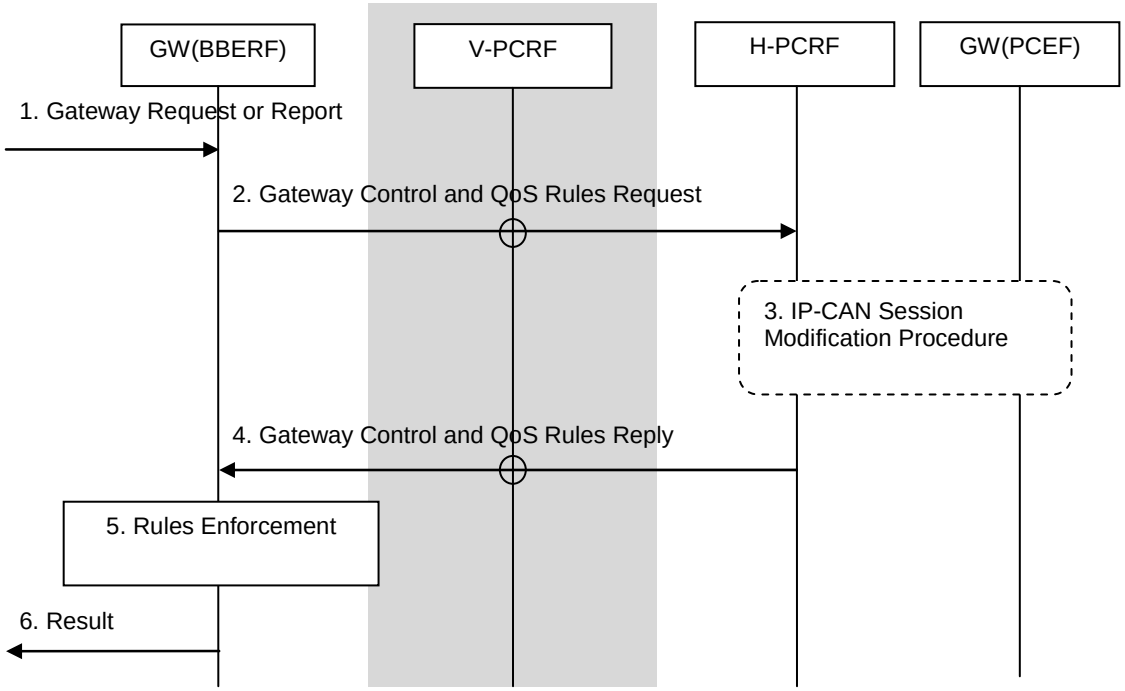

Figure 7.7.3-1: Gateway Control and QoS Rules Request

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 H-PCRF. If the GW (BBERF) is deployed in a roaming scenario, the message is sent to the V-PCRF and the V-PCRF forwards it to the H-PCRF.

Editor's Note: It is FFS whether the V-PCRF may be able to respond to the QoS Rules Request from the GW (BBERF) directly, without involving the H-PCRF, for example to support LBO scenarios.

3. The IP-CAN Session Modification Procedure may occur as the result of the Gateway Control and QoS Rules Request message, either to forward an Event Report to the GW (PCEF) or to issue revised PCC Rules, or both.

4. The H-PCRF sends a Gateway Control and QoS Rules Reply message to the GW (BBERF). If the GW (BBERF) is deployed in a roaming scenario the message is sent to the V-PCRF by the H-PCRF, and the V-PCRF forwards it to the GW (BBERF). This message may include QoS Rules and Event Triggers.

5. 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. Subsequent events corresponding to the Event Triggers will cause an Event Report to be delivered to the H-PCRF by means of a Gateway Control and QoS Rules Request procedure.

6. The GW (BBERF) has completed terminating the session and can continue with the activity that prompted this procedure.

7.7.4 Gateway Control and QoS Rules Provision

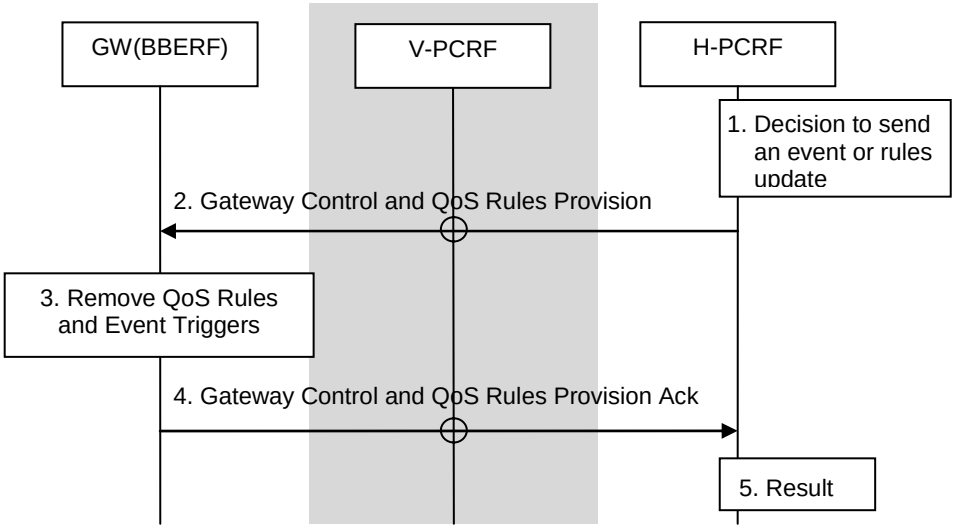

Figure 7.7.4-1: Gateway Control and QoS Rules Provision

1. The H-PCRF is requested to update the QoS Rules and Event triggers for a Gateway Control Session.
2. The H-PCRF sends a Gateway Control and QoS Rules Provision message to the GW (BBERF). If the GW (BBERF) is deployed in a roaming scenario, the message is sent to the V-PCRF and the V-PCRF forwards it to the GW (BBERF). This message will include QoS Rules and Event Triggers.

Editor's Note: It is FFS whether the V-PCRF may reach the decision to send QoS Rules to the GW (BBERF) autonomously, for example in the case of LBO.

3. 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. Subsequent events corresponding to the Event Triggers will cause an Event Report to be delivered to the H-PCRF by means of a Gateway Control and QoS Rules Request procedure.
4. The GW (BBERF) sends a Gateway Control and QoS Rules Provision Ack message to the GW (BBERF). If the GW (BBERF) is deployed in a roaming scenario the message is sent to the V-PCRF by the GW (BBERF), and the V-PCRF forwards it to the H-PCRF.
5. H-PCRF has completed updating the session and can continue with the activity that prompted this procedure.

7.7.5 Gateway Control Session Relocation

Gateway control session relocation occurs as a sequence. The new GW (BBERF) establishes a Gateway Control Session as described in clause 7.7.1. Then the old GW (BBERF) terminates its Gateway Control Session as described in clause 7.7.2.

NOTE: Between the conclusion of the first step (making a new session) and the second step (breaking the old session), there will be more than one Gateway Control Session Active.

Annex A (normative): Access specific aspects (3GPP)

A.1 GPRS

Editor's Note: It is FFS whether this section need to be maintained for Rel-8.

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.

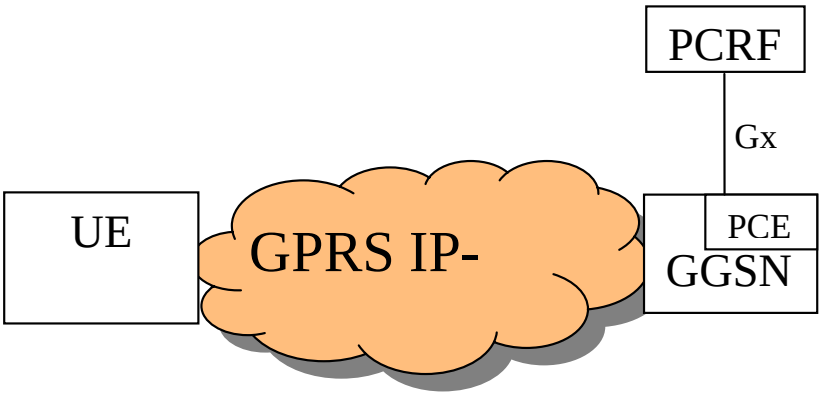

Figure A.1: The GPRS IP-CAN

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;
- 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 pre-defined 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.1.2 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.1.3 Functional description

A.1.3.1 Overall description

A.1.3.1.1 Binding mechanism

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 GPRS case bearer binding is performed by:

- PCRF, when the selected operation mode is UE-only, see [12], either due to PCRF decision or network/UE capability;
- PCEF, when the selected operation mode is NW-only;
- 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.

In order to identify the candidate PDP context the bearer binding shall compare:

- the PCC rule service data flow template with the TFT filters; and
- the PCC rule QoS parameters with the PDP context QoS parameters.

The binding mechanism shall comply with the established traffic flow template (TFT) packet filters (for the whole IP-CAN session).

The bearer binding shall bind a PCC rule:

- to a candidate PDP context with a matching QoS class;
- to a candidate PDP context with a matching QoS class that, after modification of the bitrates, fulfils the PCC rule QoS demands;
- to a new PDP context with a matching QoS class, 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).

A.1.3.1.1.2 Bearer binding mechanism allocated to the PCRF

If a new PDP context is required 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 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 TFT:s;
  - 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".

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.

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 credit re-authorisation triggers in table A.1 shall apply in addition to the ones in table 6.1.

Table A.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, has 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.

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-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 credit re-authorization if the report received is more detailed than requested by the OCS.

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.

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, has 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.

NOTE 1: Available only when the bearer binding mechanism is allocated to the PCRF.

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 procedures in TS 23.060 [12]).

A.1.3.2 Functional entities

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

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.

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 QoS Class Identifier to a UMTS QoS profile and vice versa. Each 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 QoS Class Identifier to/from QoS parameters

GPRS QoS Class Identifier value	UMTS QoS parameters			
	Traffic Class	**THP**	**Signalling Indication**	**Source Statistics Descriptor**
a	Conversational	n/a	n/a	speech (NOTE)
b	Conversational	n/a	n/a	unknown
c	Streaming	n/a	n/a	speech (NOTE)
d	Streaming	n/a	n/a	unknown
e	Interactive	1	Yes	n/a
f	Interactive	1	No	n/a
g	Interactive	2	No	n/a
h	Interactive	3	No	n/a
i	Background	n/a	n/a	n/a
NOTE: The operator's configuration should reserve QCI values that map to "speech" for service data flows consisting of speech (and the associated RTCP) only.				

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.

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.

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)

Void.

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

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.1.4 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.

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.

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.

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 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.

A.2 Void

A.3 Void

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

Editor's note: This clause is a placeholder for 3GPP Accesses (GERAN/UTRAN/E-UTRAN EPC) for GTP-based S5/S8.

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

Editor's note: This clause is a placeholder for 3GPP Accesses (GERAN/UTRAN/E-UTRAN EPC) for PMIP-based S5/S8.

Annex B (informative): Usage of PCC in the visited network

Editor's note: The content of this clause has been copied from TS 23.203 v.7.4.0. Roaming aspects in Release 8 will be specified in the normative parts of this specification. This annex is kept for information only and does not imply any specific guidance for Release 8.

Editor's note: The text in this annex includes information above and beyond clarifications to other normative clauses in this TS. It is FFS whether this annex will be made normative or be moved to another TR/TS.

B.1 Introduction

This clause relates to the use, by a roaming user, of services accessed via a GW in the visited network (i.e. a generic network; GPRS or IP-CAN).

B.1.1 General aspects

It cannot be assumed that service identifiers, pre-defined PCC rule names and PCC rule base names may be commonly understood between the home network and the visited network. The usage of PCC in the visited network is therefore limited to dynamic PCC rules

B.1.2 Charging related aspects

It cannot be assumed that charging keys may be commonly understood between the home network and the visited network.

B.1.2.1 Reporting

The reporting level of service usage within the visited network is based on the charging key and optionally, the service identifier value of the PCC rule.

The charging key and service identifier associated with reporting of service usage within the visited network shall be provided by the home network within the dynamic PCC rule information.

B.1.2.2 Credit Control

The account balance management function is located in the home network. The rating function is located in the home network and credit control shall only supply non-monetary units in credit control responses towards the visited network.

B.1.3 Policy control related aspects

PCC usage in the visited network is based on proxying of Gx messages between the V-PCEF and the H-PCRF by the V-PCRF. The H-PCRF includes additional functionality above the basic PCRF functions described in clause 6. The V-PCRF ensures that visited network policies can be enforced. The V-PCRF is an enhanced proxy and includes the functionality listed in clause B.1.6.4.

The logical V-PCRF and H-PCRF functions may be physically co-located with PCRF entities for non-roaming users.

B.1.4 Subscription related aspects

The subscription profile for the visiting user is located in the home network.

Typically, the home network shall provide sufficient subscription information so that the appropriate PCC rules can be provisioned to the visited GW. This includes providing information to identify PCC rules at bearer or access point level,

but may be unable to provide detailed enough subscription information for the visited network to construct service flow based rules. Charging parameters (e.g. charging method and OCS/OFCS addresses) may be provided only at bearer or access point level.

B.1.5 Architectural aspects

B.1.5.1 Logical architecture of PCEF in the visited network

When the PCEF is in the visited network for routing optimization, a reference point between the home PCRF and the visited PCRF is needed for information exchange. A logical roaming architecture is shown below.

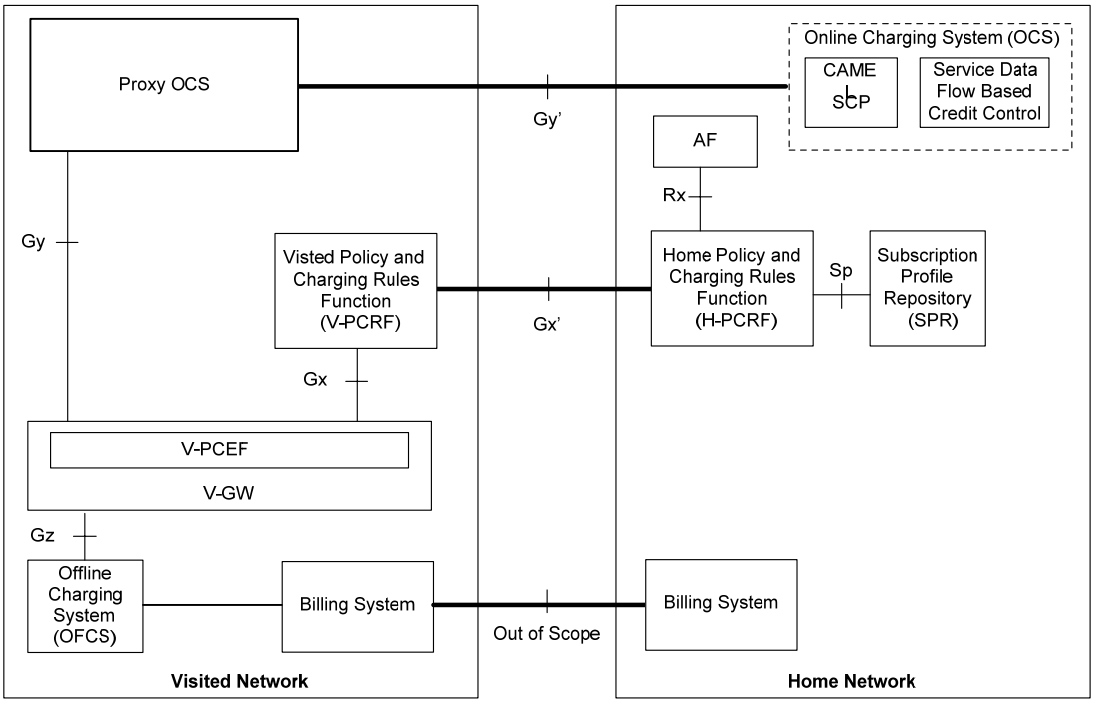

Figure B.1: Logical architecture of PCEF in the visited network

Editor's note-i: Whether to introduce a new reference point between the home PCRF and the visited PCRF or just to extend the existing reference point to support the PCC roaming is FFS.

Editor's note-ii: The need for a proxy OCS and whether to introduce a new reference point between the home OCS and the proxy OCS or just to extend the existing reference points to support the PCC roaming is FFS.

NOTE: The interface between the Billing systems is out of scope of this TS.

The following aspects have been identified for the architecture in figure B.1:

- Predefined PCC rules that are not part of the roaming agreement can not be dynamically activated by the H-PCRF. I.e. if a service data flow in the home network GW would use a dynamically activated pre-defined PCC rule that is not contained in the roaming agreement, then this service data flow will have to use a different PCC rule in the visited GW.

- The solution of the PCC roaming case should consider the topology hiding issue among operators.

B.1.5.1.1 Functional Requirements for supporting PCC Rules in the visited network

The support of V-PCEF requires the following functionality to be supported by the PCC Architecture:

- The PCC Architecture should enable the H-PCRF to determine whether a PCC rule needs to be implemented on a V-PCEF or a H-PCEF.

- The PCC Architecture should enable the initialization and maintenance of the connection between the V-PCRF and H-PCRF.

- The PCC Architecture should enable the VPLMN to indicate to the HPLMN that network initiated procedures for IP-CAN bearer establishment are supported for roaming subscribers.

B.1.5.1.2 Functional Requirements for Supporting On-line Charging in the visited network

The support of on-line charging in the VPLMN requires the following functionality to be supported by the PCC Architecture:

- The PCC Architecture should enable the VPLMN to indicate to the HPLMN that on-line charging is supported for roaming subscribers.

- The PCC Architecture should enable the HPLMN to indicate to the VPLMN that on-line charging is required for a particular IP-CAN session.

- The PCC Architecture should enable the VPLMN to discover the identity of the home OCS to which Credit Control messages will be sent.

- The PCC Architecture should enable the HPLMN to indicate to the VPLMN the Charging Key and optionally, the service identifier value of the PCC rule, to be used for a service-data flow.

B.1.6 Functional Entities

B.1.6.1 Visited-PCEF

In addition to the functionality defined in clause 6, the V-PCEF shall:

- when on-line charging is supported for roaming users, extract any OCS identifier received from the V-PCRF and include it in credit control messages sent to the proxy-OCS.

B.1.6.2 SPR

In addition to the information defined in clause 6, the SPR may provide the following subscription profile information for roaming users:

- Subscriber's roaming charging requirements, including whether a service cannot be used in case of roaming if on-line charging for roaming users is not supported by the visited network.

B.1.6.3 H-PCRF

In addition to the functionality defined in clause 6, the H-PCRF shall:

- be able to distinguish between policy and charging sessions for roaming users and home users (e.g., based on the domain which originated a request);

- be able to receive an indication from the V-PCRF regarding support for on-line charging and/or support of network initiated procedures for IP-CAN bearer establishment for roaming users;

- be able to reject any request for Policy and Charging rules from a visited network if the subscriber profile requirements cannot be met;

- in the case that on-line charging in the visited network is used, provide an OCS identifier to the V-PCRF.

B.1.6.4 V-PCRF

The V-PCRF is an enhanced Gx proxy between the V-PCEF and H-PCRF. The V-PCRF only includes the following functionalities:

- the V-PCRF shall be able to determine based on a subscriber identity included in a request for policy and charging rules whether the user is a roaming user and to identify the user's home network;
- the V-PCRF provides proxying of requests and responses between the V-PCEF and the H-PCRF
- the V-PCRF allows the visited network to implement local policy for roaming users. For example, enforcing inter-operator service level agreements. This includes the ability to reject authorized QoS decisions sent by the H-PCRF.
- the V-PCRF may include in any requests towards the H-PCRF information indicating visited network support of on-line charging and/or support of network initiated procedures for IP-CAN bearer establishment for roaming users;
- the V-PCRF shall include any OCS identifier received from the H-PCRF in messages sent to the V-PCEF

B.1.6.5 Proxy OCS

The proxy-OCS does not implement OCS functionalities as defined in specified in TS 32.296. The proxy-OCS provides simple proxying of credit control requests and responses between the V-PCEF and the OCS in the home network.

The proxy-OCS includes the following functionalities:

- The proxy-OCS is able to use information in requests received from the V-PCEF in order to determine the destination identity and realm of the OCS in the home network

B.2 Roaming Procedures and Flows

B.2.1 Introduction

The description includes procedures for establishing a V-PCEF to H-PCRF communication link including an example of V-PCRF rejection of a H-PCRF initiated policy decision.

Flows where the V-PCRF is providing simple proxying of Gx messages between the V-PCEF and H-PCRF are not included.

B.2.2 V-PCEF to H-PCRF communication link establishment

This clause describes the establishment of the communication link between a V-PCEF and H-PCRF. The signalling flow for IP-CAN Session establishment when the PCEF is in the VPLMN is used. The AF is not involved.

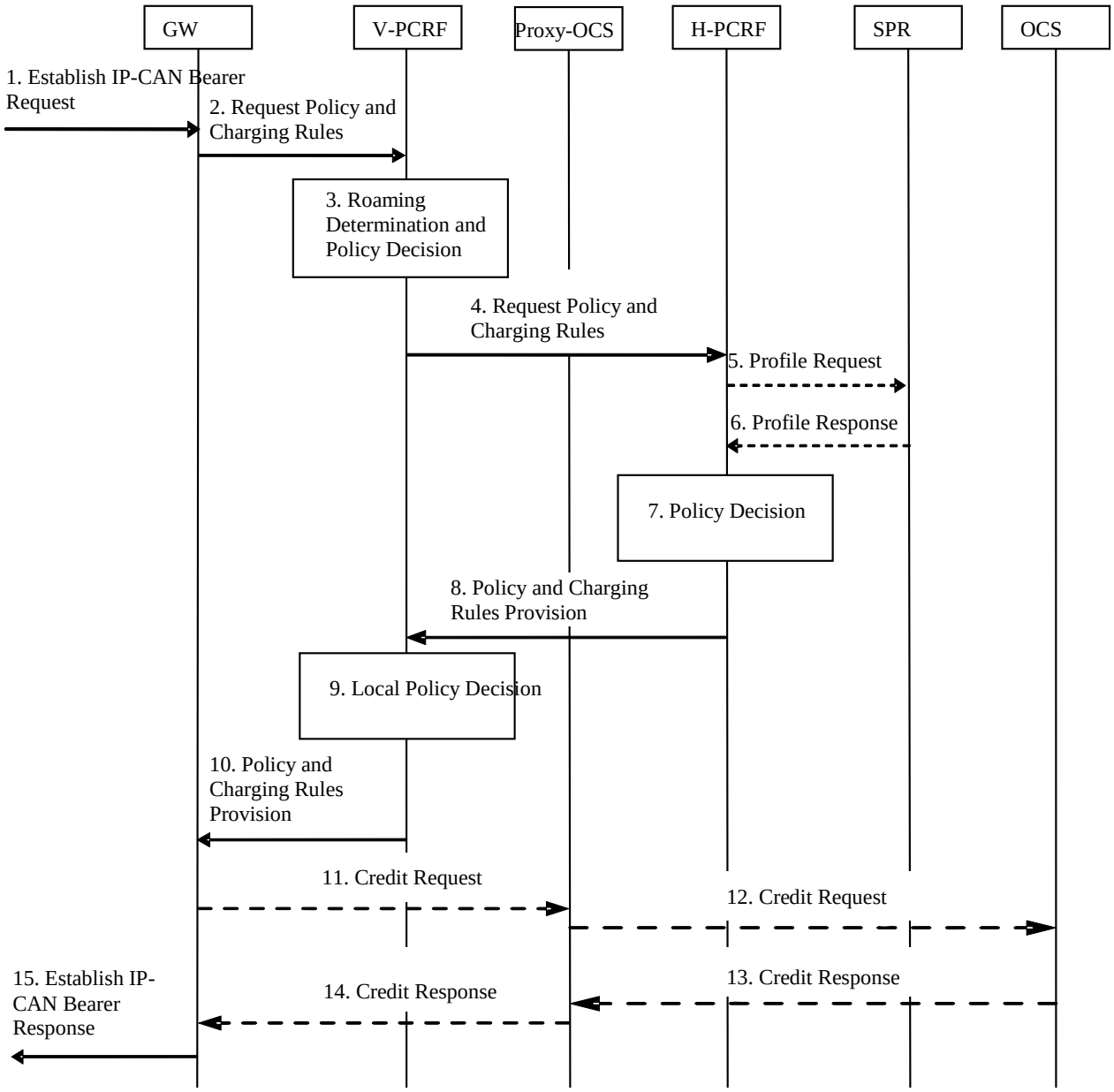

Figure B.2: V-PCEF to H-PCRF communications link establishment

1. The GW receives a request for IP-CAN Bearer establishment. The GW accepts the request and assigns an IP address for the user.

2. The GW determines that the PCC authorization is required, requests the authorization of allowed service(s) and PCC Rules information. The GW includes sufficient information in the request in order for the V-PCRF to determine that the user is roaming and to identify the user's home network.

3. The V-PCRF determines that PCC Authorization is required for a roaming user.

4. The V-PCRF requests the authorization of allowed service(s) and PCC Rules information from the H-PCRF. The V-PCRF includes information on whether on-line charging and/or support of network initiated procedures for IP-CAN bearer establishment for roaming subscribers is/are supported. The identification of the H-PCRF shall be derived from the identity of the user's home network.

5. If the H-PCRF does not have the subscriber's subscription related information, it sends a request to the SPR in order to receive the information.

6. The SPR responds with the subscription related information containing the information about the allowed service(s), PCC Rules information and information whether the on-line charging is necessary.

7. The H-PCRF determines that authorization is being requested from a visited network. The H-PCRF makes the authorization and policy decision. This may include denying the establishment of IP-CAN bearers for users of an on-line charging service if the VPLMN does not support on-line charging for roaming users.

8. The H-PCRF sends the decision(s) to the V-PCRF and charging keys and optionally, the service identifier value of the charging rule. If on-line charging is required to be supported, the identity of the OCS in the HPLMN is additionally provided.

9. The V-PCRF ensures that the decision(s) sent by the H-PCRF meet(s) local policy requirements. For example, based on the roaming agreement between the visited network and the user's home network, the V-PCRF may reject the authorized QoS received from the H-PCRF.

10. The V-PCRF sends the decision(s) to the GW including home OCS identity when included. The GW enforces the decision.

11. If online charging is applicable, and at least one PCC rule was activated, the GW shall activate the online charging session towards proxy OCS, and provide relevant input information for OCS decision. The GW shall additionally include the OCS identity in the credit request.

12. If online charging is applicable the proxy OCS shall activate online charging session towards HPLMN OCS, and provide relevant input information for the OCS decision. The proxy OCS shall derive the identity of the OCS from information provided by the GW.

13. If online charging is applicable the OCS provides the credit information to the proxy OCS and may provide re-authorisation triggers for each of the credits.

14. If online charging is applicable the proxy OCS provides the credit information to the GW and may provide re-authorisation triggers for each of the credits.

15. If credit is available for at least one charging key and at least one PCC rule was activated, the GW acknowledges the IP-CAN Bearer Establishment Request. When online charging is not applicable the IP-CAN bearer establishment is accepted if at least one PCC rule was activated.

B.2.3 V-PCRF rejection of a H-PCRF policy decision

This clause describes the rejection of a H-PCRF policy decision by the V-PCRF. The example signalling flow is for the roaming IP-CAN Session modification initiated by the H-PCRF. The AF may be involved.

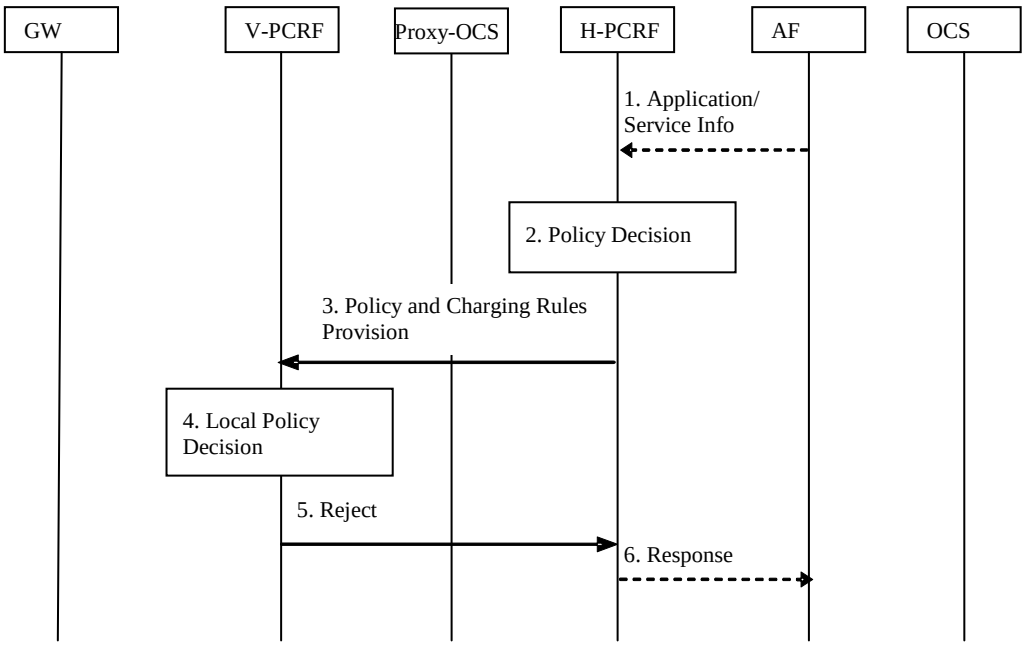

Figure B.3: V-PCRF rejection of a H-PCRF decision

1. Optionally, the AF provides service information to the H-PCRF due to AF session signalling.

Editor's Note: Optionally, without AF interaction, a trigger event in the H-PCRF may cause the H-PCRF to determine that the PCC rules require updating at the GW, e.g. change to configured policy.

2. The H-PCRF makes the authorization and policy decision.
3. The H-PCRF sends the decision(s) to the V-PCRF.
4. The V-PCRF polices the policy decision(s) sent by the H-PCRF, for example, based on the roaming agreement between the visited network and the user's home network..
5. The V-PCRF sends a response to the H-PCRF indicating that the policy decision(s) are rejected.
6. The H-PCRF responds with an indication to the AF indicating that the change in the AF session cannot be performed by the network.

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 (and its subclauses) 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.

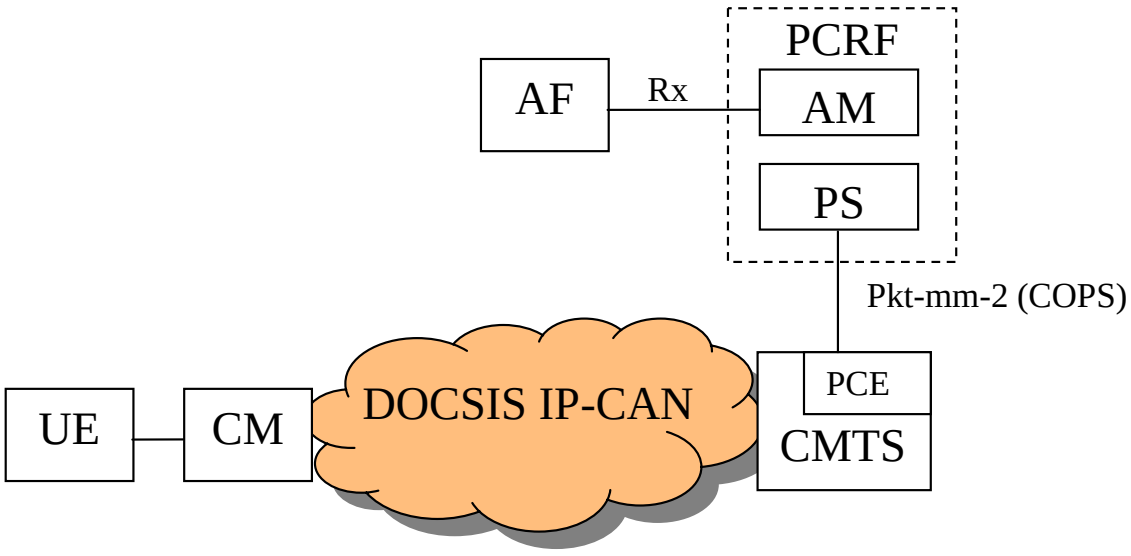

Figure D.1.1: DOCSIS IP-CAN

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.

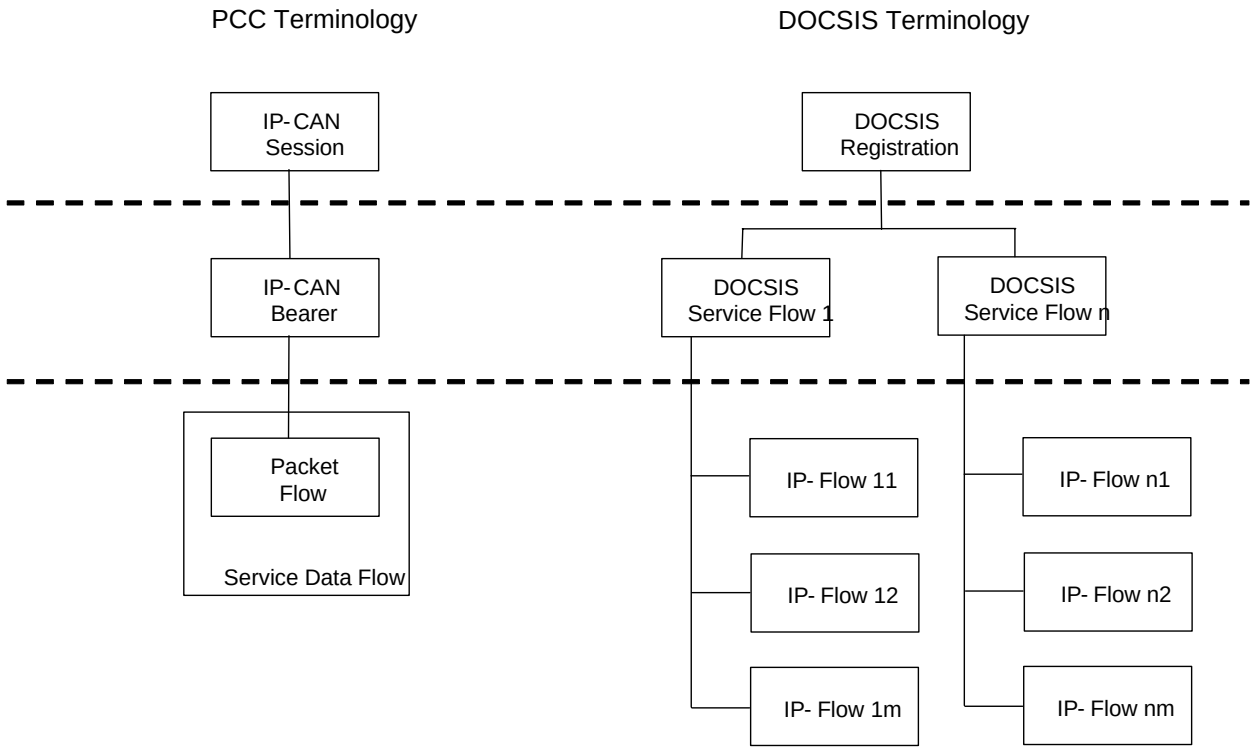

Figure D.1.2: PCC to DOCSIS terminology mapping

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 Sp reference point

Editor's note: Requirements placed on the Sp interface are FFS.

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.

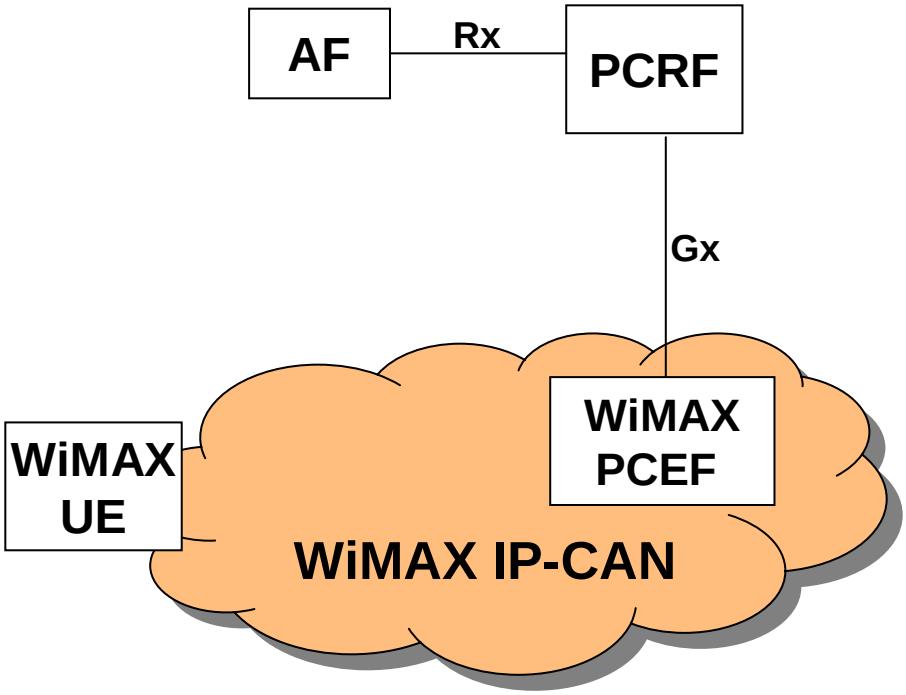

Figure D.2.1: WiMAX IP-CAN and 3GPP PCC

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): Reference Scenario for the evolution of QoS control

Editor's note: The content of this annex is copied from Release 7 TS 23.203. It is kept for information only with the intention to remove it when appropriate.

It is expected that following the successful standardisation of a network based QoS control mechanism in 3GPP, this functionality would start to appear in commercial networks in subsequent years. The specific time frame for this deployment will depend on many market factors, however for the purposes of the evaluation of this transitory phase the arbitrary timeframe of 2008-2010 is used purely as a point of reference.

In the period leading up to the availability of network based QoS control, it is anticipated that there will be a steady increase in the number of applications which use UE based QoS control to establish the necessary higher QoS bearers.

After network based QoS control becomes available, new applications may be deployed which make use of this model and older applications may be upgraded to make use of this new approach to QoS. However due to the population of legacy terminals and the need to manage migration of applications the UE based QoS control model will continue to be used in coexistence with the network based QoS control model. It is one possibility that over time the use of the UE based model will plateau and finally start to decrease. This projected usage of the two QoS models is shown in figure E.1.

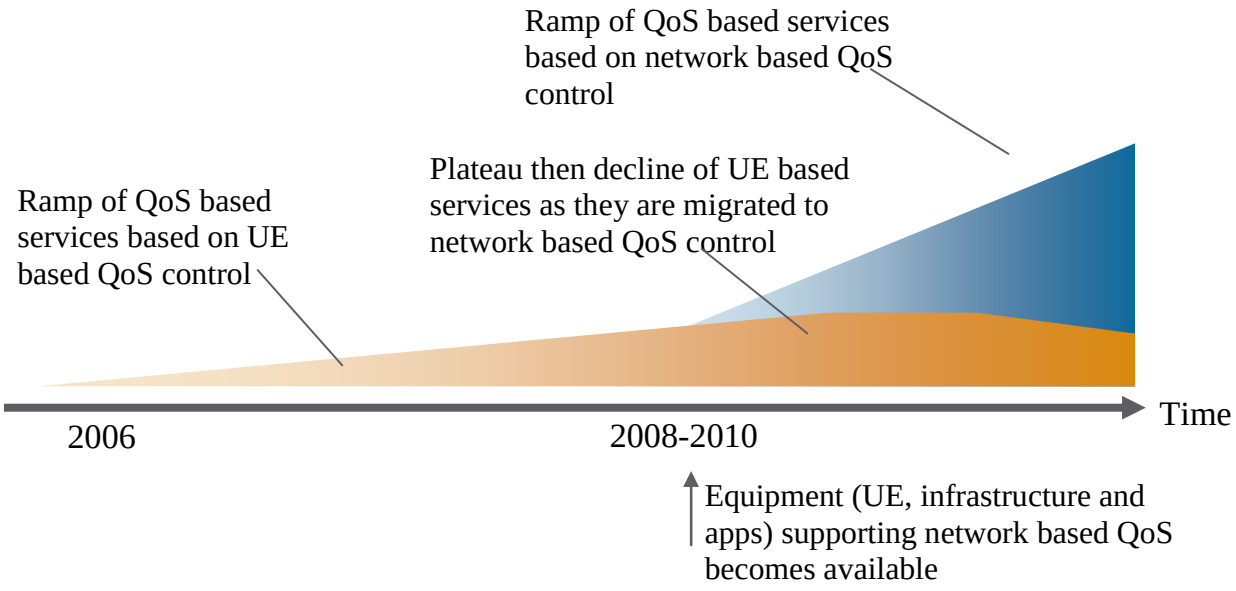

Figure E.1: Evolution Scenario for QoS Control

It can there be concluded that there is a requirement that 3GPP standards, in particular the GPRS and PCC specifications, efficiently facilitate the use of both the UE based and Networked based control of QoS to ensure a smooth evolution, following the introduction of Network based control of QoS.

Annex F (informative): Co-existence between SBLP based (Release 6) and PCC based (Release 7 and later) policy control

Editor's note: The content of this annex is copied from Release 7 TS 23.203. It is kept for information only with the intention to remove it when appropriate.

F.1 General

TS 23.203 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, I WLAN, Fixed Broadband, etc.):

- Flow Based Charging, including charging control and online credit control to allow for more granularity for end-user charging, accounting and online credit control;
- Enhanced Policy Control (e.g. gating control, QoS control, etc.) to allow the operator to perform service based QoS policy control;

TS 23.203 is an evolution of Flow Based Charging (i.e. FBC) as defined in TS 23.125 [7] and a replacement for Service Based Local Policies (i.e. SBLP) as defined in TS 23.207 [5]. From Release 7 onwards PCC supersedes FBC and replaces the SBLP architecture and functionality.

The purpose of this annex is to describe issues related to co-existence between Release 6 UEs/Networks with Release 7 UEs/Networks, in particular the role of the authorization token.

The following principles govern the co-existence between Release 6 SBLP and Release 7 PCC:

- Stage 2 specifications do not contain any requirements about which release nodes are allowed to interface with each other. It is assumed that nodes within an architecture belong to the same release.
- The Release 7 PCC architecture does not include any Gq reference point, Go reference point nor PDF (TS 23.207 [5]). Thus, there is no PDF generating any authorization token in the Release 7 PCC architecture.
- If the network employs SBLP, then the UE shall include the authorization token and flow identifier(s) in the secondary PDP context activation request as specified for Release 6. The UE may deduce that the network operates in Release 6 mode if an authorization token is received within AF signalling (SIP/SDP in the case of IMS).
- Alternatively, if there is no support for SBLP at the UE, the UE may decide to activate bearers without returning the authorization token by itself and it is up to the local policy as to whether these bearers are allowed. It should be noted that the return path for the authorization token is in GPRS session management signalling and not within AF SIP signalling (SIP in the case of IMS).

F.2 GPRS network scenario where the UE supports a previous Release

For GPRS, the PCC architecture is deployed on a per APN configuration basis, so that all IP-CAN sessions to that APN will use the Gx reference point for all the policy and charging control. An APN providing IMS services shall be configured to provide P-CSCF destinations to the UE, so that the P-CSCF will operate according to the Release 7 architecture, using the Release 7 Rx reference point for service authorizations. Since the SBLP authorization token is obsolete in the Release 7 architecture a UE connecting to an APN, configured for Release 7, will not receive any authorization token. Should a UE provide authorization token and flow identifiers to a Release 7 network, the GGSN will silently discard the authorization token and flow identifiers.

For the use of a UE in a network configured for a previous release, refer to that release.

The PCC architecture performs service to GPRS bearer binding as described in clause 6.1.1, without the need for an authorization token.

Annex G (informative): PCC rule precedence configuration

The precedence information is part of the PCC rule (see section 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.

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 pre-defined 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;
- pre-defined PCC rules known to the PCRF;
- pre-defined 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)

Editor's note: This clause is a placeholder for EPC-based non-3GPP accesses. This section focuses on aspects specific for a given non-3GPP access that terminates Gxa. The generic aspects of Gxa are described in the main body of this specification.

Annex I (informative): Documentation guideline for incorporating items from 23.401/23.402 into 23.203

This Annex contains a list of items that need to be added and/or updated in this specification to cover TS 23.401 [17] and TS 23.402 [18]. The list is sorted according to the outline of the main body of this specification.

This annex will serve as a guideline when writing and discussing Change Requests (CRs) to TS 23.203. It is assumed that the content of the annex will be removed once TS 23.203 is sufficiently stable.

In some cases multiple alternatives are possible as pointed out below. It is likely that actual work to produce the corresponding CRs is needed in order to agree on which way is preferable in these cases.

NOTE: The number within parenthesis refers to clause numbers in TS 23.203.

Definitions (3.1):

- Update of the definitions (e.g. GW control session).

Abbreviations (3.3):

- New abbreviations likely introduced ...

Charging Related Requirements (4.2):

- If is FFS if and what impact there is on the charging related requirements.

Policy Control Requirements (4.3):

- Roaming aspects of Policy Control, including LBO (4.3.3).

NOTE: Gateway Control related requirements (if needed) are captured in clause 6.

Architecture Model and Reference Points (5):

- The Reference Architecture for PCC to address both TS 23.401 [17] and TS 23.402 [18] is covered in this clause. It is FFS whether all scenarios fit in one reference architecture or if more than one reference architecture figure is needed. It is FFS whether on-path and off-path scenarios are shown in the same or in different reference architecture figures. It is also FFS whether a further sub structuring of clause 5.1 is useful when capturing the PCC reference architecture(s).
- In addition to the scenario shown in the Rel-7 PCC reference architecture, the following scenarios should be covered by TS 23.203:
  - Roaming architecture for LBO for both home and visited services: V-PCRF, H-PCRF, V-AF, H-AF (5.1).
  - Non-roaming architecture for PMIP-based S5/S8 (5.1).
  - Roaming architecture for PMIP-based S5/S8 (HR & LBO) (5.1) (LBO may not be needed as it should be equal to the combination of the above two).
- Reference points definition: Rx+ (5.2.1), Gx (5.2.2), S9 (5.2.x).

  NOTE: Gx is an evolution of Rel-7 Gx and is described in clause 5.2.2.

- Reference points definition for "off-path": Gxx (5.2.y), S9 (5.2.x).

Functional Description (6):

- QoS control: Default Bearer QoS control (PCRF may override default bearer QoS coming from HSS), ARP.
- Selection of PCRF (PCEF finds PCRF, AF finds PCRF, V-PCRF finds H-PCRF, AF finds H/V-PCRF) (6.1.x).

- Policy control (6.1.5):
  - PCEF vs functional role in S-GW/A-GW ("BBERF").
  - Policy control distribution and GW control.
- Event Trigger Handling in both entities (new IP-CAN types, etc.) (6.1.4).
- Functional Entities definition: V-PCRF (6.2.1.x), H-PCRF (6.2.1.y).
- PCRF handling of multiple legs (Gx, Gxa/Gxc, S9, Rx+) (6.2.1).
- Functional definition of the entity terminating Gxx: "Bearer Binding and Event Reporting Function (BBERF) (6.2.x).

PCC Rule definition (6.3):

- ARP support (6.3.1).

IP-CAN bearer and IP-CAN session related policy information (6.4):

- AMBR.

QoS Rule definition (6.x):

- *This description may also fit in 6.3.*

IP-CAN bearer and GW control session related information (6.y):

- Including description GW control event triggers and their scope (bearer/session).

PCC Procedures and Flows (7):

- *It is desirable that a small number of generic procedures cover multiple scenarios (on-path/off-path, roaming/non-roaming, Gxa/Gxc procedures when using S2a/S2c,…).*
- *There are different approaches for documenting the procedures:*

  1. *Include the GW control session signalling as optional elements in the procedures for IP-CAN session establishment/modification/termination, i.e. show both Gx and Gxa/Gxc procedures in the same call flows. Two sub-cases are possible:*

     a) *Same call flows for off-path and on-path. E.g: update existing flows in 23.203 with (optional) Gxa/Gxc and add new flows if needed, e.g. for "BBERF"-initiated procedures.*

     b) *Different call flows for on-path and off-path. Keep existing call flows for "on-path" and add new call flows for "off-path".*

     To avoid duplication of work in TS 23.402 [18] and TS 23.203 it may be feasible to remove or at least reduce the amount of PCC specification that is currently present in TS 23.402 [18].

  2. *Another approach is to describe Gx signalling in existing clauses 7.1-7.5 and GW control session signalling (Gxa/Gxc) in a separate sub-clause (7.6?), i.e. using separate call flows for Gx and Gxa/Gxc. The combined call flows with both Gx and Gxa/Gxc are instead shown in TS 23.402 [18]. The detailed PCRF handling and interactions between the Gxa/Gxc procedures and Gx procedures will have to be described separately, e.g. in clause 6.2.*

- The following use cases need to be covered:
  - UE-Requested Resource Handling: IP-CAN session modification (7.4.1), termination (7.3.1).
  - Off-path procedures (for S5/S8-PMIP, S2a): IP-CAN session establishment, modification, termination, including Gateway Control Session procedures.
  - Off-path procedures (for S2c): IP-CAN session establishment, modification, termination, including Gateway Control Session Procedures.

- Off-path procedures with roaming (for S5/S8-PMIP, S2a): IP-CAN session establishment, modification, termination, including Gateway Control Session Procedures.

- Off-path procedures with roaming (for S2c): IP-CAN session establishment, modification, termination, including Gateway Control Session Procedures.

Annex A.4. 3GPP Accesses (GTP-based):

- Specific charging requirements, event triggers, input for PCC decisions, identities, etc.

Annex A.5. 3GPP Accesses (PMIP-based):

- Specific charging requirements, event triggers, input for PCC decisions, identities, etc.

- Specific aspects of Gxc that are not covered by the generic Gxx description in the main body.

Annex X. EPC-based Non-3GPP:

- Specific charging requirements, event triggers, input for PCC decisions, identities, etc.

- Specific aspects of Gxa that are not covered by the generic Gxx description in the main body.

Annex J (informative): Change history

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**Old**	**New**
2007-12	SP-38	SP-070812	0059	2	B	Scope of the new 23.203	7.5.0	8.0.0
2007-12	SP-38	SP-070812	0060	2	B	Proposal of content for TS 23.203	7.5.0	8.0.0
2007-12	SP-38	SP-070812	0061	1	B	PCRF discovery principles	7.5.0	8.0.0
2008-03	SP-39	SP-080107	0062	2	B	Role of the V-PCRF	8.0.0	8.1.0
2008-03	SP-39	SP-080107	0063	1	B	Architecture and functional entities for Rel-8	8.0.0	8.1.0
2008-03	SP-39	SP-080107	0064	1	D	Documentation strategy for incorporating items from 23.401/23.402 into 23.203	8.0.0	8.1.0
2008-03	SP-39	SP-080107	0065	2	F	Rx reference point domain definition	8.0.0	8.1.0
2008-03	SP-39	SP-080107	0066	2	B	Clarification for PCRF Selection	8.0.0	8.1.0
2008-03	SP-39	SP-080107	0094	2	C	Definitions for 23.203	8.0.0	8.1.0
2008-03	SP-39	SP-080107	0095	2	C	PCRF Selection in roaming scenario	8.0.0	8.1.0
2008-03	SP-39	SP-080107	0096	2	C	CR for information storage in DRA	8.0.0	8.1.0
2008-03	SP-39	SP-080107	0105	2	B	Additional Procedures for PCC	8.0.0	8.1.0
2008-03	SP-39	SP-080107	0107	3	C	Tunnelled and untunnelled PCC rules in Release 8	8.0.0	8.1.0
2008-03	SP-39	SP-080106	0113	1	A	Clarification for PCRF initiated IP-CAN session termination	8.0.0	8.1.0
2008-03	SP-39	SP-080107	0115	-	F	Reference points renaming for 23.203	8.0.0	8.1.0
2008-03	-	-	-	-	-	Correction by MCC of Figure 5.1.2 (missing PCRF box) added by CR0063R1	8.1.0	8.1.1