

3GPP TR 23.803 V7.0.0 (2005-09)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Evolution of policy control and charging (Release 7)



The present document has been developed within the 3rd Generation Partnership Project (3GPP™) and may be further elaborated for the purposes of 3GPP.

The present document has not been subject to any approval process by the 3GPP Organizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPP only. The Organizational Partners accept no liability for any use of this Specification. Specifications and reports for implementation of the 3GPP™ system should be obtained via the 3GPP Organizational Partners' Publications Offices.

Keywords

UMTS, charging, QoS

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>

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© 2005, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TTA, TTC).
All rights reserved.

Contents

Foreword	5
Introduction	5
1 Scope	6
2 References.....	6
3 Definitions and abbreviations.....	6
3.1 Definitions	6
3.2 Abbreviations.....	7
4 Migration of FBC and SBLP => PCC.....	7
4.0 General	7
4.1 Functional requirements	7
4.1.1 Overall functional requirements	7
4.1.2 Policy related functional requirements	8
4.1.3 Charging related functional requirements	8
4.1.4 Unified method for routing and transfer of packets	9
4.1.4.1 The dedicated IM CN signalling context	11
4.1.4.2 Services, which are subject to policy control.....	11
4.1.4.3 Services, not subject to policy control	12
4.2 Architectural concepts	12
4.2.0 General.....	12
4.2.1 Reference Model.....	13
4.2.2 Reference Points.....	13
4.2.2.0 General.....	13
4.2.2.1 Rx+ reference point	13
4.2.2.2 Gx+ reference point	14
4.2.3 Functional elements	14
4.2.3.1 Policy Control and Charging Rules Function (PCRF)	14
4.2.3.2 Gateway (GW)	15
4.2.3.3 Application Function (AF).....	15
4.2.4 Relationship between functional elements.....	16
5 Subscription aspects.....	16
5.0 General	16
5.1 Functional requirements	16
5.2 Architectural concepts	16
5.2.1 Reference Model.....	16
5.2.2 Reference Points.....	16
5.2.2.1 Sp reference point	16
5.2.3 Functional elements	17
5.2.3.1 Subscription Profile Repository (SPR)	17
5.2.3.2 Policy and Charging Rules Function (PCRF)	17
6 Binding IP bearers to services	17
6.0 General	17
6.1 Architectural concepts	17
6.1.1 Authorisation Token based binding	17
6.1.1.1 General.....	17
6.1.1.2 Authorization Token based binding for PCC.....	19
6.1.2 UE IP address based binding.....	19
6.1.3 UE IP address + TFT based binding.....	19
6.1.4 UE Identity based binding	22
6.1.5 Exchange of filter information	22
6.2 Conclusions	22
7 Signalling Flows	23
7.1 Bearer Service Establishment and Modification without AF Interaction	23

7.2 Bearer Service Establishment and Modification with AF Interaction24

7.3 Bearer Service Termination25

7.4 Rule Update26

8 Conclusions and recommendations27

Annex A: Service Data Flow based QoS control.....29

A.1 Functional requirements29

A.2 Impacts to interfaces.....29

A.2.1 Gx+ interface29

Annex B: Change history30

Foreword

This Technical Report 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

During the course of Release 6 standards development some new features have been introduced to provide advanced core network capabilities for packet-based services:

- Enhanced policy control allows the operator to perform service based QoS policy control for their session-based PS applications;
- Flow-based charging allows more granularity for end-user charging, accounting and online credit control.

While some level of convergence between these functions has already been achieved in Release 6, a full harmonization of these functions is studied within the present document. Such harmonization is essential when optimizing realtime interactions of the GGSN (and gateways of other IP Connectivity Access Networks), and optimizing the realtime control architecture of GPRS in general.

A further aspect that remains to be studied is how differentiation based on end-user subscription classes can be achieved. In addition it should be studied how non-QoS policy control functions (e.g. service authorization, control of redirect functions etc.) fits in the harmonised architecture. These aspects are important in order to fully capitalize on the new core network capabilities described above. It shall also be studied whether the Authorization Token can be removed in the PCC architecture.

1 Scope

The present document intends to study the following items:

- 1) Complete harmonization and merger of the policy control and flow based charging architecture and procedures;
- 2) Possible architectures and solutions for adding end-user subscription differentiation and general policy control aspects to the policy- and charging control;
- 3) Alternative solutions for binding bearers to services (provided today by the authorization token). This includes studying solutions for the network to control bearer usage by service flows.

Editors Note: The document may also study the impact on policy control and flow based charging architecture based on the conclusion and approved recommendations of the E2E QoS Work Item in a Release 7 context if deemed feasible.

2 References

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

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

- [1] 3GPP TR 41.101: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Technical Specifications and Technical Reports for a GERAN-based 3GPP system".
- [2] 3GPP TS 23.207: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; End-to-end Quality of Service (QoS) concept and architecture".
- [3] 3GPP TS 23.125: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Overall high level functionality and architecture impacts of flow based charging; Stage 2".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply.

Default PDP context: In GPRS, a general purpose PDP context for which the GW has no information to use for downlink traffic mapping for a particular PDP address and APN pair.

Gateway: For the purposes of this document, "Gateway" refers to the gateway element of the IP-CAN, e.g. the GGSN in case of GPRS, or the PDG in case of WLAN Interworking. The Gateway contains functionalities of the Traffic Plane Function defined in TS 23.125 [3], and of the 3GPP Policy Enforcement Point defined in TS 23.207 [2].

Policy and Charging Control architecture: An architecture based on functionality provided by both service based local policy, see TS 23.207 [2], and flow based charging, see TS 23.125 [3].

Service data flow: aggregate set of packet flows. In the case of GPRS, it shall be possible that a single PDP Context transports multiple service data flows.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AF	Application Function
CRF	(Service Data Flow Based) Charging Rules Function
FBC	Flow Based Charging
GW	Gateway
IP-CAN	IP Connectivity Access Network
PCC	Policy and Charging Control
PCRF	Policy and Charging Rules Function
PDF	Policy Decision Function
PEP	Policy Enforcement Point
SBLP	Service Based Local Policy
SPR	Subscription Profile Repository
TPF	Traffic Plane Function

4 Migration of FBC and SBLP => PCC

4.0 General

TS 23.207 [2] specifies the Service Based Local Policy architecture, and TS 23.125 [3] specifies the Flow Based Charging architecture. This clause studies a merged architecture in order to provide more efficient real time control of the service flows in the GWs (e.g. the GGSN, and other IP-CAN gateways, like the PDG).

The PCC architecture should build on the work achieved in Rel-6 Flow Based Charging which includes how policy can be provided with the Rel-6 FBC reference points (Gx, Gy, Rx) in the context of multiple service data flows on one single bearer. PCC should continue the rel6 work by enhancing the Rel-6 interface specifications of the relevant FBC reference points.

4.1 Functional requirements

4.1.1 Overall functional requirements

The migration towards a PCC architecture should be simple. The migration may be from any possible combination of implementations e.g. policy control only architecture towards a PCC architecture or independent SBLP and FBC architectures towards a PCC architecture.

It shall be possible for the PCRF to base decisions upon Subscription information. The PCC architecture shall minimize the amount of Subscription information duplicated to what is relevant input for policy decisions.

It shall be possible to apply the PCC model to any kind of bearer (e.g. for GPRS to any PDP Context).

The PCC architecture shall allow for service data flows to have only FBC applied without associated policy related control concurrently with service data flows that have both FBC and policy related functions applied to one bearer. The architecture shall have a binding method that allows the unique association between AF IP flows and their bearer (for GPRS the PDP context).

The PCRF shall provide a single set of filters for policy control and flow based charging.

To ensure that the architecture is not too complex there shall be a single reference point:

1. between the PCRF and the AF, and
2. between the PCRF and the GW.

4.1.2 Policy related functional requirements

Gating control: The process of blocking or allowing packets, belonging to a service data flow, to pass through to the desired endpoint. It shall be possible to apply gating control to control sessions that may otherwise be prohibited by operator policy and irrespective of the charging applied. An example of this is the opening and closing of specific connections for peer-to-peer sessions.

Session events: The notification of and reaction to application events (such as session termination and modification) to trigger new behaviour in the user plane. To enable gating control, session events shall be supported. For example, session termination, in gating control, may trigger the blocking of packets or "closing the gate".

QoS authorisation: The "Authorised QoS" specifies the maximum QoS that is authorised for IP flow(s). In case of an aggregation of multiple IP flows within one bearer (e.g. for GPRS a PDP context), the combination of the "Authorised QoS" information of the individual IP flows is provided as the "Authorised QoS" for the bearer. It shall be possible to grant, deny or change the "Authorised QoS" of a bearer by using criteria such as the QoS subscription information.

Editor's note: Minimum QoS authorization is FFS.

The QoS policies can be service-based, subscription-based, or default policies. The PCRF communicates with Application Functions to determine the proper authorized resources for the session-based services.

QoS policies may be dynamically provisioned by the PCRF or predefined as a default policy in the GW. In case the PCRF provides charging rules dynamically over Gx+ interface, "Authorised QoS" information for the bearer (combined QoS) is provided. When the PCRF activates predefined charging rules within the TPF it can be assumed also that corresponding authorized QoS information are predefined in the GW and activated at same time. The GW shall combine the different sets of authorized QoS information, i.e. the information received from the PCRF and the information corresponding to the predefined charging rules.

Editor's note: Considerations on providing QoS class for individual service data flows are described in Annex A.

QoS enforcement: QoS enforcement shall be supported in line with PEP capabilities defined for SBLP. QoS enforcement can include downgrading of the requested bearer QoS by the Gateway as part of bearer establishment. The Gateway shall also enforce unsolicited changes in the "Authorised QoS" that arrives through the Gx+ interface.

Editor's note: the ability to upgrade the requested bearer QoS by the Gateway as part of bearer establishment is FFS.

The alternatives to the Token based binding do not inherently convey any information to the PCRF whether a bearer authorization from an AF is required for the specific bearer. If the AF provides the authorization to the PCRF prior to signalling that service is granted to the terminal the PCRF already has the authorization when the GW makes the request. However, if a terminal requests a bearer, corresponding to a service requiring authorization, prior to the AF providing the authorization to the PCRF or where no AF interaction is expected, the PCRF must make a decision based on other information, available locally at the PCRF.

Editor's note: The details on how the PCRF shall behave when a request for a bearer, lacking from the corresponding authorization, is received is FFS. The PCRF procedures shall be specified in such a way that PDP contexts, without any active charging rule, are not allowed.

The PCRF may maintain information on, or receive such information from an AF, whether a service may start on any bearer that could transfer the traffic or whether a bearer dedicated for this traffic is required (TFT). For such services the PCRF may permit the service on an already established bearer. When the UE requests the dedicated bearer, the PCRF shall map the service data flow to this bearer.

4.1.3 Charging related functional requirements

Charging correlation: Charging correlation, between application level and bearer level, shall be supported.

Charging Control: IP Flows are identified based on the charging rules defined in TS 23.125 [3] (although it is expected that the rules are evolved in a Rel-7 context). Subscription data could be taking into account in this process. A (evolved) charging rule may be predefined in the GW or dynamically provisioned by the PCRF.

The AF charging identifier (e.g. ICID in case of IMS), if available, shall be transferred from the AF to the PCRF, which shall forward it to the Gateway. Access Network charging identifier (e.g. GCID in the GPRS case), if available, shall be transferred to the AF.

4.1.4 Unified method for routing and transfer of packets

The Rel-6 architecture specifies 3 methods for mapping traffic to a PDP context. They are:

- a) the IM CN dedicated signalling context method, defined in TS 29.061,
- b) the SBLP filter method, defined in TS 29.207, and
- c) the TFT filter method, defined TS 23.060 (section 9.3 "Packet Routing and Transfer Function").

Unifying these methods, retaining the desired features of each method, is feasible.

Unifying the packet mapping methods to a single PCC filter method, based on PCC filters, simplifies understanding what governs that a certain downlink IP packet is transmitted on a certain PDP context. The user plane routing and transfer of packets involves the steps:

1. The GW locates the set of PCC filters, corresponding to the destination IP address for the packet.
2. The GW evaluates for a match against the installed PCC filters in precedence order.
3. In case of a match, the GW maps the packet to the PDP context associated with the matching PCC filter.
4. In case of no match the GW discards the packet.

NOTE: For GPRS, the concept of a default PDP context (i.e. without TFT) is retained by the possibility to have a PCC filter that is completely wildcarded.

Editor's note: The term "PCC filter" shall be considered as a temporary working name only, and may be changed to a proper name once the work enters normative specification stage.

If the PCRF provides PCC rules with the same filters and precedence order, as the UE provides with the TFT filters, the PCC filter method yields the same result. However, as there is no means to inform the UE about the way how PCC filters are assigned to multiple bearers, it is important to base the PCRF assignment on the UE provided TFT filters. Otherwise, the UE would have a different understanding about which service data flows are allowed on which bearers.

The features of the 3 methods differ. A comparison is shown in Table 4.1.

Table 4.1: Rel-6 methods vs. PCC methods for downlink traffic mapping

Characteristic / feature	Rel-6			Rel-7
	Dedicated signalling context method	SBLP method	TFT filter method	PCC filter method
Precondition for the method	The PCO flag <i>IMCN Subsystem signalling</i> is set for the PDP context.	The UE has provided SBLP binding information for the PDP context and the PDF has provided one or more <i>SBLP filters</i> .	The UE has provided one or more <i>TFT filters</i> for the PDP context.	The UE has provided one or more <i>TFT filters</i> for the PDP context and the PCRF has provided PCC filters (note 1)
Source for filter definition	Local configuration at the GGSN	PDF	UE	PCRF or GW (note 2).
Filter format	TFT filter (TS 24.008)	FrwkIpFilterEntry (RFC 3318) (note 3)	TFT filter (TS 24.008)	IPFilterRule (RFC 3588) (note 4)
Method for resolving filter overlap within the method	Not a problem. All filters map to the same PDP context and these filters are tried before any other kind of filter.	Every filter maps to a single PDP context and as long as these filters are accurate no precedence order is needed.	TFT filter precedence	PCC filter precedence.
Filter precedence within the method	Same for all filters.	Same for all filters	According to TFT filter precedence value.	PCC filter precedence.
Filter precedence in relation to other methods	Higher than the SBLP methods.	Higher than the TFT filter method.	Lower than dedicated signalling PDP context and SBLP filters.	Not applicable. One unified method for all traffic.
Method for modifying a filter	Local configuration at the GGSN. (Constant throughout the PDP context life cycle?)	PDF decision based on AF session modification.	PDP context modification procedure (MS-initiated) and TFT change occurs.	The source (note 5) of the filter may modify a filter.
Add/remove filter	Local configuration at the GGSN. (Constant throughout the PDP context life cycle?)	PDF decision based on UE initiated binding modification..	PDP context modification procedure (MS-initiated)	The PCRF (note 5) may add/remove PCC filters, which are installed on demand. Default predefined PCC filters (note 6) may be added/removed by local administration at the GW.
Gating	No.	Yes.	By special Configuration of charging rules.	A PCRF-controlled attribute of the PCC filter.
Re-map a service data flow to another PDP context.	N/A	UE-controlled.	UE-controlled (note 7).	UE-controlled

NOTE 1: Includes filters that are predefined at the GW. c.f. FBC predefined charging rules.

NOTE 2: e.g. for IMCN dedicated signalling.

NOTE3: This is the representation on Go. The PDF receives the filter over the Gq (TS 29.209) in IPFilterRule (RFC 3588) format.

NOTE 4: The GW may define predefined PCC rules, by local means, based on any format. e.g. TFT filter for IMCN signalling.

NOTE 5: i.e. the PCRF for filters provided from there and local configuration at the GW for predefined filters .

NOTE 6: i.e. filters that are unconditionally installed on all PDP contexts.

NOTE 7: The UE modifies the sets of TFT filters on both PDP contexts.

4.1.4.1 The dedicated IM CN signalling context

For the dedicated IM CN signalling context, a flag in the Protocol Configuration Options indicates that the UE requests such a PDP context (at PDP context activation). The flag is returned in the PCO field of the accept message to the UE if the request is successfully completed. A dedicated signalling context shall be considered to have a TFT.

Thus, the Rel-6 specification specifies that:

- the dedicated signalling shall be described in TFT filter format and
- the description is a static description at the GGSN.

For PCC:

- a) At PDP context activation, the GW shall report to the PCRF whether the PCO "IM CN Subsystem Signaling Flag" will be set or not.
- b) The GW shall have an inactive predefined PCC rule (or set of rules) taking priority over any other PCC rule and corresponding to the static packet filters as defined in TS 29.061;
- c) The PCRF shall install (i.e. activate) that PCC rule (or set of rules) as the sole PCC rule (or set of rules) for that PDP context when the PCO "IM CN Subsystem Signaling Flag" was received.

NOTE: A dedicated signalling context is normally not subject to any end user charges. The charging key(s) shall be coordinated with the OCS in order to yield the proper charge for signalling.

4.1.4.2 Services, which are subject to policy control

For services, which are subject to policy control a PCRF either

- Based on PCRF configuration knows the information required for policy control and charging or,
- PCRF relies on AF interaction for completing the information required for policy control and charging.

It is assumed that the UE provides accurate TFT filters

Thus, the PCRF can always determine whether a TFT filter captures any traffic requiring policy control.

Multiplexing services requiring policy control and other services on the same PDP context is an option, which may reduce the total number of PDP contexts required.

Editors note: It is FFS if multiplexing can maintain the appropriate QoS for the services subject to policy control.

For PCC:

- a) For each PCC filter the PCRF shall analyze all TFT filters in the order of their precedence indicated within the TFT. The PCRF shall install the PCC filter on the PDP context corresponding to the first matching TFT filter. Any remaining PCC filters shall be installed on the bearer for which no TFT filters have been received if such a bearer is available.
- b) The PCRF may be configured or receive information from the AF, indicating whether a PCC filter may be installed for a PDP Context without any signalling of a corresponding TFT filter from the UE for the PDP context.

Editors note: It is FFS how the PCRF selects the appropriate PDP context if there is more than one bearer capable to transfer the service data flow (e.g. one PDP context without TFT and one PDP context with a coarse but matching TFT filter).

- c) It shall be possible that both traffic subject to, and traffic not subject to policy control is multiplexed on the same PDP context. The traffic not subject to policy control should be policed at the GW, so that the integrity of the authorized QoS for the traffic subject to policy control is maintained.

Editors note: It is FFS how the GW derives the information required for the policing of the traffic that is not subject to policy control.

4.1.4.3 Services, not subject to policy control

For services, which are not subject to policy control, full backwards compatibility with Rel-6 FBC shall be maintained. As the PCC filters replace the TFT filters for the actual mapping of downlink traffic mapping, the PCRF should not install any PCC filter, which captures traffic that would not have matched any TFT filter, for a PDP context (except for a PDP context without TFT).

4.2 Architectural concepts

4.2.0 General

The SBLP and FBC architectures each provide a set of data flow filters, and associated rules / instructions to the Gateway (e.g. to the GGSN). The Gateway then uses these filters to perform policy control and flow-based charging functions, respectively. To optimize the handling of IP packet filters in the Gateway, it shall be possible for the PCC architecture to provide a single set of filters to the Gateway that would be used for policy control and/or flow-based charging.

The SBLP and FBC architectures each provide an interface for Application Functions so that AFs can provide service related information that serve as input for policy control and flow based charging, respectively. To optimize the handling of service related information in the network, it shall be possible to use a single interface for AFs to provide this information.

For Rel-6 policy control over the binding mechanism, as specified in 23.207, uses an Authorization Token and one, or more Flow Identifiers. An important role for the token is to provide address information to the GGSN for finding the PDF that issued the token, thus being the node to contact for seeking authorization for the flows described by the Flow Identifiers. The Rel-6 Flow Based Charging architecture ensures that both the TPF and an AF, which requires information being provided to the CRF for the user session, contacts the same CRF. For Flow Based Charging, the TPF contacts the CRF based on access point the UE connects to (i.e. APN) and the AF contacts the CRF based on the end user (IP) address as experienced at the AF.

The Rel-7 PCC shall re-use the Rel-6 FBC TPF --> CRF addressing mechanism of Flow Based Charging for the GW --> PCRF addressing. As the Flow Based Charging solves the problem of the AF finding the same CRF as the TPF contacts, the Rel-7 AF shall re-use the Rel-6 AF --> CRF addressing mechanism of Flow Based Charging for the AF --> PCRF addressing.

4.2.1 Reference Model

The reference model of the PCC architecture is described in figure 4.1 below:

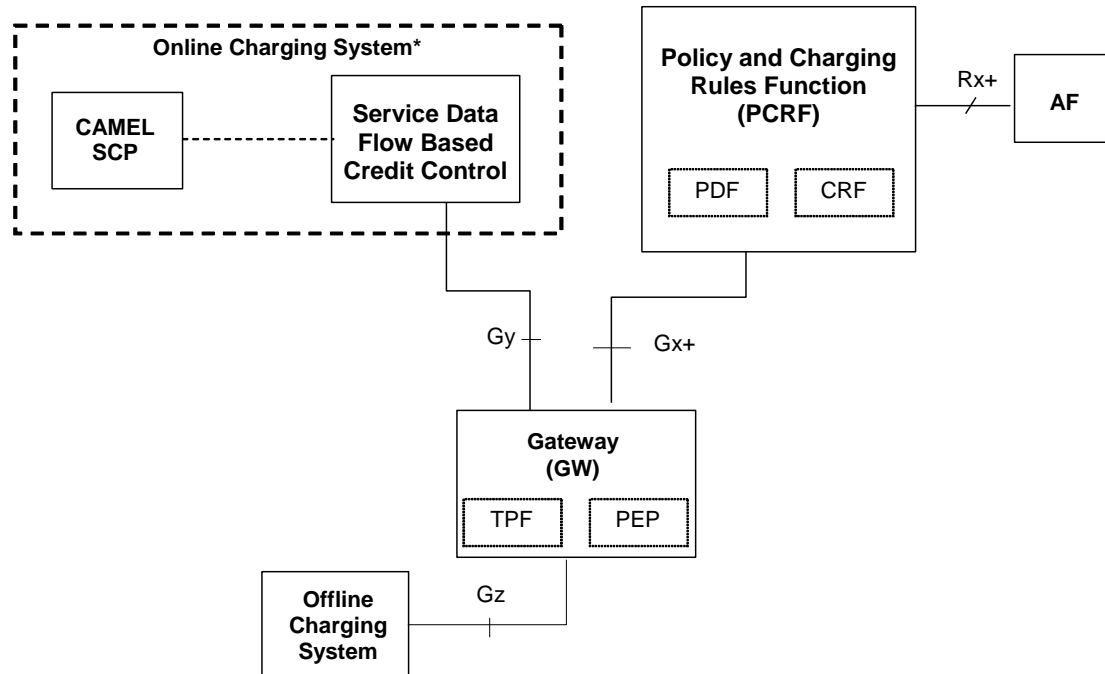


Figure 4.1: Overall architecture for combined policy and charging control

NOTE: Support for the Rel-6 Gq and Rx reference points is implementation and deployment specific and is therefore not further addressed in this TR..

4.2.2 Reference Points

4.2.2.0 General

The reference points for the PCC architecture use and enhance the interfaces used in Rel-6 FBC.

4.2.2.1 Rx+ reference point

The Gq reference point enables transport of dynamic service information from the AF to the PDF. An example of such information is IP filter information to identify the service data flow for gating control and media/application information with bandwidth requirements for QoS control. The Gq reference point is also used to transport Authorisation Token from PDF to AF. The Rx reference point enables transport of dynamic service information from the AF to the CRF. An example of such information is IP filter information to identify the service data flow for differentiated charging.

Rx+ reference point can be realized by combining relevant parts of Rx and Gq reference points within a single protocol, as most of the information transferred between the AF and the CRF/PDF are common.

The single protocol of this Rx+ single reference point between AF and PCRF that allows for all Rel-6 capabilities of the Gq and Rx reference points, plus all identified enhancements of Rel-7, shall be backwards compatible with the Rel-6 (i.e. Rel-7 PCRF can support interacting with Rel-6 AFs and Rel-7 AFs can support interacting with a Rel-6 PDF and/or Rel-6 CRF).

Editor's note: "Rx+" shall be considered as a temporary working name only, and will be changed to a proper reference point name once the work enters normative specification stage.

4.2.2.2 Gx+ reference point

The Rel-6 Gx reference point enables the use of service data flow based charging rules such as counting number of packets belonging to a rate category in the IP-Connectivity Network. This functionality is required for both offline and online charging. The Rel-5/6 Go reference point enables service-based local policy and QoS inter-working information to be transferred from the PDF to the PEP. In the PCC architecture the Go reference point can be realized together with Gx reference point with single protocol, using single message sequence to communicate both SBLP decisions and charging rules. Adding some new information elements to the existing Rel-6 Gx protocol to fulfil also SBLP requirements described in the chapter 4.1.2 can do this.

One of the enhancements to be made to R6 Gx is to include the "Authorised QoS" information from PCRF to Gateway, so the Gateway can enforce the Authorised QoS at any time.

Gx+ shall evolve the charging rules defined in TS 23.125 [3] to support gating functionality (uplink and downlink).

The following list defines additions needed for Rel-6 Gx interface to support Rel-5/Rel-6 Go functionality:

- New parameters for authorization token and flow Id are needed;
- New parameters for "Authorized QoS" information (QoS class and bitrate) are needed;
- Flow description needs to be completed with enable/disable information for proper gating;
- Support of abort Gx+ session messages must be added to enable PCRF to revoke authorization, e.g. when application session is deactivated.

"Authorised QoS" information contains a combined maximum QoS class and bitrate for all dynamically provided charging rules.

Gx+ may also support additional enhancements identified for Rel-7.

Editor's note-i: Functions for providing service data flow level QoS is addressed in Annex A.

Editor's note-ii: "Gx+" shall be considered as a temporary working name only, and will be changed to a proper reference point name once the work enters normative specification stage.

4.2.3 Functional elements

4.2.3.1 Policy Control and Charging Rules Function (PCRF)

The PCRF encompasses policy control decision and flow based charging control functionalities. It provides network control regarding the QoS and flow based charging (except credit management) towards the Gateway.

When the PCRF receives service information from the AF, depending on the network operator's configuration, the PCRF may check whether the AF is allowed to pass the application/service information to the PCRF.

The PCRF shall control how a certain service data flow that is under policy control shall be treated in the GW, e.g. discarded etc. and ensure that the GW user plane traffic mapping and treatment is in accordance with the user subscription profile. For GPRS, it shall be possible to support policy control on a per PDP context basis.

The PCRF may check that the service information provided by the AF is consistent with the operator defined policy rules before storing the service information. The service information is used to derive the QoS for the service. The PCRF may reject the request received from the AF. The PCRF indicates in the response the service information that can be accepted by the PCRF.

Editors Note: For Go it was defined that the controller provides the authorized QoS to the GW. In PCC it is FFS what the gain and benefits would be to change this concept such that the PCRF checks the requested QoS against the authorized QoS and hence may downgrade the requested QoS from the GW when it exceeds the authorized QoS instead of sending the authorized QoS to the GW.

The PCRF interacts with the GW by either responding to a request from the GW or by sending an unsolicited update of policy and charging rule information. An unsolicited update (i.e. the addition, modification or removal of policy and charging rules) may be triggered by a change of PCRF internal policy configuration or by receiving updated session information from an AF. The PCRF shall check whether the new policy configuration or session information changes the allocation of service data flows to bearers. If the binding of service data flows to bearers is not affected, the PCRF may send the unsolicited update, e.g. in case of a change of QoS or charging key. Otherwise, the PCRF shall wait for a request from the GW with new information for the mapping (e.g. an updated TFT) and may only send unsolicited decisions that do not change the installed set of service data flow filters (e.g. change of gate status or QoS). For new policy and charging rules or service data flow filters, the PCRF may also be configured or instructed by the AF to send the unsolicited update. Then, the PCRF shall bind these new rules or filters to the bearers based on the mapping information that was previously received from the GW.

NOTE: Another request from the GW may still occur if the UE modifies the mapping information for these service data flows for which the new rules or filters have already been installed based on the old mapping information (e.g. by updating the TFT).

4.2.3.2 Gateway (GW)

The Gateway encompasses policy enforcement and flow based charging functionalities. It provides the user plane traffic handling and it's the QoS handling, and provides service data flow detection and counting as well as online and offline charging interactions.

A GW, operating Gx+, shall ensure that an IP packet, which is discarded at the GW as a result from policy enforcement or flow based charging, is neither reported for offline charging nor cause credit consumption for online charging. Note though that for certain cases e.g. suspected fraud an operator shall be able to account for the discarded IP packets on a per bearer basis.

For a service data flow that is under policy control the GW shall allow the service data flow to pass through the GW if and only if the corresponding gate is open. If the GW receives an Authorization token and Flow Id(s) from an UE, the GW shall report them to the PCRF over Gx+.

For a service data flow that is controlled by FBC the GW shall allow the service data flow to pass through the GW if and only if there is a corresponding active charging rule with and, for online charging, the OCS has authorized the applicable credit with that Charging key, cf. TS 23.125 [3]. The GW may let a service data flow pass through the GW during the course of the credit re-authorization procedure.

At establishment or modification of a bearer with a TFT, the GW shall check any predefined policy and charging rules against the TFT filters received from the UE. A predefined policy and charging rule shall be only installed for a bearer if it fits to one of the TFT filters of that bearer.

4.2.3.3 Application Function (AF)

The Application Function (AF) is an element offering applications that require the control of IP bearer resources. The AF is capable of communicating with the PCRF to transfer dynamic service information, which can then be used for selecting the appropriate charging rule and service based local policy by the PCRF. 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 be accepted by the PCRF and the service information that can be accepted by the PCRF. Then, the AF rejects the service establishment towards the UE. If possible the AF forwards service information to the UE that can be accepted by the PCRF.

An AF may communicate with multiple PCRFs. The AF shall contact the appropriate PCRF based on either:

- the end user IP Address; and/or
- optionally a UE identify information 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.

4.2.4 Relationship between functional elements

The AF and the PCRF need not exist within the same operator's network. The Rx+ interface may be intra- or inter-domain and shall support the relevant protection mechanisms for an inter-operator or third party interface.

Editor's note: It is for further study how to handle the scenario where the GW is in the visited network.

5 Subscription aspects

5.0 General

This clause studies possible architectures and solutions for adding end-user subscription differentiation and general policy control aspects to the policy- and charging control.

5.1 Functional requirements

The FBC architecture described in TS 23.125 [3] incorporates the notion of the CRF taking subscriber-specific knowledge into account for the construction of charging rules. However, TS 23.125 [3] does not specify how the CRF acquires subscriber-specific knowledge. The PCRF may also benefit to use subscriber-specific information as basis for the SBLP decision. This clause shall address developing the architecture for the combined PCRF to retrieve subscription information as an input to policy and charging control.

5.2 Architectural concepts

5.2.1 Reference Model

Figure 5.1 below depicts the architecture for adding subscription aspects to the PCC architecture:

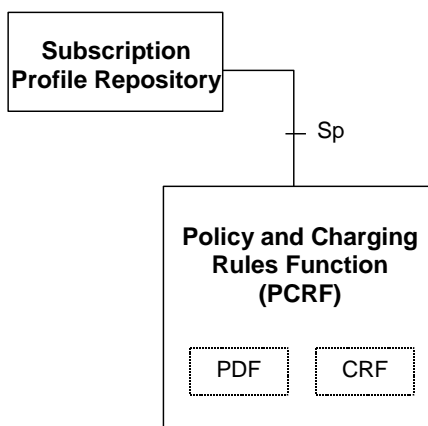


Figure 5.1: Adding subscription aspects to the PCC architecture

5.2.2 Reference Points

5.2.2.1 Sp reference point

The Sp reference point allows the Subscription Profile Repository to provide subscription-based input to policy and charging control.

The Sp reference point allows PCRF to request subscription information related to bearer level policies from the SPR based on subscriber ID. The subscriber ID can be e.g. IMSI. The interface allows the SPR to notify the PCRF when the subscription information has been changed if the PCRF has requested such notifications.

NOTE: Authorization of service usage based on subscription information may also be undertaken on the application level. Precedence and resolution of possible conflicts between bearer level and application level service authorization is FFS.

5.2.3 Functional elements

5.2.3.1 Subscription Profile Repository (SPR)

Editor's note: The SPR's relation to existing subscriber databases are for further study.

The SPR contains all subscriber/subscription related information needed for subscription-based policies and bearer level charging rules by the PCRF. The SPR may be combined with other databases in the operator's network, but those functional elements and their requirements for the SPR are out of scope of this TR.

5.2.3.2 Policy and Charging Rules Function (PCRF)

The PCRF may use the subscription information as basis for the policy and charging control. The subscription information can be used for both session based and non-session based services. The subscription specific information for each service may contain e.g. max QoS class and max bit rate for each APN the subscriber has access permission to and for each charging key of the subscriber.

6 Binding IP bearers to services

6.0 General

Both the policy control and the flow based charging have legitimate interest in what bearer carries what services. E.g. the policy control may be applied so that a bearer with suitable transmission characteristics is assigned for a specific service and is therefore interested in maintaining the integrity of the transmission resources (other payload travelling on the same bearer might degrade the transmission quality below an acceptable level), and for flow based charging the charging rule function may e.g. provide different charging key values depending on the QoS of the bearer.

This clause studies architectural alternatives for binding bearers to services. This includes studying solutions for the network to control bearer usage by service flows. It presents the currently available binding mechanisms in Rel-5 based Gs interface and in Rel-6 Gx interface to analyse, which mechanisms are needed and for what purpose in Gx+ interface. Additionally, it introduces possible new binding concepts for consideration. These new concepts should cover the case where a bearer (for GPRS a PDP Context) is shared by multiple services.

6.1 Architectural concepts

6.1.1 Authorisation Token based binding

6.1.1.1 General

Authorisation Token based binding is the only binding mechanism supported for the Gs interface. Rel-6 Gx interface does not support Authorisation Token based binding.

The Authorization Token is used by session based services for binding the bearer authorization request to the session specific service information. The Authorization token contains the fully qualified domain name of the PDF and a session id in the PDF, which allows the PDF to uniquely identify the AF session.

In the Rel-6 policy control architecture the Authorisation Token is allocated by the PDF and transferred via Gq interface to the AF. The AF forwards the Authorisation Token in the AF session signalling to the UE and UE includes the Authorisation Token together with flow id(s) into the PDP Context Activation/Modification request of the media PDP context. The GGSN resolves the PDF address from the Authorisation Token and includes the Authorisation Token and flow id(s) to the request of bearer authorization from the PDF.

The PDF can identify the AF session from the session id in the Authorisation token and the IP flow(s) within the session from the flow id(s). In case media flows from multiple sessions are associated to the same PDP context, multiple Authorisation Tokens are received in the same bearer authorization request allowing PDF the to combine the policy of multiple sessions. Figure 6.1 below shows the Authorization Token based binding concept:

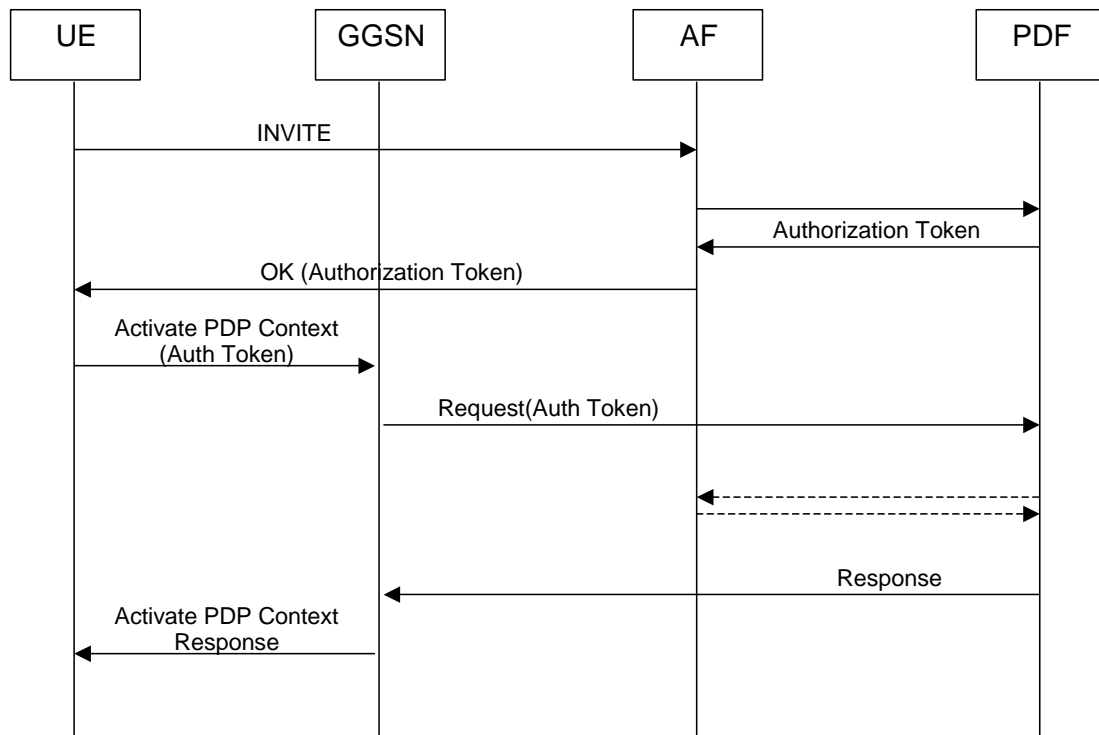


Figure 6.1: Authorization token based binding as per Release 6 specifications

The Authorisation Token based binding is an optimised solution for binding the bearer related request to the session information allowing fast binding in the PDF as the token refers directly to the session information with session id. Drawback of the Authorisation Token based binding mechanism is that it requires terminal support, and application session signalling and bearer setup signalling where it is transported over the network(s). Thus it is possible to use only in GPRS access and with specific application services (e.g. real-time IMS applications).

Another drawback is that the current use of Authorization token assumes the use of a PDP context activated using the secondary PDP context activation procedure to carry the specific IMS media. For PCC the binding mechanism needs to work irrespective of whether there are single or multiple PDP contexts. Therefore by using this mechanism alone, it is not possible to apply flow based charging or policy control to the default PDP context.

Further, when SBLP and media grouping is applied a Rel-5 network/UE is not allowed to convey media belonging to different IMS sessions onto the same PDP context established using Secondary PDP context activation procedure. This may lead to a proliferation of PDP contexts as services get deployed if legacy Rel-5 entities are used. A Rel-6 network/UE is allowed to convey media belonging to different IMS sessions onto the same PDP context established using Secondary PDP context activation procedure.

6.1.1.2 Authorization Token based binding for PCC

For the PCC architecture, the Authorisation Token based binding mechanism is required to be supported for backwards compatibility reasons as the TFT based binding mechanism cannot be used alternatively if Authorisation Token is provided in the PDP context activation/modification signalling based on earlier release specifications. The presence of the Authorisation Token will be dependent on whether the PCRF generates it and on UE implementation. To make the Authorisation Token based binding mechanism work in the PCC architecture it is required that the same PCRF is selected by all AFs that communicate with the same end user. Therefore, the AF of a session based service using the Authorization Token based binding shall select the appropriate PCRF based on the end user IP Address.

6.1.2 UE IP address based binding

UE IP address based binding is supported by Rel-6 Gx interface.

The use of UE IP address for binding the bearer request for the service information in PCRF is access and service independent solution. This binding mechanism does not require any special support from other interfaces like Authorisation Token passing does. However, the UE IP address alone cannot be used for PDP context specific policy/charging rules control and thus some more GPRS access specific information is needed in addition. For access systems that do not use simultaneous bearers, UE IP address based binding may be sufficient.

6.1.3 UE IP address + TFT based binding

UE IP address + TFT based binding is supported by Rel-6 Gx interface.

In case of GPRS access the TFT filter information may be used in addition to UE IP address to select policy/charging rules for the specific PDP context. As a consequence, for a token-less binding mechanism to apply to all PDP contexts, the UE IP address + TFT based binding must be combined with simple UE IP address based binding.

The UE may provide the TFT in the secondary PDP context activation procedure and in any PDP context modification procedure as per definition in TS 23.060. The TFT includes the TFT filters. The service information may originate from an AF providing it to the PCRF over the Rx+ interface, or be derived at the PCRF (e.g. based on the user subscription profile). There is set of requirements on information in the TFT filter from the UE and service information from the AF for proper binding to an authorized IP flow to occur at the PCRF.

Increasing the accuracy of an authorization reduces the risk for authorizing a flow on multiple PDP contexts to occur. However a TFT filter need not necessarily specify all the parameters of the flow. Proper binding at the PCRF is possible if the UE and the AF provide a common subset of parameters:

- the source (source IP address/network and/or source port/port range), which identifies the remote end of communication (assuming sending and receiving are symmetric); or
- the destination (destination port/port range), which identifies the UE end of communication; and
- the protocol number, if the same source and/or destination appears in more than one authorization.

Editors note: How to draft the specific requirements on how each side i.e. the AF and the UE shall provide with as much information that is available to describe the IP flow is FFS

However as a general issue in IMS, SDP negotiation does not provide any information about the source of media (IP address and port number) and therefore it may not be possible to well define charging rules from SDP information (i.e. the full IP 5-tuple in both directions).

Figure 6.2 below shows an example flow where TFT is included in PDP context activations or modifications.

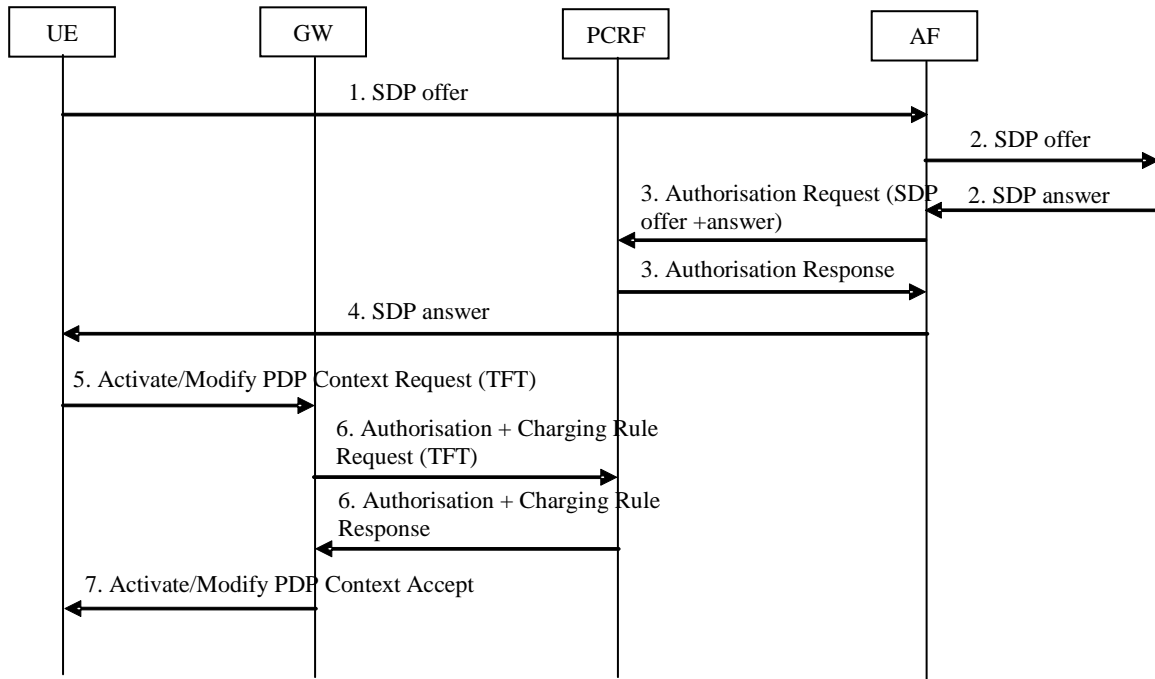


Figure 6.2: Example flow for UE IP address + TFT based binding mechanism

The TFT filter is not included into the PDP context activation/modification request by the UE if it receives Authorisation Token from the AF and includes it in the PDP context activation/modification request. Thus it is not possible to use this binding mechanism if the Authorization Token is provided and the UE supports the use of Authorization Tokens. If there exist UEs that support and UEs that do not support Authorization Tokens, then this binding mechanism can co-exist with the token-based mechanism.

The decision on the mapping of flows to appropriate bearers resides at the UE. A benefit of this is that the UE can multiplex PCC controlled service data flows with flows not subject to full PCC control (e.g. where no AF interaction is required) onto the same bearer. Therefore in GPRS, the PCRF will require flexibility to provide charging rules and authorisation information in an unsolicited manner to the GW to e.g. a default PDP context if no PDP context activation or modification occurs that can be bound to received AF information. If subsequently, a PDP context activation or modification, which can be bound to AF information, occurs then charging rules and authorisation information needs to be moved from the default PDP context to the PDP context that is being activated or modified. Such a push mechanism is already required for gating control (opening and closing of gates). An example of this can be found in figure 6.3 below.

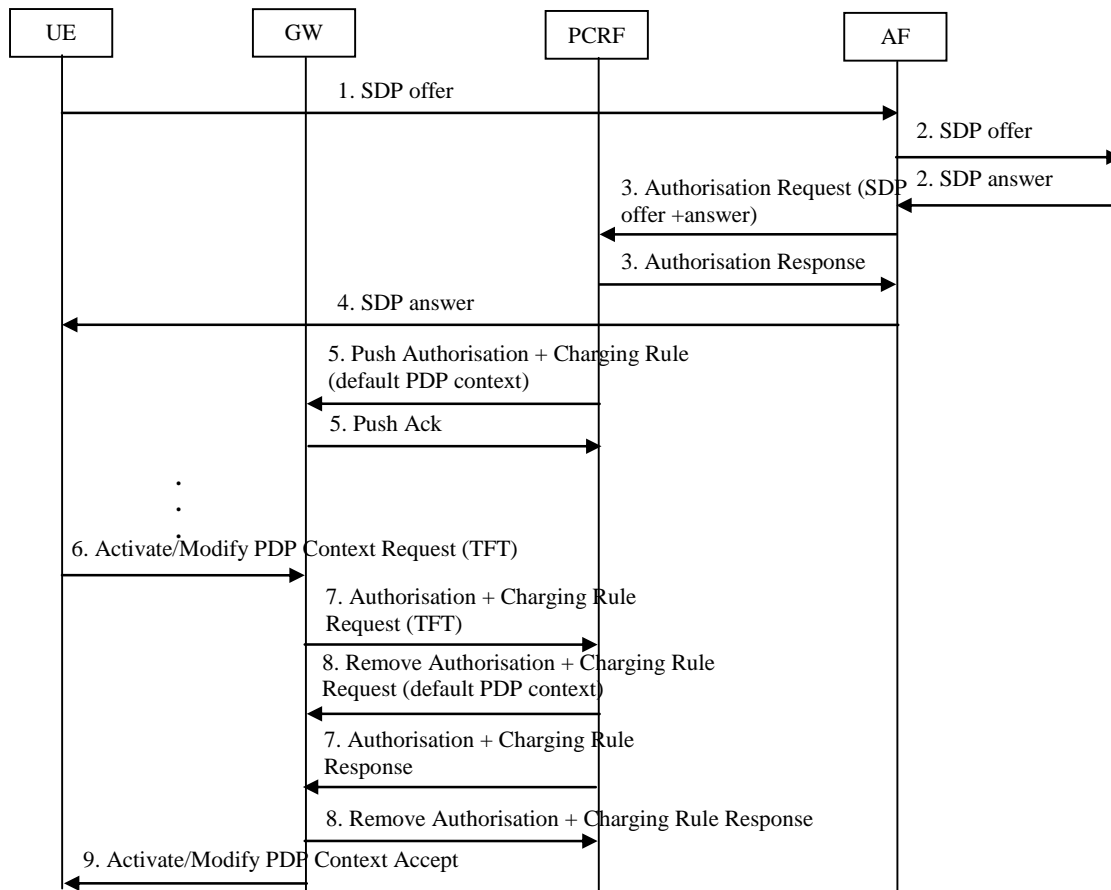


Figure 6.3: Example flow where PDP context activation/modification occurs after session setup

The use of TFT presents some limitations; The TFT is only interpreted as downlink filters. Therefore the use of TFT, as currently defined, as binding may not work for uplink IP flows, especially in case of unidirectional media with direction send only, since the UE does not indicate any uplink IP filter for the PDP context. As result the PCRF cannot know to which PDP context the applicable rules/policies shall be sent.

To overcome this limitation the following solutions can be foreseen:

- For a bi-directional media flow (i.e. 2 IP flows with IP address/port number pairs), both downlink and uplink packets shall travel on the same PDP context, thus making the TFT filter for the downlink traffic to be sufficient for determining what PDP context will carry the uplink traffic.
- For a unidirectional media flow combined with RTCP flows in both directions, the media flow shall travel on the same PDP context as the RTCP flows, thus making the TFT filter for the downlink RTCP flow to be sufficient for determining what PDP context will carry the uplink RTCP and media traffic.
- The TFT packet filter could be used to transfer mapping information for the uplink, i.e. especially for unidirectional media with direction send only. A dedicated parameter of the TFT packet filter shall indicate that this TFT packet filter provides mapping information for the uplink. Any parameter of the TFT packet filter that can be set to a value which does not occur in any downlink IP packet could be used for this purpose (e.g. IP source address of the TFT packet filter set to UE IP address or source port number of the TFT packet filter set to zero). The other parameters of the TFT packet filter can then be used to transfer information that describes the uplink IP flow(s).
- The UE is required to set the indication parameter as well as the other parameters of the TFT packet filter according to the uplink IP flow(s). The GGSN behaves as already specified, installing the TFT and forwarding the TFT to the PCRF including the TFT packet filters for the uplink. Alternatively, the GGSN could also recognize any TFT packet filter for the uplink and not install it. The PCRF recognizes the indication parameter and applies the other TFT packet filter parameters to bind any applicable unidirectional media with direction send only.

- A new encoding of the TFT packet identifier could be used to transfer the IP flow direction information while using the other parameters of the TFT packet filter to describe the uplink IP flow(s). The GGSN forwards the TFT packet filters to the PCRF including the packet identifiers containing the directional information. The GGSN should not install any TFT packet filter declared to be uplink only. The PCRF recognizes the directional information encoded in the TFT packet identifier and applies the other TFT packet filter parameters to bind any applicable unidirectional media with direction send only.

Editors Note: There may be other solutions to overcome this limitation.

6.1.4 UE Identity based binding

UE identity based binding is supported by Rel-6 Gx interface.

Use of UE identity for the binding to the session based service information requires mapping between access network identities and AF identities, thus other mechanisms described above suit better for binding the policy/charging rule request to the session based service information. However UE Identity can be used to access directly to the subscription information, thus it can be used also as complementary information together with other information to allow subscription based limits and settings to be taken into account together with session based service information for policy decisions and charging rules.

6.1.5 Exchange of filter information

The UE may instruct the GW how to map downlink traffic by providing suitable filters for each bearer (for GPRS TFT filters for each PDP context). The PCRF addressing as well as correlating service authorizations to the appropriate user session (the UE IP address) is defined in Rel-6. However, the IP flow authorizations, the QoS demands for them and possible demands/restrictions regarding flow grouping remains to be resolved.

For this purpose, an approach that presumably considers a wide class of applications is studied as described below:

- a) the UE provides both TFT-like mapping information for downlink traffic and the intended uplink traffic mapping upon PDP context activation and modification;
- b) the PCRF may then return a modified uplink traffic mapping for the UE to use.

Editors Note: By sending uplink traffic mapping from the UE there is a terminal impact. Hence there is a cost to control what traffic flows on what PDP context. It is expected that the study will consider this cost aspect and the feasibility of sending uplink traffic mapping from the UE.

6.2 Conclusions

Binding mechanisms described in sections 6.1.2 through 6.1.4 need to be supported by the Gx+ specification in order to support various application services and access networks as well as subscription-based differentiation.

Editor's note: Support for Authorization Token based binding needs to be further studied along with further binding mechanism alternatives. The decision to use authorisation tokens require co-ordination in the provisioning of the AF and PCRF.

The GW shall always report the TFT filters, token and flow identifiers (if present) as well as the PCO IM CN signalling flag and the QoS signalling flag for a PDP context to the PCRF as input for binding at the PCRF. The PCRF shall be capable to do proper binding, based on the information provided from the GW.

The PCRF contact information shall be configured to the GW. The GW may be served by more than one PCRF. For GPRS the appropriate PCRF is contacted based on which APN the UE is connected to. For other IP-CANs the GW shall contact the appropriate CRF based on the access point the UE is connected to and, optionally, a UE identify information that is applicable for that IP-CAN.

7 Signalling Flows

7.1 Bearer Service Establishment and Modification without AF Interaction

This sub-clause describes the signalling flow for bearer service establishment when the AF is not involved. In addition, this sequence is applicable for bearer service modification when the AF is not involved. An example of the scenario is authorization of non-session based services in conjunction with a bearer establishment that do not require realtime QoS authorization.

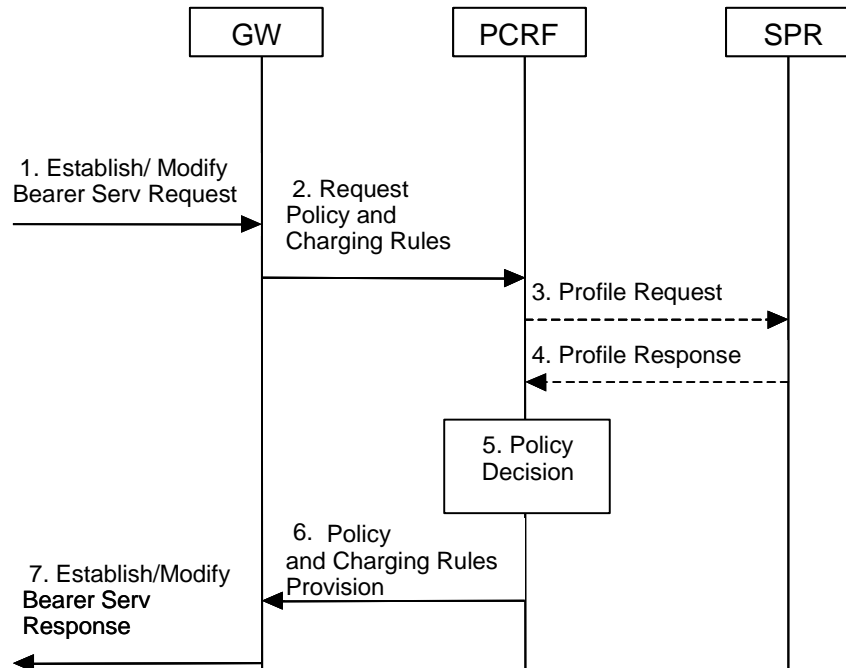


Figure 7.1: Bearer Service Establishment without AF interaction

1. The GW receives a request for bearer establishment/modification. For GPRS, this is the Create PDP Context Request or Update PDP Context Request depending on whether a new PDP context is created or an existing one modified, respectively.
2. When the GW determines that the PCC authorization is required, it requests the authorization, of allowed service(s) and Policy and Charging Rules information.
3. 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.
4. The SPR replies with the subscription related information containing the information about the allowed service(s) and Policy and Charging Rules information.
5. The PCRF makes the authorization and policy decision.
6. The PCRF sends the decision(s) to the GW. The GW enforces the decision.
7. The GW acknowledges the Bearer Establishment/Modification Request. For GPRS, this is Create PDP Context Response or Update PDP Context Response depending on whether a new PDP context is created or an existing one modified, respectively.

7.2 Bearer Service Establishment and Modification with AF Interaction

This sub-clause describes the signalling flow for the bearer services establishment when the AF is involved. In addition, this sequence is applicable for bearer service modification when the AF is involved and if the triggering conditions given by the GW in the bearer service establishment phase are fulfilled. An example of the scenario is authorization of a session-based service for which a secondary PDP context is also established.

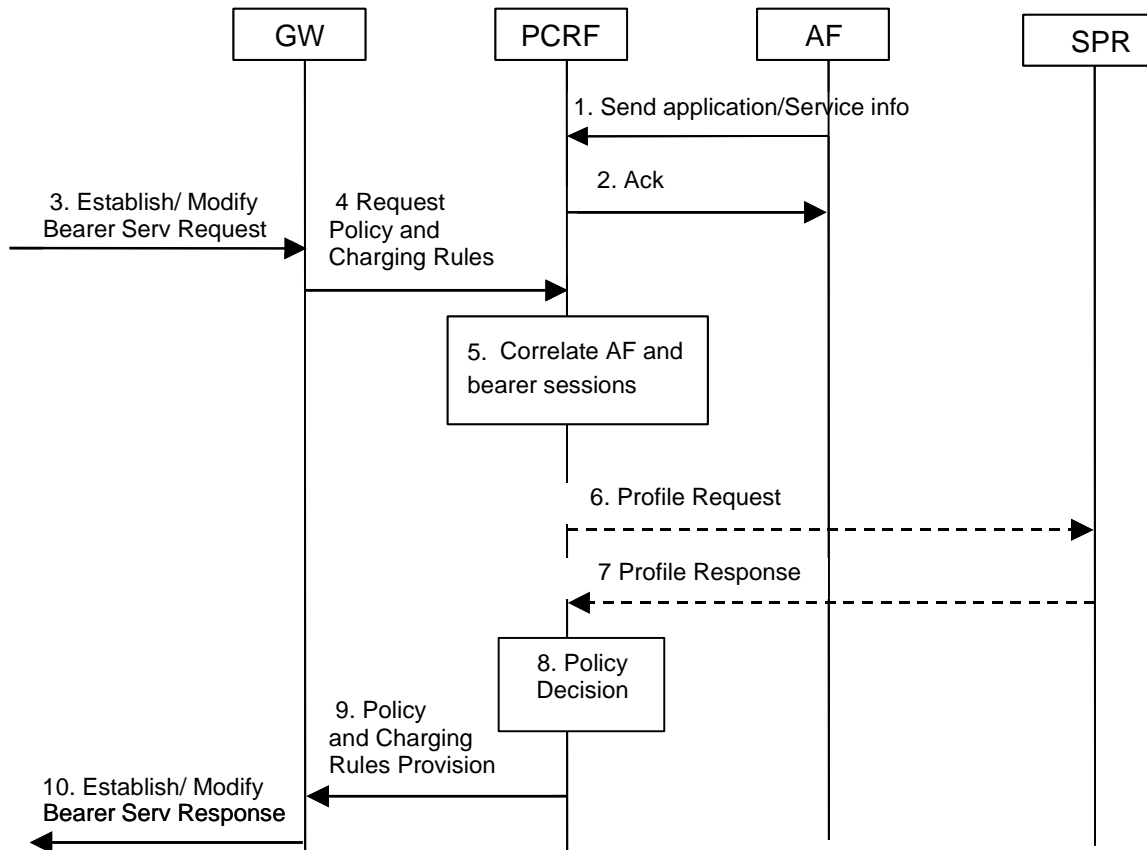


Figure 7.2: Bearer Service Establishment and Modification with AF Interaction

1. The AF provides service information to the PCRF at a set-up of a new AF session or at a modification of an existing AF session.
2. The PCRF stores the service information and replies with the Acknowledgement to the AF.
3. The GW receives a request for bearer establishment/modification. For GPRS, this is the Create PDP Context Request or Update PDP Context Request depending on whether a new PDP context is created or an existing one modified, respectively.
4. The GW determines that the PCC interaction is required and sends the Policy and Charging Rules request to the PCRF.
5. The PCRF correlates the application and bearer sessions with the binding information (e.g. user's IP address) provided from AF and TPF. If available, the PCRF also retrieves the saved application service information in order to make the authorization and policy decision.
6. The PCRF may fetch the subscription related information from the SPR, if the PCRF does not have it.
7. If step 6 took place, then SPR replies with the subscription related information, and the PCRF stores the information.

NOTE 1: For bearer service modification, the PCRF contacts AF at this point, if the AF requested it at initial authorisation, or if PCRF requires more information from the AF before authorising the network resources modification. The AF also replies with the requested information. This is described in sub-clause 6.3.6a in TS 23.207 [2].

8. The PCRF makes the authorization and policy decision.
9. The PCRF sends the decision(s) to the GW. The GW enforces the decision.
10. The GW acknowledges the Bearer Establishment/Modification request. For GPRS, this is Create PDP Context Response or Update PDP Context Response depending on whether a new PDP context is created or an existing one modified, respectively.

NOTE 2: For bearer service modification, if PCRF contacted the AF after step 7) then the successful installation of the decision is reported to the AF. This is described in sub-clause 6.3.6a in TS 23.207 [2].

7.3 Bearer Service Termination

Figure 7.3 describes the signalling flow for the bearer service termination. An example of the scenario is UE originated PDP context termination.

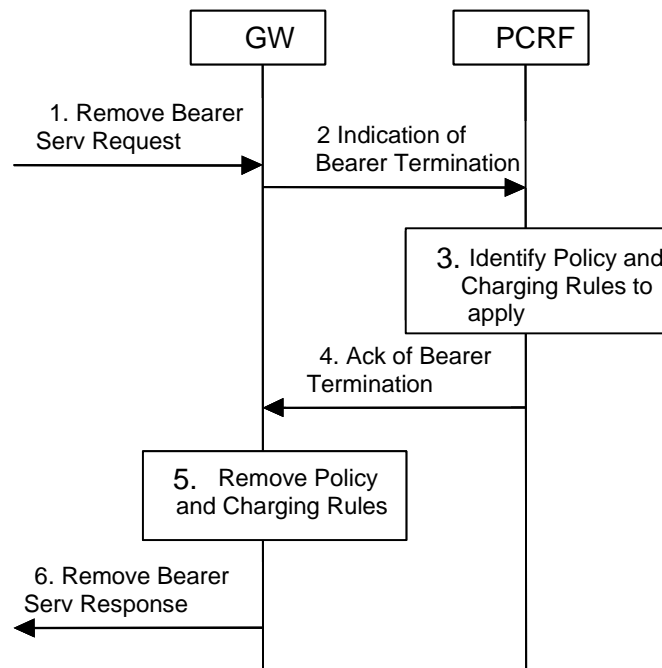


Figure 7.3: Bearer Service Termination

1. The GW receives a request to remove bearer service. For GPRS, this is the Delete PDP context request.
2. The GW indicates that the bearer service (for GPRS, a PDP context) is being removed and provides relevant information to the PCRF.
3. Policy and Charging Rules may need to be removed for the terminated bearer service. However, there is no need for the PCRF to remove Policy and Charging Rules explicitly. The PCRF also determines whether the Policy and Charging Rules need to be provisioned for any other bearer service of the same IP network connection, the details are FFS.
4. The PCRF provides the Policy and Charging Rule information to the GW. This message is flagged as the response to the GW request.
5. The GW removes the Policy and Charging Rules.
6. The GW continues with the bearer service removal procedure.

NOTE: The bearer service removal procedure may proceed in parallel with the indication of bearer service termination.

Figure 7.4 describes the signalling flow for the GW initiated bearer service termination.

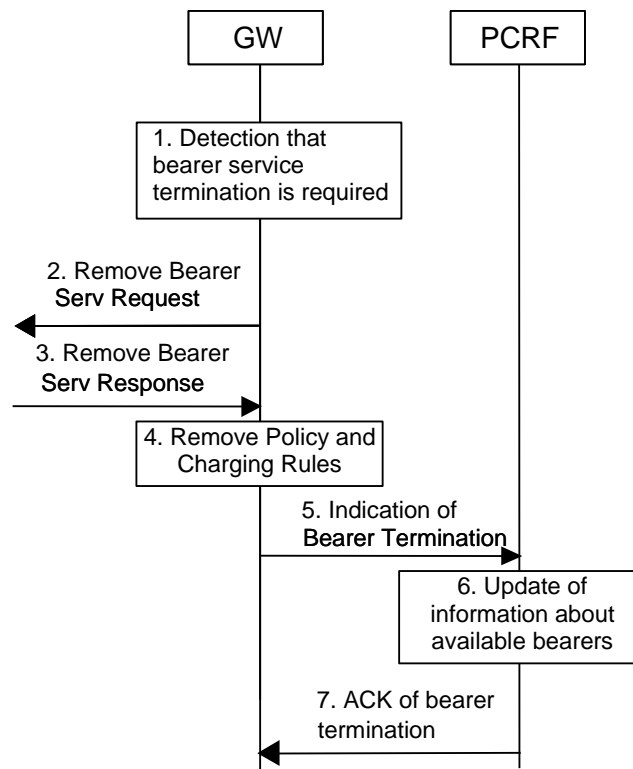


Figure 7.4: GW Initiated Bearer Service Termination

1. The GW detects that bearer service termination is required.
2. The GW sends a request to remove the bearer service. For GPRS, this is the Delete PDP context request.
3. The GW receives the response for the bearer service removal.
4. The GW removes the Policy and Charging Rules.
5. The GW indicates that the bearer service (for GPRS, a PDP context) has been removed and provides relevant information to the PCRF.
6. The PCRF updates its information about the available bearers by removing the information related to the terminated bearer service. The PCRF also determines whether the Policy and Charging Rules need to be provisioned for any other bearer service of the same IP network connection, the details are FFS.
7. The PCRF sends an acknowledgement to the bearer termination indication.

7.4 Rule Update

This subclause describes the signalling flow for the PCRF to update policy and charging rules to the GW for an already established bearer.

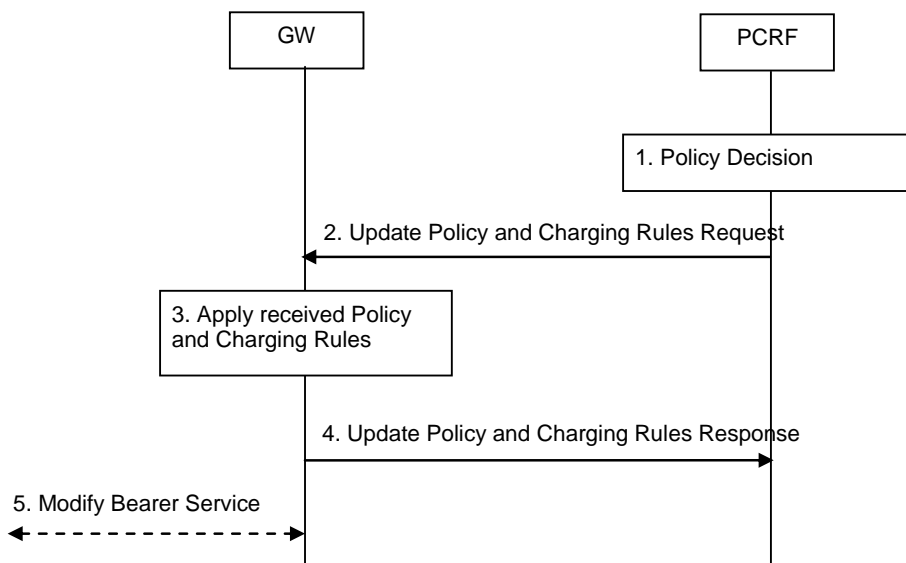


Figure 7.5: Policy and Charging Rule update

1. A trigger event causes the PCRF to determine that the policy and charging rules require updating at the GW, e.g. change to configured policy or received, from an AF, new or updated session information. The PCRF shall check whether the new policy configuration or session information changes the allocation of service data flows to bearers and continues only if the binding of service data flows to bearers is not affected. Otherwise, the PCRF shall wait for a request from the GW with new information for the mapping as shown in 7.1 or 7.2 and may only send unsolicited decisions that do not change the installed set of service data flow filters. For new policy and charging rules or service data flow filters, the PCRF may also be configured or instructed by the AF to send the unsolicited update.
2. The PCRF sends the updated policy and charging rules for the affected bearer service. This may be a combination of additional rules, removal of rules, or changes to installed rules or changed authorised QoS.
3. The GW performs the appropriate actions.
4. The GW acknowledges the request from the PCRF.
5. The GW may optionally trigger bearer service modification based on the updated policy and charging rules e.g. a downgrade to the authorised QoS.

8 Conclusions and recommendations

This feasibility study has investigated the following 3 areas:

- 1) Complete harmonization and merger of the policy control and flow based charging architecture and procedures;
- 2) Possible architectures and solutions for adding end-user subscription differentiation and general policy control aspects to the policy- and charging control;
- 3) Alternative solutions for binding bearers to services (provided today by the authorization token). This includes studying solutions for the network to control bearer usage by service flows.

It is concluded that:

- the complete harmonization and merger of the policy control and flow based charging architecture and procedures is feasible;
- adding end-user subscription differentiation and general policy control aspects to the policy- and charging control is feasible;

- alternative solutions for binding bearers to services (provided today by the authorization token) are feasible;

Editor's Note: The precise mechanism used to bind service data flows to bearers for GPRS for all scenarios still requires further study.

- it shall be possible to apply the PCC model to any kind of bearer from any IP-CAN.

It is recommended that:

- the PEP and TPF are replaced by a new single functional element inside the Gateway;
- the PDF and CRF are replaced by a new single functional element called PCRF;
- the reference points for the PCC architecture use and enhance the R6 interface specifications of the relevant FBC reference points:
 - There shall be a single reference point between PCRF and Gateway: the Gx+ reference point, that shall be realized combining G_o and G_x enhancing the existing R6 G_x protocol to fulfil also SBLP requirements;
 - There shall be a single reference point between PCRF and AF: the Rx+ reference point that shall be realized by combining R_x and G_q;

Editor's note: Rx+ and Gx+ may be changed to a proper reference point name in the normative specification stage.

- the PCRF shall be able to base decisions upon subscription information. For this it can communicate through the new Sp reference point with a Subscription Profile Repository;
- that the binding of bearer to service data flows over Gx+ will be mainly done through the use of UE IP address, which is access and service independent. In the GPRS case (access system that supports simultaneous bearers) TFT may also be needed. The UE identity can be used complementarily.

Annex A: Service Data Flow based QoS control

This section contains temporary considerations regarding PCC functionality for service data flow-based QoS control.

A.1 Functional requirements

In case the PCRF provides charging rules dynamically over Gx+ interface, "Authorised QoS" information for the bearer (combined QoS) is provided. At the same time, QoS class for individual service data flows may also be provided.

A.2 Impacts to interfaces

A.2.1 Gx+ interface

In addition to the combined max QoS class and bitrate, service data flow level QoS class may be provided within the charging rule definition. This QoS class may be used e.g. for DiffServ Code Point marking in the GW. In GPRS access the DSCP marking on downlink direction is based on the negotiated UMTS QoS profile and thus controlled by the combined maximum QoS class, but the uplink DSCP marking could be based on the service data flow level QoS class. In other type of access networks it is up to IP-CAN specific QoS mechanisms and GW capabilities how it will use "Authorized QoS" and service data flow level QoS class information.

Annex B: Change history

Change history							
Date	TSG #	Doc #	CR	Rev	Subject/Comment	Old	New
2005-09	SP#29	SP-050495	-	-	Editorial update by MCC for presentation to TSG SA#29 for approval	1.2.0	2.0.0
2005-09	-	-	-	-	Updated by MCC for publication as version 7.0.0	2.0.0	7.0.0