Technical Specification Group Services and System Aspects **TSGS#28(05)0354**

Meeting #28, 06 - 08 June 2005,

Quebec, Canada

Presentation of Specification to TSG or WG

Presentation to:	**TSG SA Meeting #28**
Source:	**SA WG2**
Document for presentation:	**TR 23.803, Version 1.0.0**
Presented for:	**Information**

Abstract of document:

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:

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.

Changes since last presentation to TSG-SA Meeting:

This is the first time thedocument gets presented to TSG-SA.

Outstanding Issues:

Further flows need to be introduced and the existing flows need to be fine-tuned.

More detailed study and eventual conclusion is needed on alternative binding mechanisms.

Description of the functional entities needs to be enhanced and completed.

Contentious Issues:

None identified.

3GPP TR 23.803 V1.0.0 (2005-05)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Evolution of Policy Control and Charging (Release 7)

Keywords

QoS, Flow Based Charging, Service Based Local Policy

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 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, the default PDP context is the PDP context, if any, with no TFT associated for a particular PDP address and APN pair. This may be either a primary or secondary PDP context.

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 service data flow is more granular than a PDP context.

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

3GPP TS 23.207 [2] specifies the Service Based Local Policy architecture, and 3GPP 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 rel6 Flow Based Charging which includes how policy can be provided with the Rel6 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 rel6 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

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: Separate IP-flow-level QoS and minimum QoS authorization are 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.

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 presence of complete Rel-6 style binding information (Token and Flow Identifier(s)), in the GW request to the PCRF indicates that bearer authorization from an AF is required for the specific bearer

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.

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 release 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.

4.2 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 policy control over Go 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 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 the network connected to (i.e. APN) and the AF contacts the CRF based on the end user (IP) address as experienced at the AF.

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

4.2.1 Reference Model

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

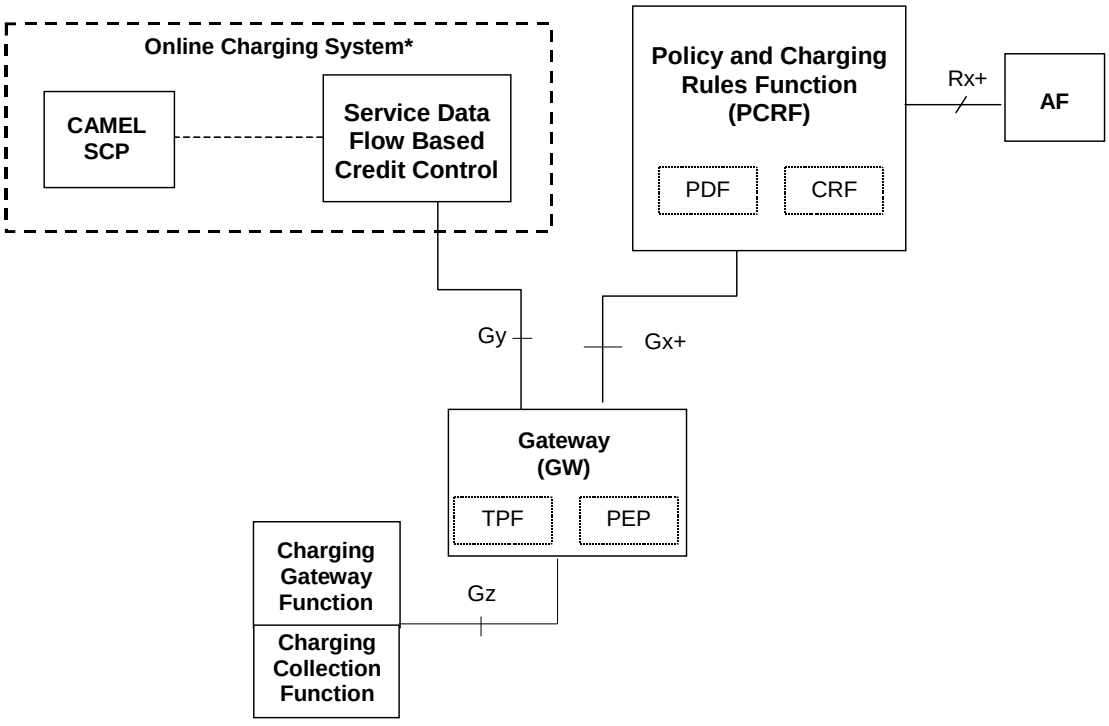


Figure 4.1: Overall architecture for combined policy and charging control

Editor's note-i: Standalone Go interface may be supported for backwards compatibility reasons although it is not shown in the figure.

Editor's note-ii: Support for the existing Rel6 Gq and Rx interfaces is FFS.

4.2.2 Reference Points

4.2.2.0 General

The reference points for the PCC architecture use and enhance the interfaces used in rel6 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 Rx together with Gq reference points with 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 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.

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 stipulate how a certain IP 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 and the PCRF policy decision(s). 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 receives the requested QoS. Then the PCRF checks it against the authorized QoS and hence may downgrade the requested QoS from the GW when it exceeds the authorized QoS.

4.2.3.2 Gateway (GW)

The Gateway encompasses policy enforcement and flow based charging functionalities. It provides control over the user plane traffic handling at the GW and its QoS, 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 block the IP flow but still be able to account for it.

For an IP flow that is under policy control the GW shall allow the IP 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 an IP flow that is controlled by FBC the GW shall allow the IP 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 an IP flow pass through the GW during the course of the credit re-authorization procedure.

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
- other 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 ppossible 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 3GPP TS 23.125 incorporates the notion of the CRF taking subscriber-specific knowledge into account for the construction of charging rules. However, 23.125 does not specify how the CRF acquires subscriber-specific knowledge. The PDF 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:

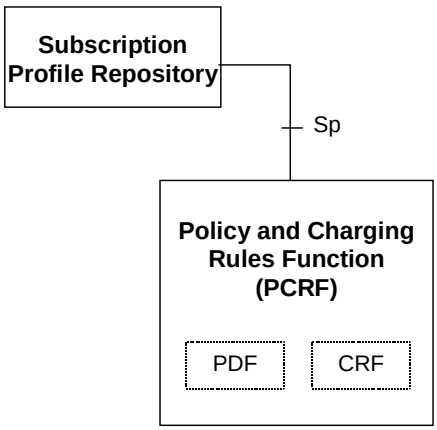


Figure 5.1: Adding subscription aspects to the PCC architecture

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 Go 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 Go 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 policyof multiple sessions. Figure 6.1 below shows the Authorization Token based binding concept:

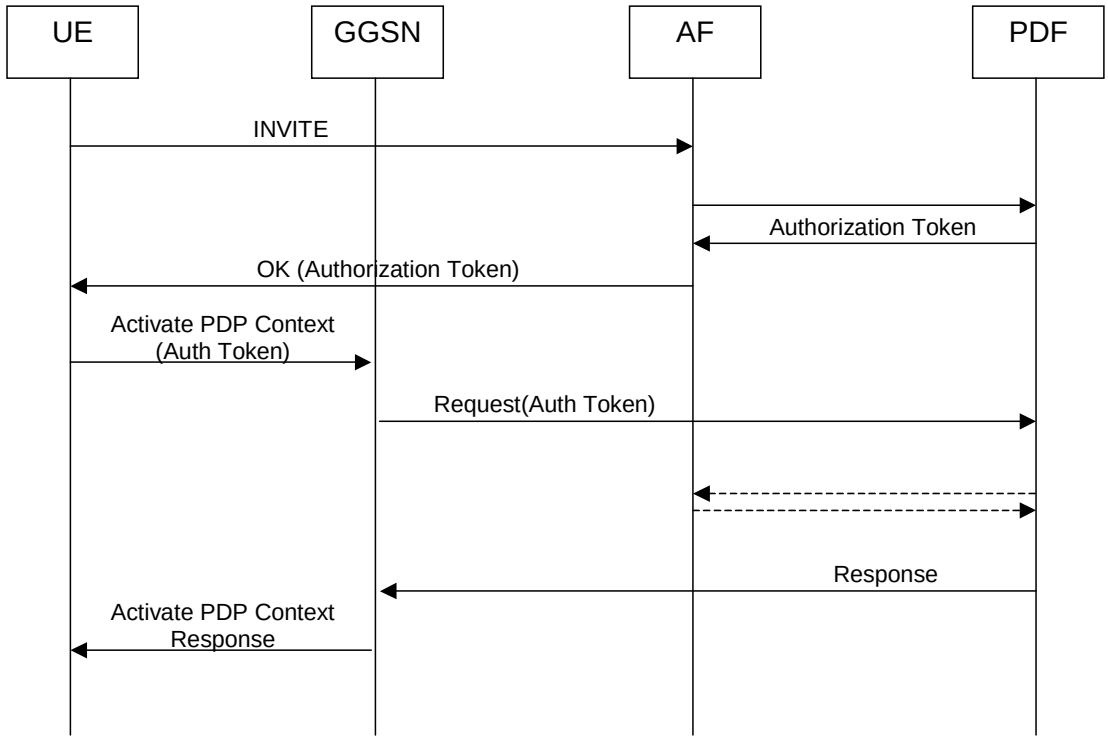


Figure 6.1: Authorization token based binding as per Release 6 specifications

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. 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

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

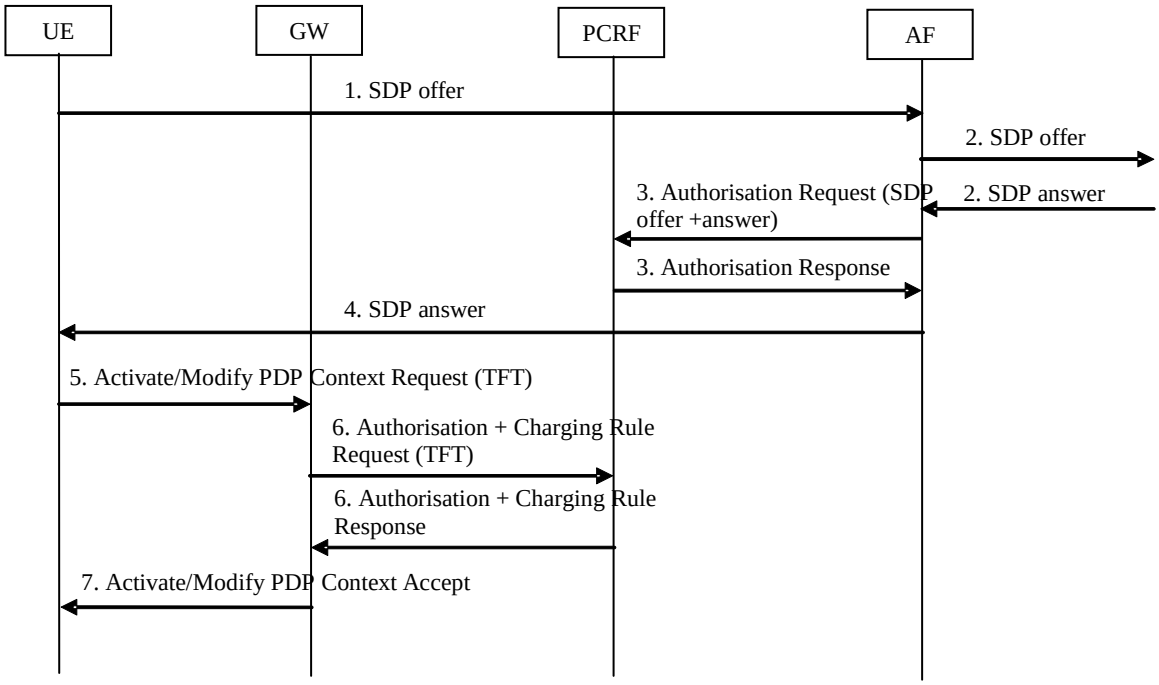


Figure 6.2: Example flow for UE IP address + TFT based binding mechanism

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.

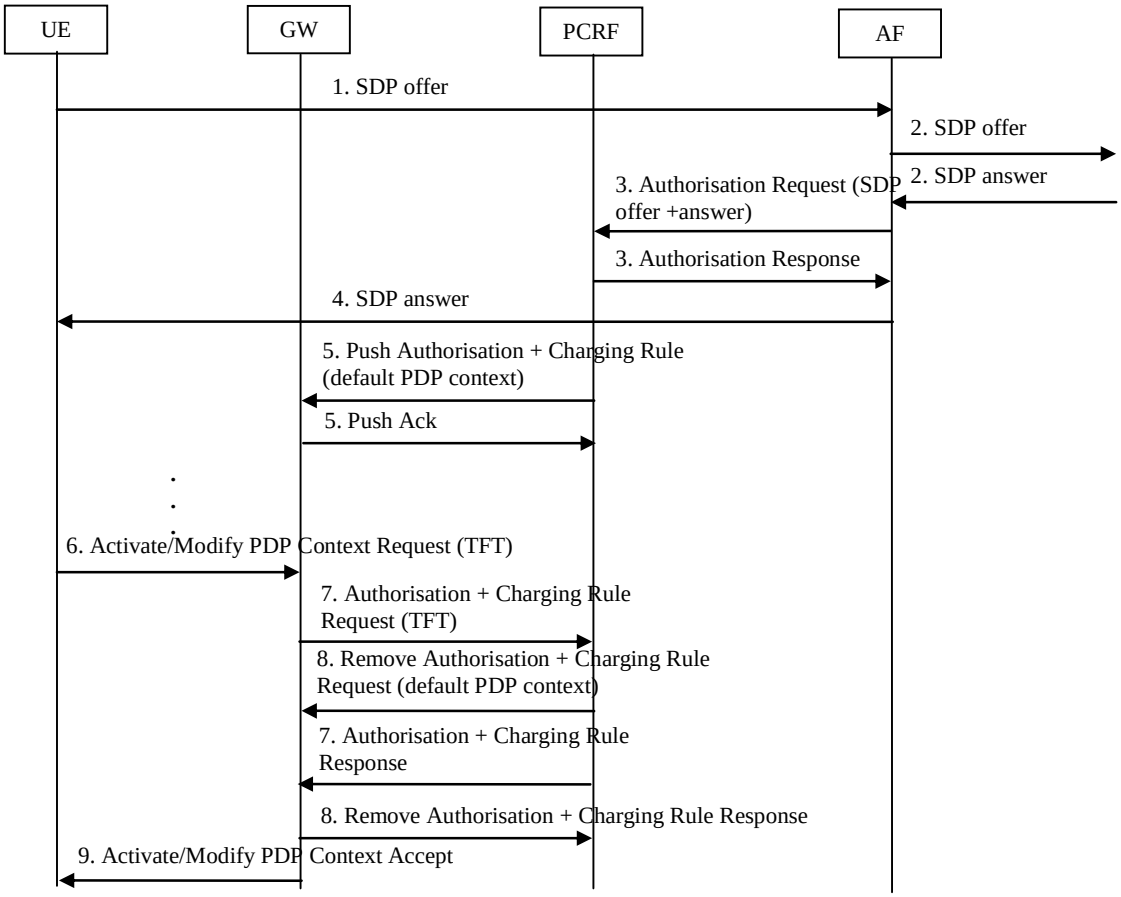


Figure 6.3: Example flow where PDP context activation/modification occurs after session setup

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 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. 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).

To overcome this limitation the following solutions can be foreseen:

- For a bi-directional IP flow (i.e. 2 IP address/port number pairs in a bi-directional communication), both downlink and uplink packets must 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

- The UE shall declare unidirectional uplink flows by specifying a TFT filter for the downlink direction on the intended PDP context.

- 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.

Editors Note-i: By modifying the handling of TFT packet filters for sending uplink traffic mapping information 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 information from the UE.

Editors Note-ii: 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 Rel6. 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, especially from backwards compatibility perspective, along with further binding mechanism alternatives.

It is up to GW to select the appropriate binding information depending what information is available at the GW. The PCRF architecture shall be capable to use any of the specified binding information.

For other binding mechanisms than Authorisation Token based binding the PCRF contact information shall be configured to the GW. The GW may be served 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.

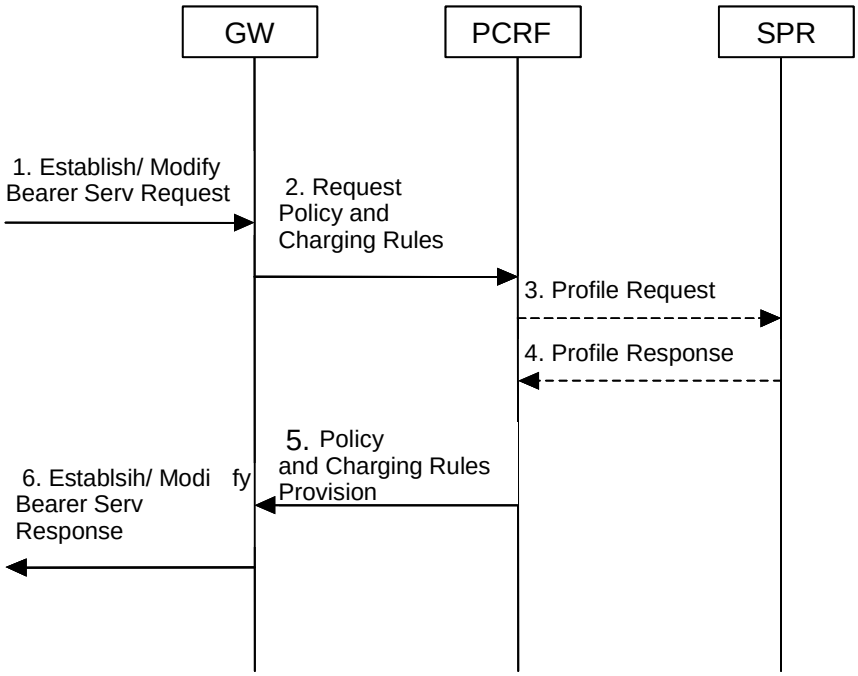


Figure 7.1: Bearer Service Establishment without AF interaction

1. The GW receives a request for bearer establishment. 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 subscriber's authorization, allowed service(s) and Policy and Charging Rules information.
3. If the PCRF does not have the subscriber's profile, it sends a request to the SPR in order to receive the profile.
4. The SPR replies with the subscription profile containing the subscriber's authorization, allowed service(s) and Policy and Charging Rules information.
5. The PCRF makes the authorization and policy decision and sends it the GW. The GW enforces the decision.
6. The GW acknowledges the Bearer Authorization 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 establishment.

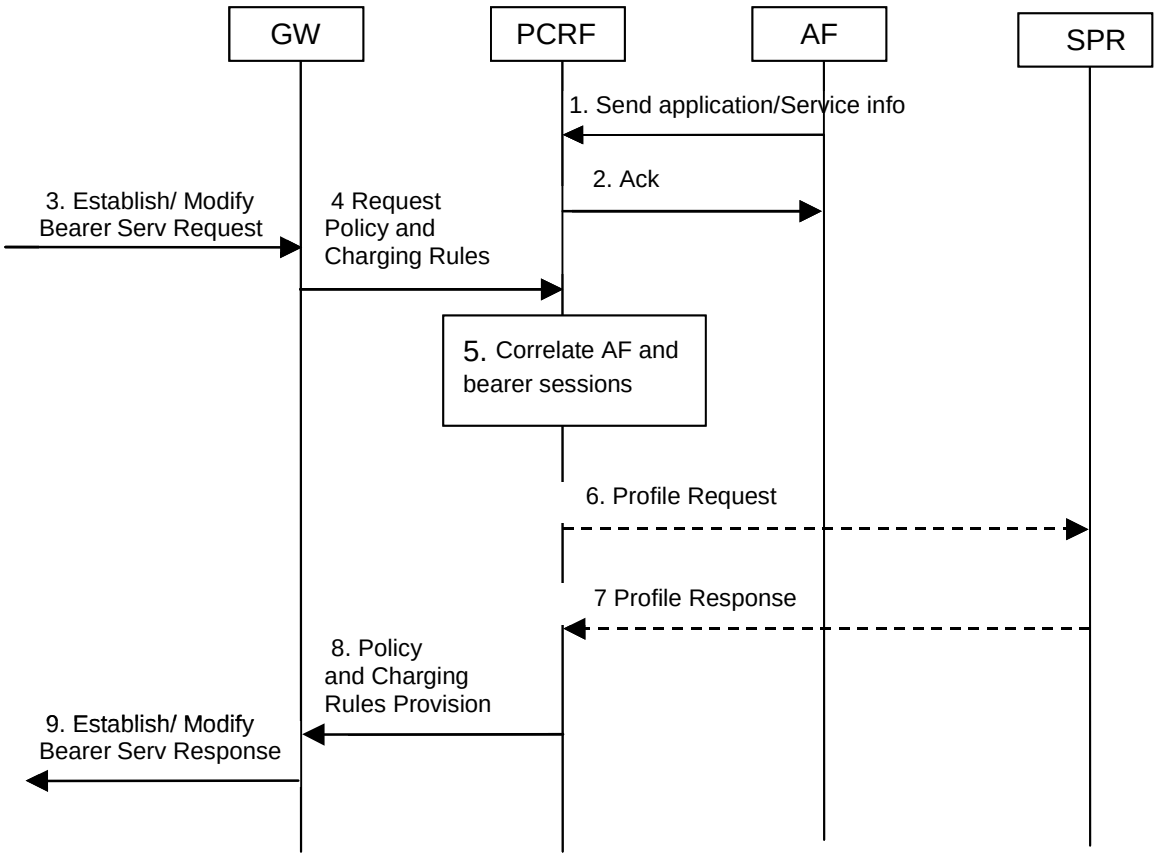


Figure 7.2: Bearer Service Establishment and Modification with AF Interaction

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. 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 information from the SPR, if the PCRF does not have it.
7. If step 6 took place, then SPR replies with the subscriber's profile, and the PCRF stores the profile.

NOTE 1: For bearer service modification, the PCRF contacts AF at this point, it 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 and sends it to the GW. The GW enforces the decision.

9. The GW acknowledges the Bearer authorization 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

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

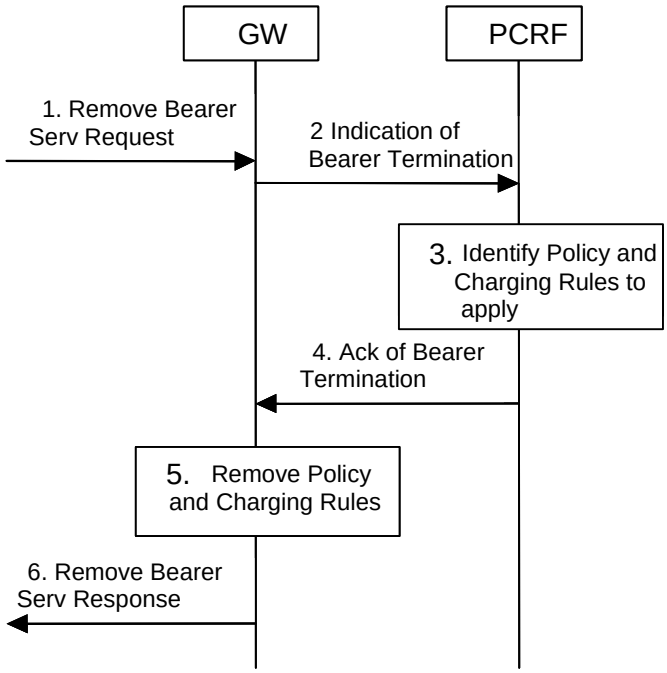


Figure 7.3: Bearer Service Termination

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.

Editor's note: The case where the GW or the PCRF removes the bearer is FFS.

Annex A:
Change history

Change history							
Date	**TSG SA2 #**	**TSG SA2 Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2004-10					*First version created*	*0.0.0*	*0.0.1*
2004-10-15	SA2#42	S2-043313			Agreed document at SA2#42	0.0.1	0.1.0
2004-10-15	SA2#42	S2-043314			Agreed document at SA2#42	0.0.1	0.1.0
2004-01-11	SA2#43	S2-043899			Agreed document at SA2#43	0.1.0	0.2.0
2005-03-24	SA2#44	S2-050355rev1			Agreed document at SA2#44		
2005-03-24	SA2#44	S2-050463			Agreed document at SA2#44		
2005-03-24	SA2#44	S2-050357			Agreed document at SA2#44		
2005-03-24	SA2#44	S2-050467			Agreed document at SA2#44		
2005-03-24	SA2#44	S2-050360			Agreed document at SA2#44		
2005-03-24	SA2#44	S2-050468			Agreed document at SA2#44		
2005-03-24	SA2#44	S2-050354			Agreed document at SA2#44	0.2.0	0.3.1
2005-04-20	SA2#45	S2-050844			Agreed document at SA2#45	0.3.2	0.4.0
2005-04-20	SA2#45	S2-050845			Agreed document at SA2#45	0.3.2	0.4.0
2005-04-20	SA2#45	S2-050846			Agreed document at SA2#45	0.3.2	0.4.0
2005-04-20	SA2#45	S2-050847			Agreed document at SA2#45	0.3.2	0.4.0
2005-04-20	SA2#45	S2-050969			Agreed document at SA2#45	0.3.2	0.4.0
2005-04-20	SA2#45	S2-050970			Agreed document at SA2#45	0.3.2	0.4.0
2005-04-20	SA2#45	S2-050750			Agreed document at SA2#45	0.3.2	0.4.0
2005-04-20	SA2#45	S2-050852			Agreed document at SA2#45	0.3.2	0.4.0
2005-04-20	SA2#45	S2-050850			Agreed document at SA2#45	0.3.2	0.4.0
2005-04-20	SA2#45	S2-050851			Agreed document at SA2#45	0.3.2	0.4.0
2005-04-20	SA2#45	S2-050854rev1			Agreed document at SA2#45	0.3.2	0.4.0
2005-05-13	SA2#46	S2-051424			Agreed document at SA2#46	0.4.0	0.5.0
2005-05-13	SA2#46	S2-051374			Agreed document at SA2#46	0.4.0	0.5.0
2005-05-13	SA2#46	S2-051375			Agreed document at SA2#46	0.4.0	0.5.0
2005-05-13	SA2#46	S2-051376			Agreed document at SA2#46	0.4.0	0.5.0
2005-05-13	SA2#46	S2-051378			Agreed document at SA2#46	0.4.0	0.5.0
2005-05-13	SA2#46	S2-051371			Agreed document at SA2#46	0.4.0	0.5.0
2005-05-13	SA2#46	S2-051372			Agreed document at SA2#46	0.4.0	0.5.0
2005-05-13	SA2#46	S2-051377			Agreed document at SA2#46	0.4.0	0.5.0
2005-05-25	SA2#46	-			Updated by Rapporteur after meeting to include changes and agreed to sent to TSG SA for information	0.5.0	0.5.2
2005-05-27	SA#28	SP-05xxx	-	-	Edited by MCC for presentation to TSG SA for information	0.5.2	1.0.0

3GPP TR 23.803 V0.54.20 (2005-054)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Evolution of Policy Control and Charging (Release 7)

GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS

Keywords

QoS, Flow Based Charging, Service Based Local Policy

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 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*.

[<seq>] <doctype> <#>[([up to and including]{yyyy[-mm]|V<a[.b[.c]]>}[onwards])]: "<Title>".

[1] 3GPP TR 41.001: "GSM Release specifications".

[2] 3GPP TS 23.207: “End-to-end Quality of Service (QoS) concept and architecture”

[3] 3GPP TS 23.125: “Overall high level functionality and architecture impacts of flow based charging”

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the [following] terms and definitions [given in ... and the following] apply.

*<**defined term**>: <definition>.*

~~**example:** text used to clarify abstract rules by applying them literally.~~

default PDP context: In GPRS, the default PDP context is the PDP context, if any, with no TFT associated for a particular PDP address and APN pair. This may be either a primary or secondary PDP context.

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 3GPP TS 23.125, and of the 3GPP Policy Enforcement Point defined in 3GPP TS 23.207.

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 23.125 [3].

Service data flow: aggregate set of packet flows. In the case of GPRS, it shall be possible that a service data flow is more granular than a PDP context.

3.2 Symbols

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

<symbol> <Explanation>

3.3 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

3GPP TS 23.207 [2] specifies the Service Based Local Policy architecture, and 3GPP 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 rel6 Flow Based Charging which includes how policy can be provided with the Rel6 FBC reference points (Gx, Gy, Rx~~, Ry~~) in the context of multiple service data flows on one single bearer. PCC should continue the rel6 work by enhancing the rel6 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

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: Separate IP-flow-level QoS and minimum QoS authorization are 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.

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 presence of complete Rel-6 style binding information (Token and Flow Identifier(s)), in the GW request to the PCRF indicates that bearer authorization from an AF is required for the specific bearer

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 F~~.~~F~~.~~S. The PCRF procedures shall be specified in such a way that PDP contexts, without any active charging rule, are not allowed.

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 release 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.

4.2 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 ~~both~~ 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 policy control over Go 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 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 the network connected to (i.e. APN) and the AF contacts the CRF based on the end user (IP) address as experienced at the AF.

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

4.2.1 Reference Model

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

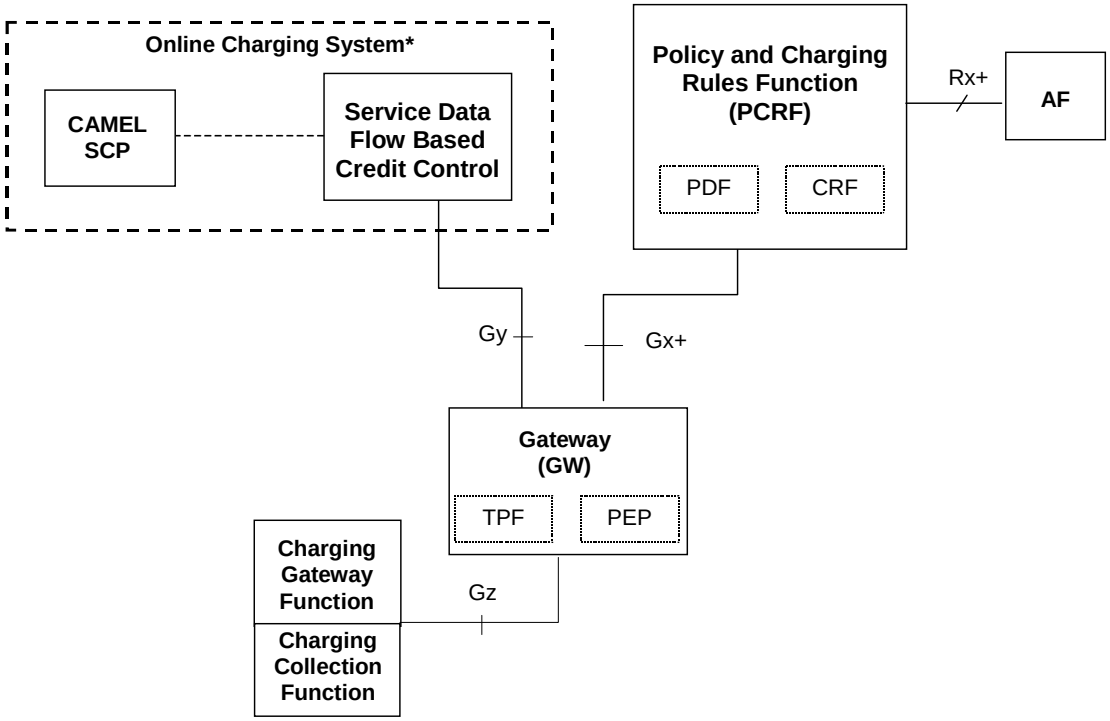


Figure 4.1: Overall architecture for combined policy and charging control

Editor's note-i: Standalone Go interface may be supported for backwards compatibility reasons although it is not shown in the figure.

Editor's note-ii: Support for the existing Rel6 Gq and Rx interfaces is FFS.

4.2.2 Reference Points

4.2.2.0 General

The reference points for the PCC architecture use and enhance the interfaces used in rel6 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 Rx together with Gq reference points with 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 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.

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 ~~functionalities of the PDF and the CRF, and provides for a single point of~~ policy control decision and flow based charging control functionalities. It provides network control regarding the QoS and flow based ~~policy and~~ 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 stipulate how a certain IP 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 and the PCRF policy decision(s). 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 receives the requested QoS. Then the PCRF checks it against the authorized QoS and hence may downgrade the requested QoS from the GW when it exceeds the authorized QoS.

4.2.3.2 Gateway (GW)

The Gateway encompasses policy enforcement and flow based charging functionalities. It provides control over the user plane traffic handling at the GW and its QoS, and provides service data flow detection and counting as well as ~~functionalities of the PEP and the TPF. It provides QoS control of the traffic to enforce the Authorised QoS and~~

~~provides flow based packet counting functionalities along with~~ online and offline charging ~~interactions. For GPRS, QoS enforcement can be either in a synchronous response to the SGSN PDP context messages, or as a GGSN initiated PDP context modification~~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 block the IP flow but still be able to account for it.

For an IP flow that is under policy control the GW shall allow the IP 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 an IP flow that is controlled by FBC the GW shall allow the IP 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 an IP flow pass through the GW during the course of the credit re-authorization procedure.

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
- other 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 ppossible 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 3GPP TS 23.125 incorporates the notion of the CRF taking subscriber-specific knowledge into account for the construction of charging rules. However, 23.125 does not specify how the CRF acquires subscriber-specific knowledge. The PDF 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:

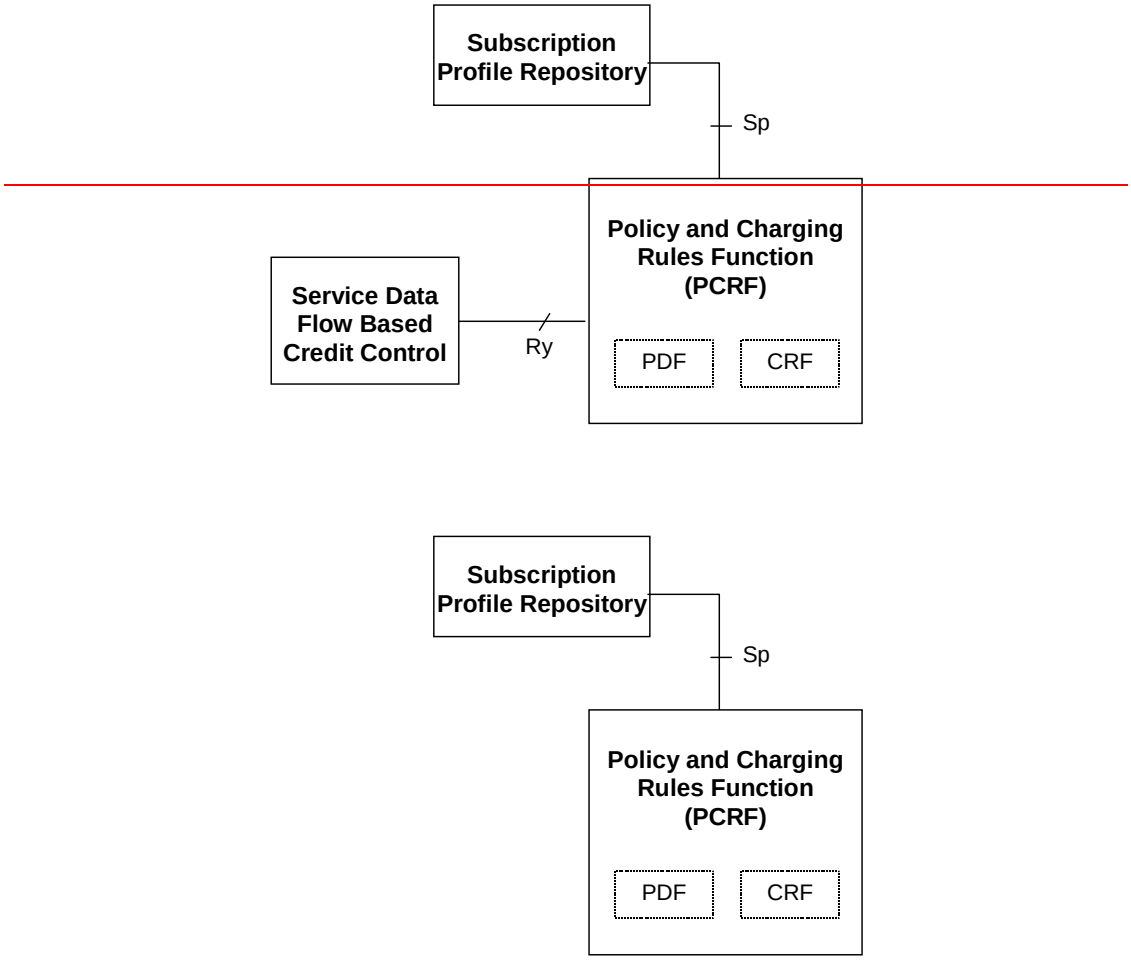


Figure 5.1: Adding subscription aspects to the PCC architecture

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 ~~functions of the~~ SPR's ~~as well as it'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 Go 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

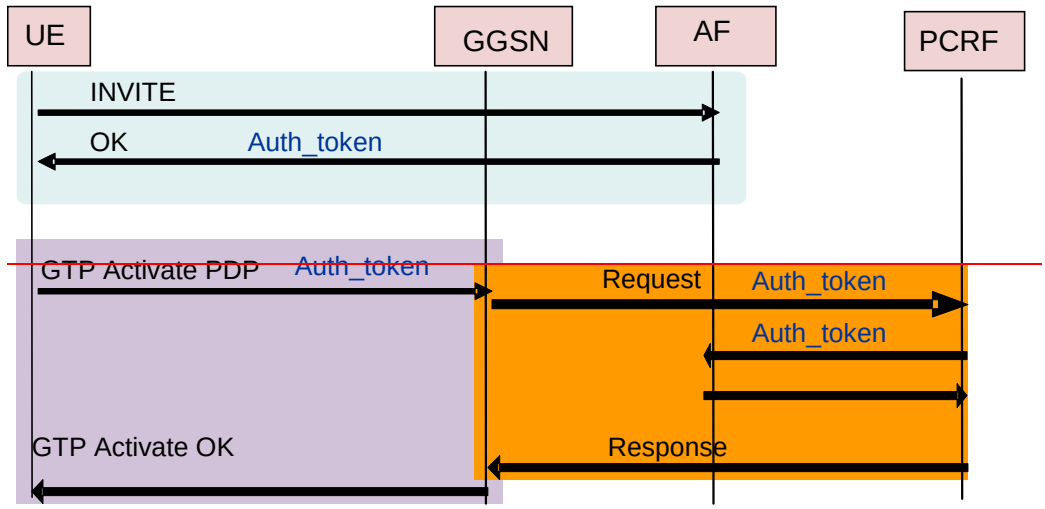
Authorisation Token based binding is the only binding mechanism supported ~~in~~ for the Go interface. Rel-6 Gx interface does not support Authorisation Token based binding.

The Authorization Token is used ~~in the~~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 ~~policy/charging~~authorization ~~rules~~ from the PDF~~/CRF~~.

The PDF~~/CRF~~ 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 ~~of~~ media flows from multiple sessions are associated to the same PDP context, multiple Authorisation Tokens are received in the same ~~policy/charging rules~~bearer authorization request allowing PDF the to combine the policy~~/charging rules from~~of multiple ~~sources~~sessions. Figure 6.1 below shows the Authorization Token based binding concept:



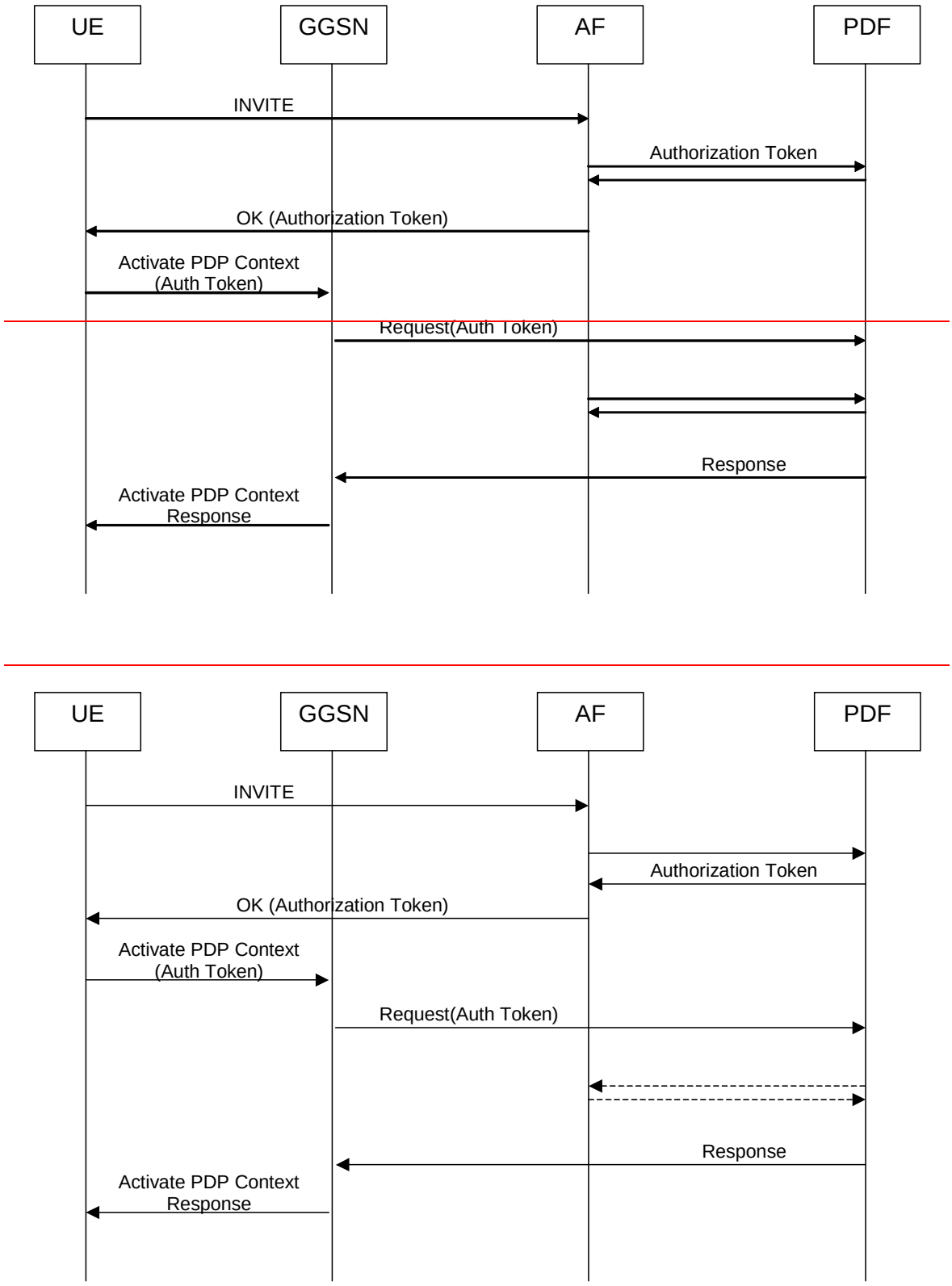


Figure 6.1.: Authorization token based binding as per Release 6 specifications

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. 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 ~~secondary~~ 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 ~~the~~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

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

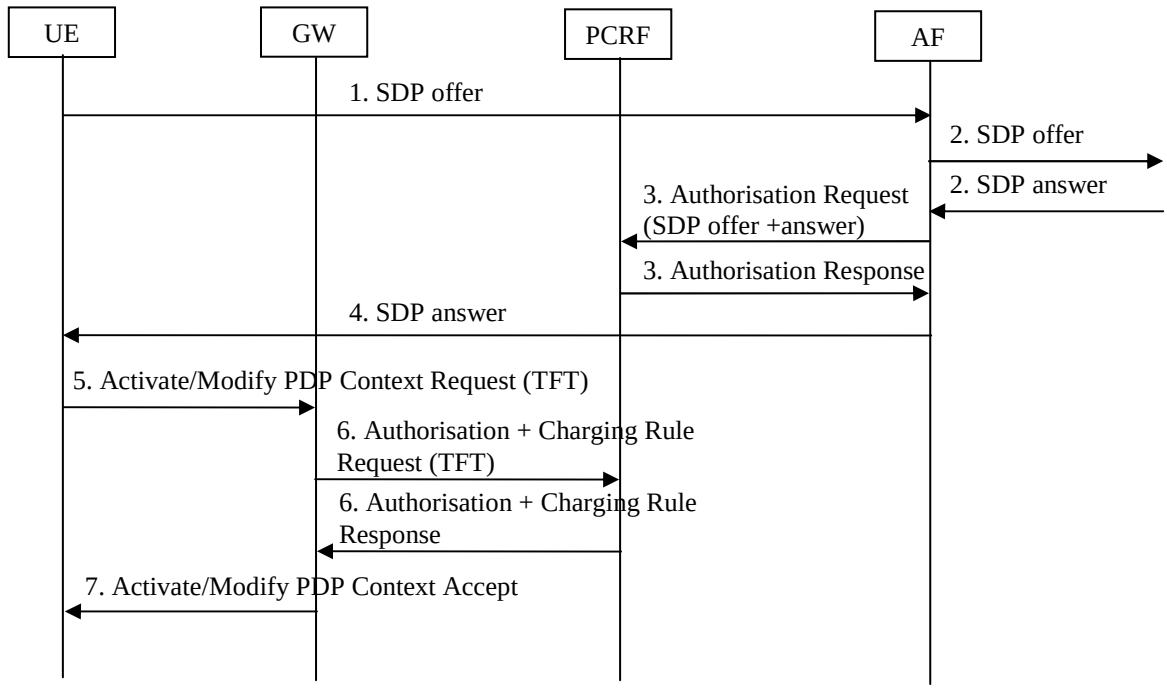


Figure 6.2: Example flow for UE IP address + TFT based binding mechanism

The TFT filter is not included into the PDP context activation/modification request by the UE ~~in case when~~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 ~~in case~~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.

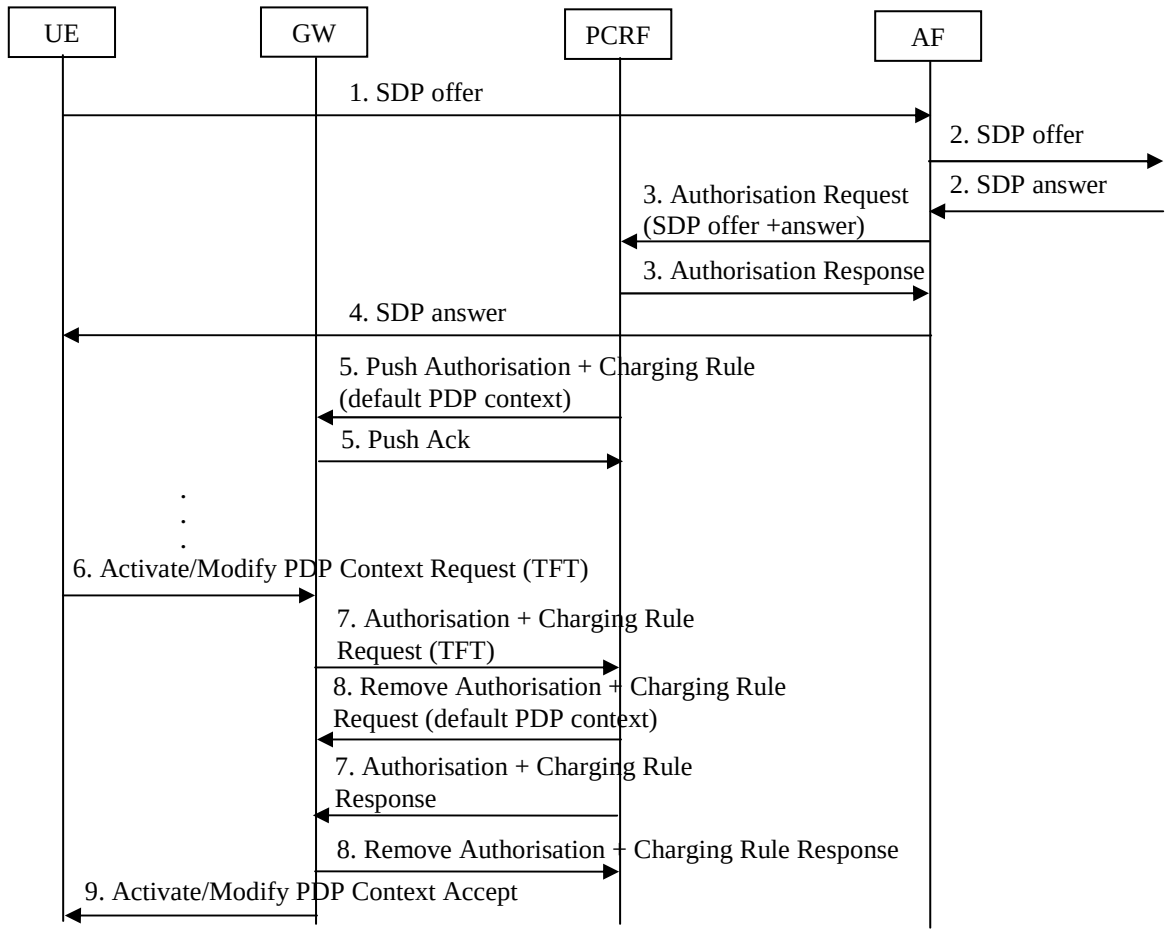


Figure 6.3: Example flow where PDP context activation/modification occurs after session setup

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 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. 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).

To overcome this limitation the following solutions can be foreseen:

- For a bi-directional IP flow (i.e. 2 IP address/port number pairs in a bi-directional communication), both downlink and uplink packets must 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

- The UE shall declare unidirectional uplink flows by specifying a TFT filter for the downlink direction on the intended PDP context.

- 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).

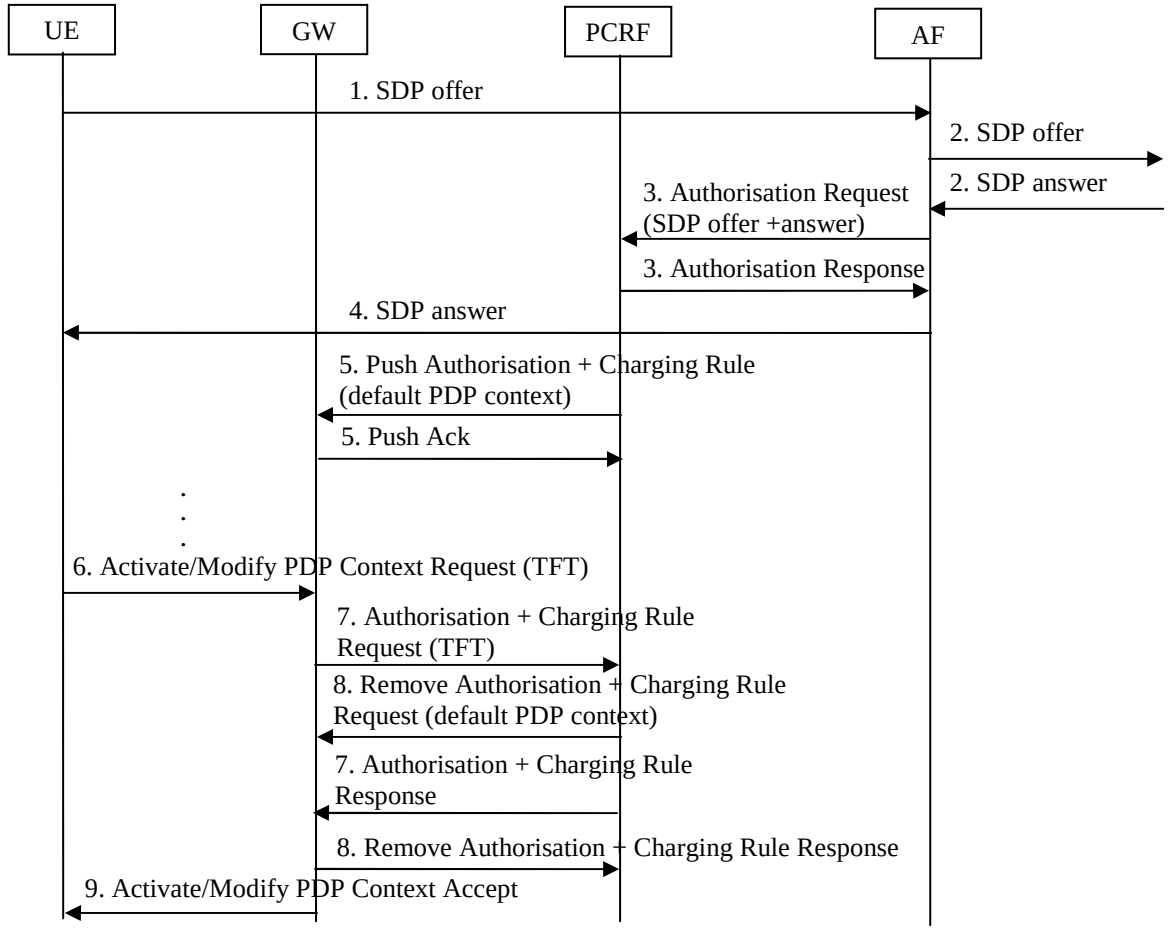
- The UE is required to set the indication parameter as well as the other parameters of the TFT packet filter according to the uplink IP flow(s). The GGSN behaves as already specified, installing the TFT and forwarding the TFT to the PCRF including the TFT packet filters for the uplink. Alternatively, 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.

Editors Note-i: By modifying the handling of TFT packet filters for sending uplink traffic mapping information 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 information from the UE.

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

~~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**~~

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 Rel6. 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, especially from backwards compatibility perspective, along with further binding mechanism alternatives.

It is up to GW to select the appropriate binding information depending what information is available at the GW. The PCRF architecture shall be capable to use any of the specified binding information.

For other binding mechanisms than Authorisation Token based binding the PCRF contact information shall be configured to the GW. The GW may be served 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.

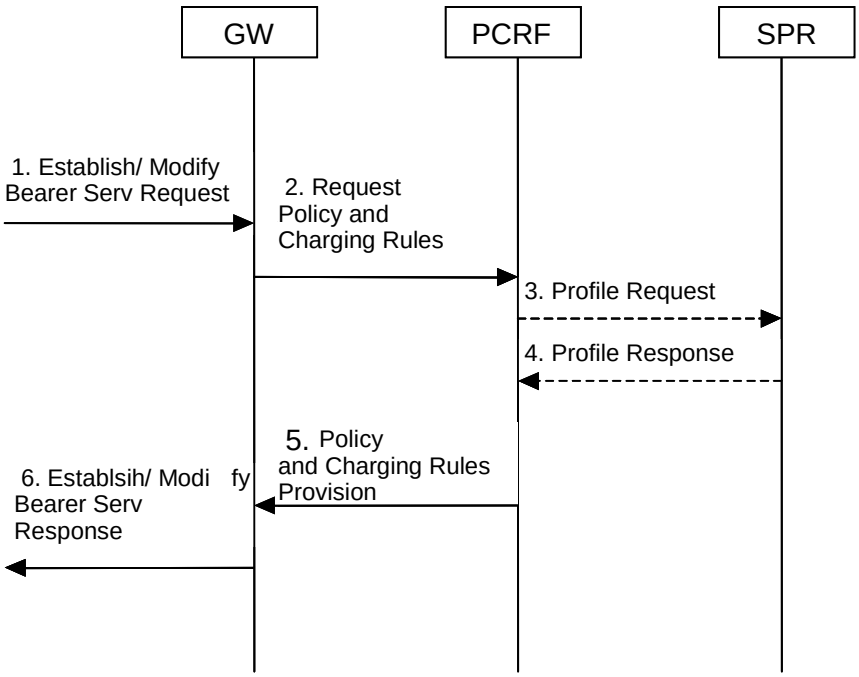


Figure 7.1: Bearer Service Establishment without AF interaction

1. The GW receives a request for bearer establishment. 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 subscriber's authorization, allowed service(s) and Policy and Charging Rules information.

3. If the PCRF does not have the subscriber's profile, it sends a request to the SPR in order to receive the profile.

4. The SPR replies with the subscription profile containing the subscriber's authorization, allowed service(s) and Policy and Charging Rules information.

5. The PCRF makes the authorization and policy decision and sends it the GW. The GW enforces the decision.

6. The GW acknowledges the Bearer Authorization 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 establishment.

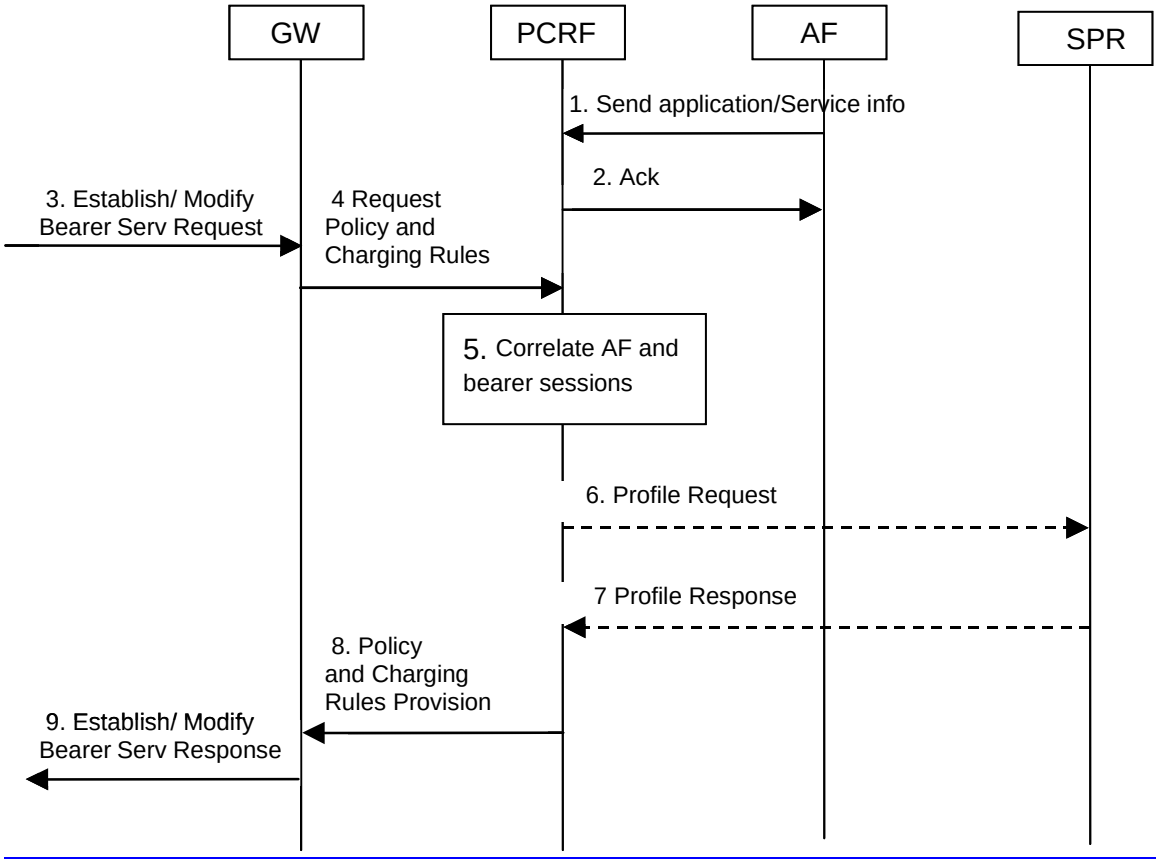


Figure 7.2: Bearer Service Establishment and Modification with AF Interaction

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. 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 information from the SPR, if the PCRF does not have it.

7. If step 6 took place, then SPR replies with the subscriber's profile, and the PCRF stores the profile.

NOTE 1: For bearer service modification, the PCRF contacts AF at this point, it 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 23.207 [2].

8. The PCRF makes the authorization and policy decision and sends it to the GW. The GW enforces the decision.

9. The GW acknowledges the Bearer authorization 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 23.207 [2].

7.3 Bearer Service Termination

This sub-clause describes the signalling flow for the bearer service termination. An example of the scenario is UE originated PDP context termination.

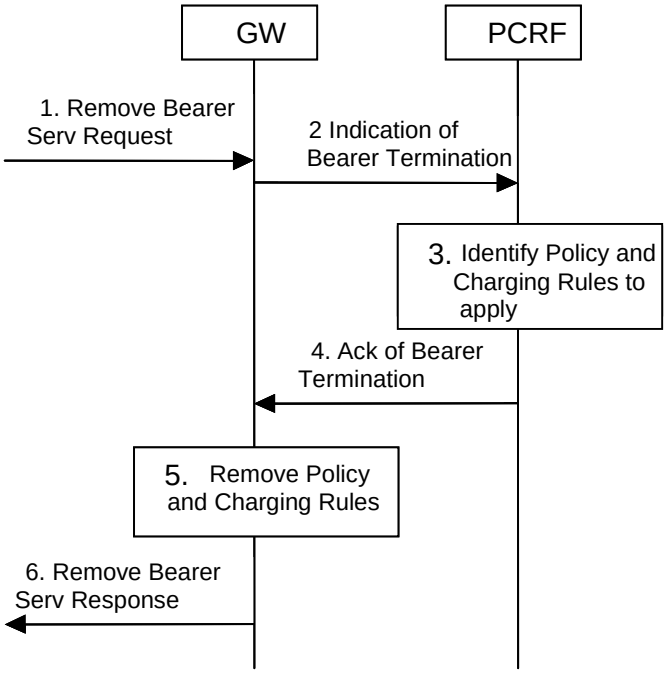


Figure 7.3: Bearer Service Termination

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.

Editor's note: The case where the GW or the PCRF removes the bearer is FFS.

Annex <X>: Change history

Change history							
Date	**TSG SA2 #**	**TSG SA2 Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2004-10					*First version created*	*0.0.0*	*0.0.1*
2004-10-15	SA2#42	S2-043313			Agreed document at SA2#42	0.0.1	0.1.0
2004-10-15	SA2#42	S2-043314			Agreed document at SA2#42	0.0.1	0.1.0
2004-01-11	SA2#43	S2-043899			Agreed document at SA2#43	0.1.0	0.2.0
2005-03-24	SA2#44	S2-050355rev1			Agreed document at SA2#44		
2005-03-24	SA2#44	S2-050463			Agreed document at SA2#44		
2005-03-24	SA2#44	S2-050357			Agreed document at SA2#44		
2005-03-24	SA2#44	S2-050467			Agreed document at SA2#44		
2005-03-24	SA2#44	S2-050360			Agreed document at SA2#44		
2005-03-24	SA2#44	S2-050468			Agreed document at SA2#44		
2005-03-24	SA2#44	S2-050354			Agreed document at SA2#44	0.2.0	0.3.1
2005-04-20	SA2#45	S2-050844			Agreed document at SA2#45	0.3.2	0.4.0
2005-04-20	SA2#45	S2-050845			Agreed document at SA2#45	0.3.2	0.4.0
2005-04-20	SA2#45	S2-050846			Agreed document at SA2#45	0.3.2	0.4.0
2005-04-20	SA2#45	S2-050847			Agreed document at SA2#45	0.3.2	0.4.0
2005-04-20	SA2#45	S2-050969			Agreed document at SA2#45	0.3.2	0.4.0
2005-04-20	SA2#45	S2-050970			Agreed document at SA2#45	0.3.2	0.4.0
2005-04-20	SA2#45	S2-050750			Agreed document at SA2#45	0.3.2	0.4.0
2005-04-20	SA2#45	S2-050852			Agreed document at SA2#45	0.3.2	0.4.0
2005-04-20	SA2#45	S2-050850			Agreed document at SA2#45	0.3.2	0.4.0
2005-04-20	SA2#45	S2-050851			Agreed document at SA2#45	0.3.2	0.4.0
2005-04-20	SA2#45	S2-050854rev1			Agreed document at SA2#45	0.3.2	0.4.0
2005-05-13	SA2#46	S2-051424			Agreed document at SA2#46	0.4.0	0.5.0
2005-05-13	SA2#46	S2-051374			Agreed document at SA2#46	0.4.0	0.5.0
2005-05-13	SA2#46	S2-051375			Agreed document at SA2#46	0.4.0	0.5.0
2005-05-13	SA2#46	S2-051376			Agreed document at SA2#46	0.4.0	0.5.0
2005-05-13	SA2#46	S2-051378			Agreed document at SA2#46	0.4.0	0.5.0
2005-05-13	SA2#46	S2-051371			Agreed document at SA2#46	0.4.0	0.5.0
2005-05-13	SA2#46	S2-051372			Agreed document at SA2#46	0.4.0	0.5.0
2005-05-13	SA2#46	S2-051377			Agreed document at SA2#46	0.4.0	0.5.0