3GPP TR 23.813 V11.0.0 (2011-06)

Technical Report

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Study on Policy solutions and enhancements
(Release 11)

Keywords

3GPP, ANDSF, Charging, QoS

3GPP

Postal address

3GPP support office address

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

Internet

http://www.3gpp.org

Copyright Notification

Contents

Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

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

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

Introduction

The importance of policy based service delivery has been recognized within 3GPP and has resulted in following work in the last few releases:

- QoS and Charging related policies
  - PCRF
- Non 3GPP access inter-working
  - ANDSF
  - Mobility protocol selection

In addition there has been work done in IMS that defines policies related to selection of IMS for service delivery vs other mechanisms. 3GPP work in this area reflects efforts to improve service delivery based on operator policy, user preferences etc. However the approach so far has been fragmented and a more comprehensive approach would ensure better policy decisions. Some examples of what is missing are:

- Deep Packet Inspection coupled with user privacy policies to improve user experience. For example, by intelligently identifying service in use and providing service enhancement via e.g. appropriate QoS for the service, location related info for use with the service etc.
- Service based traffic steering e.g. to use different PDNs for different services. For example issues such as source address selection when the UE is connected to multiple PDNs.
- Standardized and extensible ways to implement service policies that go beyond existing PCC IP flow policies. For example transactional service policies such as a policy to enforce max limit on SMSIP/month based on user profile etc. Other example could be service policy such as redirect and firewall control.

1 Scope

The objective is to study an evolved policy solution through enhancement of 3GPP policy framework. One of the aims of the study is to ensure a policy architecture that provides an extensible framework for easy reuse with new IP based services by identifying areas where improvement of specifications are feasible. The study item will look into solutions for the examples in the section above.

Existing components for consideration in the Policy Study are functions and interfaces to/from

- PCRF, PCEF and BBERF;
- SPR, HSS;
- ANDSF;
- IMS policy decision making entities.

The study aims to provide a more comprehensive way (e.g. going beyond existing 3GPP PCC framework) to handle operator policies for all IP / service flows (IMS and non-IMS) in a coordinated manner and under varying network conditions while keeping in view aspects such as:

- user preferences;
- user subscriptions;
- service requirements;
- terminal capabilities (including converged terminals);
- network capabilities (3GPP and those non 3GPP accesses inter- working with 3GPP);
- Session transfer and terminating policies;
- Security policy control, e.g. firewalling and gating.

Roaming scenarios are considered as part of this study. Compatibility with existing system architecture elements are protected and backward compatibility is expected. All types of policies i.e. static/pre-provisioned, dynamic, network based, UE based are considered in the study.

When a key issue is resolved sufficiently to be incorporated into the specification in an independent manner, the study work may move forward for a decision for normative specification work on such issue(s) using a new work item or a TEI.

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 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 41.001: "GSM Release specifications".

[3] 3GPP TS 23.203: "Policy and charging control architecture".

[4] 3GPP TS 22.101: "Service aspects; Service principles".

[5] 3GPP TS 23.335: "User Data Convergence (UDC); Technical realization and information flows".

[6] 3GPP TS 23.198 v9.0.0: "Open Service Access (OSA)".

[7] 3GPP TS 32.296: "Online Charging System (OCS): Applications and interfaces".

[8] 3GPP TS 32.299: "Charging management: Diameter charging applications".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

4 Key issues

4.1 Key Issue 1: Policy enhancement for sponsored data connectivity

4.1.1 Introduction

The target of this key issue is to study policy enhancement needed for sponsored data connectivity With sponsored data connectivity, the sponsor has a business relationship with the operator and compensates the operator for user's connectivity in order to allow the user access to one or more services provided by the sponsor, a 3rd party service provider or the operator. For example, existing OSA standards, defined in 3GPP TS 3GPP TS 23.198 [6] provide a comprehensive framework to support 3rd party applications. The framework supports security, authentication an authorisation of 3rd party providers, and open APIs to facilitate controlled access to SP's resources, QoS requests, charging and other capabilities. Whether the user pays the sponsor for the connectivity or not, in the context of sponsored IP-CAN connectivity, makes no difference with respect to the handling of end user charges for the connectivity.

The following actors are involved in a scenario of sponsored connectivity:

Sponsor: the one willing to take the operator's charge for connectivity.

Application Service provider: the one providing the sponsored service. May coincide with the sponsor.

Operator: the one providing connectivity. May also be service provider.

End user: the one using the sponsored service. Is a subscriber at the operator.

It is assumed the user has already a subscription for PDN access with a mobile operator. In particular, the following areas will be studied:

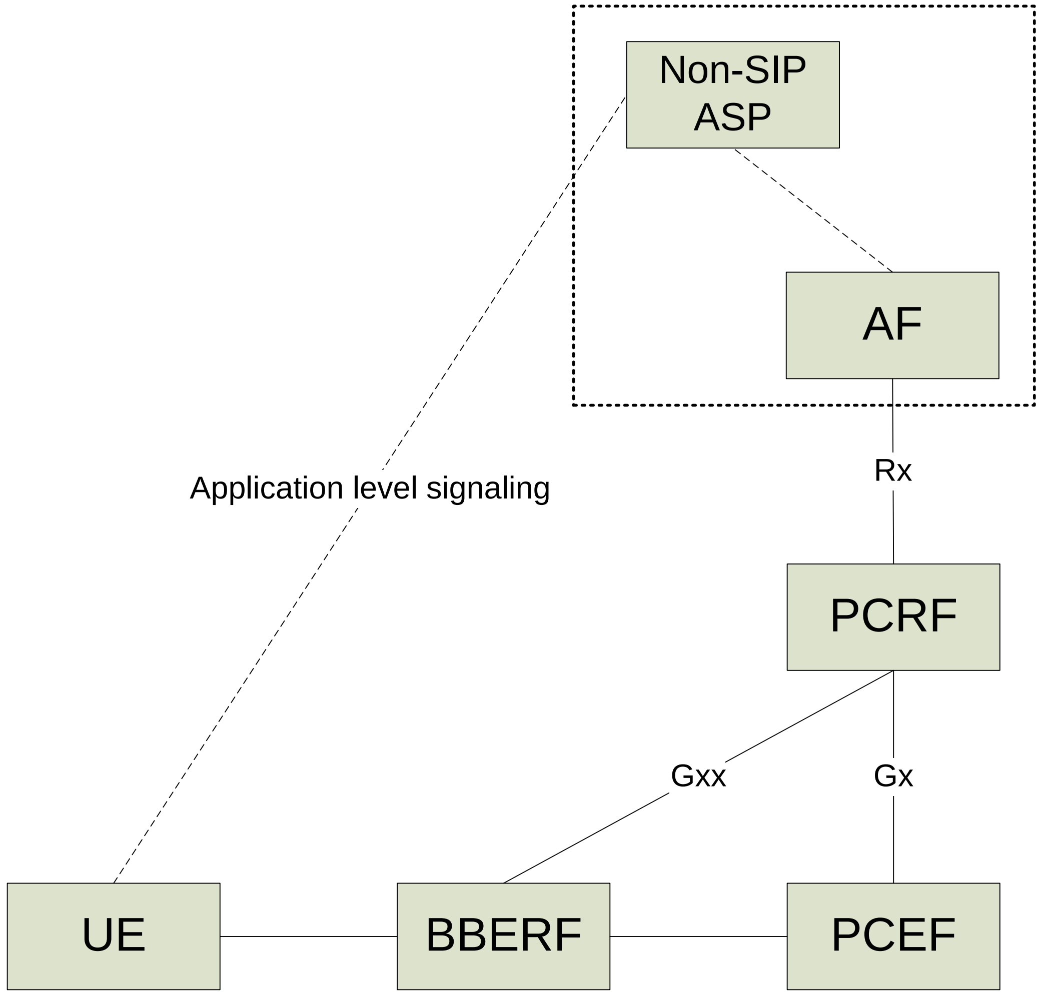
- Capability for a service provider's application functions to authorize IP flows that are subject to a specific sponsorship.
- Capability to validate dynamic authorizations for sponsored IP flows .
- Capability to exclude the sponsored IP flows from the monitoring for user's volume cap.
- Capability to charge the end user, including pre-paid credits users, at a different rate when the service is sponsored (often, but not necessarily, free of charge) compared to non-sponsored usage of the same service.

- Capability to create accounting and/or usage data records where the usage data associated with sponsorship is separated from other usage data.

4.1.2 Alternative solutions

4.1.2.1 Alternative 1

A possible architecture for sponsored data connectivity is shown illustrated in Figure 4.1.2.1-1 in the non roaming case. In the roaming case a S9 reference point is present between the H-PCRF and the V-PCRF.



NOTE: The interface between the AF and Non-SIP ASP which requires sponsored data connectivity may be based on the OSA standards per 3GPP TS 3GPP TS 23.198 [6] but is out of scope of this specification. A one to one mapping between the Non-SIP ASP and the AF is not needed as a single AF can be used to serve multiple Non-SIP ASPs.

Figure 4.1.2.1-1: Architecture for sponsored data connectivity

There are two scenarios for the Non-SIP ASP possible: the ASP is only involved in the application level signalling or the ASP is in addition involved in the user data exchange, i.e. the IP packets carrying the payload of the application.

In the latter case it is possible to keep the decision about the duration of the sponsored data connectivity at the ASP so that the interaction with the PCRF follows the existing Rx procedures. The PCRF does only need to know the required information to identify the service (e.g. via the AF Application identifier and the AF Application event identifier) and to describe the sponsored IP flows that the ASP wants to get authorized. The ASP can initiate the Rx session termination once the sponsored usage of the ASP service can be stopped, e.g. if a download is complete.

If the ASP is only involved in the application level signalling, the PCRF needs to know in addition the information about the duration and/or the volume which is authorized by the ASP because the ASP does not necessarily know when the sponsored usage of the ASP service can be stopped. These parameters would have to be added to the Rx signalling.

NOTE: Retransmissions should be taken into account in the duration/volume allowance given by the ASP.

In both scenarios the charging systems and the PCRF need to be configured in the following way:

- In case a Sponsor Identity is not used a service specific Charging Key and Monitoring Key has to be used for the sponsored IP flows (that is not shared with any other service of the UE in this PDN connection) so that the PCEF can generate separate accounting and/or usage data records.
- In case a Sponsor Identity is used to separate accounting and/or usage data records the same Charing Key and Monitoring Key may be used both for sponsored IP flows and for the IP flows that are not sponsored. The Sponsor Identifier will be used to correlate measurements from different users and for different services for accounting purposes.
- The PCRF needs to know the ASPs that have a business relationship with the operator and the policies that are related to them, primarily the QoS that is to be authorized for the sponsored IP flows.
- If the AF is in the operator's network and is based on the OSA/Parlay X GW as defined in TS 23.198 [6] OSA specification the PCRF is not required to verify that a trust relationship exists the operator and the 3rd party ASP

4.1.2.1.1 Reference points enhancements

4.1.2.1.1.1 AF - PCRF reference point (Rx)

The Rx reference point between the AF and the PCRF is described in TS 23.203 [3]. The Rx reference point is further enhanced to optionally provide service information related to sponsored data connectivity. The following information shall be possible to provide over the Rx reference point:

- Sponsor Identifier;
- Information identifying the application service provider and application;
- Optionally allowed volume of the sponsored connectivity and/or a time interval and whether the PCRF reports these events to the AF.

4.1.2.1.1.2 PCEF- PCRF reference point (Gx)

The charging part of the PCC rule is augmented with the possibility to include the Sponsor Identity and Application Service Provider Identity with the rule.

4.1.2.1.1.3 PCEF - OCS and PCEF - OFCS reference points (Gy and Rf/Gz)

The normal usage reporting per user (a.k.a. containers) is augmented with the Sponsor Identity and Application Service Provider Identity.

Editor's note: This is potentially SA WG5 domain.

For Gy the quota handling is separate for Charging keys accompanied by a Sponsor Identity and Application Service Provider Identity.

In the charging domain, reports are extracted and consolidated, possibly from all users when that applies for the sponsored service, to form the usage data for a Service Identifier. The Sponsor Identity, The Application Service Provider Identity, the Service Identifier and the usage data suffice to make the settlement with the sponsor and Application Service Provider.

4.1.2.1.1.4 PCRF - SPR reference point (Sp)

The SPR includes profiles for sponsor data connectivity containing Sponsor Identities and list of applications per Application Service Provider.

4.1.2.1.2 Call flows

4.1.2.1.2.1 General

This clause contains call flows to demonstrate the PCC interaction for sponsored data connectivity under various scenarios, including rule installation when sponsored data connectivity is activated, rule modification when sponsored data connectivity is extended, usage reporting for sponsored data connectivity, and rule remove when sponsored data connectivity is terminated.

4.1.2.1.2.2 Call flow for sponsored data connectivity rule installation

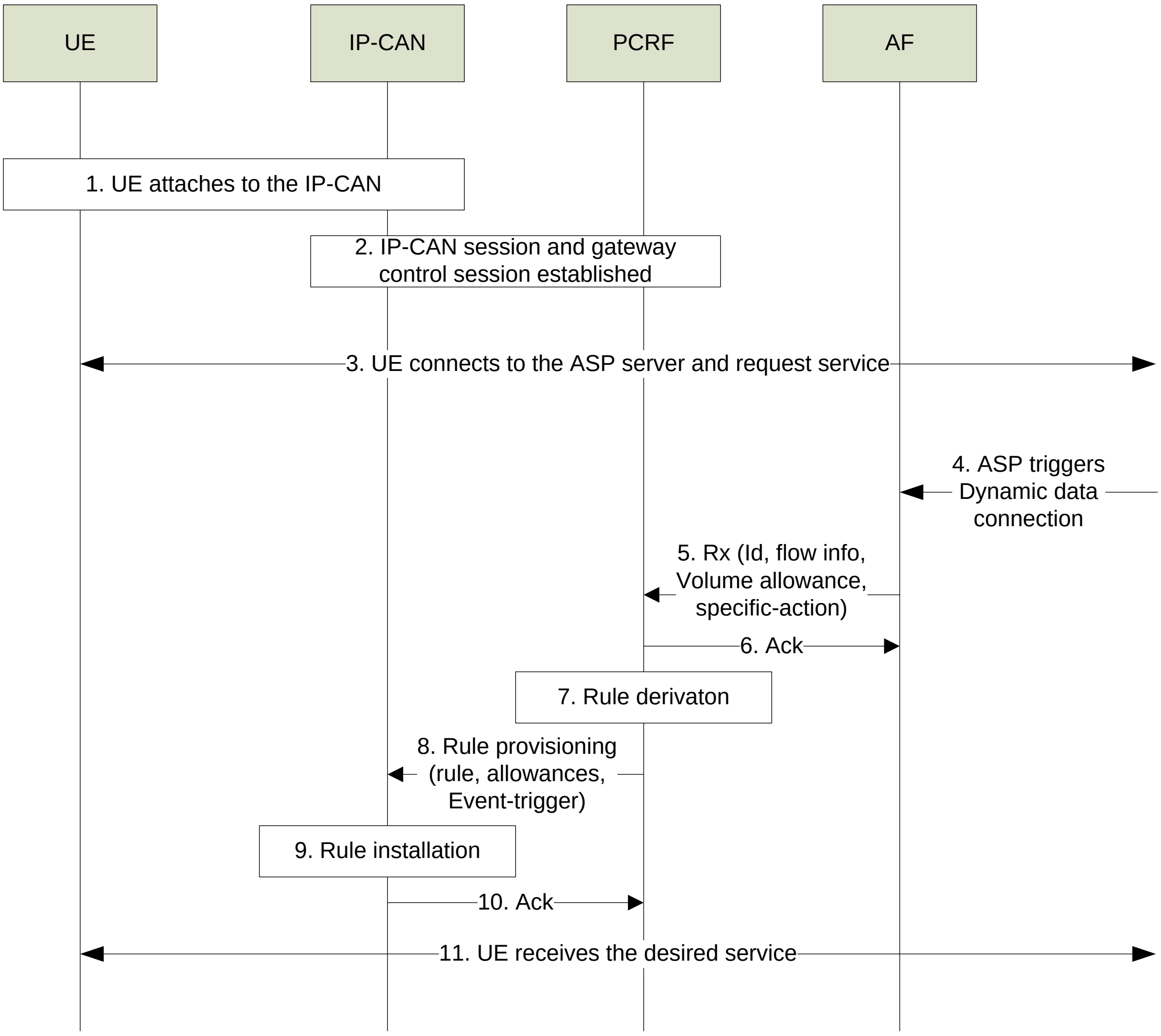

UE
IP-CAN
PCRF
AF
1. UE attaches to the IP-CAN
2. IP-CAN session and gateway control session established
3. UE connects to the ASP server and request service
4. ASP triggers Dynamic data connection
5. Rx (Id, flow info, Volume allowance, specific-action)
6. Ack
7. Rule derivaton
8. Rule provisioning (rule, allowances, Event-trigger)
9. Rule installation
10. Ack
11. UE receives the desired service

Figure 4.1.2.1.2.2-1: Call flow for sponsored data connectivity rule installation

1. The UE attaches to the IP-CAN following the normal procedures specific to the IP-CAN.

2. The PCEF and/or the BBERF establish IP-CAN session and/or gateway control session toward the PCRF following the procedures described in TS 23.203 [3]. The UE's IP connection may have a limited amount of data usage.

3. The UE connects to the 3rd party ASP server and requests services from the ASP.

4. The ASP server decides to sponsor the data connection used to access the ASP service for the user and provide dynamic sponsoring information, as agreed with the operator, to the AF within the operator's network. The dynamic sponsoring information includes the user identity to be sponsored (e.g. the IP address), the IP flow information to be sponsored, Sponsor Identity, Application Service Provider Identifier. Optionally the usage amount to be sponsored and the threshold request related to the sponsored data connectivity.

5. For each sponsored service occasion, the AF establishes an Rx session toward the PCRF as described in TS 23.203 [3] and provides the identity of the AF, a Sponsor Identity, an Application Identity, the user identity and the service information optionally including volume allowance and specific-actions related to the service.

6. The PCRF authorizes and acknowledges the service information received from the AF.

7. The PCRF derives PCC/QoS rules related to the sponsored data connectivity and may take into account the Sponsor Identity and Application Identifier.

8. The PCRF provision the rules and event triggers for the sponsored data connectivity to the PCEF/BBERF within the IP-CAN.

9. The PCEF/BBERF installs the provisioned rules and event triggers.

10. The PCEF/BBERF sends acknowledgement to the PCRF.

11. The UE uses the sponsored connectivity to receive the desired service from the ASP.

4.1.2.1.2.2 Call flow for sponsored data connectivity usage report

This call flow is only required if the ASP is not involved in the user data exchange and thus the PCRF needs to manage the information about the duration and/or the volume which is authorized by the ASP.

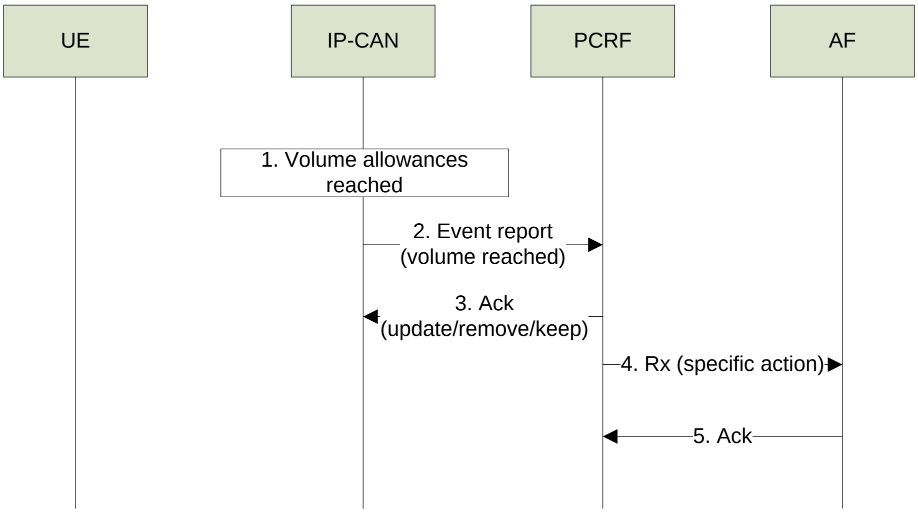

UE
IP-CAN
PCRF
AF
1. Volume allowances reached
2. Event report (volume reached)
3. Ack (update/remove/keep)
4. Rx (specific action)
5. Ack

Figure 4.1.2.1.2.2-1: Call flow for sponsored data connectivity usage report

1. At one point of time, the volume allowance set for the sponsored data connectivity is reached.

2. The PCEF sends an IP-CAN session modification request toward the PCRF including an event trigger to indicate that the data usage has reached the volume threshold.

3. The PCRF, based on information received from the AF, may update the threshold or remove the PCC rule and QoS rule related to the sponsored connectivity; the PCRF may also keep the same rules active but notify the AF as described in the subsequent steps.

4. The PCRF sends an notification message to notify the AF that data usage has reached threshold.

5. The AF acknowledge the notification from the PCRF. If needed, the AF may follow the procedures described in clause 4.1.2.1.2.3 to extend the sponsorship or the procedures described in clause 4.1.2.1.2.4 to terminate the sponsorship.

4.1.2.1.2.3 Call flow for sponsored data connectivity extension

This call flow is only required if the ASP is not involved in the user data exchange and thus the PCRF needs to manage the information about the duration and/or the volume which is authorized by the ASP.

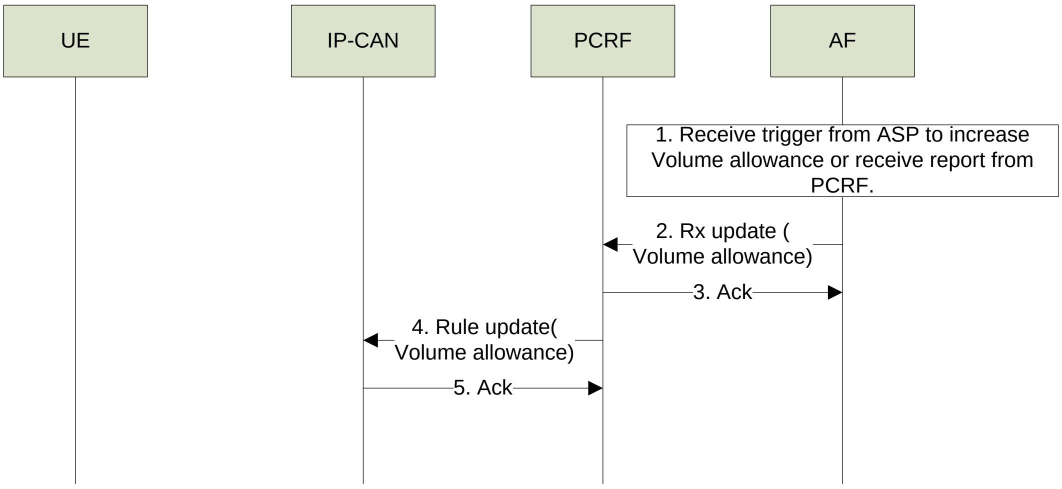

UE
IP-CAN
PCRF
AF
1. Receive trigger from ASP to increase Volume allowance or receive report from PCRF.
2. Rx update (Volume allowance)
3. Ack
4. Rule update(Volume allowance)
5. Ack

Figure 4.1.2.1.2.3-1: Call flow for sponsored data connectivity extension

1. The AF receives trigger from the ASP to increase volume allowance or receives report from the PCRF to indicate that previously set threshold has been met.

2. The AF sends new allowance information to the PCRF to extend the previous sponsored connectivity.

3. The PCRF sends acknowledgement to the AF.

4. The PCRF updates the corresponding PCC rules with new volume allowance information received.

5. The PCEF acknowledges the updated PCC rules.

4.1.2.1.2.4 Call flow for sponsored data connectivity release

When the AF receives a trigger from the ASP or an internal trigger to terminate the sponsorship, the AF terminates the Rx session as specified in TS 23.203 [3].

4.2 Key issue 2: Coherent access to Policy related databases

4.2.1 Description

To enable operator policies, currently a number of logical databases have to be accessed. These include HSS, SPR and possible databases tied to ANDSF functionality. While implementation of many of these databases will continue to be deployment specific it is possible to consolidate them logically by providing a single logical interface to access them.

4.2.2 Alternative solutions

4.2.2.1 SPR as an Application Front-End of the UDC Architecture

In order to provide coherent accesses to operator policy databases, the SPR shall be part of the 3GPP UDC architecture. According to TS 22.101 [4], the UDC concept supports a layered architecture, separating the data from the application logic in the 3GPP system. In that way user data is stored in a logically unique repository allowing access from core and service layer entities, named application front-ends

For such purpose, the SPR shall be an Application Front-End according to TS 23.335 [5]. This SPR-FE shall support the Ud reference point for querying, creating, updating or deleting data from the UDR. The SPR-FE shall make also use of the Ud reference point for subscribing to and receiving notifications from the UDR.

The SPR Application Front-End shall interact with the PCRF via Sp reference point.

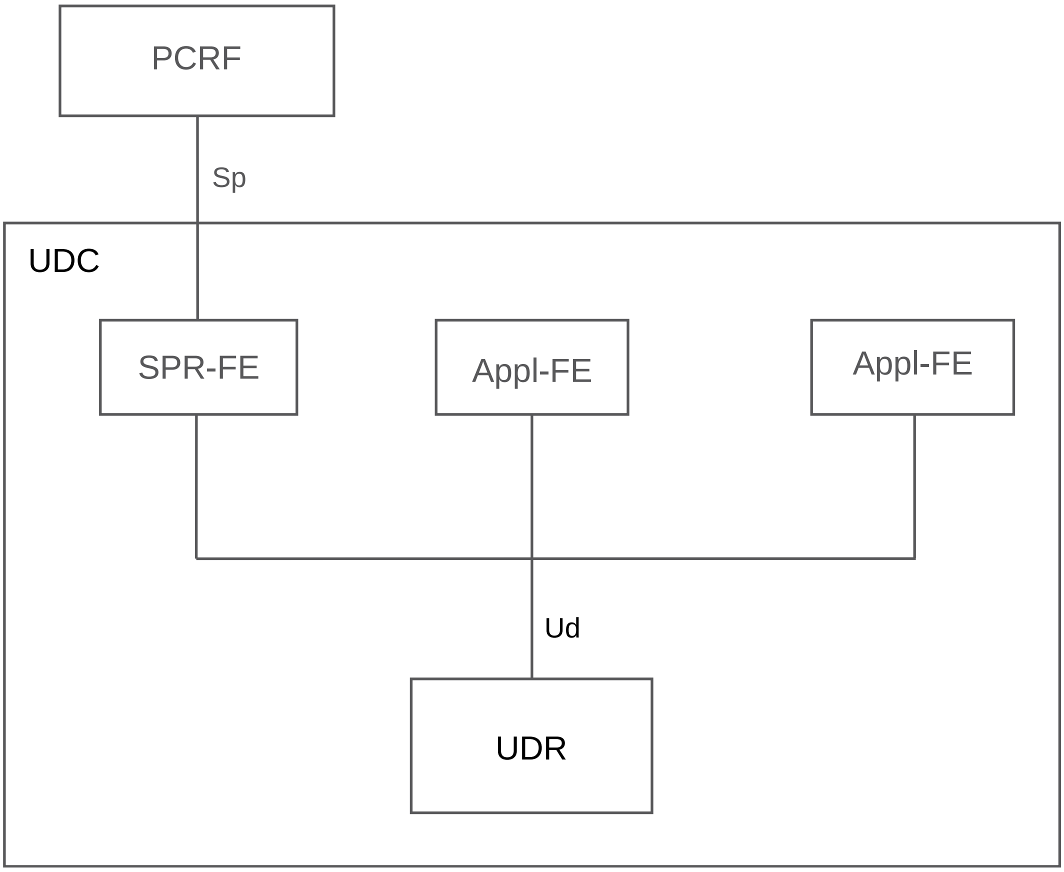


Figure 4.2.2.1-1: SPR as Application Front-End within the User Data Convergence architecture

In order to fulfil the requirements that UDC architecture sets into the Application Front-Ends (clause 4.1 of TS 22.101 [4]), the SPR-FE shall be a subscriber dataless entity.

4.2.2.2 PCRF as an Application Front-End of the UDC Architecture

An alternative solution is that the PCRF as an entity without persistent subscriber data has direct access to the User Data Repository (UDR) which is part of the 3GPP UDC architecture. Sp reference point and SPR entity would disappear in such a configuration. PCC related persistent subscriber data are stored in the UDR while the related application logic is implemented in the PCRF.

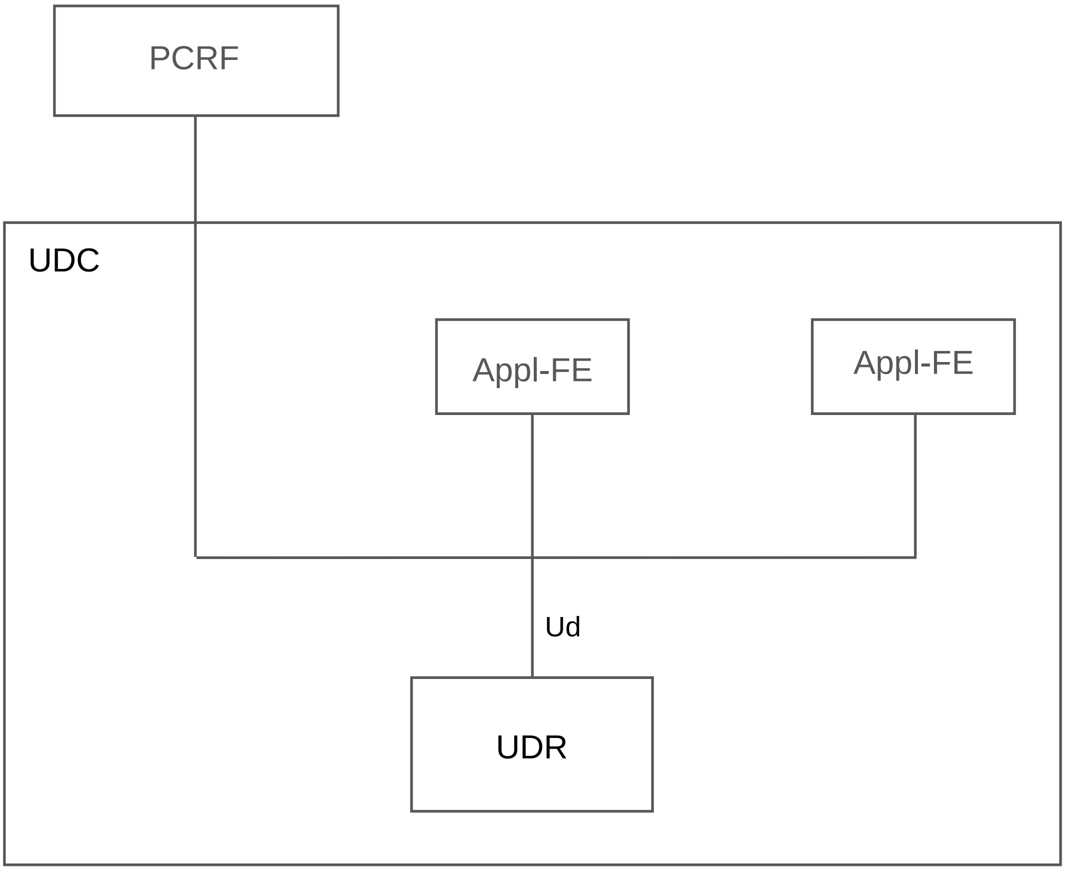


Figure 4.2.2.2-1: PCRF as Application Front-End within the User Data Convergence architecture

CT WG4 concluded that the PCRF meets the requirements of an application front end. Consequently, this alternative does fulfil 3GPP UDC requirements as they are specified in TS 22.101 [4], clause 4.11. While the PCRF is not a subscriber dataless entity, due to it's managing the user context for IP-CAN sessions, it only stores user data temporarily while an IP-CAN session for the user is ongoing. When no IP-CAN session is ongoing for a user, no user data need to be kept in the PCRF.

In this use case the PCRF shall support the Ud reference point instead of Sp to access PCC related data stored in the UDR. It shall also use the Ud reference point for subscribing to and receiving notifications from the UDR.

4.2.3 Comparison of alternatives

According to the CT WG4 evaluation both alternatives describe valid architectures to integrate PCC related subscriber data into the UDC architecture and to access these data from the UDR.

As the PCRF can be seen as a network element, which represents pure application logic with no persistent data storage functionality but with user data access towards an external database, it may be assumed to perform the functionality of an application frontend and access the user data via the Ud interface directly from the UDR.

On the other hand PCC implementations may already exist where the Sp interface has been implemented in a vendor specific manner. In those cases, without impacting the existing PCRF implementation, PCC related persistent subscriber data stored in the SPR can be moved to the UDR with the SPR migrating to a pure Application Frontend from the UDC point of view that interworks between Sp and Ud interface.

4.2.4 Conclusion

The alternative architecture options as described in clauses 4.2.2.1 and 4.2.2.2 are both valid. Whether the one or other is chosen depends on the actual network deployment.

If the SPR is used in a network to store the PCC related subscriber data, introducing the UDC concept (i.e. the UDR as centralized subscriber database) can be done in an evolutionary step by migrating from the existing SPR database to a SPR Application Frontend that provides interworking between Sp and Ud interfaces. This alternative is covered by the general UDC system architecture that can be found in TS 23.335 [5].

NOTE: The SPR information model has to be replaced by an appropriate UDR information model.

Alternatively data stored in the SPR can be moved to the UDR requiring the PCRF to support the Ud interface in order to fetch PCC related subscriber data instead of Sp. This architectural option needs to be documented in TS 23.203 [3], introducing the UDR as an alternative to the existing SPR and Ud as alternative to Sp.

4.3 Key issue 3: QoS and gating control based on spending limits

4.3.1 Description

The following use case has been identified, which requires the PCRF to perform QoS and gating control decisions based on information only available in the OCS:

- **QoS control based on spending limits** - ability to change the QoS level based on spending limits. Example scenario: the subscriber plan allows for high QoS up to $2 per day and a lower QoS beyond that.

4.3.1.1 Common Principles

These principles apply to all of the proposed alternative solutions. Signalling may take place directly between OCS and PCRF or via PCEF as outlined in the alternative solutions.

- A counter as defined in TS 32.296 [7] shall exist in the ABMF within the OCS that tracks a subscriber's spend over a period of time.
- The OCS may have more than one counter per subscriber. Each counter can track a subscriber's overall spend or that of an individual service. An identification mechanism will be required to differentiate counters.
- Counter management is the responsibility of the OCS, including any associated threshold value(s) (e.g. $2).
- Policy decisions relating to gating and QoS are the responsibility of the PCRF.
- When the counter value reaches an associated threshold, the OCS notifies the PCRF.

Editor's note: Further information being passed from OCS to PCRF is not excluded by this principle.

- At least two conditions shall trigger information flow between OCS and PCRF in relation to these use cases:
  - On IP-CAN session establishment, the OCS will inform the PCRF what thresholds have already been reached, allowing the PCRF to make an initial policy decision for the session.
  - When a threshold is reached mid-session, the OCS shall notify the PCRF triggering modification of the subscriber's policy appropriately.

4.3.2 Alternative solutions

4.3.2.1 Alternative solution 1 - configuration based solution

A QoS control based on spending limits can be realized based on existing PCC and online charging functionality. This requires however, that the OCS and the PCRF are configured in the following way:

- A service specific Charging Key has to be used for the service for the time the service has not reached its spending limits. This service specific Charging Key cannot be shared with any other service of the UE in this PDN connection.- A second Charging Key has to be available for the service after reaching the spending limit (i.e. the "out of credit" event). This Charging Key can only be shared with other services if the service can remain with the current setting until the service is terminated. If the service should ever return to the original setting (e.g. after a certain time interval has been passed), the second Charging Key cannot be shared with any other service. The OCS can then instruct the PCRF to return to the original setting by denying credit for this second Charging Key.
- The PCRF needs to apply a second QoS authorization after it gets informed about the "out of credit" event.
- The OCS needs to store the spending limits for the service specific Charging Key when the credit management interaction for the service is terminated.

- The OCS needs to reset the spending limit for the service specific Charging Key after the corresponding time interval has been passed.

Editor's note: Configuration efforts (e.g. increased number of Charging Keys) and potential functionality enhancements (e.g. accounting of packets when applying the termination action) needs to be further analyzed.

If the PCRF and the OCS are configured appropriately, the QoS control based on spending limits proceeds in the following way:

- The PCRF applies a service specific Charging Key A for the service (that is not shared with any other service of the UE in this PDN connection) together with the QoS that is intended to be used before the spending limit is reached. In addition, the PCRF sets the "out of credit" event trigger.

- The OCS receives the Charging Key A during the credit management interaction and starts (or continues) to measure the parameter that is subject to the spending limit control (i.e. time, volume and/or event) in addition to the normal charging functionality.

- Once the OCS detects that the spending limit is reached, it denies any further credit to the PCEF. In addition, the OCS may set the Termination Action to "Allowing the packets to pass through" to enable the continuation of the service.

- The PCEF reports the "out of credit" event to the PCRF together with the corresponding PCC rule.

- The PCRF can now react and modify the PCC rule according to the operator configuration. The PCRF would select a different Charging Key B and the QoS that has to be applied after reaching the spending limit.

- The PCEF enforces the modifications for the PCC rule and may need to modify the bearer or even bind the PCC rule to a different bearer. In addition, the new Charging Key B is used for the credit management.

- The OCS receives the new Charging Key B and continues to grant credits for this service.

- If the OCS wants the service to return to the original QoS (e.g. after the time interval that is relevant for the spending limit has been passed), the OCS may apply the very same mechanism (i.e. denying credit, setting Termination Action). The PCRF would get informed about it in the very same way and modify the PCC rule back to the original QoS and the Charging Key A.

4.3.2.2 New reference point (Sy) between PCRF and OCS

4.3.2.2.1 General

A solution is to define a new reference point Sy between the PCRF and the OCS to enable transport of indications about charging related events from the OCS to the PCRF.

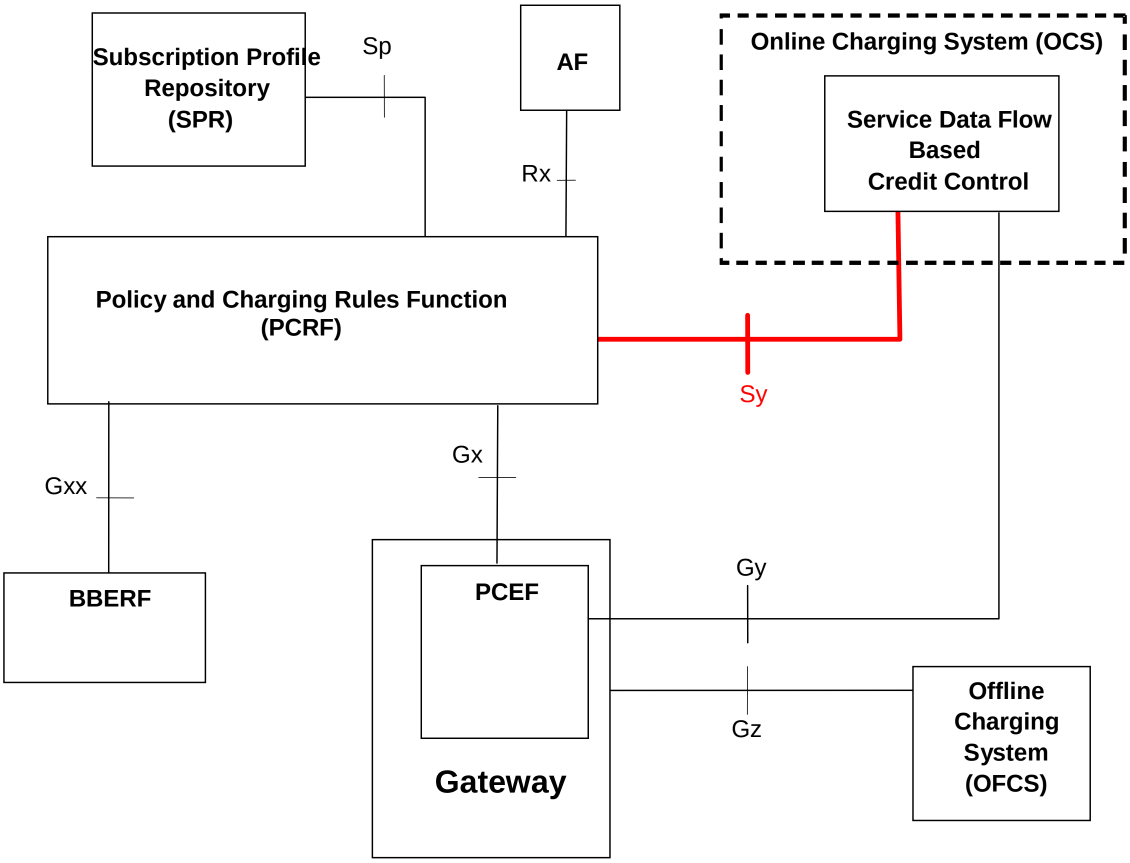

Subscription Profile Repository (SPR)
Sp
AF
Online Charging System (OCS)
Service Data Flow Based Credit Control
Rx
Policy and Charging Rules Function (PCRF)
Sy
Gx
Gxx
BBERF
PCEF
Gy
Gz
Offline Charging System (OFCS)
Gateway

Figure 4.3.2.2.1-1: Overall PCC architecture (non-roaming) including the Sy reference point

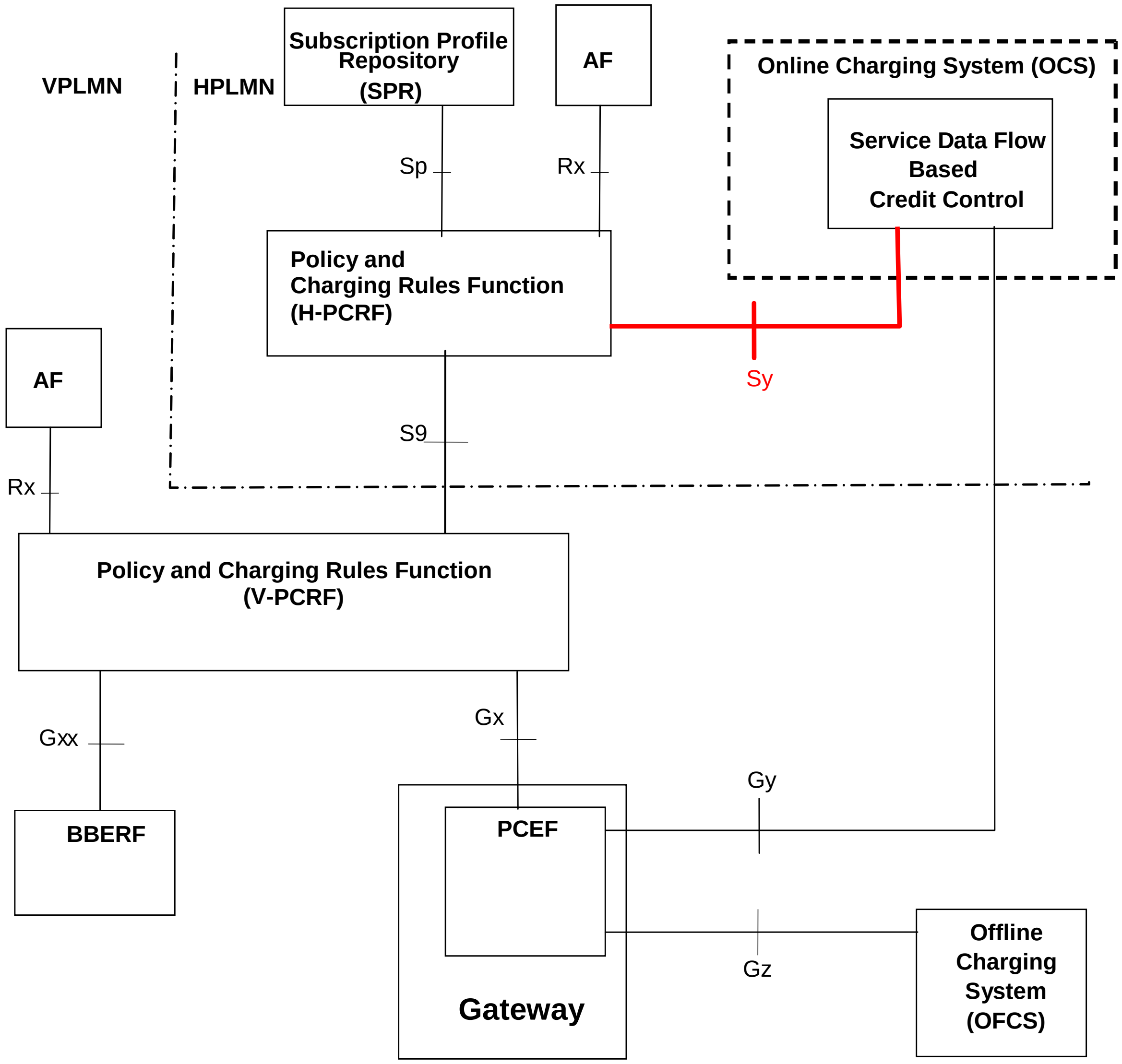

VPLMN
HPLMN
Subscription Profile Repository (SPR)
AF
Online Charging System (OCS)
Service Data Flow Based Credit Control
Sp
Rx
Policy and Charging Rules Function (H-PCRF)
Sy
AF
S9
Rx
Policy and Charging Rules Function (V-PCRF)
Gxx
Gx
Gy
BBERF
PCEF
Gateway
Gz
Offline Charging System (OFCS)

Figure 4.3.2.2.1-2: Overall PCC architecture including the Sy reference point roaming with PCEF in visited network (local breakout)

4.3.2.2.2 PCRF contacting the OCS (PCRF-Centric approach)

4.3.2.2.2.1 Session scope

For efficient communication and to be able to support multiple PDN-connections of a user the scope of the Sy connection should be organised on a per subscriber ID and PDN identifier basis, i.e. (at least) all PDN-connections of a UE to the same APN are bound to the same Sy session. This is possible since multiple PDN-connections to the same APN are always controlled by the same PCRF since PCC Rel-8.

4.3.2.2.2.2 Session initiation

At IP-CAN session establishment, according to TS 23.203 [3], Gx interactions take places prior to Gy interactions. For the PCRF to be able to provide correct policies at IP-CAN session establishment it is necessary for the PCRF to interact with the OCS prior to sending acknowledge of IP-CAN session establishment to the PCEF. Additionally it is the PCRF that is aware of if the policies of an IP-CAN session are dependent on charging related information. Sy Session Establishment should therefore be initiated by the PCRF.

The Sy reference point allows the PCRF to request and subscribe to indications about charging related events that affect session and service policies of PDN connections for different users and PDNs.

The OCS shall support to bind a Sy session with associated Gy sessions and shall notify the PCRF over the Sy interface whenever there is charging related event occurring that the PCRF has subscribed to.

4.3.2.2.2.3 Information exchange

The Sy reference point shall support to provide the following indications:

- Provisioning of indication based on credit balance (e.g. when OCS decides that a prepaid subscriber has reached a balance limit)
- Provisioning of indication per rating group or per IP-CAN session based on previously consumed volume or spending limits (e.g. when OCS decides that a previously consumed volume or spending limit per period has reached a certain value).

4.3.2.2.2.3.1 Charging Status Reports

Provisioning of Charging Status Reports is based on the assumption that that the OCS maintains the necessary counter(s) used to track spending between sessions.

The OCS maintains pre-configured counter(s) with an associated threshold, which it resets according to a known time schedule. Counters could be applicable either per subscriber, per subscriber and active PDN or for a group of services for a certain subscriber.

The identities of the counters that are relevant for a policy decision are stored in the PCRF or in the SPR. The PCRF is configured with the actions associated with the counter status that is received from OCS.

The request and provisioning of Charging Status Reports may be used for:

The initial request for counter state at IP-CAN session establishment.

The notification from the OCS to the PCRF of threshold reached by OCS. When counters that are applicable either for a single service or for a group of services are referenced over the Sy interface a new identifier called Policy-Counter-Id shall be used. All services that are mapped to the same Policy-Counter-Id will share the same counter state and applicable threshold values in the OCS.

NOTE: The relation between a Policy-Counter-Id and the Charging Key could be 1-1. However it could also be assumed that services that share the same Charging Key may be associated with different Policy-Counters i.e. although they are rated in the same way they are subject to different actions regarding (e.g. QoS and gating) and are therefore counted separately.

When a certain threshold has been reached (e.g. daily spending limit of 2$ reached) in the OCS and/or when a certain threshold has been increased or the accumulated usage is reset the OCS shall provide the new Policy Counter Status to the PCRF for the associated Policy Counter or for the associated UE and active PDN.

The PCRF shall based on the counter status apply operator defined actions, e.g. downgrade the QoS, for affected IP-CAN Sessions and/or PCC-rules and provide this as policy decisions to the PCEF and to the BBERF (if applicable).

4.3.2.2.2.4 Roaming

The Sy reference point should support scenarios where a UE is located in a HPLMN (figure 4.2.2.2-1), roaming with home routed or roaming with visited access (figure 4.3.2.2.1-2). For roaming with visited access the Sy reference point is defined between the H-PCRF and the OCS in the HPLMN. With this approach Sy will be a PLMN internal reference point regardless of if the user is roaming or accessing via the HPLMN.

4.3.2.2.2.5 Signalling flows

4.3.2.2.2.5.1 General

This clause contains signalling flows to demonstrate the PCC interaction to request charging status reports and to provide charging status reports over the Sy reference point. The Sy reference point supports the following functions:

- Request from PCRF to OCS on the initial Policy Counter Status for a certain subscriber or for a certain subscriber and PDN connection.;
- Reports from the OCS to the PCRF on the Policy Counter Status for a certain subscriber or for a certain subscriber and PDN connection.

4.3.2.2.2.5.2 Changes to the IP-CAN Session establishment procedure

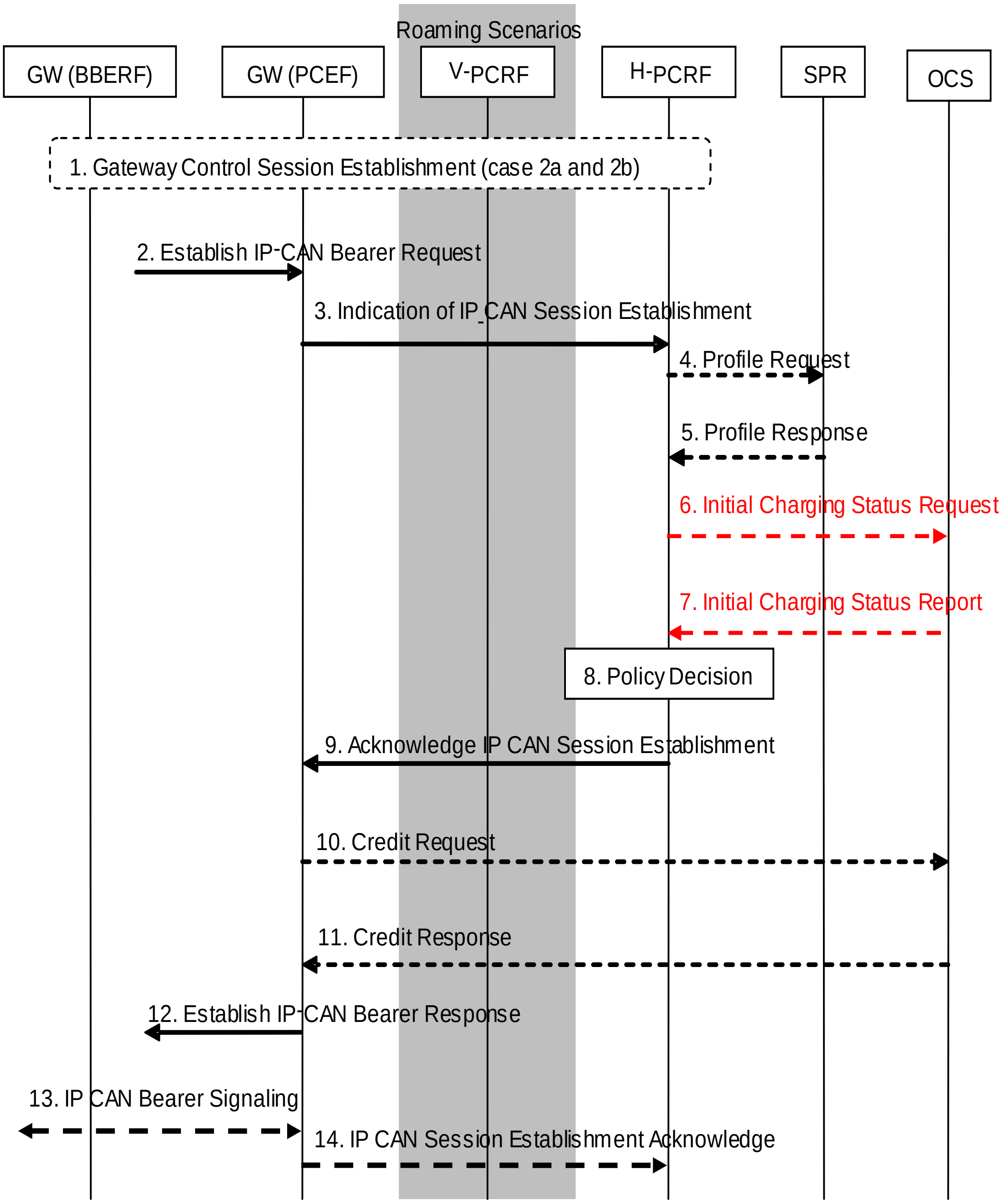

Roaming Scenarios
GW (BBERF)
GW (PCEF)
V-PCRF
H-PCRF
SPR
OCS
1. Gateway Control Session Establishment (case 2a and 2b)
2. Establish IP-CAN Bearer Request
3. Indication of IP_CAN Session Establishment
4. Profile Request
5. Profile Response
6. Initial Charging Status Request
7. Initial Charging Status Report
8. Policy Decision
9. Acknowledge IP CAN Session Establishment
10. Credit Request
11. Credit Response
12. Establish IP-CAN Bearer Response
13. IP CAN Bearer Signaling
14. IP CAN Session Establishment Acknowledge

Figure 4.3.2.2.2.5.2-1

1-5. IP-CAN Session Establishment as per TS 23.203 [3], clause 7.2.

6. If the subscription data received from the SPR indicated that policy decisions are dependent on charging related information and if this is the first IP-CAN session for this subscriber then PCRF sends an Initial Charging Status Request towards the OCS. The PCRF includes the UE identifier and the Policy-Counter-Id(s) for which status is requested. The PCRF may optionally include PDN-id (e.g. APN), the UE IP address and subscribers to changes in the status of the Policy Counters in the OCS.

Editor's note: The possibility for the OCS to report all the Policy-Counter-Status or only those relevant for a policy decision is FFS.

7. The OCS acknowledges the request by sending a Charging Policy Session Acknowledge and may notify whether threshold(s) have already been reached.

8-11. Continued IP-CAN Session Establishment as per TS 23.203 [3], clause 7.2

4.3.2.2.2.5.3 Changes to the IP CAN Session termination procedures

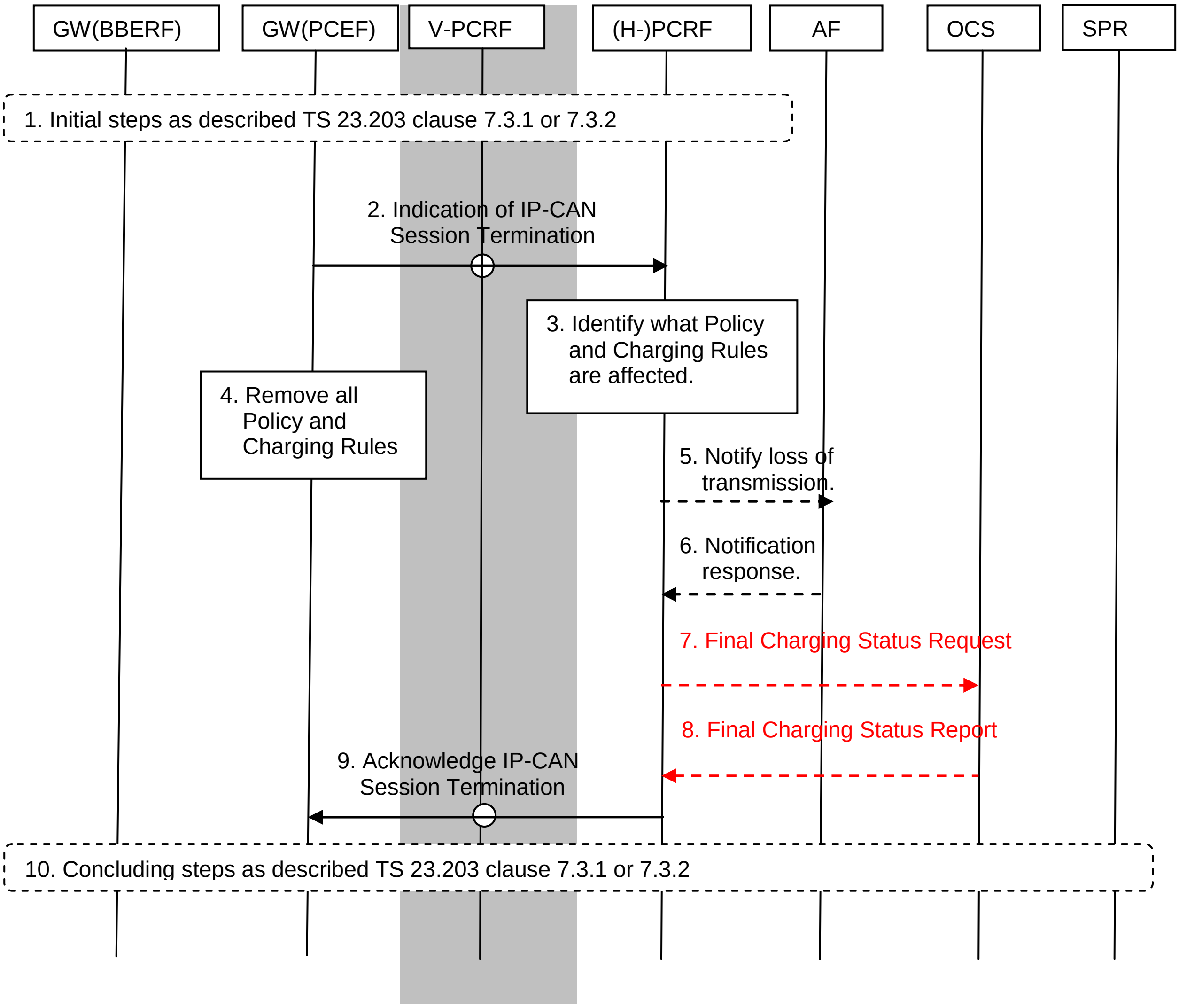

GW(BBERF)
GW(PCEF)
V-PCRF
(H-)PCRF
AF
OCS
SPR
1. Initial steps as described TS 23.203 clause 7.3.1 or 7.3.2
2. Indication of IP-CAN Session Termination
3. Identify what Policy and Charging Rules are affected.
4. Remove all Policy and Charging Rules
5. Notify loss of transmission.
6. Notification response.
7. Final Charging Status Request
8. Final Charging Status Report
9. Acknowledge IP-CAN Session Termination
10. Concluding steps as described TS 23.203 clause 7.3.1 or 7.3.2

Figure 4.3.2.2.2.5.3-1

1-6. IP-CAN Session Termination as per TS 23.203 [3] clause 7.3.1 or 7.3.2.

7. If this is the last IP-CAN session of a subscriber for the PDN-id the PCRF sends a Final Charging Status Request to cancel the subscription to changes in the status of the Policy Counters in the OCS.

8. The OCS acknowledges to the PCRF that the subscription is cancelled.

9-10 Continued IP-CAN Session Termination as per TS 23.203 [3] clause 7.3.1 or 7.3.2.

4.3.2.2.2.6 Provisioning of notifications from OCS to PCRF

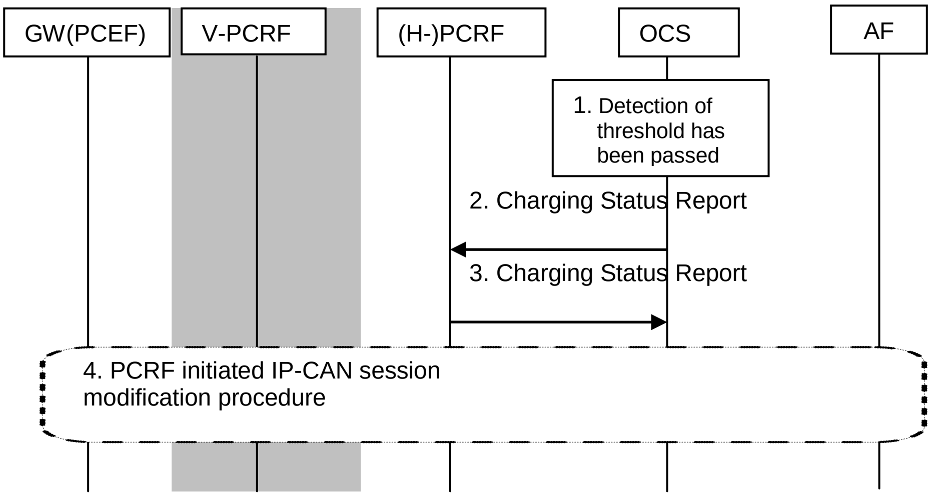

GW(PCEF)
V-PCRF
(H-)PCRF
OCS
AF
1. Detection of threshold has been passed
2. Charging Status Report
3. Charging Status Report
4. PCRF initiated IP-CAN session modification procedure

Figure 4.3.2.2.2.6-1

1. The OCS detects that the status of a Policy-Counter-Id(s) has changed and the PCRF requested notifications of changes in the status of the policy counters.

2. The OCS sends a Charging Status Report to the PCRF. The OCS sends the Policy-Counter-Status(s) per each Policy-Counter-Id(s) that has changed. The Policy-Counter-Status received from the OCS overrides the Policy-Counter-Status stored for a certain Policy-Counter-Id in the PCRF.

3. The PCRF acknowledges the Charging Policy Report.

4. A PCRF initiated IP-CAN Session modification procedure may occur as a result from the received report.

4.3.2.2.2.7 Intermediate Charging Status Request

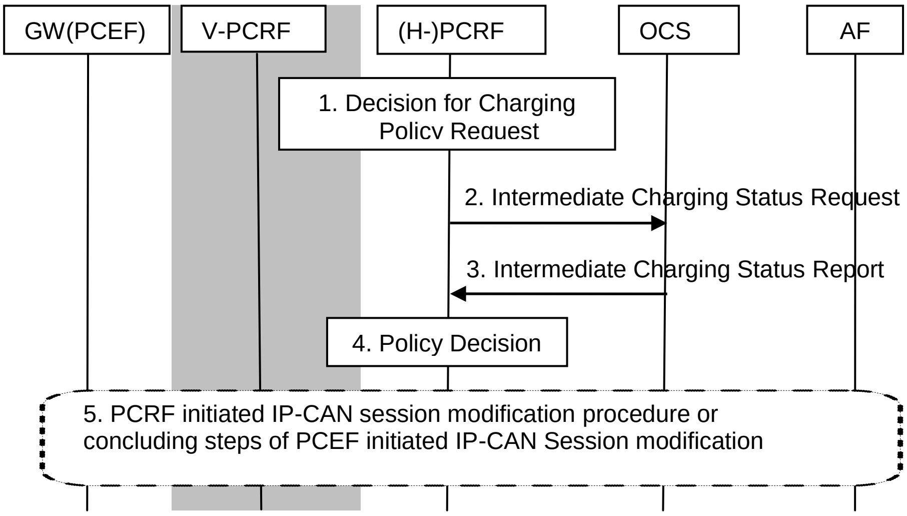

GW(PCEF)
V-PCRF
(H-)PCRF
OCS
AF
1. Decision for Charging Policy Request
2. Intermediate Charging Status Request
3. Intermediate Charging Status Report
4. Policy Decision
5. PCRF initiated IP-CAN session modification procedure or concluding steps of PCEF initiated IP-CAN Session modification

Figure 4.3.2.2.2.7-1

1. The PCRF decides based on interaction with the SPR, AF, BBERF (if applicable) or the PCEF that the need for Charging Status Reports of a user has changed.

2. The PCRF sends an Intermediate Charging Status Request to the OCS, including the applicable Policy-Counter-Id(s).

Editor's note: The possibility for the OCS to report all the Policy-Counter-Status or only those relevant for a policy decision is FFS.

3. The OCS acknowledges the Intermediate Charging Status Request that includes the Policy-Counter-Status per Policy-Counter-Id provided by the PCRF in the Intermediate Charging Status Request.

4. The PCRF makes an updated policy decision based on the received report from the OCS. The Policy-Counter-Status received from the OCS overrides the Policy-Counter-Status stored for a certain Policy-Counter-Id in the PCRF.

5. In case the procedure was triggered by an indication of IP-CAN Session Modification procedure the PCRF concludes this procedure as per TS 23.203 [3], clause 7.4.1 steps 10-18.

4.3.2.2.3 OCS contacting the PCRF (OCS-Centric approach)

4.3.2.3 Alternative solution 3 - enhancing Gy and Gx

A QoS control based on spending limits can be realized by enhancing the Gy and Gx procedures with additional functionality and parameters.

The solution relies on the following procedures:

A. OCS threshold/s reached notification on IP-CAN session establishment

Gy: Credit Request procedure

The Credit Request procedure is initiated by the PCEF in accordance with the TS 23.203 [3] IP CAN session establishment procedure Session

The OCS includes in the Credit Request Response message and indication that the value of counter/s associated with spending limits has reached a threshold.

Gx: IP CAN Session Modification Procedure

When the PCEF receives an indication from the OCS that a threshold/s has been reached it initiates the IP CAN session Modification request to request PPC rules re-authorization due to spending threshold/s reached.

The PCC determines the new/modified PCC rules and responds to the PCRF.

Gy: The PCEF may initiate the Credit Request procedure with the OCS

B. OCS thresholds reached notification in mid-session

Gy: (Credit) Re-Authorization- Request procedure

The OCS initiates the Re-Authorization- Request procedure (according to TS 32.299 [8]) when threshold/s has been reached

Gx: IP CAN Session Modification Procedure

When the PCEF receives an indication from the OCS that a threshold/s has been reached it initiates the IP CAN session Modification request to request PPC rules re-authorization due to spending threshold/s reached.

The PCC determines the new/modified PCC rules and responds to the PCRF.

Gy: (Credit) Re-Authorization- Request Response

The PCEF sends the new/modified PCC rules to the OCS

NOTE: The Session between the PCEF and the OCS is not impacted by this solution and it is terminated as part of the TS 23.203 [3] IP CAN Session termination procedure.

4.3.3 Conclusion

Alternative 2 has the advantage of causing no increase in signalling load at the PCEF, along with the fact that it allows H-PCRF and H-OCS to communicate directly in the LBO roaming scenario, simplifying interworking in that case.

The impact of adding the new Sy reference point is therefore seen as lower than that of the other alternative solutions, both in terms of complexity and network signalling overhead.

The Sy based solution where PCRF initiates Sy interaction (alternative 2) shall be used to achieve the aims of the key issue.

NOTE 1: The behaviour of the OCS and PCRF on Sy failure shall be studied during the resulting normative work.

NOTE 2: No modification to the Gx and Gy reference points is required to resolve key issue #3 or due to the introduction of the Sy reference point.

4.4 Key issue 4: Service Awareness and Privacy Policies

4.4.1 Description

The network may have policies related to specific services but currently it may not always become aware of usage of these services. The service unawareness can occur when there is no explicit service level signalling and hence no interaction between the Application Function and PCRF or when filters related to a service has not been installed in the PCEF. The user experience can be enhanced if the network becomes service aware and the network is able to apply service specific policies. Service traffic detection mechanisms helps achieve service awareness. Traffic detection functionality can be implemented by a standalone entity as well as be collocated with PCEF. Use of service traffic detection mechanism however may require user consent and for this purpose PCC architecture would have to be extended to include user privacy policies.

4.4.2 Actions resulting from service detection

Existing charging and enforcement actions based on PCC rules performed at the PCEF and defined in TS 23.203 [3] are still performed. Charging and enforcement actions based on PCC rules at the PCEF may be influenced by the detected services. Additionally, the following are examples of actions to be taken on the detected service:

- Gating of the detected service traffic (either blocking or permitting unrestricted the detected service traffic)

- Traffic shaping of the detected service traffic

- Redirecting of detected service traffic (for services / protocols that permit redirection)

4.4.3 Alternative solutions

4.4.3.1 Alternative 1

At the time of IP-CAN session establishment, the PCEF contacts the PCRF as per existing procedures. User privacy policy settings are received from the SPR together with the other subscriber related information (the management of the user privacy policy settings is out of scope). The PCRF checks the user privacy policy settings to see if usage of service traffic detection mechanism is allowed and for what services. If it is allowed the PCRF can instruct the Traffic Detection Function (TDF) on what services it should detect and if detection notification is required. After detecting a service with a service traffic detection mechanism, the TDF may inform the PCRF about the detected service, if detection notification is required. The PCRF can then react in the desired way with regard to the policy and charging control information for the detected traffic.

A new mechanism/ parameter for instructing the TDF on what service traffic to detect needs to be defined. While the actual mechanism for the service traffic detection should not be standardized, TDF has to be able to detect the start and the end of the respective service and notify the PCRF correspondingly.

NOTE 1: The potential mechanisms to enable steering of user traffic either to a particular TDF or to bypass this TDF are FFS. A key aspect of the evaluation will be the ability to ensure a subscriber's downlink traffic can be steered to the same TDF which is handling the uplink traffic.

For a collocated PCEF/TDF, the existing PCC rule concept can be extended to include the parameters, which form an SDPR rule, that identifies the service to be detected.

For a standalone TDF, a Service Detection and Policy (SDPR) rule used both to provide the instruction for service detection and the potential enforcement actions to be applied for the detected service need to be defined.

It is proposed to use Application Identifier known both to PCRF and to TDF as a set of characteristics of the service, required for detection. An Application identifier can be mapped by the TDF to a pre provisioned service related information e.g. application layer protocol e.g. http, sip, P2P, and TCP/UDP port number / ranges to be detected.

NOTE 2: Application identifier communicated by the PCRF can be mapped to variety of information pre-provisioned into the TDF, that can allow for expansion of TDF role to be used with new protocols and services without having to standardize new parameters across the interface.

Two scenarios are addressed below:

- Solicited service reporting: The TDF is instructed on which services to detect, report to the PCRF and the actions to be enforced on a per IP-CAN session basis.
- Unsolicited service reporting: The TDF is pre-configured on which services to detect and report. The enforcement is done in the PCEF. It is assumed that user consent is not required.

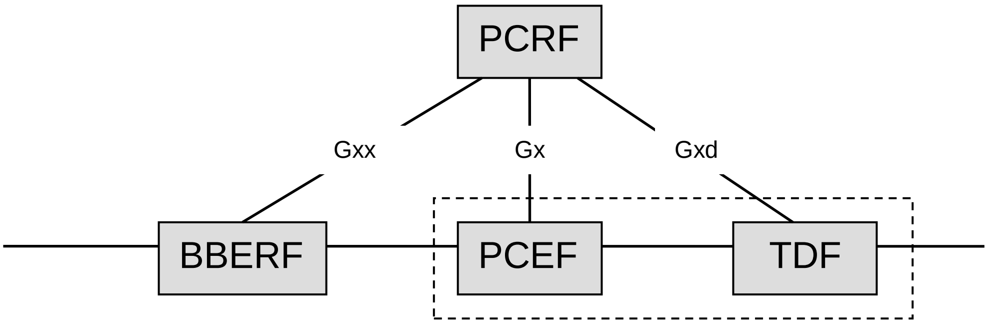


Figure 4.4.3.1-1: Architecture including TDF

NOTE 3: This architecture option can be applied for a stand-alone TDF and a TDF that is collocated with the PCEF in the same gateway.

In case of collocated TDF, the Gxd interface doesn't apply.

A new reference point Gxd between standalone TDF and PCRF that enables gating, shaping and redirection functions in the TDF is defined.

4.4.3.1.1 Reference Points

The Gxd reference point enables communication between TDF and PCRF for the purpose of:

- Reporting of the start and the stop of a detected services and transfer of service data flow descriptions for detected services from the TDF to the PCRF.
- Signalling of Service Detection and Policy Rules from the PCRF for the purpose of traffic detection and enforcement at the TDF to the PCRF. Functions are provided to establish a TDF session, to modify a TDF session from the PCRF and to terminate a TDF session.

4.4.3.1.2 Functional entities

The TDF performs service detection and reporting of detected service and its service data flow description to the PCRF.

For those cases where service data flow description is not possible to be provided by the TDF to the PCRF, the TDF performs gating, redirection and bandwidth limitation for the detected services. The existing PCEF/BBERF functionality remains as defined in TS 23.203 [3].

For those cases where service data flow description is provided by the TDF to the PCRF the actions resulting of service detection may be performed by the PCEF as part of the charging and policy enforcement per service data flow and by the BBERF for bearer binding as defined in TS 23.203 [3] or may be performed by the TDF as described above.

The PCEF may encompass the TDF functionality.

4.4.3.2 Solicited service detection reporting

To trigger the interaction with the PCRF, the start and the end of a detected service have to be added as new event triggers. The TDF notifies the PCRF when it detects the start or the end of a detected service, if detection event trigger is provisioned. After detecting a service, the TDF shall also apply the enforcement actions to the detected service, if they were provided by the corresponding PCC/SDPR rule. The TDF may also inform the PCRF via a Gx/Gxd interface, by providing an Identifier corresponding to the detected service (i.e. SD rule identifier), the service start event notification and the detected filter information, when available. The PCRF may then create/modify the PCC/SDPR rule in the desired way with regard to the policy and charging control information.

NOTE 1: Charging control applies to PCC rules only.

When the TDF detects the end of the service, it shall notify the PCRF, if subscribed, with the corresponding SD rule identifier and the service stop event trigger. This may trigger the PCRF to modify the PCC rule in the desired way with regard to the policy and charging control information..

The following enforcement actions may be applied by standalone TDF to the detected traffic:

a. Permit Unrestricted - the detected service/flow is allowed to continue without further policy action

b. Block - the detected service / application flows are blocked (or the "gate is closed")

c. Shape - apply some regime of traffic shaping to the detected service / application flows (e.g. to bandwidth limit for P2P file sharing flows)

d. Redirection - Redirect detected flows to another controlled address (e.g. redirect to a top-up / service provisioning page). This may not be possible for all types of detected flows (e.g. this may only be performed on specific HTTP based flows)

NOTE 2: Additional PCC functions (i.e. credit management, reporting, policy control, event reporting, binding mechanisms) besides those listed above are always performed by the PCEF as currently described in TS 23.203 [3].

In case the standalone TDF is involved in the communication and required to apply enforcement actions, it is PCRF's responsibility to coordinate the PCC rules and QoS rules, if applicable, with SDPR rules in order to ensure consistent service delivery.

NOTE 3: The following alignments may be done by PCRF in case the standalone TDF is involved in the communication:

1. Gate/redirection enforcement. There shall be no contradiction between PCC rules gate/redirection status and SDPR rules gate/redirection status. Note: This mean that, for example, when a P2P traffic has to be gated (blocked) at the TDF, the P2P traffic shall not get redirected at the PCEF, and traffic shall not get gated (blocked) at the PCEF but rather let through.

2. The uplink and downlink maximum bit rates for corresponding detected services shall not exceed the Authorized APN-AMBR, for the IP-CAN Session.

   The mechanisms covering the issue of charging interface, when standalone TDF is used, are out of this key issue's scope.

4.4.3.2.1 Specific functions description

In order to establish the session between PCRF and standalone TDF, the PCEF may send the IP address of the related standalone TDF to the PCRF in the request message upon the IP-CAN session establishment.

The PCRF may then establish user related session towards the TDF including the SDPR rules and event triggers, if required.

For roaming with home routed traffic, PCEF and TDF reside in the HPLMN, while only BBERF, if applicable, reside in the VPLMN. The S9 interface enables the H-PCRF to provide dynamic QoS control policies from the HPLMN, via a V-PCRF, to a BBERF in the VPLMN. The functionality is not affected by the introduction of Service Awareness and Privacy Policies, as all of the involved entities (H-PCRF, PCEF, TDF) reside in the same network (i.e. HPLMN) and S9 is not required to transfer any new parameters.

For Local Breakout (i.e. roaming with a visited access), V-PCRF, PCEF, TDF and BBERF, if applicable, reside in the VPLMN, while H-PCRF and SPR reside in the HPLMN. One of already defined S9 reference point functionalities in this case is to enable the H-PCRF (via the V-PCRF) to have dynamic PCC control, including both the PCEF and, if applicable, BBERF, in the VPLMN. In order to provide Service Awareness and Privacy Policies functionality, S9 is required additionally:

- To carry Application Identifier and service detection start/stop detected traffic event triggers report from V-PCRF to H-PCRF, informing on start and stop of service traffic detection.

NOTE: For local breakout, there may be situations where the TDF is not able to detect the traffic requested by the H-PCRF. Prior agreements could be arranged to ensure that there is a common understanding of the meaning of Application Identifiers transferred between PLMNs.

- In addition to the existing functionality, the V-PCRF provides functions to extract SDPR rules from PCC rules provided by the H-PCRF over the S9 reference point. The V-PCRF provides updated PCC rules to the PCEF and SDPR rules to the standalone TDF, if appropriate.

1.4.3.2.2 Signalling Flows

This clause contains signalling flows for:

- TDF session establishment and Activation of Service Detection and Policy Rules by the PCRF into the TDF based on user privacy rules at IP-CAN Session Establishment.

- 'Start of Service' detection notification at service start from the TDF to the PCRF.

- 'Stop of Service' detection notification at service stop from the TDF to the PCRF.

- Activation/deactivation/modification of PCC/SDPR Rules by the PCRF into the TDF.

NOTE: The external trigger does not have to be necessarily limited to SPR.

- TDF session termination and deactivation of Service Detection and Policy Rules by the PCRF into the TDF at IP-CAN Session termination.

4.4.3.2.2.1 Changes to IP-CAN session establishment

This clause includes the changes to IP-CAN session establishment signalling flow to provision of Service Detection and Policy Rules to the TDF, both for TDF collocated with the PCEF and for the standalone TDF.

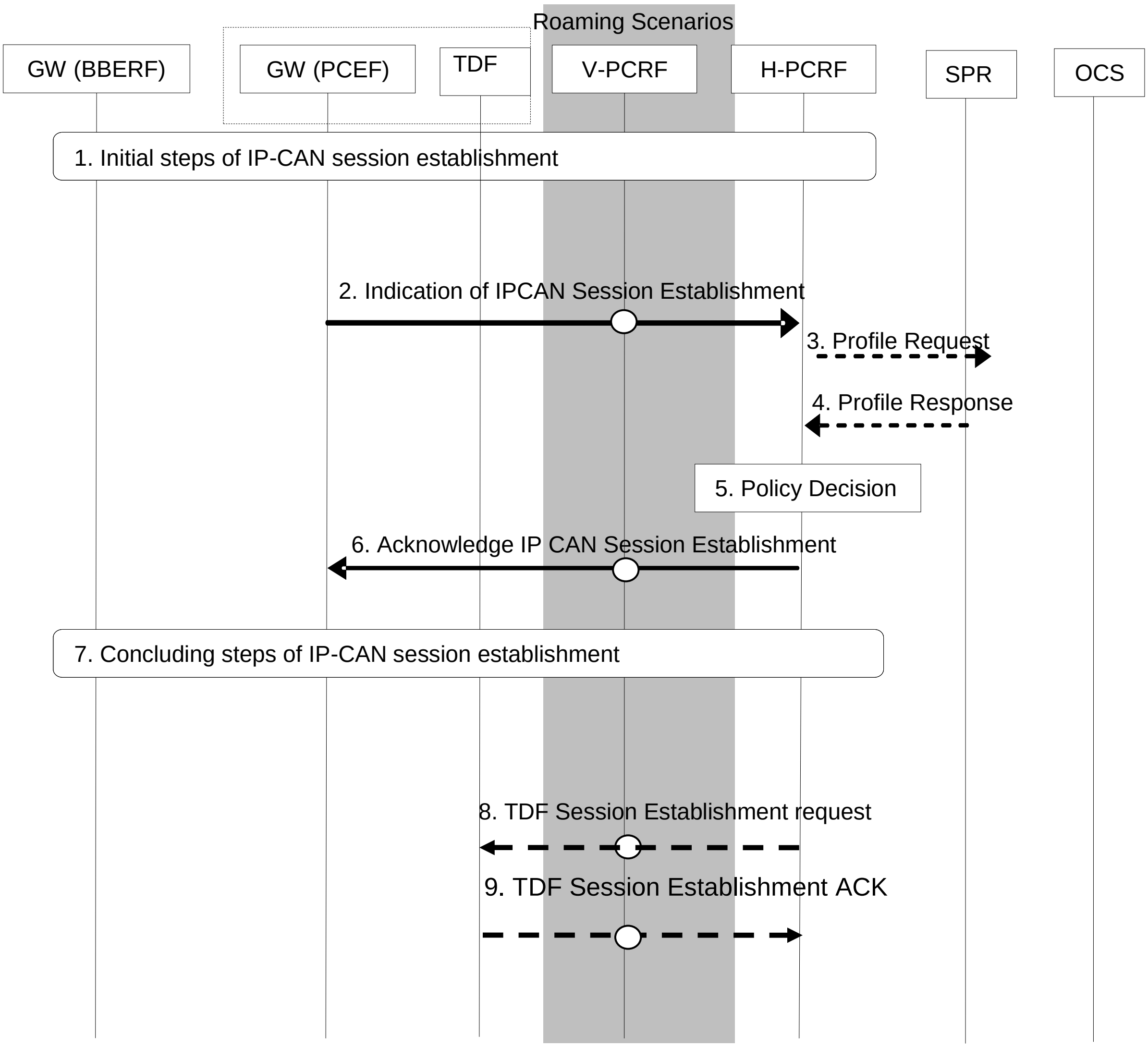

Roaming Scenarios
GW (BBERF)
GW (PCEF)
TDF
V-PCRF
H-PCRF
SPR
OCS
1. Initial steps of IP-CAN session establishment
2. Indication of IPCAN Session Establishment
3. Profile Request
4. Profile Response
5. Policy Decision
6. Acknowledge IP CAN Session Establishment
7. Concluding steps of IP-CAN session establishment
8. TDF Session Establishment request
9. TDF Session Establishment ACK

Figure4.4.3.2.2.1-1: Provisioning of Service Detection Rules to the TDF at IP-CAN session establishment

1. IP-CAN Session Establishment as specified in TS 23.203 [3] clause 7.2 steps 1 to 2.

2. The PCEF determines that the PCC authorization is required, requests the authorization of allowed service(s) and PCC Rules information as specified in TS 23.203 [3] step 3. The PCEF also includes information on whether the TDF is collocated with the PCEF or it is not and standalone TDF IP address, if applicable. The existing Supported Features mechanism (TS 29.212) may be applied by PCEF and TDF to indicate the detection feature support.

3. IP-CAN Session Establishment as specified in TS 23.203 [3] clause 7.2 step 4.

4. IP-CAN Session Establishment as specified in TS 23.203 [3] clause 7.2 step 5, including user privacy policies.

5. IP-CAN Session Establishment as specified in TS 23.203 [3] clause 7.2 step 6.

6. The PCRF sends a decision as specified in TS 23.203 [3] step 7. If the TDF is collocated with the PCEF, PCRF checks user privacy policies to traffic detection mechanisms. If user's privacy policies as indicated by the profile, allow for the use of service traffic detection, the PCRF also sends the PCC rules for the service detection and enforcement to the PCEF and may include subscription to the service detection start /stop event trigger. The PCEF provisions the detection requirements to the TDF.

7. IP-CAN Session Establishment as specified in TS 23.203 [3] clause 7.2 steps 8 to 12.

8. If the TDF is standalone, steps 8 and-9 take place. If user's privacy policies as indicated by the profile, allow for the use of service traffic detection, the PCRF requests the identified TDF to establish the relevant session

towards PCRF and provides Service Detection and Policy Rules to the TDF and may subscribe to the service detection start and service detection stop event triggers.

9. The TDF acknowledges the request and may indicate policy enforcement actions support in case some of the enforcement actions required by PCRF are not supported.

NOTE: Steps 8-9 can occur immediately after step 2.

4.4.3.2.2.2 Service Detection notification

This clause describes the provisioning of service information from the TDF at the start of a service detected by the TDF for both standalone TDF and collocated TDF.

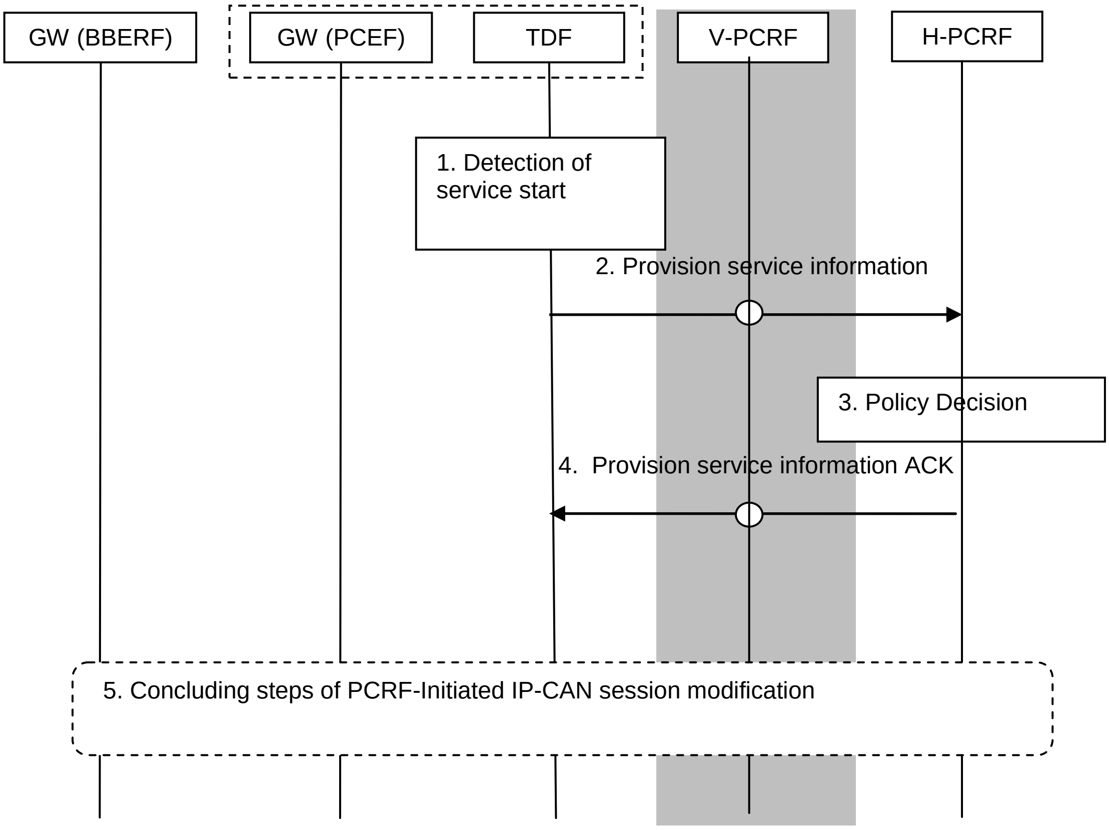

GW (BBERF)
GW (PCEF)
TDF
V-PCRF
H-PCRF
1. Detection of service start
2. Provision service information
3. Policy Decision
4. Provision service information ACK
5. Concluding steps of PCRF-Initiated IP-CAN session modification

Figure4.4.3.2.2.2-1: Provisioning of service information from the TDF

1. The standalone or collocated TDF detects the start of a service flow that matches with one of the activated PCC/SDPR Rules. Then, in case the enforcement actions were provided as a part of SDPR rules, TDF shall apply those actions.

NOTE 1: the detection procedure is out of the scope of this study.

2. If the service start event trigger request was received, the TDF shall provide service information to the PCRF, including the SD Rule Identifier, service detection start event trigger and the flow descriptions, if available.

NOTE 2: In case of collocated TDF, the information is provided by TDF through PCEF-PCRF communication. The interface between TDF and PCEF is out of scope.

3. Upon receiving the notification, PCRF may modify the PCC/SDPR rule (and the QoS Rules if they are applicable), based on the received flow descriptions and operator local policies for the detected service, otherwise step 5 is not applicable.

4. If step 2) was initiated by the standalone TDF, then the PCRF sends acknowledge to the TDF.

5. The PCRF-Initiated session modification take place as per TS 23.203 [3] clause 7.4.2 steps 4-11.

4.4.3.2.2.3 Notification for stop of service from the TDF

This clause describes the reporting of the stop of a service detected by the TDF both for standalone TDF and for collocated TDF.

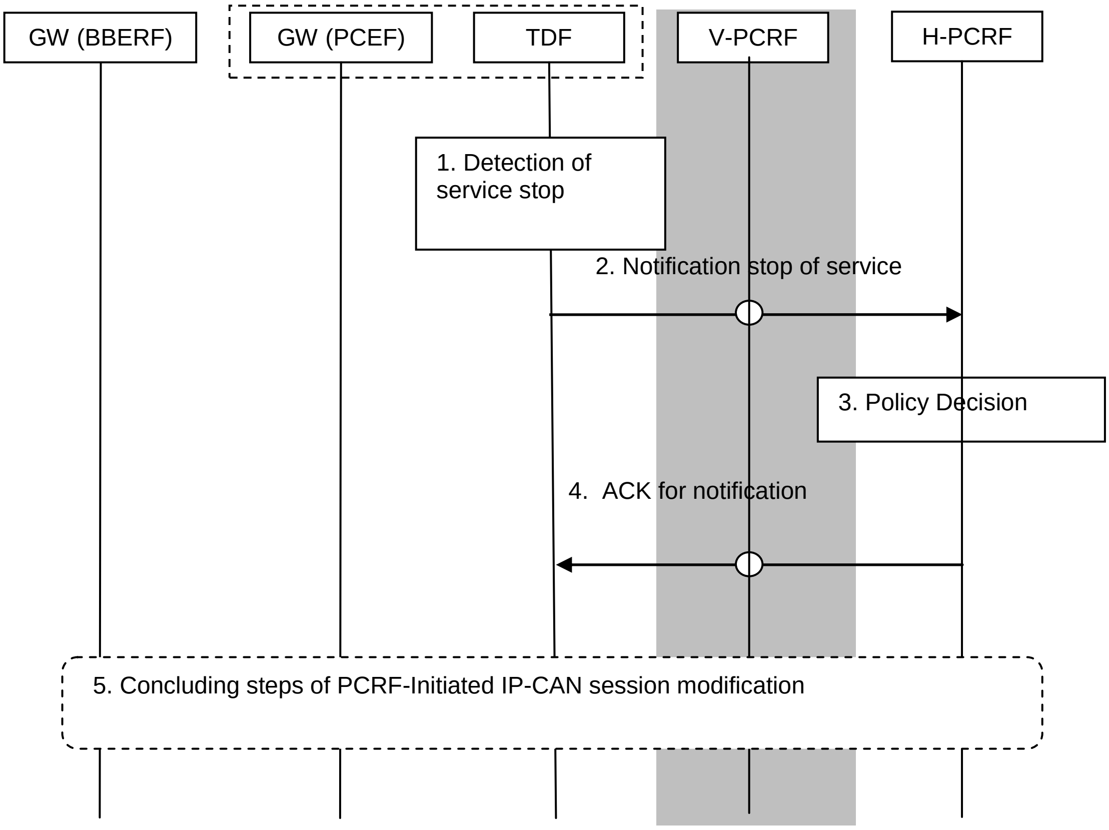

GW (BBERF)
GW (PCEF)
TDF
V-PCRF
H-PCRF
1. Detection of service stop
2. Notification stop of service
3. Policy Decision
4. ACK for notification
5. Concluding steps of PCRF-Initiated IP-CAN session modification

Figure4.4.3.2.2.3-1: Notification for stop of service from the TDF

1. The standalone or collocated TDF detects the stop of a service flow that matches with one of the activated PCC/SDPR Rules.
2. If the service stop event trigger was subscribed to, the TDF shall send stop of service event trigger to the PCRF. The notification shall include the SDPR Rule Identifier and service detection stop event trigger. It may also include filters associated with the reported service.

NOTE: In case of collocated TDF, the information is provided by TDF through PCEF-PCRF communication. The interface between TDF and PCEF is out of scope.

3. Upon receiving the notification, the PCRF may modify the PCC/SDPR rule (and the QoS Rules if they are applicable), as a result of service detection stop. Then, the step 5 is applicable.
4. If step 2) was initiated by a standalone TDF, then the PCRF sends acknowledge to the TDF.
5. The PCRF-Initiated session modification take place as per TS 23.203 [3] clause 7.4.2 steps 4-11.

4.4.3.2.2.4 Activation/deactivation of PCC/SDPR Rules in the TDF

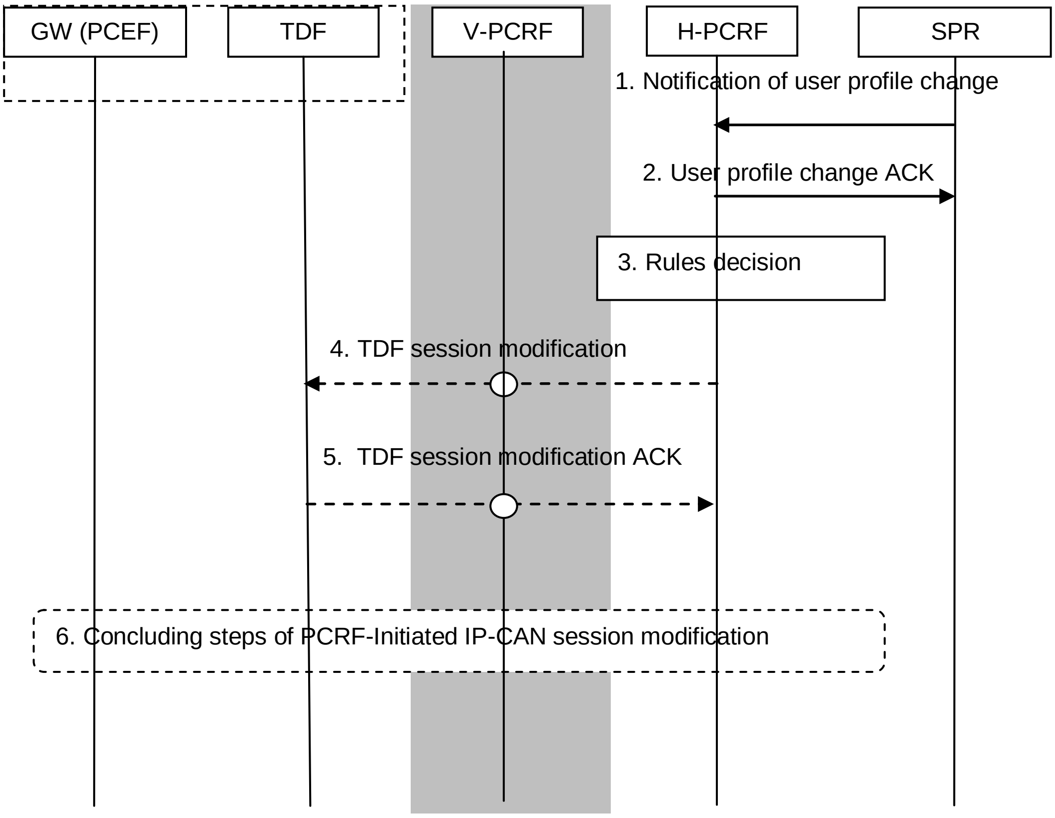

GW (PCEF)
TDF
V-PCRF
H-PCRF
SPR
1. Notification of user profile change
2. User profile change ACK
3. Rules decision
4. TDF session modification
5. TDF session modification ACK
6. Concluding steps of PCRF-Initiated IP-CAN session modification

Figure4.4.3.2.2.4-1: Provisioning/Removal of Service Detection and Policy Rules in the TDF

1. The PCRF is notified that the user profile has changed (e.g. by receiving the appropriate request from SPR).

2. The PCRF acknowledges the user profile change to SPR.

3. PCRF decides on PCC/SDPR rules change.

NOTE: A change of SDPR rules may also happen as a result of internal PCRF logic execution; in such a case steps 1-2 are not required.

If the TDF is standalone:

4. PCRF activates/deactivates/modifies the SDPR rules in the TDF.

5. TDF acknowledges the SDPR rules' activation/deactivation/modification.

If the TDF is collocated with the PCEF, then steps 4 and 5 are omitted and:

6. PCRF provisions PCC Rules to the TDF by applying PCRF-Initiated IP-CAN session modification procedure per TS 23.203 [3] clause 7.4.2 step 5 to 11.

4.4.3.2.2.5 Changes to IP-CAN session termination

This clause includes the changes to IP-CAN session termination to deactivate SDPR Rules at the TDF.

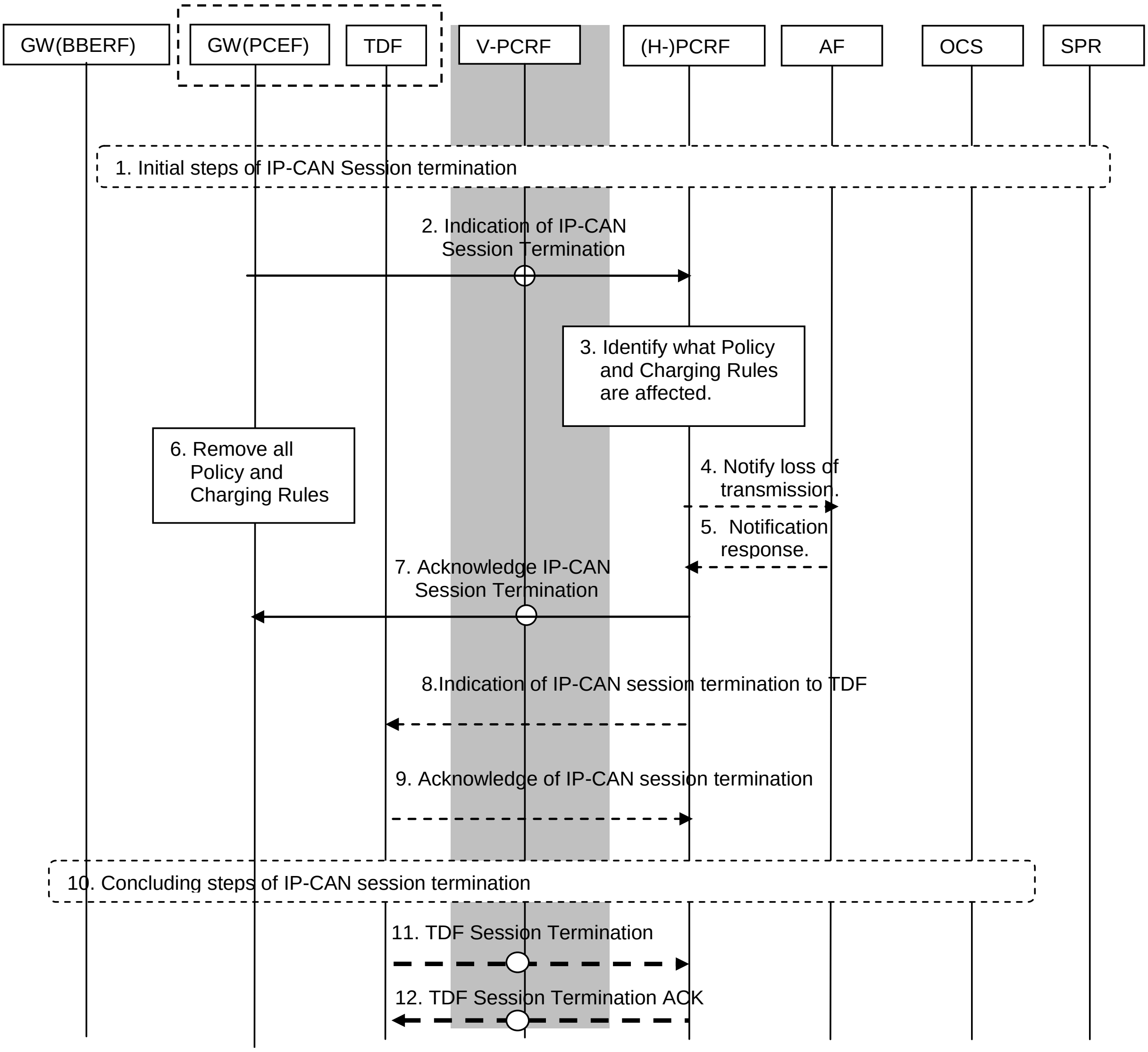

GW(BBERF)
GW(PCEF)
TDF
V-PCRF
(H-)PCRF
AF
OCS
SPR
1. Initial steps of IP-CAN Session termination
2. Indication of IP-CAN Session Termination
3. Identify what Policy and Charging Rules are affected.
6. Remove all Policy and Charging Rules
4. Notify loss of transmission.
5. Notification response.
7. Acknowledge IP-CAN Session Termination
8.Indication of IP-CAN session termination to TDF
9. Acknowledge of IP-CAN session termination
10. Concluding steps of IP-CAN session termination
11. TDF Session Termination
12. TDF Session Termination ACK

Figure4.4.3.2.2.5-1: Removal of Service Detection Rules from the TDF at IP-CAN session termination

1. IP-CAN Session Termination initial steps as specified in TS 23.203 [3] clause 7.3.1, steps 1- 2 or clause 7.3.2, steps 1-4.

2. The GW (PCEF) indicates that the IP-CAN Session is being removed and provides relevant information to the PCRF.

3. The PCRF finds the PCC Rules that require an AF to be notified and removes PCC Rules for the IP-CAN session.

4. The PCRF notifies the AF that there are no transmission resources for the service if this is requested by the AF.

5. The AF acknowledges the notification of the loss of transmission resources.

6. The GW (PCEF) removes all PCC Rules associated with the IP-CAN session.

7. The PCRF removes the information related to the terminated IP-CAN Session (subscription information etc.), and acknowledges the IP-CAN Session termination.

8. If the TDF is standalone, then steps 8-9 take place. The PCRF informs TDF about IP-CAN session termination.

9. TDF deactivates all SDPR Rules associated with the IP-CAN session and acknowledges the termination request from the PCRF.

10. IP-CAN Session Termination concluding steps takes place as specified in TS 23.203 [3] clause 7.3.1, steps 9-14 or clause 7.3.2, steps 11-15.

11. TDF terminates the session with the PCRF.

12. PCRF acknowledges the TDF session termination.

4.4.3.3 Unsolicited service detection reporting

4.4.3.3.1 Signalling Flows

This clause contains signalling flows for those cases where the TDF role is service detection and reporting to the PCRF.

- Provisioning of service information at service start/modification from the TDF.

- Revoke service session information at service stop from the TDF.

4.4.3.3.1.1 Provision service information from the TDF

This clause describes the provisioning of service information from the TDF at the start or modification of a service detected by the TDF. The TDF performs service detection and reporting functions only.

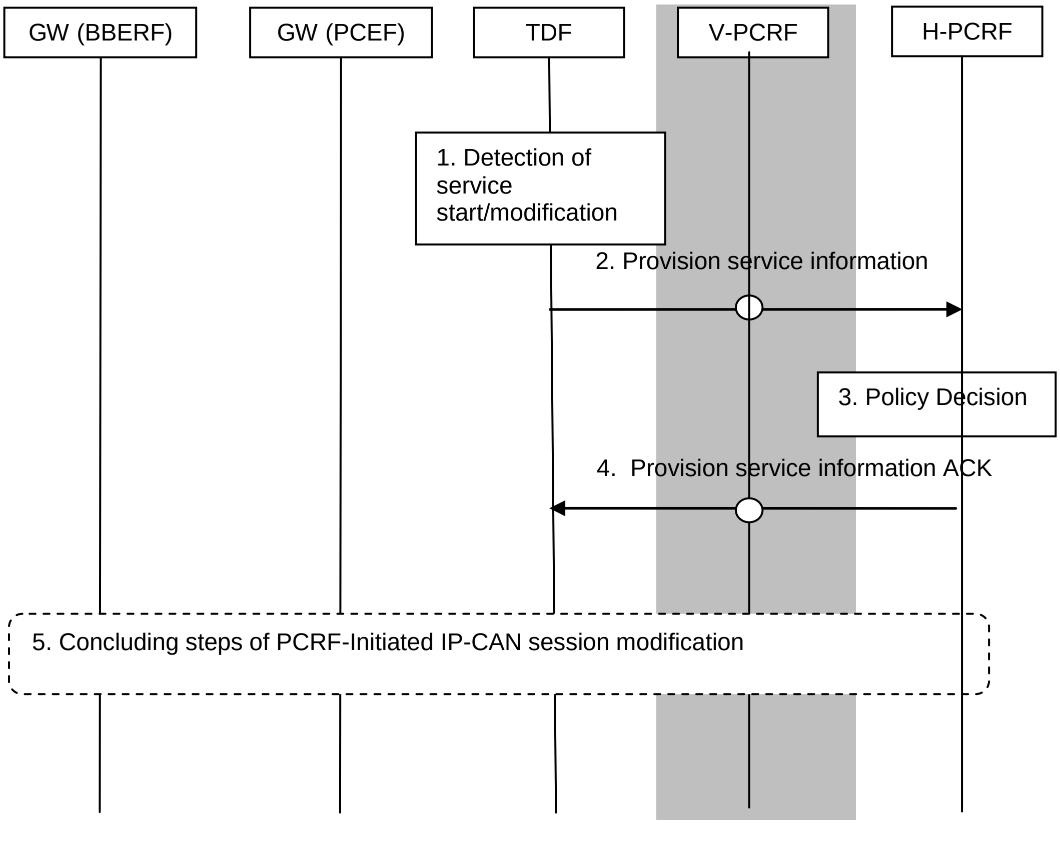

GW (BBERF)
GW (PCEF)
TDF
V-PCRF
H-PCRF
1. Detection of service start/modification
2. Provision service information
3. Policy Decision
4. Provision service information ACK
5. Concluding steps of PCRF-Initiated IP-CAN session modification

Figure4.4.3.3.1.1-1: Provisioning of service information from the TDF

1. The TDF detects the start or the modification of a service flow that matches with one of the SD Rules installed in the TDF, enforces the service control for the detected service..

NOTE 1: The detection procedure is out of the scope of this study.

2. The TDF provide service information to the PCRF, the TDF includes the application identifier and if available the flow descriptions.

3. If operator policies indicates that PCC/QoS Rules shall be provisioned then the PCRF generates PCC Rules (and the QoS Rules if they are applicable) based on the received flow descriptions and operator local policies for the detected service, otherwise step 5 is not applicable.

4. The PCRF sends a confirmation to the TDF.

5. The PCRF- Initiated IP-CAN session modification takes place as per TS 23.203 [3] clause 7.4.2 steps 4-11.

NOTE 2: Step 4 may take place at anytime after step 3.

4.4.3.3.1.2 Revoking service information from the TDF

This clause describes the reporting of the stop of a service detected by the TDF. The TDF performs service detection functions only.

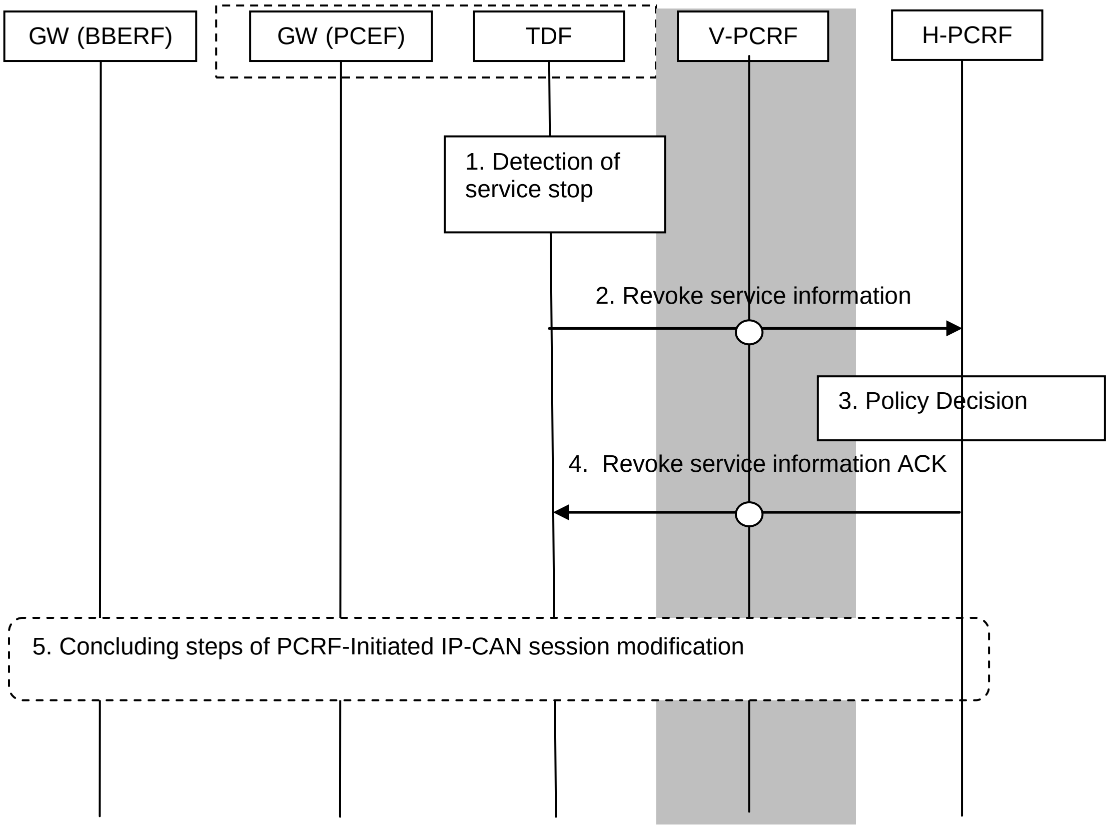

GW (BBERF)
GW (PCEF)
TDF
V-PCRF
H-PCRF
1. Detection of service stop
2. Revoke service information
3. Policy Decision
4. Revoke service information ACK
5. Concluding steps of PCRF-Initiated IP-CAN session modification

Figure4.4.3.3.1.2-1: Revoke service information to the PCRF

1. The TDF detects the stop of a service flow that matches with one of the SD Rules installed in the TDF.

NOTE: The detection procedure is out of the scope of this study.

2. The TDF revokes service information to the PCRF.

3. If PCC Rules are installed in the PCEF steps 5 applies.

4. The PCRF sends a confirmation to the TDF.

5. The PCRF- Initiated IP-CAN session modification takes place as per TS 23.203 [3] clause 7.4.2 steps 4-11

NOTE 2: Step 4 may take place at anytime after step 3.

4.4.3.4 Service Detection and Policy rules definition and structure

This clause is relevant only in the case of standalone TDF.

4.4.3.4.1 General

The Service Detection and Policy rule (SDPR rule) comprises the information that is required in order to apply the detection and enforcement actions for the specified service traffic.

Two different types of SDPR rules exist: dynamic rules and predefined rules. The dynamic SDPR rules are provisioned by the PCRF via the Gxd reference point, while the predefined SDPR rules are directly provisioned into the TDF and only referenced by the PCRF. The pre-defined SDPR rules may be used in a non-roaming situation.

NOTE 1: The procedure for provisioning predefined SDPR rules is out of scope.

There are defined procedures for activation, modification and deactivation of SDPR rules (as described in clause 4.4.2.3.2.2). The PCRF may activate, modify and deactivate a SDPR rule at any time, over the Gxd reference point. The modification procedure is applicable to dynamic SDPR rules only.

Upon detecting end of service traffic for the corresponding SDPR rule, the TDF shall notify the PCRF, if originally controlled by the PCRF, of the end of service traffic.

The operator defines the SDPR rules.

The following table lists the information contained in a SDPR rule, including the information element name, the description and whether the PCRF may modify this information in a dynamic SDPR rule which is active in the TDF. The Category field indicates if a certain piece of information is mandatory or not for the construction of a SDPR rule, i.e. if it is possible to construct a SDPR rule without it.

Table 4.4.3.4.1-1

Information name	Description	Category	PCRF permitted to modify for a dynamic SDPR rule in the TDF
SDPR Rule identifier	Uniquely identifies the SDPR rule, within an IP-CAN session. It is used between PCRF and standalone TDF for referencing SDPR rules.	Mandatory	No
Application identifier	References the corresponding application (i.e. service), for which the rule applies.	Mandatory	No
Enforcement control	Defines how the standalone TDF shall apply enforcement actions for the detected service traffic.		
Gate status	The gate status indicates whether the service data flow, detected by the service data flow template, may pass (Gate is open) or shall be discarded (Gate is closed) at the TDF.		Yes
UL-maximum bitrate	The uplink maximum bitrate authorized for the service traffic		Yes
DL-maximum bitrate	The downlink maximum bitrate authorized for the service traffic		Yes
Redirect	Redirect detected service traffic to another controlled address		Yes

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

The *Application identifier* references the corresponding application (i.e. service), for which the rule applies.

The *Gate status* indicates whether the TDF shall let a service traffic matching the Application identifier, pass through (gate is open) the TDF or the TDF shall discard (gate is closed) the service traffic.

The *UL maximum-bitrate* indicates the authorized maximum bitrate for the uplink component of the detected service traffic.

The *DL maximum-bitrate* indicates the authorized maximum bitrate for the downlink component of the detected service traffic.

The *Redirect* indicates whether the detected service traffic should be redirected to another controlled address. The target redirect address is included also.

4.4.3.4.2 Service Detection and Policy rule relevant operations

Service Detection and Policy rule operations consist of activation, modification and de-activation of SDPR rules.

Activation of a dynamic SDPR rule: The PCRF provides the SDPR rule information to the TDF via the Gxd reference point.

Activation of a predefined SDPR rule: The PCRF provides an identifier of the relevant SDPR rule to the TDF via the Gxd reference point.

An active SDPR rule means that the service traffic, matching the corresponding application (i.e. service), is detected and enforced as per enforcement control actions, if defined within the SDPR rule.

The PCRF may, at any time, modify an active, dynamic SDPR rule.

The PCRF may, at any time, deactivate an active SDPR rule in the TDF via the Gxd reference point. At IP-CAN session termination all active SDPR rules are deactivated upon information, received from the PCRF about IP-CAN session termination.

Upon detecting end of service traffic for the application (i.e. service), TDF shall deactivate the corresponding SDPR rule.

4.4.3.4.3 PCC rules modifications

The following additional fields should be added to PCC rules' structure in order to support service awareness functionality:

- The *Application identifier* references the corresponding application (i.e. service), for which the rule applies.
- The *Redirect* indicates whether the detected service traffic should be redirected to another controlled address. The target redirect address is included also.

Additionally, Event triggers of start and stop of detected traffic should be added.

4.4.4 Conclusion

The general AF, as part of the PCC architecture defined in TS 23.203 [3], shall not be enhanced to support enforcement functionality assigned to the PCEF, according to TS 23.203 [3], for the purpose of service detection / this key issue. As a consequence the Rx reference shall not be enhanced to carry QoS enforcement information.

Both solicited and unsolicited service detection reporting scenarios as described in key issue 4 are valid. Whether the one or other is chosen depends on the actual network deployment. Therefore, it is proposed to cover both of them in the normative standardization.

4.5 Key issue 5: Service Based Traffic Steering

4.5.1 Description

In a service aware network it is possible to optimally route the traffic. For IP services that get identified using service traffic detection mechanism it may only be possible after the session has been established and the some traffic has already traversed the network. In order to improve service experience it should be possible to steer traffic after its establishment for example from a Home PDN Gateway to a local breakout.

Editor's Note: Further changes can be done to this key issue description based on SA WG1 feedback.

4.5.2 Conclusion

No viable solution was presented to resolve this issue during the period of the study. The issue is therefore being closed.

4.6 Key issue 6: Extending Policy Architecture to handle transactional services

4.6.1 Description

Current 3GPP PCC architecture usage is designed around the handling of IP flows. Many current / legacy (e.g. SMS) and future services (e.g. video rental) are however of transactional nature. In many scenarios it can be beneficial if there is a standardized mechanism for handling policies for such services via the PCC. For transactional services while the PCRF will authorize requests for such services, the service logic and enforcement of PCRF authorized decisions will continue to reside within the service.

Editor's note: The extent of such interaction and enforcement are subject to 3GPP scope and FFS.

4.6.2 Alternative solutions

4.6.2.1 Alternative 1 - Use Rx to authorize transactional services

4.6.2.1.1 General

The AF acting as Charging Trigger Function, as described in TS 32.229 [x], performs a check balance request for the transactional service using the Ro Interface. If successful the AF can then proceed to authorize the user to receive the service using Rx.

Video download is an example of a transactional service that is addressed in this alternative solution.

The PCRF can be used to authorize the user to receive a service based on network and user preferences (e.g. user has or does not have the priority/subscription to receive the service in the current location) that are available at the PCRF.

The PCRF plays the role of an authorization server that takes into account at least the user profile (stored in the SPR/UDR), the network information (received from the PCEF/BBERF).

A successful authorization will trigger installation of PCC/QoS Rules as normal PCC procedures defined in TS 23.203 [3]

4.6.2.1.2 Architecture

A possible architecture for transactional services is shown in Figure 4.6.2.1.2-1 in the non roaming case. In the roaming case a S9 reference point is present between the H-PCRF and the V-PCRF.

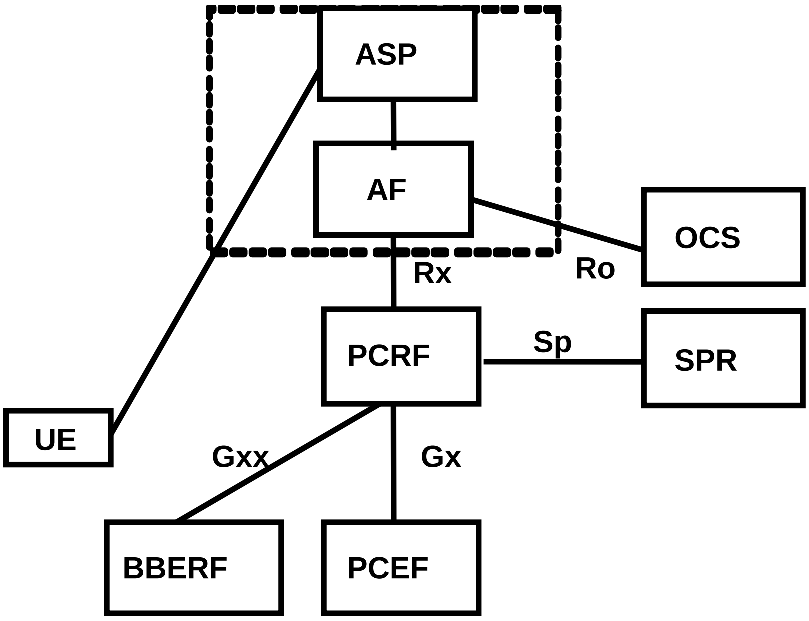


Figure4.6.2.1.2-1: Architecture for transactional services

The ASP receives application level signalling from a UE that request a transactional service, in this example, to download a video.

The AF receives user authorization requests from the ASP, an AF may receive user authorization request from multiple ASPs.

NOTE: The AF is assumed to be part of the operator's domain.

The AF communicates with the OCS over Ro using existing procedures to check the balance for the requested service.

If credit balance check is successful the AF requests PCRF authorization over Rx using existing procedures and subscribes to notifications of successful and unsuccessful resource reservation.

The PCRF authorizes the user to receive the service based on network and user preferences that are stored in the SPR/UDR,

If the service is authorized a successful response is returned over Rx interface to the ASP via the AF and PCC/QoS Rules are installed in the PCEF/BBERF. If the service is not authorized an unsuccessful response is returned over Rx interface to the ASP via the AF.

If there is enough credit, the service is authorized and the underlying resources are established, the AF responds that there are service can be successful delivery to the user.

4.6.2.1.3 Reference points

4.6.2.1.3.1 AF - PCRF reference point (Rx)

The Rx reference point between the AF and the PCRF is described in TS 23.203 [3]. The Rx reference point enables transport of application level session information from AF to PCRF.

4.6.2.1.3.2 AF - OCS reference point (Ro)

The Ro reference point between the AF and the OCS is described in TS 32.299 [8]. The Ro reference point enables the AF (acting as a Charging Trigger Function) to perform a check balance request for the transactional service.

4.6.2.1.4 PCC Information Flows

This clause includes PCC information flows to authorize a user to receive a transactional service, including installation of PCC/QoS Rule for the transactional service and to remove PCC/QoS Rules when the user has received the service.

4.6.2.1.4.1 Authorization of a user to receive a transactional service

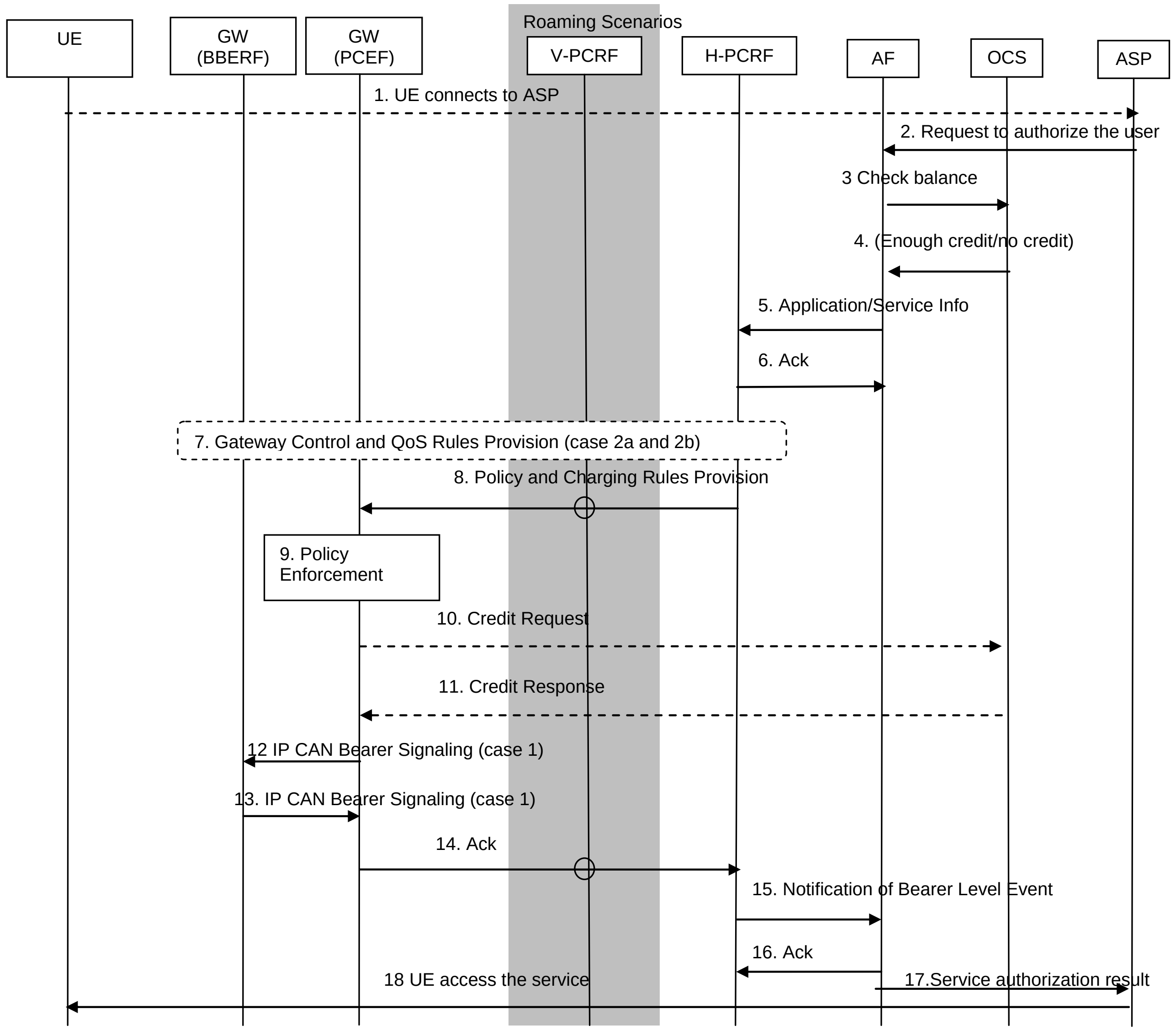

Roaming Scenarios
UE
GW (BBERF)
GW (PCEF)
V-PCRF
H-PCRF
AF
OCS
ASP
1. UE connects to ASP
2. Request to authorize the user
3 Check balance
4. (Enough credit/no credit)
5. Application/Service Info
6. Ack
7. Gateway Control and QoS Rules Provision (case 2a and 2b)
8. Policy and Charging Rules Provision
9. Policy Enforcement
10. Credit Request
11. Credit Response
12 IP CAN Bearer Signaling (case 1)
13. IP CAN Bearer Signaling (case 1)
14. Ack
15. Notification of Bearer Level Event
16. Ack
18 UE access the service
17.Service authorization result

Figure 4.6.2.1.4.1-1: User authorization to receive the service

1. The UE connects to the ASP server and requests transactional services, in this example to download a video from the ASP.

2. Triggered by step 2 or alternatively by the ASP deciding to deliver the service to the user (assuming that the UE location is known), the ASP server decides to check if the user is authorized to receive the service.

3. The AF performs a check balance request using the Ro as described in RFC4006 and TS 32.299 [8]

4. The OCS sends a response on whether there is enough credit.

5. If there is enough credit the AF establishes an Rx session toward the PCRF as described in TS 23.203 [3] and provides the user identity (IMSI, MSISDN or UE IP address), the service identifier for the transactional service and the service information including the Flow Descriptions. Furthermore the AF subscribes to the notification to the AF related bearer level events (transmission resources are established/released/lost)

6. The PCRF checks if the user is allowed to receive the service, taking into account the user profile (e.g. gold/silver/bronze) in the SPR (UDR), the user context (e.g. user location).. If the user is not authorized to receive the service in step 7 the PCRF sends a response to the AF that the service is not authorized steps 7 to 18 does not take place.

7. If there is a need to provision QoS rules, the PCRF initiates a Gateway Control and QoS Rules Provision Procedure to request resources for a transactional service and may subscribe to notification of resource reservation as described in TS 23.203 [3].
8. The PCRF sends the Policy and Charging Rules Provision (PCC Rules, Event Trigger) to the PCEF and may subscribes to notification of resources reservation (successful or unsuccessful)
9. The PCEF enforces the decision.
10. If online charging is applicable, the PCEF may request credit for new charging keys from and/or shall return the remaining credit for charging keys no longer active to the OCS.
11. If OCS was involved, the OCS provides the credit information to the PCEF, and/or acknowledges the credit report
12. Triggered by the installation of PCC Rules, the PCEF sends an IP-CAN Bearer establishment request for the GTP case.
13. The GW (PCEF) receives the response for the IP-CAN Bearer establishment request for the GTP case to confirm if the resources are available for service delivery.
14. The PCEF sends Acknowledge Policy and Charging Rules Provisioning (accept or reject of the PCC rule operation(s)) to the PCRF.
15. Triggered by the response from the PCEF the PCRF notifies the AF related bearer level events (transmission resources are established or released).
16. The AF acknowledges the notification from the PCRF.
17. As there is enough credit, the service is authorized and the underlying resources are established, the AF responds that there are service can be successful delivery to the user.
18. The UE receives the desired service from the ASP.

4.1.2.1.2.4 Termination of the authorization of the user to receive the service

When the user has received the service the ASP will request the AF to terminate the Rx session, as specified in TS 23.203 [3].

4.6.3 Comparison of alternatives

4.6.4 Conclusion

Alternative 1 enables the PCRF to perform user authorization to access the service for a transactional service.

The Ro interface is used to perform a check balance request for the transactional service as per RFC 4006 and TS 32.299 [x].

The Rx interface is used to request the PCRF to perform user authorization for a transactional service according to user profile and user context.

Based on this evaluation no impacts on normative work are expected.

Annex A:
Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2011-06	SP-52	SP-100355	-	-	MCC editorial update for presentation to TSG SA for approval	0.6.0	1.0.0
2011-06	SP-52	-	-	-	MCC update to version 11.0.0 after TSG SA approval	1.0.0	11.0.0