ETSI TS 129 213 V8.1.1 (2008-11)

Technical Specification

**Digital cellular telecommunications system (Phase 2+);
Universal Mobile Telecommunications System (UMTS);
Policy and charging control signalling flows and Quality of Service (QoS) parameter mapping
(3GPP TS 29.213 version 8.1.1 Release 8)**

Reference

RTS/TSGC-0329213v811

Keywords

GSM, UMTS

ETSI

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

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

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Intellectual Property Rights

Foreword

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

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

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

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.

1 Scope

The present specification adds detailed flows of Policy and Charging Control (PCC) over the Rx , Gx, Gxx and S9 reference points and their relationship with the bearer level signalling flows over the Gn interface.

The calls flows depicted in this Technical Specification represent usual cases, i.e. not all situations are covered. Detailed information provided in TS 29.212 [9], TS 29.214 [10] , and TS 29.215 [22] shall be taken into consideration.

The present specification also describes the binding and the mapping of QoS parameters among SDP, UMTS QoS parameters, and QoS authorization parameters.

The present specification also describes the PCRF addressing using DRA.

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 and/or edition number or version number) 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 TS 23.203: "Policy Control and charging architecture".

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

[4] 3GPP TS 23.107: "Quality of Service (QoS) concept and architecture".

[5] 3GPP TS 24.229: "IP Multimedia Call Control Protocol based on SIP and SDP; Stage 3".

[6] 3GPP TS 26.234: "End-to-end transparent streaming service; Protocols and codecs".

[7] 3GPP TS 26.236: "Packet switched conversational multimedia applications; Transport protocols".

[8] 3GPP TS 29.207, version 6.5.0: "Policy control over Go interface".

[9] 3GPP TS 29.212: " Policy and Charging Control over Gx reference point".

[10] 3GPP TS 29.214: "Policy and Charging Control over Rx reference point".

[11] IETF RFC 2327: "SDP: Session Description Protocol".

[12] IETF RFC 3264: "An Offer/Answer model with the Session Description Protocol (SDP)".

[13] IETF RFC 3556: "Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth".

[14] IETF RFC 3588: "Diameter Base Protocol".

[15] draft-ietf-mmusic-ice-18 (September 2007): "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[16] IETF RFC 4145: "TCP-Based Media Transport in the Session Description Protocol (SDP)".

[17] IETF RFC 4975: "The Message Session Relay Protocol (MSRP)".

[18] 3GPP2 C.S0046: "3G Multimedia Streaming Services".

[19] 3GPP2 C.S0055: "Packet Switched Video Telephony Services (PSVT/MCS)".

[20] Void

[21] 3GPP TS 23.402: "Architecture Enhancements for non-3GPP accesses".

[22] 3GPP TS 29.215: " Policy and Charging Control over S9 reference point".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply:

Example: example

3.2 Abbreviations

For the purpose of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply:

AF Application Function
DRA Diameter Routing Agent
PCC Policy and Charging Control
PCEF Policy and Charging Enforcement Function
PCRF Policy and Charging Rule Function

4 Signalling Flows over Gx, Gxx, Rx and S9

4.0 General

There are three distinct network scenarios for an IP-CAN Session:

Case 1. No Gateway Control Session is required, no Gateway Control Establishment occurs at all (e.g. 3GPP Access where GTP-based S5/S8 are employed.

Case 2. A Gateway Control Session is required. There are two subcases:

2a) The BBERF assigns a Care of Address (CoA) to the UE and establishes a Gateway Control Session prior to any IP-CAN session establishment that will apply for all IP-CAN sessions using that CoA.

2b) A Gateway Control Session is required before the PCEF has announced the IP-CAN Session to the PCRF. Each IP-CAN session is handled in a separate Gateway Control Session.

The following considerations shall be taken into account when interpreting the signalling flows:

- V-PCRF is included to also cover the roaming scenarios.
- H-PCRF will act as a PCRF for non-roaming UEs.
- The steps numbered as “number+letter” (e.g. “3a”) will be executed, for the roaming case, instead of steps numbered as “number” (e.g. “3”), as indicated in the explanatory text below the signalling flows.

4.1 IP-CAN Session Establishment

This clause is applicable if a new IP-CAN Session is being established.

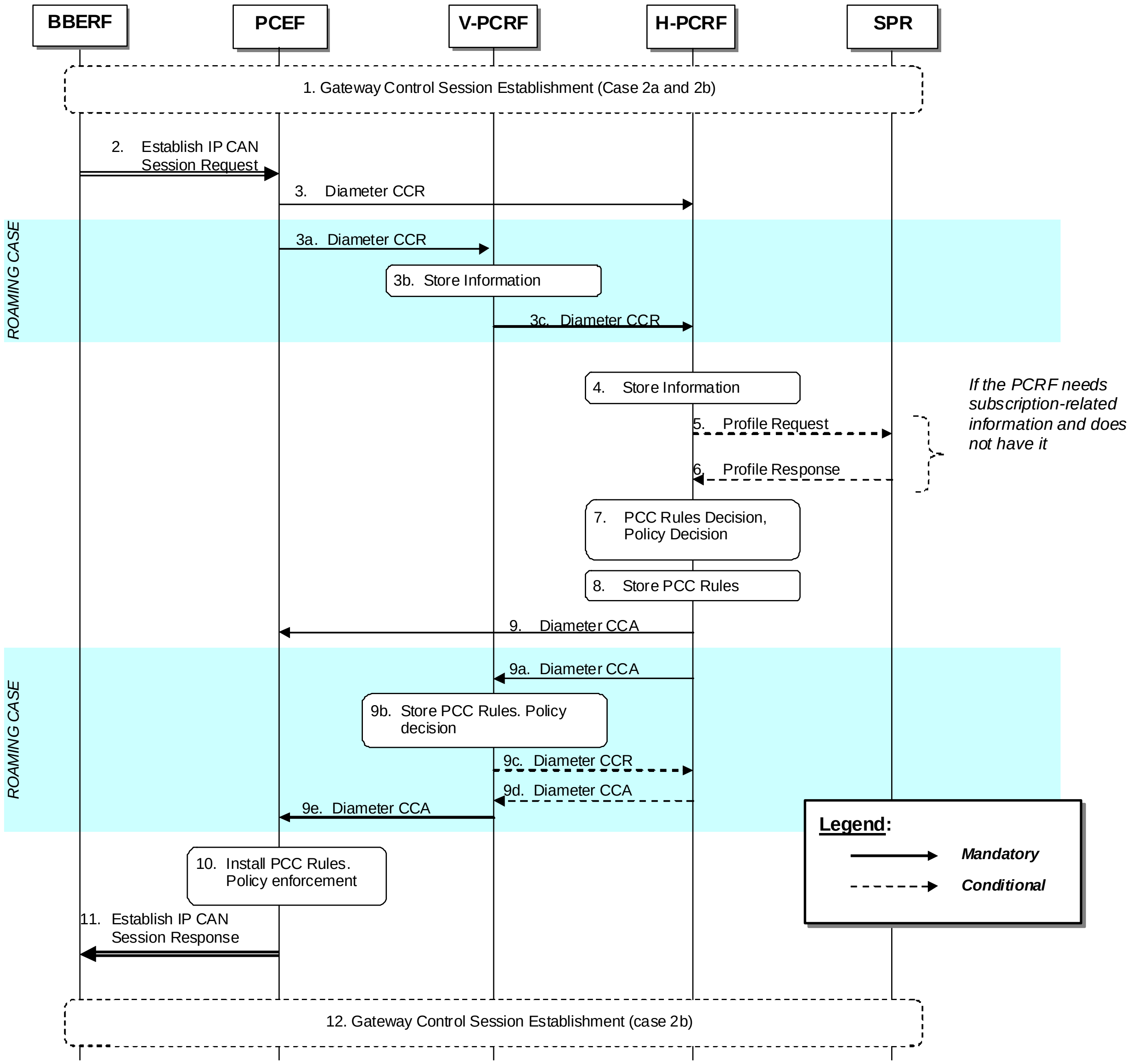


Figure 4.1.1: IP-CAN Session Establishment

1. The BBERF may initiate a Gateway Control Session Establishment procedure as defined in 4.4.1 (applicable for case 2a and 2b, as defined in clause 4.1), if appropriate.
2. The PCEF receives an Establish IP-CAN Session Request. The form of the Establish IP-CAN Session Request depends upon the type of the IP-CAN. For GPRS, the GGSN receives the first Create PDP Context Request within an IP-CAN session. For I-WLAN, the GW receives an IPSec tunnel establishment request.

NOTE 1: After this step, UE has been assigned an IP address, as described, for example, in 23.060 [3].

3. The PCEF informs the H-PCRF of the establishment of the IP-CAN Session. The PCEF starts a new DCC session by sending a CCR using the CC-Request-Type AVP set to the value INITIAL_REQUEST. The PCEF provides UE identity information , PDN identifier, the UE IPv4 address and/or UE IPv6 address prefix and, if available, the IP-CAN type, RAT type and/or the default charging method. For types of IP-CAN, where the H-PCRF can be in control of IP-CAN Bearers, e.g. GPRS, the PCEF also provides a new bearer identifier and information about the requested bearer, such as QoS. If case 1 applies, it will also provide information to indicatewhether NW-initiated bearer control procedures are supported, if available.

When the UE is roaming in a Home-Routed scenario, step 3 also applies. If the UE is roaming in a Visited Access scenario, the following steps 3x are executed instead of step 3:

3a. The PCEF informs the V-PCRF of the establishment of the IP-CAN session by starting a new Gx session as in step 3.

3b. For the roaming case, the V-PCRF will determine that the request is for a roaming user and will conclude the the IP-CAN session use visited access. V-PCRF will store the received information

3c. V-PCRF issues an IP-CAN session establishment request to the H-PCRF.

4. The H-PCRF stores the information received in the Diameter CCR.

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

6. The SPR replies with the subscription related information containing the information about the allowed service(s), QoS information and PCC Rules information.

NOTE 2: For steps 5 and 6: The details associated with the Sp reference point are not specified in this Release. The SPR's relation to existing subscriber databases is not specified in this Release.

7. The H-PCRF selects or generates PCC Rule(s) to be installed.
   The H- PCRF may also make a policy decision by deriving an authorized QoS and by deciding whether service flows described in the PCC Rules are to be enabled or disabled.

8. The H-PCRF stores the selected PCC Rules. The H-PCRF selects the Bearer Control Mode that will apply during the IP-CAN session if applicable for the particular IP-CAN. If the H-PCRF controls the binding of IP-CAN Bearers, the H-PCRF stores information about the IP-CAN Bearer to which the PCC Rules have been assigned. If the BBERF/PCEF controls the binding of IP-CAN bearers, the H-PCRF may derive the QoS information per QCI applicable to that IP-CAN session for non-GBR bearers.

9. The PCC Rules are provisioned by the H-PCRF to the PCEF using Diameter CCA. The H-PCRF will also provide the selected Bearer Control Mode if applicable for the particular IP-CAN and if available, the QoS information per QCI. The PCRF may also provide event triggers listing events for which the PCRF desires PCC Rule Requests. Furthermore, the PCRF may provide authorized QoS.

   For types of IP-CAN, where the PCRF controls IP-CAN Bearers, e.g. GPRS, the PCRF indicates the IP-CAN Bearer where the PCC Rules shall be installed and that the authorized QoS refers to. Otherwise, the PCRF operates without any further reference to any specific bearer.

When the UE is roaming in a Home-Routed scenario, step 9 also applies. If the UE is roaming in a Visited Access scenario, the following steps 9x are executed instead of step 9:

9a. The PCC Rules are provisioned by the H-PCRF to the V-PCRF by using a Diameter CCA. The parameters listed in step 9 are also applicable here.

9b. The V-PCRF enforces visited operator policies regarding QoS authorization requested by the H-PCRF as indicated by the roaming agreements.

9c. The V-PCRF informs the H-PCRF when a request has been denied and may provide the acceptable QoS Information for the service.

9d. The H-PCRF acknowledges the CCR and may additionally include new or modified PCC rules to the V-PCRF

9e. The V-PCRF provisions PCC rules to the PCEF.PCEF

10. The PCEF installs the received PCC Rules. The GW also enforces the authorized QoS and enables or disables service flow according to the flow status of the corresponding PCC Rules. If QoS information is received per QCI, PCEF shall set the upper limit accordingly for the MBR that the PCEF assigns to the non-GBR bearer(s) for that QCI.

11. The PCEF sends a response to the Establish IP-CAN Session Request.
For GPRS, the GGSN accepts the PDP Context Request based on the results of the authorisation policy decision enforcement. If the requested QoS parameters do not correspond to the authorized QoS, the GGSN adjusts (downgrades /upgrades) the requested UMTS QoS parameters to the authorized values.

12. The Gateway Control Session Establishment procedure may proceed as defined in 4.4.1, if appropriate.

NOTE 3: The PCRF can reject the IP-CAN session establishment, e.g. the PCRF cannot obtain the subscription-related information from the SPR and the PCRF cannot make the PCC rule decisions, as described in 3GPP TS 29.212 [9].

The PCEF can also reject the IP-CAN session establishment, e.g. there is no activated/installed PCC rules for the IP-CAN session as specified in 3GPP TS 23.203 [2].

Editor's note: Correctness of S9 procedures are still to be confirmed.

4.2 IP-CAN Session Termination

4.2.1 UE-Initiated

This clause is applicable if an IP-CAN Session is being released by the UE.

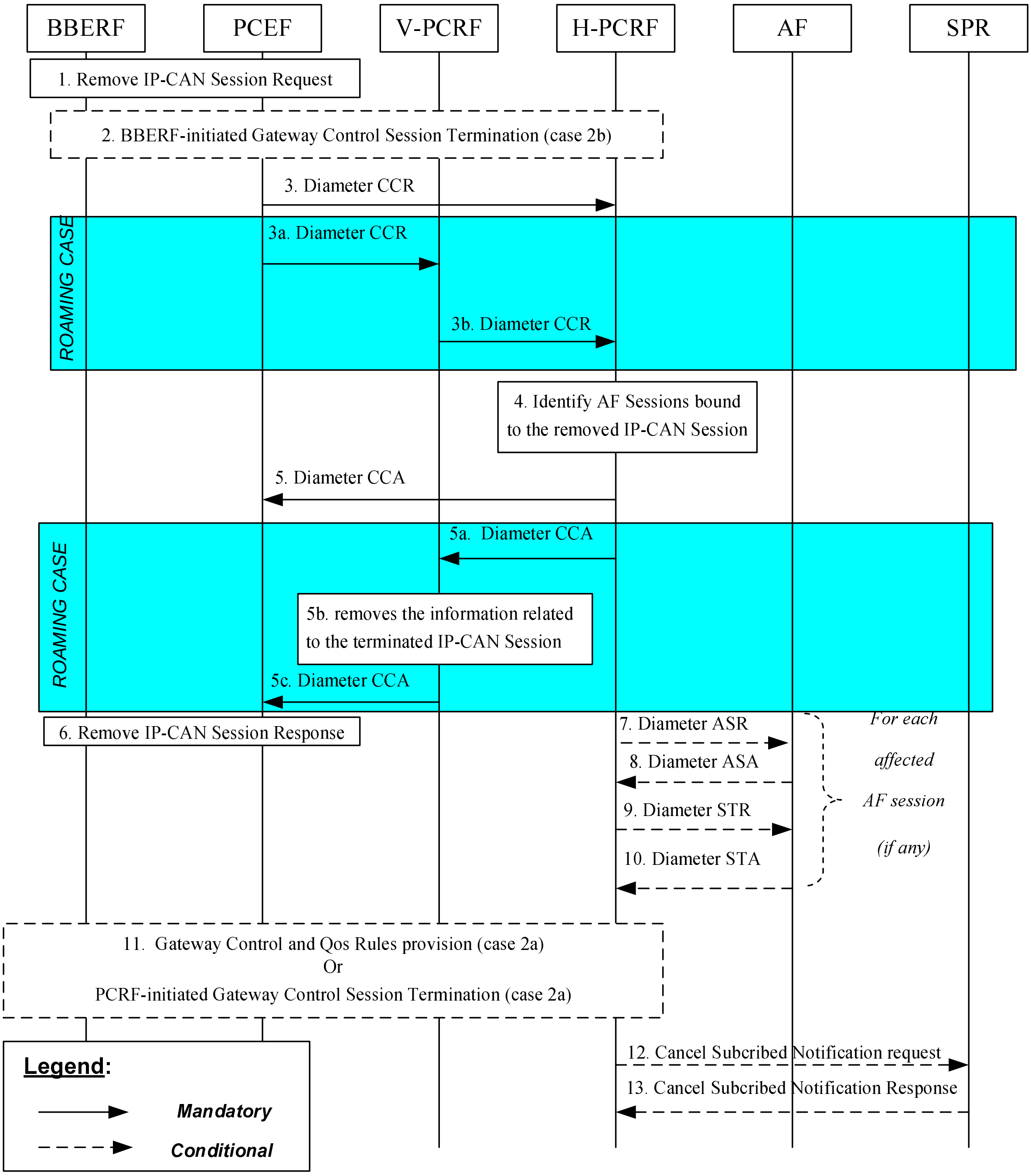


Figure 4.2.1.1: UE-Initiated IP-CAN Session Termination

If the AF relies in the VPLMN, the V-PCRF shall proxy AF session signalling over S9 between the AF and the H-PCRF.

Editor's Note: The case when the AF resides in the VPLMN is not showed in this flow.

In the following procedures, the V-PCRF is included to depict the roaming scenarios. H-PCRF will act as a PCRF for non-roaming UEs.

1. If case 2b applies (as defined in clause 4.0), the BBERF receives a request to remove the IP-CAN session. In case 2a, the request goes transparently through the BBERF. In all cases, the PCEF receives a request to remove the IP-CAN Session. The form of the Remove IP-CAN Session Request depends upon the type of the IP-CAN. For GPRS, the GGSN receives a Delete PDP Context Request for the last PDP context within an IP-CAN session. For I-WLAN, the GW receives an IPSec tunnel termination request.

2. If case 2b applies (as defined in clause 4.0), the BBERF-initiated GW Control Session Termination procedure as defined in clause 4.4.4(BBERF-Initiated Gateway Control Session Termination) is initiated.

3. The PCEF sends a Diameter CCR message to the H-PCRF, indicating the IP-CAN Session termination. The GW requests the termination of the DCC session using the CC-Request-Type AVP set to the value TERMINATION_REQUEST.

   When the UE is roaming, then steps 3a~3bb are executed instead of step 3:

   3a. The PCEF sends a Diameter CCR message to the V-PCRF, indicating the IP-CAN Session termination. The GW requests the termination of the DCC session using the CC-Request-Type AVP set to the value TERMINATION_REQUEST.

   3b. The V-PCRF sends the CCR command to the H-PCRF

4. The PCRF identifies AF sessions that are bound to IP flows of the removed IP-CAN Session.

   5. The PCRF acknowledges the session termination by sending a Diameter CCA message.When the UE is roaming, then steps 5a~5c are executed instead of step 5:

   5a. The PCRF acknowledges the session termination by sending a Diameter CCA message to the V-PCRF.

   5b. The V-PCRF removes the information related to the terminated IP-CAN Session.

   5c. The V-PCRF sends the Diameter CCA message to the PCEF.

6. The GW sends a response to the Remove IP-CAN Session Request. For GPRS, the GGSN sends a Delete PDP Context Response message. The form of the Remove IP-CAN Session Request depends upon the type of the IP-CAN. For GPRS, the GGSN receives a Delete PDP Context Request for the last PDP context within an IP-CAN session. For I-WLAN, the GW sends an IPSec tunnel termination response.

NOTE 1: Step 6 may already be executed in parallel to step 3.

For each AF session identified in step 4:

7. The H-PCRF indicates the session abort to the AF by sending a Diameter ASR message to the AF.

8. The AF responds by sending a Diameter ASA message to the H-PCRF.

9. The AF sends a Diameter STR message to the H-PCRF to indicate that the session has been terminated.

10. The H-PCRF responds by sending a Diameter STA message to the AF.

11. If case 2a applies (as defined in clause 4.0), the GW Control and QoS Rules Provision procedure as defined in clause 4.4.3(Gateway Control and QoS Rules Provision) may be initiated to remove the QoS rules associated with the IP-CAN session being terminated. This applies e.g. in case the Gateway Control Session shall remain to serve other IP-CAN sessions.

    Alternatively, if UE acquires a care of address (CoA) that is used for the S2c reference point and the H-PCRF determines that all QoS rules are to be removed and the Gateway Control Session shall be terminated, the PCRF-initiated GW Control Session Termination procedure as defined in clause 4.4.4(PCRF-Initiated Gateway Control Session Termination) is initiated. This applies e.g. in case the UE is detached and the CoA acquired by the UE is not used for any other IP-CAN session.

12. The H-PCRF sends a cancellation notification request to the SPR if it has subscribed such notification.

NOTE 2: Step 12 may be initiated any time after step 5.

13. The SPR sends a response to the H-PCRF.

NOTE 3: For steps 12 and 13: The details associated with the Sp reference point are not specified in this Release. The SPR's relation to existing subscriber databases is not specified in this Release.

Editor's note: Correctness of S9 procedures are still to be confirmed.

4.2.2 GW-Initiated

This clause is applicable if an IP-CAN Session is being released by the GW.

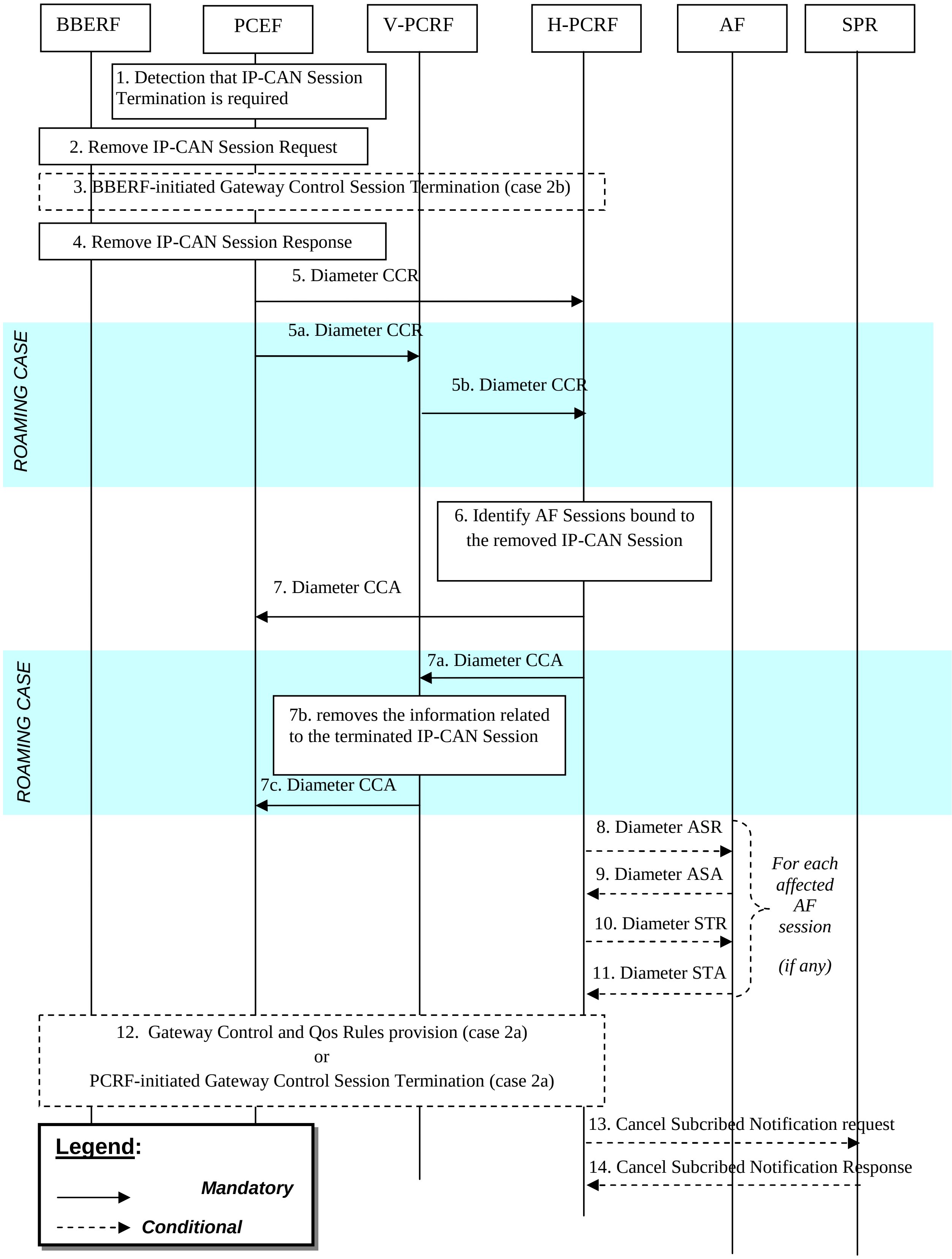

BBERF
PCEF
V-PCRF
H-PCRF
AF
SPR
1. Detection that IP-CAN Session Termination is required
2. Remove IP-CAN Session Request
3. BBERF-initiated Gateway Control Session Termination (case 2b)
4. Remove IP-CAN Session Response
5. Diameter CCR
ROAMING CASE
5a. Diameter CCR
5b. Diameter CCR
6. Identify AF Sessions bound to the removed IP-CAN Session
7. Diameter CCA
ROAMING CASE
7a. Diameter CCA
7b. removes the information related to the terminated IP-CAN Session
7c. Diameter CCA
8. Diameter ASR
9. Diameter ASA
10. Diameter STR
11. Diameter STA
For each affected AF session
(if any)
12. Gateway Control and Qos Rules provision (case 2a)
or
PCRF-initiated Gateway Control Session Termination (case 2a)
13. Cancel Subcribed Notification request
14. Cancel Subcribed Notification Response
Legend:
Mandatory
Conditional

Figure 4.2.2.1: GW-initiated IP-CAN Session Termination

If the AF relies in the VPLMN, the V-PCRF shall proxy AF session signalling over S9 between the AF and the H-PCRF.

Editor's Note: The case when the AF resides in the VPLMN is not showed in this flow.

In the following procedures, the V-PCRF is included to depict the roaming scenarios. H-PCRF will act as a PCRF for non-roaming UEs.

1. The PCEF detects that the termination of an IP-CAN Session or bearer is required.

2. If case 2b applies (as defined in clause 4.0), PCEF sends the Remove IP-CAN Session Request to the BBERF.If case 2a applies (as defined in clause 4.0), the request goes transparently through the BBERF.In all case,the PCEF sends a Remove IP-CAN Session Request to remove the IP-CAN Session.. The form of the Remove IP-CAN Session Request depends upon the type of the IP-CAN. It can consist of separate requests for each IP-CAN Bearer within a IP-CAN Session. For GPRS, the GGSN sends a separate Delete PDP Context Requests for each of the PDP contexts within an IP-CAN session. For I-WLAN, the GW sends an IPSec tunnel termination request.3. If case 2b applies (as defined in clause 4.0), the BBERF-initiated GW Control Session Termination procedure as defined in clause 4.4.4(BBERF-Initiated Gateway Control Session Termination) is initiated.

4. The PCEF receives a response to the Remove IP-CAN Session Request. For GPRS, the GGSN receives a Delete PDP Context Response for each PDP context within the IP-CAN session. For I-WLAN, the GW receives an IPSec tunnel termination response.

5 - 7. Same as Steps 3-5 in figure 4.2.1.1.

8 - 14. Same as Steps 7-13 in figure 4.2.1.1.

NOTE 1: Steps 2 and 5 may be executed in parallel.

Editor's note: Correctness of S9 procedures are still to be confirmed.

4.2.3 PCRF-Initiated

This clause is applicable if an IP-CAN Session is being released by the PCRF.

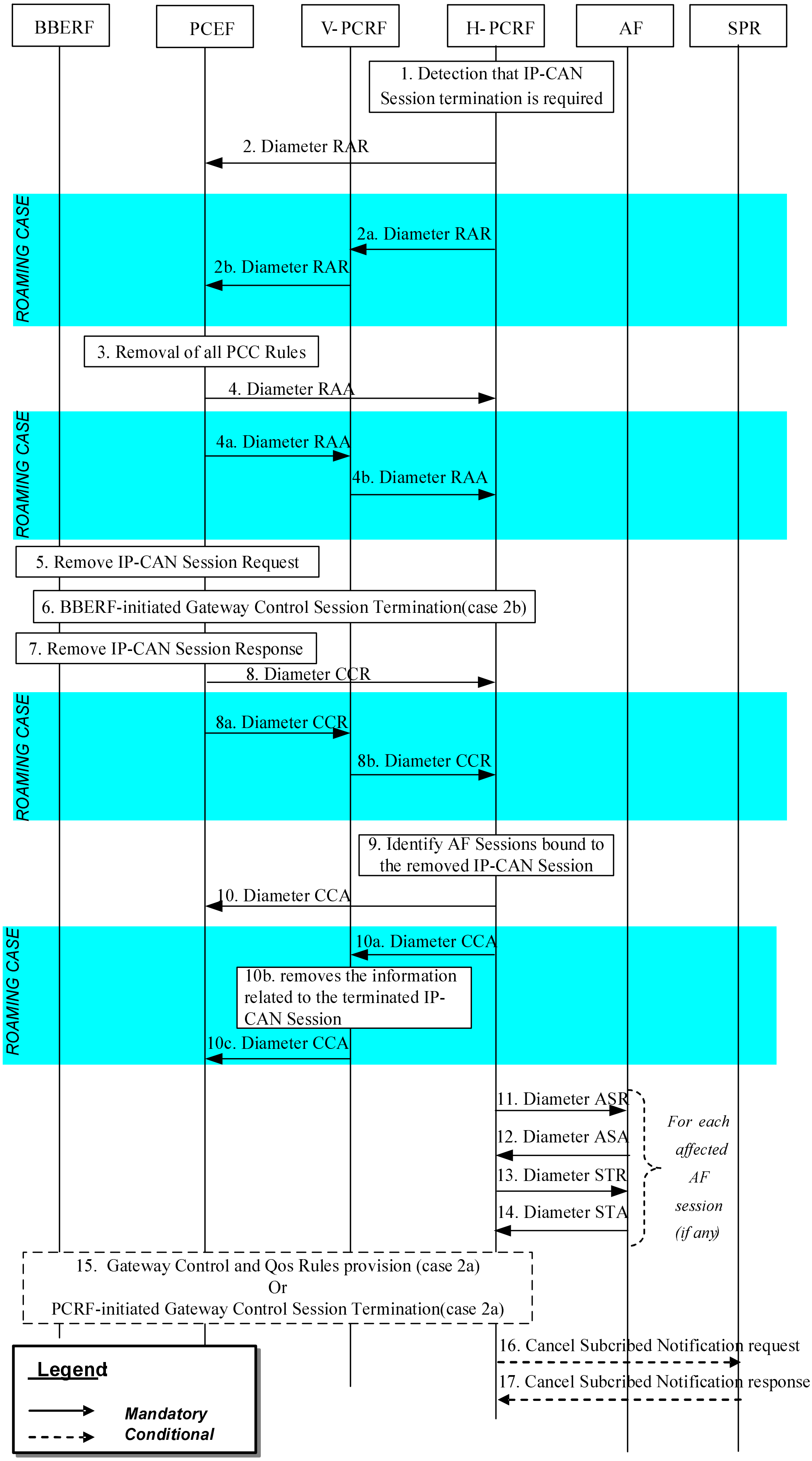

BBERF
PCEF
V- PCRF
H- PCRF
AF
SPR
1. Detection that IP-CAN Session termination is required
2. Diameter RAR
ROAMING CASE
2a. Diameter RAR
2b. Diameter RAR
3. Removal of all PCC Rules
4. Diameter RAA
ROAMING CASE
4a. Diameter RAA
4b. Diameter RAA
5. Remove IP-CAN Session Request
6. BBERF-initiated Gateway Control Session Termination(case 2b)
7. Remove IP-CAN Session Response
8. Diameter CCR
ROAMING CASE
8a. Diameter CCR
8b. Diameter CCR
9. Identify AF Sessions bound to the removed IP-CAN Session
10. Diameter CCA
ROAMING CASE
10a. Diameter CCA
10b. removes the information related to the terminated IP-CAN Session
10c. Diameter CCA
11. Diameter ASR
12. Diameter ASA
13. Diameter STR
14. Diameter STA
For each affected AF session (if any)
15. Gateway Control and Qos Rules provision (case 2a) Or PCRF-initiated Gateway Control Session Termination(case 2a)
16. Cancel Subcribed Notification request
17. Cancel Subcribed Notification response
Legend
Mandatory
Conditional

Figure 4.2.3.1: PCRF-initiated IP-CAN Session Termination

If the AF relies in the VPLMN, the V-PCRF shall proxy AF session signalling over S9 between the AF and the H-PCRF.

Editor's Note: The case when the AF resides in the VPLMN is not showed in this flow.

In the following procedures, the V-PCRF is included to depict the roaming scenarios. H-PCRF will act as a PCRF for non-roaming UEs.

1. The H-PCRF detects that the termination of an IP-CAN Session is required.
2. The H-PCRF sends a Diameter RAR to request that the PCEF terminates the IP CAN session.

   When the UE is roaming, then steps 2a~2b are executed instead of step 2:

   2a. The H-PCRF sends the Diameter RAR message to the V-PCRF.

   2b. The V-PCRF sends the Diameter RAR message to the PCEF.
3. The PCEF removes the identified PCC Rules.
   4. The PCEF sends RAA to acknowledge the RAR.When the UE is roaming, then steps 4a~4b are executed instead of step 4:

   4a. The PCEF sends RAA to the V-PCRF.

   4b. The V-PCRF sends RAA to the H-PCRF.
5. The PCEF shall apply IP CAN specific procedures to terminate the IP CAN session.

6. -17. Same as Steps 3-14 in figure 4.2.2.1.

Editor's note: Correctness of S9 procedures are still to be confirmed.

4.3 IP-CAN Session Modification

4.3.1 Network-Initiated IP-CAN Session Modification

4.3.1.1 Interactions between GW and PCRF (PCC Rule Provisioning in PUSH mode)

This flow shows the provisioning of PCC Rules and/or authorized QoS triggered by an event in the PCRF.

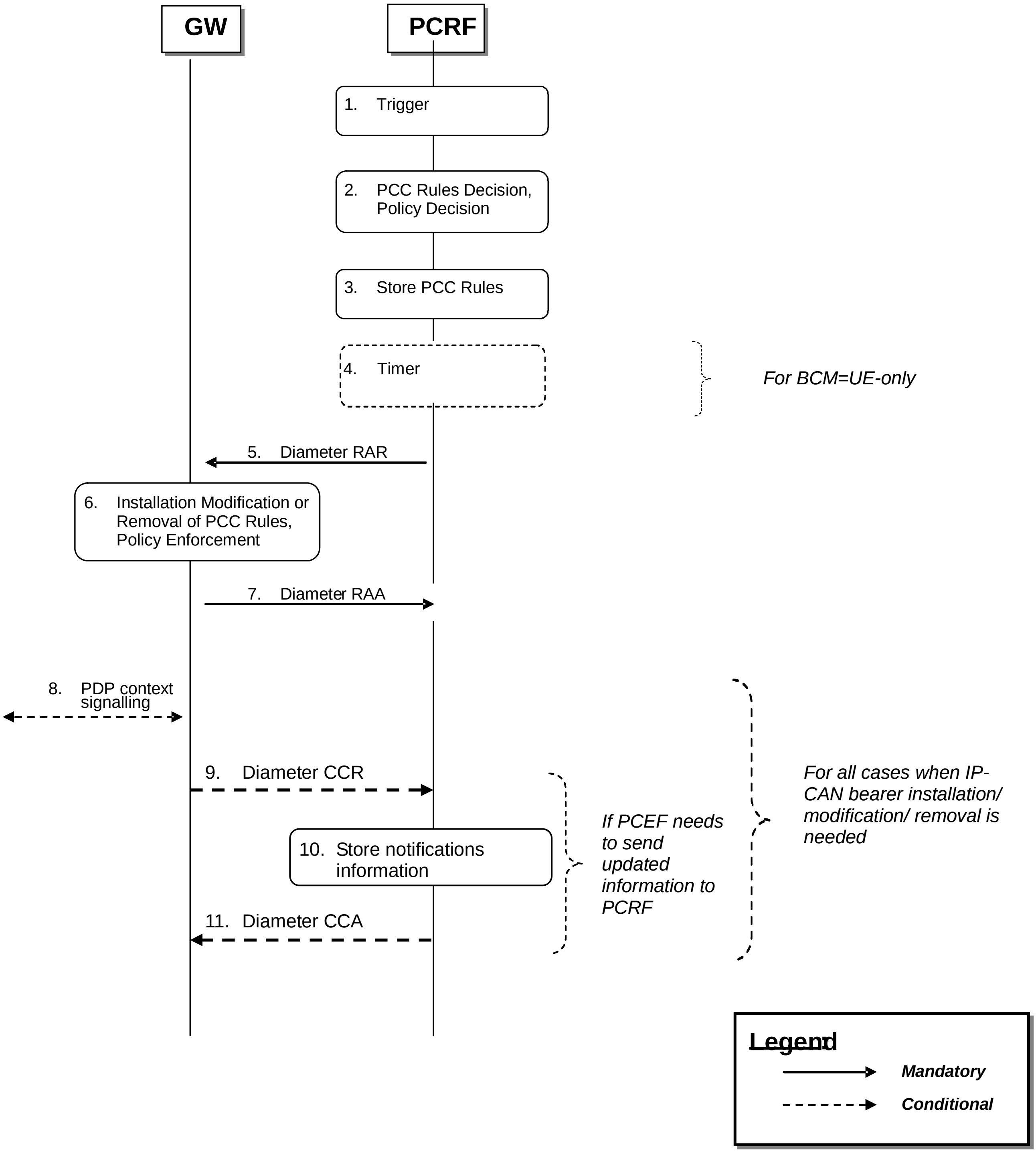


Figure 4.3.1.1.1: Interactions between GW and PCRF for PCRF-Initiated IP-CAN Session Modification

1. The PCRF receives an internal or external trigger to re-evaluate PCC Rules and policy decision for an IP-CAN Session. Possible external trigger events are described in clause 4.3.1.2.

2. The PCRF selects the PCC Rule(s) to be installed, modified or removed for the IP-CAN Session. The PCRF may also update the policy decision by defining an authorized QoS and enable or disable the service flow(s) of PCC Rules. If the PCEF controls the binding of IP-CAN bearers, PCRF may add or change QoS information per QCI applicable to that IP-CAN session.

3. The PCRF stores the updated PCC Rules.

4. Step 4 is only applicable if the Bearer Control Mode (BCM) selected is UE-only and the PCRF receives an external trigger from the AF.

The PCRF may start a timer to wait for an IP CAN bearer initiation, modification or removal procedure initiated by the UE, as depicted in figure 4.3.2.1.1 or figure 4.3.2.2.1 in the following cases:

- If the authorized QoS for an IP-CAN bearer is changed, or
- if one or more Flow Descriptions need to be added, deactivated or removed in any of the PCC rules bound to an IP-CAN bearer, or
- if as a result of policy decisions in step 2, new PCC rules need to be installed and the PCRF requires additional filter information from the UE to execute the bearer binding.

If an IP-CAN bearer initiation, modification or termination procedure initiated by the terminal is received for the affected PCC rules while the timer is running, all subsequent steps in the present figure shall not be executed and the steps in figure 4.3.2.1.1 or figure 4.3.2.2.1 (on provisioning based on PULL procedure at UE-initiated IP-CAN bearer establishment, modification or termination) shall be executed instead.

If the timer expires and the PCRF still requires additional filter information coming from the UE in order to decide on bearer binding for new PCC rules to be installed, all subsequent steps in the present figure shall not be executed, and further reactions of the PCRF are left unspecified. As a possible option, the PCRF could abort the AF session.

Otherwise, the PCRF shall proceed with the subsequent steps (provisioning based on PUSH procedure) in the present figure after timer expiry.

5. The PCRF sends a Diameter RAR to request that the GW installs, modifies or removes PCC Rules and updates the policy decision.

   For types of IP-CAN, where the PCRF controls IP-CAN Bearers, e.g. GPRS, the PCRF identifies the IP-CAN Bearer for each of the PCC Rules and the authorized QoS. The PCRF may provision PCC Rules and authorized QoS for several IP-CAN Bearers within the same RAR.

6. The GW installs, modifies or removes the identified PCC Rules. The GW also enforces the authorized QoS and enables or disables service flow according to the flow status of the corresponding PCC Rules. If QoS information is received per QCI, PCEF shall set/update the upper limit for the MBR that the PCEF assigns to the non-GBR bearer for that QCI.

7. The GW sends RAA to acknowledge the RAR. The PCEF informs the PCRF about the outcome of the PCC rule operation. If network initiated procedures apply for the PCC rule and the corresponding IP-CAN bearer can not be established or modified to satisfy the bearer binding, then the PCEF rejects the activation of a PCC rule.

   For GPRS, the subsequent steps are executed separately for each IP-CAN bearer under the following conditions:

   - if all PCC rules bound to a PDP context have been removed or deactivated (PDP Context deactivation is applicable)
   - if one or more PDP contexts have to be modified
   - if in UE/NW Bearer Control Mode, the GGSN needs to establish a new PDP context (PDP Context establishment is applicable) if the bearer binding is located at the PCEF.

8. For GPRS, the GGSN initiates the procedure to Create/Update or Terminate PDP Context Request message to the SGSN. If in the case of updating the PDP Context the authorized QoS for the bearer has changed, the GGSN will modify the UMTS QoS parameters accordingly.

   When the procedure in step 8 is completed and requires of notifications from the GW to the PCRF the following steps are additionally executed:

9. The GW sends the notifications needed to the PCRF. The notification is made by using a CCR messages with the needed AVPs. For an IP-CAN Bearer termination in UE-Only Bearer Control Mode, the GGSN sends a Diameter CCR with the Bearer-Identifier and Bearer-Operation AVPs to indicate "Termination".

10. The PCRF stores the information coming in the notification.

11. The PCRF acknowledge the CCR with a CCA command.

4.3.1.2 Interactions between PCRF, AF and SPR

4.3.1.2.1 AF Session Establishment

4.3.1.2.1.1 AF located in H-PLMN

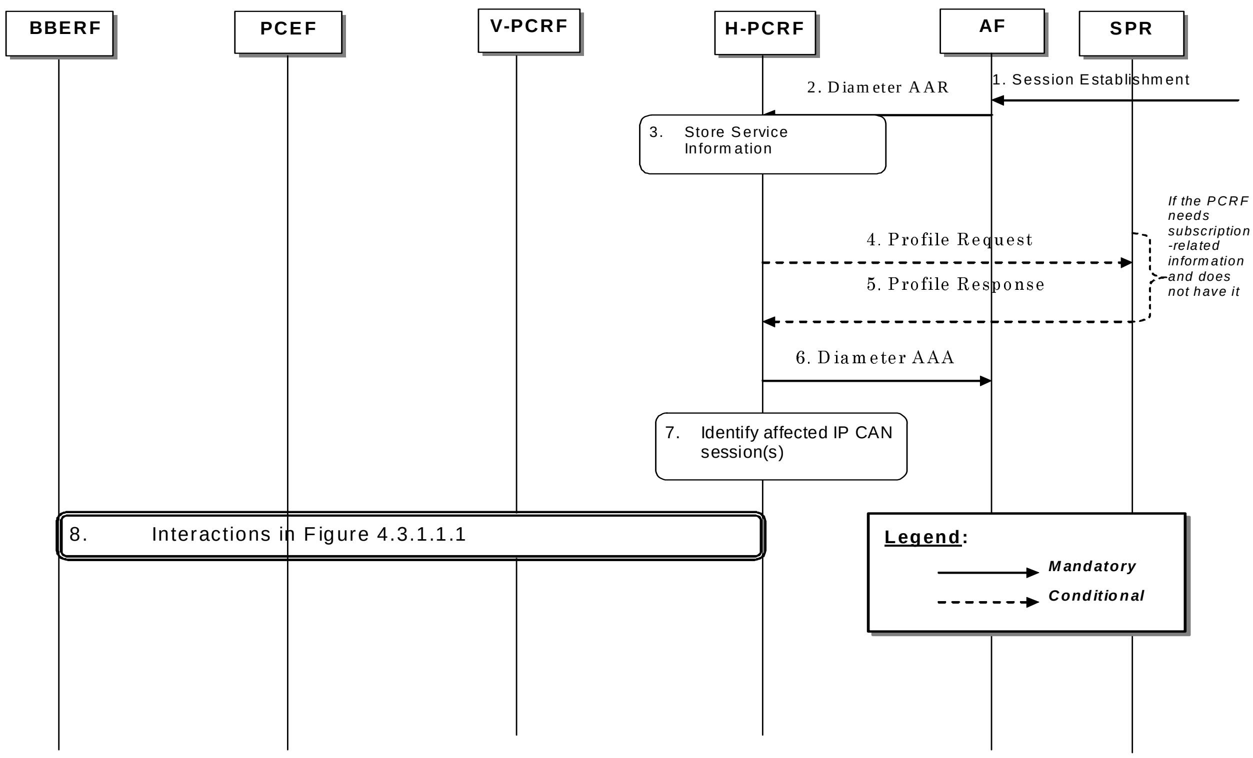


Figure 4.3.1.2.1.1.1 AF located in the H-PLMN

1. The AF receives an internal or external trigger to set-up a new AF session and provide Service Information. The AF identifies the Service Information needed (e.g. IP address of the IP flow (s), port numbers to be used, information on media types, etc).

2. The AF provides the Service Information to the PCRF by sending a Diameter AAR for a new Rx Diameter interface.

3. The PCRF stores the received Service Information, The PCRF identifies the affected established IP-CAN Session(s)using the information previously received from the PCEF and the Service Information received from the AF.

4. If the PCRF requires subscription –related information and does not have it. The PCRF sends a request to the SPR in order to receive the information.

5. The SPR replies with the subscription related information containing the information about the allowed service(s), QoS information and PCC Rules information.

6. The H-PCRF forwards an AAA to the AF

7. The PCRF identifies the affected established IP-CAN Session(s) using the information previously received from the PCEF and the Service Information received from the AF.

8. The PCRF interacts with the PCEF/BBERF according to figure 4.3.1.1.1 (Interactions between GW and PCRF for PCRF-Initiated IP-CAN Session Modification).

4.3.1.2.1.2 AF in the Visited network

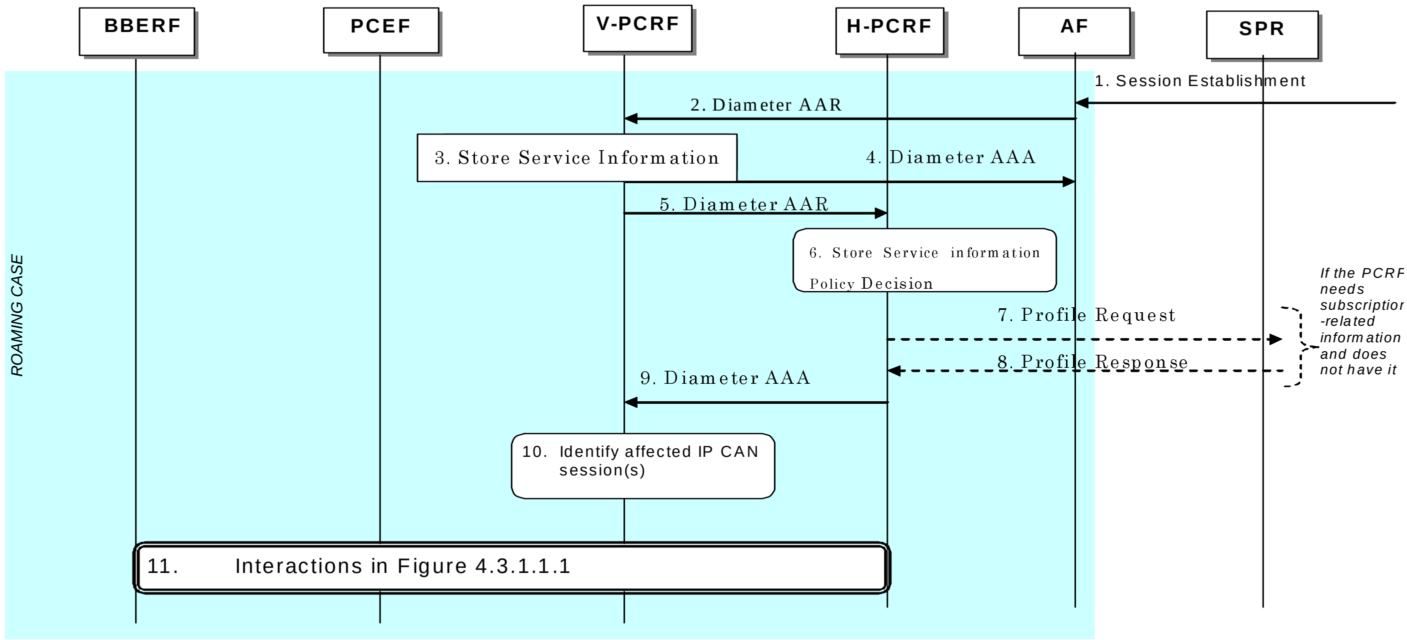


Figure 4.3.1.2.1.2.1 AF in the Visited PLMN

1. The AF receives an internal or external trigger to set-up a new AF session and provide Service Information. The AF identifies the Service Information needed (e.g. IP address of the IP flow (s), port numbers to be used, information on media types, etc).

2. The AF provides the Service Information to the V-PCRF by sending a Diameter AAR for a new Rx Diameter interface.

3. V-PCRF stores the Service Information.

4. V-PCRF responds to the AF with a AA-Answer command.

5. V-PCRF forwards the AA-Request to the H-PCRF.

6. If the PCRF requires subscription-related information and does not have it, the PCRF sends a request to the SPR in order to receive the information.

7. The SPR replies with the subscription related information containing the information about the allowed service(s), QoS information and PCC Rules information.

8. H-PCRF stores the Service Information and identifies the affected established IP-CAN Session (s) using the information previously received from the PCEF and the Service Information received from the AF.

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

10. The PCRF identifies the affected established IP-CAN Session(s) using the information previously received from the PCEF and the Service Information received from the AF.

11. The PCRF interacts with the PCEF/BBERF according to figure 4.3.1.1.1 (Interactions between GW and PCRF for PCRF-Initiated IP-CAN Session Modification).

Editor's Note: It is FFS if the AAA message to the AF should be send as step 4 or after step 9.

Editor's Note: It is FFS which messages will be used to provision the PCC rules over the S9 interface.

4.3.1.2.2 AF session modification

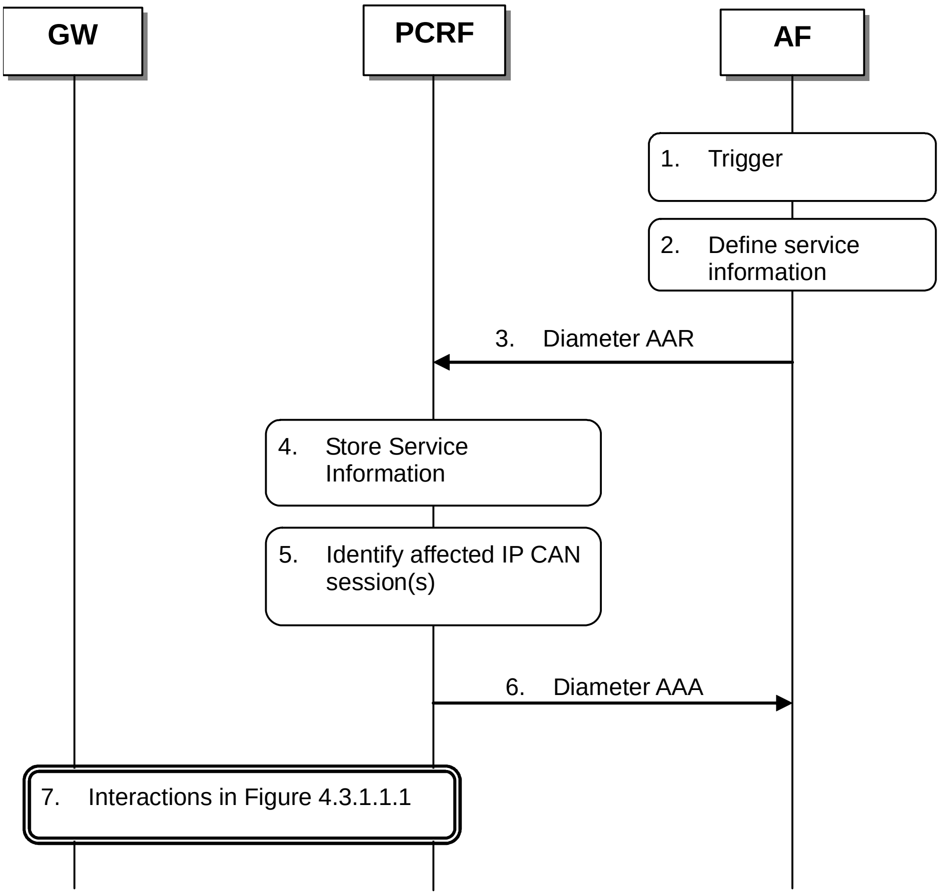


Figure 4.3.1.2.2.1: AF session modification triggers PCRF-Initiated IP-CAN Session Modification

1. The AF receives an internal or external trigger to modify an existing AF session and provide related Service Information.
2. The AF identifies the Service Information needed (e.g. IP address of the IP flow(s), port numbers to be used, information on media types, etc.).
3. The AF provides the Service Information to the PCRF by sending a Diameter AAR for the existing Rx Diameter session corresponding to the modified AF session.
4. The PCRF stores the received Service Information.
5. The PCRF identifies the affected established IP-CAN Session(s) using the information previously received from the GW and the Service Information received from the AF.
6. The PCRF sends a Diameter AAA to the AF.
7. The PCRF interacts with the GW according to figure 4.3.1.1.1.

4.3.1.2.3 AF session termination

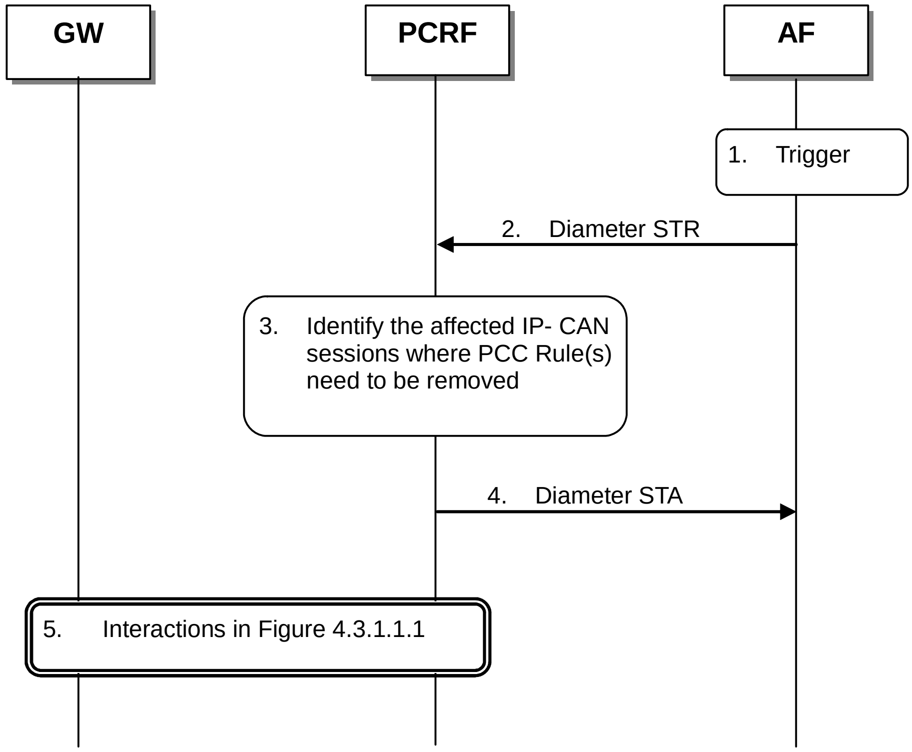


Figure 4.3.1.2.3.1: Removal of PCC Rules at AF session release

1. The AF receives an internal or external trigger for a session release.
2. The AF sends a session termination request, Diameter STR, to the PCRF to request the removal of the session.
3. The PCRF identifies the affected IP-CAN Session where PCC Rules for the IP flow(s) of this AF session are installed. These PCC Rules need to be removed.
4. The PCRF sends Diameter STA, session termination answer, to the AF.
5. The PCRF interacts with the GW according to figure 4.3.1.1.1.

4.3.2 UE-Initiated IP-CAN Session Modification (PCC Rule Provisioning in PULL Mode)

4.3.2.1 UE-initiated IP-CAN Bearer Establishment or IP-CAN Bearer Modification

This clause is applicable for the establishment of a new IP-CAN Bearer (other than the one which created the IP-CAN session) and for the modification of an already established IP-CAN Bearer. The signalling flows for these cases are as per Figure 4.3.1.2.1.

A bearer-event-initiated Request of PCC Rules occurs when a new bearer is established or when an existing bearer is modified. For GPRS, these are PDP Context Modification(s) or secondary PDP context Activation(s). An IP-CAN Session modification triggers a PCC Rule request only if the PCRF has previously requested a PCC Rule request for the given modification event.

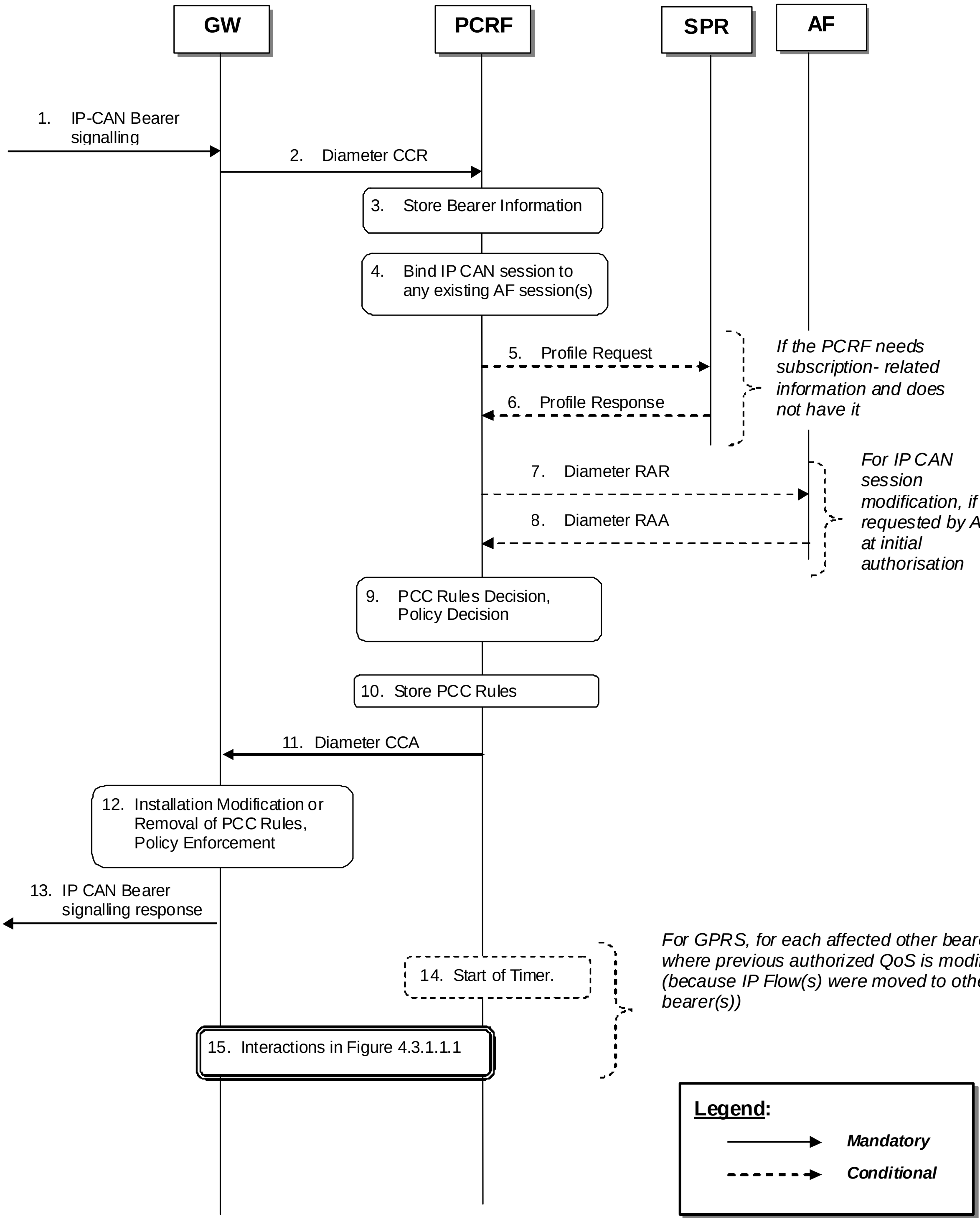


Figure 4.3.2.1.1: UE-initiated IP-CAN Bearer Establishment and Modification.

1. The GW receives IP-CAN Bearer signalling that is a trigger for a PCC Rule request. The form of the Establish IP-CAN Bearer signalling depends upon the type of the IP-CAN. For GPRS, the GGSN receives a secondary Establish PDP Context Request or an Update PDP Context Request.

2. The GW informs the PCRF of the modification of the IP-CAN Session due to the IP-CAN Bearer signalling in step 1, using a Diameter CCR with the CC-Request-Type AVP set to the value UPDATE_REQUEST. The GW reuses the existing Gx DCC session corresponding to the IP-CAN Session.
For types of IP-CAN, where the PCRF controls IP-CAN Bearers, e.g. GPRS: If the IP-CAN Bearer signalling in step 1 established a new IP-CAN Bearer, the GW assigns a new bearer identifier to this IP-CAN Bearer. The GW provides information about the new of modified bearer, e.g. requested QoS and TFT filters. If the event that caused the bearer modification applies uniquely to that bearer and PCRF performs the bearer binding, then, the

bearer identifier should be provided within the CCR. If no bearer identifier is provided, the event trigger will apply to the IP-CAN session.

3. The PCRF stores the received information in the Diameter CCR.

4. The PCRF binds the IP-CAN Session to existing of AF session(s) using the information received from the GW and the Service Information included in the stored PCC rules, which was previously received from the AF(s) , as depicted in figure 4.3.1.1.1.
For types of IP-CAN, where the PCRF controls IP-CAN Bearers, e.g. GPRS, the PCRF also binds the IP-CAN Bearers within the IP-CAN Session to all matching IP flow(s) of existing AF session(s) using the bearer information received from the GW and the Service Information received from the AF(s). If IP flow(s), which have previously been bound to other bearers, have been bound to the modified bearer, PCC Rules in other bearer(s) may need to be removed. For GPRS, an IP flow may need to be removed if a matching higher priority TFT filter in the newly established PDP context takes precedence over a matching lower priority TFT filter in another PDP context. Furthermore, if IP Flow(s), which have previously been bound to the modified bearer are be bound to other bearer(s), PCC Rules may need to be installed in other bearers. For GPRS, an IP flow may be bound to another PDP context if it was previously bound to the modified PDP context due to a removed higher priority TFT filter, and a lower priority TFT filter in the other PDP context matches the IP flow.

5. If the PCRF requires subscription-related information and does not have it, the PCRF sends a request to the SPR in order to receive the information.

6. The SPR replies with the subscription related information containing the information about the allowed service(s) and PCC Rules information.

NOTE: For steps 5 and 6: The details associated with the Sp reference point are not specified in this Release. The SPR's relation to existing subscriber databases is not specified in this Release.

7. For IP CAN session modification, if the AF requested a notification of the corresponding event at the initial authorisation of the AF session, the PCRF shall sent a Diameter RAR with the Specific-Action AVP set to indicate the trigger event that caused the request.

8. If step 7 happens, the AF replies with a Diameter RAA and may provide updated service information within.

9. The PCRF selects the new PCC Rule(s) to be installed. The PCRF can also identify existing PCC Rules that need to be modified or removed. The PCC Rules may relate to any of the matching AF sessions identified in step 4 or may exist in the PCRF without matching to any AF session. The PCRF may also make a policy decision by defining an authorized QoS and by deciding whether service flows described in the PCC Rules are to be enabled or disabled.
For types of IP-CAN, where the PCRF controls IP-CAN Bearers, e.g. GPRS, the PCC Rules may affect the IP-CAN Bearer identified in the CCR of step 2 or any other IP-CAN Bearer identified in step 4.

10. The PCRF stores the modified PCC Rules.

11. The PCC Rules are provisioned by the PCRF to the GW using Diameter CCA. The PCRF may also provide authorized QoS.
For types of IP-CAN, where the PCRF controls IP-CAN Bearers, e.g. GPRS, the PCRF identifies the affected IP-CAN Bearer for each of the PCC Rules and the authorized QoS. The PCRF may provision PCC Rules and authorized QoS for several IP-CAN Bearers within the same CCA.

12. The GW installs the received PCC Rules. The GW also enforces the authorized QoS and enables or disables service flow according to the flow status of the corresponding PCC Rules.

13. The GW sends a response to the IP-CAN Bearer signalling in step 1.
For GPRS, the GGSN accepts the secondary Establish PDP Context Request or the Update PDP Context Request based on the results of the authorisation policy decision enforcement and sends an Establish PDP Context Response or Update PDP Context Response. If the requested QoS parameters do not correspond to the authorized QoS, the GGSN adjusts (downgrades/upgrades) the requested UMTS QoS parameters to the authorized values.

    For types of IP-CAN, where the PCRF controls IP-CAN Bearers, e.g. GPRS, the PCRF may have decided in step 4 to modify PCC Rules and/or authorized QoS of other IP CAN bearers than the IP-CAN Bearer identified in the CCR of step 2. For each such other IP-CAN Bearer identified in step 4, the GGSN executes the following steps.

14. The PCRF may start a timer to wait for PDP context modification requests from the UE.

15. The PCRF interacts with the GW according to figure 4.3.1.1.1.

4.3.2.2 UE-initiated IP-CAN Bearer Termination

This clause is applicable if an IP-CAN Bearer is being released while other IP-CAN Bearers and thus the IP-CAN Session are not released.

For the termination of IP-CAN Bearers, three cases are covered:

- Bearer release that does not cause service data flow(s) within an AF session to be disabled;
- Bearer release that causes at least one but not all the service data flow(s) within an AF session to be disabled; and
- Bearer release that causes all the service data flows within an AF session to be disabled.

A Bearer release may not cause a service data flow within this bearer to be disabled if the IP flow can be bound to another bearer. For GPRS, an IP flow can be bound to another PDP context if a lower precedence TFT filter matching the IP flow is installed at the other PDP context.

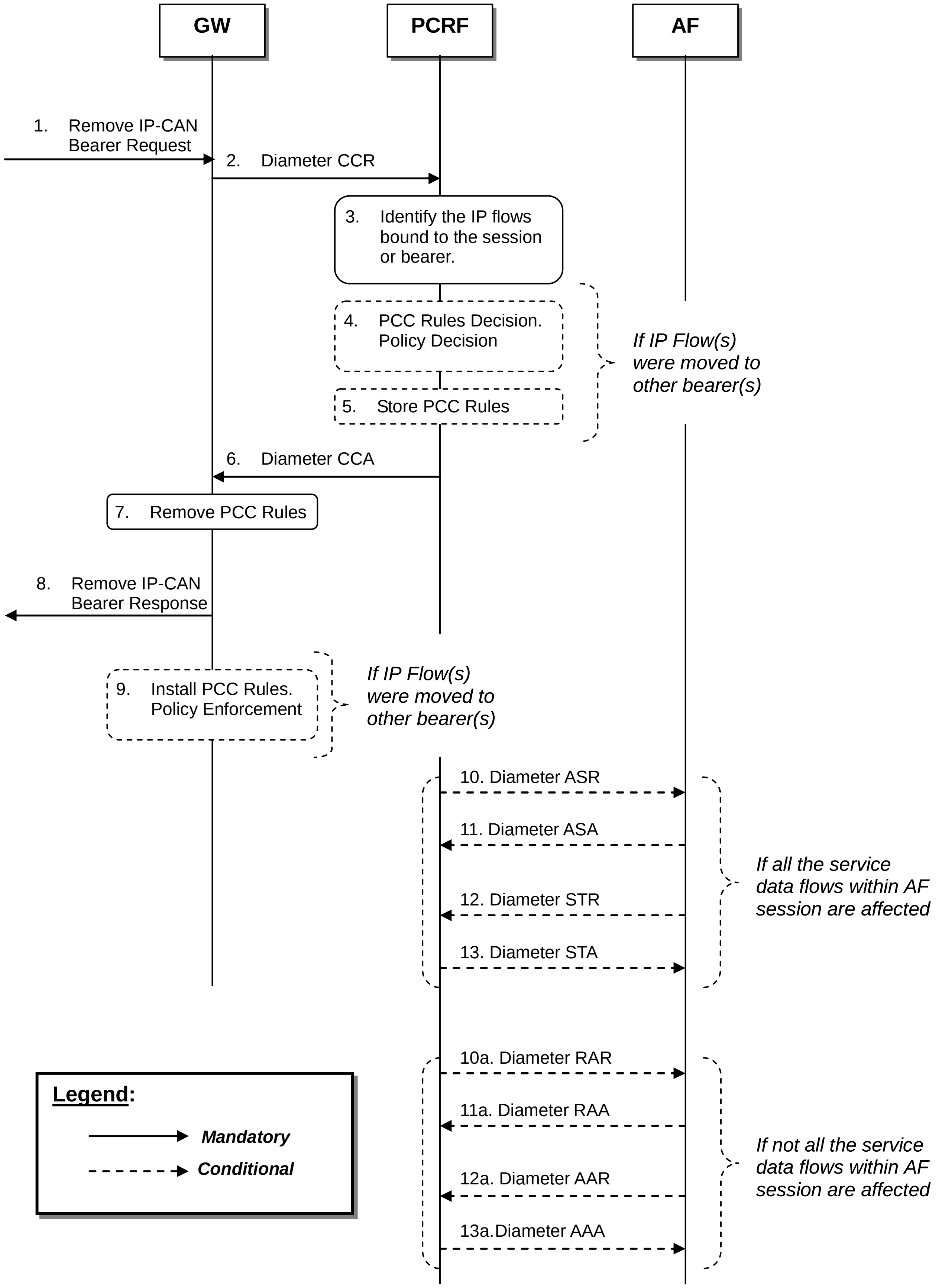


Figure 4.3.2.2.1: UE-Initiated IP-CAN Bearer Termination

1. The GW receives a Remove IP-CAN Bearer Request that request the deactivation of an IP-CAN Bearer while other IP-CAN Bearers and thus the IP-CAN Session are not released. The form of the Remove IP-CAN Bearer Request depends upon the type of the IP-CAN. For GPRS, the GGSN receives a Delete PDP Context Request.

2. The GW sends a Diameter CCR message with the CC-Request-Type AVP set to the value UPDATE_REQUEST to the PCRF, indicating the IP-CAN Bearer termination.

3. For types of IP-CAN, where the PCRF controls IP-CAN Bearers, e.g. GPRS, the PCRF identifies the IP flows bound to the removed bearer and updates the stored bearer information. The PCRF re-evaluates the binding of IP flows, as IP flows may now be bound to other bearers. For GPRS, an IP flow may be bound to another PDP Context if it was previously bound to the removed PDP context due to a higher priority TFT filter, and a lower priority TFT filter in another PDP context matches the IP flow.

For types of IP-CAN, where the PCRF controls IP-CAN Bearers, e.g. GPRS, the following steps 4 and 5 are performed for each of the other bearers identified in step 3:

4. The PCRF selects the PCC Rule(s) to be installed or modified for the affected bearer. The PCRF may also update the policy decision for this bearer.

5. The PCRF stores the updated PCC Rules for the affected bearer.

6. The PCRF acknowledges the bearer termination by sending a Diameter CCA message.
   For types of IP-CAN, where the PCRF controls IP-CAN Bearers, e.g. GPRS, the PCRF provides PCC Rules and possibly updated authorized QoS for each of the other bearers identified in step 3. The PCRF identifies the affected IP-CAN Bearer for each of the PCC Rules and the authorized QoS.

7. The GW removes those PCC Rules, which have not been moved to other IP CAN bearers by the CCA message and are installed in the IP-CAN bearer, for which a termination has been requested in step 1.

8. The GW sends a Remove IP-CAN Bearer Response. For GPRS, the GGSN sends the Delete PDP Context Response message.

9. It the PCRF has provided PCC Rules and possibly updated authorized QoS for other bearers in step 6, the GW installs or modifies the identified PCC Rules. The GW also enforces the authorized QoS and enables or disables service flow according to the flow status of the corresponding PCC Rules.

The following steps 10 to 13 or 10a to 13a apply for the case where at least one IP Flow within an AF session is being disabled, i.e. if the IP Flow is not bound to any other bearer that is still established. The steps shall be performed separately for each ongoing AF session that is affected by the bearer release as explained below.

If all IP flow(s) within the AF session are disabled by the bearer release:

10. The PCRF indicates the session abort to the AF by sending a Diameter ASR message to the AF.

11. The AF responds by sending a Diameter ASA message to the PCRF.

12. The AF sends a Diameter STR message to the PCRF to indicate that the session has been terminated.

13. The PCRF responds by sending a Diameter STA message to the AF.

If at least one but not all of the IP flow(s) within the AF session are disabled by the bearer release, and the AF has requested notification of bearer removal:

10a. The PCRF indicates the release of the bearer by sending a Diameter RAR to the AF.

11a. The AF responds by sending a Diameter RAA to the PCRF.

12a. The AF may send an AAR to the PCRF to update the session information.

13a. If step 12a occurs, the PCRF responds by sending a AAA to the AF.

Editor´s Note: This flow requires updates to reflect the differences between binding at PCEF and PCRF.

4.4 Gateway Control Session Procedures

There are two kinds of Gateway Control (GC) sessions:

- A Gateway Control session that serves a single IP-CAN session (e.g. S-GW/BBERF connecting to PDN-GW using S5/S8 PMIP according to 23.402 [22]).

- A Gateway Control session that serves all the IP-CAN sessions from the same UE (e.g. a GW/BBERF connecting to PDN-GW using S2c according to TS 23.402 [22]).

These Gateway Control sessions are initiated in connection with IP-CAN session establishment and Initial Attach respectively. For the first case, the PCRF will identify that the GC session serves a single IP-CAN session based on the PDN Identifier received in the request.

An access network may support mobility with BBERF change. The new BBERF shall establish new Gateway Control sessions according to the procedures defined for the new access type and the PCRF shall correlate those sessions with ongoing IP-CAN sessions as part of the handover procedure.

These scenarios are shown separately in different flows.

In the following procedures, the V-PCRF is included to depict the roaming scenarios. H-PCRF will act as a PCRF for non-roaming UEs.

4.4.1 Gateway Control Session Establishment

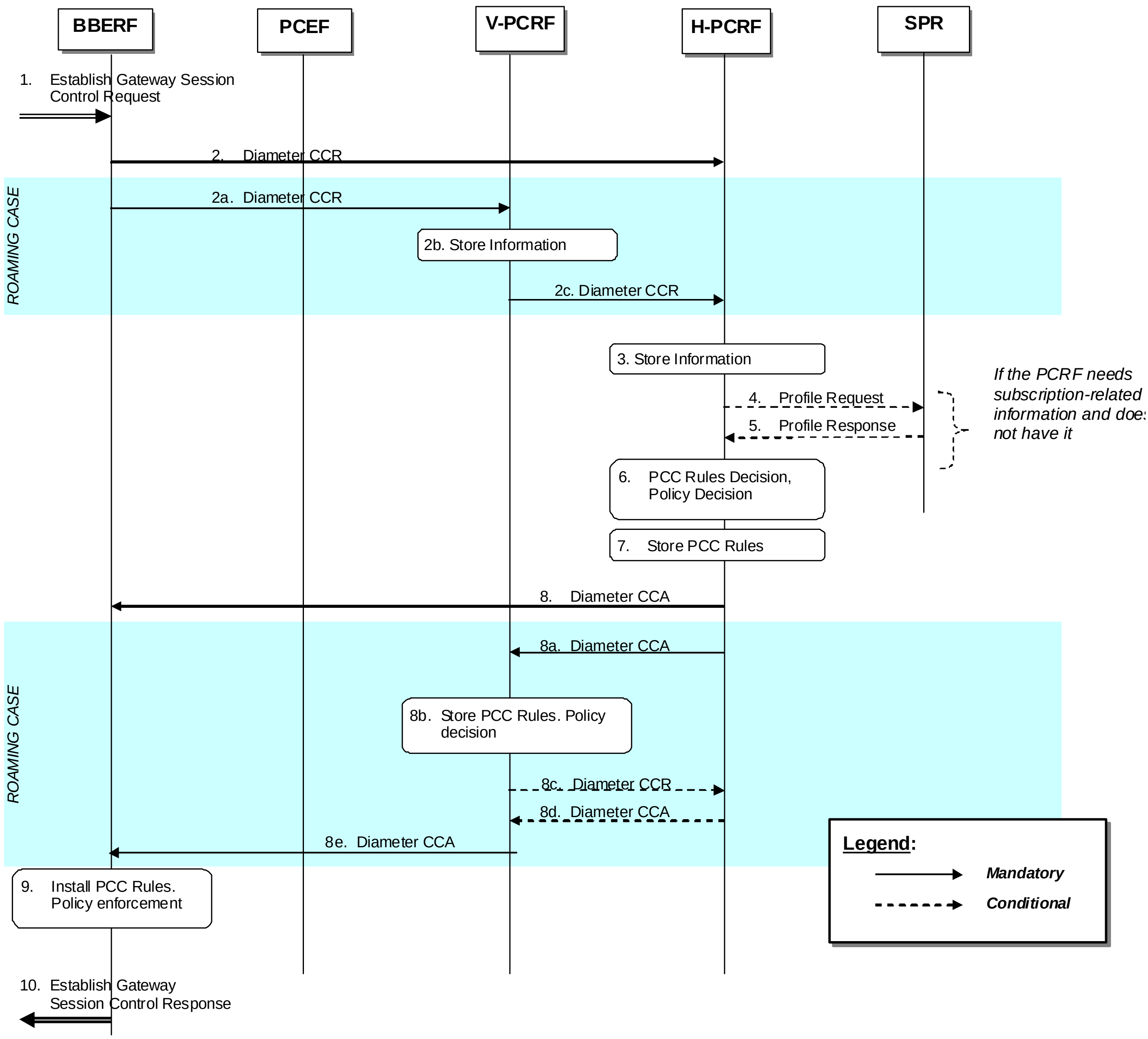


Figure 4.4.1.1 Gateway Control Session Establishment.

1. The BBERF receives a message or indication that it shall establish a Gateway Control session

2. The BBERF initiates a Gateway Control session with the H-PCRF by sending a CCR using the CC-Request-Type AVP set to the value INITIAL_REQUEST to the H-PCRF. The BBERF provides UE identity information, the IP-CAN type. If present the the PDN identifier and the UE IP address are also provided. If applicable for the IP-CAN type, it additionally provides information whether NW-initiated procedures are supported.

When the UE is roaming, the following steps are executed instead of step 2:

2a. The BBERF initiates a Gateway Control session with the V-PCRF by sending a CCR using the CC-Request-Type AVP set to the value INITIAL_REQUEST to the V-PCRF. The BBERF provides UE identity information, the IP-CAN type. If present the PDN identifier and the UE IP address are also provided. If applicable for the IP-CAN type, it additionally provides information whether NW-initiated procedures are supported.

2b. The V-PCRF determines based on the UE identity information that the request is for a roaming user. The V-PCRF checks, based on the PDN identifier received in the request and roaming agreements, if the V-PCRF have send the request to the H-PCRF. If not, the V-PCRF may generate QoS rules based on VPLMN roaming agreements. The V-PCRF shall additionally select the bearer control mode if applicable for the particular IP-CAN type.

2c. The V-PCRF sends the CCR command to the H-PCRF.

3. The H-PCRF stores the information received in the Diameter CCR.

4. If the H-PCRF requires subscription-related information and does not have it, the H-PCRF sends a request to the SPR in order to receive the information.

5. The SPR replies with the subscription related information containing the information about the allowed service(s), QoS information and PCC Rules information.

6. The H-PCRF may select or generate and store PCC Rule(s) in preparation for the anticipated Gx session and derive the QoS rules from them, and may derive the QoS information per QCI applicable to that IP-CAN session for non-GBR bearers.

7. The H-PCRF stores the selected QoS Rules and PCC Rules. If applicable the H-PCRF selects the Bearer Control Mode that will apply during the Gateway Control session.

8. The H-PCRF acknowledges the Gateway Control Session by sending a Diameter CCR to the BBERF.The H-PCRF includes the selected BCM if applicable, the QoS rules and QoS information per QCI and the event triggers.

When the UE is roaming, the following steps are executed instead of step 8:

8a. The H-PCRF acknowledges the Gateway Control Session by sending a Diameter CCR to the V-PCRF. The V-PCRF includes the QoS rules and QoS information per QCI and also provides the event triggers.

8b. The V-PCRF enforces visited operator policies regarding QoS authorization requested by the H-PCRF as indicated by the roaming agreements.

8c. If the V-PCRF denies an authorization, it informs the H-PCRF and may provide the acceptable QoS Information for the service.

8d. The H-PCRF may provide new or modified QoS rules to the V-PCRF

8e. The V-PCRF acknowledges the Gateway Control Session and provisions, when applicable, the selected BCM, policy decisions and event triggers to the BBERF.

9. The BBERF installs the received QoS Rules. If QoS information is received per QCI, the BBERF shall set the upper limit accordingly for the MBR that the BBERF assigns to the non-GBR bearer(s) for that QCI.

4.4.2 Gateway Control and QoS Rules Request

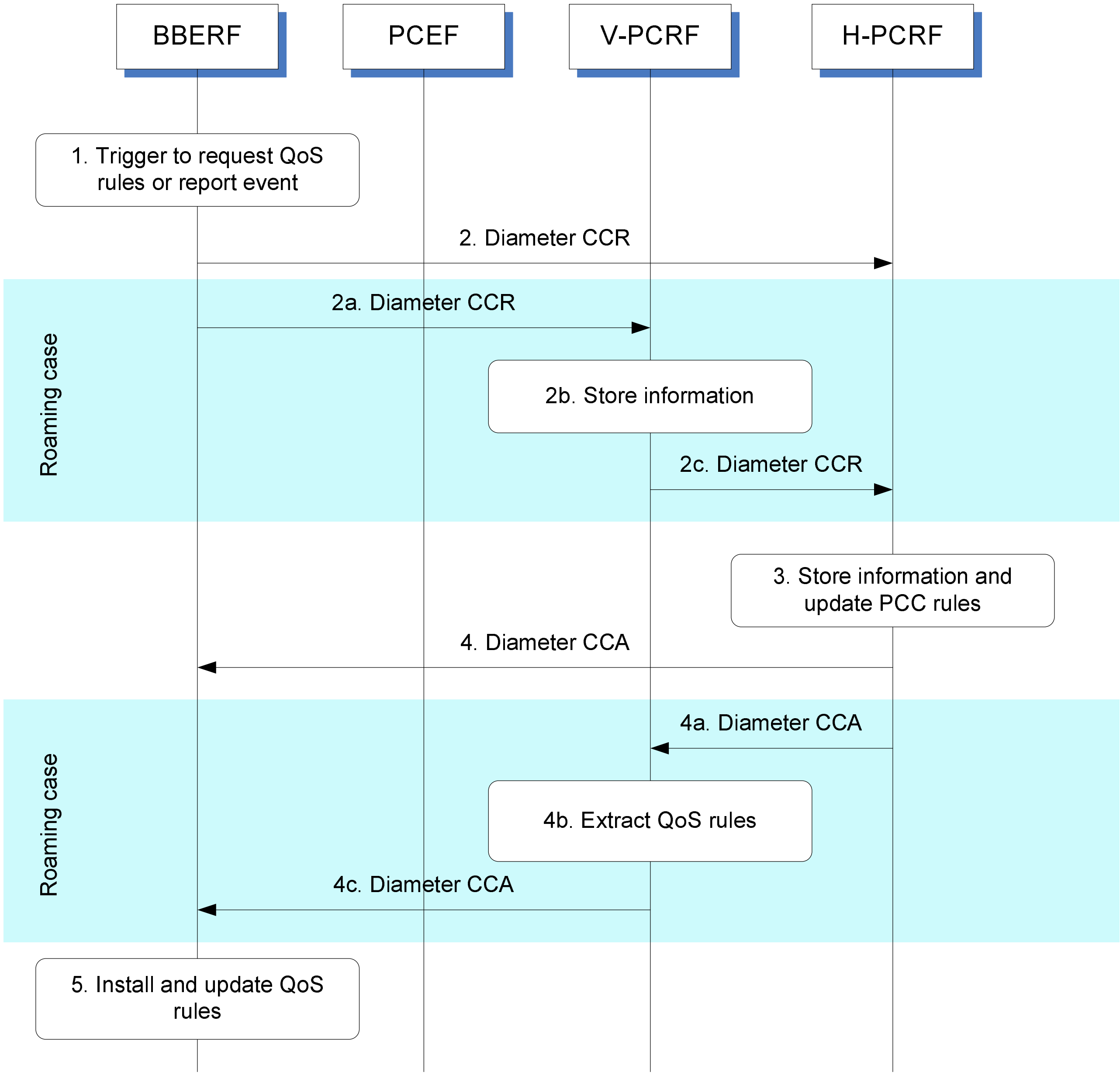


Figure 4.4.2.1: Gateway Control and QoS Rules Request

1. The BBERF is triggered to either report an event or obtain QoS rules or both for a gateway control session.

2. The BBERF sends a Diameter CCR to the H-PCRF with the CC-Request-Type AVP set to the value UPDATE_REQUEST to report event or request QoS rules.

   When the UE is roaming, steps 2a ~ 2c are executed instead of step 2:

   2a. The BBERF sends a Diameter CCR to the V-PCRF with the CC-Request-Type AVP set to the value UPDATE_REQUEST to report event or request QoS rules.

   2b. The V-PCRF stores the information received.

   2c. The V-PCRF forwards the Diameter CCR to the H-PCRF.

3. The H-PCRF stores the received information in the Diameter CCR and derives updated PCC rules and event triggers.

4. The H-PCRF provisions the updated PCC rules and event triggers to the BBERF using Diameter CCA. The CCA may also only acknowledge that the event report has been received successfully.

   When the UE is roaming, steps 4a ~ 4c are executed instead of step 4:

   4a. The H-PCRF sends the updated PCC rules and event triggers to the V-PCRF using Diameter CCA. The CCA may also only acknowledge that the event report has been received successfully.

   4b. The V-PCRF derives the updated QoS rules and event triggers from the rules received from H-PCRF. The V-PCEF may also perform further authorization of the rules based on local policies.

   4c. The V-PCRF sends the updated QoS rules and event triggers to the BBERF using Diameter CCA.

5. The BBERF installs the received QoS Rules and event triggers. This may result in bearer binding being performed according to the rules. The BBERF also enables or disables service flow according to the flow status of the corresponding QoS Rules. The result of the QoS rule activation may trigger the BBERF to send an additional Diameter CCR as described above to the PCRF, for example, to indicate that QoS rule activation has failed.

4.4.3 Gateway Control and QoS Rules Provision

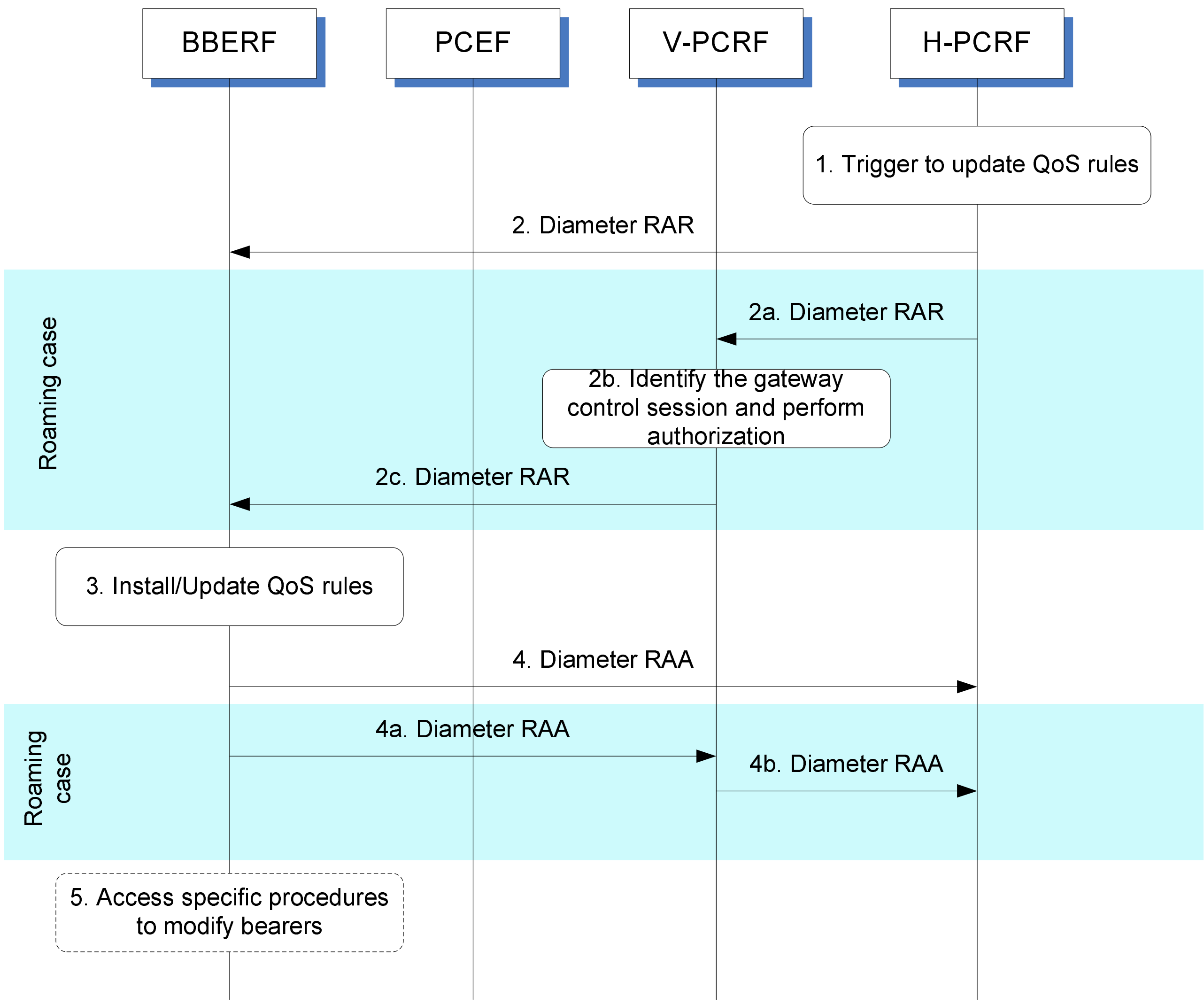


Figure 4.4.3.1: Gateway Control and QoS Rules Provision

1. The H-PCRF receives an internal or external trigger to update QoS Rules and event triggers for a gateway control session.

2. The H-PCRF sends a Diameter RAR to request that the BBERF installs, modifies or removes QoS Rules and/or updates the event triggers.

   If the UE is roaming, then steps 2a ~ 2c are executed instead of step 2:

   2a. The H-PCRF sends a Diameter RAR to the V-PCRF to provision updated QoS Rules and updated event triggers.

   2b. The V-PCRF identifies the gateway control session if needed and performs local authorization of the updated QoS rules when necessary.

   2c. The V-PCRF sends a Diameter RAR to the BBERF to provision updated QoS rules and updated event triggers.

3. The BBERF installs, modifies or removes the identified QoS Rules. The BBERF also enforces the authorized QoS and enables or disables service flow according to the flow status of the corresponding QoS Rules. If QoS information is received per QCI, the BBERF shall set/update the upper limit for the MBR that the BBERF assigns to the non-GBR bearer for that QCI.

4. The BBERF sends RAA to the H-PCRF to acknowledge the RAR and informs the H-PCRF about the outcome of the QoS rule operation. If network initiated resource allocation procedures apply for the QoS rules and the corresponding IP-CAN bearer can not be established or modified to satisfy the bearer binding, then the BBERF rejects the activation of a PCC rule.

   If the UE is roaming, then steps 4a ~ 4b are executed instead of step 4:

   4a. The BBERF sends RAA to to the V-PCRF to acknowledge the RAR and informs the V-PCRF about the outcome of the QoS rule operation. If network initiated resource allocation procedures apply for the QoS rules and the corresponding IP-CAN bearer can not be established or modified to satisfy the bearer binding, then the BBERF rejects the activation of a PCC rule.

   4b. The V-PCRF forwards the RAA to the H-PCRF to acknowledge the RAR and informs the H-PCRF about the outcome of the QoS rule operation.

5. If needed, the BBERF initiates the access specific procedures to create or modify exisiting IP-CAN bearers. When the procedure in step 5 is completed and requires of notifications from the BBERF to the PCRF, the steps described as in clause 4.4.2 are additionally executed.

4.4.4 Gateway Control Session Termination

4.4.4.1 BBERF-Initiated Gateway Control Session Termination

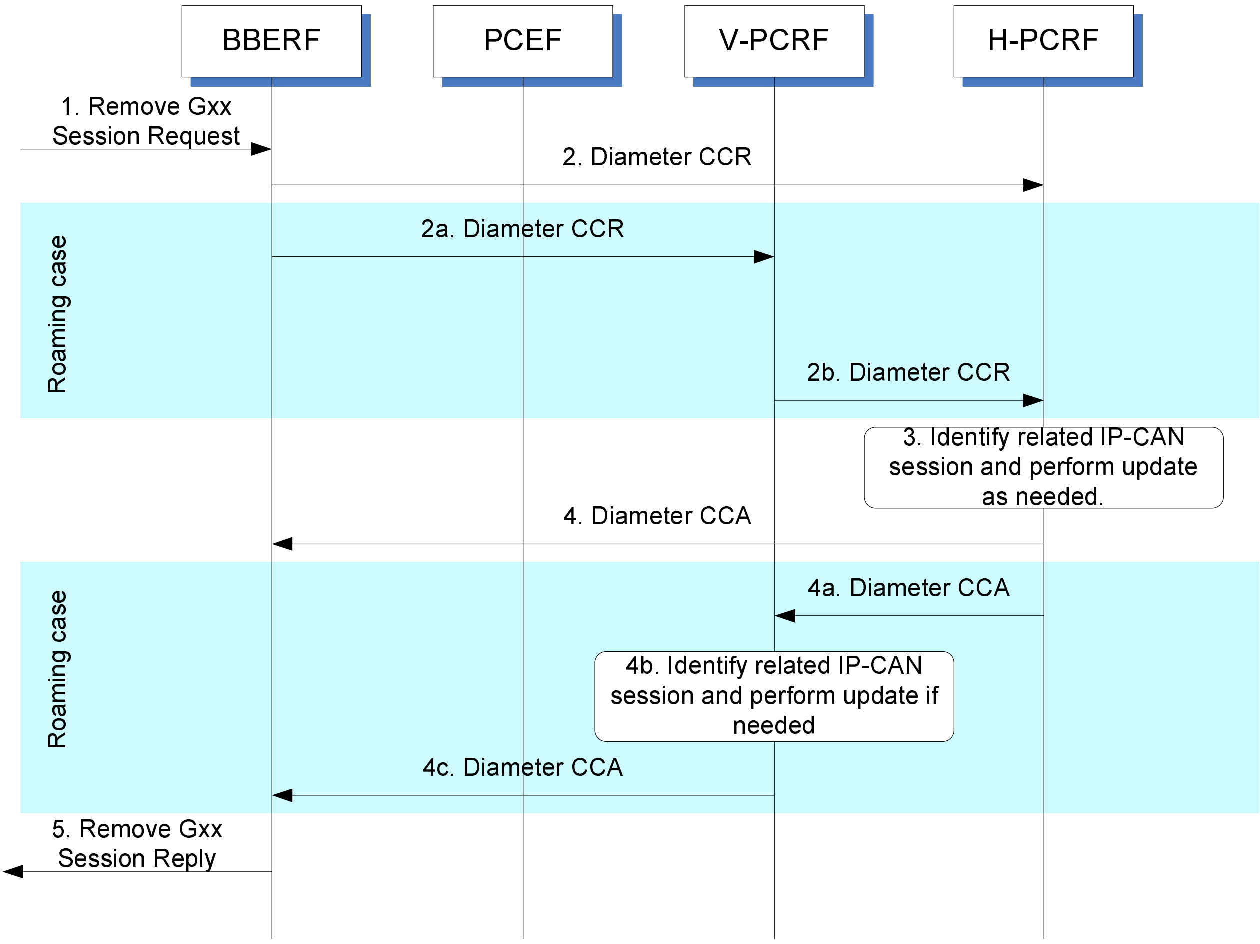


Figure 4.4.4.1.1: BBERF-Initiated Gateway Control Session Termination

1. The BBERF is requested to terminate its gateway control session. The form of the remove gateway control session request depends upon the type of the IP-CAN.

2. The BBERF sends a Diameter CCR message to the H-PCRF, indicating the gateway control session termination. The BBERF requests the termination of the DCC session using the CC-Request-Type AVP set to the value TERMINATION_REQUEST.

   If the UE is roaming, then steps in 2a ~ 2b are executed instead of step 2:

   2a. The BBERF sends a Diameter CCR message to the V-PCRF, indicating the gateway control session termination. The BBERF requests the termination of the DCC session using the CC-Request-Type AVP set to the value TERMINATION_REQUEST.

   2b. If needed, the V-PCRF forwards the Diameter CCR message to the H-PCRF indicating the gateway control session termination. Otherwise, the V-PCRF continues from step 4b.

3. The H-PCRF identifies the related IP-CAN session and performs update as necessary.

4. The H-PCRF acknowledges the session termination by sending a Diameter CCA message.

   If the UE is roaming, then steps 4a ~ 4c are executed instead of step 4:

   4a. The H-PCRF acknowledges the session termination by sending a Diameter CCA message to the V-PCRF.

   4b. The V-PCRF identifies the related IP-CAN session and performs update as necessary.

4c. The V-PCRF acknowledges the session termination by sending a Diameter CCA message to the BBERF. 5. The BBERF sends a reply to the remove gateway control session request. The form of the reply to remove gateway control session request depends upon the type of the IP-CAN.

4.4.4.2 PCRF-Initiated Gateway Control Session Termination

Editor's Note: The call flow for PCRF-initiated gateway control session termination is FFS.

5 Binding Mechanism

5.1 Overview

The binding mechanism associates the session information provided by the AF with the IP-CAN bearer that is intended to carry the service data flow.

The binding mechanism includes three steps as defined in 3GPP TS 23.203 [4]:

1. Session binding.
2. PCC and QoS Rule authorization.
3. Bearer binding.

The Session Binding function receives the Session Information and determines the relevant IP-CAN session. With this information the PCC Rule Authorization function runs the policy rules and constructs the PCC rule(s) if the authorization is granted. Finally the Bearer Binding function selects the IP-CAN bearer where the PCC rule(s) should be installed within the IP-CAN session already known.

PCC Rule Authorization and Bearer Binding can take place without Session Binding at certain IP-CAN Session events (e.g. IP-CAN Session Establishment).

5.2 Session Binding

Session binding is the association of the AF session information to an IP-CAN session.

When the PCRF accepts an AA-Request from the AF over the Rx interface with service information, the PCRF shall perform session binding and associate the described service IP flows within the AF session information (and therefore the applicable PCC rules) to an existing IP-CAN session. This association is done using the user IP address received via the Rx interface in either the Frame-IP-Address AVP or the Framed-IPv6-Prefix AVP. The UE Identity if present in the Subscription-Id AVP and the PDN information if available in the Called-Station-ID AVP may also assist on this association.

The PCRF will determine that the UE has an IP-CAN session if the IP address received over the Rx interface matches the IP address received via one or more of the following interfaces: Gx interface and S9 interface, and if the UE identity is used to assist the association, the UE identity received over the Rx interface matches the UE identity received via one or more of the following interfaces: Gx interface and S9 interface.

NOTE: In case the UE identity in the IP-CAN and the application level identity for the user are of different kinds, the PCRF needs to maintain, or have access to, the mapping between the identities. Such mapping is not subject to specification within this TS.

As a result from the session binding function, the PCRF identifies what IP-CAN session the current AF session is related with. If the PCRF is not capable of executing the Session Binding, the PCRF shall issue an AA-Answer command to the AF with a negative response.

5.3 PCC and QoS Rule Authorization

The PCRF shall perform the PCC and QoS rule authorization when the PCRF receives session information from an AF over Rx interface, when the PCRF receives notification of IP-CAN session events (e.g. establishment, modification) from the PCEF over Gx or S9 interface, or when the PCRF receives IP-CAN events from the BBERF over Gxa/Gxc inferface. The PCRF shall also perform PCC and QoS Rule Authorization for dynamic PCC Rules already provisioned to the PCEF and dynamic QoS rules already provisioned to the BBERF due to internal PCRF triggers (e.g. policies are included or modified within PCRF).

If the PCRF receives any traffic mapping information from the BBF that does not match any service data flow filter, the PCRF shall also perform PCC and/or QoS rule authorization when the UE's subscriber profile allows subscription based authorization. In this case, the PCRF shall treate the received traffic mapping information as if it is service data flow filter information.

The PCRF assigns appropriate QoS parameters (QCI, ARP, GBR, MBR, etc.) to each PCC or QoS rule.

The PCRF authorizes the affected PCC rules and /or QoS rules after successful Session Binding. By the authorization process the PCRF will determine whether the user can have access to the requested services and under what constraints. If so, the PCC rules and QoS rules are created or modified. If the Session Information is not authorized, a negative answer shall be issued to the AF by sending an AA-Answer command.

The PCRF assigns an appropriate QCI to each PCC or QoS rule. IP-CAN specific restrictions and other information available to the PCRF (e.g. users subscription information, operator policies) shall be taken into account. Each PCC or QoS rule shall receive a QCI that can be supported by the IP-CAN. The PCRF shall ensure consistency between the QoS rules and PCC rules authorized for the same service data flow when QoS rules are derived from corresponding PCC rules.

In roaming scenarios, the V-PCRF may further authorize the rules received from the H-PCRF based on local operator policy. Depending on the local policy, the V-PCRF may change the authorized QoS for the affected rules. If local authorization of the rules fails, the V-PCRF shall issue a negative answer to the H-PCRF.

5.4 Bearer Binding

The Bearer Binding function is responsible for associating a PCC rule and QoS rule (if applicable) to an IP-CAN bearer within the IP-CAN session. The QoS demand in the rule, as well as the service data flow template, is input to the bearer binding. The selected bearer shall have the same QoS Class and ARP as the one indicated by the PCC or QoS rule.

The Bearer Binding Function (BBF) is located either at the BBERF or at the PCEF.

The PCRF shall supply the PCC rules to be installed, modified or removed over Gx interface to PCEF. If there are gateway controls sessions associated with the Gx session, the PCRF shall also supply the QoS rules to be installed, modified, or removed over Gxa/Gxc interface to the BBERF.

The BBF shall then check the QoS class identifier and ARP indicated by the rule and bind the rule with an IP-CAN bearer that has the same QoS class identifier and ARP. The BBF shall evaluate whether it is possible to use one of the existing IP-CAN bearers or not and, if applicable, whether to initiate IP-CAN bearer modification or not. If none of the existing bearers are possible to use, the BBF should initiate the establishment of a suitable IP-CAN bearer.

NOTE: For an IP-CAN, limited to a single IP-CAN bearer per IP-CAN session, the bearer is implicit, so finding the IP-CAN session is sufficient for successful bearer binding.

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

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

Whenever the service data flow template, the QoS authorization or the negotiated traffic mapping information change, the existing bearer bindings shall be re-evaluated. The re-evaluation may, for a service data flow, require a new binding with another IP-CAN bearer.

Requirements specific for each type of IP-CAN are defined in the IP-CAN specific Annex. The Bearer Binding Function may also be located in the PCRF as specified in Annex D (e.g. for GPRS running UE only IP-CAN bearer establishment mode). Selection of the Bearer Binding location shall be based on the Bearer Control Mode selected by the PCRF.

Editor's Note: SA2 is still working on access specific binding mechanisms, the content of this clause and the related annexes may need to be updated based on the final outcome of SA2 work.

If the Bearer Binding function is located at the PCRF, the PCRF shall compare the TFT(s) of all IP-CAN bearer(s) within the IP-CAN session received via PCEF from the UE with the existing service data flow filter information. The PCRF shall indicate to the PCEF the IP-CAN bearer within the IP-CAN session where the PCC Rules shall be installed, modified or removed. This is done including the Bearer-Identifier AVP together with the associated PCC Rules within the corresponding RAR and/or CCA commands.

- When the PCRF does not require additional filter information coming from the UE in order to decide on bearer binding, the PCRF shall supply the PCC rules to be installed over the Gx interface to the PCEF within a RAR command.

- Otherwise, the PCRF shall wait for the PCEF requesting a policy decision for the establishment of a new IP-CAN bearer or the modification of an existing one within a CCR command over the Gx interface.

- In GPRS access when the PCEF reports the bearer event, it shall include within the CCR command a bearer reference together with the new or modified TFT information, the QoS class identifier and associated bitrates for new or modified PDP-Contexts.

6 QoS Parameters Mapping

6.1 Overview

Several QoS parameters mapping functions are needed during PCC interaction. These functions are located at the AF, PCRF, PCEF and UE. The main purpose of these mapping functions is the conversion of QoS parameters from one format to another. Examples of QoS information are:

- Parts of a session description language (SDI), e.g. SDP.

- IP QoS parameters.

- Access specific QoS parameters.

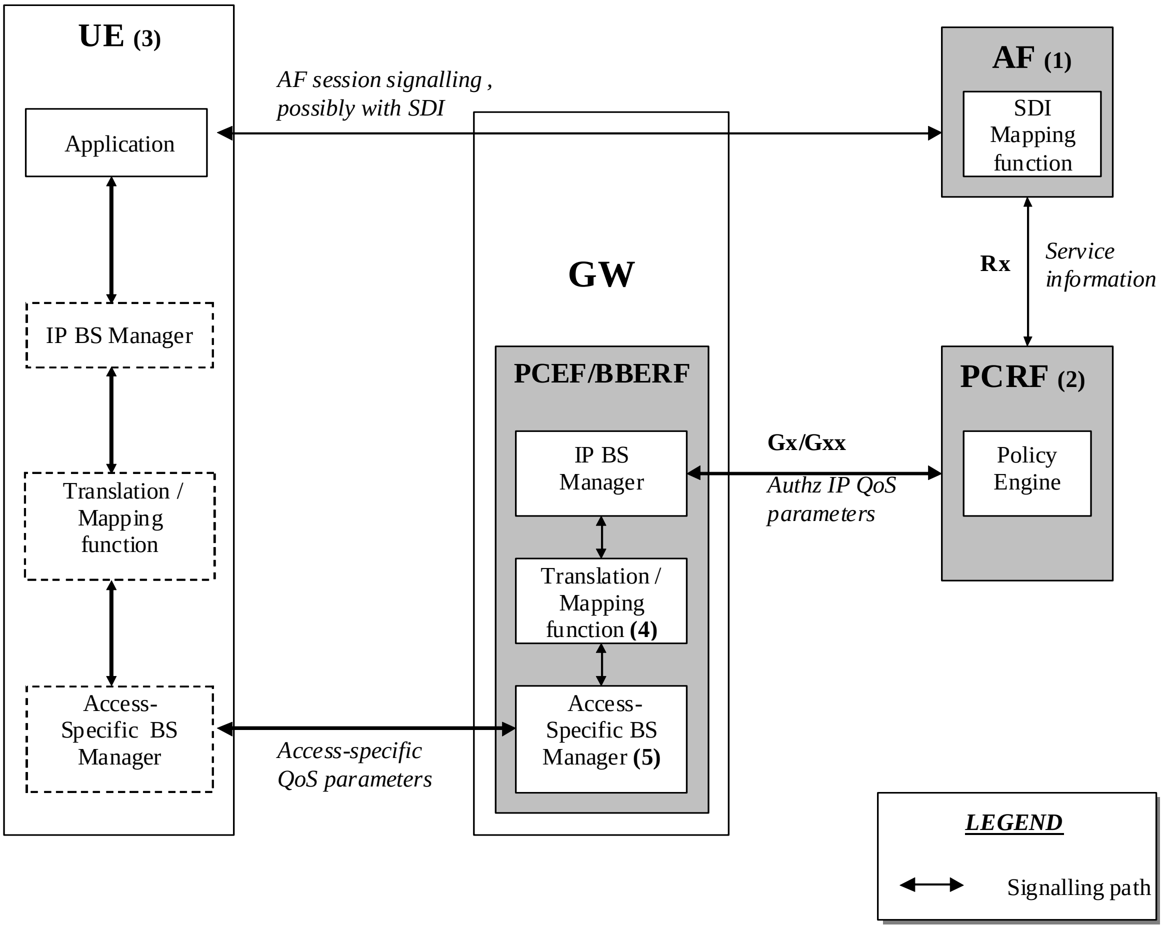
One QoS mapping function is located at the AF, which maps the application specific information into the appropriate AVPs that are carried over the Rx interface.The AF derives information about the service from the SDI or from other sources. The mapping is application specific. If SDP (IETF RFC 2327[11]) is used as SDI, the AF should apply the mapping described in Clause 6.2. For IMS, the mapping rules in Clause 6.2 shall be used at the P-CSCF. The AF passes service information to the PCRF over the Rx interface. Clause 6.2 specifies the QoS parameter mapping functions at the AF applicable for all IMS P-CSCFs regardless of the access technology.

One QoS mapping function is located at the PCRF, which maps the service information received over the Rx interface into IP QoS parameters (e.g. QCI, GBR, MBR, ARP, …). This mapping is access independent. Clause 6.3 specifies the QoS mapping functions at the PCRF applicable for all accesses.

The other mapping functions located at PCEF, BBERF, and UE are implementation dependent and are not specified within this specification except for GPRS case.

The PCRF notes and authorizes the IP flows described within this service information by mapping from service information to Authorized IP QoS parameters for transfer to the PCEF/BBERF via the Gx/Gxx interface. Both the PCEF and BBERF will map from the Authorized IP QoS parameters to the access specific QoS parameters. For GPRS, the GGSN acting as PCEF will map from the Authorized IP QoS parameters to the Authorized UMTS QoS parameters.

The general QoS mapping framework is shown in figure 6.1.1.



NOTE 1: The AF can derive the Service information from the AF session signalling.
NOTE 2: Service Information on Rx interface to Authorized IP QoS parameters mapping.
NOTE 3: For the UE initiated bearer setup, the UE may derive IP QoS parameters, requested Access-Specific QoS parameters mapping and Authorized Access-Specific QoS parameters from the AF session signalling.
NOTE 4: Authorized IP QoS parameters to Authorized Access-Specific QoS parameters mapping.
NOTE 5: Access Specific QoS parameters with Authorized Access-Specific QoS parameters comparison.

Figure 6.1.1: Framework for QoS mapping

6.1.1 UE-Initiated IP-CAN bearers

This clause covers the case where the UE is capable to initiate/modify the IP-CAN bearers sending requests to the PCEF/BBERF. When a UE desires to establish/modify an IP-CAN bearer the following steps are followed:

1. The AF can map from SDI within the AF session signalling to service information passed to the PCRF over the Rx interface. (see clause 6.2).

2. The PCRF shall map from the service information received over the Rx interface to the Authorized IP QoS parameters that shall be passed to the PCEF/BBERF via the Gx/Gxx interface. The mapping is performed for each IP flow. Upon a request from the PCEF/BBERF, the PCRF combines per direction the individual Authorized IP QoS parameters per flow (see clause 6.3).

3. The UE derives access specific QoS parameters, e.g. UMTS QoS parameters, and, if an IP BS manager is present, IP QoS parameters from the AF session signalling in an application specific manner. The IP and access specific QoS parameters should be generated according to application demands.

   For GPRS, the recommendations for conversational (3GPP TS 26.236 [7]) or streaming applications (3GPP TS 26.234 [6]) should also be taken into account when the UE derives the IP and UMTS QoS parameters. If SDP is used as SDI, e.g. for IMS, the UE should apply clause 6.5.1.and should also apply mapping rules for the authorised QoS parameters in clause 6.5.2 to derive the maximum values for the different requested bit rates and traffic classes. In case the UE multiplexes several IP flows onto the same PDP Context, it has to combine their IP and UMTS QoS parameters. If an IP BS manager is present, the Translation/Mapping function maps the IP QoS parameters to the corresponding UMTS QoS parameters.

4. The PCEF/BBERF shall map from the Authorized IP QoS parameters received from PCRF to the Authorized access specific QoS parameters.

   For GPRS. the GGSN shall map to the Authorized UMTS QoS parameters (see clause 6.4.1.1).

5. The PCEF/BBERF shall compare the requested access specific QoS parameters against the authorized access specific QoS parameters.

   For GPRS, the GGSN shall compare the UMTS QoS parameters of the PDP context against the Authorized UMTS QoS parameters (see clause 6.4.1.2).

The mapping that takes place in the UE and the network should be compatible in order to ensure that the PCEF will be able to correctly authorize the session.

Figure 6.1.1.1 shows the different kind of QoS parameters in the different points of QoS mapping figure. Due to the UE requests, there are bidirectional flows between the UE and the PCRF.

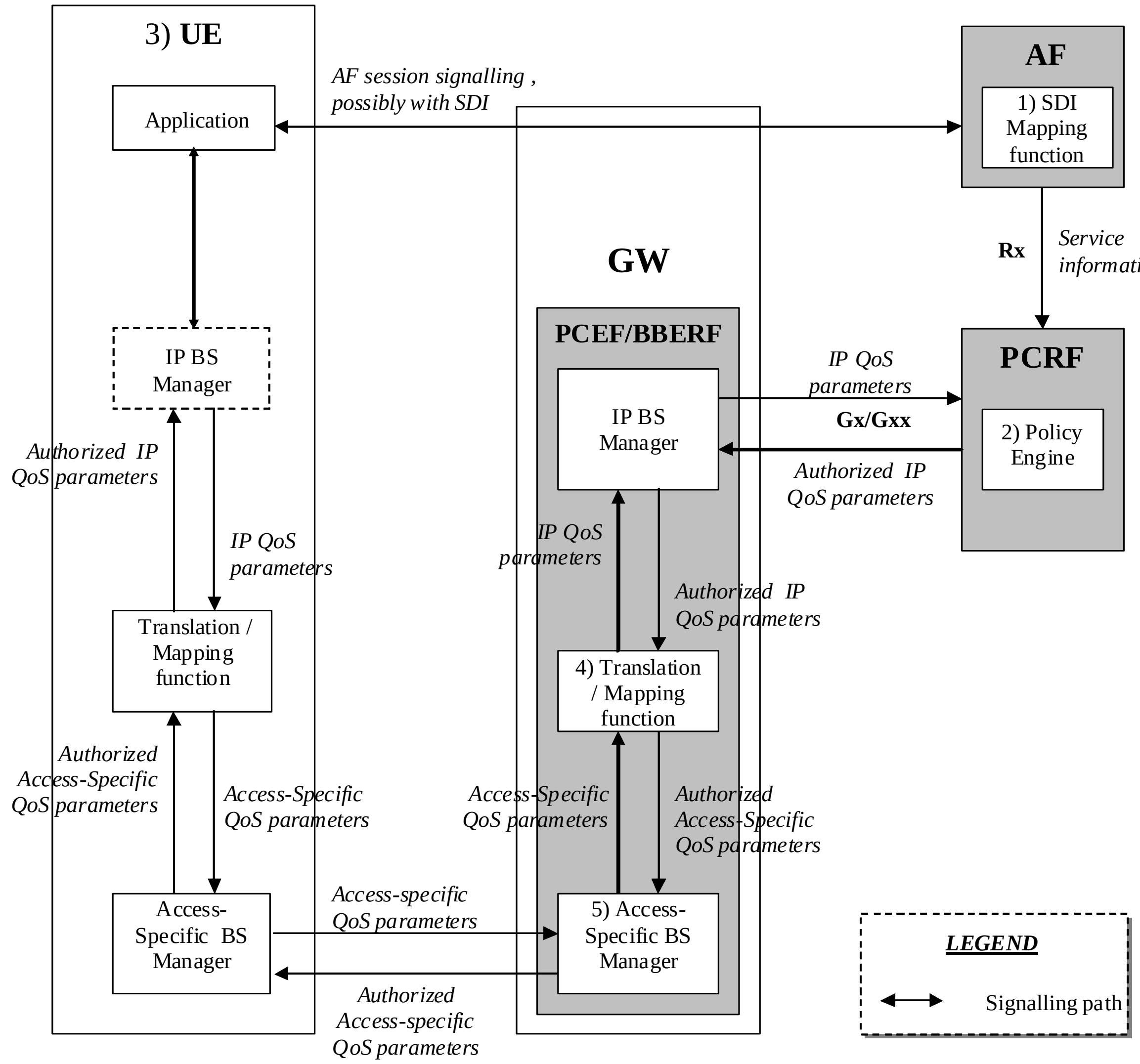


Figure 6.1.1.1: QoS mapping for UE initiated IP CAN bearers

6.1.2 Network-Initiated IP-CAN bearers

When the IP-CAN session supports Network-Initiated bearers, the network sets up IP CAN bearer(s) with a suitable QoS. If the type of IP CAN supports such an indication, the network indicates to the terminal the QoS characteristics of those IP-CAN bearer(s). Therefore the flow of QoS related information will be unidirectional as indicated in the figure 6.1.2.1.

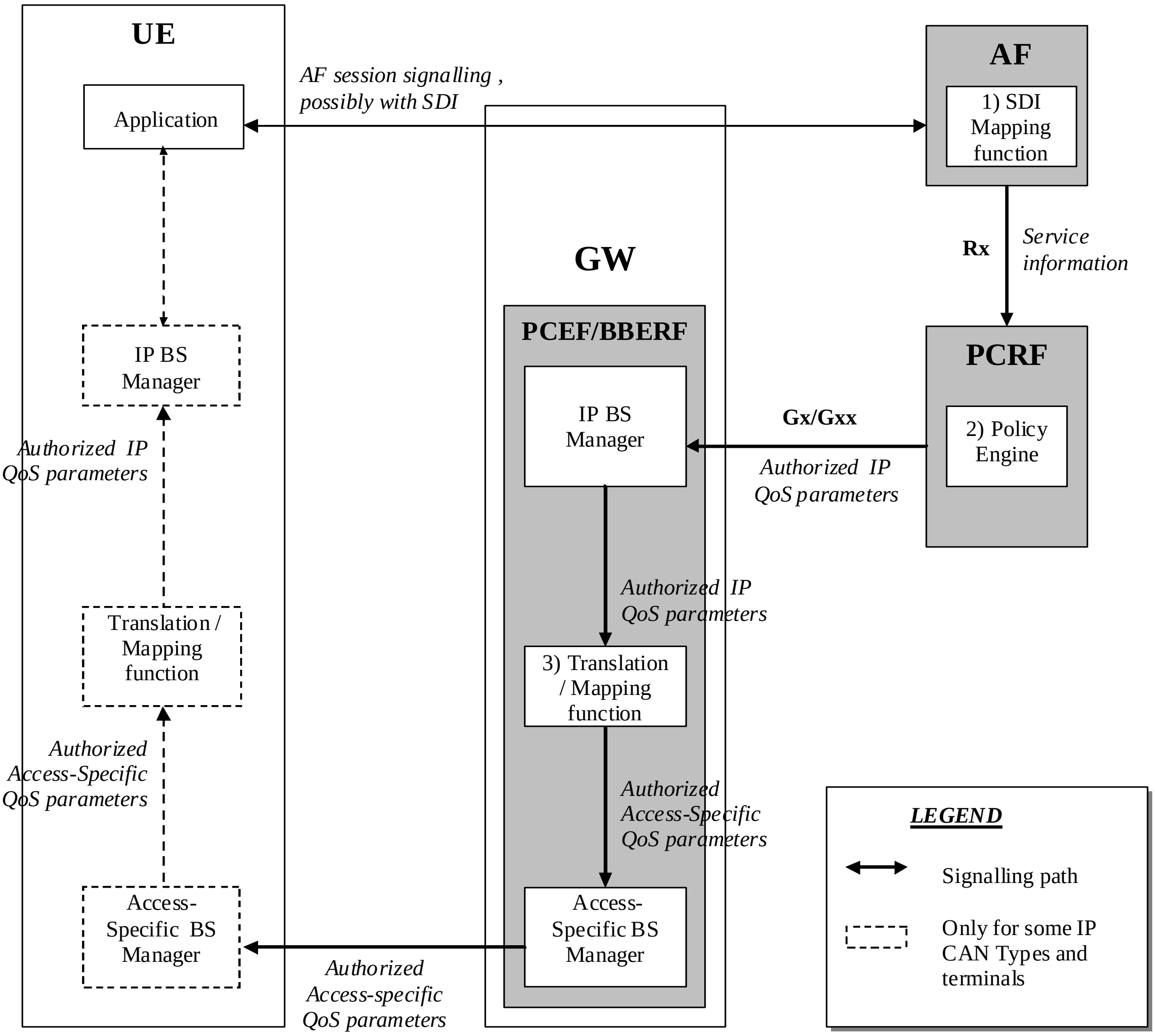


Figure 6.1.2.1: QoS mapping for network initiated IP CAN bearers

1. The AF can map from SDI within the AF session signalling to service information passed to the PCRF over the Rx interface (see clause 6.2).

2. The PCRF shall map from the service information received over the Rx interface to the Authorized IP QoS parameters that shall be passed to the PCEF/BBERF via the Gx/Gxx interface. The mapping is performed for each IP flow. Upon a request from the PCEF/BBERF, the PCRF combines per direction the individual Authorized IP QoS parameters per flow (see clause 6.3).

3. The PCEF/BBERF shall map from the Authorized IP QoS parameters received from PCRF to the access specific QoS parameters. For GPRS. the GGSN shall map to the UMTS QoS parameters (see clause 6.4.1.1).

6.2 QoS parameter mapping Functions at AF

The mapping described in this clause is mandatory for the P-CSCF and should also be applied by other AFs if the SDI is SDP.

When a session is initiated or modified the P-CSCF shall use the mapping rules in table 6.2.1 for each SDP media component to derive a Media-Component-Description AVP from the SDP Parameters.

Table 6.2.1: Rules for derivation of service information within Media-Component-Description AVP from SDP media component

<table>
<tr><th>service information per Media-Component-Description AVP
(see notes 1 and 7)</th><th>Derivation from SDP Parameters
(see note 2)</th></tr>
<tr><td>Media-Component-Number</td><td>ordinal number of the position of the "m=" line in the SDP</td></tr>
<tr><td>AF-Application-Identifier</td><td>The AF-Application-Identifier AVP may be supplied or omitted, depending on the application.
For IMS, if the AF-Application-Identifier AVP is supplied, its value should not demand application specific bandwidth or QoS class handling unless the IMS application is capable of handling a QoS downgrading.</td></tr>
<tr><td>Media-Type</td><td>The Media Type AVP shall be included with the same value as supplied for the media type in the "m=" line.</td></tr>
<tr><td>Flow-Status</td><td><pre>IF port in m-line = 0 THEN
    Flow-Status:= REMOVED;
ELSE
  IF Transport in m-line is "TCP" or " TCP/MSRP" THEN (NOTE 9)
     Flow-Status := ENABLED;
  ELSE /* UDP or RTP/AVP transport
   IF a=recvonly THEN
      IF <SDP direction> = UE originated (NOTE 8) THEN
             Flow-Status := ENABLED_DOWNLINK; (NOTE 4)
      ELSE /* UE terminated (NOTE 8) */
             Flow-Status := ENABLED_UPLINK; (NOTE 4)
      ENDIF;
   ELSE
      IF a=sendonly THEN
            IF <SDP direction> = UE originated (NOTE 8) THEN
                  Flow-Status := ENABLED_UPLINK; (NOTE 4)
            ELSE /* UE terminated (NOTE 8) */
                  Flow-Status := ENABLED_DOWNLINK; (NOTE 4)
            ENDIF;
      ELSE
          IF a=inactive THEN
               Flow-Status :=DISABLED;
          ELSE /* a=sendrecv or no direction attribute */
               Flow-Status := ENABLED (NOTE 4)
          ENDIF;
      ENDIF;
   ENDIF;
  ENDIF;
ENDIF;
(NOTE 5)</pre></td></tr>
<tr><td>Max-Requested-Bandwidth-UL</td><td><pre>IF <SDP direction> = UE terminated (NOTE 8) THEN
   IF Transport in m-line is "TCP" or " TCP/MSRP" THEN (NOTE 9)
      IF a=recvonly or a=sendrecv or no direction attribute THEN
         IF b=AS:<bandwidth> is present THEN
            Max-Requested-Bandwidth-UL:= <bandwidth> * 1000; /* Unit bit/s
         ELSE
            Max-Requested-Bandwidth-UL:= <Operator specific setting>;
         ENDIF;
      ELSE
         Max-Requested-Bandwidth-UL:= <Operator specific setting>, (NOTE 10)
      ENDIF;
   ELSE /* UDP or RTP/AVP transport
      IF b=AS:<bandwidth> is present THEN
         Max-Requested-Bandwidth-UL:= <bandwidth> * 1000; /* Unit is bit/s
      ELSE
         Max-Requested-Bandwidth-UL:= <Operator specific setting>,
         or AVP not supplied;
      ENDIF;
   ENDIF
ELSE
   Consider SDP in opposite direction
ENDIF</pre></td></tr>
<tr><td>Max-Requested-Bandwidth-DL</td><td><pre>IF <SDP direction> = UE originated (NOTE 8) THEN
   IF Transport in m-line is "TCP" or " TCP/MSRP" THEN (NOTE 9)
      IF a=recvonly or a=sendrecv or no direction attribute THEN
         IF b=AS:<bandwidth> is present THEN
            Max-Requested-Bandwidth-DL:= <bandwidth> * 1000; /* Unit bit/s
         ELSE
            Max-Requested-Bandwidth-DL:= <Operator specific setting>;
         ENDIF;
      ELSE
         Max-Requested-Bandwidth-DL:= <Operator specific setting>, (NOTE 10)</pre></td></tr>
</table>

service information per Media-Component-Description AVP (see notes 1 and 7)	Derivation from SDP Parameters (see note 2)

	ENDIF;
	ELSE /* UDP or RTP/AVP transport
	IF b=AS:<bandwidth> is present THEN
	Max-Requested-Bandwidth-DL:= <bandwidth> * 1000; /* Unit is bit/s
	ELSE
	Max-Requested-Bandwidth-DL:= <Operator specific setting>,
	or AVP not supplied;
	ENDIF;
	ENDIF
	ELSE
	Consider SDP in opposite direction
	ENDIF

RR-Bandwidth	IF b=RR:<bandwidth> is present THEN
	RR-Bandwidth:= <bandwidth>;
	ELSE
	AVP not supplied
	ENDIF;
	(NOTE 3; NOTE 6)

RS-Bandwidth	IF b=RS:<bandwidth> is present THEN
	RS-Bandwidth:= <bandwidth>;
	ELSE
	AVP not supplied
	ENDIF;
	(NOTE 3: NOTE 6)

Media-Sub-Component	Supply one AVP for bidirectional combination of two corresponding IP flows, if available, and for each single IP flow without a corresponding IP flow in opposite direction. The encoding of the AVP is described in Table 6.2.2
Reservation-Priority	The AF may supply or ommit this AVP.
Codec-Data	Codec Data AVP(s) are provisioned as specified in Clause 5.3.16 of 3GPP TS 29.214 [10], including the codec-related information detailed in Clause 5.3.7 of 3GPP TS 29.214 [10].

NOTE 1: The encoding of the service information is defined in 3GPP TS 29.214 [10].

NOTE 2: The SDP parameters are described in RFC 2327 [11].

NOTE 3: The 'b=RS:' and 'b=RR:' SDP bandwidth modifiers are defined in RFC 3556 [13].

NOTE 4: As an operator policy to disable forward and/or backward early media, for media with UDP as transport protocol only the Flow-Status may be downgraded before a SIP dialogue is established, i.e. until a 200 OK(INVITE) is received. The Value "DISABLED" may be used instead of the Values "ENABLED_UPLINK" or "ENABLED_DOWNLINK". The Values "DISABLED", "ENABLED_UPLINK" or "ENABLED_DOWNLINK" may be used instead of the Value "ENABLED".

NOTE 5: If the SDP answer is available when the session information is derived, the direction attributes and port number from the SDP answer shall be used to derive the flow status. However, to enable interoperability with SIP clients that do not understand the inactive SDP attribute, if a=inactive was supplied in the SDP offer, this shall be used to derive the flow status. If the SDP answer is not available when the session information is derived, the direction attributes from the SDP offer shall be used.

NOTE 6: Information from the SDP answer is applicable, if available.

NOTE 7: The AVPs may be omitted if they have been supplied in previous service information and have not changed, as detailed in 3GPP TS 29.214 [10].

NOTE 8: "Uplink SDP" indicates that the SDP was received from the UE and sent to the network. This is equivalent to <SDP direction> = UE originated.
"Downlink SDP" indicates that the SDP was received from the network and sent to the UE. This is equivalent to <SDP direction> = UE terminated.

NOTE 9: Support for TCP at a P-CSCF acting as AF is only required if services with TCP transport are used in the corresponding IMS system.
As an operator policy to disable forward and/or backward early media, for media with TCP as transport protocol, the Max-Requested-Bandwidth-UL/DL values may be downgraded before a SIP dialogue is established, i.e. until a 200 OK(INVITE) is received. Only a small bandwidth in both directions is required in this case in order for TCP control packets to flow.

NOTE 10: TCP uses IP flows in the directionality opposite to the transferred media for feedback. To enable these flows, a small bandwidth in this direction is required.

Table 6.2.2: Rules for derivation of Media-Sub-Component AVP from SDP media component

service information per Media-Sub-Component AVP (see notes 1 and 5)	Derivation from SDP Parameters (see note 2)
Flow-Number	The AF shall assign a number to the media-subcomponent AVP that is unique within the surrounding media component AVP and for the entire lifetime of the AF session. The AF shall select the ordinal number of the IP flow(s) within the "m=" line assigned in the order of increasing downlink destination port numbers, if downlink destination port numbers are available. For uplink or inactive unicast media IP flows, a downlink destination port number is nevertheless available, if SDP offer-answer according to RFC 3264 is used. The AF shall select the ordinal number of the IP flow(s) within the "m=" line assigned in the order of increasing uplink destination port numbers, if no downlink destination port numbers are available.
Flow-Status	AVP not supplied
Max-Requested-Bandwidth-UL	AVP not supplied
Max-Requested-Bandwidth-DL	AVP not supplied

Flow-Description	For uplink and downlink direction, a Flow-Description AVP shall be provided unless no IP Flows in this direction are described within the media component.
	
	If UDP is used as transport protocol, the SDP direction attribute (NOTE 4) indicates the direction of the media IP flows within the media component as follows:
	IF a=recvonly THEN (NOTE 3)
	IF <SDP direction> = UE originated (NOTE 7) THEN
	Provide only downlink Flow-Description AVP
	ELSE /* UE terminated (NOTE 7) */
	Provide only uplink Flow-Description AVP
	ENDIF;
	ELSE
	IF a=sendonly THEN (NOTE 3)
	IF <SDP direction> = UE originated (NOTE 7) THEN
	Provide only uplink Flow-Description AVP
	ELSE /* UE terminated (NOTE 7) */
	Provide only downlink Flow-Description AVP
	ENDIF;
	ELSE /* a=sendrecv or a=inactive or no direction attribute */
	Provide uplink and downlink Flow-Description AVPs
	ENDIF;
	ENDIF;
	However, for RTCP IP flows uplink and downlink Flow-Description AVPs shall be provided irrespective of the SDP direction attribute.
	
	If TCP is used as transport protocol (NOTE 8), IP flows in uplink and downlink direction are described in SDP irrespective of the SDP direction attribute, as TCP uses an IP flow for feedback even if contents are transferred only in the opposite direction. Thus, both uplink and downlink Flow-Description AVPs shall be provided.
	
	The uplink destination address shall be copied from the "c=" line of downlink SDP. (NOTE 6) (NOTE 7)
	The uplink destination port shall be derived from the "m=" line of downlink SDP. (NOTE 6) (NOTE 7) However, for TCP transport the uplink destination port shall be wildcarded, if the local UE is the passive endpoint (NOTE 9)
	
	The downlink destination address shall be copied from the "c=" line of uplink SDP. (NOTE 6)
	The downlink destination port shall be derived from the "m=" line of uplink SDP. (NOTE 6) (NOTE 7) However, for TCP transport the downlink destination port shall be wildcarded, if the local UE is the active endpoint (NOTE 9).
	
	For IPv6, uplink and downlink source addresses shall either be derived from the prefix of the destination address or be wildcarded by setting to "any", as specified in 3GPP TS 29.214 [10]. If IPv4 is being utilized, the uplink source address shall either be set to the address contained in the "c=" line of the uplink SDP or be wildcared, and the downlink source address shall either be set to the address contained in the "c=" line of the downlink SDP or be wildcarded. However, for TCP transport, if the local UE is the passive endpoint (NOTE 9), the uplink source address shall not be wildcarded. If the local UE is the active endpoint (NOTE 9), the downlink source address shall

service information per Media-Sub-Component AVP (see notes 1 and 5)	Derivation from SDP Parameters (see note 2)
	not be wildcarded. Source ports shall not be supplied. However, for TCP transport, if the local UE is the passive end point (NOTE 9), the uplink source port shall be derived from the "m=" line of the uplink SDP. If the local UE is the active end point (NOTE 9), the downlink source port shall be derived from the "m=" line of the downlink SDP. Proto shall be derived from the transport of the "m=" line. For "RTP/AVP" proto is 17(UDP). For "TCP", as defined in RFC 4145 [16], or " TCP/MSRP", as defined in RFC 4975 [17], proto is 6(TCP).
Flow-Usage	The Flow-Usage AVP shall be supplied with value "RTCP" if the IP flow(s) described in the Media-Sub-Component AVP are used to transport RTCP. Otherwise the Flow-Usage AVP shall not be supplied. RFC 2327 [11] specifies how RTCP flows are described within SDP. If the IP flows(s) are used to transport signaling the value should be "AF-SIGNALLING"
NOTE 1: The encoding of the service information is defined in 3GPP TS 29.214 [10]. NOTE 2: The SDP parameters are described in RFC 2327 [11]. NOTE 3: If the SDP direction attribute for the media component negotiated in a previous offer-answer exchange was sendrecv, or if no direction attribute was provided, and the new SDP direction attribute sendonly or recvonly is negotiated in a subsequent SDP offer-answer exchange, uplink and downlink Flow-Description AVPs shall be supplied. NOTE 4: If the SDP answer is available when the session information is derived, the direction attributes from the SDP answer shall be used to derive the flow description. However, to enable interoperability with SIP clients that do not understand the inactive SDP attribute, if a=inactive was supplied in the SDP offer, this shall be used. If the SDP answer is not available when the session information is derived, the direction attributes from the SDP offer shall be used. NOTE 5: The AVPs may be omitted if they have been supplied in previous service information and have not changed, as detailed in 3GPP TS 29.214 [10]. NOTE 6: If the session information is derived from an SDP offer, the required SDP may not yet be available. The corresponding Flow Description AVP shall nethertheless be included and the unavailable fields (possibly all) shall be wildcarded. NOTE 7: "Uplink SDP" indicates that the SDP was received from the UE and sent to the network. This is equivalent to <SDP direction> = UE originated. "Downlink SDP" indicates that the SDP was received from the network and sent to the UE. This is equivalent to <SDP direction> = UE terminated. NOTE 8: Support for TCP at a P-CSCF acting as AF is only required if services with TCP transport are used in the corresponding IMS system. NOTE 9: For TCP transport, the passive endpoints is derived from the SDP "a:setup" attribute according to the rules in RFC 4145 [16], or, if that attribute is not present, from the rules in RFC 4975 [17].	

6.3 QoS parameter mapping Functions at PCRF

The QoS authorization process consists of the derivation of the parameters Authorized QoS Class Identifier (QCI), Allocation and Retention Priority (ARP), and Authorized Maximum/Guaranteed Data Rate UL/DL.

When a session is initiated or modified the PCRF shall derive Authorized IP QoS parameters (i.e. QCI, Authorized Maximum/Guaranteed Data Rate DL/UL, ARP) from the service information. If the selected Bearer Control Mode (BCM) is UE-only this process shall be performed according to the mapping rules in table 6.3.1 to avoid undesired misalignments with the UE QoS parameters mapping.

In the case of forking, the various forked responses may have different QoS requirements for the IP flows of the same media component. Each Authorized IP QoS Parameter should be set to the highest value requested for the IP flow(s) of that media component by any of the active forked responses.

Table 6.3.1: Rules for derivation of the Maximum Authorized Data Rates, Authorized Guaranteed Data Rates and Maximum Authorized QoS Class per IP flow or bidirectional combination of IP flows in the PCRF

Authorized IP QoS Parameter	Derivation from service information (see note 4)

Maximum Authorized Data Rate DL (Max_DR_DL) and UL (Max_DR_UL)	IF operator special policy exists THEN
	
	Max_DR_UL:= as defined by operator specific algorithm;
	Max_DR_DL:= as defined by operator specific algorithm;
	
	ELSE
	
	IF AF-Application-Identifier AVP demands application specific data rate handling THEN
	Max_DR_UL:= as defined by application specific algorithm;
	Max_DR_DL:= as defined by application specific algorithm;
	
	ELSE IF Codec-Data AVP provides Codec information for a codec that is supported by a specific algorithm THEN
	Max_DR_UL:= as defined by specific algorithm;
	Max_DR_DL:= as defined by specific algorithm;
	
	ELSE
	IF not RTCP flow(s) according to Flow-Usage AVP THEN
	IF Flow-Status = REMOVED THEN
	Max_DR_UL:= 0;
	Max_DR_DL:= 0;
	
	ELSE
	IF uplink Flow Desription AVP is supplied THEN
	IF Max-Requested-Bandwidth-UL is present THEN
	Max_DR_UL:= Max-Requested-Bandwidth-UL ;
	ELSE
	Max_DR_UL:= as set by the operator;
	ENDIF;
	
	ELSE
	Max_DR_UL:= 0;
	
	ENDIF;
	
	IF downlink Flow Desription AVPs is supplied THEN
	IF Max-Requested-Bandwidth-DL is present THEN
	Max_DR_DL:= Max-Requested-Bandwidth-DL;
	
	ELSE
	Max_DR_DL:= as set by the operator;
	ENDIF;
	
	ELSE
	Max_DR_DL:= 0;
	
	ENDIF;
	ENDIF;
	
	ELSE /* RTCP IP flow(s) */
	IF RS-Bandwidth is present and RR-Bandwidth is present THEN
	Max_DR_UL:= (RS-Bandwidth + RR-Bandwidth);
	Max_DR_DL:= (RS-Bandwidth + RR-Bandwidth);
	ELSE
	IF Max-Requested-Bandwidth-UL is present THEN
	IF RS-Bandwidth is present and RR-Bandwidth is not present THEN
	Max_DR_UL:= MAX[0.05 * Max-Requested-Bandwidth-UL,RS-Bandwidth];
	ENDIF;
	
	IF RS-Bandwidth is not present and RR-Bandwidth is present THEN
	Max_DR_UL:= MAX[0.05 * Max-Requested-Bandwidth-UL,RR-Bandwidth];
	ENDIF;
	
	IF RS-Bandwidth and RR-Bandwidth are not present THEN
	Max_DR_UL:= 0.05 * Max-Requested-Bandwidth_UL ;
	ENDIF;
	
	ELSE
	Max_DR_UL:= as set by the operator;

<table>
<tr><th>Authorized IP QoS Parameter</th><th>Derivation from service information (see note 4)</th></tr>
<tr><td></td><td><pre>
        ENDIF;

        IF Max-Requested-Bandwidth-DL is present THEN
          IF RS-Bandwidth is present and RR-Bandwidth is not present THEN
            Max_DR_DL:= MAX[0.05 * Max-Requested-Bandwidth-DL,RS-Bandwidth];
          ENDIF;

          IF RS-Bandwidth is not present and RR-Bandwidth is present THEN
            Max_DR_DL:= MAX[0.05 * Max-Requested-Bandwidth-DL,RR-Bandwidth];
          ENDIF;

          IF RS-Bandwidth and RR-Bandwidth are not present THEN
            Max_DR_DL:= 0.05 * Max-Requested-Bandwidth-DL;
          ENDIF;

        ELSE
          Max_DR_DL:= as set by the operator;

        ENDIF;

      ENDIF;
    ENDIF;
  ENDIF;

ENDIF;

IF SIP-Forking-Indication AVP indicates SEVERAL_DIALOGUES THEN
   Max_DR_UL = MAX[Max_DR_UL, previous Max_DR_UL]
   Max_DR_DL = MAX[Max_DR_DL, previous Max_DR_DL]
ENDIF;
</pre></td></tr>
</table>

Authorized IP QoS Parameter	Derivation from service information (see note 4)

Authorized Guaranteed Data Rate DL (Gua_DR_DL) and UL (Gua_DR_UL)	IF operator special policy exists THEN
	Gua_DR_UL:= as defined by operator specific algorithm;
	Gua_DR_DL:= as defined by operator specific algorithm;
	
	ELSE
	IF AF-Application-Identifier AVP demands application specific data rate handling THEN
	Gua_DR_UL:= as defined by application specific algorithm;
	Gua_DR_DL:= as defined by application specific algorithm;
	
	ELSE IF Codec-Data AVP provides Codec information for a codec that is supported by a specific algorithm (NOTE 5)THEN
	Gua_DR_UL:= as defined by specific algorithm;
	Gua_DR_DL:= as defined by specific algorithm;
	
	ELSE
	Gua_DR_UL:= Max DR UL;
	Gua_DR_DL:= Max DR DL;
	
	ENDIF;
	
	ENDIF;
	
	IF SIP-Forking-Indication AVP indicates SEVERAL_DIALOGUES THEN
	Gua_DR_UL = MAX[Gua_DR_UL, previous Gua_DR_UL]
	Gua_DR_DL = MAX[Gua_DR_DL, previous Gua_DR_DL]
	ENDIF;

Authorized QoS Class Identifier [QCI] (see notes 1, 2, 3 and 7)	IF a operator special policy exists THEN
	QCI:= as defined by operator specific algorithm;
	
	ELSE
	IF AF-Application-Identifier AVP demands application specific QoS Class handling THEN
	QCI:= as defined by application specific algorithm;
	
	ELSE IF Codec-Data AVP provides Codec information for a codec that is supported by a specific algorithm THEN
	QCI:= as defined by specific algorithm; (NOTE 5)
	ELSE
	IF Media-Type is present THEN
	/* for GPRS: streaming */
	IF (only uplink Flow Description AVPs are supplied for all IP flows of the AF session, which have media type "audio" or "video" and no flow usage "RTCP", or
	only downlink Flow Desription AVPs are supplied for all IP flows of the AF session, which have media type "audio" or "video" and no flow usage "RTCP") THEN
	CASE Media-Type OF
	"audio": MaxClassDerivation := 3 OR 4; (NOTE 9)
	"video": MaxClassDerivation := 4
	END;
	
	/* for GPRS: conversational */
	ELSE
	CASE Media-Type OF
	"audio": MaxClassDerivation:= 1 OR 2; (NOTE 6)
	"video": MaxClassDerivation:= 2
	END;
	
	ENDIF;
	
	CASE Media-Type OF
	"audio": QCI := MaxClassDerivation
	"video": QCI := MaxClassDerivation
	"application": QCI := 1 OR 2; (NOTE 6)
	/*e.g. for GPRS: conversational*/
	"data": QCI := 6 OR 7 OR 8; (NOTE 8)
	/*e.g. for GPRS: interactive with prio 1, 2 AND 3 respectively*/
	"control": QCI := 6;
	/*e.g. for GPRS: interactive with priority 1*/
	
	/* NOTE: include new media types here */

Authorized IP QoS Parameter	Derivation from service information (see note 4)

	`OTHERWISE:      QCI := 9;`
	`   /*e.g. for GPRS: background*/`
	
	`  END;`
	` ENDIF;`
	`ENDIF;`
	
	`IF SIP-Forking-Indication AVP indicates SEVERAL_DIALOGUES THEN`
	`   QCI = MAX[QCI, previous QCI](Note 10)`
	`ENDIF;`

NOTE 1: The QCI assigned to a RTCP IP flow is the same as for the corresponding RTP media IP flow. NOTE 2: When audio or video IP flow(s) are removed from a session, the parameter MaxClassDerivation shall keep the originally assigned value. NOTE 3: When audio or video IP flow(s) are added to a session, the PCRF shall derive the parameter MaxClassDerivation taking into account the already existing media IP flow(s) within the session. NOTE 4: The encoding of the service information is defined in 3GPP TS 29.214 [10]. If AVPs are omitted within a Media-Component-Description AVP or Media-Sub-Component AVP of the service information, the corresponding information from previous service information shall be used, as specified in 3GPP TS 29.214 [10]. NOTE 5: 3GPP TS 26.234 [6] , 3GPP TS 26.236 [7] , 3GPP2 C.S0046 [18], and 3GPP2 C.S0055 [19] contain examples of QoS parameters for codecs of interest. The support of any codec specific algorithm in the PCRF is optional. NOTE 6: The final QCI value will depend on the value of SSID (speech/unknown) according to 3GPP TS 23.107 [4]. If the PCRF is not able to determine the SSID, it should use the QCI value 2 that correspons to SSID unknown. For UE-init and mixed mode, the PCRF may derive from the requested QoS of an IP CAN bearer which SSID is applicable. NOTE 7: The numeric value of the QCI are based on 3GPP TS 29.212 [9]. NOTE 8: The QCI value also encodes the traffic handling priority for GPRS. If the PCRF is not able to determine a traffic handling priority, it should choose QCI 8 that corresponds to priority 3. Also, for UE-initiated bearers the PCRF should only use QCI 8 in order to have the same mapping rules in both UE and PCRF. NOTE 9: The final QCI value will depend on the value of SSID (speech/unknown) according to 3GPP TS 23.107 [4]. If the PCRF is not able to determine the SSID, it should use the QCI value 4 that corresponds to SSID unknown. For UE-init and mixed mode, the PCRF may derive from the requested QoS of an IP CAN bearer which SSID is applicable. NOTE 10: The Max function shall use the following precedence order for the QCI values: 2 > 1 > 4 > 3 > 5 > 6 > 7 > 8 > 9	

The PCRF should per ongoing session store the Authorized IP QoS parameters per for each IP flow or bidirectional combination of IP flows (as described within a Media Subcomponent AVP).

If the PCRF provides a QoS-Information AVP within a Charging-Rule-Definition AVP it may apply the rules in table 6.3.2 to combine the Authorized QoS per IP flow or bidirectional combination of IP flows (as derived according to table 6.3.1) for all IP flows described by the corresponding PCC rule.

If the PCRF provides a QoS-Information AVP for an entire IP CAN bearer (for a UE-initiated IP-CAN bearer in the GPRS case) or IP CAN session, it may apply the rules in table 6.3.2 to combine the Authorized QoS per IP flow or bidirectional combination of IP flows (as derived according to table 6.3.1) for all IP flows allowed to be transported within the IP CAN bearer or session. It is recommended that the rules in table 6.3.2 are applied for all IP flows with corresponding AF session. The PCRF may increase the authorized QoS further to take into account the requirements of predefined PCC rules without ongoing AF sessions.

NOTE: QoS-Information AVP provided at IP-CAN session level is not derived based on mapping tables, but based on subscription and operator specific policies.

NOTE: Allocation-Retention-Priority AVP is always calculated at PCC rule level according to table 6.3.2.

For a UE initiated PDP context within GPRS, the PCRF applies the binding mechanism described in Clause 5 to decide which flows are allowed to be transported within the IP CAN bearer.

Table 6.3.2: Rules for calculating the Maximum Authorized/Guaranteed Data Rates, QCI and ARP in the PCRF

Authorized IP QoS Parameter	Calculation Rule

Maximum Authorized Data Rate DL and UL	Maximum Authorized Data Rate DL/UL is the sum of all Maximum Authorized Data Rate DL/UL for all the IP flows or bidirectional combinations of IP flows (as according to table 6.3.1).
	
	IF Network = GPRS AND Maximum Authorized Data Rate DL/UL > 256 Mbps THEN
	   Maximum Authorized Data Rate DL/UL = 256 Mbps /* See 3GPP TS 23.107 [4] */
	ENDIF;

Guaranteed Authorized Data Rate DL and UL	Guaranteed Authorized Data Rate DL/UL is the sum of all Guaranteed Authorized Data Rate DL/UL for all the IP flows or bidirectional combinations of IP flows (as according to table 6.3.1).
QCI	QCI = MAX [needed QoS parameters per IP flow or bidirectional combination of IP flows (as operator's defined criteria) among all the IP flows or bidirectional combinations of IP flows.]

ARP	IF a operator special policy exists THEN
	  ARP:= as defined by operator specific algorithm;
	
	ELSE
	  IF AF-Application-Identifier AVP demands application specific ARP handling THEN
	    ARP:= as defined by application specific algorithm;
	  ENDIF;
	ELSE
	  IF Reservation-Priority AVP demands application specific ARP handling THEN
	    ARP:= as defined by application specific algorithm;
	  ENDIF;
	
	ENDIF;

6.4 QoS parameter mapping Functions at PCEF

6.4.1 GPRS

6.4.1.1 Authorized IP QoS parameters per PDP Context to Authorized UMTS QoS parameters mapping in GGSN

The Translation/Mapping function in the GGSN shall derive the Authorized UMTS QoS parameters from the Authorized IP QoS parameters received from the PCRF according to the rules in table 6.4.1.

Table 6.4.1: Rules for derivation of the Authorized UMTS QoS Parameters per PDP context from the Authorized IP QoS Parameters in GGSN

<table>
<tr><th>Authorized UMTS QoS Parameter per PDP context</th><th>Derivation from Authorized IP QoS Parameters</th></tr>
<tr><td>Maximum Authorized Bandwidth DL and UL per PDP context</td><td><pre>Maximum Authorized Bandwidth DL/UL per PDP context = Maximum Authorized Data Rate DL/UL</pre></td></tr>
<tr><td>Guaranteed Authorized Data Rate DL and UL per PDP context</td><td><pre>Guaranteed Authorized Data Rate DL/UL per PDP context = Guaranteed Authorized Data Rate DL/UL</pre></td></tr>
<tr><td>Maximum Authorized Traffic Class per PDP context</td><td><pre>IF QCI = 1 OR 2 THEN
     Maximum Authorized Traffic Class = "Conversational"

ELSEIF QCI = 3 OR 4 THEN
     Maximum Authorized Traffic Class = "Streaming"

ELSEIF QCI = 5 OR 6 OR 7 OR 8 THEN
     Maximum Authorized Traffic Class = "Interactive";

ELSE Maximum Authorized Traffic Class = "Background"
ENDIF ;</pre></td></tr>
<tr><td>Traffic Handling Priority</td><td><pre>IF QCI = 5 OR 6 THEN
     Maximum Authorized Traffic Handling Priority = "1";

ELSE IF QCI = 7 THEN
     Maximum Authorized Traffic Handling Priority = "2";

ELSE IF QCI = 8 THEN
     Maximum Authorized Traffic Handling Priority = "3";

ELSE the GGSN shall not derive Traffic Handling Priority

ENDIF ;</pre></td></tr>
<tr><td>Signalling Indication</td><td><pre>IF QCI = 5 THEN
     Signalling Indication = "Yes";

ELSE IF QCI = 6 OR 7 OR 8 THEN
     Signalling Indication = "No";

ELSE the GGSN shall not derive Signalling Indication

ENDIF ;</pre></td></tr>
<tr><td>Source Statistics Descriptor</td><td><pre>IF QCI = (1 OR 3) THEN
     Source Statistics Descriptor = "speech";

ELSE IF QCI = 2 OR 4 THEN
     Source Statistics Descriptor = "unknown";

ELSE the GGSN shall not derive Source Statistics Descriptor

ENDIF ;</pre></td></tr>
</table>

6.4.1.2 Comparing UMTS QoS Parameters against the Authorized UMTS QoS parameters in GGSN for UE initiated PDP context

Upon receiving a PDP context activation, the GGSN requests PCC rules from the PCRF (see 3GPP TS 29.212 [9] for details). The PCRF may supply Authorized UMTS QoS Parameters per PDP context together with the PCC rules. The GGSN maps the Authorized IP QoS parameters per PDP Context to Authorized UMTS QoS parameters according to clause 6.4.1.1 and then compares the requested UMTS QoS parameters against the corresponding Authorized UMTS QoS parameters. The following criteria shall be fulfilled:

- If the requested Guaranteed Bitrate DL/UL (if the requested Traffic Class is Conversational or Streaming) is equal to the Authorized Guaranteed data rate DL/UL; and

- the requested Maximum Bitrate DL/UL (if the requested Traffic Class is Interactive or Background) is equal to Maximum Authorized data rate DL/UL; and

- the requested Traffic Class is equal to Maximum Authorized Traffic Class.

Then, the GGSN shall accept the PDP context activation or modification with the UE requested parameters.Otherwise, the GGSN is adjusted (downgrade or upgrade) the requested UMTS QoS parameters to the values that were authorized.

6.5 QoS parameter mapping Functions at UE for a UE-initiated GPRS PDP Context

Figure 6.5.1 indicates the entities participating in the generation of the requested QoS parameters when the UE activates or modifies a PDP Context. The steps are:

1. The Application provides the UMTS BS Manager, possibly via the IP BS Manager and the Translation/Mapping function, with relevant information to perform step 2 or step 4. (Not subject to standardization within 3GPP).

2. If needed, information from step 1 is used to access a proper set of UMTS QoS Parameters. See 3GPP TS 26.236 [7] for Conversational Codec Applications and 3GPP TS 26.234 [6] for Streaming Codec Applications.

3. If SDP is available then the SDP Parameters should give guidance for the UMTS BS Manager (possibly via the IP Manager and the Translation/Mapping function) ,according to the rules in clause 6.5.1, to set the Maximum Bitrate UL/DL and the Guaranteed Bitrate UL/DL. Furthermore the Maximum Authorized Bandwidth UL/DL and Maximum Authorised Traffic Class should be derived according to the rules in clause 6.5.2.

4. A set of UMTS QoS Parameters values from step 2 (or directly from step 1) is possibly merged together with the Maximum Bitrate UL/DL and the Guaranteed Bitrate UL/DL from step 3. The result should constitute the requested UMTS QoS Parameters. The UE should check that the requested Guaranteed Bitrate UL/DL or requested Maximum Bitrate UL/DL (depending on the requested Traffic Class) does not exceed the Maximum Authorized Bandwidth UL/DL derived in step 3. Furthermore, if the UE has implemented the mapping rule for Maximum Authorized Traffic Class, as defined in clause 6.5.2, the UE should check that the requested Traffic Class does not exceed the Maximum Authorised Traffic Class derived in step 3.

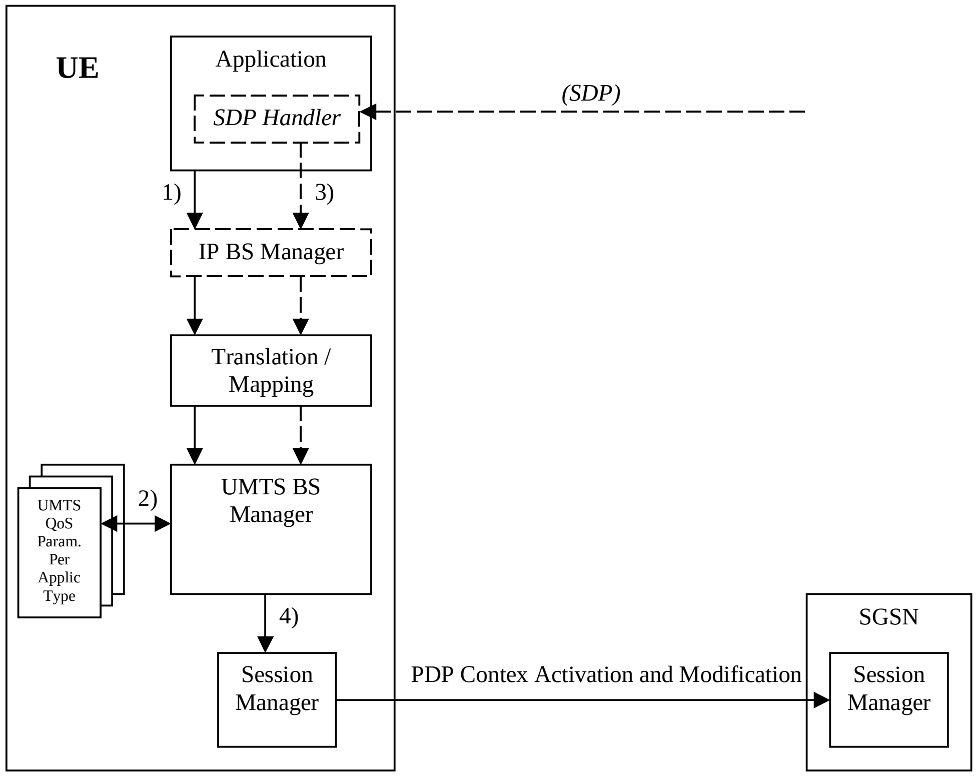


Figure 6.5.1: Framework for generating requested QoS parameters in the UE

6.5.1 SDP to UMTS QoS parameter mapping in UE

If SDP Parameters are available, then before activating or modifying a PDP Context the UE should check if the SDP Parameters give guidance for setting the requested UMTS QoS Parameters. The UE should use the mapping rule in table 6.5.1.1 to derive the Maximum and Guaranteed Bitrate DL/UL from the SDP Parameters.

Table 6.5.1.1: Recommended rules for derivation of the requested Maximum and Guaranteed Bitrate DL/UL per media component in the UE

UMTS QoS Parameter per media component	Derivation from SDP Parameters

Maximum Bitrate DL/UL and Guaranteed Bitrate DL/UL per media component	`/* Check if the media use codec(s) */`
	`IF [(<media> = ("audio" or "video")) and (<transport> = "RTP/AVP")] THEN`
	
	`    /* Check if Streaming */`
	`    IF a= ("sendonly" or "recvonly") THEN`
	`        Maximum Bitrate DL/UL and Guaranteed Bitrate DL/UL per media component as specified in reference [6] ;`
	`    /* Conversational as default !*/`
	`    ELSE`
	`        Maximum Bitrate DL/UL and Guaranteed Bitrate DL/UL per media component as specified in reference [7] ;`
	`    ENDIF ;`
	
	`/* Check for presence of bandwidth attribute for each media component */`
	`ELSEIF b=AS:<bandwidth-value> is present THEN`
	`    IF media stream only downlink THEN`
	`        Maximum Bitrate DL = Guaranteed Bitrate DL =<bandwidth-value >;`
	`    ELSEIF mediastream only uplink THEN`
	`        Maximum Bitrate UL = Guaranteed Bitrate UL =<bandwidth-value >;`
	`    ELSEIF mediastreams both downlink and uplink THEN`
	`        Maximum Bitrate DL = Guaranteed Bitrate DL =<bandwidth-value >;`
	`        Maximum Bitrate UL = Guaranteed Bitrate UL =<bandwidth-value >;`
	`    ENDIF;`
	`ELSE`
	
	`/* SDP does not give any guidance ! */`
	`Maximum Bitrate DL/UL and Guaranteed Bitrate DL/UL per media component as specified by the UE manufacturer;`
	`ENDIF ;`

6.5.2 SDP parameters to Authorized UMTS QoS parameters mapping in UE

If the PDP Context is activated or modified the UE should use the mapping rules in table 6.5.2.1 for all applications using SDP to derive the Maximum Authorized Bandwidth UL/DL per IP flow or bidirectional combinations of IP flows.

Table 6.5.2.1 also has a mapping rule for derivation of Maximum Authorized Traffic Class per IP flow or bidirectional combinations of IP flows which applies for session initiation and modification.

In future releases this mapping rule may change.

In the case of forking, the various forked responses may have different QoS requirements for the same IP flows of a media component. When the Authorized UMTS QoS Parameters are used by the UE, they shall be set equal to the highest values requested for the IP flows of that media component by any of the active forked responses. The UE should use the mapping rule in table 6.5.2.1 for each forked response.

Table 6.5.2.1: Rules for derivation of the Maximum Authorized Bandwidth DL/UL and the Maximum Authorized Traffic Class per IP flow or bidirectional combination of IP flows in the UE

Authorized UMTS QoS Parameter	Derivation from SDP Parameters (see note 4)

Maximum Authorized Bandwidth DL (Max_BW_DL) and UL (Max_BW_UL) (see NOTE 5)	IF a=recvonly THEN
	IF <SDP direction> = mobile originated THEN
	Direction:= downlink;
	
	ELSE /* mobile terminated */
	Direction:= uplink;
	ENDIF;
	
	ELSE /* a!= recvonly */
	IF a=sendonly THEN
	IF <SDP direction> = mobile originated THEN
	Direction: = uplink;
	ELSE /* mobile terminated */
	Direction:= downlink;
	ENDIF;
	ELSE /*sendrecv, inactive or no direction attribute*/
	Direction:=both;
	
	ENDIF;
	
	ENDIF;
	
	/* Max_BW_UL and Max_BW_DL */
	
	IF media IP flow(s) THEN
	IF b_{AS}=AS:<bandwidth> is present THEN
	IF Direction=downlink THEN
	Max_BW_UL:= 0;
	Max_BW_DL:= b_{AS};
	
	ELSE
	IF Direction=uplink THEN
	Max_BW_UL:= b_{AS};
	Max_BW_DL:= 0;
	
	ELSE /*Direction=both*/
	Max_BW_UL:= b_{AS};
	Max_BW_DL:= b_{AS};
	ENDIF;
	
	ENDIF;
	
	ELSE
	bw:= as set by the UE manufacturer;
	IF Direction=downlink THEN
	Max_BW_UL:= 0;
	Max_BW_DL:= bw;
	
	ELSE
	IF Direction=uplink THEN
	Max_BW_UL:= bw;
	Max_BW_DL:= 0;
	
	ELSE /*Direction=both*/
	Max_BW_UL:= bw;
	Max_BW_DL:= bw;
	
	ENDIF;
	
	ENDIF;
	ENDIF;
	
	ELSE /* RTCP IP flow(s) */
	IF b_{RS}=RS:<bandwidth> and b_{RR}=RR:<bandwidth> is present THEN
	Max_BW_UL:= (b_{RS} + b_{RR}) / 1000;
	Max_BW_DL:= (b_{RS} + b_{RR}) / 1000;
	ELSE
	IF b_{AS}=AS:<bandwidth> is present THEN
	IF b_{RS}=RS:<bandwidth> is present and b_{RR}=RR:<bandwidth> is not present THEN
	Max_BW_UL:= MAX[0.05 * b_{AS}, b_{RS} / 1000];
	Max_BW_DL:= MAX[0.05 * b_{AS}, b_{RS} / 1000];

Authorized UMTS QoS Parameter	Derivation from SDP Parameters (see note 4)

	ENDIF;
	
	IF b_{RS}=RS:<bandwidth> is not present and b_{RR}=RR:<bandwidth> is present THEN
	Max_BW_UL:= MAX[0.05 * b_{AS}, b_{RR} / 1000];
	Max_BW_DL:= MAX[0.05 * b_{AS}, b_{RR} / 1000];
	ENDIF;
	
	IF b_{RS}=RS:<bandwidth> and b_{RR}=RR:<bandwidth> is not present THEN
	Max_BW_UL:= 0.05 * b_{AS};
	Max_BW_DL:= 0.05 * b_{AS};
	ENDIF;
	
	ELSE
	Max_BW_UL:= as set by the UE manufacture;
	Max_BW_DL:= as set by the UE manufacture;
	
	ENDIF;
	
	ENDIF;
	ENDIF;

Maximum Authorized Traffic Class [MaxTrafficClass] (see NOTE 1, 2 and3)	IF (all media IP flows of media type "audio" or "video" for the session are unidirectional and have the same direction) THEN
	MaxService:= streaming;
	ELSE
	MaxService:= conversational;
	ENDIF;
	
	CASE <media> OF
	"audio": MaxTrafficClass:= MaxService;
	"video": MaxTrafficClass:= MaxService;
	"application": MaxTrafficClass:=conversational;
	"data": MaxTrafficClass:=interactive with priority 3;
	"control": MaxTrafficClass:=interactive with priority 1;
	/*new media type*/
	OTHERWISE: MaxTrafficClass:=background;
	END;

NOTE 1: The Maximum Authorized Traffic Class for a RTCP IP flow is the same as for the corresponding RTP media IP flow.
NOTE 2: When audio or video IP flow(s) are removed from a session, the parameter MaxService shall keep the originally assigned value.
NOTE 3: When audio or video IP flow(s) are added to a session, the UE shall derive the parameter MaxService taking into account the already existing media IP flows within the session.
NOTE 4: The SDP parameters are described in RFC 2327 [11].
NOTE 5: The 'b=RS:' and 'b=RR:' SDP bandwidth modifiers are defined in RFC 3556 [13].

The UE should per ongoing session store the Authorized UMTS QoS parameters per IP flow or bidirectional combination of IP flows.

Before activating or modifying a PDP context the UE should check that the requested Guaranteed Bitrate UL/DL (if the Traffic Class is Conversational or Streaming) or the requested Maximum Bitrate UL/DL (if the Traffic Class is Interactive or Background) does not exceed the Maximum Authorized Bandwidth UL/DL per PDP context (calculated according to the rule in table 6.5.2.2). If the requested Guaranteed Bitrate UL/DL or the requested Maximum Bitrate UL/DL exceeds the Maximum Authorized Bandwidth UL/DL per PDP context, the UE should reduce the requested Guaranteed Bitrate UL/DL or the requested Maximum Bitrate UL/DL to the Maximum Authorized Bandwidth UL/DL per PDP context. Furthermore, if the rule in table 6.5.2.1 for calculating Traffic Class per IP flow or bdirectional combination of IP flows is implemented, the UE should check that the requested UMTS QoS parameter Traffic Class does not exceed the Maximum Authorized Traffic Class per PDP context (calculated according to the rule in table 6.5.2.2). If the requested UMTS QoS parameter Traffic Class exceeds the Maximum Authorized Traffic Class per PDP context, the UE should reduce the requested UMTS QoS parameter Traffic Class to the Maximum Authorized Traffic Class per PDP context.

Table 6.5.2.2: Rules for calculating the Maximum Authorized Bandwidths and Maximum Authorized Traffic Class per PDP Context in the UE

Authorized UMTS QoS Parameter per PDP Context	Calculation Rule

Maximum Authorized Bandwidth DL and UL per PDP Context	`Maximum Authorized Bandwidth DL/UL per PDP Context is the sum of all Maximum Authorized Bandwidth DL/UL for all the IP flows or bidirectional combinations of IP flows (as derived according to table 6.5.2.1) associated with that PDP Context ;`
	
	`IF Maximum Authorized Bandwidth DL/UL per PDP Context > 256 Mbps THEN`
	`   Maximum Authorized Bandwidth DL/UL per PDP Context = 256 Mbps`
	`   /* See  ref [4] */`
	`END;`

Maximum Authorized Traffic Class per PDP Context	`Maximum Authorised Traffic Class per PDP Context = MAX [Maximum Authorized QoS Class per IP flow or bidirectional combination of IP flows (as derived according to table 6.5.2.1) among all the IP flows or bidirectional combinations of IP flows associated with that PDP Context] ;`
	
	`(The MAX function ranks the possible Maximum Authorised Traffic Class values as follows: Conversational > Streaming > Interactive with priority 1 > Interactive with priority 2 > Interactive with priority 3 > Background)`

7 PCRF addressing

7.1 General

The PCRF discovery procedures are needed where more than one PCRF is present in an operator's network realm. Within such a deployment, an additional functional element, called DRA, is needed. PCRF discovery procedures include all the procedures that involve a DRA functional element.

Routing of Diameter messages from a network element towards the right Diameter realm in a PLMN is based on standard Diameter realm-based routing, as specified in IETF RFC 3588 [14] using the UE-NAI domain part.

The DRA keeps status of the assigned PCRF for a certain UE and IP-CAN session across all reference points, e.g. Gx, Gxx, S9 and Rx interfaces.

The DRA shall support the functionality of a proxy agent and a redirect agent as defined in RFC 3588 [14]. The mode in which it operates (i.e. proxy or redirect) shall be based on operator's requirements.

Diameter clients of the DRA, i.e. AF, PCEF, BBERF and PCRF in roaming scenarios shall support all procedures required to properly interoperate with the DRA in both the proxy and redirect modes.

NOTE: The proxy mode includes two variants:

PA1: Proxy agent based on the standard Diameter proxy agent functionality. All the messages need to go through the DRA.

PA2: Proxy agent based on the standard Diameter proxy agent functionality. Session establishment messages always go through the DRA. Gx, Gxx and S9 session termination messages always go through the DRA. All other messages bypass the DRA.

7.2 DRA Definition

The DRA (Diameter Routing Agent) is a functional element that ensures that all Diameter sessions established over the Gx, S9, Gxx and Rx reference points for a certain IP-CAN session reach the same PCRF when multiple and separately addressable PCRFs have been deployed in a Diameter realm. The DRA is not required in a network that deploys a single PCRF per Diameter realm.

7.3 DRA Procedures

7.3.1 General

A DRA implemented as a Diameter Redirect Agent or a Diameter Proxy Agent shall be compliant to IETF RFC 3588 [14], except when noted otherwise in this document.

7.3.2 DRA Information Storage

The DRA shall maintain PCRF routing information per IP-CAN session or per UE-NAI, depending on the operator's configuration.

Editor's note: It is FFS how the Diameter clients know this configuration

The DRA has information about the user identity (UE NAI), the UE IP address(es),the APN(if available)and the selected PCRF address for a certain IP-CAN Session .

The PCRF routing information stored for an IP-CAN session in the DRA shall be removed after the IP-CAN session is terminated. In case of DRA change (e.g. inter-operator handover), the information about the IP-CAN session stored in the old DRA shall be removed.

The PCRF routing information stored per UE in the DRA shall be removed when no more IP-CAN and gateway control sessions are active for the UE.

7.3.3 Capabilities Exchange

In addition to the capabilities exchange procedures defined in IETF RFC 3588 [14], the Redirect DRA and Proxy DRA shall advertise the specific applications it supports (e.g., Gx, Gxx, Rx or S9) by including the value of the application identifier in the Auth-Application-Id AVP and the value of the 3GPP (10415) in the Vendor-Id AVP of the Vendor-Specific-Application-Id AVP contained in the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands.

7.3.4 Redirect DRA

7.3.4.1 Redirecting Diameter Requests

A DRA implemented as a Diameter redirect agent shall redirect the received Diameter request message by carrying out the procedures defined in section 6.1.7 of IETF RFC 3588 [14]. The Client shall use the value within the Redirect-Host AVP of the redirect response in order to obtain the PCRF identity

Editor's Note: It is FFS if procedures are required to cover the scenario where a client cannot connect to the redirected PCRF (eg. PCRF is offline)

The DRA shall be aware of Gx and Gxx Diameter termination requests as defined in 3GPP TS 29.212 [9] in order to detect whether release of DRA bindings is required.

If the client is the AF, the DRA (redirect) does not need not to maintain Diameter sessions and Diameter Base redirect procedures are applicable. Therefore, an AF should not send an AF session termination request to the DRA

7.3.4.2 DRA binding removal

If the DRA binding is per IP-CAN session and the IP-CAN session is terminated or if the DRA binding is per UE and the last IP-CAN session is terminated (eg. from an indication by the BBERF/PCEF) the Redirect DRA shall remove the associated DRA binding information and responds with a Diameter redirect answer message.

7.3.5 Proxy DRA

The DRA shall support the functionality of a Diameter proxy agent as defined in RFC 3588 [14].

When the DRA receives a request from a client, it shall check whether it already has selected a PCRF for the UE or the UE's IP-CAN session; if it does have a PCRF already selected for that UE or UE's IP-CAN session, it shall proxy the request to the corresponding PCRF. If the request is an IP-CAN session termination or gateway control session termination, the DRA shall check whether PCRF routing information shall be removed as specified in section 7.3.x. If the DRA does not have a PCRF already selected, it shall follow one of the procedures below:

- If the request is an IP-CAN session establishment or gateway control session establishment, it shall select a PCRF to handle all sessions for that UE or UE's IP-CAN session. It shall then proxy the request to the selected PCRF.

- Otherwise, if the request is not an IP-CAN session establishment or gateway control session establishment, it shall reject the request.

Editor's note: It is FFS which error code is returned in this failure case. Either a Diameter routing error code such as DIAMETER_UNABLE_TO_DELIVER or the DRA may follow the procedures for the corresponding application and reject with the appropriate code (e.g. IP_CAN_SESSION_NOT_AVAILABLE for an Rx request).

If a DRA is deployed in a PCRF's realm, clients of the DRA shall send the first request of a session to the DRA handling the PCRF's realm. Clients of the DRA shall as well send IP-CAN session termination and gateway control termination requests to the DRA. A client of the DRA shall be capable of sending every message of a session to the DRA. A client of the DRA may be configured to bypass the DRA on session modification messages and AF session termination messages by sending these types of messages directly to the PCRF.

7.4 DRA flows

7.4.1 Proxy DRA

7.4.1.1 Establishment of Diameter Sessions

Establishment of Diameter sessions may occur at any of the following cases:

- Gateway control establishment
- IP-CAN session establishment
- AF session establishment

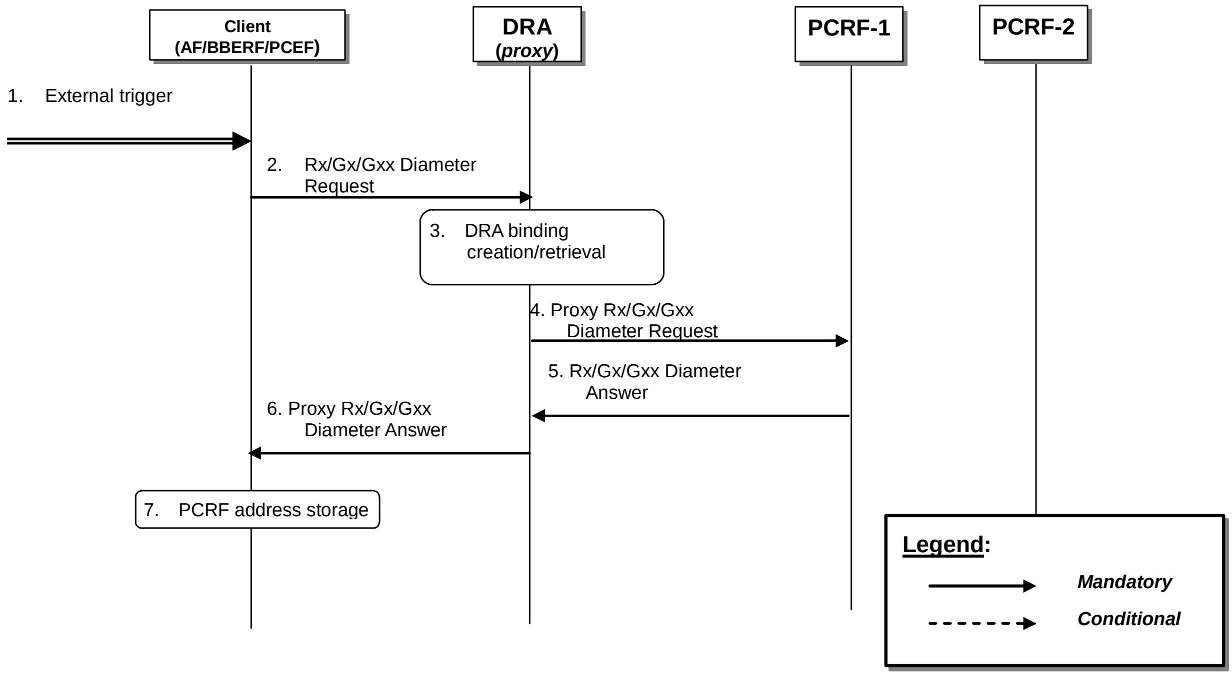


Figure 7.4.1.1.1: Establishment of Diameter sessions using DRA (proxy)

1. A Client receives an external trigger (e.g. IP-CAN session establishment request) that requires the establishment of a Diameter session with a PCRF.
2. A Diameter Request (e.g. a Diameter CCR sent by PGW to indicate establishment of an IP-CAN session as defined in clauses 4.5.1, 4a.5.1 of 3GPP TS 29.212 [9]) is sent by the Client and received by a DRA (proxy).
3. The DRA (proxy) stores the user information (e.g. UE-NAI) and checks whether an active DRA binding exists. If not the DRA creates a dynamic DRA binding (assignment of a PCRF node per UE or per IP-CAN session).
4. The DRA (proxy) proxies the Diameter Request to the target PCRF. The proxied Diameter Request maintains the same Session-Id AVP value.
5. PCRF-1 returns a Diameter Answer as defined in clauses 4.5, 4a.5 of 3GPP TS 29.212 [9] to the DRA (proxy).
6. DRA (proxy) proxies the Diameter Answer to the Client. The proxied Diameter Answer maintains the same Session-Id AVP value.
7. If PA2 option is implemented, the Client shall use the Origin-Host AVP value providing in the Diameter Answer of step 6. This value is the identity of the target PCRF. The client shall populate the Destination-Host AVP with this address and send any subsequent Diameter messages directly to this PCRF bypassing the DRA

Editor's Note: It is FFS what names will be used for PA1 and PA2 options

7.4.1.2 Modification of Diameter Sessions

7.4.1.2.1 Client-initiated

Modification of Diameter sessions may occur in any of the following cases:

- Gateway control session modification
- IP-CAN session modification
- AF session modification

If PA1 option is implemented steps 2, 3, 4, 5, 6 are only carried out. If PA2 option is implemented steps 2a, 5a are only carried out.

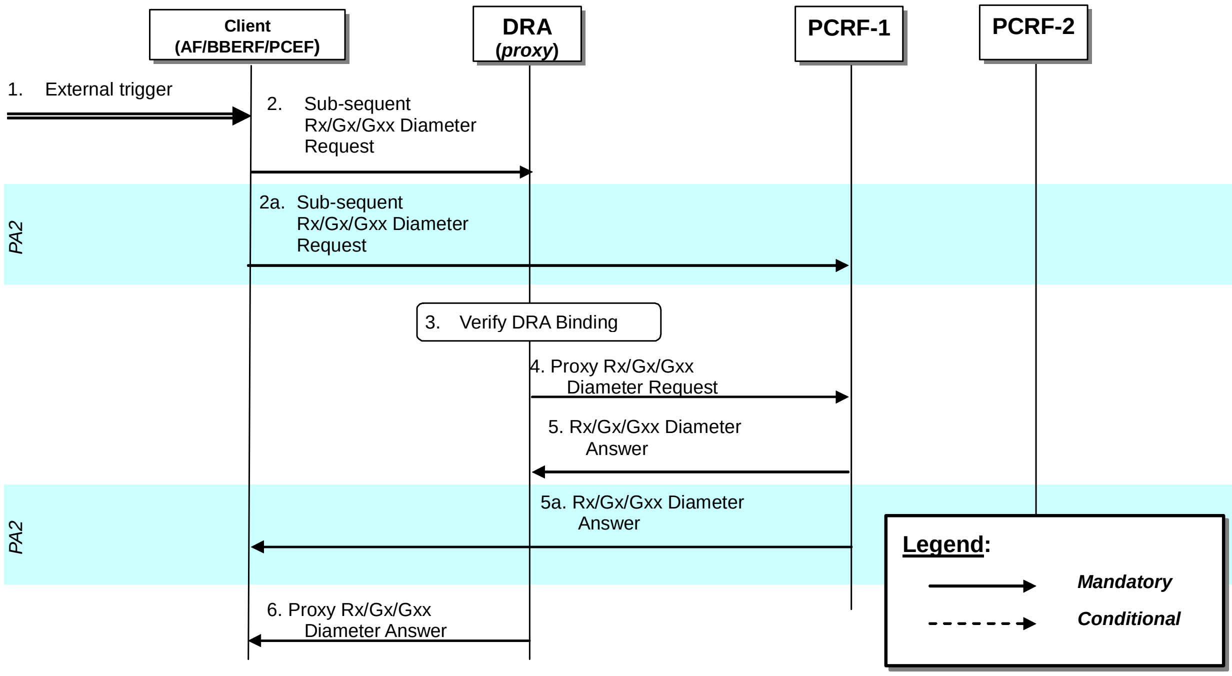


Figure 7.4.1.2.1.1: Modification of Diameter sessions through DRA (proxy)- AF/BBERF/PCEF interaction

1. A Client receives an external trigger (e.g. IP-CAN session modification) that requires a sub-sequent Diameter message to be sent to the PCRF

2. A Sub-sequent Diameter Request (e.g. a Diameter CCR sent by PGW to indicate modification of an IP-CAN session) as defined in clauses 4.5.1, 4a.5.1 of 3GPP TS 29.212 [9] or clause 4.4 of 3GPP TS 29.214 [10]) is sent by the Client and received by the DRA (proxy).

2a If PA2 option is implemented, based on Client configuration and operator policy, the Client communicates directly to the PCRF, bypassing the DRA agent, by using the PCRF identity obtained through the Origin-Host AVP (see step 7 in clause 5.2.5.7.1.1). The Client uses the same active Session-Id AVP value on the Diameter Request sent to the PCRF. In such a case steps 2, 3, 4, 5, 6 are not carried out.

3. After receiving a Diameter Request (Step 2), the DRA (proxy) verifies that there is an active DRA binding for the session identified in the request.

4. The DRA (proxy) proxies the Diameter Request to the target PCRF.

5. PCRF-1 returns a Diameter Answer as defined in clauses 4.5, 4a.5 of 3GPP TS 29.212 [9] or clause 4.4 of 3GPP TS 29.214 [10]) to the DRA (proxy).

5a Upon receiving a Diameter Request (Step 2a), PCRF-1 returns a Diameter Answer directly to the Client, bypassing the DRA (proxy).

6. DRA (proxy) proxies the Diameter Answer to the Client.

7.4.1.2.2 PCRF-initiated

Modification of Diameter sessions occur on PCRF initiated session modifications towards the clients (AF/BBERF/PCEF).

If PA1 option is implemented steps 2, 3, 4, 5, 6 are only carried out. If PA2 option is implemented steps 2a, 5a are only carried out.

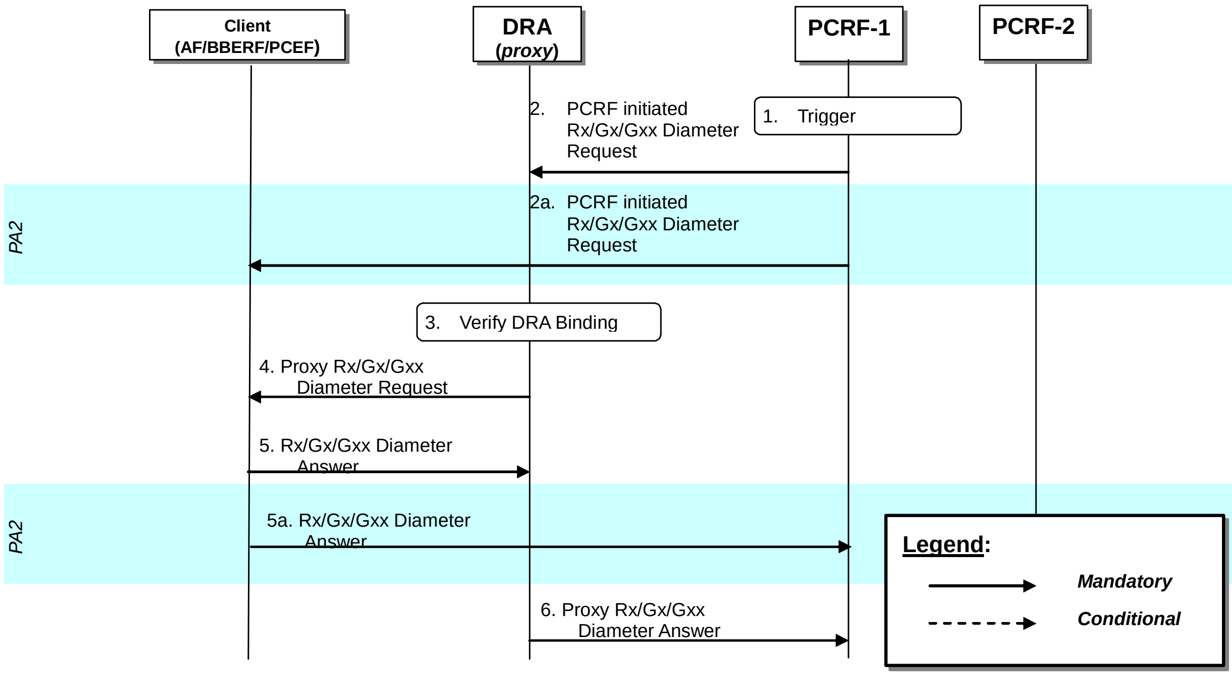


Figure 7.4.1.2.2.1: Modification of Diameter sessions through DRA (proxy)- PCRF interaction

1. PCRF receives an internal or external trigger that requires a Diameter message to be sent to the clients (either AF, BBERF, PCEF)

2. A PCRF-initiated Diameter Request (e.g. a Diameter RAR request sent to the PGW) is sent to the Clients and received by the DRA (proxy).

2a If PA2 option is implemented, the PCRF communicates directly to the client, bypassing the DRA agent. In such a case steps 2, 3, 4, 5, 6 are not carried out.

3. After receiving a Diameter Request (Step 2), the DRA (proxy) verifies that there is an active DRA binding for the session identified in the request.

4. The DRA (proxy) proxies the Diameter Request to the Client. The proxied Diameter Request maintains the same Session-Id AVP value.

5. Clients returns a Diameter Answer as defined in clauses 4.5, 4a.5 of 3GPP TS 29.212 [9] or clause 4.4 of 3GPP TS 29.214 [10]) to the DRA (proxy).

5a Upon receiving a Diameter Request (Step 2a), Client returns a Diameter Answer directly to the PCRF, bypassing the DRA (proxy).

6. DRA (proxy) proxies the Diameter Answer to the PCRF.

Editor's Note: S9 flows to be completed

7.4.1.3 Termination of Diameter Sessions

The procedures required are identical to both PA1 and PA2 options

Termination of Diameter sessions occur at the following cases:

- Gateway control session termination
- IP-CAN session termination
- AF session termination

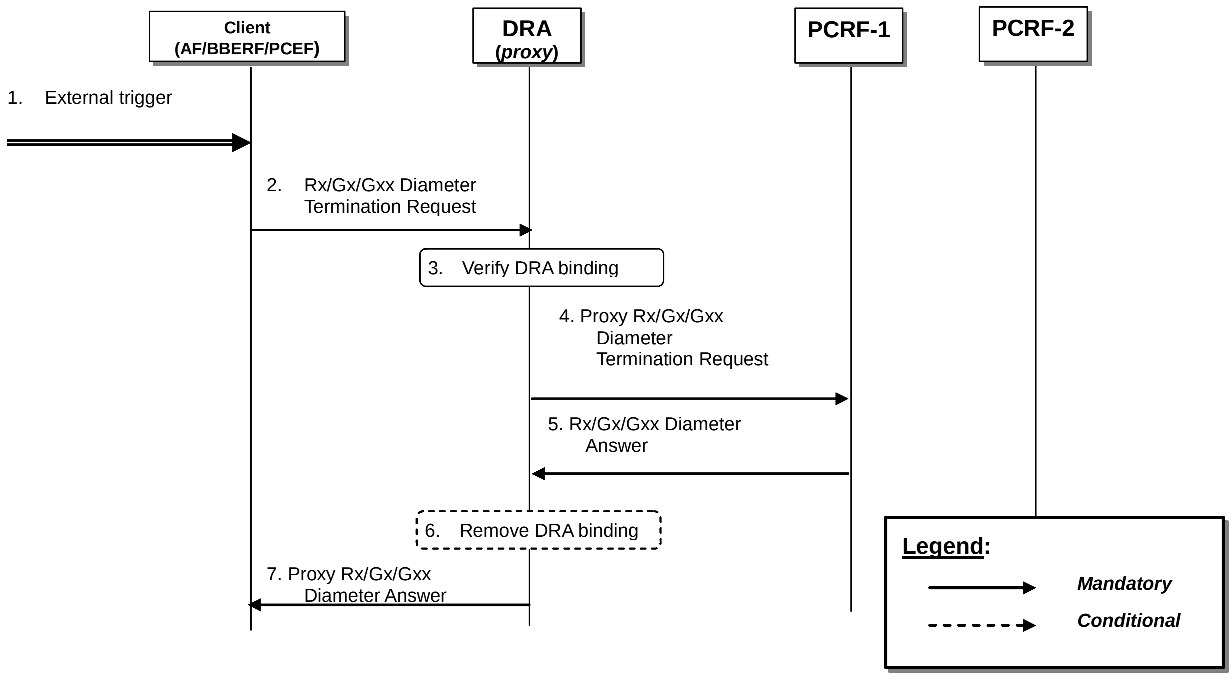


Figure 7.4.1.3.1: Termination of Diameter sessions through DRA (proxy)

1. A Client receives an external trigger (e.g., for example an IP-CAN session termination request) that requires the sending of a Diameter Termination Request.
2. A Diameter Termination Request (e.g., a Diameter CCR sent by PGW to indicate termination of an IP-CAN session) as defined in clauses 4.5, 4a.5 of 3GPP TS 29.212 [9]) is sent by the Client to the DRA (proxy).
3. The DRA (proxy) verifies that there is an active DRA binding for the IP-CAN session identified in the request.
4. The DRA (proxy) proxies the Diameter Termination Request to the target PCRF. The proxied Diameter Request maintains the same Session-Id AVP value.
5. PCRF-1 acknowledges termination of the session. PCRF-1 sends a Diameter Answer, (e.g., as defined in clauses 4.5, 4a.5 of 3GPP TS 29.212 [9]) to DRA (proxy).
6. If the DRA binding is per IP-CAN session and the IP-CAN session is terminated or if the DRA binding is per UE and the last IP-CAN session of that UE is terminated the DRA (proxy) removes the DRA binding.
7. DRA (proxy) proxies the Diameter Answer to the Client. The proxied Diameter Answer maintains the same Session-Id AVP value.

Editor's Note AF interaction with PA2 option need to be completed

7.4.2 Redirect DRA

7.4.2.1 Establishment of Diameter Sessions

Establishment of Diameter sessions may occur at the following cases:

- Gateway control session establishment
- IP-CAN session establishment

- AF session establishment

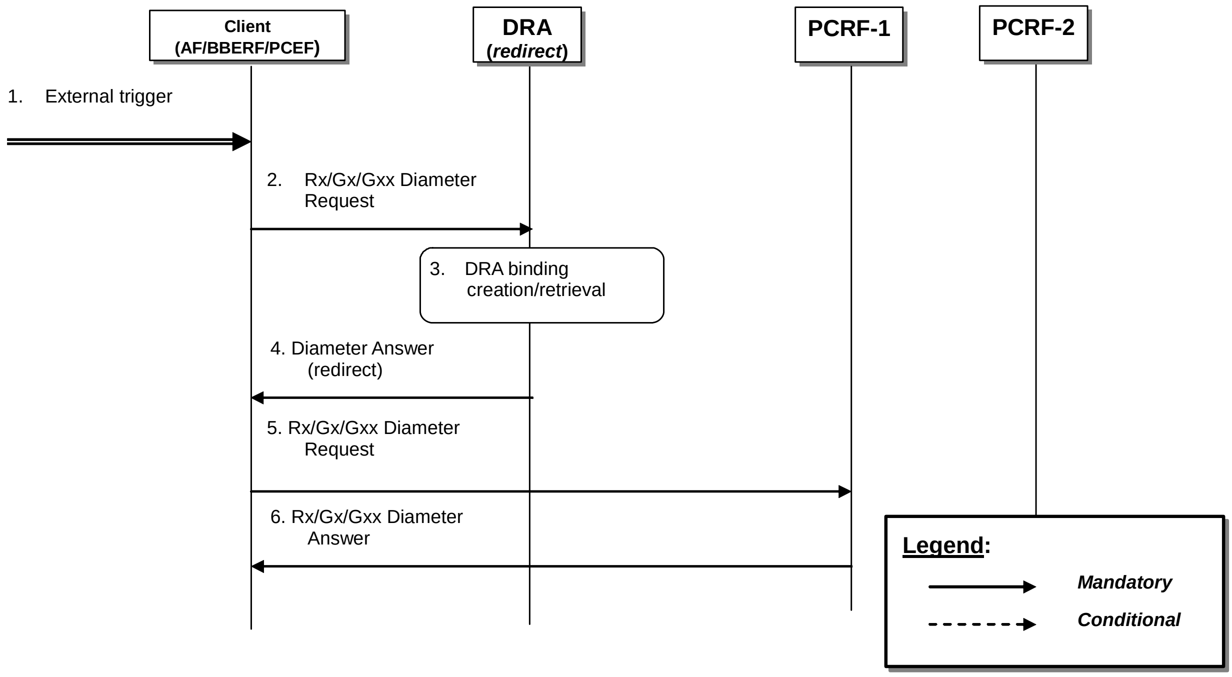


Figure 7.4.2.1: Establishment of Diameter session through DRA (redirect)

1. A Client receives an external trigger (e.g., IP-CAN session establishment request) that requires the establishment of a Diameter session with a PCRF.
2. A Diameter request (e.g., a Diameter CCR sent by PGW to indicate establishment of an IP-CAN session as defined in clauses 4.5.1, 4a.5.1 of 3GPP TS 29.212 [9]) is sent by the Client and received by the DRA (redirect).
3. The DRA (redirect) stores the user information (e.g., UE-NAI) and checks whether an active DRA binding exists. If not the DRA creates a dynamic DRA binding (assignment of a PCRF node per UE or per IP-CAN session)
4. The DRA (redirect) sends a Diameter Answer indicating redirection as defined in IETF RFC 3588 [14]. The target PCRF is included in the Redirect-Host AVP.
5. The Client re-sends the Diameter Request of step 2 to the target PCRF.
6. PCRF-1 returns a Diameter Answer, as defined in clauses 4.5, 4a.5 of 3GPP TS 29.212 [12], to the Client.

7.4.2.2 Modification of Diameter sessions

No interaction between the Clients (AF/BBERF/PCEF) and DRA (redirect) is occured

7.4.2.3 Termination of Diameter Sessions

Termination of Diameter sessions occur at the following cases:

- Gateway control session termination
- IP-CAN session termination
- AF session termination

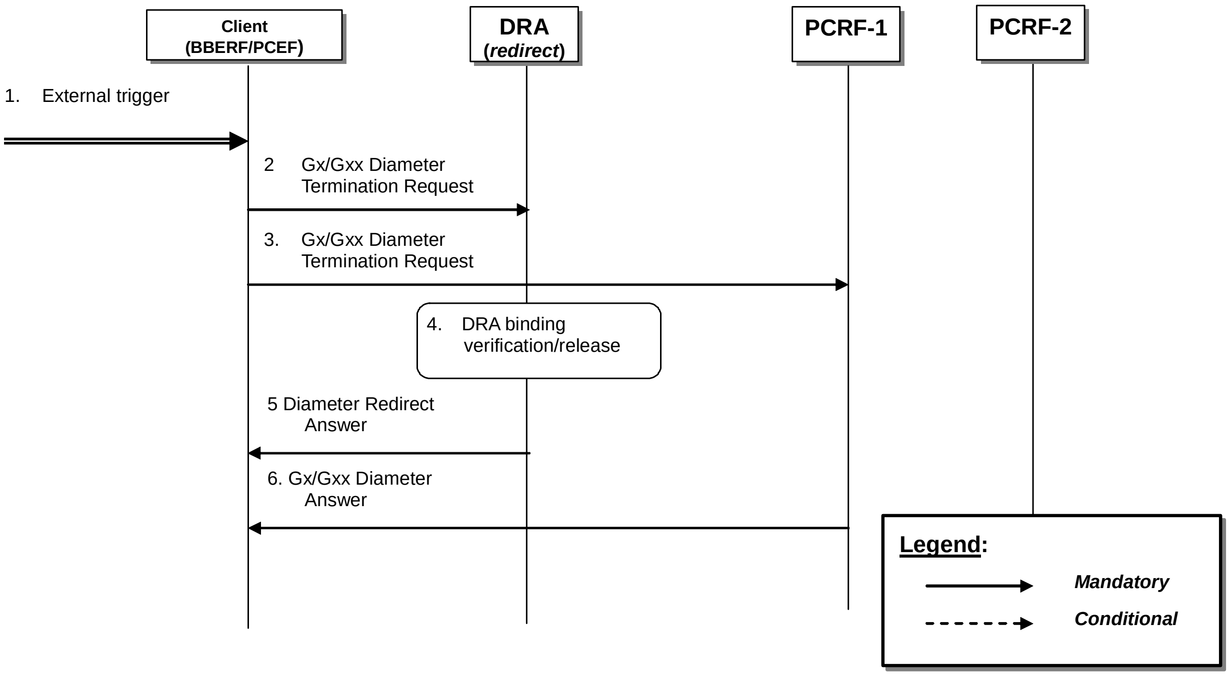


Figure 7.4.2.3.1: Termination of Diameter sessions through DRA (redirect)

1. Clients receive an external trigger (eg. IP-CAN session termination request) that triggers client to terminate Diameter session with server (i.e. PCRF)

2 A Diameter Termination Request (e.g., as defined in clauses 4.5.7 (Gx) and 4a.5.3 (Gxx) of 3GPP TS 29.212 [9]) is sent by the Client to the DRA (redirect).

3. A Diameter Termination Request (e.g., as defined in clauses 4.5.7 (Gx) and 4a.5.3 (Gxx) of 3GPP TS 29.212 [9]) is sent by the Client to PRCF-1. The message uses the same Session-Id AVP value of the active Diameter session established between the Client and PCRF-1.

NOTE: Steps 2, 3 may be carried out in parallel. Otherwise, the client after step2 may need to wait for the redirect answer before sending the Diameter termination request to the PCRF

4. DRA (redirect) verifies that there is an active DRA binding for the IP-CAN session identified in the request. If the DRA binding is per IP-CAN session and that IP-CAN session is terminated or if the DRA binding is per UE and the last IP-CAN session of that UE is terminated the DRA removes the DRA binding.

5 DRA (redirect) acknowledges termination of the session. DRA (redirect) by sending a Diameter redirect answer to the client.

6 PCRF-1 acknowledges termination of session. PCRF-1 sends a Diameter Answer (e.g., as defined in clauses 4.5.7 (Gx) and 4a.5.3 (Gxx) of 3GPP TS 29.212 [9]) to the Client.

NOTE: AF is not required to send Diameter session termination request to DRA (redirect)

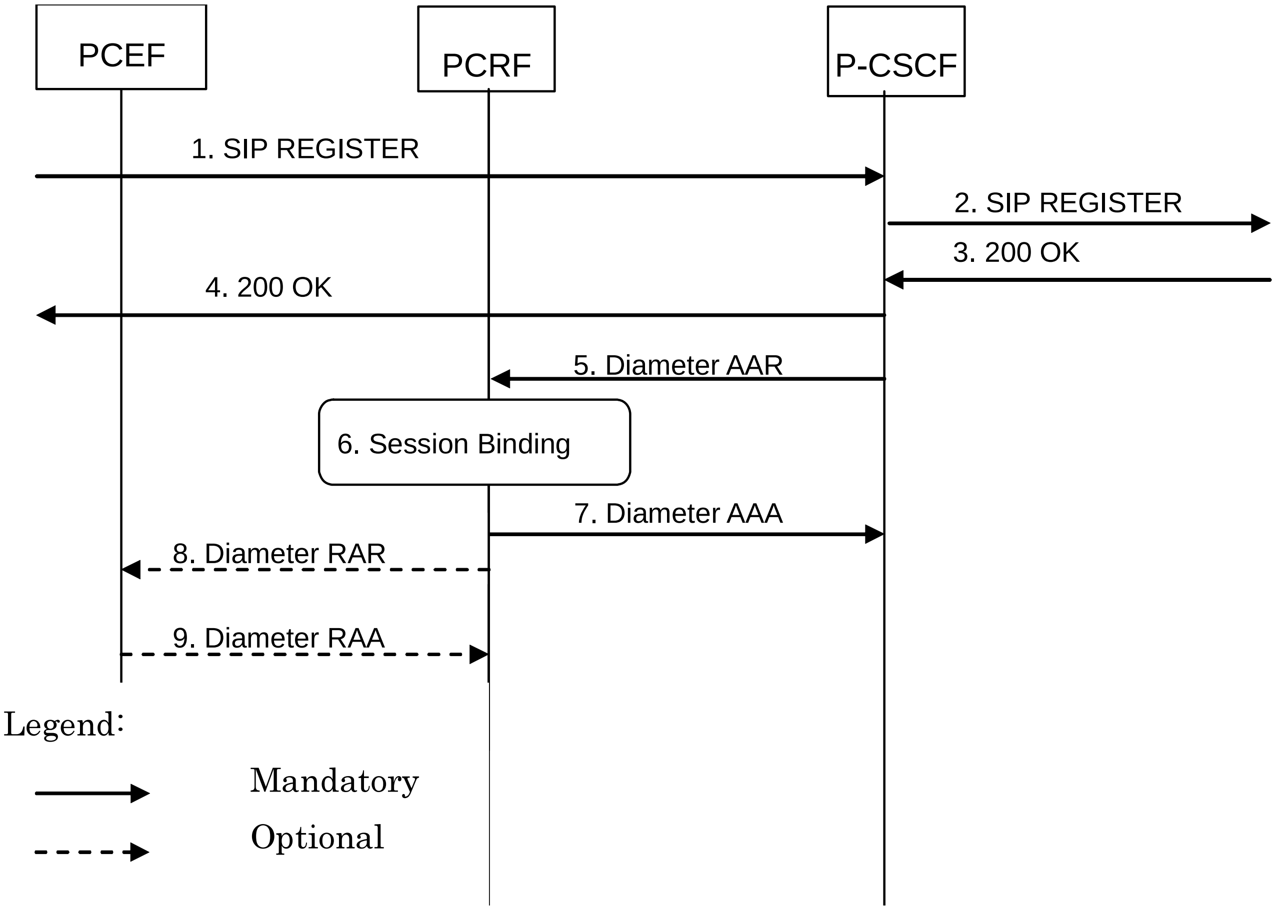
Annex A (informative): Examples of deriving the Maximum Authorized parameters from the SDP parameters

Annex B (normative): Signalling Flows for IMS

The signalling flows in Clause 4 are also applicable for IMS. This Annex adds flows that show interactions with SIP/SDP signalling of the IMS.

B.1 Subscription to Notification of Signalling Path Status at IMS Registration

This clause covers the Subscription to Notifications of IMS Signalling Path Status upon an initial successful IMS Registration procedure.



1-4. The user initiates an initial SIP Registration procedure. The SIP Registration procedure is completed successfully (user has been authenticated and registered within the IMS Core NW).

5. The P-CSCF requests the establishment of a new Diameter Rx session with the intention to subscribe to the status of the IMS Signaling path. The P-CSCF sends a Diameter AAR command to the PCRF.

6. The PCRF performs session binding and identifies corresponding PCC Rules related to IMS Signalling.

7. The PCRF confirms the subscription to IMS Signaling path status and replies with a Diameter AAR command back to the P-CSCF.

8. If the PCRF had not previously subscribed to the required bearer level events from the IP-CAN for the affected PCC Rules, then the PCRF shall send a Diameter RAR command to the PCEF in order to do so now.

9. The PCEF confirms the subscription to bearer level events and replies with a Diameter RAA command back to the PCRF.

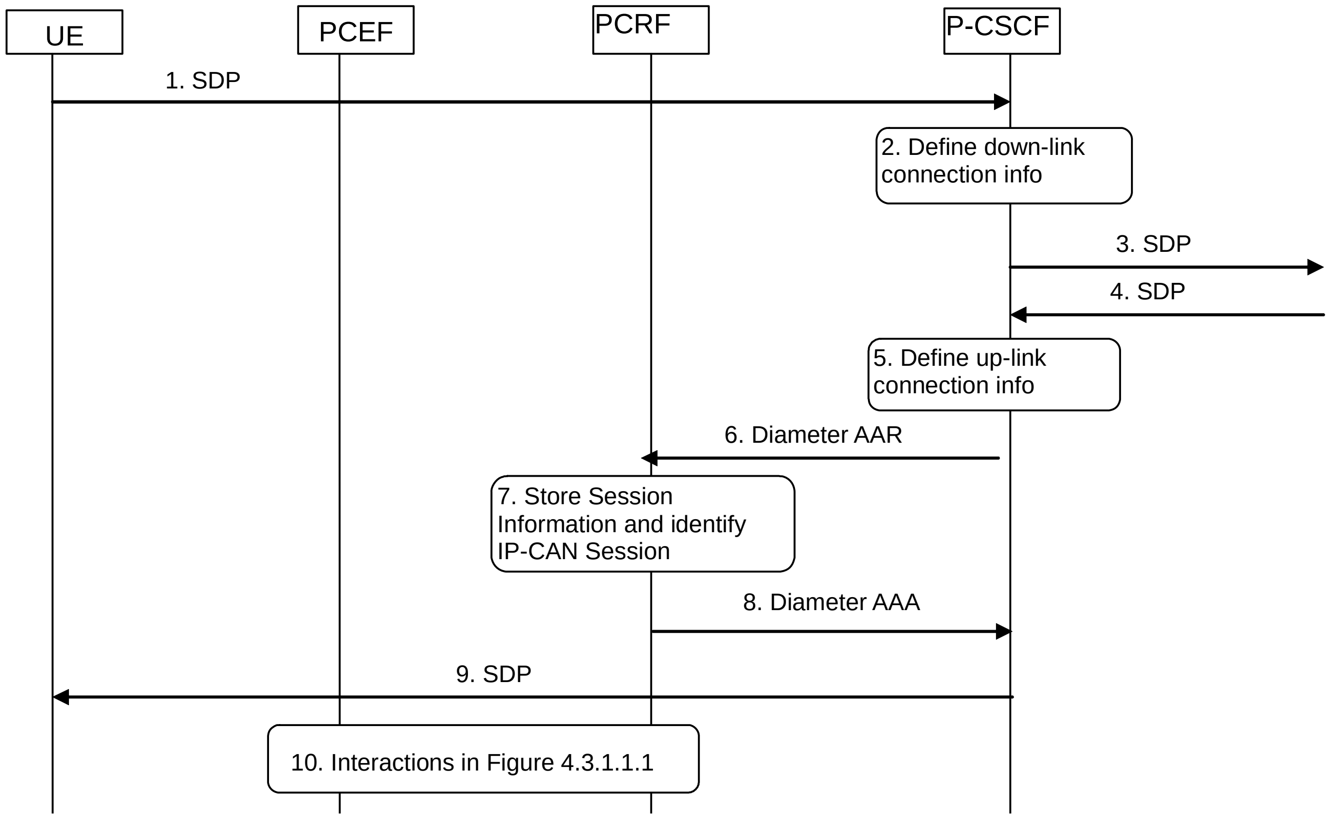
Figure B.1.1: Subscription to Notification of IMS Signaling Path Status at initial IMS Registration

B.2 IMS Session Establishment

B.2.1 Provisioning of service information at Originating P-CSCF and PCRF

This clause covers the PCC procedures at the originating P-CSCF and PCRF at IMS session establishment.

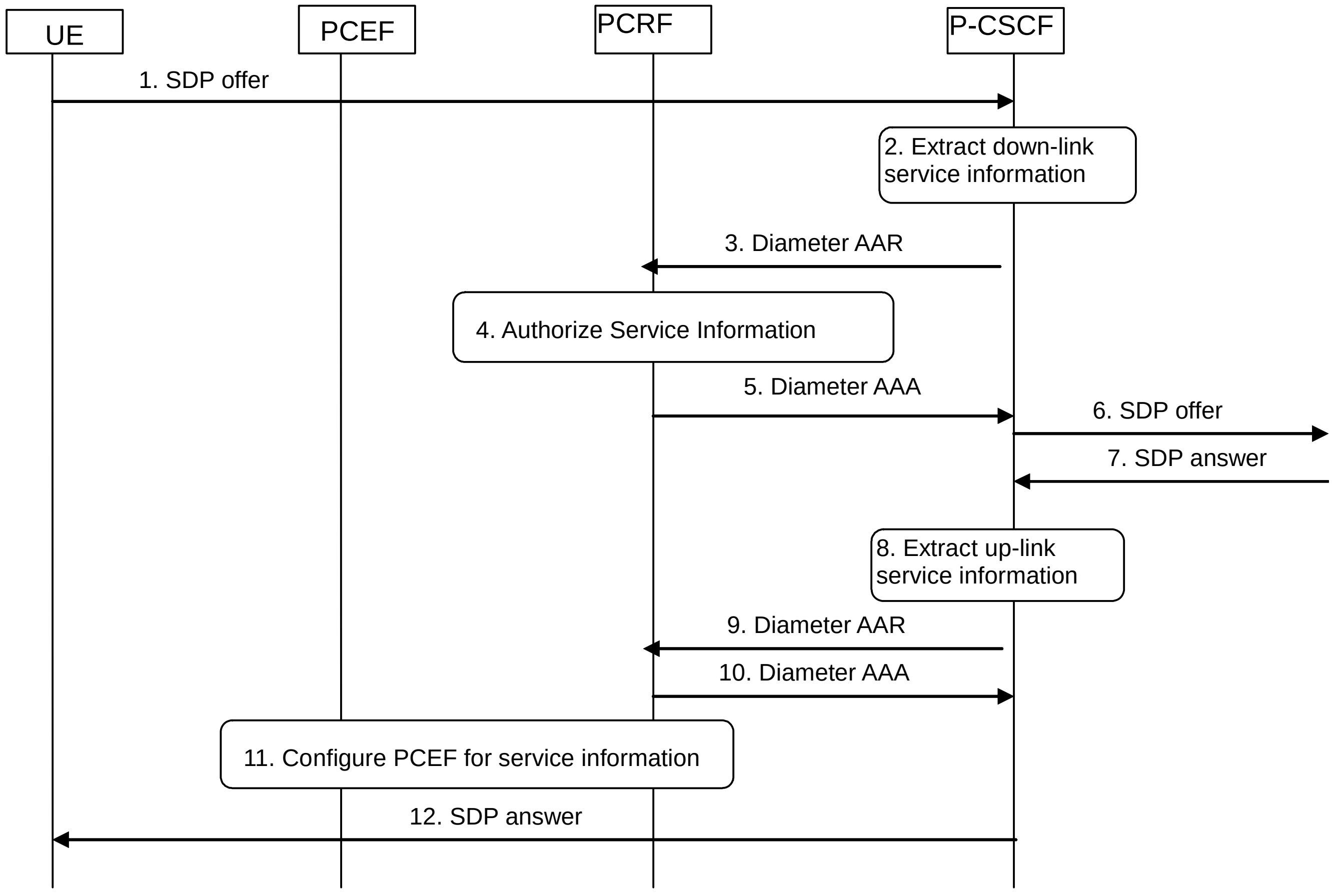
In figure B.2.1.1 the P-CSCF derives the provisioning of service information to the PCRF from the SDP offer/answer exchange.



1. The P-CSCF receives the SDP parameters defined by the originator within an SDP offer in SIP signalling.
2. The P-CSCF identifies the connection information needed (IP address of the down link IP flow(s), port numbers to be used etc…).
3. The P-CSCF forwards the SDP offer in SIP signalling.
4. The P-CSCF gets the negotiated SDP parameters from the terminating side through SIP signalling interaction.
5. The P-CSCF identifies the connection information needed (IP address of the up-link media IP flow(s), port numbers to be used etc…).
6. The P-CSCF forwards the derived session information to the PCRF by sending a Diameter AAR over a new Rx Diameter session.
7. The PCRF stores the received session information and identifies the affected established IP-CAN Session(s).
8. The PCRF replies to the P-CSCF with a Diameter AAA.
9. Upon reception of the acknowledgement from the PCRF, the SDP parameters are passed to the UE in SIP signalling.
10. The PCRF interacts with the GW according to figure 4.3.1.1.1. This step implies provisioning of PCC rules to the PCEF and is executed in parallel with steps 8 and 9.

Figure B.2.1.1: PCC Procedures for IMS Session Establishment at originating P-CSCF and PCRF

Optionally, the provisioning of service information may be derived already from the SDP offer to enable that a possible rejection of the service information by the PCRF is obtained by the P-CSCF in time to reject the service with appropriate SIP signalling. This is described in figure B.2.1.2.



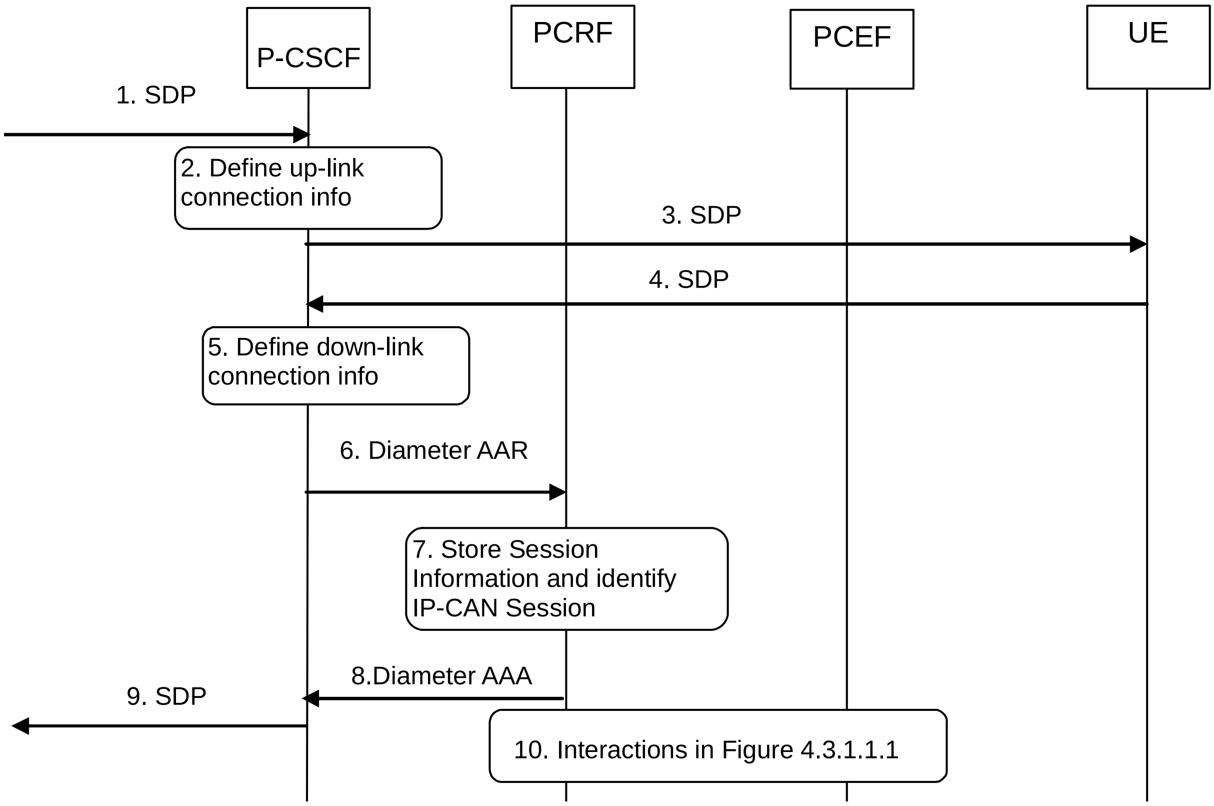
1. The P-CSCF receives the first SDP offer for a new SIP dialogue within a SIP INVITE request.
2. The P-CSCF extracts service information from the SDP offer (IP address of the down link IP flow(s), port numbers to be used etc…).
3. The P-CSCF forwards the derived service information to the PCRF by sending a Diameter AAR over a new Rx Diameter session. It indicates that only an authorization check of the service information is requested.
4. The PCRF checks and authorizes the service information, but does not configure the PCEF at this stage.
5. The PCRF replies to the P-CSCF with a Diameter AAA.
6. The P-CSCF forwards the SDP offer in SIP signalling.
7. The P-CSCF receives the negotiated SDP parameters from the terminating side within a SDP answer in SIP signalling.
8. The P-CSCF extracts service information from the SDP answer (IP address of the up-link media IP flow(s), port numbers to be used etc…).
9. The P-CSCF forwards the derived service information to the PCRF by sending a Diameter AAR over the existing Rx Diameter session.
10. The PCRF replies to the P-CSCF with a Diameter AAA.
11. The PCRF authorizes the session information. The PCRF performs steps 4. to 12 in Figure 4.3.1.2.1.1.These steps imply provisioning of PCC rules and authorized QoS to the PCEF.
12. Upon successful authorization of the session, the SDP parameters are passed to the UE in SIP signalling.

Figure B.2.1.2: PCC Procedures for IMS Session Establishment at originating P-CSCF and PCRF, provisioning of service information derived from SDP offer and answer

B.2.2 Provisioning of service information at terminating P-CSCF and PCRF

This clause covers the PCC procedures at the terminating P-CSCF and PCRF at IMS session establishment.

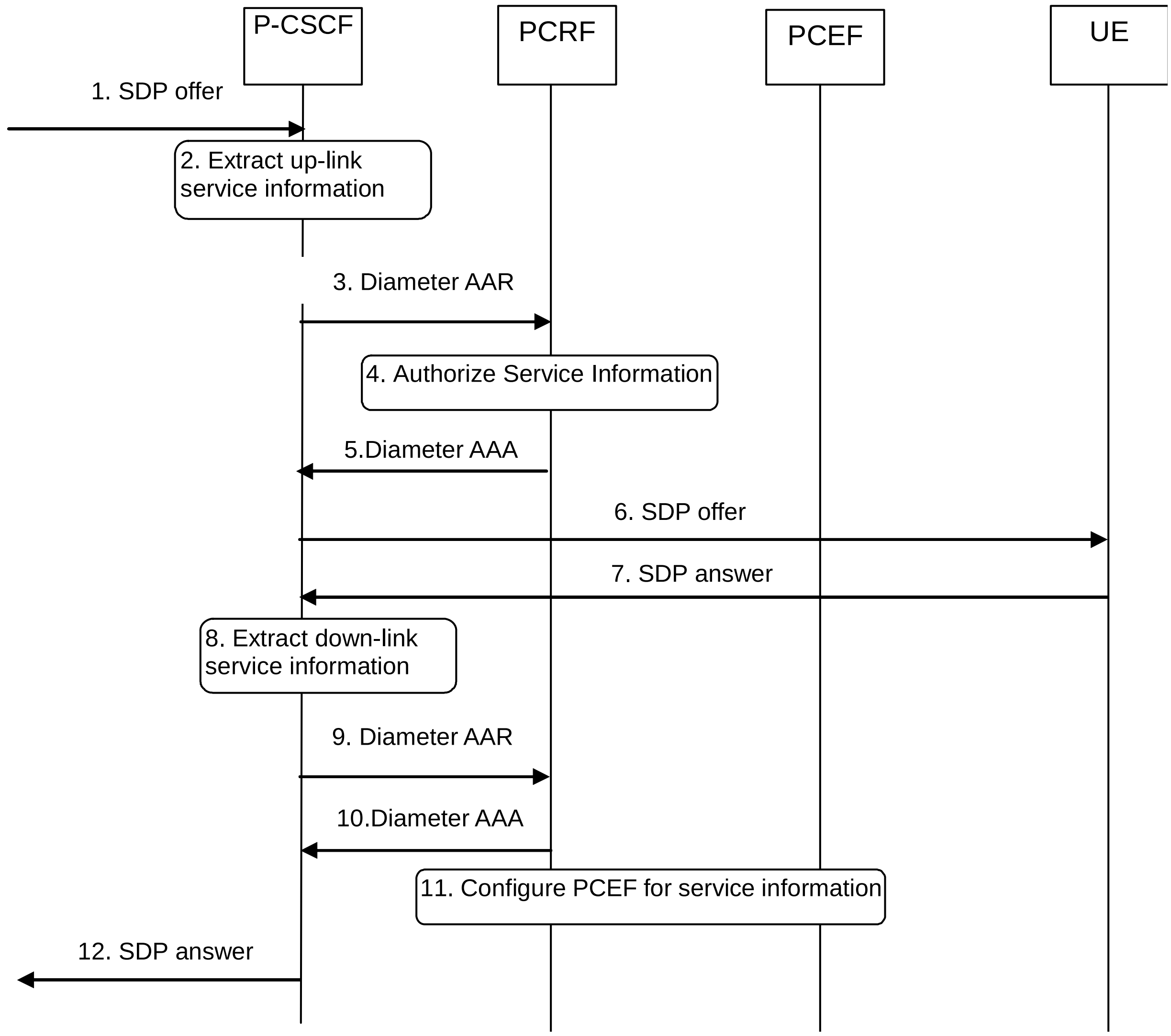
In figure B.2.2.1 the P-CSCF derives the provisioning of service information to the PCRF from the SDP offer/answer exchange.



1. The P-CSCF receives the SDP parameters defined by the originator.
2. The P-CSCF identifies the connection information needed (IP address of the up-link IP flow(s), port numbers to be used etc…).
3. The P-CSCF sends the SDP offer to the UE.
4. The P-CSCF receives the negotiated SDP parameters from the UE.
5. The P-CSCF identifies the connection information needed (IP address of the down-link IP flow(s), port numbers to be used etc…).
6. The P-CSCF forwards the derived service information to the PCRF by sending a Diameter AAR over a new Rx Diameter session.
7. The PCRF stores the received session information and identifies the affected established IP-CAN Session(s).
8. The PCRF sends a Diameter AAA to the P-CSCF.
9. Upon reception of the acknowledgement from the PCRF, the SDP parameters in the SDP answer are passed to the originator.
10. The PCRF interacts with the GW according to figure 4.3.1.1.1. This step implies provisioning of PCC rules to the PCEF and is executed in parallel with steps 8 and 9.

Figure B.2.2.1: PCC Procedures for IMS Session Establishment at terminating P-CSCF and PCRF

Optionally, the provisioning of service information may be derived already from the SDP offer to enable that a possible rejection of the service information by the PCRF is obtained by the P-CSCF in time to reject the service with appropriate SIP signalling. This is described in figure B.2.2.2.



1. The P-CSCF receives the first SDP offer for a new SIP dialogue within SIP signalling, e.g. within a SIP INVITE request.
2. The P-CSCF extracts the service information from the SDP offer (IP address of the up-link IP flow(s), port numbers to be used etc…).
3. The P-CSCF forwards the derived session information to the PCRF by sending a Diameter AAR over a new Rx Diameter session. It indicates that only an authorization check of the service information is requested.
4. The PCRF checks and authorizes the session information, but does not configure the PCEF at this stage.
5. The PCRF replies to the P-CSCF with a Diameter AAA.
6. The P-CSCF sends the SDP offer to the UE.
7. The P-CSCF receives the negotiated SDP parameters from the UE within an SDP answer in SIP signalling.
8. The P-CSCF extracts service information from the SDP answer (IP address of the down-link IP flow(s), port numbers to be used etc…).
9. The P-CSCF forwards the derived service information to the PCRF by sending a Diameter AAR over the existing Rx Diameter session.
10. The PCRF sends a Diameter AAA to the P-CSCF.
11. The PCRF authorizes the session information. The PCRF performs steps 4. to 12 in Figure 4.3.1.2.1.1.These steps imply provisioning of PCC rules and authorized QoS to the PCEF.
12. Upon successful authorization of the session the SDP parameters in the SDP answer are passed to the originator.

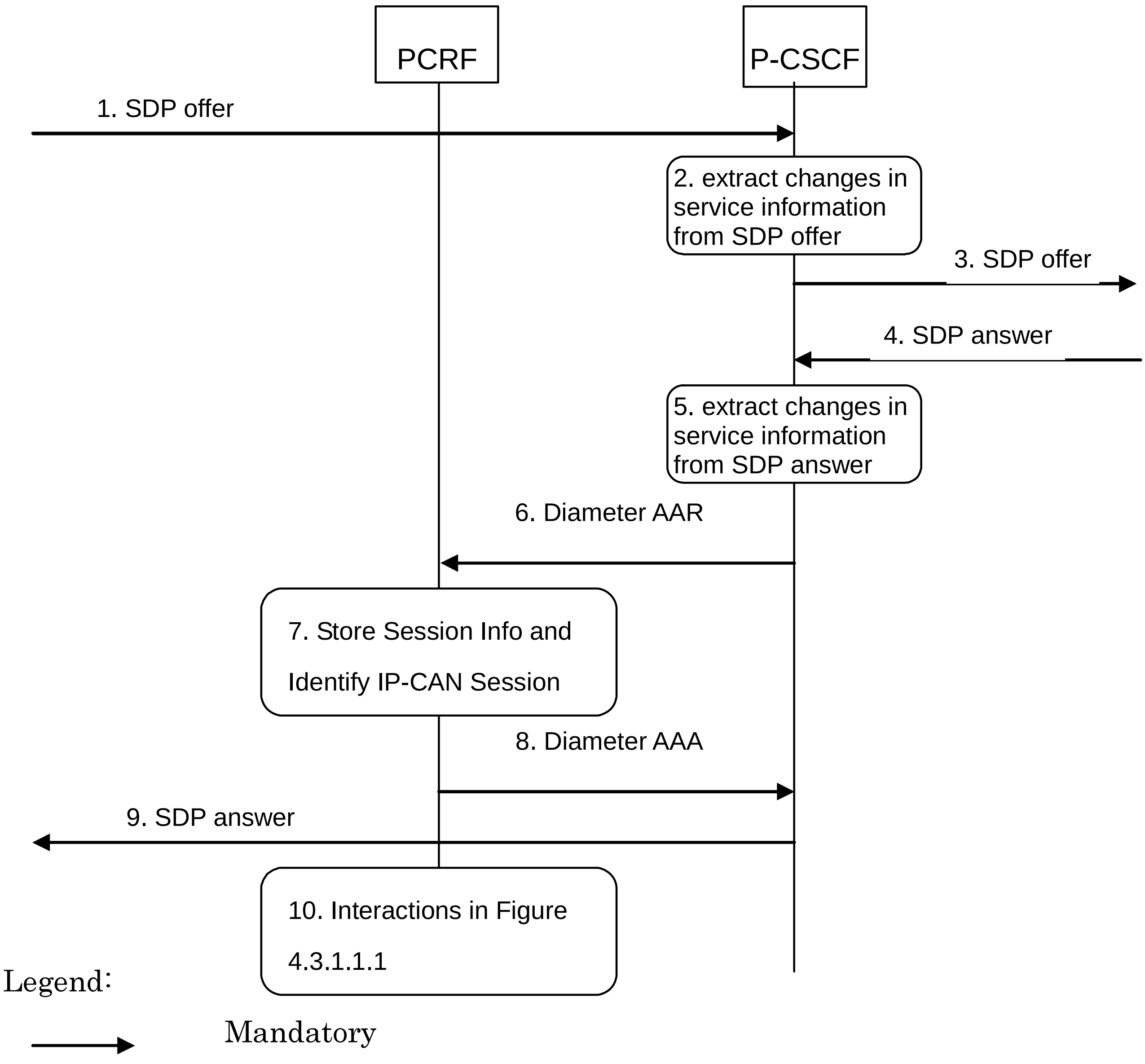
Figure B.2.2.2: PCC Procedures for IMS Session Establishment at terminating P-CSCF and PCRF, provisioning of service information derived from SDP offer and answer

B.3 IMS Session Modification

B.3.1 Provisioning of service information

This clause covers the provisioning of service information at IMS session modification both at the originating and terminating side.

In figure B.3.1.1 the P-CSCF derives the provisioning of service information to the PCRF from the SDP offer/answer exchange.

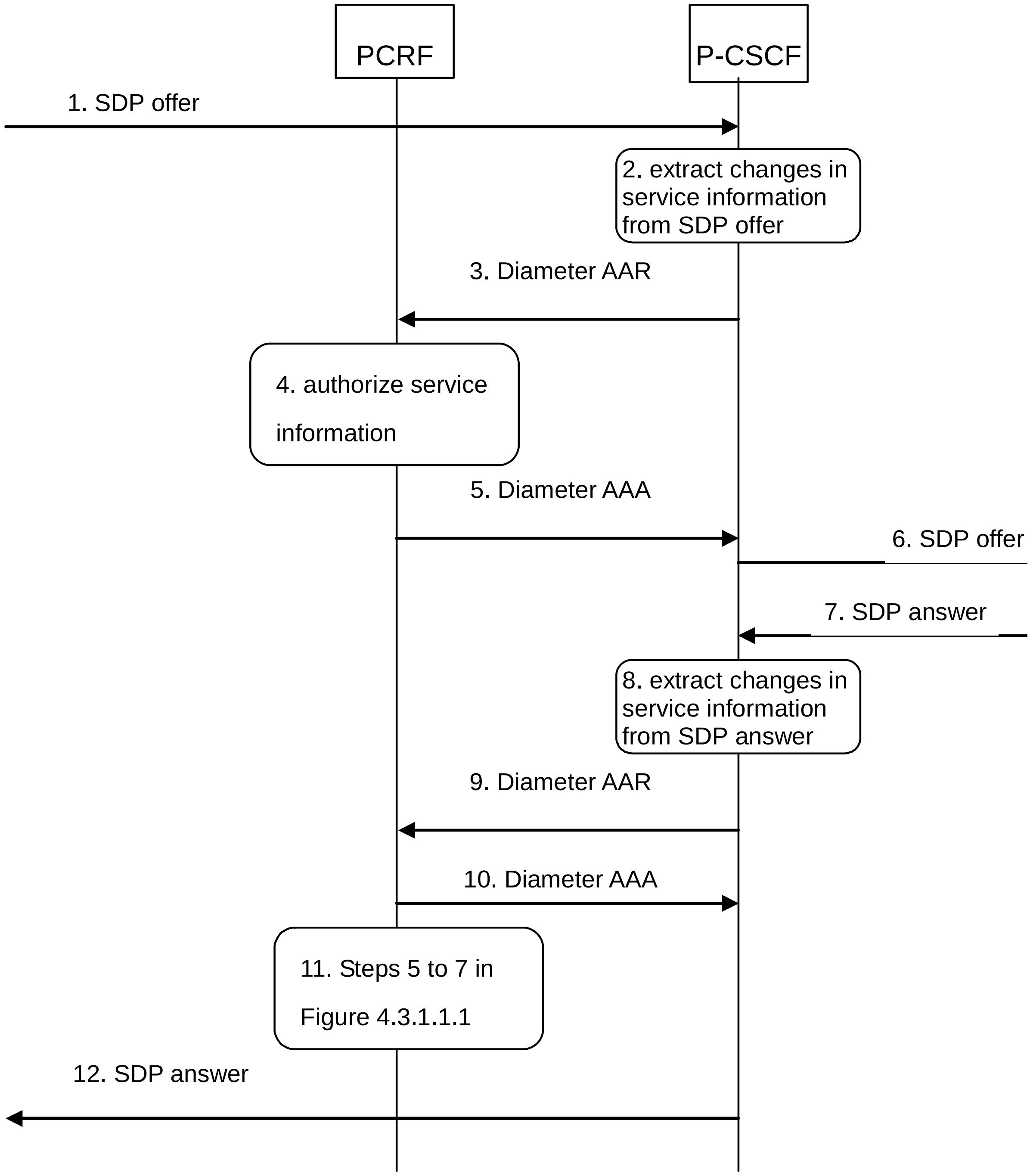


1. The P-CSCF receives the SDP parameters defined by the originator within an SDP offer in SIP signalling.
2. The P-CSCF identifies the relevant changes in the SDP.
3. The P-CSCF forwards the SDP offer in SIP signalling.
4. The P-CSCF gets the negotiated SDP parameters from the terminating side through SIP signalling interaction.
5. The P-CSCF identifies the relevant changes in the SDP.
6. The P-CSCF sends a Diameter AAR for an existing Diameter session and includes the derived updated service information.
7. The PCRF stores the received updated session information and identifies the affected established IP-CAN Session(s).

8. The PCRF answers with a Diameter AAA.
9. The P-CSCF forwards the SDP answer in SIP signalling.
10. The PCRF interacts with the GW according to figure 4.3.1.1.1. Due to the updated service information, this step may imply provisioning of PCC rules to the PCEF or the need to enable or disable IP Flows (see Clauses B.3.2 and B.3.3, respectively).

Figure B.3.1.1: Provisioning of service information at IMS session modification

Optionally, the provisioning of service information may be derived already from the SDP offer to enable that a possible rejection of the service information by the PCRF is obtained by the P-CSCF in time to reject the service with appropriate SIP signalling. This is described in figure B.3.1.2.



1. The P-CSCF receives an SDP offer in SIP signalling for an exiting SIP dialogue.
2. The P-CSCF identifies the relevant changes in the SDP and extracts the corresponding service information.
3. The P-CSCF forwards the derived service information to the PCRF by sending a Diameter AAR over the existing Rx Diameter session for the corresponding SIP session. It indicates that only an authorization check of the service information is requested.
4. The PCRF checks and authorizes the session information, but does not configure the PCEF at this stage.
5. The PCRF replies to the P-CSCF with a Diameter AAA.
6. The P-CSCF forwards the SDP offer in SIP signalling.
7. The P-CSCF receives the negotiated SDP parameters within an SDP answer in SIP signalling from the terminating side.
8. The P-CSCF identifies the relevant changes in the SDP and extracts the corresponding service information.

9. The P-CSCF sends a Diameter AAR for an existing Diameter session and includes the derived updated service information.
10. The PCRF answers with a Diameter AAA.
11. The PCRF performs Steps 4 to 6 in Figure 4.3.1.2.2.1. These steps may imply provisioning of PCC rules and authorized QoS to the PCEF. The PCRF may need to enable or disable IP Flows (see Clauses B.3.2 and B.3.3, respectively) due to the updated service information.
12. The P-CSCF forwards the SDP answer in SIP signalling.

Figure B.3.1.2: Provisioning of service information derived from SDP offer and answer at IMS session modification

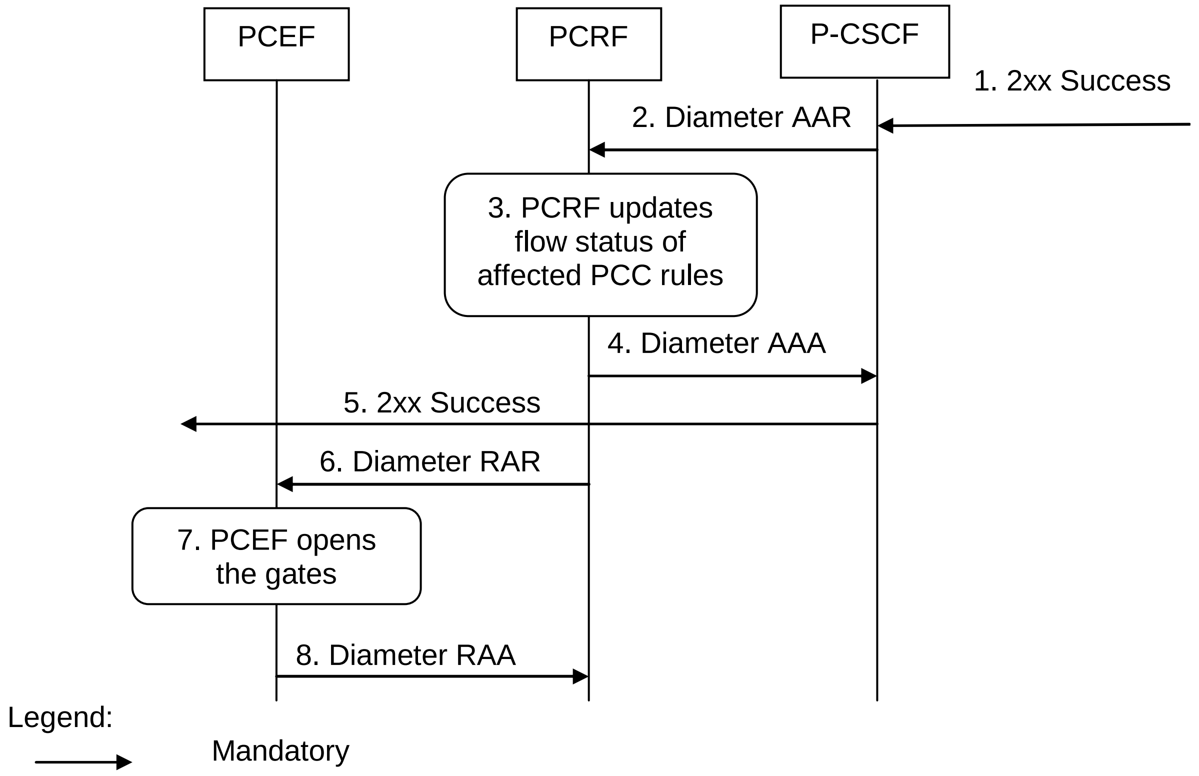
B.3.2 Enabling of IP Flows

The PCRF makes a final decision to enable the allocated QoS resource for the authorized IP flows of the media component (s) if the QoS resources are not enabled at the time they are authorized by the PCRF or if the media IP flow(s) previously placed on hold are resumed, i.e. the media IP flow(s) of the media component that was placed on hold at the time of the resource authorization or at a later stage is reactivated (with SDP direction sendrecv, sendonly, recvonly or none direction).

The Enabling of IP Flows procedure is triggered by the P-CSCF receiving any 2xx success response to an INVITE request or a 2xx success response to an UPDATE request within a confirmed dialogue (in both cases a 200 OK response is usually received). When receiving such responses, the PCRF shall take the SDP direction attribute in the latest received SDP (either within the 2xx success or a previous SIP message) into account when deciding, which gates shall be opened:

- For a unidirectional SDP media component, IP flows in the opposite direction shall not be enabled.
- For an inactive SDP media component, no IP flows shall be enabled.

Figure B.3.2.1 is applicable to the Mobile Originating (MO) side and the Mobile Terminating (MT) side.



1. The P-CSCF receives the 2xx Success message complying with the conditions specified in the paragraphs above.
2. The P-CSCF sends a Diameter AAR message to the PCRF, requesting that gates shall be opened.
3. The PCRF approves the enabling of IP flows and PCRF updates flow status of affected PCC rules.
4 The PCRF sends a Diameter AAA to the P-CSCF.
5 The P-CSCF forwards the 2xx Success message.
6. The PCRF sends a Diameter RAR message to the PCEF to open the ‘gates’ by updating the flow status of PCC rules.
7. The PCEF opens the ‘gates’ and thus enables the use of the authorised resources.
8. The PCEF sends a Diameter RAA message back to the PCRF.

Figure B.3.2.1: Enabling of IP Flows

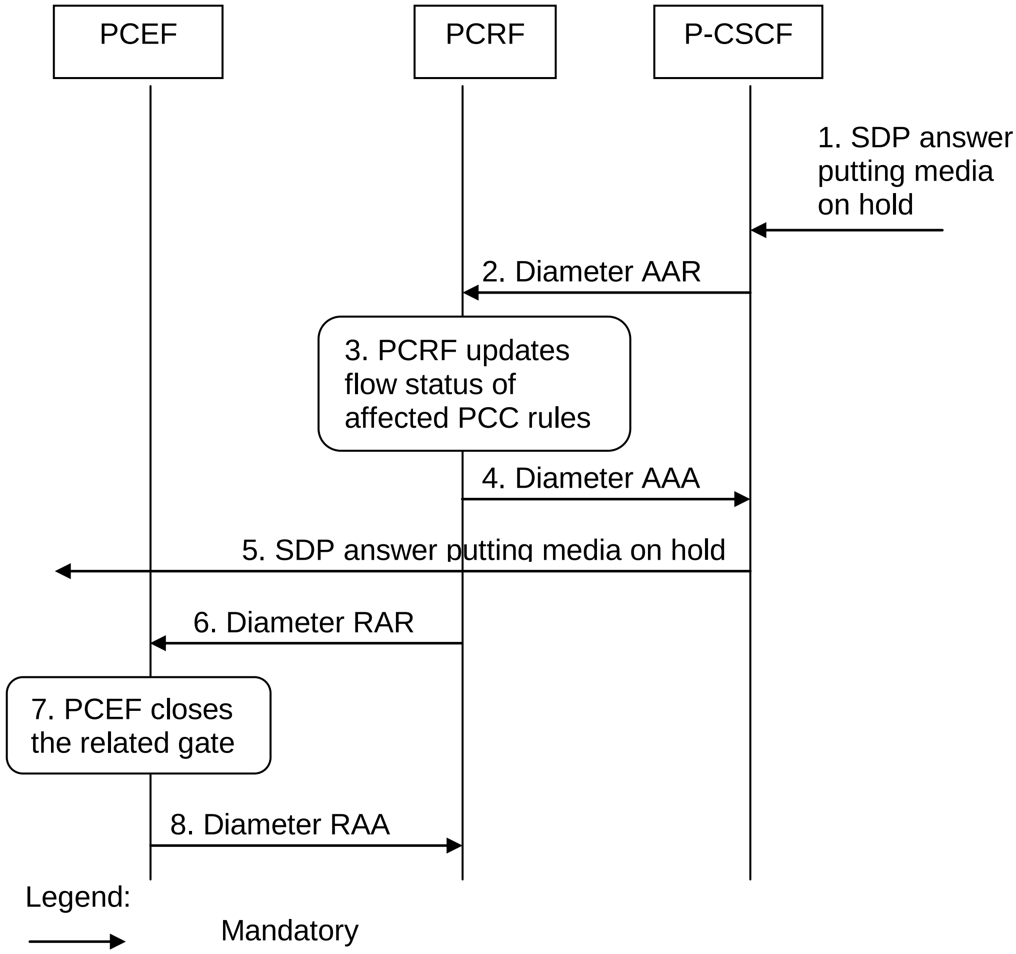
B.3.3 Disabling of IP Flows

The "Disabling of IP Flows" procedure is used when media IP flow(s) of a session are put on hold (e.g. in case of a media re-negotiation or call hold).

Media is placed on hold as specified in RFC 3264 [11]. Media modified to become inactive (SDP direction attribute) shall also be considered to be put on hold.

If a bidirectional media component is placed on hold by making it unidirectional, the IP flows shall only be disabled in the deactivated direction. If a media component is placed on hold by making it inactive, the IP flows shall be disabled in both directions.

Figure B.3.3.1 presents the "Disabling of IP Flows" procedure at media on hold for both the Mobile Originating (MO) side and the Mobile Terminating (MT) side.



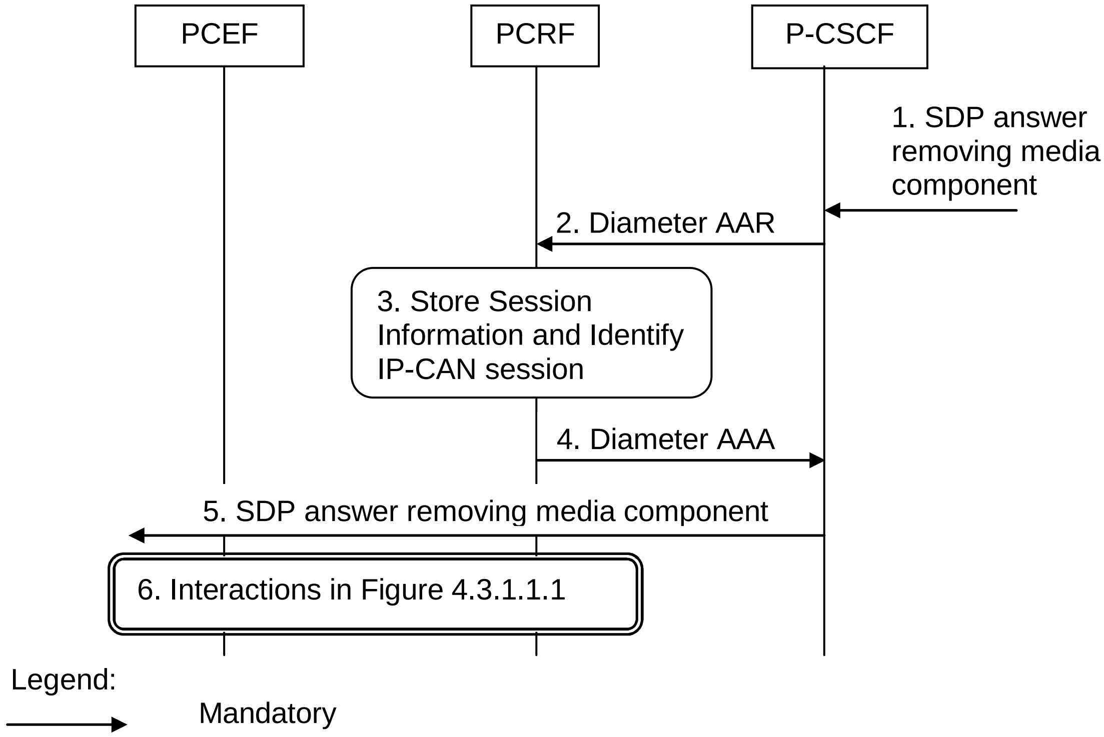
1. The P-CSCF receives an SDP answer putting media on hold within a SIP message. (NOTE 1)
2. The P-CSCF sends a Diameter AAR request to the PCRF, requesting that gates shall be closed.
3. The PCRF updates flow status of affected PCC rules for the media on hold.
4. The PCRF sends a Diameter AAA message back to the P-CSCF.
5. The P-CSCF forwards the SDP answer putting media on hold within a SIP message.
6. The PCRF sends a Diameter RAR message to the PCEF to close the relevant media IP flow gate(s), leaving the possible related RTCP gate(s) open to keep the connection alive.
7. The PCEF closes the requested gate(s).
8. The PCEF sends a Diameter RAA message back to the PCRF.

NOTE 1: This procedure occurs whenever a bidirectional media is made unidirectional or when a media is changed to inactive.

Figure B.3.3.1: Disabling of IP Flows at Media on Hold

B.3.4 Media Component Removal

Figure B.3.4.1 presents the flows of PCC procedures at the removal of media component(s) from an IMS session which is not being released for both the Mobile Originating (MO) side and the Mobile Terminating (MT) side.



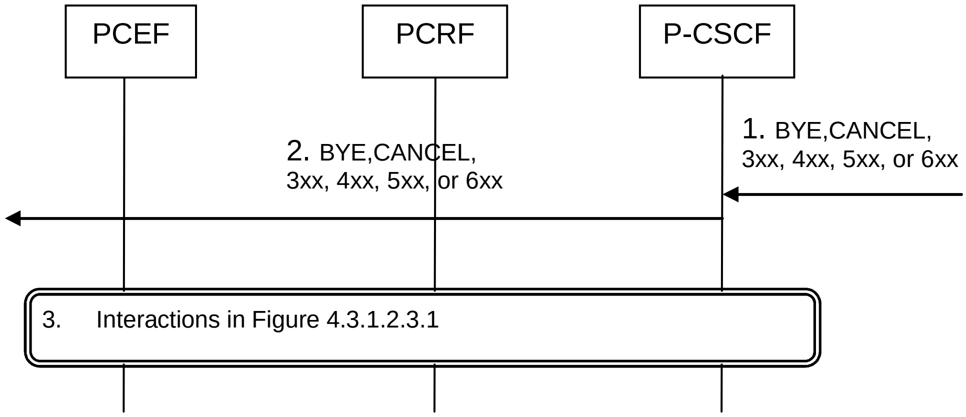
1. A SIP message containing SDP indicating the removal of media component(s) is received by the P-CSCF.
2. The P-CSCF sends Diameter AAR to the PCRF with modified service information.
3. The PCRF stores the Session information and identifies the affected IP-CAN Session(s).
4. The PCRF sends a Diameter AAA message back to the P-CSCF.
5. The P-CSCF forwards the SDP answer removing a media component.
6. The PCRF makes a decision on what PCC rules need to be modified or removed and interacts with the GW according to figure 4.3.1.1.1.

Figure B.3.4.1: Revoke authorization for IP resources at media component removal for both Mobile Originating (MO) and Mobile Terminating (MT) side

B.4 IMS Session Termination

B.4.1 Mobile initiated session release / Network initiated session release

Figure B.4.1.1 presents the mobile or network initiated IMS session release for both the Mobile Originating (MO) side and the Mobile Terminating (MT) side. The session release may be signalled by a SIP BYE message, by a SIP CANCEL request, or any SIP 3xx redirect response, or any 4xx, 5xx, or 6xx SIP final error response.



1. SIP BYE message, a SIP CANCEL request, a SIP 3xx redirect response, or any 4xx, 5xx, or 6xx SIP final error response is received by the P-CSCF.
2. P-CSCF forwards the BYE message, or the SIP 3xx redirect response, a SIP CANCEL request, or any 4xx, 5xx, or 6xx SIP final error response.
3. The Interactions in Figure 4.3.1.2.3.1 are applicable

Figure B.4.1.1: IMS session termination

B.4.2 IP-CAN Bearer Release/Loss

An IP-CAN Bearer Release or Loss event may affect all IP-Flows within an IMS Session. Flows in clause 4.3.2.2 apply.

Annex C (normative): NAT Related Procedures

C.1 Support for media traversal of NATs using ICE

The IMS calls out procedures for NAT traversal for media and signaling within IMS. One of the methods supported by IMS for media traversal of NATs is a UE controlled NAT traversal solution based on the IETF Interactive Connectivity Establishment (ICE) protocol [15]. When a UE uses the ICE protocol for media traversal of NATs, additional enhancements to the existing PCC procedures are necessary to allow for proper ICE operation.

This annex presents a set of rules that PCC network elements use to build flow descriptors, identify the proper UE IP addresses used by the PCRF for session and bearer binding, and gating control when the ICE procedures are invoked by the UE.

In order for the ICE procedures to work a static, preconfigured PCC rule needs to be in place at the PCEF which allows the UE to perform STUN binding requests prior to offering or answering an SDP.

NOTE 1: Predefined PCC rules can be created to allow the UE to communicate with the STUN relay much in the same way the UE is allowed to communicate with the IMS network for session management.

NOTE 2: Given that a STUN relay is a forwarding server under the direction of the UE, necessary precaution needs to be taken by the operator in how it chooses to craft these rules. It is recommended that such predefined rules only guarantee the minimal amount of bandwidth necessary to accomplish the necessary UE to STUN relay communication. Such an approach helps reduce the resources required to support NAT traversal mechanisms. Finally, such an approach allows the preconfigured rule to be over-ridden by dynamic rules which allow for the necessary bandwidth needed by the session.

NOTE 3: The dynamic PCC rule will need to differentiate between different media traffic between UE and STUN relay (e.g. voice vs. video), which can be identified by the different ports assigned by the residential NAT. Session bindings need to take into account that the relevant terminal IP address may be contained within the ICE candidates contained in the session description, rather than in the normal media description.

NOTE 4: It is assumed that the NAT device is located between the UE and the PCEF. NAT traversal outside of IMS in FBI services is considered FFS in the current 3GPP stage 2 specifications.

NOTE 5: When a NAT device is located between the UE and the PCEF, it is assumed that the IP CAN session signalling will contain the IP address assigned by the residential NAT, rather than the UE IP address.

NOTE 6: It is assumed that NAT devices that assign multiple IP addresses for the UE are outside the scope of release 7.

NOTE 7: In this release, only one IP address per subscription is supported by session binding at the PCRF. Multiple UEs behind a NAT will use the same IP CAN session and IP address.

C.2 P-CSCF procedures

C.2.1 General

The procedures in clause C.2 are only invoked in the case where the local UE (uplink SDP) has utilized the ICE protocol for media traversal of NATs. The P-CSCF can determine this by inspecting the UE provided SDP (uplink) for the "a=candidate" attribute(s). If such attributes are present this is an indication that the UE has invoked the ICE procedures as defined in ietf-draft-mmusic-ice [15] for media traversal of NATs and the P-CSCF shall follow the requirements in clause C.2.

C.2.2 Deriving the UEs IP address

The P-CSCF shall set the Framed-IP-Address AVP or Framed-IPv6-Prefix AVP to the source IP address of SIP messages received from the UE.

C.2.3 Deriving flow descriptions

In the case where STUN Relay and ICE are used for NAT traversal, the UE is required to place the STUN Relay provided address in the "m=" and "c=" lines of its SDP. Given that these addresses cannot be used by the P-CSCF for building a valid flow description, the P-CSCF will need to determine if a STUN Relay address has been provided in the "m=" and "c=" lines of the UE provided SDP (uplink only). The P-CSCF shall make this determination by inspecting the uplink SDP for "a=candidate" attributes and compare the candidate address with that contained in the "c=" line. If a match is found, the P-CSCF shall then look at the candidate type. If the candidate type is "relay" then the address in the "c=" line is that of a STUN Relay server. In this case, the P-CSCF shall derive the Flow-Description AVP within the service information from the SDP candidate type of "relay" as follows:

Uplink Flow-Description

- Destination Address and Port: If the P-CSCF knows the destination address and port of the STUN Relay allocation that the UE is sending media to, it should use that information. If the P-CSCF does not know this address and port, it shall wildcard the uplink destination address and port.
- Source Address and Port: The P-CSCF shall populate the uplink source address with the "rel-addr" address and the uplink source port with the "rel-port" port contained within the "a=candidate" attribute.

Downlink Flow-Description

- Destination Address and Port: The P-CSCF shall populate the downlink destination address with the "rel-addr" address and the downlink destination port with the "rel-port" port contained within the "a=candidate" attribute.
- Source Address and Port: If the P-CSCF knows the source address and port of the STUN Relay allocation that the UE is receiving media from, it should use that information. If the P-CSCF does not know this address and port, it shall wildcard the downlink source address and port.

For the other candidate types, the address in the "c=" and "m=" SDP attributes can be used for building the flow descriptor and the P-CSCF shall follow the rules to derive the Flow-Description AVP as described in table 6.2.2 of clause 6.2 of this TS.

C.2.4 Gating control

If both endpoints have indicated support for ICE (both the SDP offer and answer contain SDP attributes of type "a=candidate") ICE connectivity checks will take place between the two UEs. In order to allow these checks to pass through the PCEF, the P-CSCF shall enable each flow description for each media component upon receipt of the SDP answer.

C.2.5 Bandwidth impacts

ICE has been designed such that connectivity checks are paced inline with RTP data (sent no faster than 20ms) and thus consumes a lesser or equal amount of bandwidth compared to the media itself (given the small packet size of a STUN connectivity check it is expected that the STUN connectivity checks will always have a smaller payload than the media stream itself). Thus, there are no additional requirements on the P-CSCF for bandwidth calculations for a given media flow.

C.3 PCRF procedures

C.3.1 General

The procedures in clause C.3 are only invoked when the following two conditions are met:

1. Both the local and remote UE have utilized the ICE protocol for media traversal of NATs (see subclause C.2.1 for details on how this is determined); and

2. The IP-CAN which is servicing the IMS session does not support the concept of a default bearer.

C.3.2 Deriving additional flow descriptions

The PCRF may need to develop additional flow descriptions (beyond those provided by the P-CSCF) for a media component based on additional candidate addresses present in the SDP offer/answer exchange. The PCRF shall follow the procedures defined in draft-ietf-mmusic-ice [15] for forming candidate pairs based on the data contained within the received codec-data AVP. For each candidate pair created based on the ICE procedures and not already present in the received flow descriptions, the PCRF shall add an uplink and downlink flow description for each media component.

NOTE 1: The uplink SDP represents the local candidates while the downlink SDP represents the remote candidates.

Following the ICE procedures for forming candidate pairs will result in some flow descriptions which would never be exercised. In particular, while the UE will send connectivity checks (and ultimately its media stream) from its host candidate, from the PCEF perspective, this will appear as being from the server reflexive address. Given this, the PCRF should not form flow descrptions using host candidate addresses and should only form additional flows based on server reflexive addresses and relay addresses.

As candidates are removed from the SDP via subsequent offer/answer exchanges, the PCRF shall update its candidate pair list and shall remove any flow descriptors no longer being used.

NOTE 2: If the default candidate (the candidate used to populate the "c=" and "m=" lines of both the uplink and downlink SDP) is chosen, then an updated SDP offer/answer will not be done, and any extra flow descriptions not being used by the session will not be removed.

C.3.3 Gating control

For each additional flow description the PCRF adds to a media component (per sub-clause C.3.2), the PCRF shall enable the flow in order to allow connectivity checks to pass.

C.3.4 Bandwidth impacts

Per clause C.2.5 ICE is designed to have minimal impact on bandwidth policy control. However, it is possible that media will begin flowing while the ICE connectivity checks are still in progress. Given the possibility that no session update will be made (the default candidates will be chosen by the ICE protocol), it is not recommended that the PCRF adjust the bandwidth parameters provided by the P-CSCF.

Annex D (normative): Access specific procedures for GPRS

D.1 General

The present annex defines IP-CAN specific requirements for General Packet Radio Service (GPRS).

D.2 Binding Mechanisms

Depending on the bearer control mode, bearer binding can be executed either by PCRF, PCEF or both PCRF and PCEF.

- For "UE-only" IP-CAN bearer establishment mode, the PCRF performs bearer binding.
- For "UE/NW" IP-CAN bearer establishment mode, the PCRF performs the binding of the PCC rules for user controlled services while the PCEF performs the binding of the PCC rules for the network controlled services.

In GPRS access, if there is no suitable PDP-Context to accommodate a PCC rule when PCEF performs the bearer binding, the PCEF shall initiate the establishment of PDP-Contexts as specified in 3GPP TS 23.060 [3].

Annex E (informative): Change history

Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
12/05/2006					Includes the following TDOCs agreed at CT3#40: C3-060287	0.0.0	0.1.0
13/09/2006					Includes the following TDOCs agreed at CT3#41: C3-060350	0.1.0	0.2.0
11/11/2006					Includes the following TDOCS agreed at CT3#42: C3-060694, C3-060754, C3-060807, C3-060867	0.2.0	0.3.0
01/12/2006	TSG#33	CP-060636			Editorial update by MCC for presentation to TSG CT for information	0.3.0	1.0.0
15/02/2007					Includes the following TDOCS agreed at CT3#42: C3-070059, C3-070060, C3-070138, C3-070180, C3-070182, C3-070237, C3-070248, C3-070252, C3-070269	1.0.0	1.1.0
28/02/2007	TSG#35	CP-070098			Editorial update by MCC for presentation to TSG CT for approval	1.1.0	2.0.0
03-2007					MCC update to version 7.0.0 after approval at TSG CT#35	2.0.0	7.0.0
06-2007	TSG#36	CP-070421	002	2	Timer handling for IP-CAN Session Modification initiated by the NW	7.0.0	7.1.0
06-2007	TSG#36	CP-070421	003	2	Duplicated Bearer Binding Text	7.0.0	7.1.0
06-2007	TSG#36	CP-070421	004	1	Alignment of PCRF Acknowledgment to AF	7.0.0	7.1.0
06-2007	TSG#36	CP-070421	005	4	QoS mapping corrections in 29.213	7.0.0	7.1.0
06-2007	TSG#36	CP-070421	006		Correction of IMS signal flows	7.0.0	7.1.0
06-2007	TSG#36	CP-070421	008	1	QoS mapping correction	7.0.0	7.1.0
06-2007	TSG#36	CP-070421	010	1	Various Minor Corrections	7.0.0	7.1.0
06-2007	TSG#36	CP-070421	011		Bearer Id in IP-CAN session Establishment	7.0.0	7.1.0
06-2007	TSG#36	CP-070421	013	2	Clarification on PCC Rule Provisioning Method	7.0.0	7.1.0
06-2007	TSG#36	CP-070421	014	4	QoS mapping clarifications for forking	7.0.0	7.1.0
06-2007	TSG#36	CP-070422	016	1	Maximum authorized data rate and bandwidth	7.0.0	7.1.0
06-2007	TSG#36	CP-070421	017	2	Mixed Mode	7.0.0	7.1.0
09-2007	TSG#37	CP-070557	021	2	Assigning IP address to UE	7.1.0	7.2.0
09-2007	TSG#37	CP-070557	023	2	Align Bearer Binding mechanism with stage 2	7.1.0	7.2.0
09-2007	TSG#37	CP-070557	024	2	Modification for the timer expiry in PUSH mode	7.1.0	7.2.0
09-2007	TSG#37	CP-070557	025	2	Reject IP-CAN session establishment	7.1.0	7.2.0
09-2007	TSG#37	CP-070675	026	3	QoS upgrading and GBR calculation	7.1.0	7.2.0
09-2007	TSG#37	CP-070557	027	1	QoS parameter mapping regardless the BCM	7.1.0	7.2.0
09-2007	TSG#37	CP-070557	028	1	QoS authorization per QCI	7.1.0	7.2.0
09-2007	TSG#37	CP-070557	029	1	Editor's Notes Removal	7.1.0	7.2.0
09-2007	TSG#37	CP-070557	030		Derivation of Flow-Description AVP when IPv4 is used	7.1.0	7.2.0
09-2007	TSG#37	CP-070557	033	1	IP-CAN bearer operation failure	7.1.0	7.2.0
09-2007	TSG#37	CP-070557	034	1	Corrections to IMS call flows for rejection of service change	7.1.0	7.2.0
09-2007	TSG#37	CP-070557	035	1	Correction of implementation error of CR0004, CR0005	7.1.0	7.2.0
12-2007	TSG#38	CP-070727	039	1	Fixing Mapping Tables	7.2.0	7.3.0
			041	3	Addition of missing NAT procedures to PCC		
12-2007					Correction to cover page	7.3.0	7.3.1
03-2008	TSG#39	CP-080040	043	1	PDP Session	7.3.1	7.4.0
05-2008	TSG#40	CP-080292	047	4	Support of TCP-based media in PCC	7.4.0	7.5.0
05-2008	TSG#40	CP-080298	046	3	Updating QoS mapping procedures for 3GPP2 IP-CAN	7.5.0	8.0.0
05-2008	TSG#40	CP-080299	049	2	TS 29.213 re-structuring	7.5.0	8.0.0
05-2008	TSG#40	CP-080299	053	3	Updates to Binding Mechanisms	7.5.0	8.0.0
09-2008	TSG#41	CP-080634	054	3	Roaming Scenarios on S9 for LBO case (HPLMN)	8.0.0	8.1.0
09-2008	TSG#41	CP-080634	055	4	Roaming Scenarios on S9 for LBO case (VPLMN)	8.0.0	8.1.0
09-2008	TSG#41	CP-080553	058	1	Removal of BCM=Nw-Only	8.0.0	8.1.0
09-2008	TSG#41	CP-080553	059	1	ARP Handling	8.0.0	8.1.0
09-2008	TSG#41	CP-080634	060	3	Gateway Control session Establishment Procedure	8.0.0	8.1.0
09-2008	TSG#41	CP-080634	061	2	IP-CAN Session Establishment flow description	8.0.0	8.1.0
09-2008	TSG#41	CP-080639	063	1	Remove unused reference	8.0.0	8.1.0
09-2008	TSG#41	CP-080634	064	1	Update to binding mechanisms	8.0.0	8.1.0
09-2008	TSG#41	CP-080634	065	3	Gateway control and QoS rules request flow	8.0.0	8.1.0
09-2008	TSG#41	CP-080634	066	3	Gateway control and QoS rules provision flow	8.0.0	8.1.0
09-2008	TSG#41	CP-080634	067	2	Gateway control session termination flow	8.0.0	8.1.0
09-2008	TSG#41	CP-080634	078	3	PDN information in Rx interface	8.0.0	8.1.0
09-2008	TSG#41	CP-080634	071	4	Update of UE-Initiated IP-CAN Session termination flow	8.0.0	8.1.0
09-2008	TSG#41	CP-080634	072	3	Update of GW-Initiated IP-CAN Session termination flow	8.0.0	8.1.0
09-2008	TSG#41	CP-080634	073	3	Update of PCRF-Initiated IP-CAN Session termination folw	8.0.0	8.1.0
09-2008	TSG#41	CP-080634	074	1	Update of the scope and references of 29.213	8.0.0	8.1.0
09-2008	TSG#41	CP-080634	076	2	General description for the DRA solutions	8.0.0	8.1.0
09-2008	TSG#41	CP-080553	079		Removal of the session information request from the PCRF to the	8.0.0	8.1.0

					AF		
09-2008	TSG#41	CP-080634	082	2	Applicability of QoS mapping functions	8.0.0	8.1.0
09-2008	TSG#41	CP-080655	096	1	Proxy DRA flows during IP-CAN session establishment	8.0.0	8.1.0
09-2008	TSG#41	CP-080656	097	2	Redirect DRA flows during IP-CAN session establishment/modification	8.0.0	8.1.0
09-2008	TSG#41	CP-080657	098	3	Redirect DRA flows during IP-CAN session termination	8.0.0	8.1.0
09-2008	TSG#41	CP-080645	099	2	DRA redirect procedures	8.0.0	8.1.0
09-2008	TSG#41	CP-080653	100	2	Proxy DRA flows during IP-CAN session modification	8.0.0	8.1.0
09-2008	TSG#41	CP-080654	101	2	Proxy DRA flows during IP-CAN session termination	8.0.0	8.1.0
10-2008					Editorial correction	8.1.0	8.1.1

History

Document history		
V8.0.0	November 2008	Publication
V8.1.1	November 2008	Publication