3GPP TSG-CN Meeting #25 **NP-040338**
8th – 10th September 2004. Palm Springs, USA.

Source: **TSG CN WG3**

Title: **CRs to Rel-6 on Work Item "QoS1"**

Agenda item: **9.20**

Document for: **APPROVAL**

Introduction:

This document contains 2 CRs to Rel-6 on Work Item "QoS1" that have been agreed by TSG CN WG3, and are forwarded to TSG CN Plenary for approval.

WG_tdoc	Spec	CR	R	Cat	Title	Rel	C_Ver	Work Item
N3-040615	29.207	137		B	29.207-Rel6: accumulated CR for Gq impacts	Rel-6	6.0.0	QoS1
N3-040616	29.208	073		B	29.208-Rel6: accumulated CR for Gq impacts	Rel-6	6.0.0	QoS1

3GPP TSG-CN WG3 Meeting #33
Sophia Antipolis, France. 16th to 20th August 2004.

Tdoc ⌘N3-040615

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.207** **CR** **137** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Accumulated CR on Gq impacts
Source:	⌘	TSG_CN WG3
Work item code:	⌘	QoS1
Date:	⌘	24/08/2004
Category:	⌘	**B**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
Ph2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)
Rel-7 (Release 7)

Reason for change: ⌘ Introduction of Gq Interface between AF and PDF, allowing a split between P-CSCF and PDF and also supporting non-IMS AFs, as required according to stage 2 TS 23.207.

Summary of change: ⌘ The text is modified to allow for non-IMS applications and to cover impacts of the new Gq interface introduced in Rel-6.
Changes from the following TDOCs agreed by CN3 are included:

N3-030832	Gq interface impacts
N3-030833	Changing term SDP to SDI (Session Description Information) and service information
N3-030836	Introduction of multiple token case
N3-040213	Generic Flow Identifier
N3-040214	Indication of Gq failure on Go
N3-040224	Generic Media component
N3-040415	DRQ Reason code.
N3-040518	Binding information
N3-040541	Various Gq related corrections.

Consequences if not approved: ⌘ Missing functionality compared to stage 2 requirements.
No support for Gq interface and non-IMS applications.

Clauses affected: ⌘ 2, 3, 4, 5, 6.3.2, Annex A, Annex C

Other specs affected: ⌘

Y	N	
X		Other core specifications
	X	Test specifications
	X	O&M Specifications

⌘ TS 29.208, CR #73; new TS 29.209

Other comments: ⌘

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 23.002: "Network architecture".

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

[4] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[5] Void.

[6] IETF RFC 2753: "A Framework for Policy-based Admission Control".

[7] IETF RFC 2748: "The COPS (Common Open Policy Service) Protocol".

[8] IETF RFC 3084: "COPS Usage for Policy Provisioning (COPS-PR)".

[9] IETF RFC 3159: "Structure of Policy Provisioning Information (SPPI)".

[10] Void.

[11] IETF RFC 3520: "Session Authorization Policy Element".

[12] 3GPP TS 24.008: "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3".

[13] 3GPP TS 27.060: "Packet domain; Mobile Station (MS) supporting Packet Switched services".

[14] 3GPP TS 24.229: "IP Multimedia Call Control Protocol based on SIP and SDP; Stage 3".

[15] IETF RFC 3318: "Framework Policy Information Base".

[16] IETF RFC 3289: "Management Information Base for the Differentiated Services Architecture"

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

[18] 3GPP TS 29.208: "End-to-end Quality of Service (QoS) signalling flows".

[19] IETF RFC 3291: "Textual Conventions for Internet Network Addresses".

[20] 3GPP TS 29.060: "General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface".

[21] 3GPP TS 32.225: "Telecommunication management; Charging management; Charging data description for the IP Multimedia Subsystem (IMS)".

[22] IETF RFC 3313: "Private Session Initiation Protocol (SIP) Extensions for Media Authorization"

[23] 3GPP TS 29.209 "Policy control over Gq interface".

[24] IETF RFC 3605 "Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP)"

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:

Application Function: The Application Function (AF) is an element offering applications that require the control of IP bearer resources. The AF is capable of communicating with the PDF to transfer dynamic QoS-related application information. One example of an AF is the P-CSCF of the IM CN subsystem.

AF session: An AF session is established by an application level signalling protocol offered by the AF that requires a session set-up with explicit session description before the use of the service. One example of an application session is an IMS session.

AF session signalling: AF session signalling is used to control the AF session. One example of AF session signalling is SIP/SDP.

Authorization Token: consists of the ~~IMS~~ AF session identifier and the PDF identifier in conformance with RFC 3520 [11]. It is used for authorizing the QoS for the IP flow (s). The UE includes an authorization token as part of the binding information in order to obtain QoS authorization for the ~~IMS~~ AF session. The UE obtains this authorization token via the AF session signalling from the AF, e.g. via SIP from the P-CSCF by means of an extension SIP header described in RFC 3313 [22]. The ~~P-CSCF~~AF communicates with the PDF in order to obtain a suitable authorization token for the UE.

Binding Information: consists of an authorization token and the flow identifier(s) of IP flow(s) carried by a PDP context. When receiving an authorization token, the UE includes binding information when activating or modifying a PDP context. It is used for authorizing the QoS of the IP flows carried within a PDP context and to verify that the grouping of the IP flows is correct.

Client Handle: an object in the COPS messages used as a unique number to correlate all the COPS messages with the same dialogue. Over the Go interface the Client Handle is used to correlate COPS messages with respect to the same PDP Context. For the exact definition see RFC 2748 [7] and RFC 3084 [8].

Common Open Policy Service (COPS) protocol: is a simple query and response protocol that can be used to exchange policy information between a policy server (Policy Decision Point) and its clients (Policy Enforcement Points)

Flow identifier: used for the identification of the IP flows, described within a media component associated with an AF ~~SIP~~ session. A Flow identifier consists of two parts: 1) the ordinal number of the position of the ~~"m=" lines in the SDP (RFC 2327 [17])~~media component description in the session description information and 2) the ordinal number of the IP flow(s) within the ~~"m=" line~~media component description assigned in the order of increasing port numbers. Examples are provided in Annex C.

Go Interface: interface between PDF and GGSN (3GPP TS 23.002 [2])

Gq Interface: interface between PDF and the AF. It is specified in 3GPP TS 29.209 [23]

GPRS Charging ID (GCID): the Charging Id generated by the GGSN as defined in 3GPP TS 29.060 [20].

IP Bearer Service Manager: uses standard IP mechanisms to manage the IP Bearer Service. It resides in the GGSN and optionally in the UE.

IP flow: a unidirectional flow of IP packets with the same source IP address and port number and the same destination IP address and port number and the same transport protocol. Port numbers are only applicable if used by the transport protocol.

Media component: is a part of an ~~SDP~~ AF session description (e.g. SDP) conveying information about media (e.g. media type, format, IP address, port(s), transport protocol, bandwidth, direction).

The media described by a media component can be either bi- or unidirectional. Media using RTP for transport may also have associated RTCP If so, the media component also conveys information about the associated RTCP (port and possibly bandwidth). An ~~SDP~~ AF session description can consist of more than one media component.

~~A~~ For SDP, a media component shall not be deleted nor its position changed within the SDP session description. An SDP media component line where the port number has previously been set to 0 may be reused for a new media component.

Policy Decision Function (PDF): is a logical policy decision element that uses standard IP mechanisms to implement policy in the IP media layer
The PDF makes decisions in regard to network based IP policy using policy rules, and communicates these decisions to the PEP in the GGSN.

Proxy Call Session Control Function (P-CSCF): is a network element providing session management services (e.g. telephony call control)

Policy Enforcement Point (PEP): is a logical entity that enforces policy decisions made by the PDF. It resides in the IP BS Manager of the GGSN

Policy Information Base (PIB): is a set of policy data carried by COPS-PR
The protocol assumes a named data structure, known as a Policy Information Base (PIB), to identify the type and purpose of solicited and unsolicited policy information that is sent from the Policy Decision Point to the Policy Enforcement Point for provisioning policy or sent from the Policy Enforcement Point to the Policy Decision Point as a notification.

Provisioning Instance Identifier (PRID): uniquely identifies an instance of a PRC

QoS class: identifies a bearer service (which is associated with a set of bearer service characteristics)

Session Description Information (SDI): The set of information describing the AF session (e.g. type of media, bandwidth, IP address and port number) agreed between the UE and the AF required to perform the Service Based Local Policy (SBLP).. For example, in the IMS case, this information is negotiated between the UE and AF using SDP.

Service Information: The set of information conveyed from the AF to the PDF over the Gq interface to be used as a basis for the service-based local policy decisions at the PDF, including information about the AF session (e.g. application identifier, type of media, bandwidth, IP address and port number) and parameters controlling the PDF behavior. The encoding of the service information is provided in 3GPP TS 29.209 [23].

Translation/mapping function: provides the inter-working between the mechanisms and parameters used within the UMTS Bearer Service and those used within the IP Bearer Service

UMTS Bearer Service Manager: handles resource reservation requests from the UE. It resides in the GGSN and the UE

3.2 Abbreviations

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

AF	Application Function
COPS	Common Open Policy Service protocol
COPS-PR	COPS for policy PRovisioning
DEC	COPS DECision message
DRQ	COPS Delete ReQuest state message
GCID	GPRS Charging IDentifier
ICID	IM CN Subsystem Charging IDentifier
IMS	IP Multimedia core network Subsystem
MIB	Management Information Base
P-CSCF	Proxy Call Session Control Function
PDF	Policy Decision Function
PEP	Policy Enforcement Point

PIB	Policy Information Base
PRC	PRovisioning Class (a type of policy data)
PRI	PRovisioning Instance (an instance of a PRC)
PRID	PRovisioning Instance iDentifier
QoS	Quality of Service
REQ	COPS REQuest message
RPT	COPS RePorT state message
RTCP	RTP Control Protocol
SBLP	Service Based Local Policy
SDI	Session Description Information
SDP	Session Description Protocol

4 Go interface

4.1 Overview

The Go interface allows service-based local policy information to be "pushed" to or requested by the Policy Enforcement Point (PEP) in the GGSN from a Policy Decision Function (PDF). As defined in the stage 2 specifications 3GPP TS 23.207 [3], this information is used by the GGSN for:

- GPRS bearer authorisation;
- Charging correlation;
- Policy based "gating" function in GGSN;

The Go interface uses IP flow based policies.

The Common Open Policy Service (COPS) protocol has been developed as a protocol for use between a policy server and a network device, as described in RFC 2748 [7].

In addition, COPS for Provisioning extensions have been developed as described in RFC 3084 [8] with RFC 3159 [9] describing a structure for specifying policy information that can then be transmitted to a network device for the purpose of configuring policy at that device. The model underlying this structure is one of well-defined provisioning classes and instances of these classes residing in a virtual information store called the Policy Information Base (PIB).

The Go interface shall conform to the IETF COPS (RFC 2748 [7]) and the extensions of COPS-PR (RFC 3084 [8]). For the purpose of exchanging the required specific Go information, a 3GPP Go COPS-PR Policy Information Base (PIB) is defined in the present document.

COPS Usage for Policy Provisioning (COPS-PR) is independent of the type of policy being provisioned (QoS, Security, etc.). In the present document, COPS-PR is used to communicate service-based local policy information between PDF and GGSN. COPS-PR can be extended to provide per-flow policy control along with a 3GPP Go Policy Information Base (PIB). The 3GPP Go PIB may inherit part of the data object definitions from other PIBs and MIBs defined in the IETF.

Signalling flows related to the Go interface are specified in 3GPP TS 29.208 [18].

The minimum functionalities that the Go interface shall cover are introduced below.

1. Media Authorisation request from GGSN:

   The GGSN receives the binding information during the activation of a (Secondary) PDP context or during the modification of an existing PDP context that has been previously authorized by the PDF. To authorise the PDP context activation, the GGSN shall send a media authorisation request to the PDF. To authorise the PDP context modification, the GGSN shall send a media authorisation request to the PDF when the requested QoS exceeds the authorised QoS or new binding information is received.

   This authorisation request shall include the following information:

   - Binding information:

The binding information is used by the GGSN to identify the correct PDF and subsequently request service-based local policy information from the PDF. The GGSN may receive one or more sets of the binding information during an activation or modification of a PDP context. Each set of binding information consists of:

- One Authorisation token;
- One or more Flow identifiers within the session.

2. Media authorisation decision from PDF:

The media authorisation information sent by the PDF to the GGSN, contains at a minimum the following information:

- Decision on the binding information.

The PDF shall respond with an authorisation decision for the binding information. The authorisation decision shall identify that the binding information is validated with an ongoing ~~SIP~~ AF session. Additionally, the PDF shall verify if the IP flows of the multiple media components are correctly assigned to the PDP Context. If validated, the PDF shall also communicate the following media authorisation details to the GGSN:

- "Authorised QoS".

  This information is used by the GGSN to authorise the media resources according to the service-based local policy and the requested bearer QoS.

  The "Authorised QoS" signalled over the Go interface is based on the service information ~~SDP~~ requirements conveyed over the Gq interface, which are based on SDI possibly signalled and agreed previously within AF session~~SIP~~ signalling for this session.

  The "Authorised QoS" specifies the maximum QoS that is authorised for a PDP context for that specific binding information. In case of an aggregation of multiple media components within one PDP context, the combination of the "Authorised QoS" information of the individual IP flows of the media components is provided as the "Authorised QoS" for the bearer.

  The "Authorised QoS" contains the following information:

  - QoS class:

    The QoS class information represents the highest class that can be used for the media component. It is derived from the service information received from the AF~~SDP media description~~. The QoS class within the "Authorized QoS" information for the bearer is determined from the QoS class values of the individual IP flows of these media components identified in the binding information.

  - Data rate:

    The Data rate information is derived from the service information. In the IMS case, it is derived from the SDP-bandwidth parameters converted by the P-.CSCF to bandwidth information within the service information. The Data rate ~~shall~~ includes all the overhead coming from the IP-layer and the layers above, e.g. UDP, RTP or RTCP. If multiple codecs are agreed to be used in a session, the authorized data rate is set according to the codec requiring the highest bandwidth, meaning that terminals may under use the authorized data rate when choosing to use another agreed codec. The Data rate within the "Authorized QoS" information for the bearer is determined from the data rate values of the individual IP flows identified in the binding information.

- Packet Classifier.

  The packet classifier for media components is based on the IP-address and port number information in the service information ~~SDP~~ and shall allow for all IP flows associated with the service information ~~SDP~~ media component description.

3. Charging correlation:

The PDF ~~shall~~ may send the AF charging information e.g. ICID (see 3GPP TS 24.229 [14]) provided by the P-CSCF in the IMS case, as part of the authorisation decision. The GGSN shall send the GCID (see 3GPP TS 29.060 [20]) of the PDP Context and the GGSN address to the PDF as part of the authorisation report.

4. Approval of QoS Commit / Removal of QoS Commit / Revoke Authorisation for GPRS and IP resources:

   The PDF controls media components and may revoke resources at any time. Approval of QoS Commit / Removal of QoS Commit / Revoke Authorisation for GPRS and IP resources is communicated by the PDF to the GGSN.

5. Indication of PDP Context Release / Modification to/from 0 kbit/s:

   The GGSN informs the PDF of bearer changes related to the authorised resources for the ~~IMS~~ AF session in the following cases:

   - Loss of radio contact (modification to/from 0 kbit/s for conversational and streaming class);
   - Deactivation of PDP context.

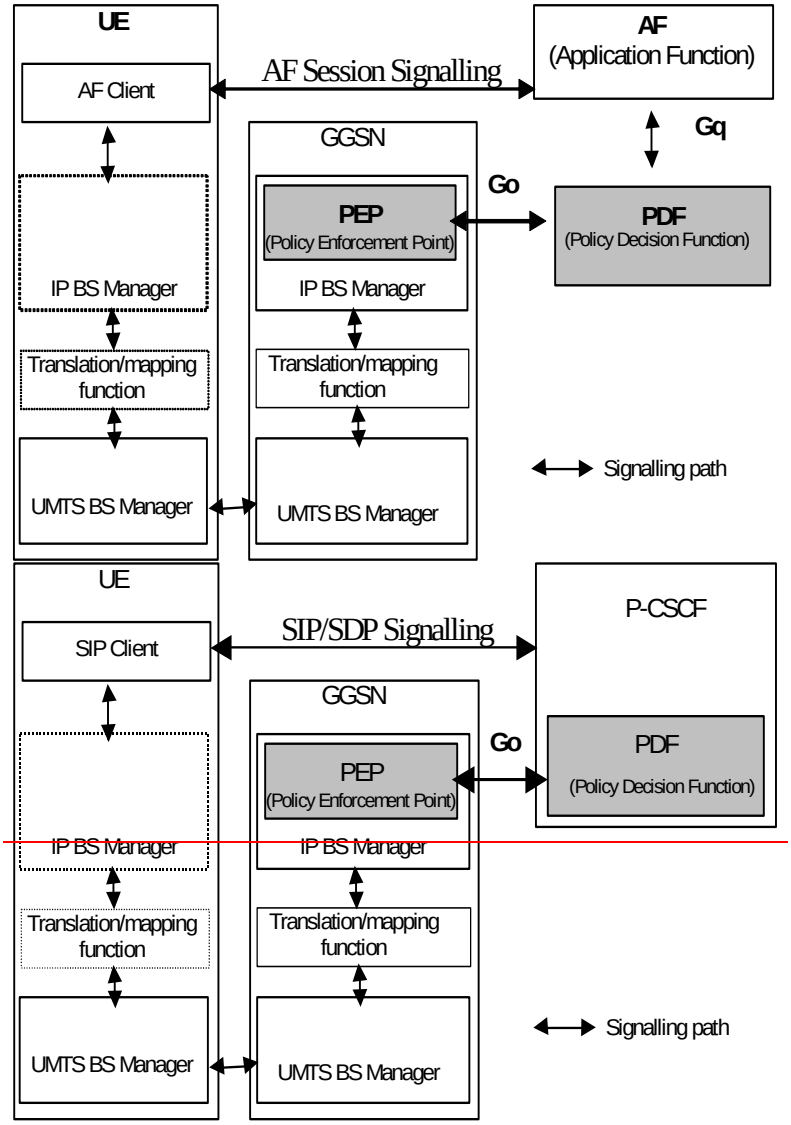
4.2 Go reference model

The Go interface is defined between the PDF and the GGSN (3GPP TS 23.002 [2]).

~~The PDF is a logical entity of the P-CSCF (if the PDF is implemented in a separate physical node, the interface between the PDF and P-CSCF is not standardised).~~

The ~~P-CSCF (~~PDF~~)~~ is in the same PLMN as the GGSN.

The relationships between the different functional entities involved are depicted in figure 4.2.



NOTE: For clarity in the diagram, network elements that are not involved in service-based local policy are not presented here (e.g. radio network elements, SGSN, etc).

Figure 4.2: Go interface architecture model

4.3 Functional elements and capabilities

4.3.1 GGSN

4.3.1.1 Service-based local policy enforcement point

The Policy Enforcement Point (PEP) is a logical entity which resides in the GGSN and communicates with the PDF regarding Service-based local policy (SBLP) control. Hereafter in the present document, the GGSN is assumed to contain the PEP implicitly unless otherwise stated. The GGSN sends requests to and receives decisions from the PDF. The GGSN may cache the policy decision data of the PDF decisions. This cached information may be used later for a local policy decision allowing the GGSN to make policy control decision about the QoS authorization for PDP context modifications without requiring additional interaction with the PDF in case the modification request does not exceed the previously authorized QoS.

The following policy enforcement point functionalities for SBLP in the GGSN are identified:

- Policy based Authorisation:

The GGSN requests authorisation information from the PDF for the IP flows carried by a PDP context. The GGSN enforces the PDF decisions for this PDP context.

The GGSN shall enforce unsolicited authorisation decisions which update the QoS and packet classifiers.

Additionally, policy-based authorisation ensures that the resources, which can be used by the PDP context are within the "Authorised QoS" specified by the PDF. This information is mapped by the Translation/mapping function in the GGSN to give the authorised resources for GPRS bearer admission control.

The GGSN shall also report to the PDF its success or failure in carrying out the PDF decision.

- Policy based gating functionality:

  Policy based gating functionality represent the control of the GGSN over the Gate Function in the user plane, i.e. the forwarding of IP packets associated with a media component. In the user plane, a "gate" is defined for each IP flow of a media component. The PDF provides the gate description and the commands to open or close the gate. The gate description is received from the PDF in the authorisation decision. The command to open or close the gate shall be sent either in the authorisation decision or in subsequent decisions from the PDF.

- Indication of bearer release/modification to/from 0 kb/s:

  The GGSN shall inform the PDF when the bearer changes to or from a data rate of 0 kb/s (an indication of bearer loss/recovery), and at bearer release.

- Charging Correlation

  To ensure charging correlation, the PEP shall send the GCID and the GGSN address to the PDF. The PDF shall also send the ~~IMS~~ AF charging identifier, if available, to the GGSN.

Next modified Clause

4.3.1.5 Binding mechanism handling

The binding information is used by the GGSN to identify the correct PDF and subsequently request service-based local policy information from the PDF. The binding information associates a PDP context with one or more media components or IP flows of an ~~IMS~~ AF session. The GGSN may receive one or more sets of the binding information during an activation or modification of a secondary PDP context. Each set of binding information consists of an authorisation token and the flow identifier(s) related to the IP flow(s) within the same session

Next modified Clause

4.3.2 PDF

4.3.2.1 Service-based local policy decision point

The PDF functions as a Policy Decision Point for the service-based local policy control. The PDF makes policy decisions based on session and media related information obtained from the AF via the Gq interface~~P-CSCF~~. The PDF shall exchange the decision information with the GGSN via the Go interface.

The following policy decision point functionalities for SBLP are identified:

- Authorisation function:

  The PDF shall be able to provide an authorisation decision upon receiving a bearer authorisation request from the GGSN. The PDF shall authorise the request according to the stored session and media related information received from the ~~P-CSCF~~AF.

  The PDF shall use the binding information to determine the ~~IMS~~ AF session(s) and the set of IP flows. Multiple sets of binding information and multiple ~~IMS~~ AF sessions may be involved, if flows from separate

AF sessions are multiplexed in the same PDP context. Based on the IP flows, the PDF shall determine the authorised QoS, packet filters, and gate status to be applied. The authorised QoS specifies the maximum allowed QoS class, and the data rate for the set of IP flows identified in the binding information.

The PDF shall be able to provide updates to the authorisation decision, if receiving modified service information from the AF ~~at session modifications~~ which changes the QoS and packet classifiers for PDP contexts which are already established.

- Revoke function:

  The PDF may revoke the authorisation of resources at any time. Revoke Authorisation for GPRS and IP resources is communicated by the PDF to the GGSN.

- Approval of QoS Commit / Removal of QoS Commit:

  The PDF may allow or deny the usage of the PDP context for the selected IP flow(s) by controlling the correlated gate(s).

  The "Approval of QoS Commit" command may either be part of the authorisation decision, or the PDF may provide a separate decision with the "Approval of QoS Commit" command to open the gate.

  The "Removal of QoS Commit" command is a separate decision to close the gate(s) e.g. when a media IP flow(s) is put on hold.

- Actions due to Indication of bearer release:

  When the GGSN informs the PDF of bearer deactivation, the PDF shall remove the corresponding authorisation request state. Additionally, the PDF shall inform the ~~P-CSCF~~ AF about this deletion event.

- Actions due to Indication of bearer modification:

  When the PDF receives an indication of bearer modification of the maximum bitrate to or from 0 kbits/s, the PDF shall inform the ~~P-CSCF~~AF about this modification event.

- Generation of authorisation token:

  ~~During the session set up the~~The PDF generates an authorisation token for the ~~IMS~~ AF session as specified in 3GPP TS 29.209 [23].

- Mapping service information ~~SDP parameters~~ to "Authorized QoS" parameters:

  To perform proper authorisation, the PDF shall map the necessary service information ~~SDP parameters~~ containing session and media related information to "Authorized QoS" parameters.

- Charging identifiers exchange:

  The PDF shall send the AF charging information (e.g. ICID if the AF is P-CSCF), if provided by the ~~P-CSCF~~AF, as part of the initial authorisation decision(s) for ~~of~~ all the bearer authorization request(s) that correspond to the respective ~~SIP~~ AF session.

  When the PDF receives the GCID together with the GGSN address from the GGSN, it shall forward this information to the ~~P-CSCF~~AF to ensure charging correlation.

4.3.2.2 Initialisation and maintenance

The PDF shall comply to the procedures described in RFC 2748 [7] for the initialisation and maintenance of the COPS protocol over the Go interface.

4.3.2.3 Binding mechanism handling

The binding information is used by the GGSN to identify the correct PDF and subsequently request service-based local policy information from the PDF. Each set of binding information consists of an authorisation token and one or more flow identifier(s).

~~During the session set up the~~The PDF generates an Authorisation Token for the ~~IMS~~ AF session as specified in 3GPP TS 29.209 [23]. ~~as described in RFC 3313 [22].~~ The Authorisation token shall be sent to the ~~P-CSCF~~AF which forwards it to the UE in the ~~SIP~~ AF session signalling. The PDF shall ~~allocate~~ provide its PDF identifier as part of the Authorization Token. This identifier shall be in the format of a fully qualified domain name.

The PDF receives the binding information and a Client Handle as part of a REQ from the GGSN. The PDF shall store the Client Handle for each flow identifier identified by the binding information for subsequent message exchanges.

The authorisation token is applied by the PDF to identify the ~~IMS~~ AF session. If flows from separate AF sessions are multiplexed in the same PDP context, there are more than one authorization token~~s~~, and the PDF identifies one ~~IMS~~ AF session per each token. If no ~~IMS~~ AF session can be found for an authorisation token, or if the authorization token for the Client Handle has been modified, or if the PDF is otherwise unable to authorise the binding information, the PDF shall send a COPS decision message carrying both an INSTALL and REMOVE decision. The INSTALL decision shall identify an authorisation failure to the GGSN, and may include further details identifying the cause. The REMOVE decision shall subsequently remove this state from the GGSN. For an initial authorisation, the PDF shall then initiate a remove for the authorisation request.

For a valid authorisation token the flow identifier(s) ~~is~~ are used to select the available information on the IP flows of this ~~IMS~~ AF session. The PDF sends the available authorisation information back to the GGSN. If there are more than one authorization tokens per client handle, the authorization information comprises an aggregate of the information of all related flows. If the PDF has already communicated authorisation for the same authorisation token and flow identifier(s) to this (or another) GGSN on this ~~IMS~~ AF session, then the previous authorisation shall be revoked, and this revocation shall be communicated to the appropriate GGSN.

If the binding information consists of more than one flow identifier, the PDF shall also verify that the media components identified by the flow identifiers are allowed to be transferred in the same PDP context. If any of these media components was mandated to be carried in a separate PDP Context, the PDF shall send a COPS decision message carrying both an INSTALL and REMOVE decision. The INSTALL decision shall identify an authorisation failure to the GGSN, and may include further details identifying the cause. The REMOVE decision shall subsequently remove this state from the GGSN. For an initial authorisation, the PDF shall then initiate a remove for the authorisation request.

For a valid binding information consisting of more than one flow identifier, the information sent back to the GGSN shall include the aggregated QoS for all the IP flows and suitable packet filter(s) for these IP flows. If there are more than one sets of binding information per client handle, the authorization information comprises an aggregate of the information of all related flows. Each flow identifier within the binding information can identify one or more IP flows of a single media component.

5 Policy control procedures

5.1 GGSN

5.1.1 Initial authorization at PDP context activation

The GGSN may receive binding information during the activation of a secondary PDP context by the UE. To perform initial authorization at the secondary PDP context activation the GGSN shall send an authorisation request to the PDF including the binding information received from the UE.

The GGSN identifies the required PDF from the authorisation token of the binding information. The authorisation token is formatted according to the structure of the policy element AUTH_SESSION defined in RFC 3520 [11]. The policy element AUTH_SESSION shall include the AUTH_ENT_ID and the SESSION_ID attributes. The GGSN checks for that Policy Element and retrieves the AUTH_ENT_ID attribute from this. If this is in the form of a Fully Qualified Domain Name, then this is used to identify the correct PDF.

The GGSN authorisation request message to the PDF shall allow the GGSN to request policy information for authorisation of the IP flows identified by the flow identifiers within the binding information carried by a PDP context.

When the GGSN receives the PDF decision, the GGSN shall enforce the policy decision. To enforce the policy decision, the GGSN shall install the packet filters received from the PDF, and ignore the UE supplied TFT.

If the PDF decision information indicates that the binding information provided by the GGSN is authorised, the GGSN shall proceed with activation of the secondary PDP context. The GGSN shall map the authorized QoS resources into authorized resources for the bearer admission control.

To ensure charging correlation, the GGSN shall send the GCID and GGSN address information to the PDF after the successful establishment of the secondary PDP context, i.e. with the report following the initial authorization decision.

When the PDF detects that the binding information provided by the GGSN is not associated with an ongoing ~~SIP~~ AF session at application layer, or is otherwise unable to authorise the binding information, the GGSN will receive a COPS decision message from the PDF carrying both an INSTALL and REMOVE decision. The reason for the rejection is indicated by the INSTALL decision with an appropriate authorisation request failure reason. The GGSN shall reject the secondary PDP context activation with a corresponding error code, see annex D. The GGSN shall subsequently remove this state according to the REMOVE decision. For an initial authorisation request, the GGSN shall then send a COPS Delete Request State (DRQ) message to the PDF to remove the state in the GGSN and the PDF.

When the GGSN sends an authorization request to the PDF but the PDF does not respond with the decision message or the communication between the GGSN and the PDF fails, the GGSN shall reject the secondary PDP context activation with the error code "Authorizing entity temporarily unavailable" (see annex D).

Next modified Clause

5.1.3 Session modification initiated decision

The PDF may receive updated service information from the AF, conveying information about an AF session modification. An AF session modification may occur that modifies the media ~~components~~ without adding or removing media components~~lines~~, for example, a change in the bandwidth for the media component~~line~~, or a change to the port number. The GGSN will receive unsolicited authorisation decision from the PDF due to such modifications.

When the GGSN receives an unsolicited authorisation decision from the PDF with updated QoS information, the GGSN shall update the stored authorised QoS. If the existing QoS of the PDP context exceeds the updated authorised QoS, the GGSN shall initiate a timer for the UE to modify the PDP context to decrease the QoS to within the authorised limit. At expiry of the timer, if the PDP context still exceeds the authorised QoS, the GGSN shall perform a network initiated PDP context modification to reduce the QoS to the authorised level.

When the GGSN receives an unsolicited authorisation decision from the PDF, the GGSN shall also install the new set of packet classifiers, removing any existing packet classifiers that are not included in the new set.

5.1.4 PDP context deactivation

The GGSN is responsible for notifying the PDF when a procedure of a PDP context deactivation is performed. In case of a PDP context deactivation, the GGSN shall inform the PDF of the bearer release related to the ~~SIP~~ AF session(s) by sending a COPS Delete Request State (DRQ) message.

When a revoke authorisation procedure is performed, the GGSN receives a decision message from the PDF for disabling the use of the "Authorised QoS" resources and deactivation of the PDP context associated with the binding information. The GGSN shall disable the use of the "Authorized QoS" resources. The GGSN shall initiate deactivation of the PDP context in case that the UE has not performed it yet.

Next modified Clause

5.2.1.1 SBLP authorisation decision

The service information needed ~~for~~ in the PDF to perform media authorization is ~~passed~~ provided by the ~~P-CSCF~~AF ~~upon receiving a SIP message that contains SDP~~ via the Gq interface. The Gq interface between the AF and the PDF is specified in the 3GPP TS 29.209 [23].

The PDF should authorize all media components if no application ID is available within the service information.

~~The SDP contains sufficient information about the session, such as the end-points' IP address and port numbers and bandwidth requirements.~~

~~All media components in the SDP are authorised. The media components contain one or more IP flows each represented by a flow identifier. The definition of flow identifier is in subclause 3.1. The P-CSCF shall send policy set-up information to the PDF upon every SIP message that includes an SDP payload. This ensures that the PDF passes proper information to perform media authorization for all possible IMS session set-up scenarios. The policy set-up information provided by the P-CSCF to the PDF for each media component shall contain the following:~~

- ~~Destination IP address;~~
- ~~Destination port number;~~
- ~~Transport Protocol id;~~
- ~~Media direction information;~~
- ~~Direction of the source (originating or terminating side);~~
- ~~Indication of the group that the media component belongs to;~~
- ~~Media type information;~~
- ~~Bandwidth parameters;~~
- ~~Indication of forking/non-forking.~~

~~Additionally, upon the P-CSCF receiving the ICID in SIP signalling, it shall send the ICID to the PDF.~~

The PDF stores the authorised policy information based on the service information received from the AF, and ~~generates~~ uses an Authorisation Token to identify this decision. ~~The Authorisation Token is passed back to the P-CSCF for inclusion in the SIP signalling back to the UE.~~

The Authorisation Token is in the form of a Session Authorisation Data Policy Element as described in RFC 3520 [11]. The PDF shall include an AUTH_ENT_ID attribute containing the Fully Qualified Domain Name of the PDF and the SESSION_ID attribute.

Upon receiving the bearer authorization request from the GGSN, the PDF shall authorize the request according to the stored service based local policy information for the session(s) identified by the binding information in the request.

- Decision on the binding information:
  - The authorisation shall contain the decision on verifying the binding information. The PDF shall identify whether each set of the binding information indeed corresponds to an initiated ~~SIP~~ AF session. If the corresponding ~~SIP~~ AF session cannot be found for a set of binding information or the binding information contains invalid flow identifier(s), or the authorization token(s) has changed in an authorization modification request, the PDF shall enforce the rejection of this PDP context request by sending an INSTALL and REMOVE decision to the GGSN. The reason for the rejection is indicated by the INSTALL decision with the "noCorrespondingSession" reason in the Authorisation Request Failure Decision. If the PDF is otherwise unable to authorise the binding information, the INSTALL decision shall identify a general authorisation failure with the "authorisationFailure" of the request reason in the Authorisation Request Failure Decision.
  - If the PDF is unable to get sufficient service information from the AF to authorise the binding information, the PDF may enforce the rejection of this PDP context request by sending an INSTALL and REMOVE decision to the GGSN. The reason for the rejection is indicated by the INSTALL decision with the "authorisationFailure" reason in the Authorisation Request Failure Decision.
  - The authorization shall also contain the decision on the list of flow identifiers contained in the bearer authorisation request sent by the GGSN representing the IP flows of the media components intended to be carried in the same PDP Context. This decision shall verify that these IP flow(s) are indeed allowed to be carried in the same PDP Context. The PDF shall make this decision by comparing the list of flow identifiers contained in the bearer authorization request received from the GGSN to the media component grouping indication information received from the ~~P-CSCF~~AF.
  - In case the UE violates the ~~IMS~~ AF level indication, and attempts to set up IP flows of multiple ~~IMS~~ media components in a single PDP context despite of an indication that mandated separate PDP contexts, the PDF shall enforce the rejection of this PDP context request by sending an INSTALL and REMOVE decision to the GGSN. The reason for the rejection is indicated by the INSTALL decision with the "invalidBundling" reason in the Authorisation Request Failure Decision.

- If the sets of binding information and the list of flow identifiers are successfully authorised (verified) as per the means described above, the PDF shall also communicate the authorisation details to the GGSN.
- If the PDF has already communicated authorisation for the same authorisation token(s) and flow identifier(s) to this (or another) GGSN, then the previous authorisation shall be revoked, and this revocation shall be communicated to the GGSN.
- The authorisation details contain the "Authorised QoS" and the packet classifier(s) of the IP flows. In case of an aggregation of multiple media components within one PDP context, the combination of the "Authorised QoS" information of the individual IP flows of the media components is provided as the "Authorised QoS".
- Based on the media direction information and the direction of the source provided by the ~~P-CSCF~~AF, the PDF shall define the direction (upstream or downstream) of the "Authorised QoS" and the packet classifier(s).

- Packet classifier(s):
  - The PDF shall derive the uplink and downlink packet classifiers from the IP addresses and port numbers for uplink and downlink IP flows provided by the AF as part of the service information. The PDF should not modify the address and port information received from the AF.~~The uplink packet classifier shall be formed as follows: The destination address and port number shall be taken from the connection information parameter of the SDP sent by the P-CSCF in downlink direction, while the source IP address may be formed from the address present in the SDP received by the P-CSCF in uplink direction (taking into account only the 64 bit prefix of the address), and the source port number shall be wildcarded. For example, assuming UE-A sends an SDP to UE-B, the PDF of UE-B uses the address present in this SDP for the destination address of UE-B's uplink packet classifier, while the PDF of the UE-A uses the 64 bit prefix of the same address for the source address of UE-A's uplink packet classifier. If the source address is not formed from the 64 bit prefix, the source address shall be wildcarded.~~

  ~~- The downlink packet classifier shall be formed as follows: The destination address and port number shall be taken from the connection information parameter of the SDP received by the P-CSCF in uplink direction, while the source IP address may be formed (in order to reduce the possibilities of bearer misuse) from the destination address in the SDP sent by the P-CSCF in downlink direction (taking into account only the 64 bit prefix of the address) and the source port number shall be wildcarded. For example, assuming UE-A sends an SDP to UE-B, the PDF of UE a uses the address present in this SDP for the destination address of UE-A's downlink packet classifier, while the PDF of UE-B uses the 64 bit prefix of the same address for the source address of UE-B's downlink packet classifier. If the source address is not formed from the 64 bit prefix, the source address shall be wildcarded.~~

  - The PDF shall send the destination address and the destination port number for each IP flow associated with the media component.

- "Authorized QoS":
  - The "Authorised QoS" information (consisting of maximum QoS Class and Data Rate) for IP flows of ~~a~~ media ~~component~~ is extracted from the service information received from the AF, e.g. from the media type information, ~~and~~ bandwidth information and AF application ID~~parameter(s) of the SDP~~. The PDF ~~shall map~~should select the ~~media type information into a~~ QoS Class which is the highest class that can be used for the media. The PDF shall use an equal QoS Class for both the uplink and the downlink directions when both directions are used. ~~As an example, the audio media type shall be mapped into QoS class A.~~
  - The PDF shall derive the Data Rate value for the ~~media~~ IP flow (s) from the service information, e.g. from contained bandwidth information, received form the AF~~, e.g. in the IMS case from the "b=AS" SDP parameter, as detailed in TS 29.208 [18]. For the possibly associated RTCP IP flows, the PDF shall use the SDP "b=AS", "b=RR" and "b=RS" parameters, if present, as specified in 29.208[18]. The "b=AS", "b=RR" and "b=RS" parameters in the SDP contain all the overhead coming from the IP layer and the layers above e.g. UDP, RTP or RTCP~~.
  - For non-real-time bearers the Data rate value shall be considered as the maximum value of the 'Maximum bitrate' parameter.
  - In case of an aggregation of multiple media components within one PDP context, the PDF shall provide the "Authorised QoS" for the bearer as the combination of the "Authorised QoS" information of the individual IP flows of the media components. The QoS Class in the "Authorised QoS" for the bearer shall contain the

highest QoS class amongst the ones applied for the individual ~~media components~~ IP flows and indicates the highest UMTS traffic class that can be applied to the PDP context.

- The Data Rate of the "Authorised QoS" for the bearer shall be the sum of the Data Rate values of the individual media IP flows of components and it is used as the maximum Data Rate value for the PDP context.

- The detailed rules for calculating the "Authorized QoS" are specified in 3GPP TS 29.208 [18].

The PDF ~~may~~ shall either include the gate enabling command as part of the authorisation decision~~, for instance to enable early media. Alternatively~~, or the PDF may provide a separate decision for opening the gate, depending on the gating policy indicated as part of the service information received from the AF.

The PDF shall send the ~~IMS~~ AF charging identifier possibly provided by the ~~P-CSCF~~AF as part of the authorisation decision to the GGSN.

Upon receiving the modified ~~SDP~~ service information from the ~~P-CSCF~~AF, the PDF shall update the media authorization information for the session. The PDF may push this updated authorisation information to the GGSN. Under certain condition e.g. revoke of authorization, the PDF shall push the updated policy decision to the GGSN. If there are IP flows of several sessions under the same client handle, the PDF shall include the aggregate authorization information of all of these flows in the push decision.

5.2.1.2 Session modification initiated decision

The PDF may receive updated service information from the AF, conveying information about an AF session modification. A session modification may occur that modifies the media ~~components~~ without adding or removing media components~~lines~~, for example, a change in the bandwidth for the media component~~line~~, or a change to the port number.

When there are updates to the ~~SDP parameters for~~ media components ~~lines~~ which are currently authorised, the authorisation information (QoS, packet classifiers) may change. The updated information (QoS, packet classifiers) shall be pushed down to the GGSN using an unsolicited authorisation decision.

However, if the update ~~to the SDP parameters~~ for media components ~~lines~~ which are currently authorised happens in the way of only changing a bidirectional media (Flow status "ENABLED"~~a=sendrecv~~) to unidirectional (Flow status "ENABLED-UPLINK" or "ENABLED-DOWNLINK"~~a=sendonly or a=recvonly~~), then the updated QoS information shall not be pushed down to the GGSN. In this case “Removal of QoS commit” for the deactivated direction of the media shall be sent to the GGSN to close the gate in that direction.

5.2.1.3 SBLP revoke decision

Upon release of the only or the last ~~SIP~~ AF session of a given client handle (PDP context), the PDF shall send a revoke authorisation decision to the GGSN after an operator specific time. The revoke authorisation decision shall be sent for each handle (PDP context) related to the session as a separate decision to the GGSN corresponding to the previous SBLP authorisation decision.

The timer for a pending session release shall be terminated if the PDF receives an indication on the termination of all PDP context(s) related to the released session.

Additionally, when a media component which is bound to a PDP context is removed from an ~~SIP~~ AF session and the UE has not performed the corresponding modification or deactivation of the PDP context within an operator specific time the PDF shall revoke the authorisation for the set of IP flows of the media components on that PDP context.

The timer for a pending media component removal shall be terminated if the PDF receives either a new authorisation request with the same handle where the IP flows of that media component has been removed, or an indication of the termination of the PDP context.

NOTE: The values of the timers for session termination and media component removal might be different, e.g. to allow for some more time for the required modification of the PDP context.

If the PDF receives a request from a GGSN for the same authorisation token and flow identifier(s) that this (or another) GGSN was already communicated authorisation, then the previous authorisation shall be revoked, and this revocation shall be communicated to the GGSN.

5.2.1.4 SBLP gate decision

Updated service information received from the AF may demand that the PDF enables or disables IP flows. The PDF may send a gate decision ~~during the session set-up or~~ whenever the status of a media component changes during the session (e.g. the media IP flow(s) of a media component is put on hold or resumed, or a media component is removed), or when a session is released and the related IP flows are removed from a PDP context that multiplexes IP flows from several sessions. The PDF shall not send a gate decision to the GGSN before it has sent the initial authorisation decision. If the initial authorisation decision has already been sent, the PDF ~~may~~ shall send a gate decision to the GGSN to modify the status of one or several gate(s) on the user plane. The gate decision shall only contain the gate(s) for which the status was changed compared to the last authorisation or gate decision sent to the GGSN. The gate decision contains for each gate either the "Approval of QoS Commit" command to open the gate or the "Removal of QoS Commit" command to close the gate. The open gate command may either be a part of the authorization decision or the PDF may provide a separate decision with the "Approval of QoS Commit" command to open the gate. When a media IP flow is put on hold, the PDF may send the "Removal of QoS Commit" command to the GGSN to close the relevant gate – the possible RTCP gate shall be left open to keep the connection alive. The open gate command shall be used to resume the media from hold.

5.2.2 Support for SIP forking

The PDF shall be able to handle SIP forking when SBLP is applied. For the IMS, f~~F~~orking can occur as specified in 3GPP TS 23.228 [4].

~~The related UE procedures are described in 3GPP TS 24.229 [14].~~

5.2.2.1 Authorization of resources for forked responses

As part of the service information, the PDF is informed by the AF if the second or subsequent SIP early dialogoues are encountered within one SIP session. The AF provides separate service information for each SIP dialogue~~When a SIP session has been originated by a connected UE, the P-CSCF may receive multiple provisional responses due to forking before the first final answer is received~~. The PDF shall allocate the same authorization token to all the ~~forked responses and the corresponding~~ early dialogues within one AF session.

~~The UE and the P-CSCF become aware of the forking only when the second provisional response arrives.~~ For the second~~this~~, and any subsequent early dialogue~~provisional response~~, the PDF shall identify the existing authorization information for that session. The PDF shall authorize any additional media components and any increased QoS requirements for the previously authorized media components, as requested by the forked response. Thus, the QoS authorized for a media component shall be equal to the highest QoS requested for that media component by any of the forked responses. Authorization is done by the procedures for authorization request in subclauses 5.1.1 and 5.1.2 and SBLP decisions in subclause 5.2.1.1.

Additional packet classifiers as required by the subsequent responses are sent to the GGSN by the session modification initiated decision specified in subclause 5.2.1.2.

5.2.2.2 Updating the authorization information at the final answer

As part of the service information, the PDF is informed by the AF when the first SIP early dialogue ~~The PDF shall keep the authorization information requested for each of the individual early dialogues till the first final answer is received. Then the related early dialogue~~ is progressed to establish the final SIP session. All the other early dialogues are terminated. The authorization information for the SIP session is updated to match the requirements of the remaining early dialogue only. Several actions may be needed in the PDF:

- Only the packet classifiers and the QoS indicated by the first final answer shall remain authorized. This information shall be sent to the GGSN by the session modification initiated decision specified in subclause 5.2.1.2. This should be done without delay in order to reduce the risk for initial clipping of the media stream, and minimising possible misuse of resources.

- The authorization for PDP contexts that were used only for the terminated early dialogues, shall be revoked as specified in subclause 5.1.4.

- The PDF shall await new authorization requests for remaining PDP contexts with updated binding information to remove any media components that were authorized for the terminated early dialogues only. If necessary (i.e. after timeout), the authorization for these PDP contexts shall be revoked as specified in subclause 5.2.1.3.

EXAMPLE: Assume that three forked responses for a certain media component indicate the bandwidths 10 kbps, 30 kbps and 20 kbps, respectively. This media component will first be authorized for 10 kbps and then upgraded to 30 kbps, which will be its final value for the early dialogue phase. If the first final answer corresponds to the third forked, provisional response, then QoS is finally downgraded to 20 kbps.

Next modified Clause

6.3.2 Message description

The following messages and events are available on the Go interface (after the initial policy provisioning described in subclause 6.3.1.5):

- Authorisation_Request (REQ) (GGSN→PDF):

  This event allows the GGSN to request authorisation data from the PDF. It contains the following information:

  - Client Handle;
  - Binding Information.

  The R-type = 0x08 for configuration request is used here and M-type = 0x02 create event state is used here.

- Authorisation_Decision (DEC)(PDF→GGSN), contains an INSTALL decision:

  This event provides the GGSN with the relevant authorisation data. The event contains the following information:

  - Client Handle;
  - ICID(s) (only in the initial Authorisation_Decision). Only one ICID is transferred in this Release. The form of the ICID is defined in 3GPP TS 32.225 [21];
  - Unidirectional set (this parameter shall appear once for each direction (uplink and downlink)):
    - Direction indicator;
    - "Authorised QoS";
    - Gate description (this parameter shall appear once for each required gate for this direction):
      - Filter Specification - The information about the authorised IP end points addresses and ports is detailed below. The Filter Specification parameters are:
        - Source IP address;
        - Destination IP address;
        - Source ports;
        - Destination ports;
        - Protocol ID.

          The Source and Destination ports are described with a range consisting of a minimum and maximum value. If only one port is authorised, the minimum value and maximum value of the range are identical.

          A filter specification describing more than one IP flow shall be only used in case of identical Protocol IDs, IP addresses and successive port numbers (e.g. RTP and RTCP IP flow of a media component). Furthermore, the gate status of all IP flows described by this filter specification shall be identical, too.

The Base and IP Filter definitions from the IETF Framework PIB [15] shall be used in the 3GPP Go PIB to represent the filter specification. Only a subset of the available filter attributes shall be used. The attributes frwkIpFilterDscp, and frwkIpFilterFlowId in the filter description shall have their values set to –1, indicating a "match-all" wildcard condition, in effect a "not used" condition. The attribute frwkBaseFilterNegation shall have its value set to "false" to indicate not using negation, in effect a "not used" condition. The GGSN shall ignore them if they are set otherwise. Wildcarding of filter elements is detailed in Annex B.

- Gate status (opened/closed)

The R-type = 0x08 for configuration request is used here and M-type = 0x02 create event state is used here.

- Authorisation_Failure (DEC) (PDF→GGSN), contains an INSTALL and a REMOVE decision:

  This event provides the GGSN with an indication of an authorisation failure, and may carry additional reason details. The event contains the following information:

  - Client Handle;
  - Authorisation failure (including any provided reason information).

  The R-type = 0x08 for configuration request is used here and M-type = 0x04 terminate event state is used here.

- Gate Decision (DEC) (PDF→GGSN), contains an INSTALL decision:

  The Gate Decision indicates to the GGSN the new status of the gate(s) established for a client handle (PDP context). The gate status indicates to the GGSN that the gate shall be opened or closed. Only the gate(s) for which the status is changed are indicated by this event. The event contains the following information:

  - Client Handle;
  - Unidirectional set (this parameter shall appear once for each direction for which gates are being updated (uplink and/or downlink)):
    - Direction indicator;
    - Gate description (this parameter shall appear once for each gate to be modified for this direction) :
      - Filter Specification - The information about the authorised IP end points addresses and ports is detailed below. The Filter Specification parameters are:
        - Source IP address;
        - Destination IP address;
        - Source ports;
        - Destination ports;
        - Protocol ID.

          The Source and Destination ports are described with a range consisting of a minimum and maximum value. If only one port is authorised, the minimum value and maximum value of the range are identical.

          A filter specification describing more than one IP flow shall be only used in case of identical Protocol IDs, IP addresses and successive port numbers (e.g. RTP and RTCP IP flow of a media component). Furthermore, the gate status of all IP flows described by this filter specification shall be identical, too.

          The Base and IP Filter definitions from the IETF Framework PIB [15] shall be used in the 3GPP Go PIB to represent the filter specification. Only a subset of the available filter attributes shall be used. The attributes frwkIpFilterDscp, and frwkIpFilterFlowId in the filter description shall have their values set to –1, indicating a "match-all" wildcard condition, in effect a "not used" condition. The attribute frwkBaseFilterNegation shall have its value set to "false" to indicate not using

negation, in effect a "not used" condition. The GGSN shall ignore them if they are set otherwise. Wildcarding of filter elements is detailed in Annex B.

- Gate status (opened/closed)

NOTE: The opening of the gate may occur at the same time / be part of the authorisation decision event.

The R-type = 0x08 for configuration request is used here and M-type = 0x03 update event state is used here.

- Report (RPT) (GGSN→PDF):

  The GGSN sends a COPS RPT message as a response to a decision (DEC) message back to the PDF reporting that it enforced or not the Authorisation_Decision or the Authorization_Failure_Decision (Authorization_Report) or the Gate_Decision (Gate_Report).

  The events contain the following information:

  - Client Handle;
  - Success / Failure.

  In addition, the Authorization_report of the initial Authorisation_Decision includes:

  - GCID;
  - GGSN address.

- Report of state changes:

  The GGSN sends the report of state change message to the PDF reporting that the maximum bit rate for the PDP context is modified to 0 kbps or that the maximum bit rate for the PDP context is changed from 0 kbps.

  The event contains the following information:

  - Client Handle;
  - Maximum bit rate (set to 0 kbps / changed from 0 kbps).

- Delete Request State (DRQ) (GGSN→PDF):

  The GGSN informs the PDF via the delete request state message, that the PDP context is deactivated and the request state identified by the client handle is no longer available/relevant at the GGSN, so the corresponding state shall also be removed at the PDF.

  The DRQ message includes the reason why the request state was deleted.

  The event contains the following information:

  - Client Handle;
  - Reason code: ~~value 4 "Tear" indicating the deactivation of the PDP context.~~

    - Value 4 "Tear": This value is used when the PDP context has been deactivated as a result from normal PDP context signalling handling.
    - Value 7 "Insufficient bearer resources": This value is used when the PDP context has been deactivated due to insufficient bearer resources at the GGSN.

- Remove_Decision (DEC) (PDF→GGSN):

  The PDF uses the Remove_Decision to inform the GGSN that the PDF revokes the authorized resources for the client handle (PDP context). The Remove_Decision is a specific Decision message with the COPS Decision Flags object set to 0x02 ("Request-State" flag) and the Command-Code set to "REMOVE"; see IETF RFC 3084 [8].

  The event contains the following information:

  - Client Handle.

The R-type = 0x08 for configuration request is used here and M-type = 0x04 terminate event state is used here.

Next modified Clause

Annex B (normative): 3GPP Go PIB

Next modified Clause

```
go3gppAuthReqFailDecReason OBJECT-TYPE
    SYNTAX         INTEGER {
                     noCorrespondingSession (1),
                     invalidBundling (2),
                     authorizationFailure (3)
                   }
    STATUS         current
    DESCRIPTION
        "Reason for Auth Request Failure Decision given by PDF:

         noCorrespondingSession:       No corresponding session was found
                                       by the PDF

         invalidBundling:              In case the UE violates the IMS AF level indication
                                       and  attempts to set up multiple IMS AF media components
                                       in a single PDP context despite of an indication that
                                       mandated separate PDP contexts or if the list
                                       of flowidentifiers contained in the bearer authorization
                                       request doesn't match with the grouping indication
                                       information the PDF has received from the P-CSCFAF.

         authorizationFailure:         The PDF is unable to authorise the binding information.
                                       This is a generic failure indication that can be used
                                       if the actual reason is not any of the other specified
                                       reasons."
    ::= { go3gppAuthReqFailDecEntry 2 }
```

Next modified Clause

Annex C (normative): Flow identifiers: Format definition and examples

C.1 Format of a flow identifier

A flow identifier is expressed as a 2-tuple as follows:

<The ordinal number of the position of the media component description in the SDP"m=" line in the SDP, The ordinal number of the IP flow(s) within the media component description "m=" line assigned in the order of increasing uplink port numbers as detailed below>

where both are numbered starting from 1. The encoding of the flow identifier is as indicated in 3GPP TS 24.008 [12].

If UE and AF share an algorithm for a given application, which guarantees that UE and AF assign the same ordinal number to each media component, the ordinal numbers of the IP Flows within a media component shall be assigned according to the following rules:

- All IP flow(s) or bidirectional combinations of two IP flow(s) within the media component, for which an uplink destination port number is available, shall be assigned ordinal numbers in the order of uplink destination port numbers.

- All IP flows, where no uplink destination port number is available, shall be assigned the next higher ordinal numbers in the order of downlink destination port numbers.

The ordinal number of a media component shall not be changed when the session description information is modified.

For SDP, the flow identifier shall be assigned in the following way:

The ordinal number of the position of the "m=" line in the SDP	The ordinal number of the IP flow(s) within the “m=” line assigned in the order of increasing uplink destination port numbers, if uplink destination port numbers are available. For downlink or inactive unicast media IP flows, an uplink destination port number is nevertheless available, if SDP offer-answer according to RFC 3264 is used. The ordinal number of the IP flow(s) within the “m=” line assigned in the order of increasing downlink destination port numbers, if no uplink destination port numbers are available.

If no SDI with fixed and unique positions for media components is exchanged between UE and AF, the UE and AF may assign the ordinal numbers of the media components in another application-dependent algorithm which guarantees that UE and AF assign the same ordinal number to each media component.

If UE and AF do not share an algorithm for a given application, which guarantees that UE and AF assign the same ordinal number to each media component, the ordinal number of the media component shall be set to zero and the ordinal number of the IP flows shall be assigned according to the following rules:

1. If ordinal numbers for several IP flows are assigned at the same time, all uplink IP flows shall be assigned lower ordinal number than all downlink IP flows.
2. If ordinal numbers for several IP flows are assigned at the same time, all uplink and all downlink IP flows shall separately be assigned ordinal numbers according to increasing internet protocol number assigned by IANA (e.g. 8 for TCP and 17 for UDP)
3. If ordinal numbers for several IP flows are assigned at the same time, for each internet protocol with a port concept, all uplink and all downlink IP flows of this internet protocol shall separately be assigned ordinal numbers according to increasing port numbers.
4. If IP flows are removed from an existing session, the previously assigned binding info shall remain unmodified for the remaining IP flows.
5. If IP flows are added to an existing session, the previously assigned binding info shall remain unmodified and the new IP flows shall be assigned ordinal numbers following the rules 1. to 3., starting with the first previously unused ordinal number. The numbers freed in step 4. shall not be reused.

Next modified Clause

C.4 Example 3 without media components.

The UE and AF do not exchange SDP for an application and do not share an algorithm, which guarantees that UE and AF assign the same ordinal number to each media component.

At the AF session initiation, the UE and AF agree to set up the following IP flows:

- Uplink UDP flow with destination port 100.
- Downlink UDP flow with destination port 100.
- Downlink TCP flow with destination port 100.
- Uplink TCP flow with destination port 100.
- Uplink UDP flow with destination port 200.

The following binding info is assigned to these IP flows.

- Uplink UDP flow with destination port 100: (0, 2)
- Downlink UDP flow with destination port 100: (0, 5)
- Downlink TCP flow with destination port 100: (0, 4)
- Uplink TCP flow with destination port 100: (0, 1)
- Uplink UDP flow with destination port 200: (0, 3)

At a later stage in the session, the TCP IP flows are removed and the following IP flows are added:

- Uplink UDP flow with destination port 150.
- Downlink UDP flow with destination port 50.

The following binding info is assigned to the IP flows existing at this stage:

- Uplink UDP flow with destination port 100: (0, 2)
- Downlink UDP flow with destination port 100: (0, 5)
- Uplink UDP flow with destination port 200: (0, 3)
- Uplink UDP flow with destination port 150: (0, 6)
- Downlink UDP flow with destination port 50: (0, 7)

C.5 Example 4

In this example, the SDP “a=rtcp” attribute defined in IETF RFC 3605 is used.

An UE, as the offerer, sends a SDP session description, as shown in table C.5.1, to an application server (only relevant SDP parameters are shown):

Table C.5.1: The values of the SDP parameters sent by the UE in example 1.

```
v=0
o=ecsreid 3262464865 3262464868 IN IP6 2001:0646:00F1:0045:02D0:59FF:FE14:F33A
s=MM01
i=One unidirectional video media
t=3262377600 3262809600
m=video 50230 RTP/AVP 31
c=IN IP6 2001:0646:00F1:0045:02D0:59FF:FE14:F33A
a=recvonly
a=rtcp:53020
```

and receives the SDP parameters, as shown in table C.5.2, from the application server:

Table C.5.2: The values of the SDP parameters sent by the application server in example 1.

v=0 o=ecsreid 3262464865 3262464868 IN IP6 2001:0646:00F1:0045:02D0:59FF:FE14:F33A s=MM01 i=One unidirectional video media t=3262377600 3262809600 m=video 51372 RTP/AVP 31 c=IN IP6 2001:0646:000A:03A7:02D0:59FF:FE40:2014 a=sendonly a=rtcp:49320

From this offer–answer exchange of SDP parameters the UE and the PDF each creates a list of flow identifiers comprising the IP flows as shown in table C.5.3:

Table C.5.3: Flow identifiers in example 4.

Order of 'm='-line	Type of IP flows	Destination IP address / Port number of the IP flows	Flow identifier
1	RTP (Video) DL	2001:0646:00F1:0045:02D0:59FF:FE14:F33A / 50230	<1,2>
1	RTCP DL	2001:0646:00F1:0045:02D0:59FF:FE14:F33A / 53020	<1,1>
1	RTCP UL	2001:0646:000A:03A7:02D0:59FF:FE40:2014 / 49320	<1,1>

3GPP TSG-CN WG3 Meeting #33
Sophia Antipolis, France. 16th to 20th August 2004.

Tdoc ⌘N3-040615

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.208** **CR** **73** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Accumulated CR on Gq impacts
Source:	⌘	TSG_CN WG3
Work item code:	⌘	QoS1
Date:	⌘	24/08/2004
Category:	⌘	**B**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
Ph2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)
Rel-7 (Release 7)

Reason for change: ⌘ Introduction of Gq Interface between AF and PDF, allowing a split between P-CSCF and PDF and also supporting non-IMS AFs, as required according to stage 2 TS 23.207.

Summary of change: ⌘ The text is modified to allow for non-IMS applications and to cover impacts of the new Gq interface introduced in Rel-6.
Changes from the following TDOCs agreed by CN3 are included:

N3-030834	Gq interface impacts on signalling flows
N3-040128	Gq flows update for Diameter
N3-040217	Updates to resource reservation flow
N3-040236	Indication of PDF-initiated PDP Context Release
N3-040237	Updates to Authorize QoS resources callflows for IMS
N3-040242	Updates to Authorize QoS resources callflows
N3-040245	Updates to Other flows
N3-040247	Updates to IMS callflows
N3-040419	Media Component removal Callflow
N3-040341	Gq actions at PDP context release
N3-040423	General Description of QoS Mapping
N3-040420rev1	Mapping of Servivce Information
N3-040538	Using Diameter ASR only for session termination
N3-040546	Encoding of RTCP flow indication

Consequences if not approved: ⌘ Missing functionality compared to stage 2 requirements.
No support for Gq interface and non-IMS applications.

Clauses affected: ⌘ 1, 2, 3, 4, 5, 6, 7, new Annex B

Y N

Other specs affected:	⌘	X		Other core specifications	⌘ TS 29.207, CR #137; new TS 29.209
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

1 Scope

The present specification shows QoS signalling flows for resource reservation to provide end-to-end QoS. The flows are used as bases of developing QoS related protocol descriptions for new and existing specifications.

~~The relationship between SIP/SDP session level and the bearer level (RSVP and GPRS) in flows is described in 3GPP TS 24.228 [2].~~ The present specification adds detailed flows of Service Based Local Policy (SBLP) procedures over the Go and Gq interfaces and their relationship with the bearer level signalling flows over the Gn interface.

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

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 24.228: "Signalling flows for the IP multimedia call control based on SIP and SDP; Stage 3".

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

[4] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[5] 3GPP TS 26.234: "End-to-end transparent streaming service; Protocols and codecs".

[6] 3GPP TS 26.236: "Packet switched conversational multimedia applications; Transport protocols".

[7] 3GPP TS 29.207: "Policy control over Go interface".

[8] 3GPP TS 23.107: "Quality of Service (QoS) concept and architecture".

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

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

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

[12] 3GPP TS 29. 209: “Policy control over Gq interface”.

[13] IETF RFC 3388: “Grouping of Media Lines in the Session Description Protocol (SDP)”

[14] IETF RFC 3524: “Mapping of Media Streams to Resource Reservation Flows”

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 in 3GPP TS 29.207 [7]~~the following~~ apply.~~:~~

~~**QoS Class:** Class of QoS used in Authorized IP QoS parameters as specified in 3GPP TS 29.207 [7].~~

3.2 Abbreviations

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

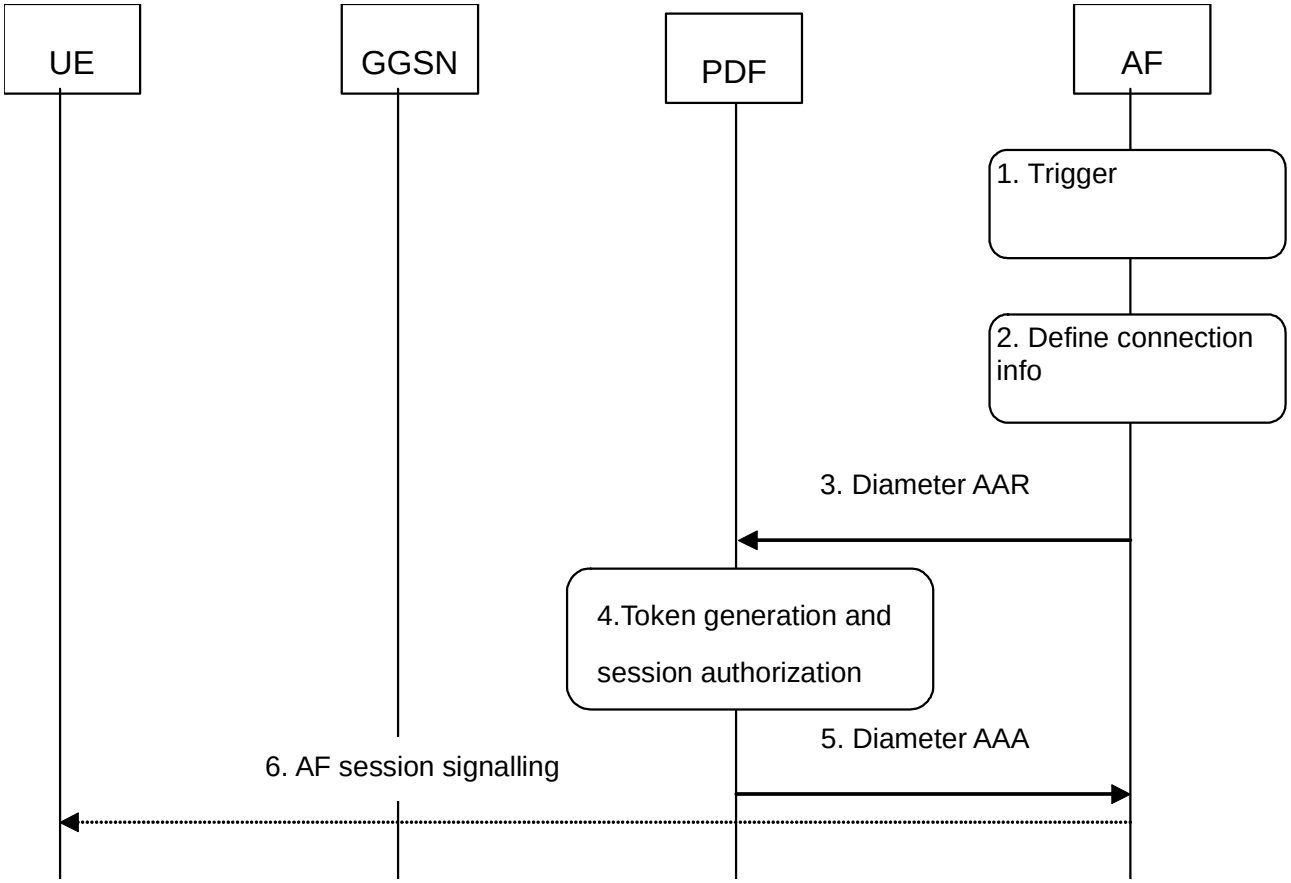
AF	Application Function
COPS	Common Open Policy Service protocol
DEC	COPS DECision message
DRQ	COPS Delete ReQuest state message
IMS	IP Multimedia CN Subsystem
PDF	Policy Decision Function
REQ	COPS REQuest message
RPT	COPS RePorT state message
SBLP	Service Based Local Policy

4 Authorize QoS resources

Editor's note: The Multi-Round feature of the Diameter base protocol is FFS.

4.1 Authorize QoS resources at AF session establishment~~originating PDF~~

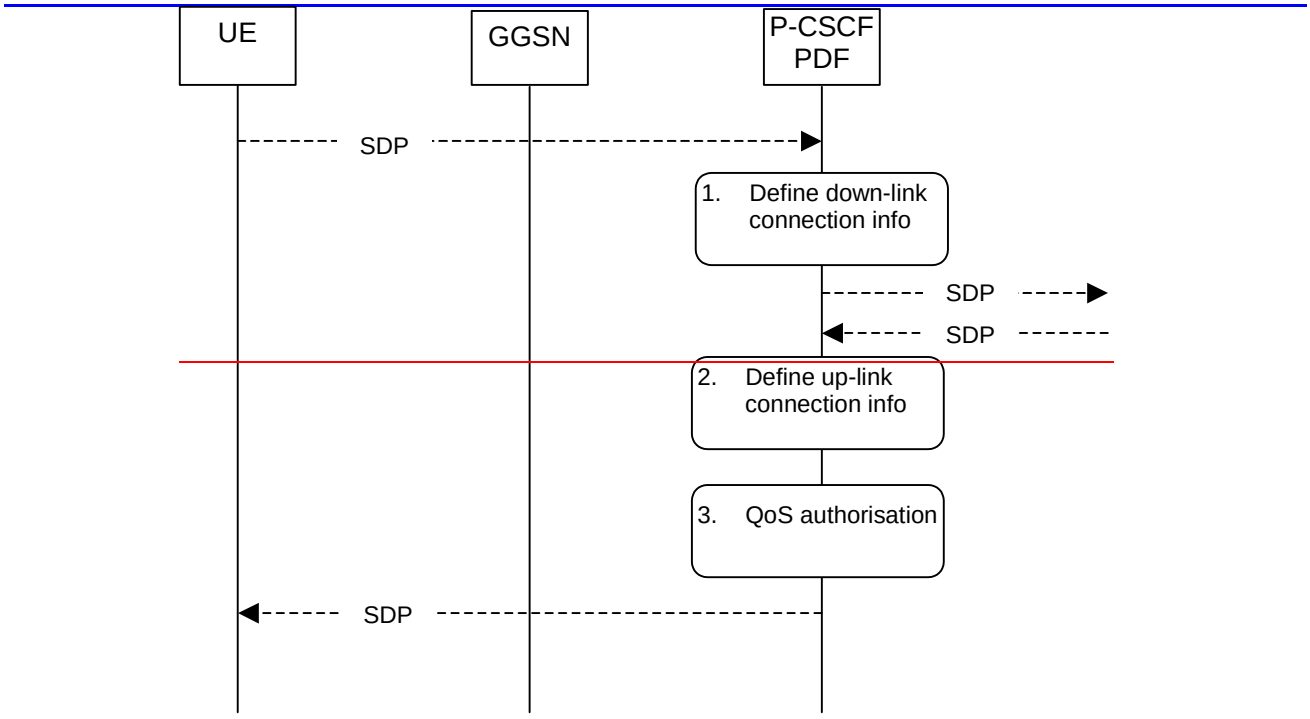
This clause covers the Authorize QoS resources procedure to be used when an AF session is established~~at the originating PDF~~.



Legend:

Mandatory

Optional



1. The AF receives an internal or external trigger to set up a new AF session.
2. The AF may identify the connection information needed (e.g. IP address of the IP flow(s), port numbers to be used etc…).

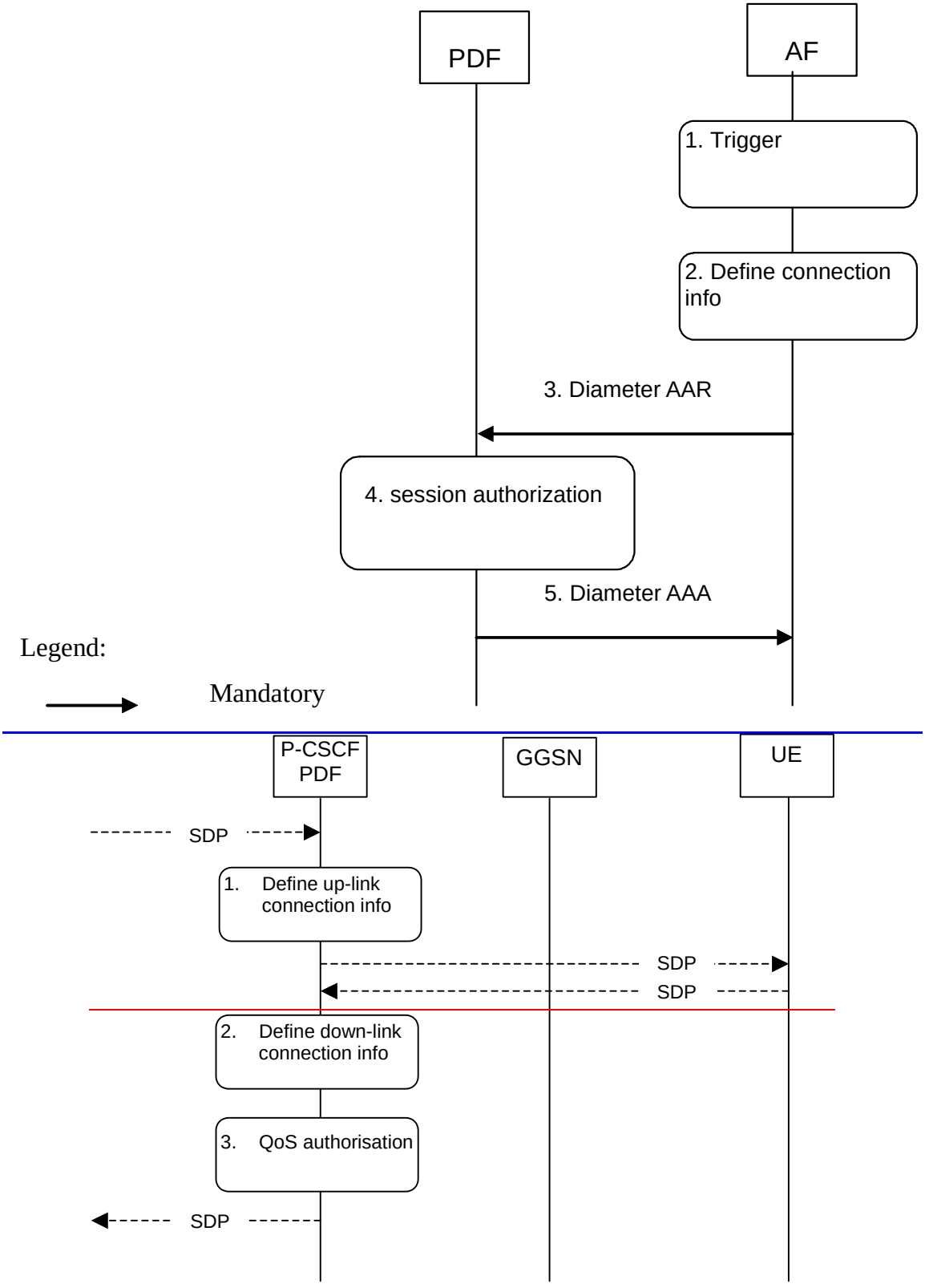
3. The AF requests the authorization token from the PDF by sending a Diameter AAR for a new Diameter session. The AF may instruct the PDF to request the full service information from the AF at resource reservation. The AF may also forward the part of or the entire service information at this stage in order to define the QoS resource authorisation.
4. The PDF authorizes the possibly received service information. The PDF generates the Authorization Token.
5. An authorization token is sent to the AF.
6. The Authorization token may be passed to the UE within AF session signalling.

~~1. The P-CSCF(PDF) gets the SDP parameters defined by the originator and identifies the connection information needed (IP address of the down link IP flow(s), port numbers to be used etc…).~~
~~2. The P-CSCF(PDF) gets the negotiated SDP parameters from the terminating side through SIP signalling interaction. The P-CSCF(PDF) identifies the connection information needed (IP address of the up-link media IP flow(s), port numbers to be used etc…).~~
~~3. The P-CSCF(PDF) uses the SDP parameters in order to define the QoS resource authorisation. The PDF authorises every component negotiated for the session. The authorization shall be expressed in terms of IP QoS parameters. An authorization token is generated by the PDF and sent to the UE.~~

Figure 4.1: Authorize QoS resources at session establishment~~originating PDF~~

4.2 Authorize QoS resources at AF session modification~~terminating PDF~~

This clause covers the Authorize QoS resources procedure at AF session modification~~the terminating PDF~~.



1. The AF receives an internal or external trigger to modify the service information for an existing AF session.

2. The AF may identify the connection information needed (e.g. IP address of the IP flow(s), port numbers to be used etc…).
3. The AF sends a Diameter AAR for an existing Diameter session and includes updated service information.
4. The PDF authorizes the received service information. The PDF may need to approve or remove the QoS commit (see Clauses 6.1 and 6.2, respectively) or perform a Session modification initiated SBLP authorization decision (see Clause 6.6) due to the updated service information.
5. The PDF answers with a Diameter AAA.

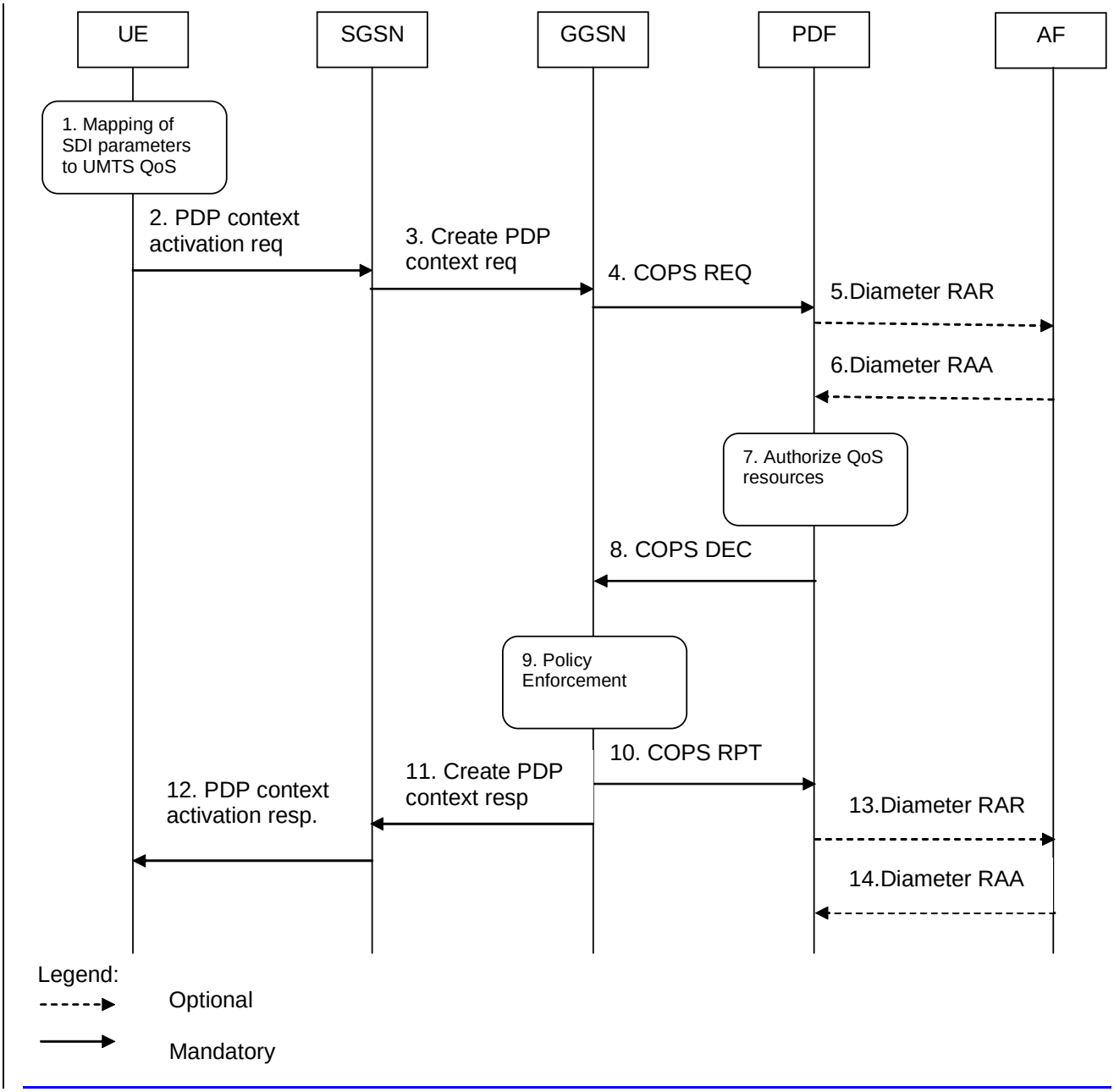
~~1. The P-CSCF(PDF) gets the SDP parameters defined by the originator and identifies the connection information needed (IP address of the up-link IP flow(s), port numbers to be used etc…). An authorization token is generated by the PDF and sent to the UE.~~
~~2. The P-CSCF(PDF) receives the negotiated SDP parameters from the UE. The P-CSCF(PDF) identifies the connection information needed (IP address of the down-link IP flow(s), port numbers to be used etc…).~~
~~3. The P-CSCF(PDF) uses the SDP parameters in order to define the QoS resource authorisation. The PDF authorises every IP flow of a media component negotiated for the session. The authorization shall be expressed in terms of IP QoS parameters.~~

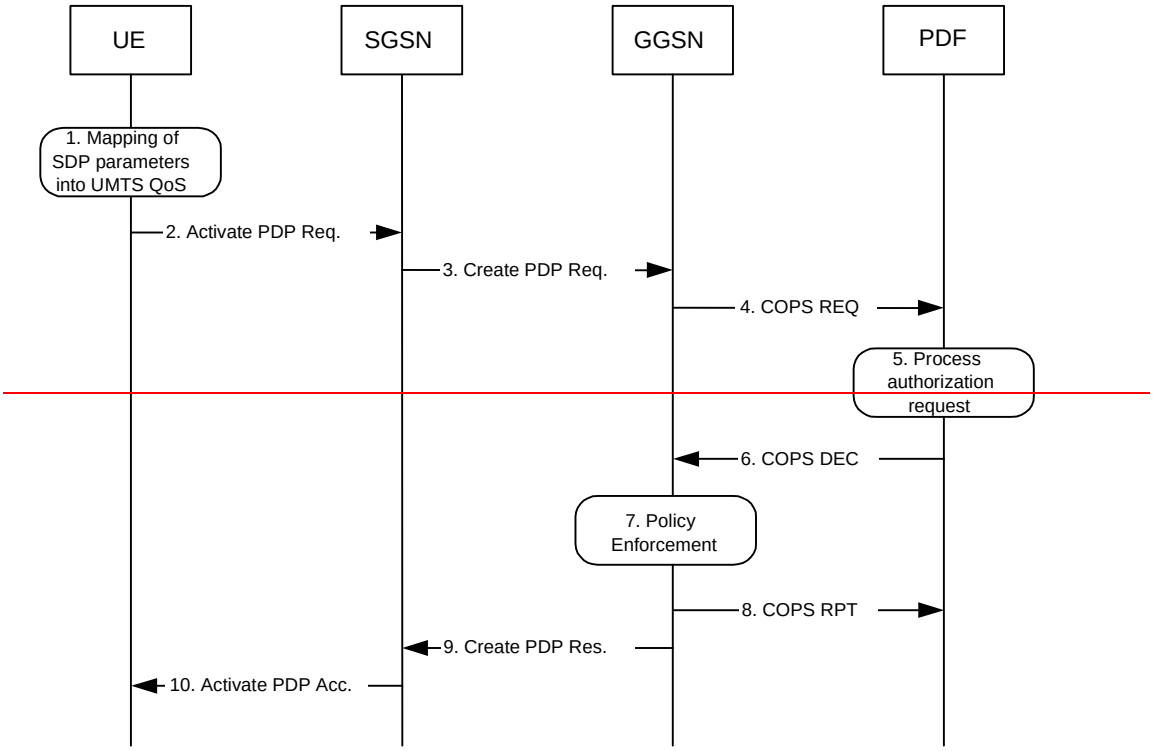
Figure 4.2: Authorize QoS resources at AF session modification~~terminating PDF~~

5 Resource reservation flow with Service-based local policy

This clause describes a resource reservation flow with service based local policy. The service based local policy is done via exchange of information through the Go and Gq interfaces. The Go and Gq interfaces allow~~s~~ the service based local policy and QoS interworking information to be requested by the GGSN from a PDF and the AF.

~~Figure 5.1 presents the "Resource Reservation" procedure at PDP context activation to both the Mobile Originating (MO) side and Mobile Terminating (MT) side.~~


UE
SGSN
GGSN
PDF
AF
1. Mapping of SDI parameters to UMTS QoS
2. PDP context activation req
3. Create PDP context req
4. COPS REQ
5.Diameter RAR
6.Diameter RAA
7. Authorize QoS resources
8. COPS DEC
9. Policy Enforcement
10. COPS RPT
11. Create PDP context resp
12. PDP context activation resp.
13.Diameter RAR
14.Diameter RAA
Legend:
Optional
Mandatory



1. The UE may use SDI or application specific settings in order to define the UMTS QoS parameter needed to request a PDP context.
2. The UE sends a PDP context activation request to the SGSN. The UE shall include binding information in the PDP context activation message to associate the PDP context bearer with policy information.
3. The SGSN carries out the procedures identified in 3GPP TS 23.060 [4] related to the PDP context activation and sends a Create PDP context request to the GGSN.
4. The GGSN receives the PDP context activation request with the binding information. The GGSN uses the authorisation token in order to localise the PDF. The GGSN sends a COPS REQ message to the PDF and includes the binding information.
5. A PDF generated authorization token enables the PDF to identify the authorisation status information. The PDF sends an authorisation request to that AF, if instructed by the AF in the initial authorisation request from the AF.
6. If step 5 happens, the AF sends the service information to the PDF.
7. The PDF performs the authorization decision.
8. The decision taken by the PDF is returned via the COPS DEC message. The DEC message includes the policy information to be used by the GGSN in order to perform the policy-based admission control.
9. The GGSN enforces the PDF policy decision on the IP flows based on the received authorization information from the PDF for the media components carried by the PDP context.
10. The GGSN sends COPS RPT message back to the PDF and reports its success or failure in carrying out the PDF decision.
11. The GGSN accepts the PDP context request based on the results of the authorisation policy decision enforcement. If the requested QoS parameters are not within the authorized QoS, the GGSN downgrades the requested UMTS QoS parameters.
12. The SGSN sends an Activate PDP Context Accept message to the UE indicating that the PDP context has been activated and that the QoS requirements have been authorized for both downlink and uplink.
13. The PDF may send an indication for the successful bearer establishment, which contains the received GPRS charging information to theAF.
14. If step 13 happens, the AF sends an answer back to the PDF.

Figure 5.1: Resource reservation flow with service based local policy

~~**1. Mapping from SDP to UMTS QoS parameters**~~

~~The UE uses the SDP parameters in order to define the UMTS QoS parameter needed to request a PDP context. The QoS parameter mapping mechanism is described in clause 7.2.~~

~~**2. GPRS: Activate PDP Context Request (UE to SGSN)**~~

~~The UE sends an Activate PDP Context Request message to the SGSN with the UMTS QoS parameters. The UE shall include binding information in the PDP context activation messages to associate the PDP context bearer with policy information. The authorization token is sent by the P-CSCF to the UE during SIP signalling.~~

~~**3. GPRS: Create PDP Context Request (SGSN to GGSN)**~~

~~The SGSN carries out the procedures identified in 3GPP TS 23.060 [4] related to the PDP context activation.~~

~~**4. COPS: REQ (GGSN to PDF)**~~

~~The GGSN receives the PDP context activation request with the binding information. The GGSN uses the authorisation token in order to localise the PDF. The GGSN sends a COPS REQ message to the PDF and includes the binding information.~~

~~**5. Process Resource Request (PDF)**~~

~~The PDF receives the information sent by the GGSN. The PDF identifies the multimedia session by using the binding information. The PDF performs an authorization decision. The PDF may include the gate enabling command as part of the authorisation decision, for instance to enable early media as described in 3GPP TS 29.207 [7]~~

~~**6. COPS: DEC (PDF to GGSN)**~~

~~The decision taken by the PDF is returned via the COPS DEC message. The DEC message includes the policy information to be used by the GGSN in order to perform the policy based admission control.~~

~~**7. Policy Enforcement (GGSN)**~~

~~The GGSN enforces the PDF policy decision on the IP flows based on the received authorization information from the PDF for the media components carried by the PDP context.~~

~~**8. COPS: RPT (GGSN to PDF)**~~

~~The GGSN sends COPS RPT message back to the PDF and reports its success or failure in carrying out the PDF decision.~~

~~**9. GPRS: Create PDP Context Response (GGSN to SGSN)**~~

~~The GGSN accepts the PDP context request based on the results of the authorisation policy decision enforcement. If the requested QoS parameters are not within the authorized QoS, the GGSN downgrades the requested UMTS QoS parameters.~~

~~**10. GPRS: Activate PDP Context Accept (SGSN to UE)**~~

~~The SGSN sends an Activate PDP Context Accept message to the UE indicating that the PDP context has been activated and that the QoS requirements have been authorized successfully for both downlink and uplink.~~

6 Other flows over Go and Gq interfaces

6.1 Approval of QoS commit

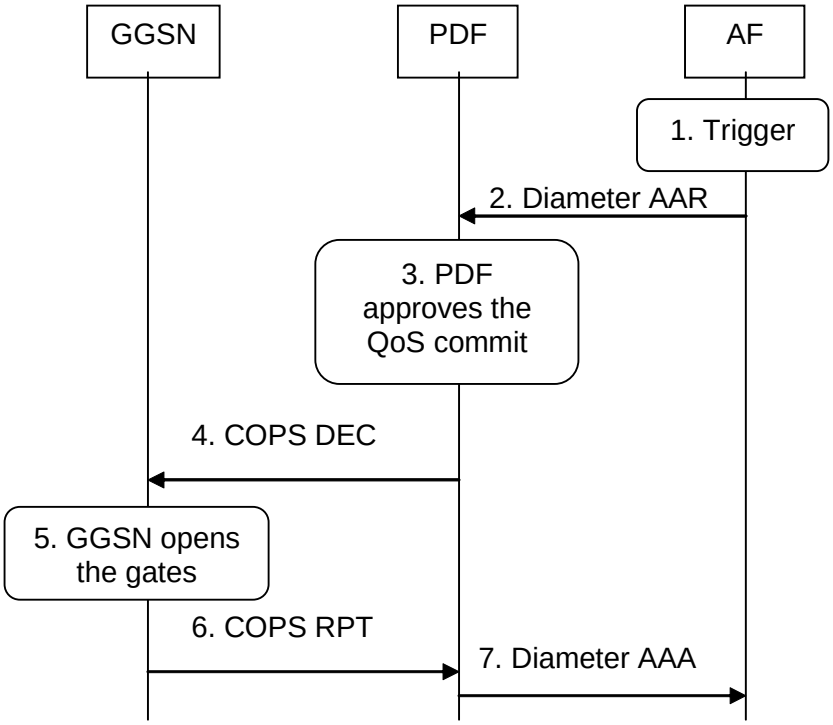
Through the Approval of QoS Commit procedure the PDF makes a final decision to enable the allocated QoS resource for the authorized IP flows of the media component (s) if the QoS resources are not enabled at the time they are authorized by the PDF, or if previously disabled~~the media~~ IP flow(s) or media components ~~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)~~.

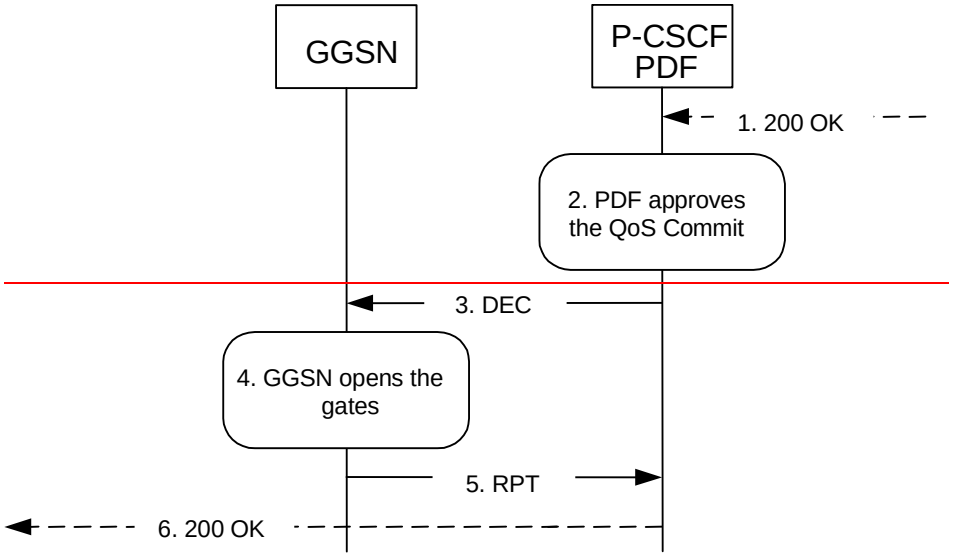
~~The Approval of QoS Commit procedure is triggered by the P-CSCF receiving a 200 OK response to an INVITE request or a 200 OK response to an UPDATE request within a confirmed dialogue. When receiving those 200 OK responses, the PDF shall take the SDP direction attribute in the latest received SDP (either within the 200 OK or a previous SIP message) into account when deciding, which gates shall be opened:~~

- ~~For a unidirectional SDP media component, the Approval of QoS Commit procedure shall not be triggered for the possible media IP flows in the opposite direction.~~

- For an inactive SDP media component, the Approval of QoS Commit procedure shall not be triggered for the media IP flows.

Figure 6.1 is applicable to the Mobile Originating (MO) side and the Mobile Terminating (MT) side.





1. The AF receives an internal or external trigger.
2. The AF sends a Diameter AAR to the PDF, requesting that gates shall be opened.
3 The PDF approves the QoS Commit.
4. The PDF sends COPS DEC message(s) to the GGSN to open the 'gates' e.g. enable the use of the authorised QoS resources.
5. The GGSN receives the COPS DEC message(s) and opens the 'gates' e.g. enables the use of the authorised QoS resources.
6 The GGSN sends COPS RPT message(s) back to the PDF.
7 The PDF sends a Diameter AAA to the AF. This may trigger further actions in the AF.

~~1. P-CSCF receives the 200 OK message complying with the conditions specified in the paragraphs above.~~
~~2. PDF approves the QoS Commit.~~
~~3. PDF sends COPS DEC message(s) to the GGSN to open the 'gates' e.g. enable the use of the authorised QoS resources.~~

~~4. GGSN receives the COPS DEC message(s) and opens the 'gates' e.g. enables the use of the authorised QoS resources.~~
~~5. GGSN sends COPS RPT message(s) back to the PDF.~~
~~6. P-CSCF forwards the 200 OK message.~~

Figure 6.1.1: Approval of QoS Commit ~~to both the Mobile Originating (MO) side and the Mobile Terminating (MT) side~~

6.2 Removal of QoS commit

The "Removal of QoS commit" procedure is used when the AF decides to disable IP flow(s) or media component(s), e.g. when a session is released and the related IP flows are removed from a PDP context that multiplexes IP flows from several sessions.

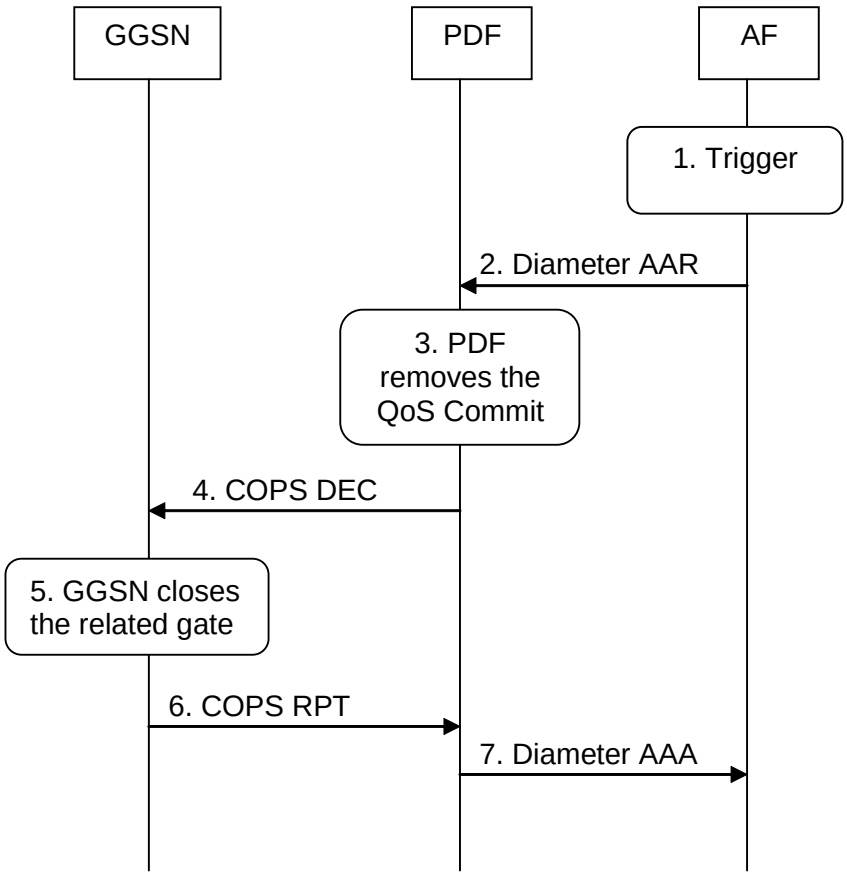
~~The "Removal of QoS commit" procedure is used e.g. when a session is released and the related IP flows are removed from a PDP context that multiplexes IP flows from several sessions, or when media IP flow(s) of a session is put on hold. (e.g. in case of a media re-negotiation or call hold). The PDF decision of "Removal of QoS commit" shall be sent as a separate decision to the GGSN corresponding to the previous "Authorize QoS Resources" request.~~

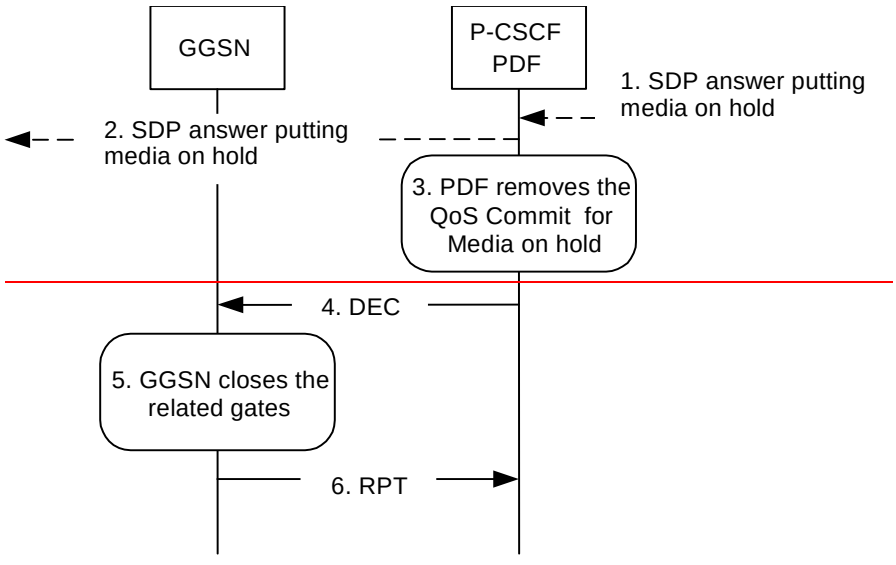
~~6.2.1 Removal of QoS commit at Media on Hold~~

~~Media is placed on hold as specified in RFC 3264 [11].~~

~~If a bidirectional media component is placed on hold by making it unidirectional, the QoS Commit shall only be removed in the deactivated direction.~~

~~Figure 6.2.1 presents the "Removal of QoS commit" procedure at media on hold to both the Mobile Originating (MO) side and the Mobile Terminating (MT) side.~~





1. The AF receives an internal or external trigger to disable the flow.
2. The AF sends a Diameter AAR to the PDF, requesting that gates shall be closed.
3. The PDF removes the QoS Commit.
4. The PDF sends the COPS DEC message(s) to the GGSN to close the relevant media IP flow gate(s), leaving the possible related RTCP gate(s) open to keep the connection alive.
5. The GGSN receives the COPS DEC message(s) and closes the requested gate(s).
6. The GGSN sends the COPS RPT message(s) back to the PDF.
7. The PDF sends a Diameter AAA back to the AF.
~~1. P-CSCF receives an SDP answer putting media on hold within a SIP message. (NOTE 1)~~

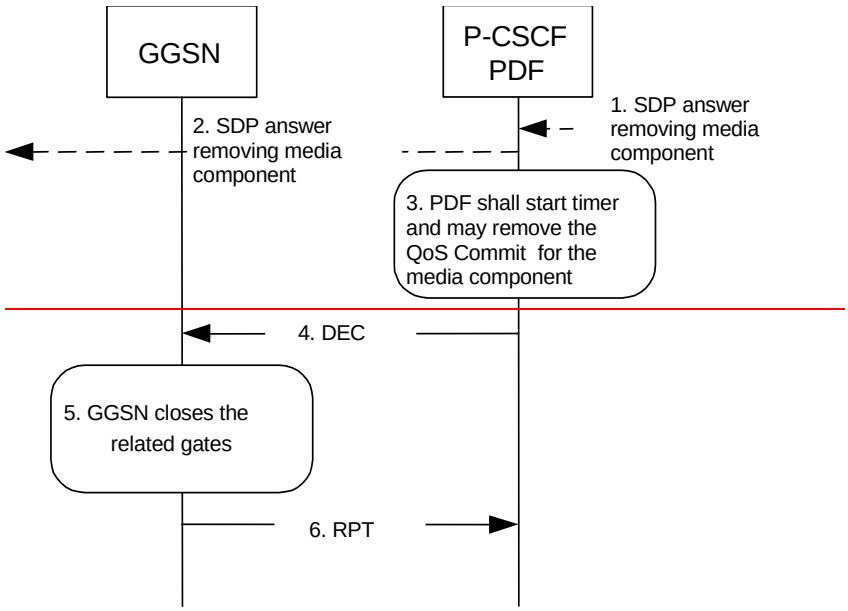
2. P-CSCF forwards an SDP answer putting media on hold within a SIP message.
3. PDF removes the QoS commit for the media on hold.
4. PDF sends COPS DEC message(s) to the GGSN to close the relevant media IP flow gate(s),leaving the possible related RTCP gate(s) open to keep the connection alive.
5. GGSN receives the COPS DEC message(s) and closes the requested gate(s).
6. GGSN sends COPS RPT message(s) back to the PDF.

NOTE 1: This procedure occurs whenever a bidirectional media is made unidirectional.

Figure 6.2.1: Removal of QoS commit at Media on Hold to both the Mobile Originating (MO) side and the Mobile Terminating (MT) side

6.2.2 Removal of QoS commit at media component removal

Figure 6.2.2 presents the "Removal of QoS commit" procedure at media component removal for both the Mobile Originating (MO) side and the Mobile Terminating (MT) side. The removal of QoS commit is optional. In addition, the procedure in Clause 6.3.1 applies in this situation after timer expiry.



1. P-CSCF receives an SDP answer removing media component.
2. P-CSCF forwards the SDP answer removing media component.
3. PDF shall start timer and may remove the QoS commit for the related IP flow(s) of the media component. After timer expiry, Figure 6.3.1 applies starting with step 4.
4. PDF sends a COPS DEC message to the GGSN to close the related 'gate(s)'.
5. GGSN receives the COPS DEC message and closes the 'gate(s)'.
6. GGSN sends a COPS RPT message back to the PDF.

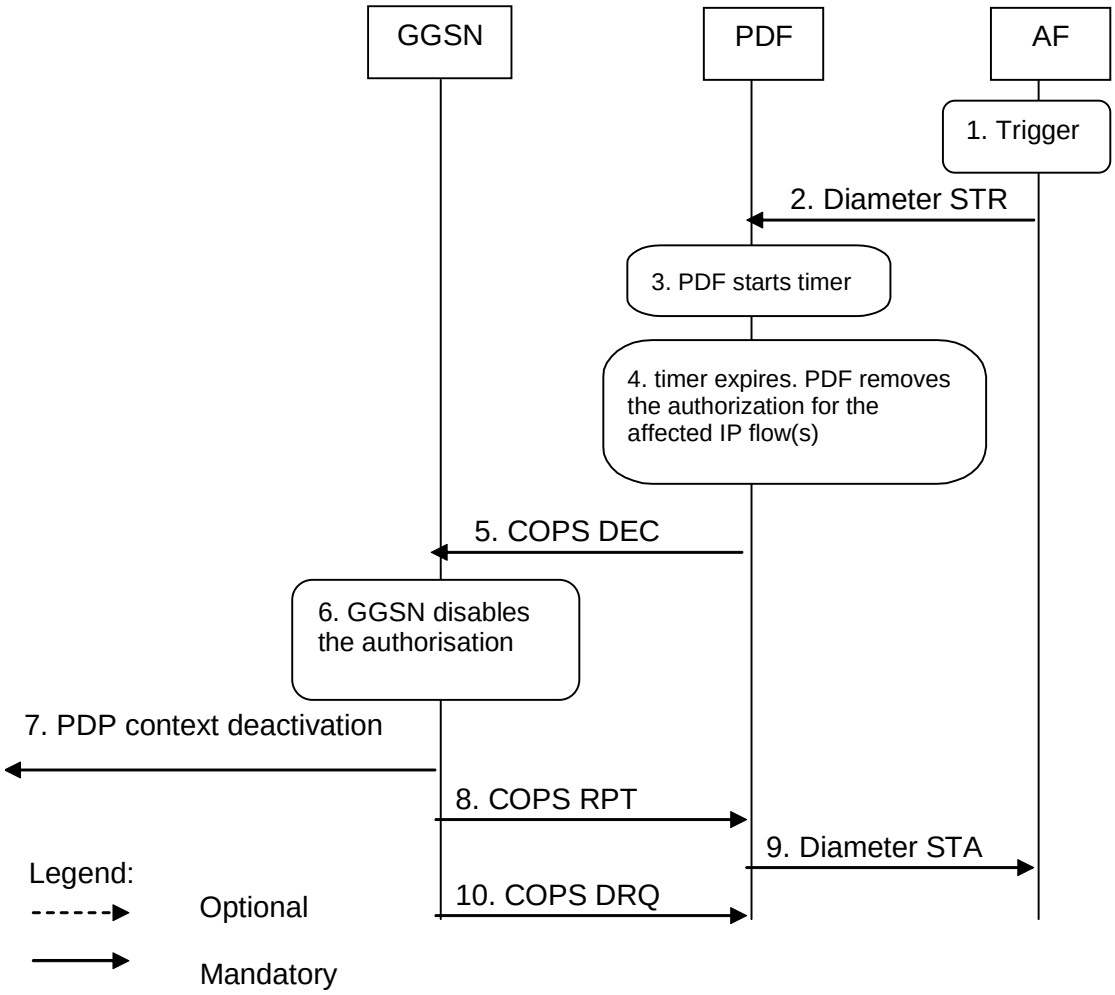
Figure 6.2.2: Removal of QoS commit at media component removal for both the Mobile Originating (MO) side and the Mobile Terminating (MT) side

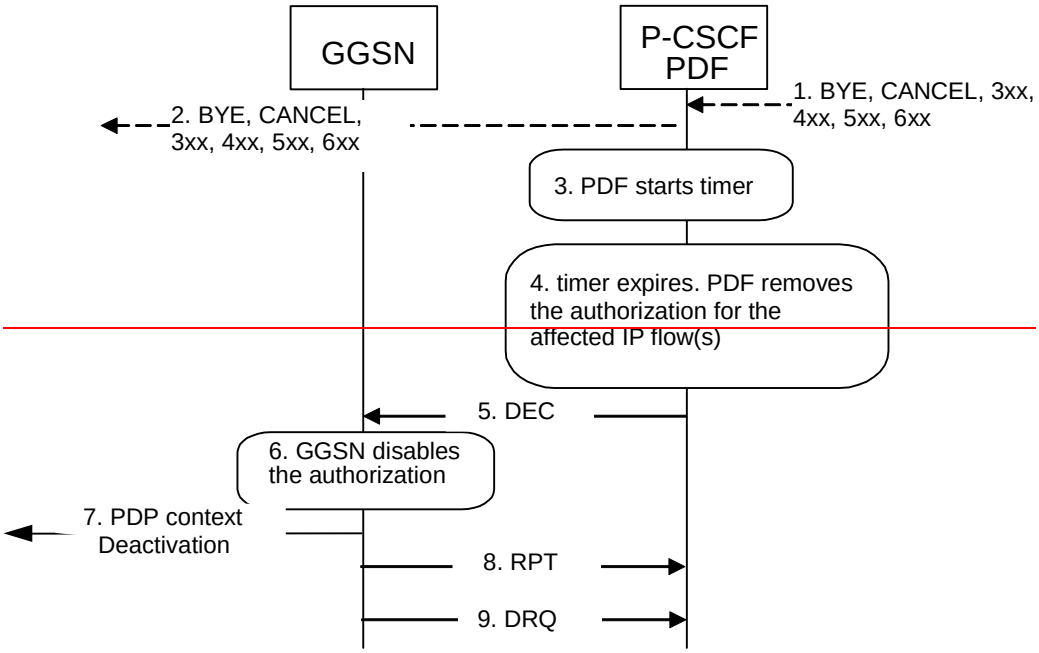
6.3 Revoke authorization for GPRS and IP resources

The "Revoke Authorization for GPRS and IP resources" procedure is used e.g. upon session release or upon session redirection of the only or last session of a given client handle (PDP context) or upon SIP final error response initiated after bearer establishment. The PDF decision of "Revoke Authorization for UMTS and IP Resources" shall be sent as a separate decision to the GGSN corresponding to the previous "Authorize QoS Resources" request.

6.3.1 ~~Mobile initiated session release / Network~~AF initiated session release

Figure 6.3.1 presents the "Revoke Authorization for UMTS and IP Resources" at ~~Mobile initiated session release or~~ Network initiated session release (of the only or last session of a given client handle) 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. In addition, the revoke authorization for GPRS and IP resources applies after timer expiry at the removal of media component(s) from an IMS session which has not been released.~~





1. The AF receives an internal or external trigger for a session release.
2. The AF sends session termination request to the PDF to initiate revocation of the authorisation
3. PDF starts timer.
4. The timer expires but the PDF has not been notified that the affected PDP context(s) have been modified or deactivated. The PDF removes the authorisation for the affected IP flow(s) of this session, which it authorized previously.
5. If step 4 occurs, the PDF sends COPS DEC message(s) to the GGSN including client handle(s), which identifies the PDP context(s) to be deactivated.

6. The GGSN receives the COPS DEC message, and disables the use of the authorized QoS resources.
7. The GGSN initiates deactivation of the PDP context(s) used for the IP multimedia session, in case the UE has not done it before.
8. GGSN sends RPT message back to the PDF.
9. The PDF sends session termination answer to the AF.
10. The GGSN sends COPS DRQ message(s) to the PDF.

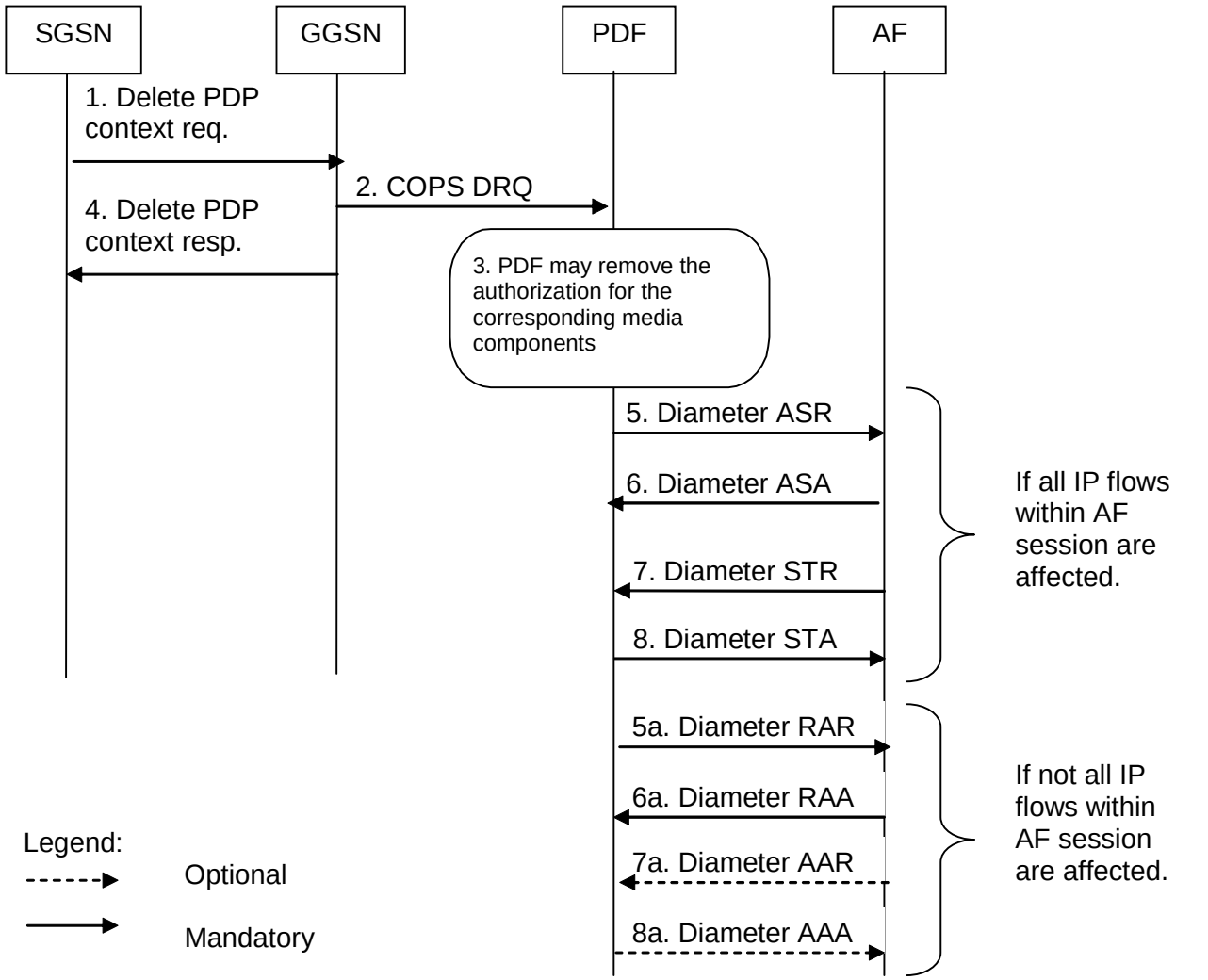
~~1. A SIP BYE message, a SIP CANCEL request, a SIP 3xx redirect response, or any 4xx, 5xx, or 6xx SIP final error response is received by the P-CSCF.~~
~~2. P-CSCF forwards the BYE message, or the SIP 3xx redirect response, a SIP CANCEL request, or any 4xx, 5xx, or 6xx SIP final error response.~~
~~3. PDF starts timer.~~
~~4. The timer expires but the PDF has not been notified that the affected PDP context(s) have been modified or deactivated. PDF removes the authorisation for the affected IP flow(s) of this session, which it authorized previously.~~
~~5. If step 4 occurs, PDF sends COPS DEC message(s) to the GGSN including client handle(s), which identifies the PDP context(s) to be deactivated.~~
~~6. GGSN receives the COPS DEC message, and disables the use of the authorized QoS resources.~~
~~7. GGSN initiates deactivation of the PDP context(s) used for the IP multimedia session, in case the UE has not done it before.~~
~~8. GGSN sends COPS RPT message(s) back to the PDF.~~
~~9. GGSN sends COPS DRQ message(s) to the PDF.~~

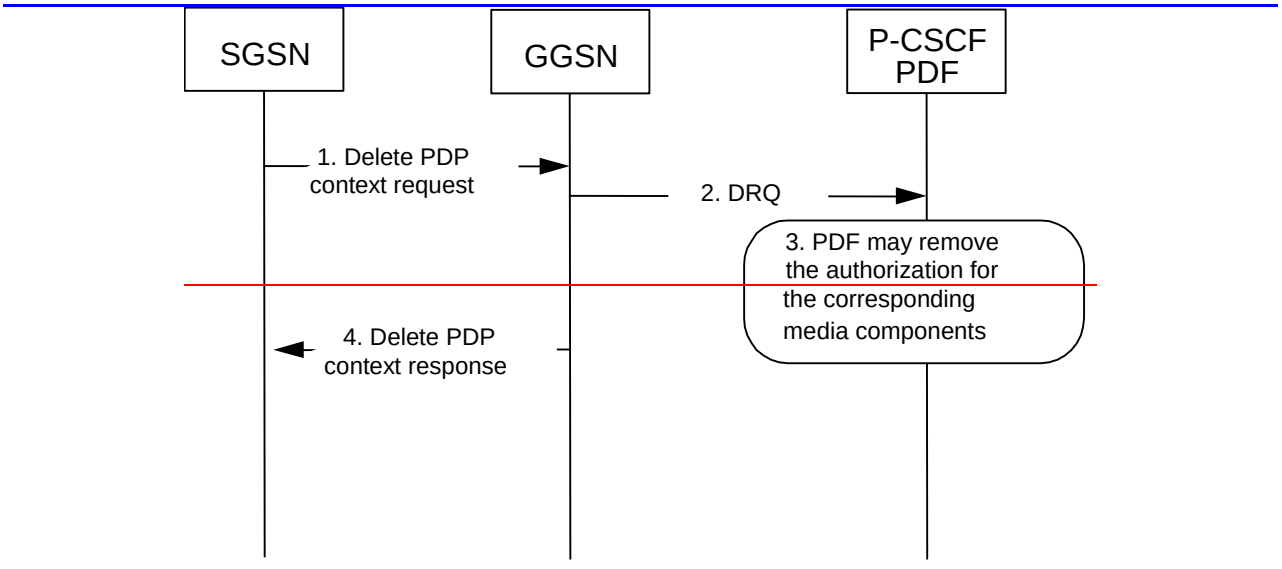
Figure 6.3.1: Revoke authorization for GPRS and IP resources -
at Mobile initiated session release or Network initiated session release
~~for both Mobile Originating (MO) and Mobile termination side~~

6.4 Indication of PDP Context Release

The "Indication of PDP Context Release" procedure is used upon the release of a PDP Context that was established based on authorisation from the PDF.

~~Figure 6.4.1 presents the "Indication of PDP Context Release" to both the Mobile Originating (MO) side and the Mobile Terminating (MT) side.~~





1. The SGSN deactivates the PDP context carrying IP flow(s) of media component(s) by sending the Delete PDP Context Request message to the GGSN.
2. The GGSN sends a COPS DRQ message to the ~~P-CSCF(~~PDF~~)~~.
3. The ~~P-CSCF(~~PDF~~)~~ receives the COPS DRQ message and the PDF may remove the authorization for the media component(s) with the client handle corresponding to that PDP context.
4. The GGSN sends the Delete PDP Context Response message to the SGSN to acknowledge the PDP context deletion.

The following steps shall be performed separately for each AF session that is affected by the PDP context release:

If all IP flow(s) within the AF session are affected by the PDP context release:

5. The PDF indicates the session abort to the AF by sending an abort session request to the AF if the PDP context was the last one for the session.
6. The AF responds by sending an abort session answer to the PDF.
7. The AF sends session termination request to the PDF to indicate that the session has been terminated.
8. The PDF responds by sending a session termination answer to the AF.

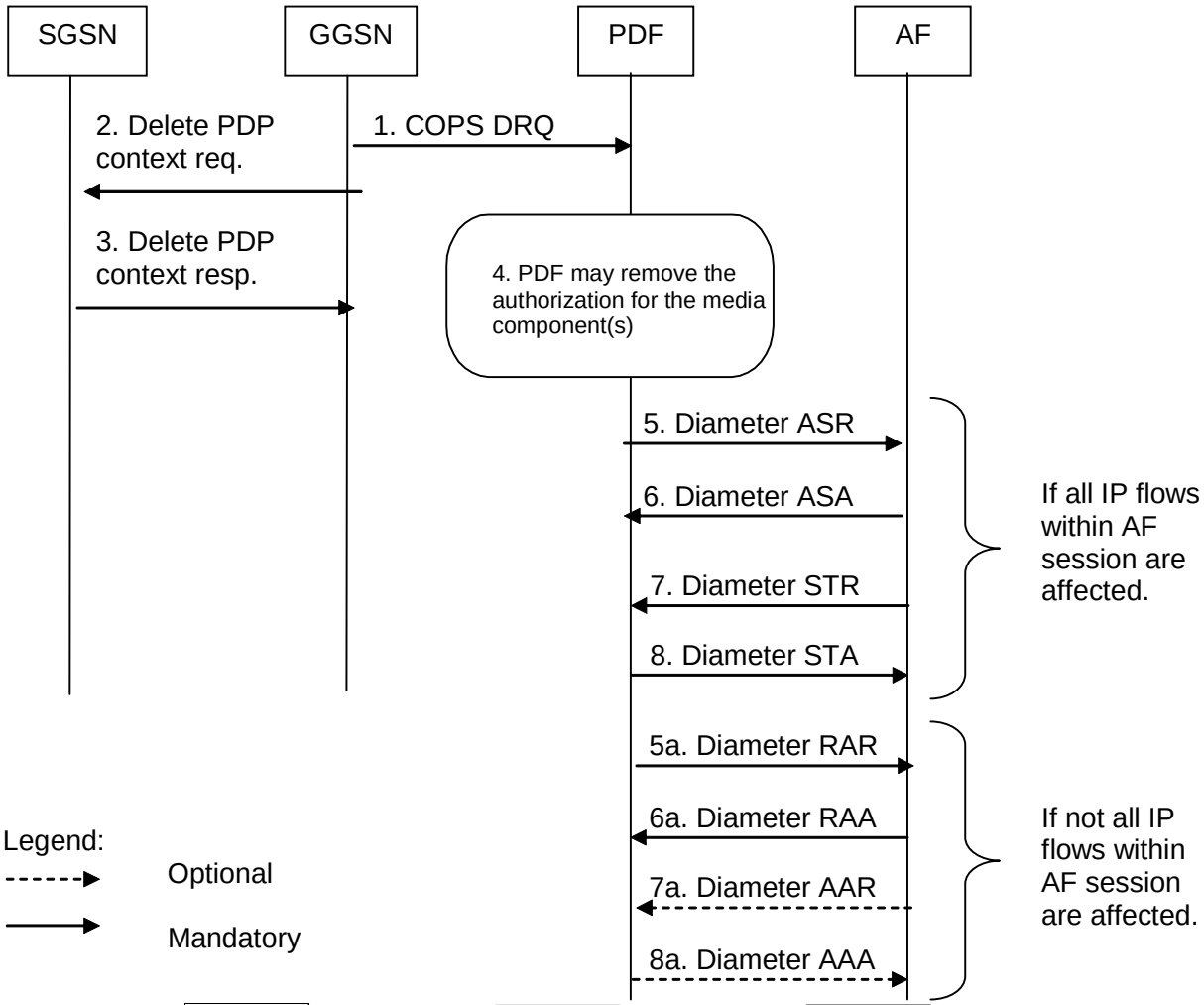
If not all IP flow(s) within the AF session are affected by the PDP context release:

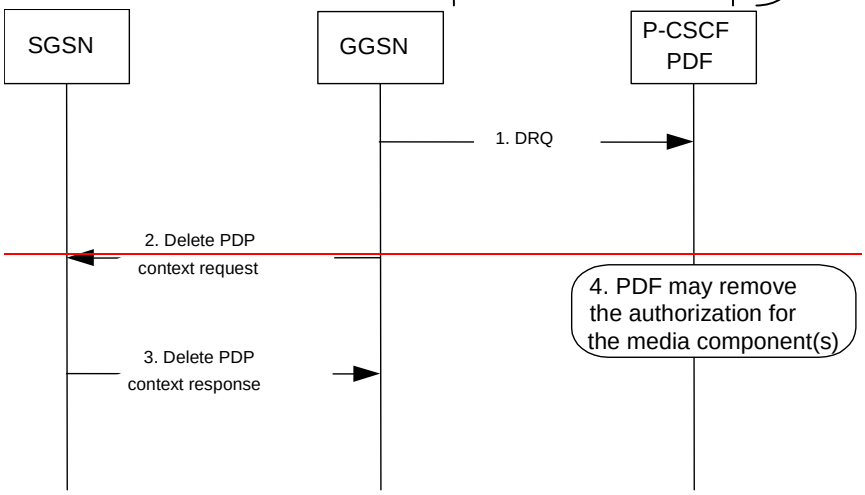
5a. The PDF indicates the PDP context release to the AF by sending an RAR.
6a. The AF responds by sending an RAA to the PDF.
7a. The AF may send an AAR to the PDF to update the session information.
8a. If step 7a occurs, the PDF responds by sending a AAA to the AF.

~~NOTE: Step 4 may also occur at the same time or before Step 3.~~

Figure 6.4.1: Indication of PDP Context Release ~~to both the Mobile Originating (MO) side and the Mobile Terminating (MT) side~~

Figure 6.4.2 presents the case when the GGSN initiates the release of a PDP context, i.e. after an error condition has been detected in GGSN.





1. The GGSN sends a COPS DRQ message to the ~~P-CSCF(~~PDF~~)~~.
2. The GGSN deactivates the PDP context carrying IP flow(s) of media component(s) by sending the Delete PDP Context Request message to the SGSN.
3. The SGSN sends the Delete PDP Context Response message to the GGSN to acknowledge the PDP context deletion.
4. The ~~P-CSCF(~~PDF~~)~~ receives the COPS DRQ message and the PDF may remove the authorization for the media component(s) authorized for this client handle.

The following steps shall be performed separately for each AF session that is affected by the PDP context release:

If all IP flows within an AF session are affected by the PDP context release:

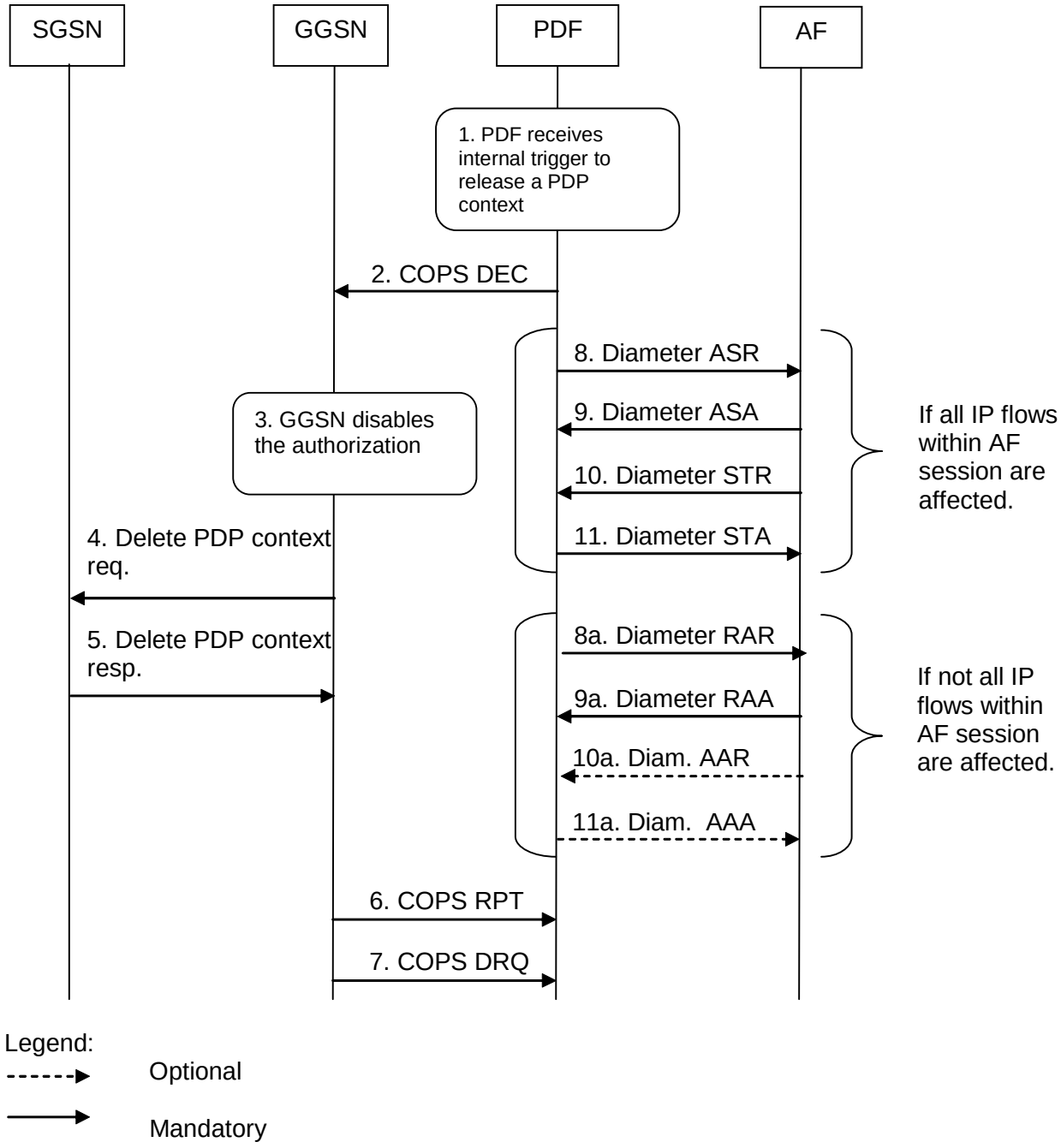
5. The PDF indicates the session abort to the AF by sending an abort session request to the AF if the PDP context was the last one for the session.

6. The AF responds by sending an abort session answer to the PDF.
7. The AF sends session termination request to the PDF to indicate that the session has been terminated.
8. The PDF responds by sending a session termination answer to the AF.

If not all IP flows within an AF session are affected by the PDP context release:
5a. The PDF indicates the PDP context release to the AF by sending an RAR:
6a. The AF responds by sending an RAA to the PDF.
7a. The AF may send an AAR to the PDF to update the session information.
8a. If step 7a occurs, the PDF responds by sending a AAA to the AF.
~~NOTE: Step 4 may also occur at the same time or before Step 2 and Step 3.~~

Figure 6.4.2: Indication of GGSN-initiated PDP Context Release ~~to both the Mobile Originating (MO) side and the Mobile Terminating (MT) side~~

Figure 6.4.3 presents the case when the PDF initiates the release of a PDP context. This may occur due to an internal error or overload condition within the PDF, or if the PDF decides to terminate AF sessions due to a shortage of bearer resources.



1. The PDF receives an internal trigger to disable a PDP context. The PDF removes the authorization for the IP flow(s) within this PDP context, which it authorized previously.
2. The PDF sends COPS DEC message to the GGSN including client handle, which identifies the PDP context to be deactivated.
3. The GGSN receives the COPS DEC message, and disables the use of the authorized QoS resources.
4. The GGSN initiates deactivation of the PDP context.
5. The GGSN receives delete PDP context response from SGSN.
6. The GGSN sends a COPS RPT message back to the PDF.
7. The GGSN sends COPS DRQ message to the PDF.

The following steps shall be performed separately for each AF session that is affected by the PDP context release:

If all IP flows within the AF session are affected by the PDP context release:

8. The PDF indicates the session abortion to the AF by sending an abort session request.
9. The AF responds by sending an abort session answer to the PDF.
10. The AF sends session termination request to the PDF to indicate that the session has been terminated
11. The PDF responds by sending a session termination answer to the AF.

If not all IP flows within the AF session are affected by the PDP context release:

8a. The PDF indicates the PDP context release to the AF by sending an RAR.
9a. The AF responds by sending an RAA to the PDF.
10a. The AF may send an AAR to the PDF to update the session information.
11a. If step 10a occurs, the PDF responds by sending a AAA to the AF.

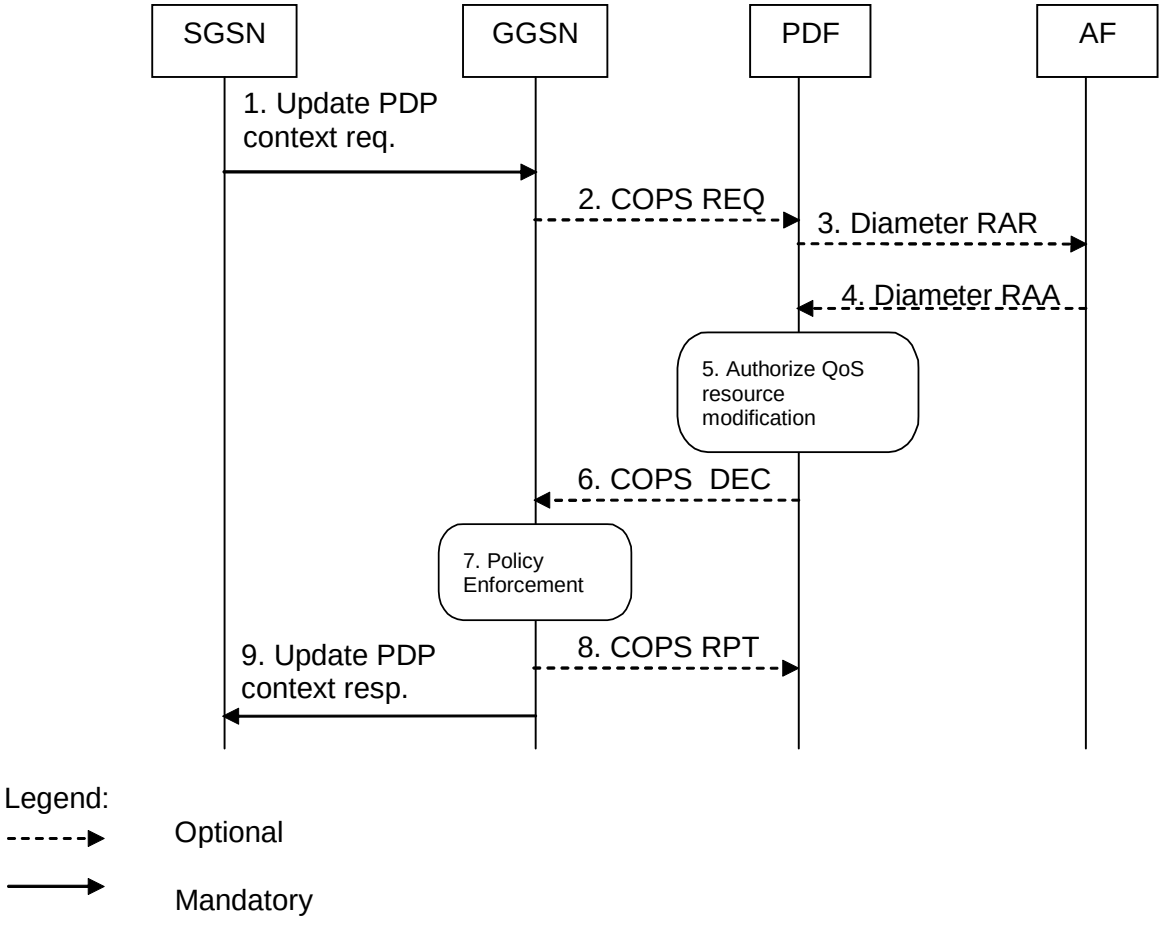
Figure 6.4.3: Indication of PDF-initiated PDP Context Release

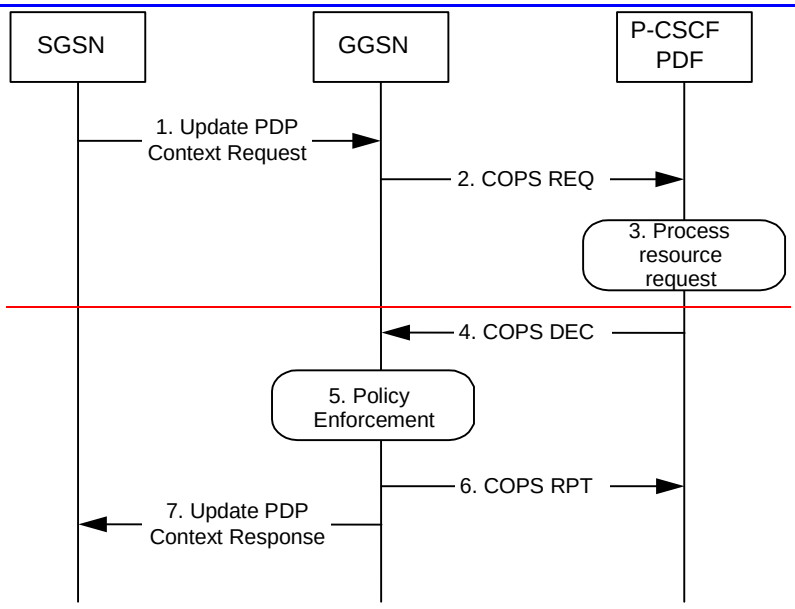
6.5 Modification of PDP Context

The "Modification of PDP Context" procedure is used when a PDP Context is modified such that the requested QoS falls outside of the limits that were authorized at PDP context activation (or last modification) or such that the maximum bit rate (downlink and uplink) is downgraded to 0 kbit/s. In these cases, the GGSN communicates with the PDF as described below.

6.5.1 Authorization of PDP Context Modification

Figure 6.5.1 presents the "Modification of PDP Context" ~~procedure to both the Mobile Originating (MO) side and the Mobile Terminating (MT) side~~ when the UMTS QoS which were authorized at PDP context activation (or last modification) has been changed by UE.





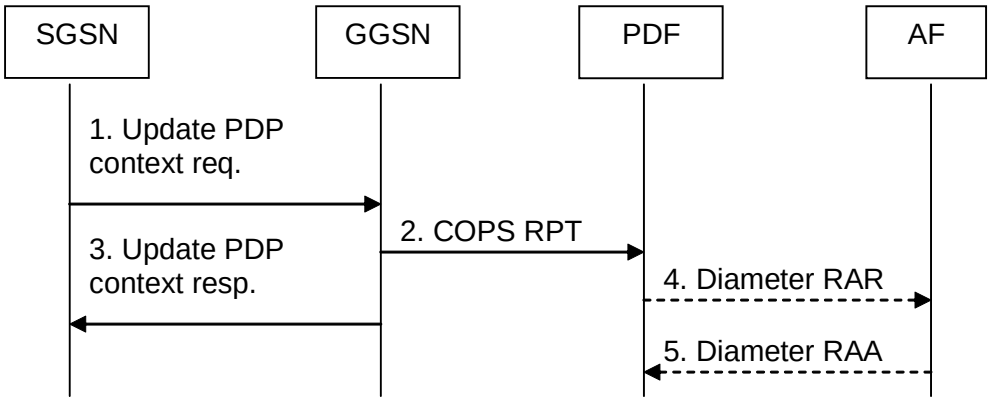
1. A request to modify the PDP context carrying the IP flows of media component(s), of which at least one may have been modified or removed, is indicated by sending the Update PDP Context Request message to the GGSN with the changed UMTS QoS parameters.
2. If the GGSN supports a Local Policy Decision Point(LPDP), it can consult the local policy decision stored in the LPDP before sending the COPS REQ message to the PDF. In case the requested QoS is within the already authorized QoS and the binding information is not changed, the GGSN does not need to send an authorization request to the PDF and proceeds to step ~~5~~7. Otherwise, the GGSN sends a COPS REQ message to the PDF.
3. If t~~T~~he PDF receives the COPS REQ message, it ~~and~~ performs an authorization decision according to the requested modification. If the AF has instructed earlier that the PDF needs to contact the AF in bearer modification, the PDF sends a re-authorization request to the AF.
4. If step 3 happens, the AF responds to the re-authorisation request.

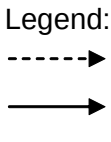
5. If the PDF has received a COPS REQ message in step 2, the PDF performs the authorization decision.
~~4~~6. If the PDF has received a COPS REQ message in step 2, t~~T~~he decision taken by the PDF is returned via the COPS DEC message. The DEC message includes the policy information to be used by the GGSN in order to perform the policy-based admission control.
~~5~~7. The GGSN enforces the policy decision based on the authorization information cached on the GGSN LPDP or received from the PDF for the IP flows of media component(s) carried by the PDP context.
~~6~~8. If step 6 has happened, ~~T~~the GGSN sends COPS RPT message back to the PDF and reports its success or failure in carrying out the PDF decision and notifies state changes if any.
~~7~~9. The Update PDP Context Response message is sent to the SGSN to acknowledge the PDP context modification.

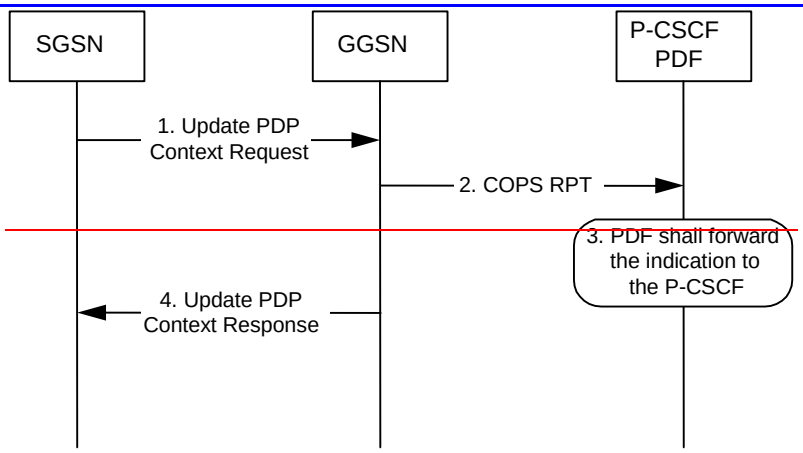
Figure 6.5.1: Authorization of PDP Context Modification ~~to both the Mobile Originating (MO) side and the Mobile Terminating (MT) side~~

6.5.2 Indication of PDP Context Modification

Figure 6.5.2 presents the "Indication of PDP Context Modification" procedure to both the Mobile Originating (MO) side and the Mobile Terminating (MT) side when the maximum bit rate (downlink and uplink) for the PDP context is modified to and from 0 kbit/s.







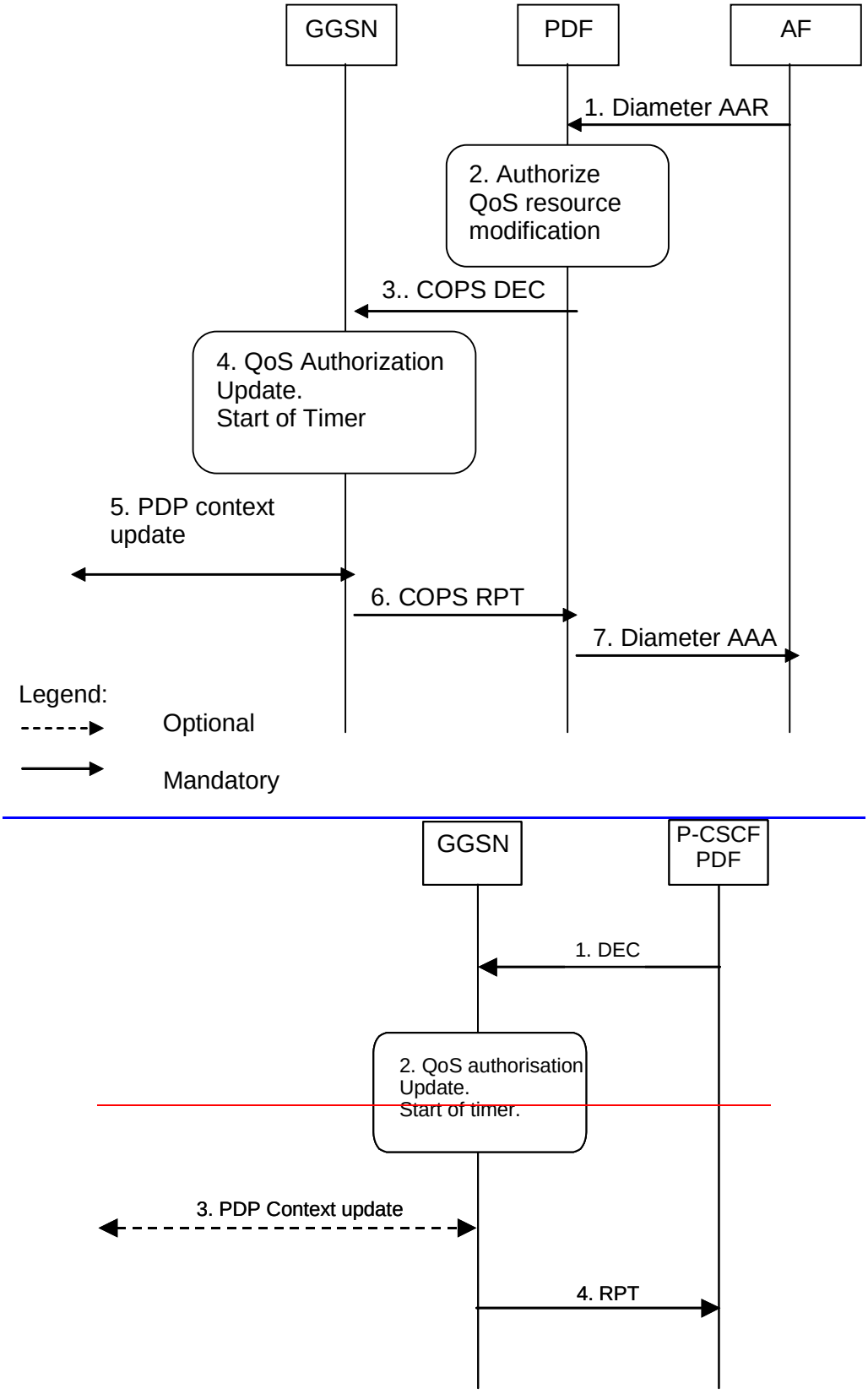
1. The SGSN modifies the PDP context carrying the IP flows of media component(s) by sending the Update PDP Context Request message to the GGSN.
2. The GGSN sends a COPS RPT message to the PDF notifying the PDP context modification.
~~3. PDF receives the COPS RPT message and forwards the indication to the P-CSCF.~~
~~At this point the authorization may be kept or removed depending on operators policies.~~
~~4~~3. The GGSN sends the Update PDP Context Response message to the SGSN to acknowledge the PDP context modification.
4. If the AF has instructed the PDF earlier that the PDF needs to contact the AF when the bandwidth of the PDP context is modified to 0 kbit/s, the PDF sends a re-authorization request to the AF.
5. If step 4 happens, the AF sends a re-authorisation answer back to the PDF. If the PDP context is modified to 0 kbit/s, the authorization may be kept or removed depending on operator's policies.

~~NOTE: Step 4 may also occur at the same time or before Step 3.~~

Figure 6.5.2: Indication of PDP Context Modification ~~to both the Mobile Originating (MO) side and the Mobile Terminating (MT) side~~

6.6 Session modification initiated SBLP authorization decision

The GGSN receives an unsolicited authorization decision from the PDF, when a session is modified without adding or removing media components or IP flows ~~lines~~ (refer to 3GPP TS 29.207 [7]) , i.e. when the binding information of the AF session remains unchanged.. The authorization update operation through the Go interface, described in figure 6.6.1, is identical in the originating and terminating cases. If the existing QoS of the PDP context exceeds the updated authorised QoS and the UE does not modify the PDP context accordingly, the GGSN shall perform a network initiated PDP context modification to reduce the QoS to the authorised level ~~(as shown with the dash arrows in the figure)~~.



1. The AF sends a Diameter AAR to the PDF to indicate the change in the session information
2. The PDF analyses the session information and updates the authorization accordingly.
~~1~~3. The PDF sends a COPS DEC message to the GGSN to indicate the change of the authorised QoS resources (e.g. bandwidth or port numbers).
~~2.~~4. The GGSN updates the QoS authorization information of the session and starts a timer to supervise the PDP context update.

~~3.~~5. If the existing QoS of the PDP context exceeds the updated authorised QoS and the UE does not modify the PDP context accordingly, the GGSN sends an Update PDP Context Request message to the SGSN after the expiry of the timer.
~~4.~~6. The GGSN sends a COPS RPT message back to the PDF.
7. The PDF sends an AAA to the AF.

Figure 6.6.1: Authorization update upon session modification ~~without adding or removing media lines~~

7 QoS parameter mapping

7.0 Overview of QoS parameter mapping

The AF derives information about the service from the SDI or from other sources. The AF passes service information to the PDF. The PDF 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 GGSN via the Go interface. The GGSN will map from the Authorized IP QoS parameters to the Authorized UMTS QoS parameters.

The UE derives the Authorized UMTS QoS parameters in an application specific manner. It should use information from the AF session signalling and SDI for that purpose. If SDP is used as SDI, the UE should apply the mapping rules within this specification. The UE shall use the received authorization token as criterion to decide if SBLP is applied. If the UE contains an IP BS manager, IP QoS parameters are also generated.

Upon receiving the PDP context activation or modification, the GGSN shall compare the UMTS QoS parameters against the Authorized UMTS QoS parameters. If the request lies within the limits authorized by the PDF, the PDP context activation or modification shall be accepted.

Figure 7.0 indicates the network entities where QoS mapping functionality is performed. This mapping is performed by:

1. If SBLP is applied then the AF may map from SDI within the AF session signalling to service information passed to the PDF over the Gq interface. The mapping is application specific. If SDP is used as SDI, the AF should apply the mapping described in Clause 7.1.0. For IMS, the mapping rules in Clause 7.1.0 shall be used at the P-CSCF.

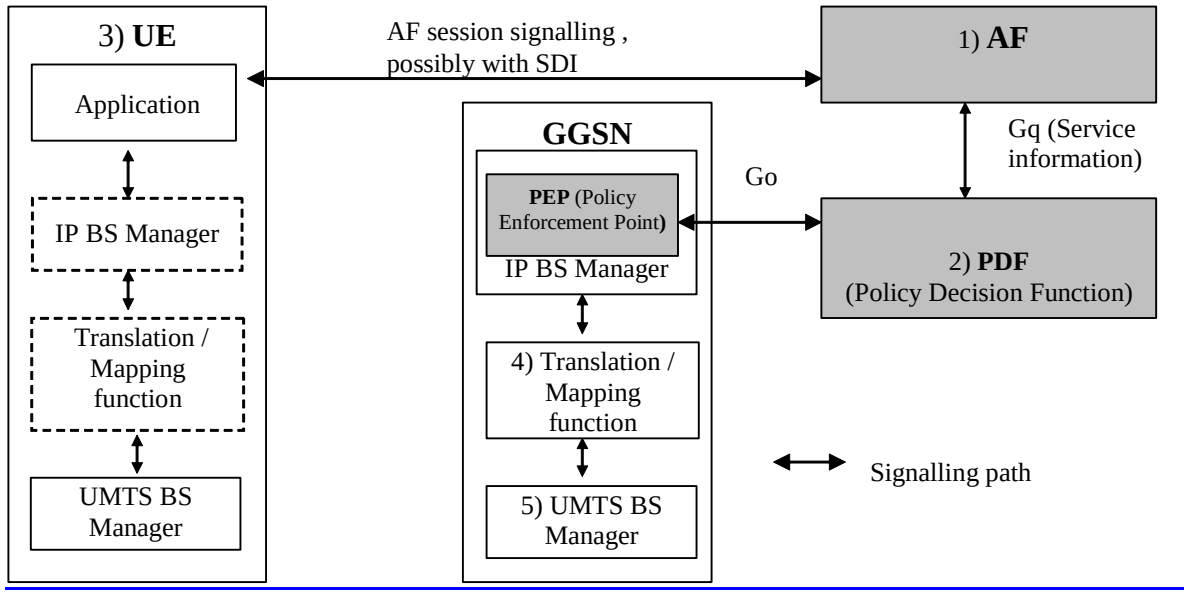
2. The PDF shall map from the service information received over the Gq interface to the Authorized IP QoS parameters that shall be passed to the GGSN via the Go interface. The mapping is performed for each flow identifier. Upon a request from the GGSN, the PDF combines per direction the individual Authorized IP QoS parameters per flow identifier that are identified by the binding information (see clause 7.1.1).

3. The UE derives UMTS QoS parameters and, if an IP BS manager is present, IP QoS parameters from the AF session signalling in an application specific manner for each flow identifier. The IP and UMTS QoS parameters should be generated according to application demands and recommendations for conversational (3GPP TS 26.236 [6]) or streaming applications (3GPP TS 26.234 [5]). IF SDP is used as SDI, e.g. for IMS, the UE should apply Clause 7.2.1. If SBLP is applied, i.e. the UE has received an authorization token, and SDP is used as SDI, the UE should also apply mapping rules for the authorised QoS parameters in Clause 7.2.2 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 GGSN shall map from the Authorized IP QoS parameters received from PDF to the Authorized UMTS QoS parameters (see clause 7.1.2).

5. The GGSN shall compare the UMTS QoS parameters of the PDP context against the Authorized UMTS QoS parameters (see clause 7.1.3).

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



NOTE 1: The AF may derive the Service information from the AF session signalling.
NOTE 2: Service Information on Gq interface to Authorized IP QoS parameters mapping.
NOTE 3: The UE may derive IP QoS parameters, requested UMTS QoS parameters mapping and Authorized UMTS QoS parameters from the AF session signalling.
NOTE 4: Authorized IP QoS parameters to Authorized UMTS QoS parameters mapping.
NOTE 5: UMTS QoS parameters with Authorized UMTS QoS parameters comparison.

Figure 7.0: Framework for QoS mapping between AF and GPRS

7.0.1 QoS parameter mapping for IMS

Within the IMS, session establishment and modification involves an end-to-end message-exchange using SIP/SDP with negotiation of media attributes (e.g. Codecs) as defined in 3GPP TS 24.229 [3] and 3GPP TS 24.228 [2]. If the IMS applies Service Based Local Policy (SBLP), as specified in 3GPP TS 29.207 [7], then the P-CSCF shall provide service information derived from the relevant SDP information to the PDF via the Gq interface. The P-CSCF shall apply the mapping rules in Clause 7.1.0 to derive service information from SDP. The SIP/SDP message will also have been passed on to the UE, where the UE will perform its own mapping from the SDP parameters and application demands to some UMTS QoS Parameters in order to populate the requested QoS field within the PDP context activation or modification. If SBLP is applied, i.e. the UE has received an authorization token, then the UE should also derive the Authorized UMTS QoS parameters from the SDP parameters. If the UE contains an IP BS manager IP QoS parameters are also generated.

7.1 QoS parameter mapping between ~~IMS~~ AF and GPRS

~~Within the IMS, session establishment and modification involves an end-to-end message-exchange using SIP/SDP with negotiation of media attributes (e.g. Codecs) as defined in 3GPP TS 24.229 [3] and 3GPP TS 24.228 [2]. If the IMS applies Service Based Local Policy (SBLP), as specified in 3GPP TS 29.207 [7], then the P-CSCF shall forward the relevant SDP information to the PDF together with an indication of the originator. The PDF notes and authorises the IP flows of the chosen media components by mapping from SDP parameters to Authorized IP QoS parameters for transfer to the GGSN via the Go interface. The GGSN will map from the Authorized IP QoS parameters to the Authorized UMTS QoS parameters. The SIP/SDP message will also have been passed on to the UE, where the UE will perform its own mapping from the SDP parameters and application demands to some UMTS QoS Parameters in order to populate the requested QoS field within the PDP context activation or modification. If SBLP is applied, i.e. the UE has received an authorization token, then the UE should also derive the Authorized UMTS QoS parameters from the SDP parameters. If the UE contains an IP BS manager IP QoS parameters are also generated. Upon receiving the PDP context activation or modification, the GGSN shall compare the UMTS QoS parameters against the Authorized UMTS QoS parameters. If the request lies within the limits authorised by the PDF, the PDP context activation or modification shall be accepted.~~

~~Figure 7.1 indicates the network entities where QoS mapping functionality is required. This mapping is performed by:~~

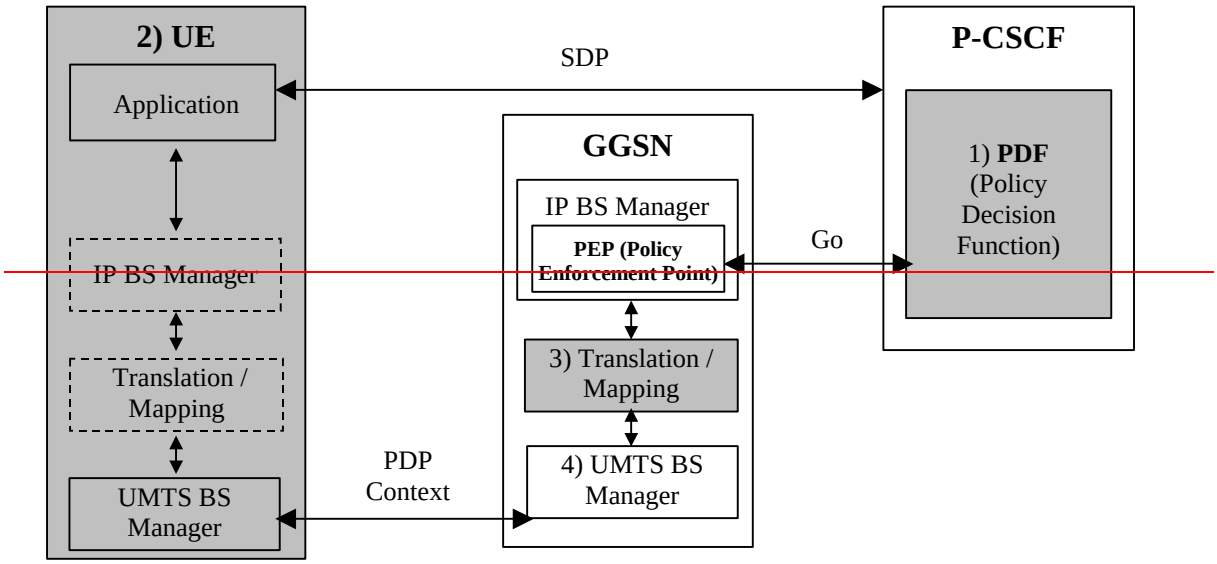
1. If SBLP is applied then the PDF maps from the SDP parameters determined from the SIP signalling to the Authorized IP QoS parameters that shall be passed to the GGSN via the Go interface. The mapping is performed for each flow identifier. Upon a request from the GGSN, the PDF combines per direction the individual Authorised IP QoS parameters per flow identifier that are identified by the binding information (see clause 7.1.1).

2. The UE maps from the SDP parameters to IP QoS parameters (if an IP BS manager is present) and to UMTS QoS parameters. This mapping is performed for each flow identifier. The IP and UMTS QoS parameters should be generated according to application demands and recommendations for conversational (3GPP TS 26.236 [6]) or streaming applications (3GPP TS 26.234 [5]) (see clause 7.2.1). If SBLP is applied, i.e. the UE has received an authorization token, then the mapping rules for the authorised QoS parameters should be taken into consideration because they define the maximum values for the different requested bit rates and traffic classes (see clause 7.2.2). 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.

3 The GGSN maps from the Authorized IP QoS parameters received from PDF to the Authorized UMTS QoS parameters (see clause 7.1.2).

4 The GGSN compares then the UMTS QoS parameters of the PDP context against the Authorized UMTS QoS parameters (see clause 7.1.3).

The mapping that takes place in the UE and the network shall be compatible in order to ensure that the GGSN will be able to correctly authorise the session.



NOTE 1: If SBLP is applied then SDP parameters to Authorized IP QoS parameters mapping.
NOTE 2: SDP parameters to (IP QoS parameters and) requested UMTS QoS parameters mapping and, if SBLP is applied, also SDP parameters to Authorized UMTS QoS parameters mapping.
NOTE 3: Authorized IP QoS parameters to Authorized UMTS QoS parameters mapping.
NOTE 4: UMTS QoS parameters with Authorized UMTS QoS parameters comparison.

Figure 7.1: Framework for QoS mapping between IMS and GPRS

7.1.0 SDP parameters to service information mapping in 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 7.1.0.1 for each SDP media component to derive a Media-Component-Description AVP from the SDP Parameters. Furthermore, the P-CSCF shall

map information about the grouping of media lines into resource reservation flows into the Flow-Grouping AVP as specified in table 7.1.0.3.

Table 7.1.0.1: Rules for derivation of service information within Media-Component-Description AVP from SDP media component

service information per Media-Component-Description AVP (NOTE 1)	Derivation from SDP Parameters (see NOTE 2)
Media-Component-Number	ordinal number of the position of the "m=" line in the SDP
AF-Application-Identifier	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 shall not demand application specific bandwidth or QoS class handling.
Media-Type	The Media Type AVP shall be included with the same value as supplied for the media type in the "m=" line.

Flow-Status	IF port in m-line = 0 THEN
	Flow-Status:= REMOVED;
	ELSE
	IF a=recvonly THEN
	IF <SDP direction> = mobile originated THEN
	Flow-Status := ENABLED_DOWNLINK;
	ELSE /* mobile terminated */
	Flow-Status := ENABLED_UPLINK;
	ENDIF;
	ELSE
	IF a=sendonly THEN
	IF <SDP direction> = mobile originated THEN
	Flow-Status := ENABLED_UPLINK;
	ELSE /* mobile terminated */
	Flow-Status := ENABLED_DOWNLINK;
	ENDIF;
	ELSE
	IF a=inactive THEN
	Flow-Status :=DISABLED;
	ELSE /* a=sendrecv or no direction attribute */
	Flow-Status := ENABLED
	ENDIF;
	ENDIF;
	ENDIF;
	ENDIF;

Max-Requested-Bandwidth	IF b=AS:<bandwidth> is present THEN
	Max-Requested-Bandwidth:= <bandwidth> * 1000; /* Unit is bit/s
	ELSE
	Max-Requested-Bandwidth:= <Operator specific setting>,
	or AVP not supplied;
	ENDIF;

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

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

Media-Sub-Component	Supply one AVP for each Flow Identifier within the media component. The Flow identifiers are derived according to Annex D of 3GPP TS 29.207 [7]. The encoding of the AVP is described in Table 7.1.0.2

NOTE 1: The encoding of the service information is defined in TS 29.209 [12].
NOTE 2: The SDP parameters are described in RFC 2327 [9].
NOTE 3: The 'b=RS:' and 'b=RR:' SDP bandwidth modifiers are defined in RFC 3556 [10].

Table 7.1.0.2: Rules for derivation of Media-Sub-Component AVP from SDP media component

Gq service information per Media-Sub-Component AVP (NOTE 1)	Derivation from SDP Parameters (see NOTE 2)
Flow-Number	derived according to Annex C of 3GPP TS 29.207 [7]
Flow-Status	AVP not supplied
Max-Requested-Bandwidth-UL	AVP not supplied
Max-Requested-Bandwidth-DL	AVP not supplied
Flow-Description	For uplink and dowlink direction, a Flow-Description AVP shall be provided unless no IP Flows in this direction are described within the media component. The uplink destination address shall be copied from the "c=" line of downlink SDP. The uplink destination port shall be derived from the "m=" line of downlink SDP. The downlink destination address shall be copied from the "c=" line of uplink SDP. The downlink destination port shall be derived from the "m=" line of uplink SDP. Uplink and downlink source adresses should be set to "any" and source ports should not be supplied. Proto shall be derived from the transport of the "m=" line. For "RTP/AVP" proto is 17(UDP).
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 [9] specifies how RTCP flows are described within SDP.

NOTE 1: The encoding of the service information is defined in TS 29.209 [12].
NOTE 2: The SDP parameters are described in RFC 2327 [9].

Table 7.1.0.3: Rules for mapping SDP information about the grouping of media lines into resource reservation flows into the Flow Grouping AVP

Flow-Grouping AVP (NOTE1)	Derivation from SDP Parameters (see NOTE 2)
Flow Grouping	For each SDP "a=group:SRF" SDP line, a Flow Grouping AVP shall be generated. (NOTE 3)
Flows	For each identification tag within "a=group:SRF" SDP line, a Flows AVP containing a Media-Component-Number AVP identifying the corresponding m-line shall be generated. (NOTE 3) No Flow-Number AVP shall be supplied within the Flows AVP.

NOTE 1: The encoding of the service information is defined in TS 29.209 [12].
NOTE 2: The SDP parameters are described in RFC 2327 [9].
NOTE 3: The SDP "group" attribute is defined in RFC 3388 [13]. The "SRF" semantics attribute within this grouping framework is defined in RFC 3524 [14].

7.1.1 Gq service information ~~SDP parameters~~ to Authorized IP QoS parameters mapping in PDF

The QoS authorization is to be based on the parameters Maximum Authorized QoS Class and Maximum Authorized Data Rate UL/DL.

When a session is initiated or modified the PDF shall use the mapping rules in table 7.1.1.1 to derive the Authorized IP QoS parameters Maximum Authorized Data Rate DL/UL and the Maximum Authorized QoS Class from the service information~~SDP Parameters~~. 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 shall be set to the highest value requested for the IP flow(s) of that media component by any of the active forked responses. These values are derived by the rules in table 7.1.1.1

Table 7.1.1.1: Rules for derivation of the Maximum Authorized Data Rates and Maximum Authorized QoS Class per flow identifier in the PDF

Authorized IP QoS Parameter per flow identifier	Derivation from service information~~SDP Parameters~~ (see note 4)

Maximum Authorized Data Rate DL (Max_DR_DL) and UL (Max_DR_UL) per flow identifier ~~(see note 5)~~	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 not RTCP flow(s) according to Flow-Usage AVP THEN
	IF Max-Requested-Bandwidth is present THEN
	bw:= Max-Requested-Bandwidth ;
	ELSE
	bw:= as set by the operator;
	ENDIF
	IF Flow-Status = ENABLED_DOWNLINK THEN
	Max_DR_UL:= 0;
	Max_DR_DL:= bw;
	ELSE
	IF Flow-Status = ENABLED_UPLINK THEN
	Max_DR_UL:= bw;
	Max_DR_DL:= 0;
	IF Flow-Status = REMOVED THEN
	Max_DR_UL:= 0;
	Max_DR_DL:= 0;
	ELSE /* Flow-Status = ENABLED or DISABLED */
	Max_DR_UL:= bw;
	Max_DR_DL:= bw;
	ENDIF;
	ENDIF;
	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 is present THEN
	IF RS-Bandwidth is present and
	RR-Bandwidth is not present THEN
	Max_DR_UL:= MAX[0.05 * Max-Requested-Bandwidth,
	RS-Bandwidth];
	Max_DR_DL:= MAX[0.05 * Max-Requested-Bandwidth,
	RS-Bandwidth];
	ENDIF;
	IF RS-Bandwidth is not present and
	RR-Bandwidth is present THEN
	Max_DR_UL:= MAX[0.05 * Max-Requested-Bandwidth,
	RR-Bandwidth];
	Max_DR_DL:= MAX[0.05 * Max-Requested-Bandwidth,
	RR-Bandwidth];
	ENDIF;
	IF RS-Bandwidth and RR-Bandwidth is not present THEN
	Max_DR_UL:= 0.05 * Max-Requested-Bandwidth ;
	Max_DR_DL:= 0.05 * Max-Requested-Bandwidth ;
	ENDIF;
	ELSE
	Max_DR_UL:= as set by the operator;
	Max_DR_DL:= as set by the operator;
	ENDIF;
	ENDIF;
	ENDIF;
	
	/* MAX-Requested-Bandwidth-UL and MAX-Requested-Bandwidth-DL take precedence*/
	IF Max-Requested-Bandwidth-UL is present THEN
	Max_DR_UL:= Max-Requested-Bandwidth-UL;
	ENDIF
	IF Max-Requested-Bandwidth-DL is present THEN
	Max_DR_DL:= Max-Requested-Bandwidth-DL;

```
    ENDIF

ENDIF;/* Direction of the IP flow(s) identified by the flow identifier */

IF a=recvonly THEN
      IF <SDP direction> = mobile originated THEN
            Direction:= downlink;
      ELSE /* mobile terminated */
            Direction:= uplink;
      ENDIF;
ELSE
      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_DR_UL and Max_DR_DL */

IF media IP flow(s) THEN
   IF bAS=AS:<bandwidth> is present THEN
      IF Direction=downlink THEN
         Max_DR_UL:= 0;
         Max_DR_DL:= bAS;
      ELSE
         IF Direction=uplink THEN
            Max_DR_UL:= bAS;
            Max_DR_DL:= 0;
         ELSE /*Direction=both*/
            Max_DR_UL:= bAS;
            Max_DR_DL:= bAS;
         ENDIF;
      ENDIF;
   ELSE
      bw:= as set by the operator;
      IF Direction=downlink THEN
         Max_DR_UL:= 0;
         Max_DR_DL:= bw;
      ELSE
         IF Direction=uplink THEN
            Max_DR_UL:= bw;
            Max_DR_DL:= 0;
         ELSE /*Direction=both*/
            Max_DR_UL:= bw;
            Max_DR_DL:= bw;
         ENDIF;
      ENDIF;
   ENDIF;
ELSE /* RTCP IP flow(s) */
   IF bRS=RS:<bandwidth> and bRR=RR:<bandwidth> is present THEN
      Max_DR_UL:= (bRS + bRR) / 1000;
      Max_DR_DL:= (bRS + bRR) / 1000;
   ELSE
      IF bAS=AS:<bandwidth> is present THEN
         IF bRS=RS:<bandwidth> is present and bRR=RR:<bandwidth> is not
present THEN
            Max_DR_UL:= MAX[0.05 * bAS, bRS / 1000];
            Max_DR_DL:= MAX[0.05 * bAS, bRS / 1000];
         ENDIF;
         IF bRS=RS:<bandwidth> is not present and bRR=RR:<bandwidth> is
present THEN
            Max_DR_UL:= MAX[0.05 * bAS, bRR / 1000];
            Max_DR_DL:= MAX[0.05 * bAS, bRR / 1000];
         ENDIF;
         IF bRS=RS:<bandwidth> and bRR=RR:<bandwidth> is not present THEN
            Max_DR_UL:= 0.05 * bAS;
            Max_DR_DL:= 0.05 * bAS;
         ENDIF;
      ELSE
         Max_DR_UL:= as set by the operator;
         Max_DR_DL:= as set by the operator;
      ENDIF;
   ENDIF;
```

	~~ENDIF;~~

Maximum Authorized QoS Class [MaxClass] per flow identifier (see notes 1, 2 and 3)	IF AF-Application-Identifier AVP demands application specific QoS Class handling THEN
	MaxClass:= as defined by application specific algorithm;
	ELSE
	IF Media-Type is present THEN
	IF (all media IP flows of media type "audio" or "video" for the session have the same direction) THEN
	MaxClassDerivation:=B; /*streaming*/
	ELSE
	MaxClassDerivation:=A; /*conversational*/
	ENDIF;
	
	CASE Media-Type OF
	"audio": MaxClass:= MaxClassDerivation
	"video": MaxClass:= MaxClassDerivation
	"application": MaxClass:=A; /*conversational*/
	"data": MaxClass:=E; /*interactive with priority 3*/
	"control": MaxClass:=C; /*interactive with priority 1*/
	/*new media type*/
	OTHERWISE: MaxClass:=F; /*background*/
	END;
	ELSE
	MaxClass:= as defined by by operator;
	ENDIF;
	ENDIF;~~IF (all media IP flows of media type "audio" or "video" for the session have the same direction) THEN
	MaxClassDerivation:=B; /*streaming*/
	ELSE
	MaxClassDerivation:=A; /*conversational*/
	ENDIF;~~
	
	~~CASE <media> OF
	"audio": MaxClass:= MaxClassDerivation
	"video": MaxClass:= MaxClassDerivation
	"application": MaxClass:=A; /*conversational*/
	"data": MaxClass:=E; /*interactive with priority 3*/
	"control": MaxClass:=C; /*interactive with priority 1*/
	/*new media type*/
	OTHERWISE: MaxClass:=F; /*background*/
	END;~~

NOTE 1: The Maximum Authorized QoS 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 maximum Authorized QoS class shall keep the originally assigned value.
NOTE 3: When audio or video IP flow(s) are added to a session, the PDF shall derive the maximum Authorized QoS Class taking into account the already existing media IP flow(s) within the session.
NOTE 4: The encoding of the service information is defined in TS 29.209 [12]~~The SDP parameters are described in RFC 2327 [9]~~.
~~NOTE 5: The "b=RS:" and "b=RR:" SDP bandwidth modifiers are defined in RFC 3556 [10].~~

The PDF shall per ongoing session store the Authorized IP QoS parameters per flow identifier.

When the GGSN requests the Authorized UMTS QoS parameters for an activated/modified PDP Context carrying IP flows of media component(s), the PDF shall use the rules in table 7.1.1.2 to calculate the Authorized IP QoS parameters per Client Handle.

Table 7.1.1.2: Rules for calculating the Maximum Authorized Data Rates and Maximum Authorized QoS Class per Client Handle in the PDF

Authorized IP QoS Parameter per Client Handle	Calculation Rule

Maximum Authorized Data Rate DL and UL per Client Handle	Maximum Authorized Data Rate DL/UL per Client Handle is the sum of all Maximum Authorized Data Rate DL/UL for all the flow identifiers associated with that Client Handle.
	
	IF Maximum Authorized Data Rate DL/UL per Client Handle > 16000 kbps THEN
	Maximum Authorized Data Rate DL/UL per Client Handle = 16000 kbps /* See 3GPP TS 23.107 [8] */
	
	END;

Maximum Authorized QoS Class per Client Handle	Maximum Authorized QoS Class per Client Handle = MAX [Maximum Authorized QoS Class per flow identifier among all the flow identifiers associated with that Client Handle. (The MAX function ranks the possible Maximum Authorized QoS Class values as follows: "A" > "B" > "C" > "D" > "E" > "F") /* See 3GPP TS 29.207 [7]) */

7.1.2 Authorized IP QoS parameters 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 PDF according to the rules in table 7.1.2.

Table 7.1.2: Rules for derivation of the Authorized UMTS QoS Parameters per PDP context from the Authorized IP QoS Parameters per Client Handle in GGSN

Authorized UMTS QoS Parameter per PDP context	Derivation from Authorized IP QoS Parameters
Maximum Authorized Bandwidth DL and UL per PDP context	Maximum Authorized Bandwidth DL/UL per PDP context = Maximum Authorized Data Rate DL/UL per CLient Handle
Maximum Authorized Traffic Class per PDP context	IF Maximum Authorized QoS Class = "A" THEN Maximum Authorized Traffic Class = "Conversational" ELSEIF Maximum Authorized QoS Class = "B" THEN Maximum Authorized Traffic Class = "Streaming" ELSEIF Maximum Authorized QoS Class = "C" THEN Maximum Authorized Traffic Class = "Interactive"; Maximum Authorized Traffic Handling Priority = "1"; ELSEIF Maximum Authorized QoS Class = "D" THEN Maximum Authorized Traffic Class = "Interactive"; Maximum Authorized Traffic Handling Priority = "2"; ELSEIF Maximum Authorized QoS Class = "E" THEN Maximum Authorized Traffic Class = "Interactive"; Maximum Authorized Traffic Handling Priority = "3"; ELSE Maximum Authorized Traffic Class = "Background" ENDIF ;

7.1.3 Comparing UMTS QoS Parameters against the Authorized UMTS QoS parameters in GGSN

Upon receiving a PDP context activation containing binding information, the GGSN requests the Authorized QoS information from the PDF, and may request the Authorized UMTS information if a PDP context containing binding

information is modified (see 3GPP TS 29.207 [7] for details). The GGSN compares the requested UMTS QoS parameters against the corresponding Authorized UMTS QoS parameters received via the translation/mapping function. If all the requested parameters lie within the limits, the PDP context activation or modification shall be accepted. I.e. the following criteria shall be fulfilled:

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

If any of the requested parameters do not lie within their respective limit, the GGSN shall downgrade the requested UMTS QoS parameters.

7.2 QoS parameter mapping in the UE

Figure 7.2 indicates the entities participating in the generation of the requested QoS parameters when activate or modify a PDP Context in the UE. 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 [6] for Conversational Codec Applications and 3GPP TS 26.234 [5] 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 7.2.1, to set the Maximum Bitrate UL/DL and the Guaranteed Bitrate UL/DL. Furthermore if the SDP Parameters are received in an IMS context in which SBLP is applied, i.e. an authorization token has been received, the Maximum Authorized Bandwidth UL/DL and Maximum Authorised Traffic Class should be derived according to the rules in clause 7.2.2.
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. If the PDP Context is activated or modified in an IMS context in which SBLP is applied, 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 7.2.2, the UE should check that the requested Traffic Class does not exceed the Maximum Authorised Traffic Class derived in step 3.

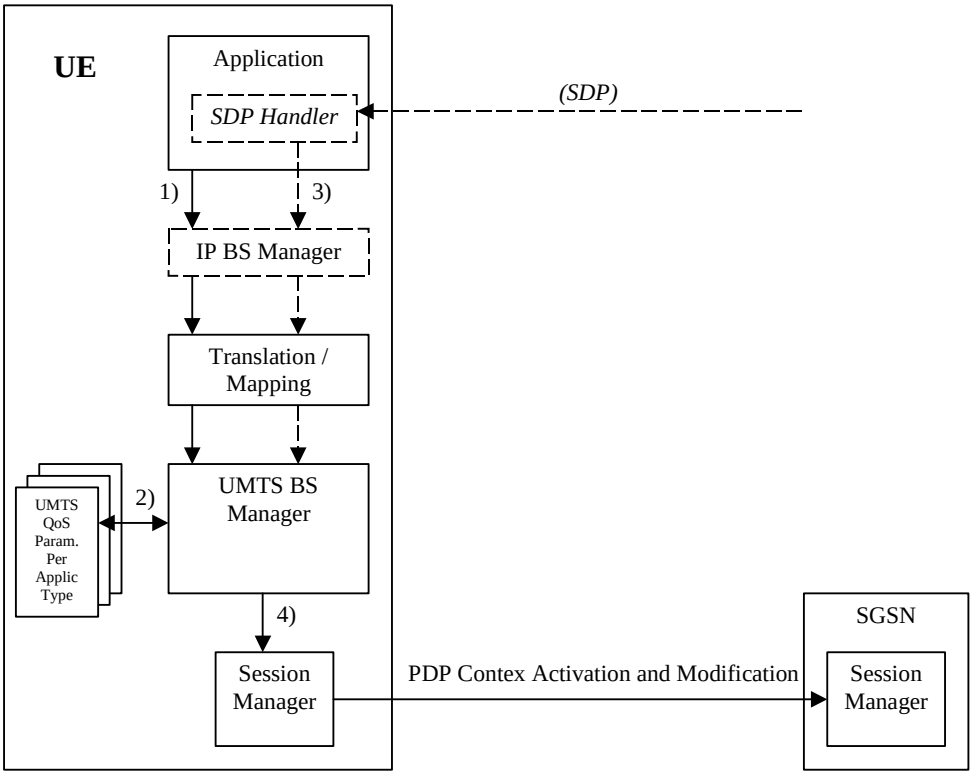


Figure 7.2: Framework for generating requested QoS parameters in the UE

7.2.1 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 7.2.1 to derive the Maximum and Guaranteed Bitrate DL/UL from the SDP Parameters.

Table 7.2.1: 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 [5] ;`
	`/* Conversational as default !*/`
	`ELSE`
	`Maximum Bitrate DL/UL and Guaranteed Bitrate DL/UL per media component as specified in reference [6] ;`
	`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>;`
	`ELSEIF mediastream only uplink THEN`
	`Maximum Bitrate UL = Guaranteed Bitrate UL =<bandwidth>;`
	`ELSEIF mediastreams both downlink and uplink THEN`
	`Maximum Bitrate DL = Guaranteed Bitrate DL =<bandwidth>;`
	`Maximum Bitrate UL = Guaranteed Bitrate UL =<bandwidth>;`
	`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 ;`

7.2.2 SDP parameters to Authorized UMTS QoS parameters mapping in UE

If the PDP Context is activated or modified ~~in an IMS context in which~~and SBLP is applied, i.e. an authorization token has been received, then the UE should use the mapping rules in table 7.2.2.1 for all applications using SDP to derive the Maximum Authorized Bandwidth UL/DL per flow identifier.

Table 7.2.2.1 also has a mapping rule for derivation of Maximum Authorized Traffic Class per flow identifier which applies for session initiation and modification.

In future releases this mapping rule may change. ~~For release 5 this mapping rule is optional for the UE~~

~~i~~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 7.2.2.1 for each forked response.

Table 7.2.2.1: Rules for derivation of the Maximum Authorized Bandwidth DL/UL and the Maximum Authorized Traffic Class per flow identifier in the UE

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

Maximum Authorized Bandwidth DL (Max_BW_DL) and UL (Max_BW_UL) per flow identifier (see note 5)	IF SBLP is applied THEN
	
	/* The Direction of the IP flow(s) identified by the flow identifier */
	
	IF a=recvonly THEN
	IF <SDP direction> = mobile originated THEN
	Direction:= downlink;
	ELSE /* mobile terminated */
	Direction:= uplink;
	ENDIF;
	ELSE;
	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];
	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};

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

	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;
	
	ELSE
	No authorization is done ;
	ENDIF ;

Maximum Authorized Traffic Class [MaxTrafficClass] per flow identifier (see NOTE 1, 2 and3)	IF SBLP is applied THEN
	IF (all media IP flows of media type "audio" or "video" for the session 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;
	ELSE
	No authorization is done ;
	ENDIF ;

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 maximum Authorized Traffic Class 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 maximum Authorized Traffic Class taking into account the already existing media IP flows within the session
NOTE 4: The SDP parameters are described in RFC 2327 [9].
NOTE 5: The 'b=RS:' and 'b=RR:' SDP bandwidth modifiers are defined in RFC 3556 [10].

The UE should per ongoing session store the Authorized UMTS QoS parameters per flow identifier.

Before activate or modify 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 7.2.2.2). Furthermore, if the rule in table 7.2.2.1 for calculating Traffic Class per flow identifier 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 7.2.2.2).

Table 7.2.2.2: 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	IF SBLP is applied THEN
	
	Maximum Authorized Bandwidth DL/UL per PDP Context is the sum of all Maximum Authorized Bandwidth DL/UL for all the flow identifiers associated with that PDP Context ;
	
	IF Maximum Authorized Bandwidth DL/UL per PDP Context > 16000 kbps THEN
	Maximum Authorized Bandwidth DL/UL per PDP Context = 16000 kbps
	/* See ref [8] */
	END;
	
	ELSE
	No authorization is done ;
	ENDIF ;

Maximum Authorized Traffic Class per PDP Context	IF SBLP is applied THEN
	
	Maximum Authorised Traffic Class per PDP Context = MAX [Maximum Authorised Traffic Class per flow identifier among all the flow identifiers associated with that PDP Context] ;
	
	ELSE
	No authorization is done ;
	ENDIF ;
	
	(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)

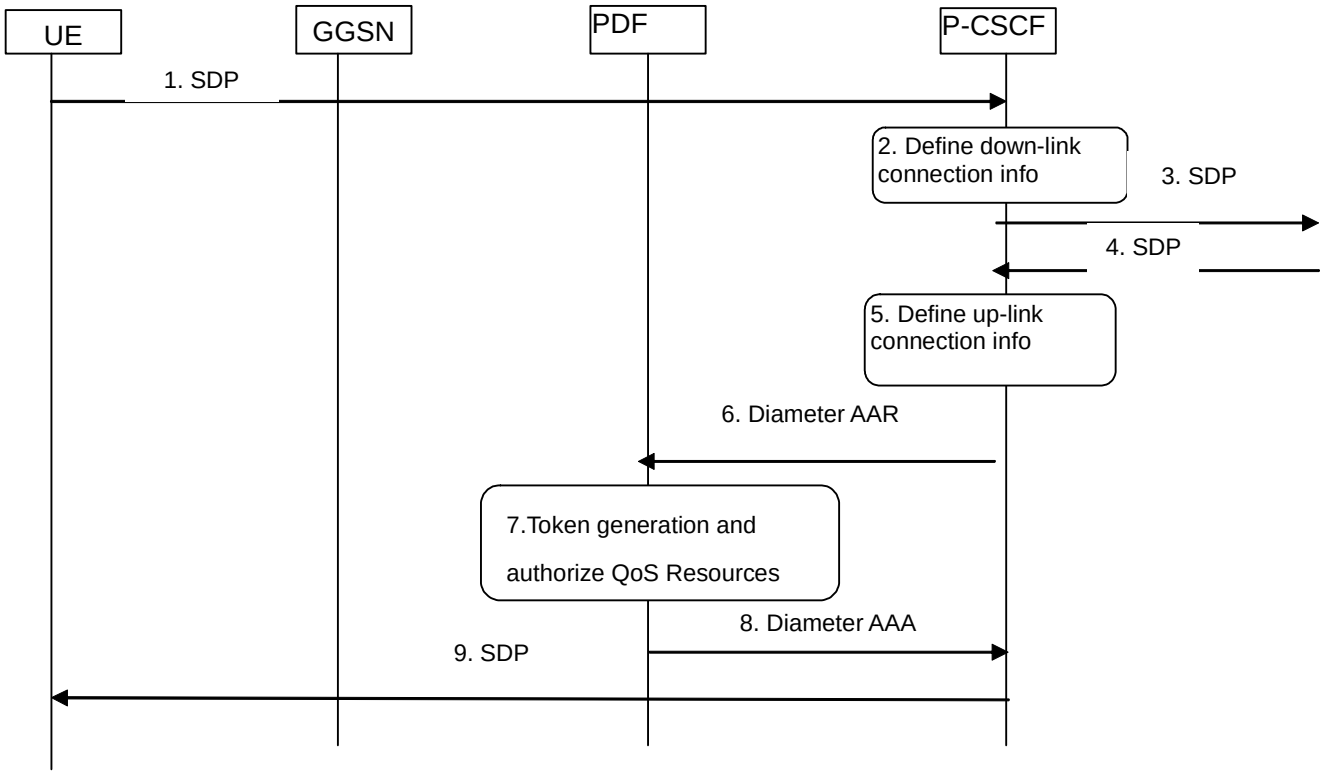
Next modified clause

Annex B (normative): Signalling Flows for IMS

B.1 Authorize QoS resources

B.1.1 Authorize QoS resources at originating P-CSCF and PDF at IMS session establishment

This clause covers the Authorize QoS resources procedure at the originating P-CSCF and PDF at IMS session establishment.

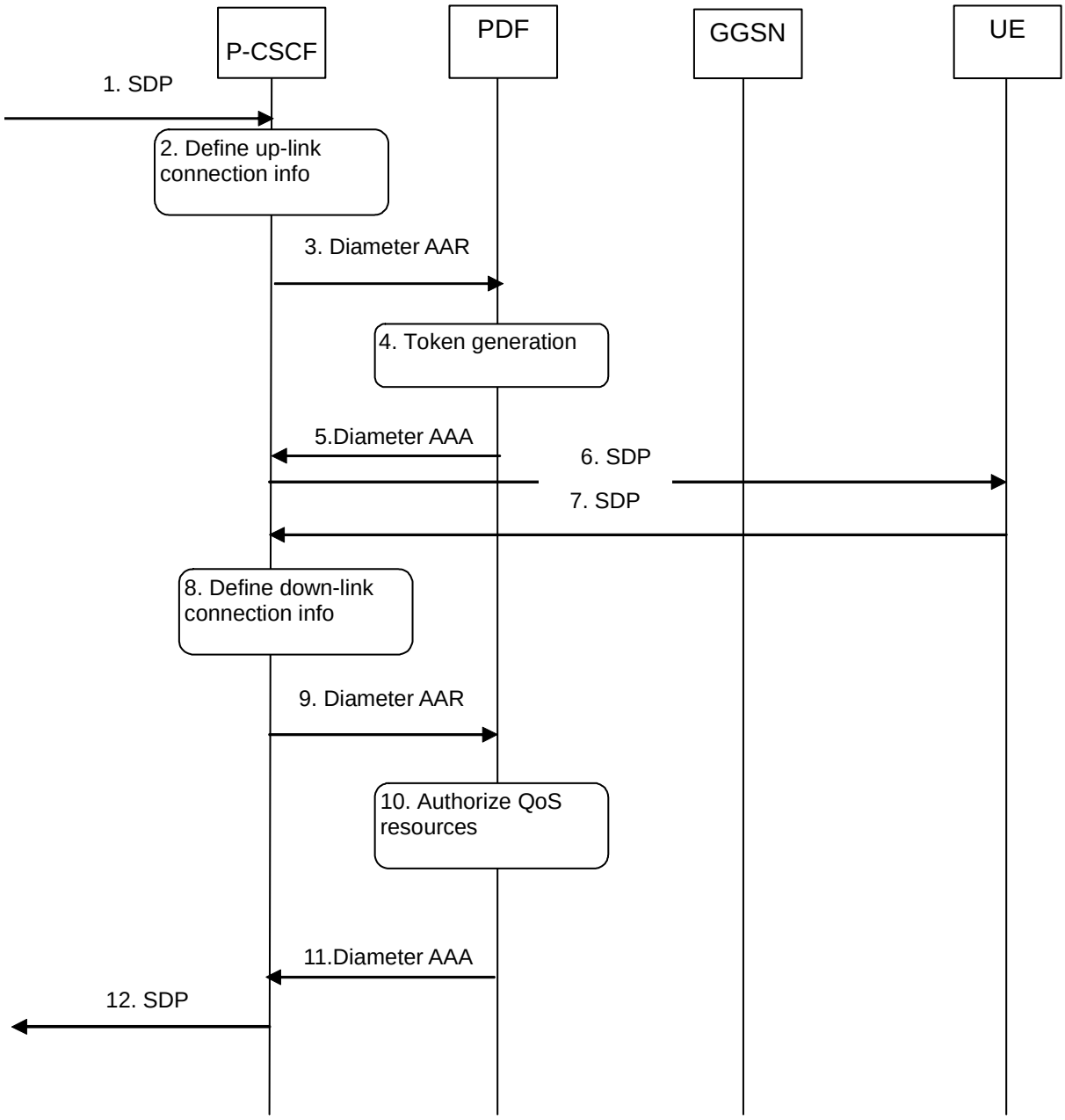


1. The P-CSCF receives the SDP parameters defined by the originator within an SDP offer in SIP signalling.
2. The P-CSCF identifies the connection information needed (IP address of the down link IP flow(s), port numbers to be used etc…).
3. The P-CSCF forwards the SDP offer in SIP signalling.
4. The 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 PDF and requests an authorization token by sending a Diameter AAR for a new Diameter session.
7. The PDF authorizes every component negotiated for the session. An authorization token is generated by the PDF.
8. The PDF sends the authorization token to the P-CSCF.
9. Upon successful authorization of the session the SDP parameters and the Authorization token are passed to the UE in SIP signalling.

Figure B.1.1: Authorize QoS resources at originating PDF

B.1.2 Authorize QoS resources at terminating P-CSCF and PDF at IMS session establishment

This clause covers the Authorize QoS resources procedure at the terminating P-CSCF and PDF at IMS session establishment.

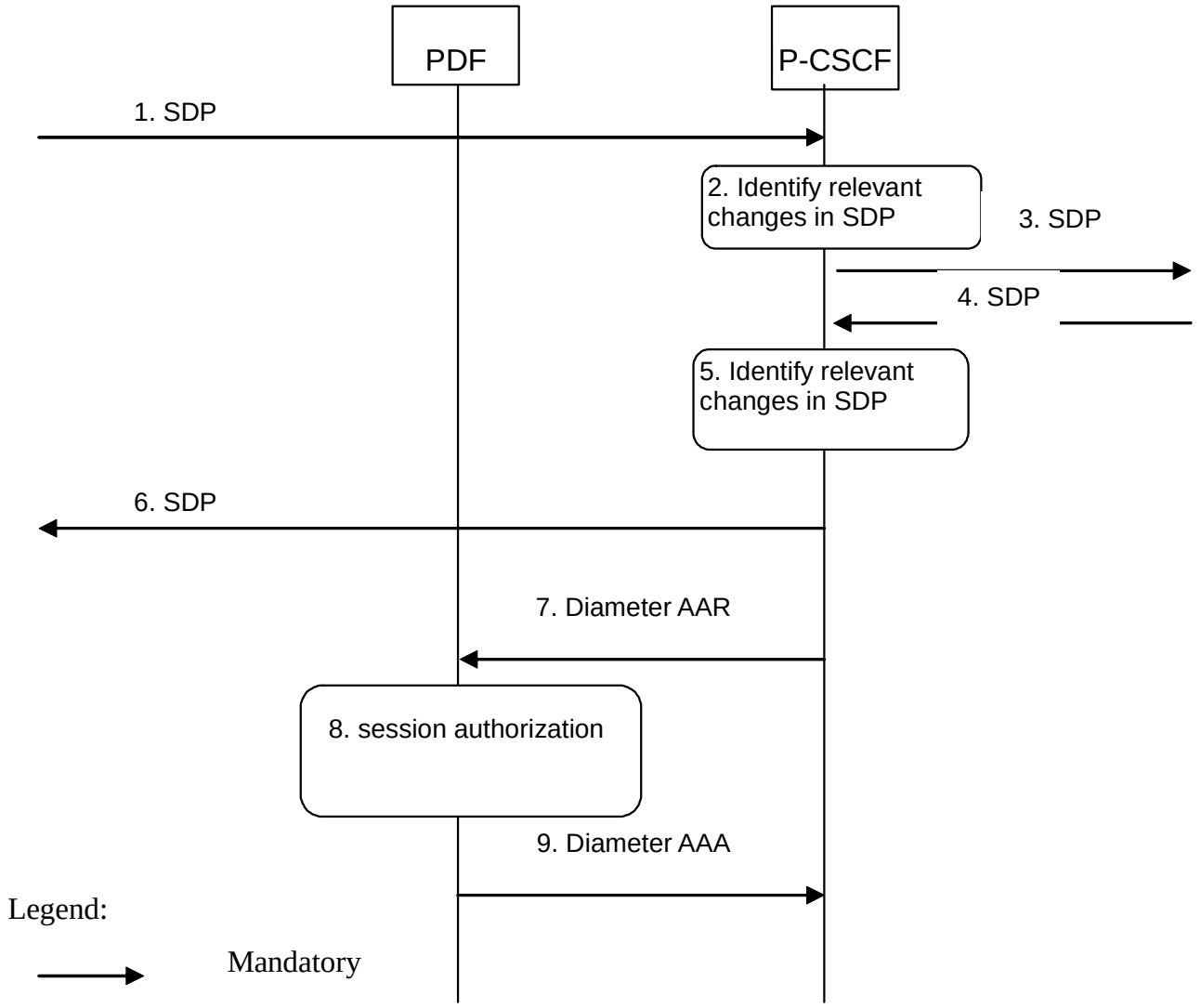


1. The P-CSCF receives the SDP parameters defined by the originator.
2. The P-CSCF identifies the connection information needed (IP address of the up-link IP flow(s), port numbers to be used etc…).
3. The P-CSCF requests the Authorisation Token from the PDF by sending a Diameter AAR for a new Diameter session.
4. An authorization token is generated by the PDF.
5. The PDF sends the authorization token to the P-CSCF.
6. The P-CSCF sends the SDP offer and the authorization token to the UE-
7. The P-CSCF receives the negotiated SDP parameters from the UE.
8. The P-CSCF identifies the connection information needed (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 PDF by sending a Diameter AAR for the existing Diameter session.
10. The PDF authorizes every component negotiated for the session.
11. The PDF sends an Diameter AAA to the P-CSCF.
12. Upon successful authorization of the session the SDP parameters in the SDP answer are passed to the originator.

Figure B.1.2: Authorize QoS resources at terminating PDF

B.1.3 Authorize QoS resources at IMS session modification

This clause covers the Authorize QoS resources procedure at IMS session modification both at the originating and terminating side.



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 forwards the SDP answer in SIP signalling.
7. The P-CSCF sends a Diameter AAR for an existing Diameter session and includes the derived updated service information.
8. The PDF authorizes the received service information. The PDF may need to approve or remove the QoS commit (see Clauses B.3 and B.4, respectively) , revoke the authorization for GPRS and IP resources at media component removal (see Clause B.5.2), or perform a Session modification initiated SBLP authorization decision (see Clause B.8) due to the updated service information.
9. The PDF answers with a Diameter AAA.

Figure B.1.3: Authorize QoS resources at IMS session modification

B.2 Resource reservation flow with Service-based local policy

Clause 5 applies.

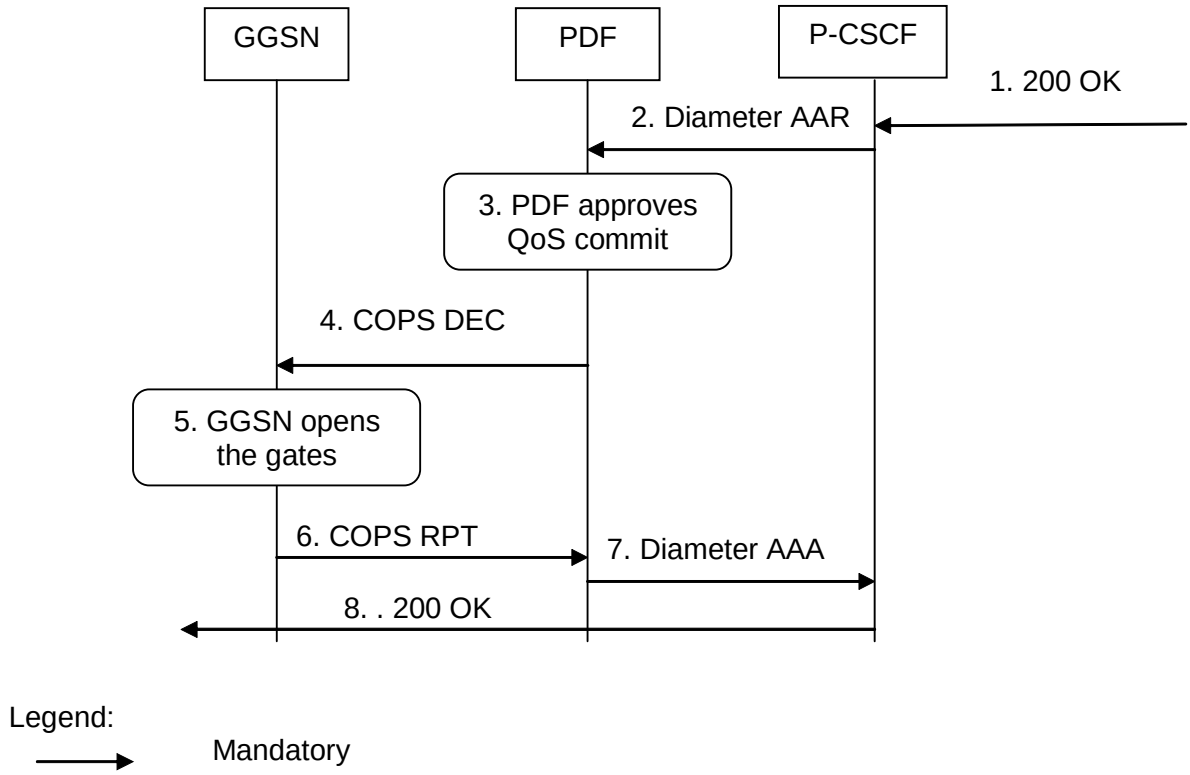
B.3 Approval of QoS commit

Through Approval of QoS Commit the PDF 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 PDF 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 Approval of QoS Commit procedure is triggered by the P-CSCF receiving a 200 OK response to an INVITE request or a 200 OK response to an UPDATE request within a confirmed dialogue. When receiving those 200 OK responses, the PDF shall take the SDP direction attribute in the latest received SDP (either within the 200 OK or a previous SIP message) into account when deciding, which gates shall be opened:

- For a unidirectional SDP media component, the Approval of QoS Commit procedure shall not be triggered for the possible media IP flows in the opposite direction.
- For an inactive SDP media component, the Approval of QoS Commit procedure shall not be triggered for the media IP flows.

Figure B.3.1.1 is applicable to the Mobile Originating (MO) side and the Mobile Terminating (MT) side.



1. The P-CSCF receives the 200 OK message complying with the conditions specified in the paragraphs above.
2. The P-CSCF sends a Diameter AAR message to the PDF, requesting that gates shall be opened.
3 The PDF approves the QoS Commit.
4. The PDF sends COPS DEC message(s) to the GGSN to open the 'gates' e.g. enable the use of the authorised QoS resources.
5. The GGSN receives the COPS DEC message(s) and opens the 'gates' e.g. enables the use of the authorised QoS resources.
6 The GGSN sends COPS RPT message(s) back to the PDF.
7 The PDF sends a Diameter AAA to the P-CSCF.
8 The P-CSCF forwards the 200 OK message.

Figure B.3.1.1: Approval of QoS Commit to both the Mobile Originating (MO) side and the Mobile Terminating (MT) side

B.4 Removal of QoS commit

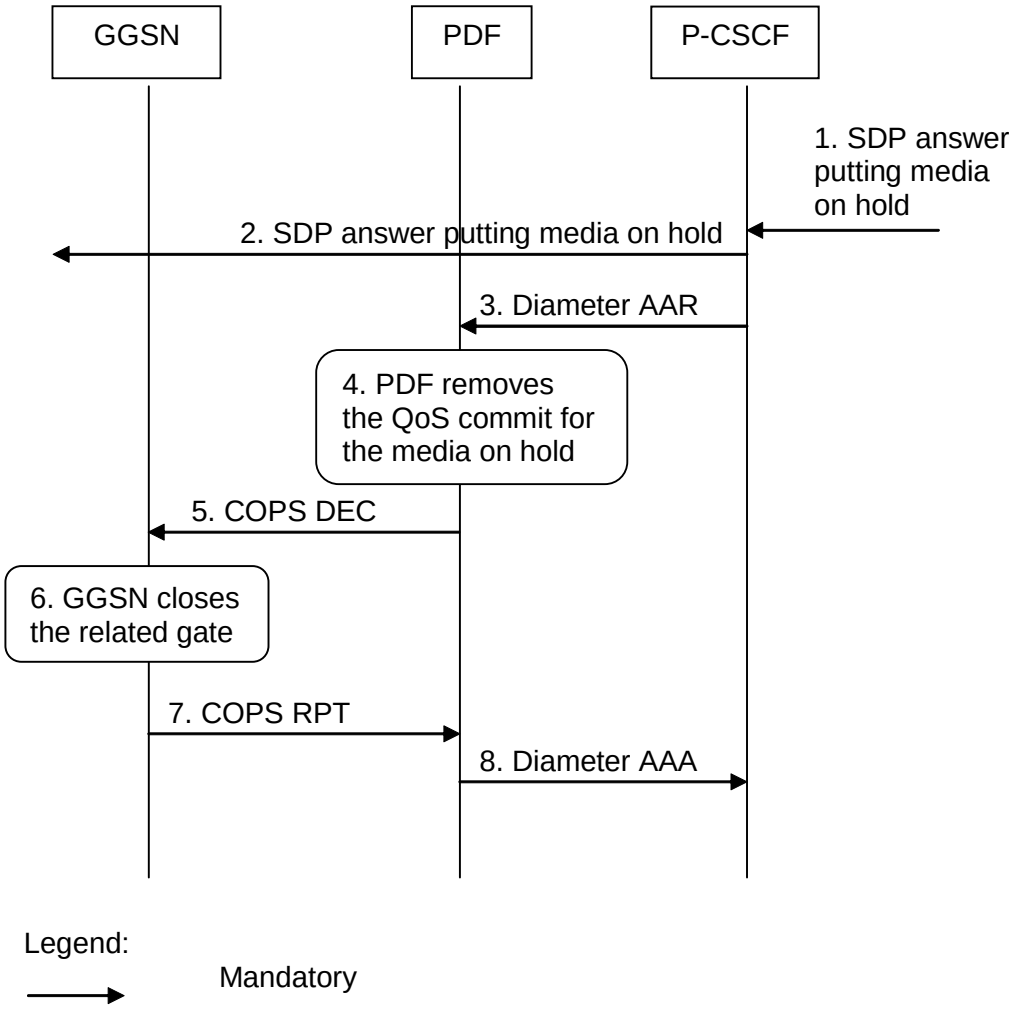
The "Removal of QoS commit" procedure is used e.g. when a session is released and the related IP flows are removed from a PDP context that multiplexes IP flows from several sessions, or when media IP flow(s) of a session are put on hold (e.g. in case of a media re-negotiation or call hold). The PDF decision of "Removal of QoS commit" shall be sent as a separate decision to the GGSN corresponding to the previous "Authorize QoS Resources" request.

B.4.1 Removal of QoS commit at Media on Hold

Media is placed on hold as specified in RFC 3264 [11].

If a bidirectional media component is placed on hold by making it unidirectional, the QoS Commit shall only be removed in the deactivated direction.

Figure B.4.1.1 presents the "Removal of QoS commit" procedure at media on hold to both the Mobile Originating (MO) side and the Mobile Terminating (MT) side.



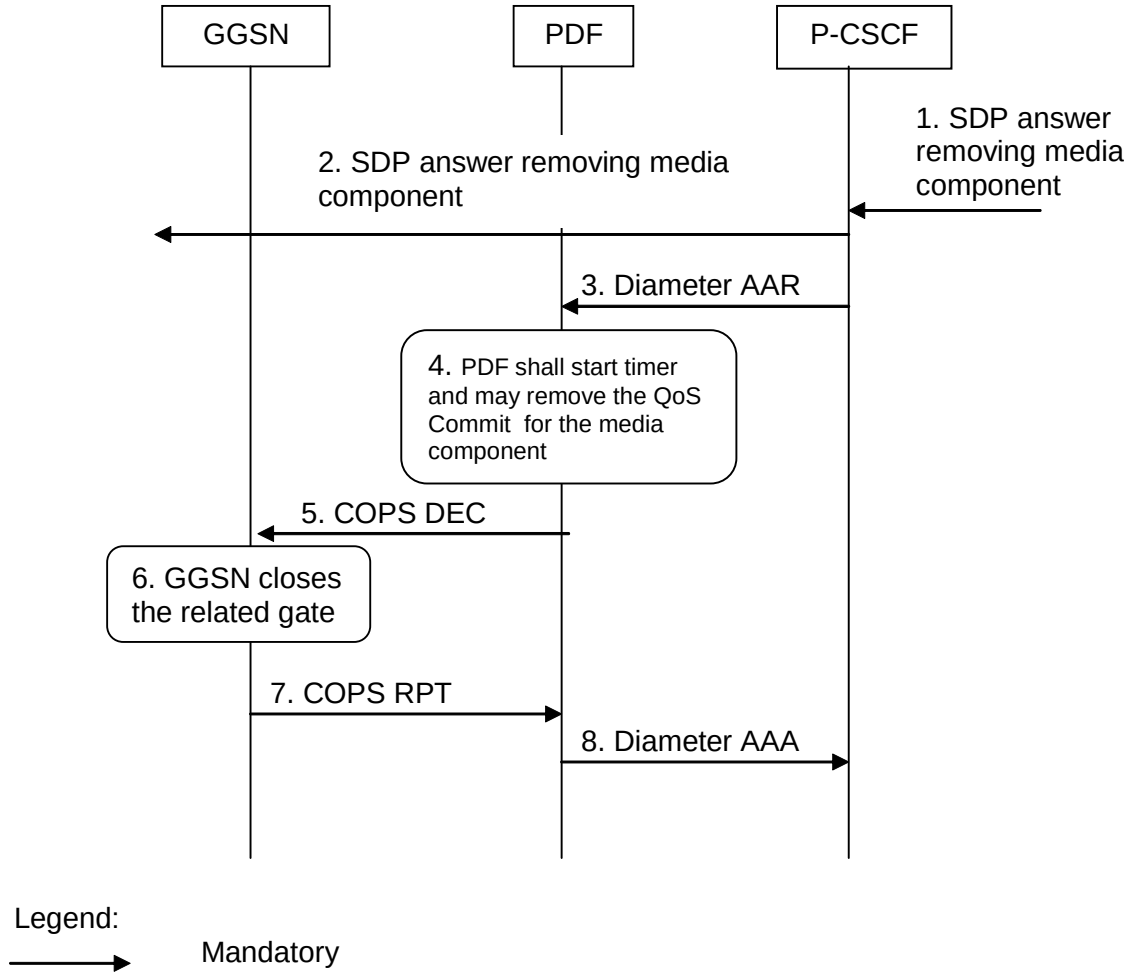
1. The P-CSCF receives an SDP answer putting media on hold within a SIP message. (NOTE 1)
2. The P-CSCF forwards the SDP answer putting media on hold within a SIP message.
3. The P-CSCF sends a Diameter AAR request to the PDF, requesting that gates shall be closed.
4. The PDF removes the QoS commit for the media on hold.
5. The PDF sends the COPS DEC message(s) to the GGSN to close the relevant media IP flow gate(s),leaving the possible related RTCP gate(s) open to keep the connection alive.
6. The GGSN receives the COPS DEC message(s) and closes the requested gate(s).
7. The GGSN sends the COPS RPT message(s) back to the PDF.
8. The PDF sends a Diameter AAA message back to the P-CSCF.

NOTE 1: This procedure occurs whenever a bidirectional media is made unidirectional.

Figure B.4.1.1: Removal of QoS commit at Media on Hold to both the Mobile Originating (MO) side and the Mobile Terminating (MT) side

B.4.2 Removal of QoS commit at media component removal

Figure B.4.2.1 presents the "Removal of QoS commit" procedure at media component removal for both the Mobile Originating (MO) side and the Mobile Terminating (MT) side. This procedure is optional. In addition, the procedure in Clause B.5.2 applies in this situation after timer expiry.



1. The P-CSCF receives an SDP answer removing media component.
2. The P-CSCF forwards the SDP answer removing media component.
3. The P-CSCF sends a Diameter AAR to the PDF, requesting that corresponding gates shall be closed.
4. The PDF shall start timer and may remove the QoS commit for the related IP flow(s) of the media component. After timer expiry, Figure B.5.1.1applies.
5. The PDF sends a COPS DEC message to the GGSN to close the related 'gate(s)'.
6. The GGSN receives the COPS DEC message and closes the 'gate(s)'.
7. The GGSN sends a COPS RPT message back to the PDF.
8. The PDF sends a Diameter AAA message back to the P-CSCF.

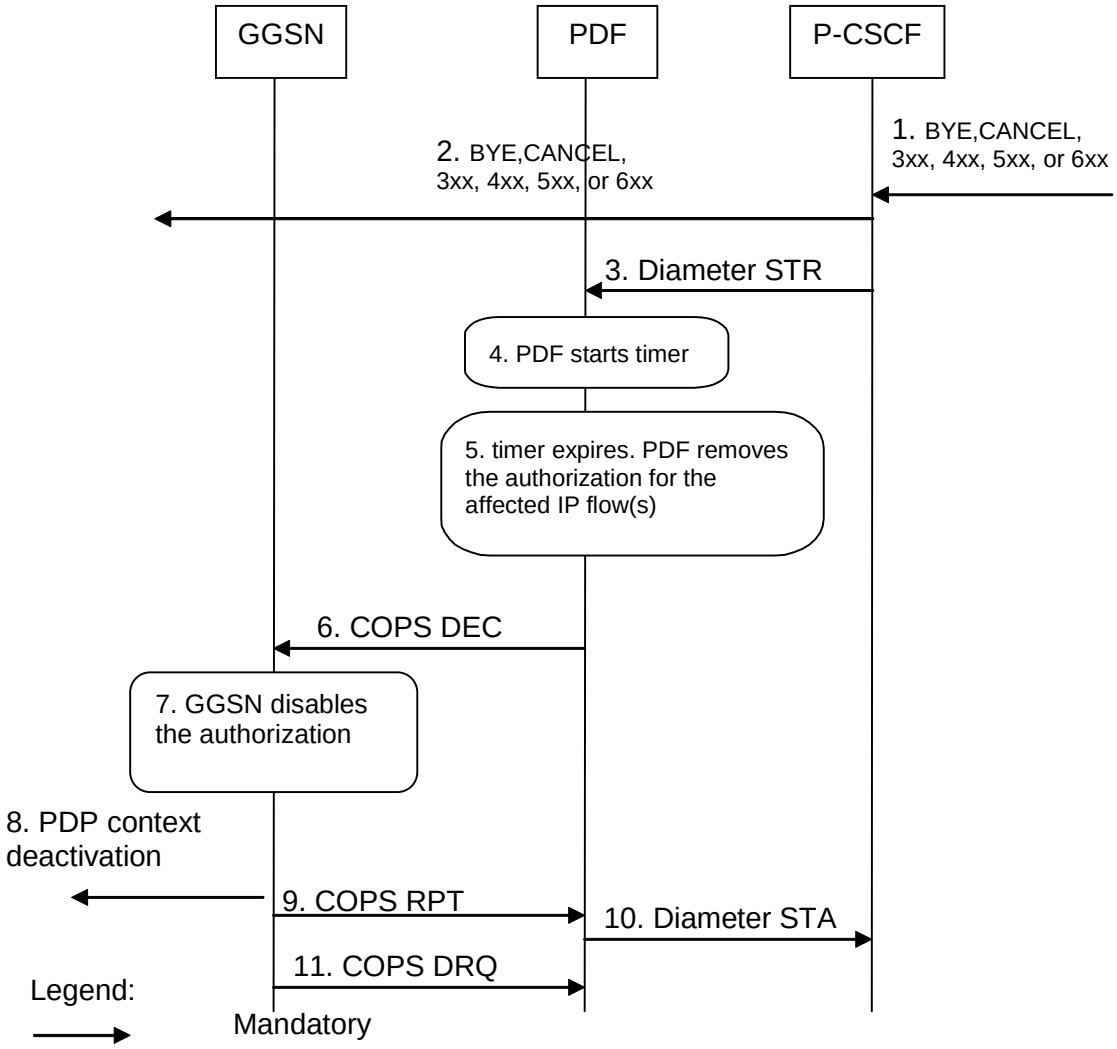
Figure B.4.2.1: Removal of QoS commit at media component removal for both the Mobile Originating (MO) side and the Mobile Terminating (MT) side

B.5 Revoke authorization for GPRS and IP resources

The "Revoke Authorization for GPRS and IP resources" procedure is used e.g. upon session release or upon session redirection of the only or last session of a given client handle (PDP context) or upon SIP final error response initiated after bearer establishment. The PDF decision of "Revoke Authorization for UMTS and IP Resources" shall be sent as a separate decision to the GGSN corresponding to the previous "Authorize QoS Resources" request.

B.5.1 Mobile initiated session release / Network initiated session release

Figure B.5.1.1 presents the "Revoke Authorization for UMTS and IP Resources" at Mobile initiated session release / Network initiated session release (of the only or last session of a given client handle) 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.

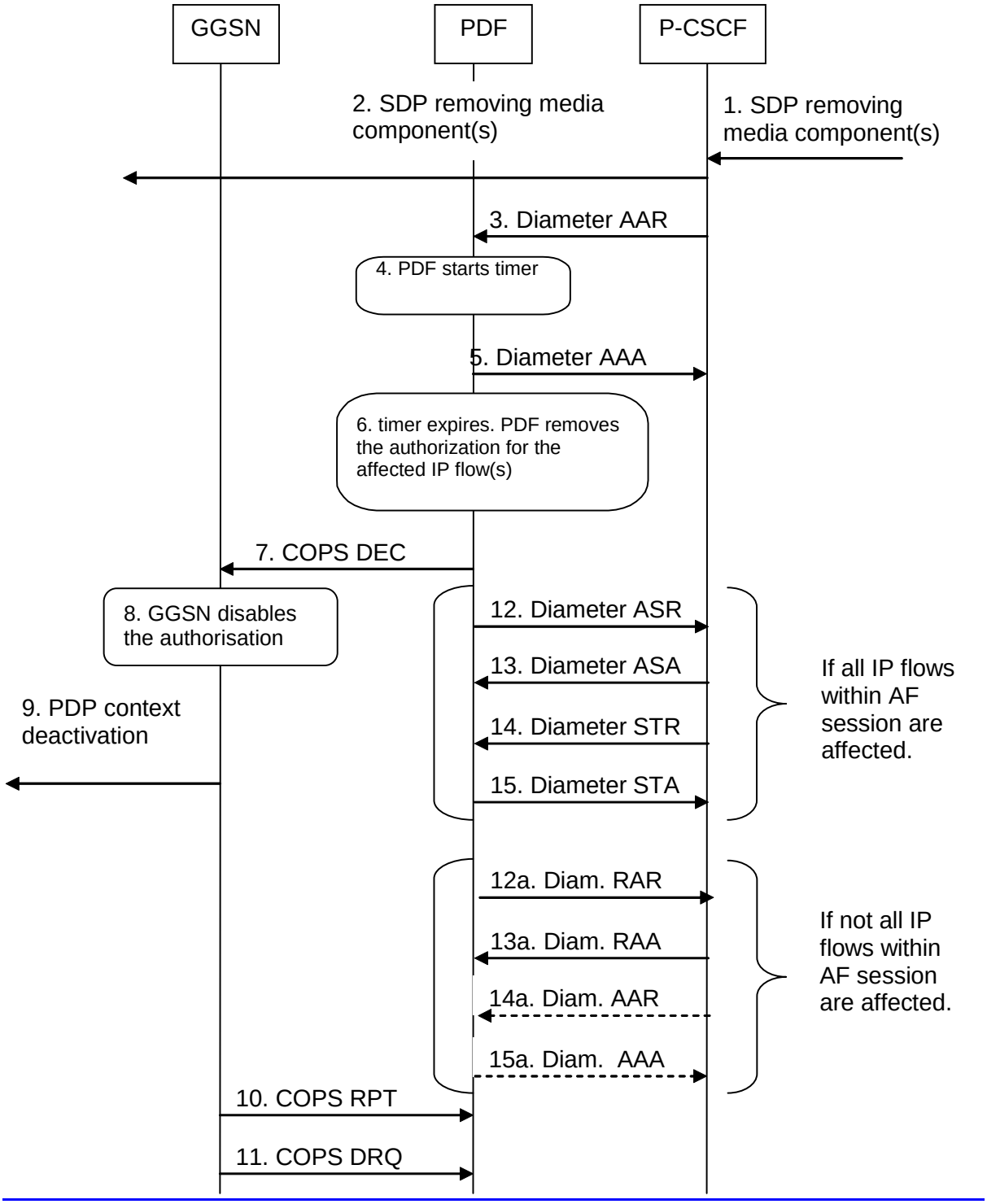


1. SIP BYE message, a SIP CANCEL request, a SIP 3xx redirect response, or any 4xx, 5xx, or 6xx SIP final error response is received by the P-CSCF.
2. P-CSCF forwards the BYE message, or the SIP 3xx redirect response, a SIP CANCEL request, or any 4xx, 5xx, or 6xx SIP final error response.
3. The P-CSCF sends a session termination request to the PDF to initiate the revocation of the authorization
4. PDF starts timer.
5. The timer expires, but the PDF has not been notified that the affected PDP context(s) have been modified or deactivated to match the revoked authorization. The PDF removes the authorization for the IP flow(s) of this session, which it authorized previously.
6. If step 5 occurs, the PDF sends the COPS DEC message(s) to the GGSN including the client handle(s), which identifies the PDP context(s) to be deactivated.
7. The GGSN receives the COPS DEC message, and disables the use of the authorized QoS resources.
8. The GGSN initiates the deactivation of the PDP context(s) used for the IP multimedia session, in case the UE has not done it before.
9. The GGSN sends the COPS RPT message(s) back to the PDF.
10. The PDF indicates the result of the authorization revocation by sending a Diameter session termination answer to the P-CSCF
11. The GGSN sends the COPS DRQ message(s) to the PDF.

Figure B.5.1.1: Revoke authorization for GPRS and IP resources - Mobile initiated session release / Network initiated session release for both Mobile Originating (MO) and Mobile termination side

B.5.2 Media component removal

Figure B.5.2.1 presents the "Revoke Authorization for UMTS and IP Resources" 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. In addition, the procedure in Clause B.4.2 may have been applied before the PDF removes the authorization for the affected IP flow(s).



1. A SIP message containing SDP indicating the removal of media component(s) is received by the P-CSCF.
2. The P-CSCF forwards the SIP message.
3. The P-CSCF sends Diameter AAR to the PDF with modified service information.
4. PDF starts timer.
5. The PDF send Diameter AAA to P-CSCF
6. The timer expires, but the PDF has not been notified that the affected PDP context(s) have been modified or deactivated to match the revoked authorization. The PDF removes the authorization for the affected IP flow(s), which it authorized previously.
7. If step 6 occurs, the PDF sends the COPS DEC message(s) to the GGSN including the client handle(s), which identifies the PDP context(s) to be deactivated.
8. The GGSN receives the COPS DEC message, and disables the use of the authorized QoS resources.
9. The GGSN initiates the deactivation of the PDP context(s), in case the UE has not done it before.
10. The GGSN sends the COPS RPT message(s) back to the PDF.
11. The GGSN sends the COPS DRQ message(s) to the PDF.

If step 6 occurs and all IP flows within AF session are affected by PDP context release:
12. The PDF indicates the bearer removal to the AF by sending an abort session request to the AF.
13. The AF responds by sending an abort session answer to the PDF.
14. The AF sends session termination request to the PDF to indicate that the session has been terminated
15. The PDF responds by sending a session termination answer to the AF.

If step 6 occurs and not all IP flows within AF session are affected by PDP context release:
12a. The PDF indicates the PDP context release to the AF by sending an RAR.
13a. The AF responds by sending an RAA to the PDF.
14a. The AF may send an AAR to the PDF to update the session information.
15a. If step 14a occurs, the PDF responds by sending a AAA to the AF.

Figure B.5.1.1: Revoke authorization for GPRS and IP resources - media component removal for both Mobile Originating (MO) and Mobile termination side

B.6 Indication of PDP Context Release

Clause 6.4 applies.

B.7 Modification of PDP Context

Clause 6.5 applies.

B.8 Session modification initiated SBLP authorization decision

The GGSN receives an unsolicited authorization decision from the PDF, when a session is modified without adding or removing media lines from SDP (refer to 3GPP TS 29.207 [7]). The procedures in Clause 6.6 apply.