

# ETSI TS 123 207 V6.6.0 (2005-09)

---

*Technical Specification*

**Digital cellular telecommunications system (Phase 2+);  
Universal Mobile Telecommunications System (UMTS);  
End-to-end Quality of Service (QoS) concept and architecture  
(3GPP TS 23.207 version 6.6.0 Release 6)**

---



---

**Reference**

RTS/TSGS-0223207v660

---

**Keywords**

GSM, UMTS

**ETSI**

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

---

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

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

---

**Important notice**

---

Individual copies of the present document can be downloaded from:

<http://www.etsi.org>

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

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at

<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, please send your comment to one of the following services:

[http://portal.etsi.org/chaicor/ETSI\\_support.asp](http://portal.etsi.org/chaicor/ETSI_support.asp)

---

**Copyright Notification**

---

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

© European Telecommunications Standards Institute 2005.  
All rights reserved.

**DECT**<sup>TM</sup>, **PLUGTESTS**<sup>TM</sup> and **UMTS**<sup>TM</sup> are Trade Marks of ETSI registered for the benefit of its Members.  
**TIPHON**<sup>TM</sup> and the **TIPHON logo** are Trade Marks currently being registered by ETSI for the benefit of its Members.  
**3GPP**<sup>TM</sup> is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

---

## Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<http://webapp.etsi.org/IPR/home.asp>).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

---

## Foreword

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

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

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

# Contents

Intellectual Property Rights .....	2
Foreword.....	2
Foreword.....	5
1 Scope .....	6
2 References .....	6
3 Definitions and Abbreviations.....	7
3.1 Definitions .....	7
3.2 Abbreviations .....	8
4 High Level Requirements for End-to-End IP QoS.....	8
4.1 End-to-End QoS Negotiation Requirements .....	8
4.2 QoS Policy Requirements .....	9
5 End-to-End QoS Architecture .....	9
5.1 QoS Management Functions in the Network .....	9
5.1.1 Description of functions.....	10
5.1.1.1 QoS management functions for end-to-end IP QoS in UMTS Network .....	10
5.1.1.2 (void).....	11
5.1.1.3 Interaction to External Networks .....	11
5.1.1.4 Translation/mapping function in the GGSN and the UE.....	11
5.1.2 Allocation of QoS management functions .....	12
5.1.2.1 QoS management functions for end-to-end IP QoS .....	12
5.2 Capabilities of Functional Elements.....	12
5.2.1 GGSN .....	12
5.2.2 UE.....	13
5.2.3 PDF.....	14
5.2.4 Application Function (AF).....	15
5.3 Go interface (PDF – GGSN) .....	15
5.3.1 Go Functional Requirements .....	15
5.3.2 Information Exchanged via Go Interface.....	16
5.3a Gq Interface (PDF - AF) .....	17
5.3a.1 Gq Functional Requirements .....	17
5.3a.2 Information Exchanged via Gq interface .....	17
5.4 QoS Parameters .....	19
5.5 QoS Parameter Mapping .....	19
6 End-to-End QoS Procedures .....	19
6.1 QoS Procedures in Functional Elements .....	19
6.1.1 Procedures in the GGSN.....	19
6.1.2 Procedures in the UE .....	19
6.1.3 Procedures in the PDF .....	20
6.1.4 Procedures in the AF.....	21
6.2 IP Bearer Level / Application Level Binding Mechanism .....	21
6.3 Session Flow: QoS Interaction Procedures .....	22
6.3.1 Authorize QoS Resources, AF session establishment.....	22
6.3.2 Resource Reservation Message Flows.....	23
6.3.2.1 Resource Reservation with Service-based Local Policy .....	23
6.3.2.2 Resource Reservation with IP QoS signalling .....	25
6.3.2.3 Resource Reservation with IP QoS reservation signalling and Service-based Local Policy.....	25
6.3.2.4 (void).....	25
6.3.3 Enable Media procedure .....	25
6.3.4 Disable Media procedure .....	26
6.3.5 Revoke Authorization for GPRS and IP Resources.....	26
6.3.6 Indication of PDP Context Release.....	27
6.3.6a Authorization of PDP Context Modification .....	28

6.3.7	Indication of PDP Context Modification .....	29
6.3.8	Update Authorization procedure.....	29
6.4	PDP Context Used for Application Level Signalling Transport.....	30
<b>Annex A (informative):</b>	<b>QoS Conceptual Models .....</b>	<b>32</b>
A.1	Introduction .....	32
A.2	Scenarios .....	33
A.2.1	Scenario 1 .....	33
A.2.2	Scenario 2 .....	34
A.2.3	Scenario 3 .....	35
A.2.4	Scenario 4 .....	38
A.2.5	Scenario 5 .....	39
<b>Annex B (informative):</b>	<b>(void) .....</b>	<b>41</b>
<b>Annex C (informative):</b>	<b>Sample Mapping of SDP Descriptions Into QoS Authorization.....</b>	<b>42</b>
<b>Annex D (informative):</b>	<b>Resource reservation and end-to-end RSVP .....</b>	<b>45</b>
D.1	Resource reservation with end-to-end RSVP .....	45
D.2	Resource Reservation with End-to-End RSVP and Service-based Local Policy .....	48
<b>Annex E (informative):</b>	<b>Change history .....</b>	<b>52</b>
History .....		54

---

# Foreword

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

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

Version x.y.z

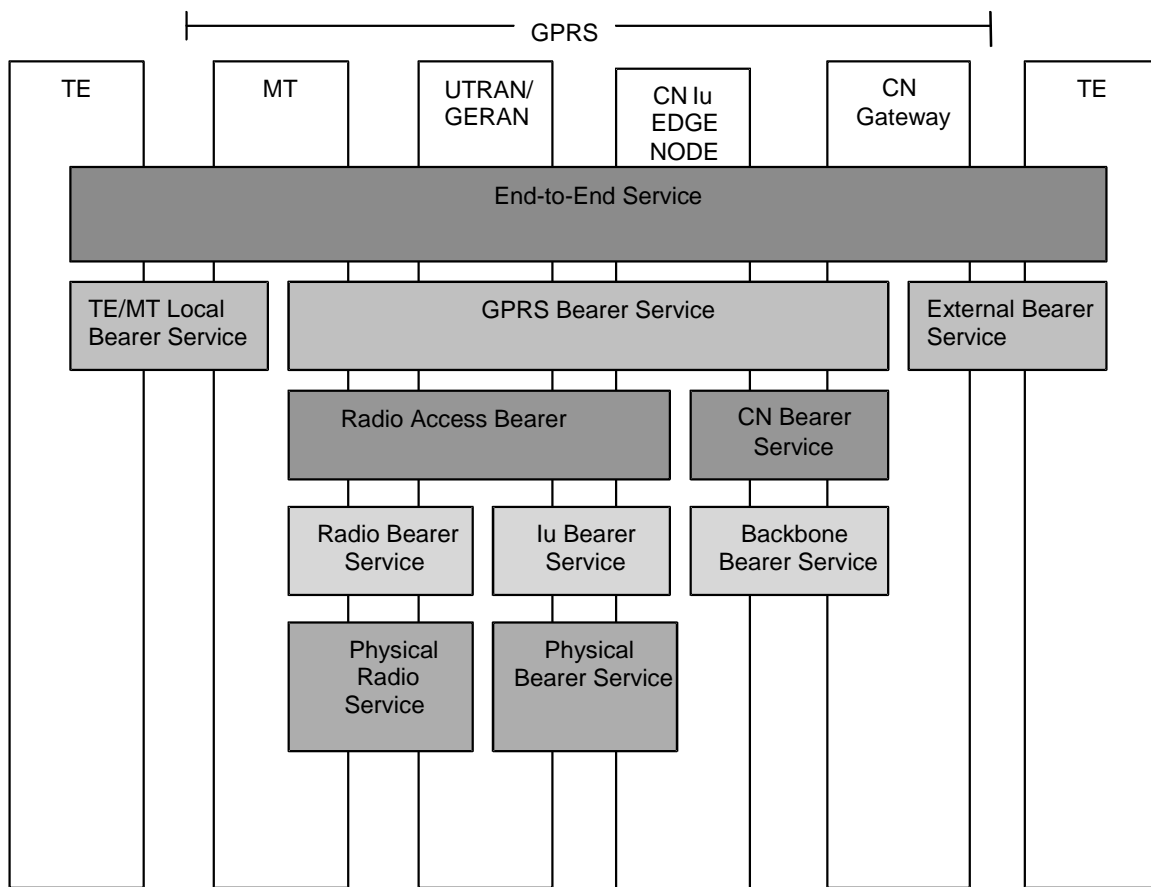
where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

# 1 Scope

The present document provides the framework for end-to-end Quality of Service involving GPRS and complements TS 23.107 [3] which describes the framework for Quality of Service within UMTS. The end-to-end QoS architecture is provided in Figure 1. The document describes the interaction between the TE/MT Local Bearer Service, the GPRS Bearer Service, and the External Bearer Service, and how these together provide Quality of Service for the End-to-End Service. The document also describes IP level mechanisms necessary in providing end-to-end Quality of Service involving GPRS networks, including possible interaction between the IP level and the GPRS level, as well as the application level and the IP level.

In contrast to the TS 23.107 [3], the present document is only applicable to GPRS packet switched access services, and includes aspects of interworking to the IM subsystem as well as PSTN and other networks. The document does not cover the circuit switched access services.



**Figure 1: End-to-End QoS Architecture**

# 2 References

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

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

- [1] 3GPP TS 22.228: "Service requirements for the Internet Protocol (IP) multimedia core network subsystem (IMS); Stage 1".
- [2] 3GPP TS 23.002: "Network Architecture".
- [3] 3GPP TS 23.107: "QoS Concept and Architecture".
- [4] 3GPP TS 23.228: "IP Multimedia (IM) Subsystem – stage 2".
- [4a] 3GPP TS 29.207: "Policy control over Go interface".
- [4b] 3GPP TS 29.208: "End to end Quality of Service (QoS) signalling flows".
- [4c] 3GPP TS 29.209: "Policy control over Gq interface".
- [5] 3GPP TS 22.105: "Vocabulary for 3GPP Specifications".
- [6] RFC 2475: "An Architecture for Differentiated Services (DiffServ)".
- [7] RFC 2753: "A Framework for Policy-based Admission Control".
- [8] RFC 2748: "Common Open Policy Service protocol (COPS)".
- [9] RFC 2205: "Resource ReSerVation Protocol (RSVP)".
- [10] RFC 2209: "Resource ReSerVation Protocol (RSVP) Message Processing Rules".
- [11] RFC 2210: "The use of RSVP with IETF integrated Services".
- [12] RFC 1633: "Integrated Services in the Internet Architecture: an Overview".
- [13] RFC 3261: "SIP: Session Initiation Protocol".
- [14] RFC 2327: "Session Description Protocol".
- [15] RFC 2998: "A Framework For Integrated Services Operation Over DiffServ Networks".
- [16] RFC 2750: "RSVP Extensions for Policy Control".
- [17] RFC 2474: "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers".
- [18] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".
- [19] 3GPP TS 23.060: "General Packet Radio Service (GPRS) Service description; Stage 2".
- [20] 3GPP TS 23.221: "Architecture requirements".

---

## 3 Definitions and Abbreviations

### 3.1 Definitions

**RSVP:** Resource ReSerVation Protocol: The RSVP protocol, RFC 2205 [9], is used by a host to request specific qualities of service from the network for particular application data streams or flows. The network responds by explicitly admitting or rejecting RSVP requests.

**DiffServ:** DiffServ networks classify packets into one of a small number of aggregated flows or "classes", based on the DiffServ codepoint (DSCP) in the packet's IP header. This is known as behavior aggregate (BA) classification (RFC 2475 [6]). At each DiffServ router, packets are subjected to a "per-hop behavior" (PHB), which is invoked by the DSCP (RFC 2474 [17]).



**IntServ:** The integrated services architecture RFC 1633 [12] defined a set of extensions to the traditional best effort model of the Internet with the goal of allowing end-to-end QoS to be provided to applications. One of the key components of the architecture is a set of service definitions; the current set of services consists of the controlled load and guaranteed services. The architecture assumes that some explicit setup mechanism is used to convey information to routers so that they can provide requested services to flows that require them. While RSVP is the most widely known example of such a setup mechanism, the IntServ architecture is designed to accommodate other mechanisms.

**COPS:** Common Open Policy Service: The COPS protocol RFC 2748 [8] is a simple query and response protocol that can be used to exchange policy information between a policy server (Policy Decision Point or PDP) and its clients (Policy Enforcement Points or PEPs).

**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 service 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 AF 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.

## 3.2 Abbreviations

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

AF	Application Function
APN	Access Point Name (*)
COPS	Common Open Policy Service protocol
DiffServ	Differentiated Services
DSCP	DiffServ Code Point
GERAN	GSM/EDGE Radio Access Network (*)
GGSN	Gateway GPRS Support Node (*)
HTTP	Hypertext Transfer Protocol (*)
IMS	IP Multimedia Subsystem
IntServ	Integrated Services
LAN	Local Area Network
LDP	Label Distribution Protocol
MPLS	Multiprotocol Label Switching Architecture
PDF	Policy Decision Function
PEP	Policy Enforcement Point
PHB	Per Hop Behaviour
RNC	Radio Network Controller (*)
SDP	Session Description Protocol
SIP	Session Initiation Protocol (*)
SNMP	Simple Network Management Protocol (*)
TFT	Traffic Flow Template (*)

\* This abbreviation is covered in 21.905v 4.2.0 [18]

---

# 4 High Level Requirements for End-to-End IP QoS

## 4.1 End-to-End QoS Negotiation Requirements

- The UMTS QoS negotiation mechanisms used for providing end-to-end QoS shall be backward compatible with UMTS Release 1999.
- The UMTS QoS negotiation mechanisms used for providing end-to-end QoS shall not make any assumptions about the situation in external networks which are not within the scope of 3GPP specifications.

- The UMTS QoS negotiation mechanisms used for providing end-to-end QoS shall not make any assumptions about application layer signalling protocols.
- No changes to non-UMTS specific QoS negotiation mechanisms.
- The UMTS QoS negotiation mechanisms used for providing end-to-end QoS shall not make any assumptions about applications which may be used on terminal equipment attached to mobile terminals.
- Unnecessary signalling complexity and processing complexity in the network elements as well as the mobile terminal shall be avoided.
- Unnecessary signalling traffic due to end-to-end QoS negotiation shall be avoided.
- Methods for user authentication as well as billing and charging mechanisms related to the end-to-end QoS negotiation shall be kept as simple as possible.
- Minimum changes to network architecture and mechanisms due to introduction of end-to-end QoS negotiation.
- It shall be possible for an application on the external device to request end-to-end QoS.
- In order to enable the proper operation of service based local policy control, and to facilitate roaming in different networks, the mappings performed in various parts of the network need to be consistent.

## 4.2 QoS Policy Requirements

- The UMTS policy mechanisms described in TS 23.060 [19] shall be used for control of the UMTS bearers.
- Interaction between UMTS bearer services and IP bearer services shall only occur at the translation function in the UE and GGSN.

---

# 5 End-to-End QoS Architecture

## 5.1 QoS Management Functions in the Network

To provide IP QoS end-to-end, it is necessary to manage the QoS within each domain. An IP BS Manager is used to control the external IP bearer service. Due to the different techniques used within the IP network, this communicates to the UMTS BS manager through the Translation function.

At PDP context setup the user shall have access to one of the following alternatives:

- Basic GPRS IP connectivity service: The bearer is established according to the user's subscription, local operator's IP bearer resource based policy, local operator's admission control function and GPRS roaming agreements. In this case, IP bearer resource based local policy decisions may be applied to the bearer.
- Enhanced GPRS based services: The bearer is used to support an enhanced application-layer service, such as IM. In this case, service-based local policy decisions (e.g., authorization and policy based control) are also applied to the bearer.

To enable coordination between events in the application layer and resource management in the IP bearer layer, a logical element, the Policy Decision Function (PDF), is used as a logical policy decision element. It is also possible to implement a policy decision element internal to the IP BS Manager in the GGSN. The IP policy architecture does not mandate the policy decision point to be external to the GGSN.

Whenever resources not owned or controlled by the UMTS network are required to provide QoS, it is necessary to interwork with the external network that controls those resources. Interworking may be realised in a number of ways, including:

- signalling along the flow path (e.g. RSVP, LDP).
- packet marking or labelling along the flow path (e.g. DiffServ, MPLS)

- interaction between Policy Control and/or Resource Management elements.
- Service Level Agreements enforced by the border routers between networks.

For the policy control the following should apply:

- The IP policy framework employed in UMTS should, as far as possible, conform to IETF "Internet Standards". The IETF policy framework may be used for policy decision, authorization, and control of the IP level functionality, at both user and network level.
- There should be separation between the scope and roles of the UMTS policy mechanisms and the IP policy framework. This is to facilitate separate evolution of these functions.

## 5.1.1 Description of functions

### 5.1.1.1 QoS management functions for end-to-end IP QoS in UMTS Network

NOTE: The end-to-end QoS management functions do not cover the cases of a circuit switched service, or an IP service interworking with an ATM service at the gateway node.

**IP BS Manager** uses standard IP mechanisms to manage the IP bearer services. These mechanisms may be different from mechanisms used within the UMTS, and may have different parameters controlling the service. When implemented, the IP BS Manager may include the support of DiffServ Edge Function and the RSVP function. The **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, and interacts with the IP BS Manager. In the GGSN, the IP QoS parameters are mapped into UMTS QoS parameters, where needed. In the UE, the QoS requirements determined from the application layer (e.g., SDP) are mapped to either the PDP context parameters or IP layer parameters (e.g., RSVP).

If an IP BS Manager exists both in the UE and the Gateway node, it is possible that these IP BS Managers communicate directly with each other by using relevant signalling protocols.

The required options in the table define the minimum functionality that shall be supported by the equipment in order to allow multiple network operators to provide interworking between their networks for end-to-end QoS. Use of the optional functions listed below, other mechanisms which are not listed (e.g. over-provisioning), or combinations of these mechanisms are not precluded from use between operators.

The IP BS Managers in the UE and GGSN provide the set of capabilities for the IP bearer level as shown in table 1. Provision of the IP BS Manager is optional in the UE, and required in the GGSN.

**Table 1: IP BS Manager capability in the UE and GGSN**

Capability	UE	GGSN
DiffServ Edge Function	Optional	Required
RSVP/IntServ	Optional	Optional
IP Policy Enforcement Point	Optional	Required (*)

(\*) Although the capability of IP policy enforcement is required within the GGSN, the control of IP policy through the GGSN is a network operator choice.

Figure 2 shows the scenario for control of an IP service using IP BS Managers in both possible locations in the UE and Gateway node. The figure also indicates the optional communication path between the IP BS Managers in the UE and the Gateway node.

**Policy Decision Function (PDF)** is a logical policy decision element which uses standard IP mechanisms to implement Service Based Local Policy (SBLP) in the IP bearer layer. These mechanisms may be conformant to, for example, the framework defined in IETF (RFC 2753 [7]) "A Framework for Policy-based Admission Control" where the PDF is effectively a Policy Decision Point (PDP). The PDF makes decisions in regard to SBLP using policy rules, and communicates these decisions to the IP BS Manager in the GGSN, which is the IP Policy Enforcement Point (PEP).

The interface between the PDF and the Application Function (AF) is the Gq interface specified in TS 23.002 [2].

The interface between the PDF and GGSN is specified within 3GPP, named Go interface, and is included in the Reference Architecture depicted in TS 23.002 [2]. The interface between the PDF and GGSN supports the transfer of information and policy decisions between the policy decision point and the IP BS Manager in the GGSN.

The PDF makes policy decisions based on information obtained from the AF. The PDF maps the policy set-up information received from the AF via the Gq interface into IP QoS parameters. The PDF is in the same domain as the GGSN. The AF may either be in the same domain as the PDF or may be in a different domain than the PDF. In the particular case of IMS, the AF is the P-CSCF which is in the same domain as the GGSN, as specified in TS 23.221 [20].

NOTE: Currently in IETF, inter-domain policy interactions are not defined.

**Application Function (AF)** offers services that require the control of IP bearer resources. The AF maps QoS-related application level parameters (e.g. SDP) into policy set-up information, and sends this information to the PDF via the Gq interface.

#### 5.1.1.2 (void)

#### 5.1.1.3 Interaction to External Networks

Within the UMTS network, there is resource management performed by various nodes in the admission control decision. The resources considered here are under the direct control of the UMTS network.

In IP Networks, it is also necessary to perform resource management to ensure that resources required for a service are available. Where the resources for the IP Bearer Service to be managed are not owned by the UMTS network, the resource management of those resources would be performed through an interaction between the UMTS network and that external network.

In addition, where the UMTS network is also using external IP network resources as part of the UMTS bearer service (for example for the backbone bearer service), it may also be necessary to interwork with that network.

The GGSN shall support DiffServ edge functionality. There are a number of other mechanisms provided to support interoperator interworking, some of which are given below.

NOTE: This list is not exhaustive. Other options are possible.

- Signalling along the flow path: In this scenario, resource requirements are explicitly requested and either granted or rejected through the exchange of signalling messages between network elements along the path of the IP packet flow. Signalling may be performed on a per-flow basis (e.g. using end to end RSVP) or it may be performed for an aggregate set of flows. In the latter case, it is expected that signalling exchanges would only be required when there are changes required in the resources allocated to an aggregate set of flows.
- Interaction between network management entities: In this scenario, resource requirements need to be explicitly negotiated and provisioned through network management entities. The results of this exchange are then enforced in the border nodes separating DiffServ administrative domains.
- Service Level Agreements enforced by the border routers between networks: In this scenario, resources are allocated along the path based on agreements between the network operators. The border routers along the path flow are provisioned with the characteristics of the aggregated traffic that is allowed to flow between systems.

#### 5.1.1.4 Translation/mapping function in the GGSN and the UE

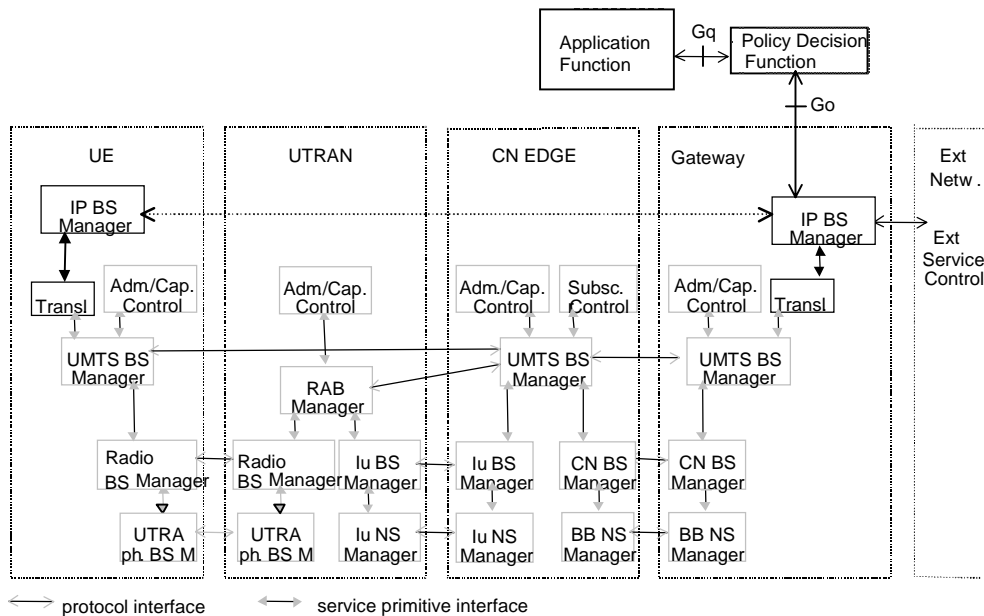
Translation/mapping function interacts with the IP BS Manager and with the UMTS BS Manager in the GGSN and in the UE. It provides interworking between the mechanisms and parameters used within the UMTS bearer service and those used within the IP bearer service.

For service-based local policy, the Translation/mapping function in the GGSN maps IP bearer based policy information into UMTS bearer based policy information. This mapping is used by the GGSN for service-based local policy over the UMTS network.

## 5.1.2 Allocation of QoS management functions

### 5.1.2.1 QoS management functions for end-to-end IP QoS

The QoS management functions for controlling the external IP bearer services and how they relate to the UMTS bearer service QoS management functions are shown in Figure 2.



**Figure 2: QoS management functions for UMTS bearer service in the control plane and QoS management functions for end-to-end IP QoS**

NOTE 1: The dimmed boxes in Figure 2 are clarified in TS 23.107 [3].

NOTE 2: The UE is only shown as a combined element, but it may also consist of a split TE/MT. Standardization of the interface and operation within a split UE is outside the scope of this TS.

## 5.2 Capabilities of Functional Elements

This section provides functional descriptions of capabilities in GGSN, UE, PDF, and AF.

### 5.2.1 GGSN

This clause provides functional descriptions of capabilities in GGSN. The capabilities are part of IP BS Manager (see 5.1.1.1) or corresponding user plane functions. Determination of exactly which functions are required to support interoperator and multi-vendor aspects are not addressed in this clause.

The **DiffServ Edge Function** shall be compliant to the IETF specifications for Differentiated Services (RFC 2475 [6]). The IETF Differentiated Services architecture will be used to provide QoS for the external bearer service.

Parameters for the DiffServ Edge Function (i.e. classifiers, meters, packet handling actions) may be statically configured on the GGSN, derived from PDP Context parameters and/or derived from RSVP signalling.

DiffServ functions configured on the basis of PDP Context parameters consist of marking user packets. The DSCP to be used is derived from the PDP Context parameters according to statically configured rules.

Statically configured DiffServ functions may include classifiers, meters, markers, droppers and shapers acting on uplink traffic.

The **Service-based Local Policy Enforcement Point** controls the quality of service that is provided to a combined set of IP flows. The policy enforcement function includes policy-based admission control that is applied to the bearer associated with the flows, and configuration of the policy based "gating" functionality in the user plane. Service-based local policy decisions are either "pushed" to or requested by the GGSN via the Go interface.

Policy-based admission control ensures that the resources that can be used by a particular set of IP flows are within the "authorized resources" specified via the Go interface. The authorized resources provide an upper bound on the resources that can be reserved or allocated for the set of IP flows. The authorized resources are expressed as a maximum authorised bandwidth and QoS class. The QoS class identifies a bearer service (which has a set of bearer service characteristics associated with it). The PDF generates a maximum authorized QoS class for the set of IP flows. This information is mapped by the **Translation/mapping function** in the GGSN to give the authorized resources for UMTS bearer admission control.

In the user plane, policy enforcement is defined in terms of a "gate" implemented in the GGSN. A gate is a policy enforcement function that interacts through Go interface with PDF as the Policy Decision Point for QoS resource authorisation at the IP BS level for a unidirectional flow of packets. Gate operations as defined in TS 23.228 [4] are to control and manage media flows based on policy, and are under the control of PDF. A gate operates on a unidirectional flow of packets, i.e., in either the upstream or downstream direction. A gate consists of a packet classifier, and a gate status (open/closed). When a gate is open, the packets in a flow are accepted, and are thus subject to the DiffServ edge treatment. When a gate is closed, all of the packets in the flow are dropped.

The gate shall be applied to the PDP contexts where SBLP applies, and for such PDP contexts the information received in the TFT is ignored. In the downlink direction, packets are processed against each gate in turn until a match is found. If a match is not found, packet processing shall then continue against filters installed from UE supplied TFTs for PDP contexts where SBLP is not applied according to specification TS 23.060 [19].

In the uplink direction, packets received on a PDP context with SBLP based filters shall be matched against those filters. If a match is found, the packet shall be passed if the gate associated with that filter is open processed according to the gate functions. If the gate is closed, or if the packet does not match any of the packet filters, the packet shall be silently discarded.

The packet classifier associated with a gate is a micro-flow classifier including the standard 5-tuple: (source IP address, destination IP address, source port, destination port, protocol), identifying a set of packets associated with a unidirectional flow.

Elements of the 5-tuple that cannot be derived from the SDP according to a set of rules shall be wild-carded.

The **Binding Mechanism Handling** associates the PDP context bearer with one or more IP flows in order to support service-based local policy enforcement. Binding information is included in PDP Context Activation or Modification messages to associate the PDP context bearer with SBLP policy decision information provided by the PDF associated with the IP flow(s). 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 an authorisation token and the flow identifier(s) related to the IP flow(s) within the same session. In order to allow SBLP policy information to be "pulled" from the PDF, the binding information shall allow the GGSN to determine the address of the PDF to be used. The GGSN shall forward the binding information received from the UE to the PDF. If multiple sets of binding information are received by the GGSN, it shall forward them to the PDF.

When binding information is received, the GGSN shall ignore any UE supplied TFT, and the filters in that TFT shall not be installed in the packet processing table. When sending the binding information to the network, the UE shall populate the TFT filters with wildcard values.

## 5.2.2 UE

This clause provides functional descriptions of capabilities in UE. The capabilities are part of IP BS Manager (see 5.1.1.1) or corresponding user plane functions. Determination of exactly which functions are required to support interoperator and multi-vendor aspects are not addressed in this clause.

**DiffServ Edge Function** acts as a DiffServ (DS) boundary for the traffic from applications running on the UE. As specified in RFC 2475 [6], DS boundary node must be able to apply the appropriate PHB to packets based on the DS code point. In addition, DS boundary nodes may be required to perform traffic conditioning functions. When GGSN DiffServ marking is used, the DiffServ edge function in the UE is not needed.

**RSVP/IntServ Function** provides the capability for the UE to request end-to-end QoS using RSVP messages as defined in IETF standards. RSVP messages may also be used by the network to inform the DSCP to be used by the UE. RSVP messages shall include the authorization token and flow identifier(s) in a policy data object if the authorization token is available in the UE. RSVP may be used to trigger PDP context activation/modification. The inter-working between MT and TE is FFS.

**Binding Mechanism** associates the PDP context bearer to the IP flow(s) to support SBLP policy enforcement in the GGSN. The binding information containing the authorization token and flow identifier(s) provides the binding mechanism, and is included by the UE in the PDP Context Activation and Modification messages. The UE may include one or more sets of the binding information. 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. The binding mechanism may also be used to bind a RSVP session with a SIP session by including the one or more sets of binding information in RSVP messages. The AF provides the authorization token to the UE during AF session set-up. E.g. for IMS services, the authorization token is provided to the UE by the P-CSCF during SIP session establishment.

For each bi-directional media flow, the UE shall ensure that the 64 bit IPv6 address prefix of the source address of outgoing packets is the same as the prefix of the destination address supplied for incoming packets.

### 5.2.3 PDF

This clause provides functional descriptions of capabilities in PDF. The PDF makes policy decisions based on policy set-up information obtained from the AF via the Gq interface.

#### Service-based Local Policy Decision Point

- The PDF shall check if the policy set-up information received from the AF is consistent with operator policy rules defined in the PDF.
- Authorize QoS resources (bandwidth, etc.) for the AF session. The PDF shall use the policy set-up information received from the AF to calculate the proper authorization. The authorization shall be expressed in terms of the IP resources to be authorized. The authorization shall include limits on QoS for the set of IP flows and restrictions on individual IP flows (e.g. destination address and port).
- In the filters supplied by the PDF for bi-directional flows, the source address prefix for downstream packets may be identified as the same as the destination address prefix for the upstream. Similarly, the source address prefix for the upstream packets may be identified as the same as the destination address prefix for the downstream.
- In case of IMS, the PDF shall be able to enforce the behaviour of the UE with respect to the assignment of IMS media components to the same PDP Context or to separate PDP Contexts. This behaviour of the UE is controlled by the AF (i.e. the P-CSCF) using the indications described in Section E.2.2.1 of TS 23.228 [4]. In case the UE violates this indication, and attempts to carry multiple IMS media components in a single PDP context despite of an indication that mandated separate PDP contexts, the PDF shall take care that such a PDP context would be rejected by the GGSN. To do so, the PDF uses the Go interface.
- The PDF shall be able to decide if new QoS authorization (bandwidth, etc.) is needed due to a mid-call media or codec change. A new authorization shall be required when the resources requested by the UE for a flow exceeds previous authorization, or a new flow is added, or when elements of the packet classifier(s) for authorized flows change.
- The PDF functions as a Policy Decision Point for the service-based local policy control.
- The PDF shall exchange the authorization information with the GGSN via the Go interface.
- PDF provides final policy decisions controlling the allocated QoS resources for the authorized media stream. The decision shall be transferred from the PDF to the GGSN.
- At AF session release, the PDF shall revoke the QoS resource authorization for the AF session.

#### Binding Mechanism Handling

- The PDF generates an authorization token for each AF session on request from the AF. The authorization token includes a fully qualified domain name of the PDF. The authorization token shall be unique across all PDP contexts associated with an APN. The authorization token conforms to the IETF specification on SIP Extensions for Media Authorization.

## 5.2.4 Application Function (AF)

The Application Function (AF) is an element offering applications that require the control of IP bearer resources (e.g. UMTS PS domain/GPRS domain resources). One example of an Application Function is the P-CSCF.

Service Based Local Policy related functions

- The AF shall use Gq interface to exchange service based policy set-up information with the PDF. This applies both during session establishment, as well as upon a mid-session modification effecting the media (e.g. addition of a new media in mid-session).
- The AF shall indicate to the PDF whether or not the PDF should contact the AF at UE resource reservation, even if policy set-up information is already available in the PDF.
- The AF shall indicate to the PDF whether or not the PDF may initiate a revoke of authorization.
- The AF shall indicate to the PDF whether or not the AF explicitly enables or disables the media.
- The AF shall indicate to the PDF whether or not the PDF shall forward bearer indications (e.g. bearer release indication).
- For bi-directional media flows, the AF, according to operator policy, may assume that the 64-bit IPv6 address prefix of the source address for downstream packets is the same as the prefix of the destination address for upstream packets of the same media flow. The implementation of this AF assumption would be determined by operator policy in order to reduce the possibilities of bearer misuse.

Binding Mechanism Handling

- The AF requests authorization token from the PDF. The following are possible:
  - 1) The AF requests a single authorization token. The PDF authorizes QoS resources usage for that application for a particular session and user. The authorization token is only valid for the duration of the session for the specific user.
  - 2) The PDF rejects the authorisation because the service information is not consistent with the operator policy rules defined in the PDF. No token is sent to the AF. The PDF shall also indicate in the authorisation reject the service information that could be accepted by the PDF.
- For AF sessions to and from the same UE, the AF(s) shall request authorization tokens from the same PDF.

NOTE: As a consequence, the GGSN will contact the same PDF for SBLP authorization for all AF sessions using the same PDP context.

The AF sends the authorization token to the UE in AF session signalling.

## 5.3 Go interface (PDF – GGSN)

### 5.3.1 Go Functional Requirements

The Go interface allows service-based local policy and QoS inter-working information to be "pushed" to or requested by the GGSN from a Policy Decision Function (PDF). The Go interface provides information to support the following functions in the GGSN:

- Control of service-based policy "gating" function in GGSN
- UMTS bearer authorization
- Charging correlation related function

The Common Open Policy Service (COPS) protocol supports a client/server interface between the Policy Enforcement Point in the GGSN and Policy Decision Function (PDF). The Go interface shall conform to the IETF COPS framework as a requirement and guideline for Stage 3 work.



The COPS protocol allows both push and pull operations. For the purpose of the initial authorisation of QoS resources the pull operation shall be used. Subsequently the interactions between the PDF and the GGSN may use either pull or push operations.

Policy decisions may be stored by the COPS client in a local policy decision point allowing the GGSN to make admission control decisions without requiring additional interaction with the PDF.

### 5.3.2 Information Exchanged via Go Interface

The COPS protocol supports several messages between a client and server.

Additional 3GPP Go-specific information elements must be included in COPS messages to support the SBLP control functions identified in Section 5.3.1. Consistent with the COPS framework, the Go interface is identified by a "client type" allocated for a 3GPP Go COPS client (GGSN).

All of the information described in the remainder of this section applies specifically to the 3GPP Go COPS client type. The events specific to the UMTS or IP bearer service would trigger the request messages from the GGSN PEP to the PDF. The information elements specific to UMTS would be standardized and carried in the 3GPP Go specific interactions between the PDF and the GGSN.

A **Request** (REQ) message from the GGSN to the PDF shall allow the GGSN to request SBLP policy information for a set of IP flows identified by one or more sets of binding information (described below).

Each set of binding information associates the PDP context to the IP flow(s) of an AF session, and is used by the GGSN to request SBLP policy information from the PDF. Each set of binding information includes 1) an authorization token sent by the AF to the UE during AF session signalling, and 2) one or more flow identifiers used by the UE, GGSN and PDF to uniquely identify the IP media flow(s) within the same session.

The authorization token shall be unique within the scope of the operator's domain. The authorization token conforms to relevant IETF standards on SIP Extensions for Media Authorization.

A flow identifier identifies an IP media flow associated with the SIP session. Flow identifiers are based on the ordering of media components (media description structure defined by a single 'm=' line), and port numbers within that media component in the SDP. A flow identifier combined with the authorization token shall be sufficient to uniquely identify an IP media flow.

A **Decision** (DEC) message from the PDF to the GGSN contains decision objects. A Decision object shall include one of the following commands:

- Install (Admit request/Install configuration, Commit)
- Remove (Remove request/Remove configuration)

These commands are used to:

- Authorize QoS/Revoke QoS authorization for one or more IP flows
- Control forwarding for one or more IP flows

The **responses** from the PEP to the PDF include an acknowledgement and/or an error response to commands received by the PEP. The following response messages shall be supported:

- Report State (Success/Failure/Accounting) (RPT)

The **Delete Request State (DRQ)** message from the PEP to the PDF indicates that the request state of a previously authorised bearer resource is no longer available/relevant at the GGSN so the corresponding COPS policy state shall likewise be removed at the PDF. The DRQ message includes the reason why the request state was deleted.

The Install command used to Authorize QoS contains the following policy information associated with the IP flow(s):

- Packet classifier(s)
- Authorized QoS information
- Packet handling action

- Charging information (ICID in case of IMS)

The packet classifier includes the standard 5-tuple: (source IP address, destination IP address, source port, destination port, protocol), identifying a set of packets associated with a unidirectional flow. Elements of the 5-tuple may be wildcarded.

The authorized QoS information provides an upper bound on the resources that can be reserved or allocated for the combined set of IP flows. The authorized QoS information shall contain the DiffServ class and Data rate parameter. The DiffServ class is used only to identify the maximum allowed traffic class.

NOTE: Further elements and details of the authorized QoS information are defined in TS 29.207 [4a].

The packet handling action defines the packet handling that should be accorded to packets matching the packet classifier. The packet handling action (gate status) shall result in packets being passed (gate open), or silently discarded (gate closed).

Charging information (ICID) allows the GGSN to be aware of the IMS\_session level charging identifier of the IMS session that the Install command relates to. The PDF shall send the ICID provided by the P-CSCF as part of the authorisation (Install) decision.

The Report State contains the following information:

- Charging correlation information

Charging correlation information contains information used to correlate usage records (e.g. CDRs) of the GGSN with AF session records from the AF. For this purpose, the GGSN shall send the GCID of the PDP context and the GGSN address to the PDF as part of the authorisation report (RPT).

The messages which revoke QoS authorisation or remove configuration information provide only the information that is needed to perform the action (e.g., the COPS handle element, which is used as a way of identifying the installed decision information).

## 5.3a Gq Interface (PDF - AF)

### 5.3a.1 Gq Functional Requirements

The Gq interface is used for service-based policy set-up information exchange between the Policy Decision Function (PDF) and the Application Function (AF). This information is used by the PDF for service based local policy decisions.

The Gq interface allows service based QoS information needed for QoS authorisation to be exchanged between the AF and the PDF.

One PDF shall be able to serve more than one Application Function and one given AF may interact with a number of PDFs. On a per-AF-session basis, the AF shall interact with only a single PDF.

### 5.3a.2 Information Exchanged via Gq interface

#### Service information:

The AF provides the following service information to the PDF to be used as a basis for the service-based local policy decisions.

- a) Description of session: the AF may provide one or more of the following information when describing the session (the set of information that needs to be sent in different cases depends on the service for which the media authorisation is required):
  - Application identifier: identifies the particular service that the session belongs to. This information may be used by the PDF to differentiate QoS for different application services. For example application identifier may be used as additional information together with the indication of the type of service information when QoS class for the bearer authorisation in Gq interface is decided. The application identifier may be used also to complete the QoS authorisation with application specific default settings in the PDF if the AF does not provide all or any of the following information.

- Information defining the media stream
  - Media stream Id (to uniquely identify the media stream within the session)
  - Information defining the IP flows of the media stream.
    - direction (bi-directional, uplink / downlink)
    - 5-tuple (source/destination address and port number, protocol Id)
    - indication of the maximum and/or mean bandwidth required
  - An indication of the requested type of service information per service-flow, e.g., conversational voice or video, streaming voice or video
- b) Resource Reservation Policy: Definition of whether PDF shall contact the AF at resource reservation during the session even if policy set-up information is already available in the PDF.
- c) Media Control Policy: Definition of whether explicit AF media control is used or not in the session. If explicit AF media control is not used, the AF does not explicitly enable or disable the media. At bearer authorization the PDF shall install the gates in the GGSN and derive their state (open/close) based on the information defining the media stream.
- d) Revoke Policy: Definition of whether the PDF itself may initiate a revoke of authorization.
- e) Indication Forwarding Policy: Definition of whether the PDF shall forward bearer indications (e.g. bearer release indication).

**Authorisation token:**

The PDF generates Authorisation token on request from the AF. The Authorization token contains the fully qualified domain name of the PDF and a reference in the PDF, which allows the PDF to uniquely identify the AF session.

**Charging correlation related information:**

The AF and PDF may exchange charging correlation related information. The AF charging identifier (e.g. ICID in case of IMS), if available, shall be transferred from the AF to the PDF, which shall forward it to the GGSN. GPRS charging identifier, if available in the PDF, shall be transferred to the AF.

**Media control commands:**

If explicit media control is used the AF instructs the PDF when a media is to be enabled or disabled to pass through the access network. The command contains information referencing the media and its required status (enabled/disabled). The PDF opens or closes the corresponding gate(s) in the GGSN based on this command. The PDF shall respond with the result of the operation to the AF.

**Bearer reservation indication:**

The PDF shall send bearer reservation indication to the AF to indicate that the bearer resources have been reserved, if the AF in the initial authorisation request had requested it.

**Bearer release indication:**

Information available at the PDF on the bearer resource release is forwarded to the AF. The indication may contain information about the reason of the release.

**Bearer modification indication:**

Information available at the PDF on the bearer modification is forwarded to the AF. The indication shall contain information about the type of modification, i.e. modification to 0 kbit/s or from 0 kbit/s to a value within the previously authorized range.

**Revoke authorisation command:**

The AF determines when an authorization token and all related authorizations need to be removed e.g. due to the AF session release, and shall instruct the PDF to remove the authorizations and to enforce the removal of the resources

previously authorised for the AF session. The revoke authorisation command may contain information about the reason of the revoking.

## 5.4 QoS Parameters

See stage 3 specification TS 29.207 [4a].

## 5.5 QoS Parameter Mapping

See stage 3 specification TS 29.208 [4b].

---

# 6 End-to-End QoS Procedures

## 6.1 QoS Procedures in Functional Elements

This section describes the main procedures that are used for the end-to-end QoS management. These procedures are described in text description for each involved network elements. The procedures described in this document are meant to provide a high level description for further Stage 3 work and are not intended to be exhaustive.

### 6.1.1 Procedures in the GGSN

The QoS procedures in the GGSN are triggered by the QoS signalling messages from the UE, i.e., PDP Context Activation message or the RSVP messages. The exact QoS procedures in the GGSN depend on the GGSN and UE QoS capabilities. The GGSN is required to support DiffServ edge function. Other QoS capabilities that may be supported at the GGSN are RSVP functions and service-based local policy enforcement functions.

For UEs that do not support RSVP, the GGSN may use the PDP context level information to configure the DiffServ edge functionality and provide internetworking between PDP context and backbone IP network. The authorization token is included in the PDP context activation/modification messages.

For UEs that support RSVP, the GGSN may also support RSVP and use RSVP rather than the PDP context to control the QoS through the backbone IP network. The authorization token may be included in the RSVP signalling and the PDP context activation/modification messages. Alternatively, the RSVP messages may pass transparently through the GGSN.

If SBLP is implemented in the operator's network, the GGSN shall authorize the PDP context activation/modification messages that are subject to service based local policy by sending an authorization request to the PDF. Alternatively, the GGSN may authorize PDP context activation/modification messages that are subject to service based local policy using the cached policy in the Local Decision Point. The GGSN shall map the received IP flow based policy information into PDP context based policy information.

If SBLP is implemented in the operator's network, the GGSN shall nonetheless allow the activation/modification of at least one non-realtime PDP context per UE IP address and per APN (PDP Context with UMTS Traffic class "background" or "interactive") without a Media Authorization Token.

Note: The requirement above makes it possible for the UE to activate/modify at least one non-realtime PDP Context on each APN (with UMTS traffic class "background" or "interactive") without including the Media Authorization Token to the activation/modification message.

### 6.1.2 Procedures in the UE

The QoS procedures in the UE are triggered by the application layer (e.g., SIP/SDP) QoS requirements. The exact QoS procedures in the UE depend on the UE QoS capabilities.

For UEs that support only UMTS QoS mechanism, the application QoS requirements will trigger a PDP Context Activation procedure with the corresponding UMTS QoS parameters. For UEs that support both IP (e.g., IP BS Manager) and UMTS QoS mechanism, the application QoS requirements are mapped down to the IP layer QoS

parameters. The IP layer parameters are further mapped down to the PDP context parameters in the UE. For UEs that support RSVP, the application QoS requirements are mapped down to create an RSVP session. The UE shall establish a PDP context suitable for support of the RSVP session.

In addition in the case of IMS, the following procedures apply: if the UE received the Media Authorization Token in the SIP signalling, the UE shall include the Media Authorization Token in the PDP Context Activation request for the PDP Context(s) that are activated upon IMS session establishment to carry the media flows of the IMS session. In case the UE carries media flows from different AF sessions in the same PDP Context, the UE shall include the Media Authorization Tokens of all these AF sessions in the PDP Context Activation/Modification request.

Note: This also implies that if the UE initiates a new AF session and intends to carry media of this AF session in an already activated PDP context that carries media from other AF session(s), then the UE initiates a PDP Context Modification request and includes all authorization tokens of all AF sessions that use this PDP Context in this request.

It shall be possible for the UE to carry media flow(s) of an AF session in the non-realtime PDP Context that has already been established without a Media Authorization Token and matches the QoS requirements of the media flow(s). In this case, the Media Authorization Token received by the UE in AF session signalling will not be used, as no PDP Context with Media Authorization Token is required.

Note: Such a usage of an already activated non-realtime PDP Context is assumed to be applied only for non-realtime AF session media (e.g. for IMS session-based messaging), or for any AF session to provide a possibility for the transfer of early media (e.g. for PoC) until the PDP contexts with authorization token have been established.

For UEs that support RSVP, if the UE received the Media Authorization Token in AF session signalling, the UE shall include the Media Authorization Token in both the PDP Context Activation request for the PDP Context(s) that are activated to carry the media flows of the AF session, and the RSVP messages if the PDP Context/RSVP is associated to the session.

At the AF session release, the UE shall release all QoS resources allocated for the AF session.

NOTE: Service Based Local Policy may restrict the destination of packets to the addresses/ports included in the AF session signalling. Mechanisms such as MIPv6 Route Optimisation which send packets to other addresses/ports may therefore not operate correctly.

### 6.1.3 Procedures in the PDF

In case of applying Service based local policy:

The QoS procedures in the PDF are related to service based local policy control.

The authorize QoS resources procedure can be invoked between the PDF and the AF at AF session establishment and/or at bearer establishment. When the AF requests Authorization-Token from the PDF, it indicates whether or not the PDF should contact the AF at UE resource reservation. The Authorization-Token is generated by the PDF and sent to the AF.

When the PDF received service information from the AF, the PDF shall authorize the QoS resources if they are consistent with the operator policy rules defined in the PDF, and stores the SBLP for the AF session based on the service information received from the AF. If the service information received from the AF is not consistent with the operator policy rules defined in the PDF, the PDF shall reject the authorisation request. The PDF shall indicate in the response to the AF the service information that could be accepted by the PDF.

Upon receiving the bearer authorization request from the GGSN, the PDF shall authorize the request according to the stored SBLP for the session. The PDF shall send aggregate decisions (i.e. decisions for all media flows pertaining to the same authorization request) to the GGSN, i.e. when one session is modified, the PDF shall send an authorization decision comprising all media flows carried by the PDP context that is being authorized.

As part of the authorization, the PDF shall perform the mapping from the service information conveyed over the Gq interface to the Authorized QoS sent over the Go interface.

The PDF makes a final decision to enable the allocated QoS resource for the authorized IP flows. This may be triggered by an instruction from the AF. QoS resources may also be enabled at the time they are authorised by the PDF.

When the AF receives updated session description information, the AF may send an update for service information to the PDF. The PDF shall be able to decide if a new QoS authorization is needed and shall update the authorization for the session accordingly if the service information is consistent with the operator policy rules defined in the PDF. The PDF shall not send an updated decision to the GGSN when the AF indicates that a new media component is added. The PDF may send an updated decision to the GGSN when the new authorization exceeds the resources requested by the UE for a flow. The PDF shall send an updated decision to the GGSN when elements of the packet classifier(s) for an authorized flow are changed. The PDF shall enforce a removal of a media component.

If the service information received from the AF is not consistent with the operator policy rules defined in the PDF, the PDF shall reject the update for service information. The PDF shall indicate in the response to the AF the service information that could be accepted by the PDF.

The PDF shall revoke the resource authorization based on request from the AF.

## 6.1.4 Procedures in the AF

The authorize QoS resources procedure is triggered by the AF when it receives an AF session signalling message initiating a new AF session. Upon the authorize QoS procedure:

- The AF shall request one authorization token for the AF session from the PDF in the initial authorisation request. For AF sessions to and from the same UE, the AF(s) shall request authorization tokens from the same PDF.

NOTE: This also implies that if different AF sessions of a user are controlled by different AFs, then all these AFs will request authorization tokens from the same PDF. Hence, the bearer authorization of the PDP Context(s) carrying the media of these AF sessions will be performed by the same PDF.

- If the AF indicates to the PDF that it wishes to be contacted upon bearer resource reservation, the service information shall be passed during the Gq interaction upon bearer resource reservation. Alternatively, if the initial AF session signalling message contains session description information, such as the end-point addresses, bandwidth requirements and the characteristics of the media exchange, the AF shall forward this information to the PDF as part of the service information at the same time with the authorisation token request.
- The AF generates the information (e.g. service information) conveyed over the Gq interface from the application specific media description (e.g. SDP media description).
- The PDF shall use the service information for the QoS policy set up for the AF session. During an AF session change, the AF shall send an update for service information to the PDF based on the new session description information exchanged within AF session signalling.

The AF orders the PDF to enable or disable a media to pass through the access network. The AF shall be able to send an instruction for the PDF to wait for the Approval of QoS Commit procedure or to enable the media as part of the authorization of the bearer establishment for the media. The AF may use Removal of QoS commit procedure to disable the media e.g. when a media component of an AF session is put on hold.

At AF session release, the AF shall send an instruction to the PDF to revoke the resource authorization.

## 6.2 IP Bearer Level / Application Level Binding Mechanism

The *binding mechanism* associates the PDP context bearer with policy information in the GGSN to support service based local policy enforcement. The SBLP policy decision information in the GGSN is based on IP media flows. The binding mechanism identifies the IP media flow(s) associated with a PDP context bearer and uses this information in selecting the policy information to apply.

The UE shall be able to include one or more sets of binding information in PDP Context Activation and Modification messages to associate the PDP context bearer with policy information. Each set of binding information includes 1) an Authorization Token sent by the AF to the UE during AF session signalling, and 2) one or more Flow Identifiers which are used by the UE, GGSN and PDF to uniquely identify the IP media flow(s) within the same session.

The authorization token shall be unique within the scope of the operator's domain. The authorization token conforms to relevant IETF standards.

A Flow Identifier identifies an IP media flow associated with the SIP session. Flow Identifiers are based on the sequence of media components (media description structure defined by a single 'm=' line) in the SDP, and IP flow numbers (defined in the order of increasing port numbers) within each media component.

A flow identifier combined with the authorization token shall be sufficient to uniquely identify an IP media flow.

In order to allow SBLP policy information to be "pulled" from the PDF, the authorization token shall allow the GGSN to determine the address of the PDF to be used.

## 6.3 Session Flow: QoS Interaction Procedures

This section highlights possible additions to the GPRS bearer establishment procedures specified in TS 23.060 [19] for support of Service Based Local Policy. It describes the QoS interactions involved within the sub-procedure blocks for Authorize QoS Resources, Resource Reservation with Service-based Local Policy, Enable Media, Disable Media, Revoke Authorization for GPRS and IP Resources, Indication of PDP Context Release, Authorization of PDP Context Modification and Indication of PDP Context Modification. These procedures are utilized to provide Service based Local Policy for session-based services, e.g. for IMS as described in Chapter 5: 'IP multimedia subsystem procedures' of TS 23.228 [4].

For IMS where Service-based Local Policy is not used, the Authorize QoS Resources, the Resource Reservation with Service-based Local Policy, the Enable Media, the Disable Media, Revoke Authorization for GPRS and IP Resources, the Indication of PDP Context Release, the Authorization of PDP Context Modification and the Indication of PDP Context Modification sub-procedure blocks defined in TS 23.228 [4] are not applied.

The possible additions refer to procedures on the use of Service-based Local Policy, and RSVP Signalling as well as the allowed combinations.

It shall be possible according to operator choice to use solely the GPRS bearer establishment procedures specified in TS 23.060 [19] without the additions described in this section.

For the flow sequences involving Authorize QoS Resources and Approval of QoS Commit, the following are assumed:

- the successful authorization of QoS resources.
- the successful approval of QoS commit.

NOTE: 'Activate (Secondary) PDP Context' here means that either Primary or Secondary PDP context may be activated.

NOTE: When necessary, it is assumed that there is an existing PDP context that carries signalling (e.g., RSVP) between the UE and GGSN.

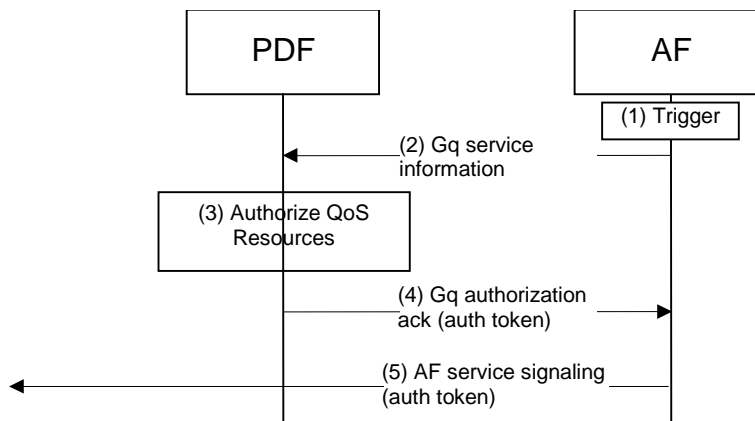
### 6.3.1 Authorize QoS Resources, AF session establishment

The Authorize QoS Resources upon AF session establishment procedure is triggered by a session establishment event in the AF (e.g. the AF receiving an AF session signalling message containing session description information (e.g. SDP)). The session description negotiation between AF session endpoints contains information about the session, such as the end-points, bandwidth requirements, and the characteristics of the media exchange.

Note: The exact type and amount of session description information exchanged between AF session endpoints depend on the nature of the session and the application.

The PDF shall authorize the required QoS resources for the session and install the IP bearer level policy based on service information received from the AF.

The following figure is applicable to both sides (i.e. originating and terminating) of the AF session.



**Figure 3: Authorize QoS Resources, AF session establishment**

- 1) An AF session signalling message is received at or generated by the AF, or an internal action at the AF triggers the need for an authorization request.
- 2) The Application Function sends a request for authorization token to the PDF with service information, which may include session description information based on the AF session signalling. Some services may require further interaction between the AF and the PDF to provide the full service information, e.g. for IMS session establishment (mobile terminated).
- 3) If the PDF has received AF session description in the service information in Step 2, the PDF shall authorize the required QoS resources for the AF session if the session description is consistent with the operator policy rules defined in the PDF, and install the IP bearer level policy based on information received from the AF. If the service information was not received in Step 2 above, the QoS authorisation is deferred. The PDF generates an authorization token for the AF session.
- 4) The PDF sends the authorisation token to the AF.
- 5) The AF forwards the AF session signalling message containing the session description. The AF shall include the authorization token in this AF session signalling message.

## 6.3.2 Resource Reservation Message Flows

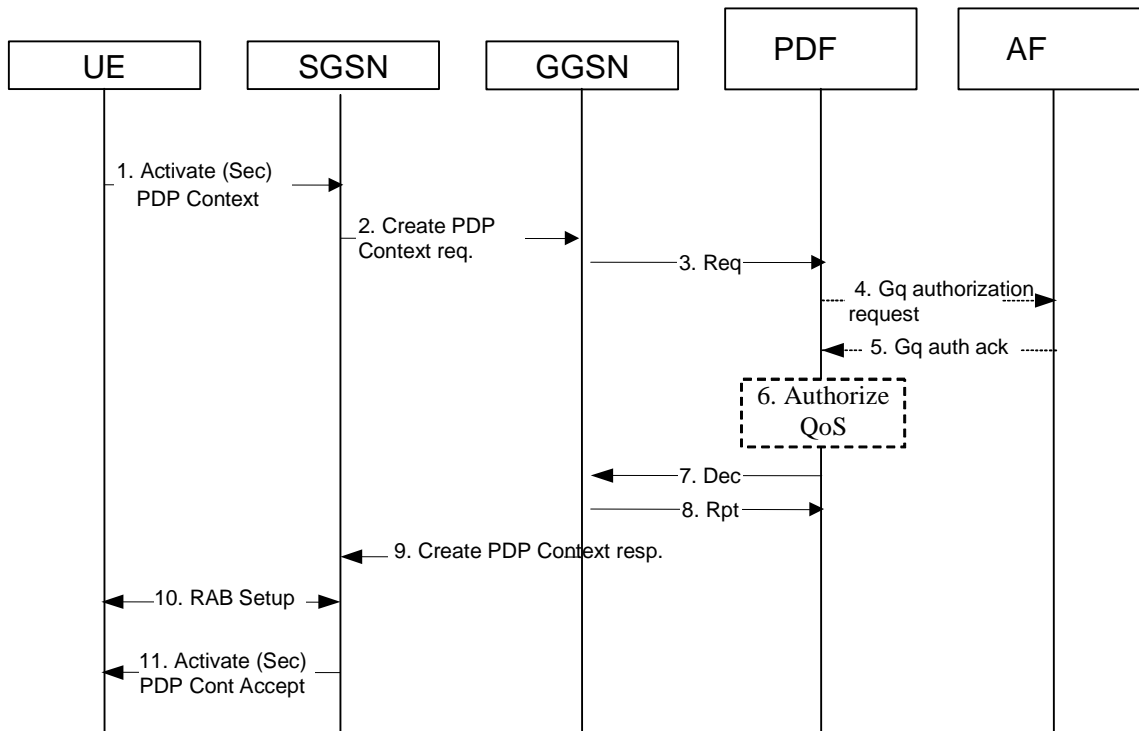
### 6.3.2.1 Resource Reservation with Service-based Local Policy

For this case, Service-based Local Policy is added to the GPRS bearer establishment procedures specified in TS 23.060 [19].

This section provides the flows for bearer establishment, resource reservation and policy control with PDP Context setup and DiffServ inter-working.

The following figure is applicable to both the Mobile Originating (MO) side and the Mobile Terminating (MT) side.





**Figure 4: Resource Reservation with Service-based Local Policy**

- 1) The UE sends an Activate (Secondary) PDP Context message to the SGSN with the UMTS QoS parameters. The UE includes the Binding Information in the Activate PDP Context message.
- 2) The SGSN sends the corresponding Create PDP Context message to the GGSN.
- 3) The GGSN sends a COPS REQ message with the Binding Information to the PDF in order to obtain relevant policy information.
- 4) A PDF generated authorization token enables the PDF to identify the authorisation status information. If the previous PDF interaction with that AF had requested this, or if the previous interaction with the AF did not include service information, the PDF sends an authorisation request to that Application Function.
- 5) The AF sends the service information to the PDF.
- 6) The PDF shall authorize the required QoS resources for the AF session if the session description is consistent with the operator policy rules defined in the PDF, and install the IP bearer level policy in its internal database. This is based on information from the Application Function.
- 7) The PDF sends a COPS DEC message back to the GGSN.
- 8) The GGSN sends a COPS RPT message back to the PDF, which may also trigger a report message to be sent from the PDF to the AF.
- 9) The GGSN maps IP flow based policy information into PDP context based policy information and uses the PDP context based policy information to accept the PDP activation request, and sends a Create PDP Context Response message back to SGSN.
- 10) RAB setup is done by the RAB Assignment procedure.
- 11) The SGSN sends an Activate (Secondary) PDP Context Accept message to UE.

### 6.3.2.2 Resource Reservation with IP QoS signalling

*Editor's note: There is still ongoing work in IETF on new IP QoS signalling techniques, hence it is not possible to include flows using those new techniques into this version of the specification. Procedures describing resource reservation with end-to-end RSVP are described in Annex X.*

### 6.3.2.3 Resource Reservation with IP QoS reservation signalling and Service-based Local Policy

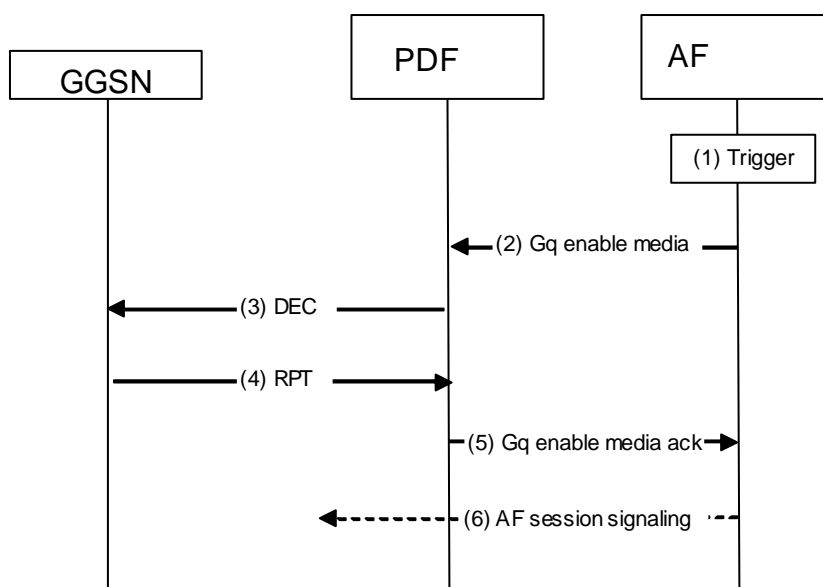
*Editor's note: There is still ongoing work in IETF on new IP QoS signalling techniques, hence it is not possible to include flows using those new techniques into this version of the specification. Procedures describing resource reservation with end-to-end RSVP and Service-based Local Policy are described in Annex X.*

### 6.3.2.4 (void)

## 6.3.3 Enable Media procedure

The 'Enable media' procedure is triggered by an AF session signalling message received at the AF, or an internal action at the AF (e.g. in IMS this is triggered by the P-CSCF receiving the 200 OK response to the INVITE request). The 'Enable media' procedure is optional and is only needed if the AF ordered the PDF to wait for the Approval of QoS Commit procedure to enable the media.

The following figure is applicable to both the Mobile Originating (MO) side and the Mobile Terminating (MT) side.



**Figure 11: Enable media procedure**

- 1) An AF session signalling message is received at the AF, or an internal action at the AF triggers the need to enable the media for the application. In IMS this is triggered by the P-CSCF receiving the 200 OK response to the INVITE request.
- 2) The Application Function sends an enable media indication to the PDF.
- 3) The PDF shall send a COPS DEC message to the GGSN to open the 'gate' e.g., enable the use of the authorised QoS resources, unless this was done based on local policy at the time the QoS resources were authorised.
- 4) The GGSN receives the COPS DEC message and opens the 'gate' e.g., enables the use of the authorised QoS resources, and sends a COPS RPT message back to the PDF.
- 5) The PDF reports the successful enable media operation to the Application Function.

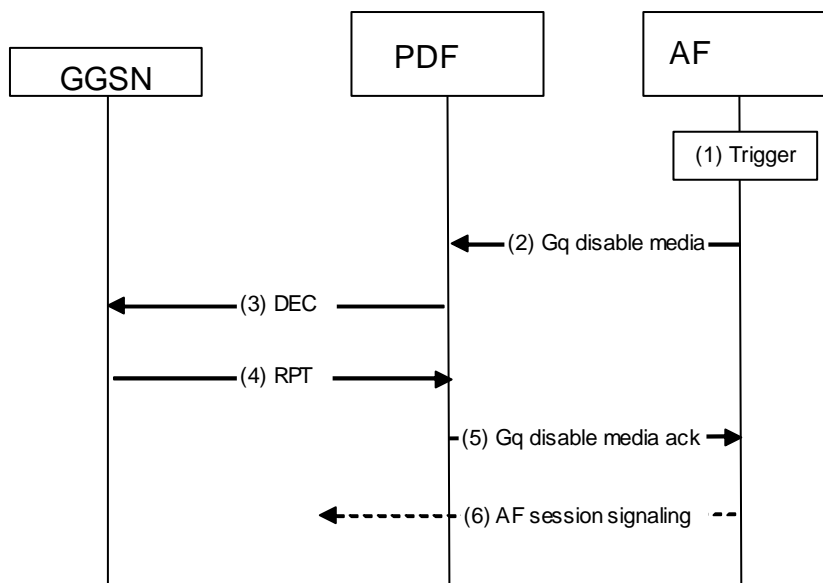
- 6) The AF session signalling message may occur in case required by the AF session procedures.  
 In IMS, the P-CSCF forwards the 200 OK message to the UE for the originating side. For the terminating side, the P-CSCF forwards the SDP message to the terminating S-CSCF.

### 6.3.4 Disable Media procedure

The 'Disable Media' procedure is used e.g. when a media component of an AF session needs to be disabled (e.g. in case of IMS a media re-negotiation or call hold). The PDF provides final decision on removal of QoS commit for the authorized media stream to the GGSN. 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" and "Resource Reservation with Service-based Local Policy" request.

The GGSN closes the gate, and the media flow will be blocked.

The following figure presents the "Removal of QoS commit" procedure.



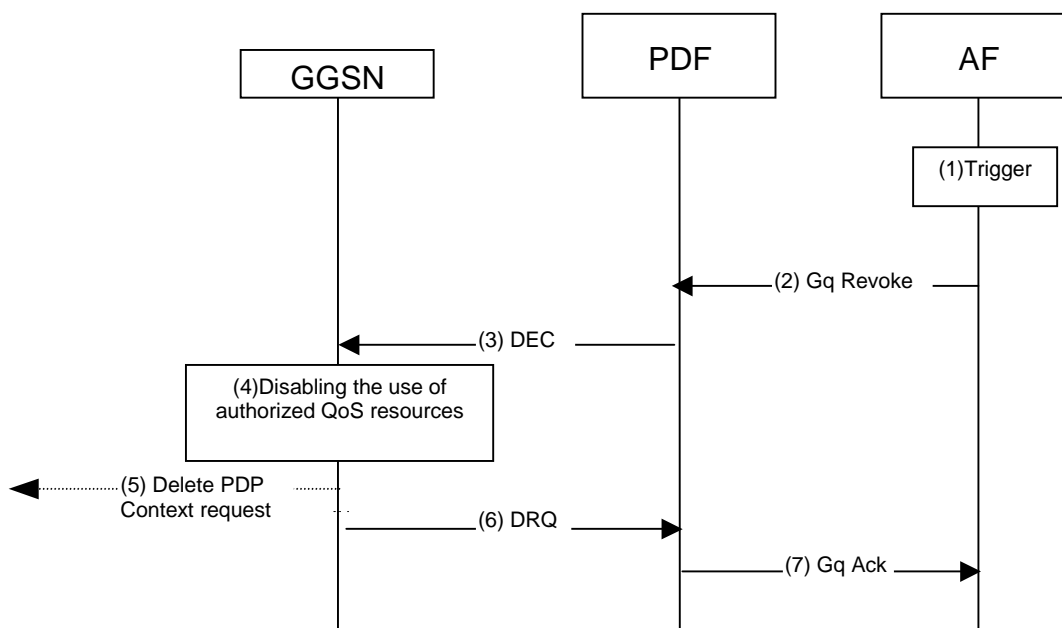
**Figure 12: Disable media procedure**

- 1) An AF session signalling message is received at the AF, or an internal action at the AF triggers the need to disable the media for the application. In IMS this is triggered by a SIP message exchanges for e.g., putting a media flow on hold.
- 2) The Application Function sends a disable media indication to the PDF.
- 3) The PDF shall send a COPS DEC message to the GGSN to close the 'gate'.
- 4) The GGSN receives the COPS DEC message, closes the gate, and sends a COPS RPT message back to the PDF.
- 5) The PDF reports the successful disable media operation to the Application Function.
- 6) The AF session signalling message may occur in case required by the AF session procedures.

### 6.3.5 Revoke Authorization for GPRS and IP Resources

The "Revoke Authorization for GPRS and IP resources" procedure is used when AF session signalling releases the AF session, e.g. upon IMS session release. The PDF decision of "Revoke Authorization for GPRS and IP Resources" shall be sent as a separate decision to the GGSN corresponding to the previous "Authorize QoS Resources" and "Resource Reservation with Service-based Local Policy" request.

The following figure presents the "Revoke Authorization for GPRS and IP Resources" procedure. This procedure is applied for user plane PDP context(s).



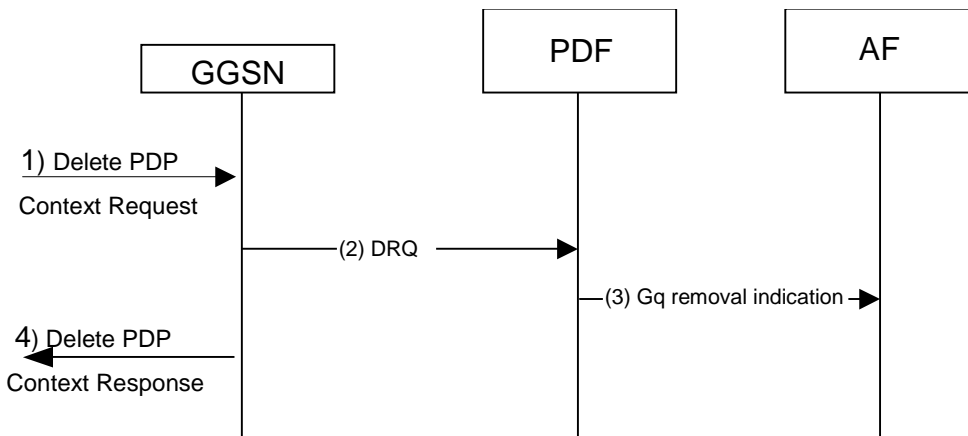
**Figure 13: Revoke Authorization for GPRS and IP Resources**

- 1) AF session signalling message exchanges for e.g. AF session release or internal action at the AF triggers the need to revoke the authorization.
- 2) The Application Function sends a message to the PDF to indicate the revocation.
- 3) The PDF shall send a COPS DEC (Decision) message containing revoke command to the GGSN.
- 4) The GGSN receives the COPS DEC message, and disables the use of the authorized QoS resources.
- 5) The GGSN initiates deactivation of the PDP context used for the AF session, in case the UE has not done it before.
- 6) Upon deactivation of the PDP Context, the GGSN sends a COPS DRQ (Delete Request State) message back to the PDF.
- 7) The PDF indicates the successful execution of the revoke indication.

### 6.3.6 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.

The following figure presents the "Indication of PDP Context Release" procedure.

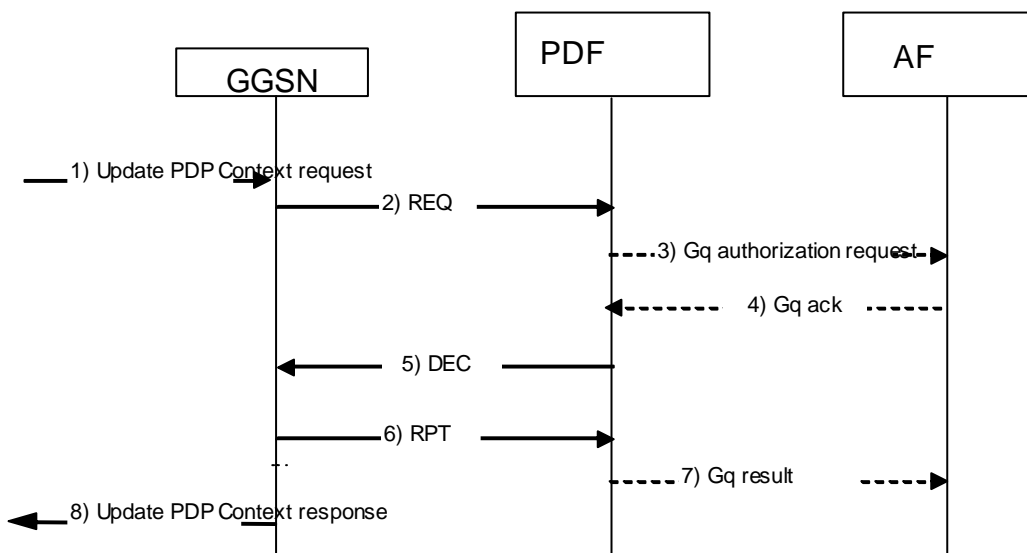


**Figure 14: Indication of PDP Context Release**

- 1) The GGSN receives a Delete PDP Context request for the PDP context related to the media flow.
- 2) The GGSN sends a COPS DRQ message to the PDF.
- 3) The PDF indicates the bearer removal to the AF.
- 4) The GGSN sends the Delete PDP Context Response message to the SGSN to acknowledge the PDP context deletion.

### 6.3.6a Authorization of PDP Context Modification

The "Authorization of PDP Context Modification" 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 new binding information is received. In this case, the GGSN communicates with the PDF as described below. The following figures present the "Authorization of PDP Context Modification" procedure.



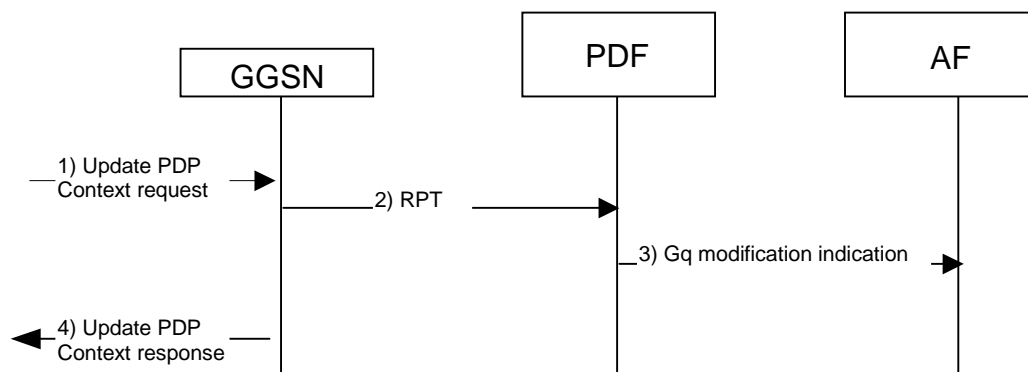
**Figure 14a: Authorization of PDP Context Modification**

- 1) A request to modify the PDP context related to the media flow is indicated by sending the Update PDP Context Request message to the GGSN.
- 2) The GGSN sends a COPS REQ message to the PDF. If the GGSN has sufficient information to authorize this PDP context modification request, then the GGSN does not send a COPS REQ message to the PDF.

- 3) The PDF may send an authorization request to the Application Function. This may be the case if this was requested from the AF at initial authorisation, and if PDF requires more information from the AF before authorising the network resources modification.
- 4) The AF shall send service information for authorization of the bearer modification.
- 5) The PDF receives the COPS REQ message, notes the requested modification and informs the GGSN of the authorization decision.
- 6) The GGSN sends a COPS RPT message back to the PDF.
- 7) In case the PDF had contacted the AF in step 3), then the successful installation of the decision is reported to the AF.
- 8) If the PDF accepted the modification, the GGSN sends the Update PDP Context Response message to the SGSN to acknowledge the PDP context modification.

### 6.3.7 Indication of PDP Context Modification

The "Indication of PDP Context Modification" procedure is used when a PDP Context is modified such that the maximum bit rate (downlink and uplink) is downgraded to 0 kbit/s or changed from 0 kbit/s to a value that falls within the limits that were authorized at PDP context activation(or last modification). In this case, the GGSN communicates with the PDF as described below. The following figures present the "Indication of PDP Context Modification" procedure.

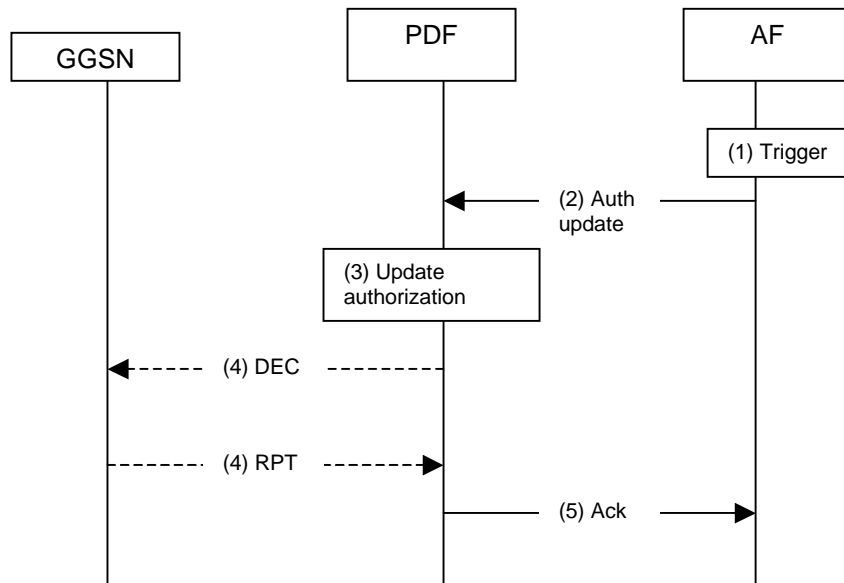


**Figure 15: Indication of PDP Context Modification**

- 1) A request to modify the PDP context related to the media flow is indicated by sending the Update PDP Context Request message to the GGSN.
- 2) The GGSN sends a COPS RPT message to the PDF to indicate the state changes of the PDP context.
- 3) If this state change matches the criteria for which that the AF had requested to be informed, the PDF shall give a bearer modification indication to the Application Function.
- 3) The GGSN sends the Update PDP Context Response message to the SGSN to acknowledge the PDP context modification.

### 6.3.8 Update Authorization procedure

When a session is modified, an update for a previous authorization of the session may be given to the PDF and possibly to the GGSN. Figure 16 below presents the "Update Authorization" procedure.



**Figure 16: Update Authorization for the session**

1. The AF is triggered to give updated service information to the PDF (e.g. as a result of the modification of the session at session control level).
2. The AF gives the updated service information to the PDF.
3. The PDF updates the authorization for the session if the session description is consistent with the operator policy rules defined in the PDF. In case the session modification requires enhancing the reserved resources, the PDF may decide not to send an updated decision authorizing the enhanced QoS to the GGSN, but would rather wait for a new authorization request from the GGSN.
4. In case the session modification affects the authorized resources, the PDF sends a COPS DEC message to the GGSN to enforce authorization according to the session modification. The GGSN updates the authorization. If the QoS of the PDP context exceeds the updated authorized 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 authorized level. The GGSN sends a COPS RPT message back to the PDF.
5. The PDF sends an acknowledgement to the AF.

## 6.4 PDP Context Used for Application Level Signalling Transport

To establish a PDP context for application level signalling, the UE shall be able to include a signalling flag in PDP context activation procedure. This indicates to the network the intention of using the PDP context for application level signalling. The only defined application level signalling flag in this release is the IM CN subsystem signalling flag. However, the network may also support other mechanisms that cater for identifying application level signalling flows within a PDP context, as described in TS 23.228 [4] section 4.2.6.

To establish a PDP context for application level signalling with prioritised handling over the radio interface, the UE shall be able to set the Signalling Indication in the QoS IE in the PDP context activation procedure. The Signalling indication in the QoS IE indicates to the radio and core networks the requirement for enhanced handling over the radio interface, once it has been negotiated with the networks.

A request for a general purpose PDP context having the "signalling indication" within the QoS IE may be accepted or downgraded according to operator policy configured at the GGSN using the usual QoS negotiation mechanisms described in TS 23.060 [19].

In the case of IMS, the IM CN Signalling Flag in the PCO IE is used to reference rules and restrictions on the PDP context used for application level signalling, as described in TS 23.228 [4] section 4.2.6.

The IM CN Signalling Flag and the Signalling indication in the QoS profile detailed in TS 23.107 [3] may be used independently of each other.

Based on operator policy the "Signalling Indication" in the QoS IE may be allowed only if the "IM CN Subsystem Signalling" flag is present in the PCO IE.



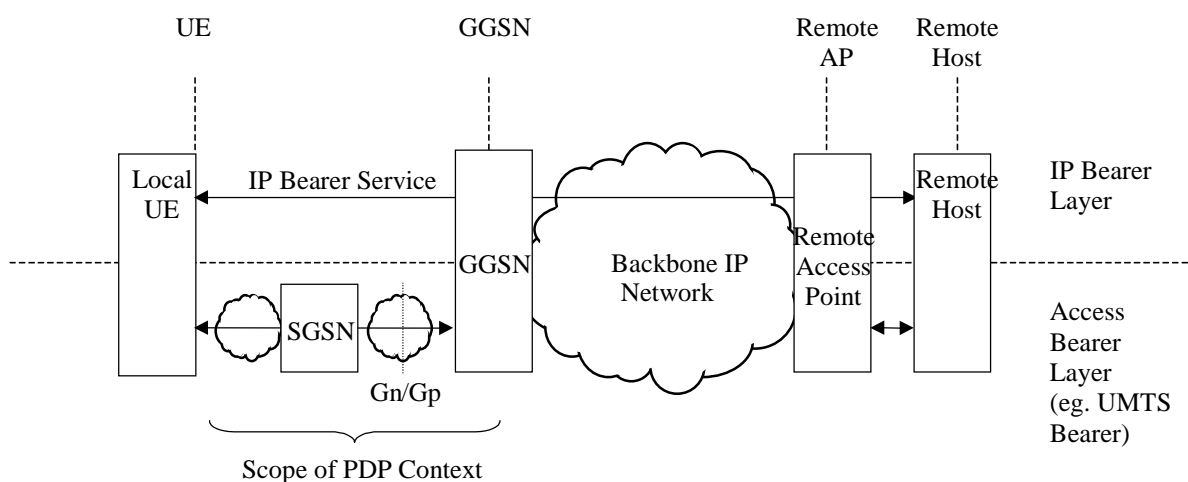
# Annex A (informative): QoS Conceptual Models

## A.1 Introduction

There are many different end-to-end scenarios that may occur from a UE connected to a UTM network. The following examples depict how end-to-end QoS will be delivered for a number of scenarios that are considered to be significant.

NOTE: Further consideration of scenarios 2 and 3 is not needed for Stage 3 work in the Release 5 timeframe. The normative aspects of scenarios 2 and 3 are considered to be already covered by scenario 1.

In all the scenarios presented below, the network architecture is as shown in Figure A.1 below.



**Figure A.1: Network Architecture for QoS Conceptual Models**

### NOTES:

- Although the backbone IP network is shown as a single domain, it may consist of a number of separate domains.
- The structure of the Local UE is not specified. It includes cases from a simple host, to a gateway to a network such as a LAN. If the UE is acting as a gateway, it is responsible for providing the IP BS Management towards the extended network.
- The remote side is shown as a simple host. Other more complex cases on the remote side such as a private LAN with over-provisioning, or possibly LAN priority marking, and DiffServ and/or RSVP capable routing elements is not depicted. It is envisaged however that interworking between the QoS mechanisms in a more complex remote user side could also be performed with some similarities to the mechanisms shown at the local side.

The reference point shown at the UE is at the interface to the UE. Within the UE, the QoS control could be derived from any of the mechanisms that occur across that reference point, or it could use a different mechanism internally.

Although the scenarios currently identified are mainly using DiffServ in the backbone IP network (RSVP is indicated as an alternative in scenario 4), it is not mandated that DiffServ must be used in the backbone IP network. Other mechanisms, for example, over-provisioning and aggregated RSVP may be used.

---

## A.2 Scenarios

These scenarios give examples of concatenating QoS mechanisms in different parts of the network which together can deliver an end-to-end QoS. These scenarios are not intended to describe the details of the interworking between the QoS mechanisms.

The different scenarios involve cases with and without service based local policy. Each scenario describes the applicable cases, possibly by referencing another scenario. In some scenarios, only one of the cases may be valid (e.g. scenario 5). Where both cases are covered, they may be described together identifying the optionality, or separately for clarity of the individual cases.

The optional authorisation token is associated with the cases involving service based local policy, and is applicable for IM services. It is an operator decision whether or not to support service based local policy for IM services. If service based local policy is not supported, or not applicable (i.e. not IM service), then the optional authorisation token and application server at the P-CSCF are not used.

IM services not using service based local policy will typically follow scenarios 1 to 4. IM services using service based local policy will typically follow scenarios 3 to 5.

NOTE: Scenario 5 is reserved for the IP multimedia services involving, e.g., SIP signalling, IP policy control, and subscription checking.

### A.2.1 Scenario 1

The UE does not provide an IP BS Manager. The end-to-end IP QoS bearer service towards the remote terminal is controlled from the GGSN.

The scenario assumes that the GGSN supports DiffServ edge functions, and the backbone IP network is DiffServ enabled.

NOTE: The UE may always include an authorisation token in establishment of the PDP context. Inclusion of the authorisation token in scenario 1 changes the QoS mechanisms to be the same as those described in scenario 5. Therefore, please refer to scenario 5 if the authorisation token is included.

The application layer (e.g. SIP/SDP) between the end hosts identifies the QoS requirements. The QoS requirements determined from the application layer (e.g. TS 23.228 [4] describes interworking from SIP/SDP to QoS requirements) are mapped down to PDP context parameters in the UE.

In this scenario, the control of the QoS over the UMTS access network (from the UE to the GGSN) may be performed either from the terminal using the PDP context signalling, or from the SGSN by subscription data.

The IP QoS for the downlink direction is controlled by the remote terminal up to the GGSN. The GGSN will apply receiver control DiffServ edge functions and can reclassify the data (remarking the DiffServ Code Point (DSCP)). This may affect the QoS applied to the data over the UMTS access (the TFT may use the DSCP to identify the data to be allocated to the PDP context).

The end-to-end QoS is provided by a local mechanism in the UE, the PDP context over the UMTS access network, DiffServ through the backbone IP network, and DiffServ in the remote access network in the scenario shown in the figure below. The GGSN provides the interworking between the PDP context and the DiffServ function. However, the interworking may use information about the PDP context which is established, or be controlled from static profiles, or dynamically through other means such as proprietary HTTP based mechanisms. The UE is expected to be responsible for the control of the PDP context, but this may instead be controlled from the SGSN by subscription.

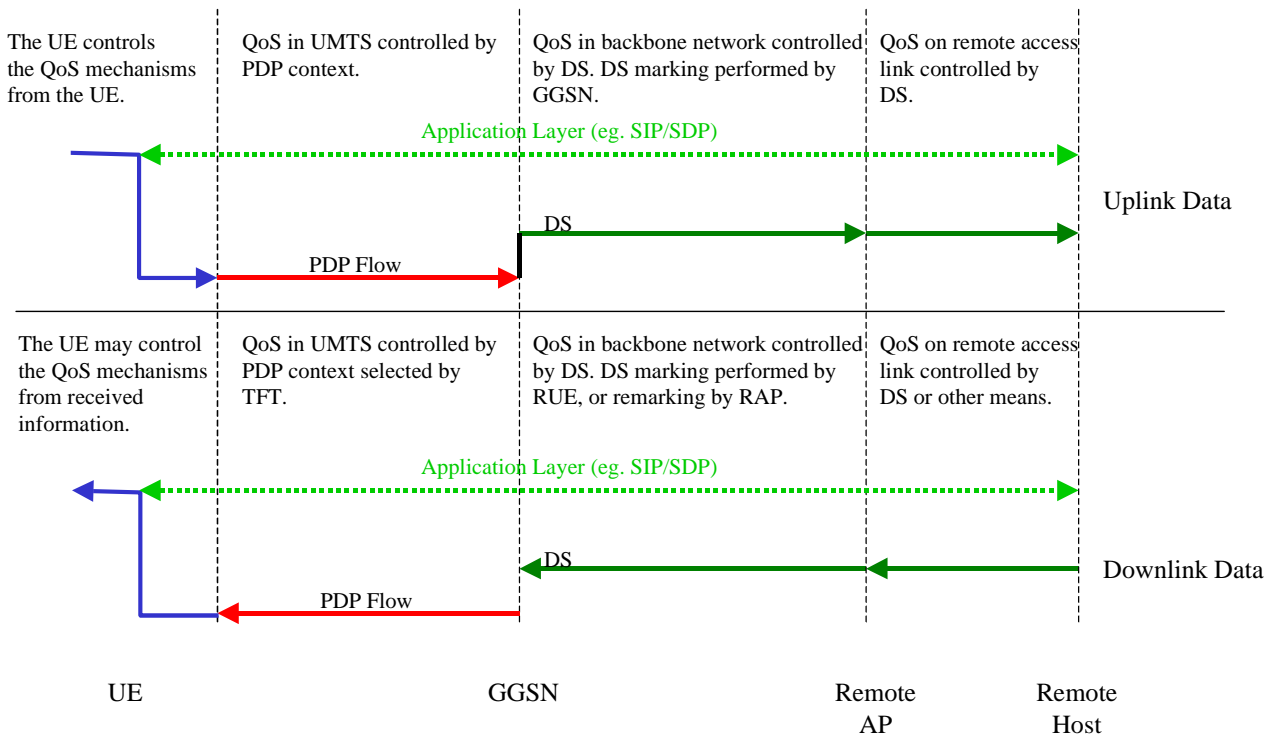


Figure A.2: Local UE does not provide IP BS Manager

Notes:

- The solid horizontal lines indicate the mechanism that is providing QoS for the flow of data in the direction indicated.
- The dashed horizontal lines indicate where QoS control information is passed that is not directly controlling the QoS in that link/domain.
- The arrows on the horizontal lines indicate nodes that receive information about QoS from that mechanism, even if that mechanism is not used to control the QoS over that link/domain.
- The solid vertical lines indicate interworking between the different mechanisms.
- In the figure, the term RAP refers to the Remote Access Point, and RUE is the Remote UE.

No solid vertical line is shown from DiffServ to PDP flow on the downlink at the GGSN. The TFT determines the QoS applicable over the UMTS access. However, the configuration of the TFT may use the DiffServ to select the PDP context to be applied, so there may be interworking between DiffServ and the PDP Flow via the TFT filters.

### A.2.2 Scenario 2

The UE performs an IP BS function which enables end-to-end QoS without IP layer signalling towards the IP BS function in the GGSN, or the remote terminal.

The scenario assumes that the UE and GGSN support DiffServ edge functions, and that the backbone IP network is DiffServ enabled.

NOTE: The UE may always include an authorisation token in establishment of the PDP context. Inclusion of the authorisation token in scenario 2 changes the QoS mechanisms to be the same as those described in scenario 5. Therefore, please refer to scenario 5 if the authorisation token is included.

The application layer (e.g. SIP/SDP) between the end hosts identifies the QoS needs. The QoS requirements from application layer (e.g. TS 23.228 [4] describes interworking from SIP/SDP to QoS requirements) are mapped down to the IP layer. The IP layer service requirements are further mapped down to the PDP context parameters in the UE.

In this scenario, the control of the QoS over the UMTS access network (from the UE to the GGSN) may be performed either from the terminal using the PDP context signalling. Alternatively, subscription data accessed by the SGSN may override the QoS requested via signalling from the UE (according to the procedures specified in TS 23.060 [19]).

In this scenario, the terminal supports DiffServ to control the IP QoS through the backbone IP network.

The IP QoS for the downlink direction is controlled by the remote terminal up to the GGSN. The PDP context controls the QoS between the GGSN and the UE. The UE may apply DiffServ edge functions to provide the DiffServ receiver control. Otherwise, the DiffServ marking from the GGSN will determine the IP QoS applicable at the UE.

The end-to-end QoS is provided by a local mechanism in the UE, the PDP context over the UMTS access network, DiffServ through the backbone IP network, and DiffServ in the remote access network in the scenario shown in the figure below. The UE provides control of the DiffServ, and therefore determines the appropriate interworking between the PDP context and DiffServ.

The GGSN DiffServ edge function may overwrite the DSCP received from the UE, possibly using information regarding the PDP context which is signalled between the UMTS BS managers and provided through the translation/mapping function to the IP BS Manager.

Note that DiffServ control at the Remote Host is shown in this example. However, other mechanisms may be used at the remote end, as demonstrated in the other scenarios.

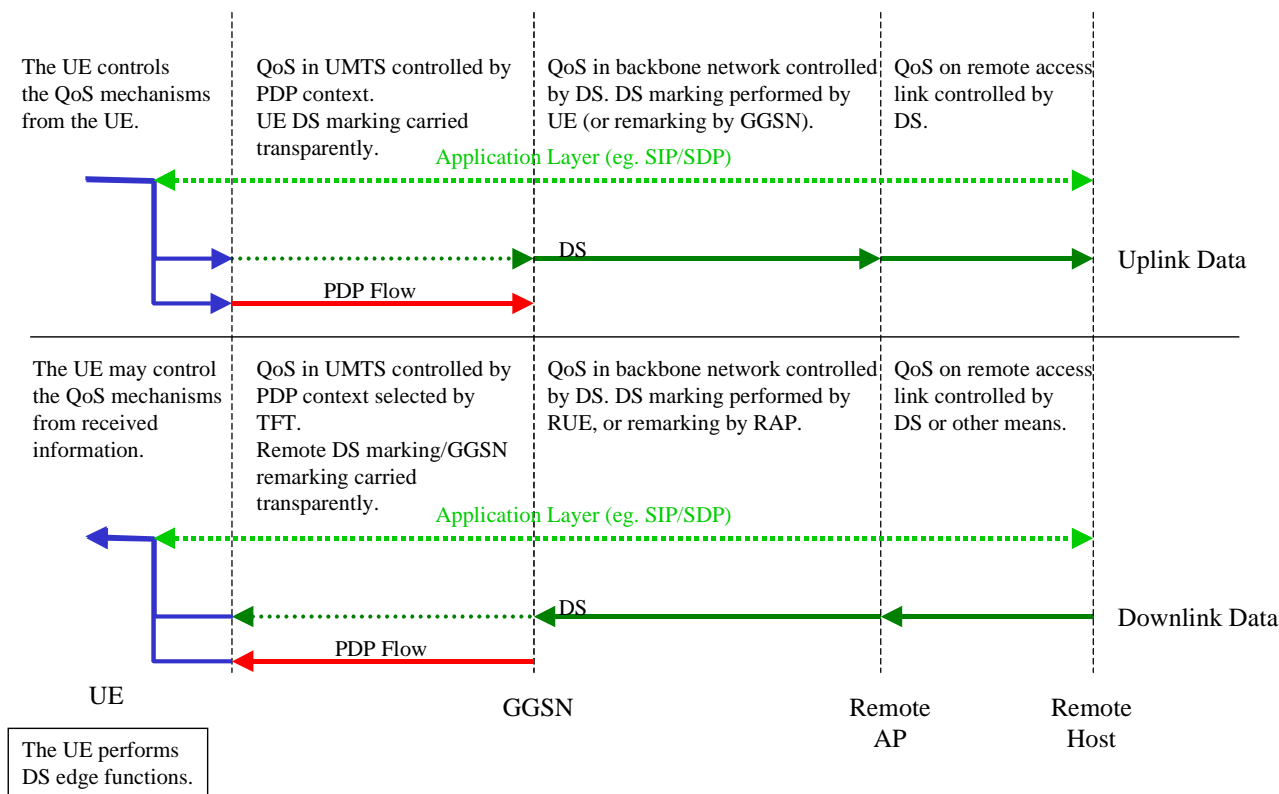


Figure A.3: Local UE supports DiffServ

### A.2.3 Scenario 3

The UE performs an IP BS function which enables end-to-end QoS using IP layer signalling towards the remote end. There is no IP layer signalling between the IP BS Managers in the UE and the GGSN. However, the GGSN may make use of information regarding the PDP context which is signalled between the UMTS BS managers and provided through the translation/mapping function.

This scenario assumes that the UE and GGSN support DiffServ edge functions, and that the backbone IP network is DiffServ enabled. In addition, the UE supports RSVP signalling which interworks within the UE to control the DiffServ.

The application layer (e.g. SIP/SDP) between the end hosts identifies the QoS requirements. The QoS requirements from application layer (e.g. TS 23.228 [4] describes interworking from SIP/SDP to QoS requirements) are mapped down to create an RSVP session. The UE shall establish the PDP context suitable for support of the RSVP session. The authorisation token from the application layer when included shall be mapped to the PDP context parameters, and may also be mapped to the RSVP signalling.

In this scenario, the control of the QoS over the UMTS access network (from the UE to the GGSN) may be performed either from the terminal using the PDP context signalling. Alternatively, subscription data accessed by the SGSN may override the QoS requested via signalling from the UE (according to the procedures specified in TS 23.060 [19]).

In this scenario, the terminal supports signalling via the RSVP protocol to control the QoS at the local and remote accesses, and DiffServ to control the IP QoS through the backbone IP network. The RSVP signalling protocol may be used for different services. It is expected that only RSVP using the Integrated Services (IntServ) semantics would be supported, although in the future, new service definitions and semantics may be introduced. The entities that are supporting the RSVP signalling should act according to the IETF specifications for IntServ and IntServ/DiffServ interwork.

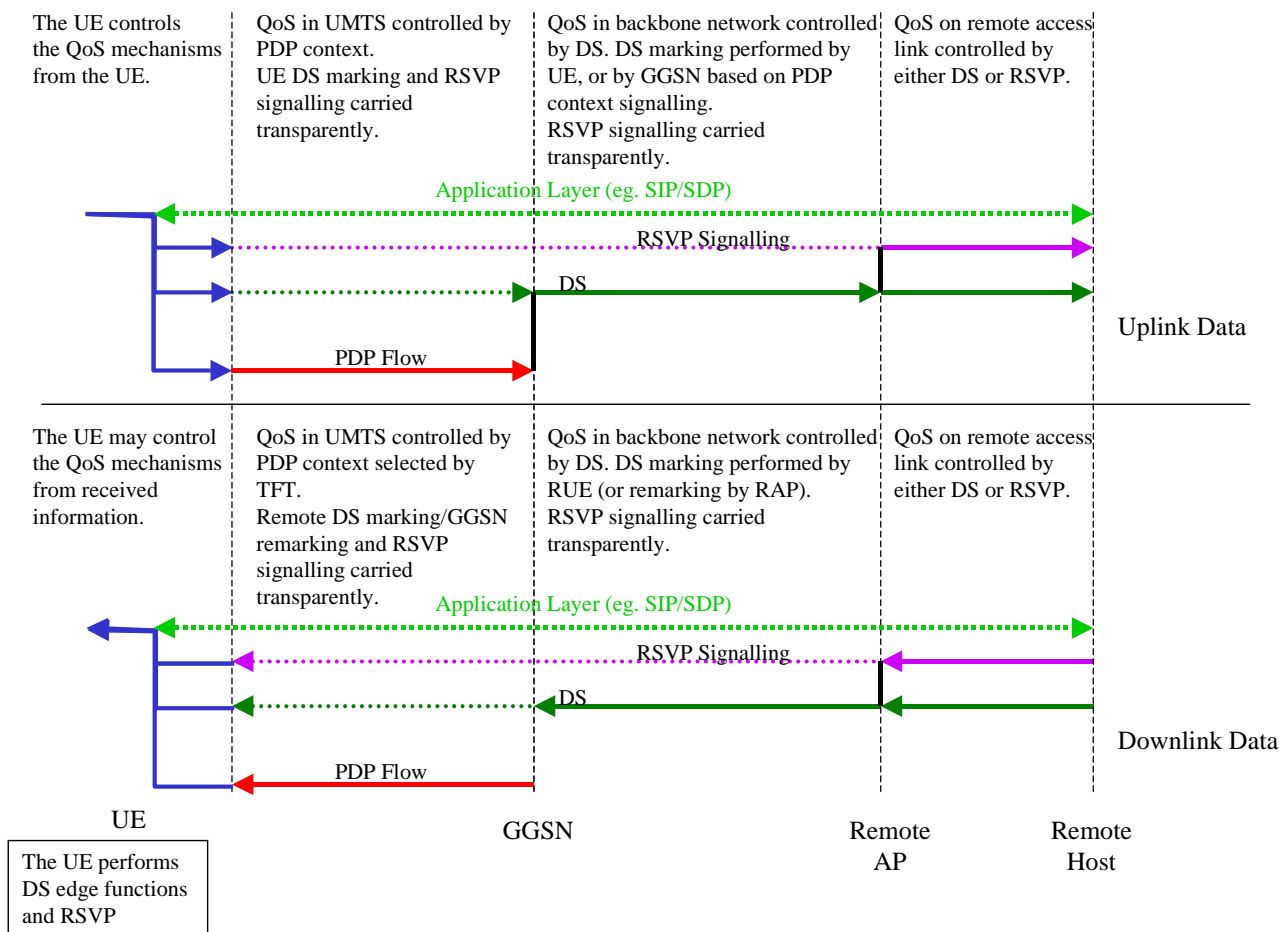
The QoS for the wireless access is provided by the PDP context. The UE may control the wireless QoS through signalling for the PDP context. The characteristics for the PDP context may be derived from the RSVP signalling information, or may use other information.

QoS for the IP layer is performed at two levels. The end-to-end QoS is controlled by the RSVP signalling. Although RSVP signalling can be used end-to-end in the QoS model, it is not necessarily supported by all intermediate nodes. Instead, DiffServ is used to provide the QoS throughout the backbone IP network.

At the UE, the data is also classified for DiffServ. Intermediate QoS domains may apply QoS according to either the RSVP signalling information or DiffServ mechanisms. In this scenario, the UE is providing interworking between the RSVP and DiffServ domains. The GGSN may override the DiffServ setting from the UE. This GGSN may use information regarding the PDP context in order to select the appropriate DiffServ setting to apply, as shown in the figure below.

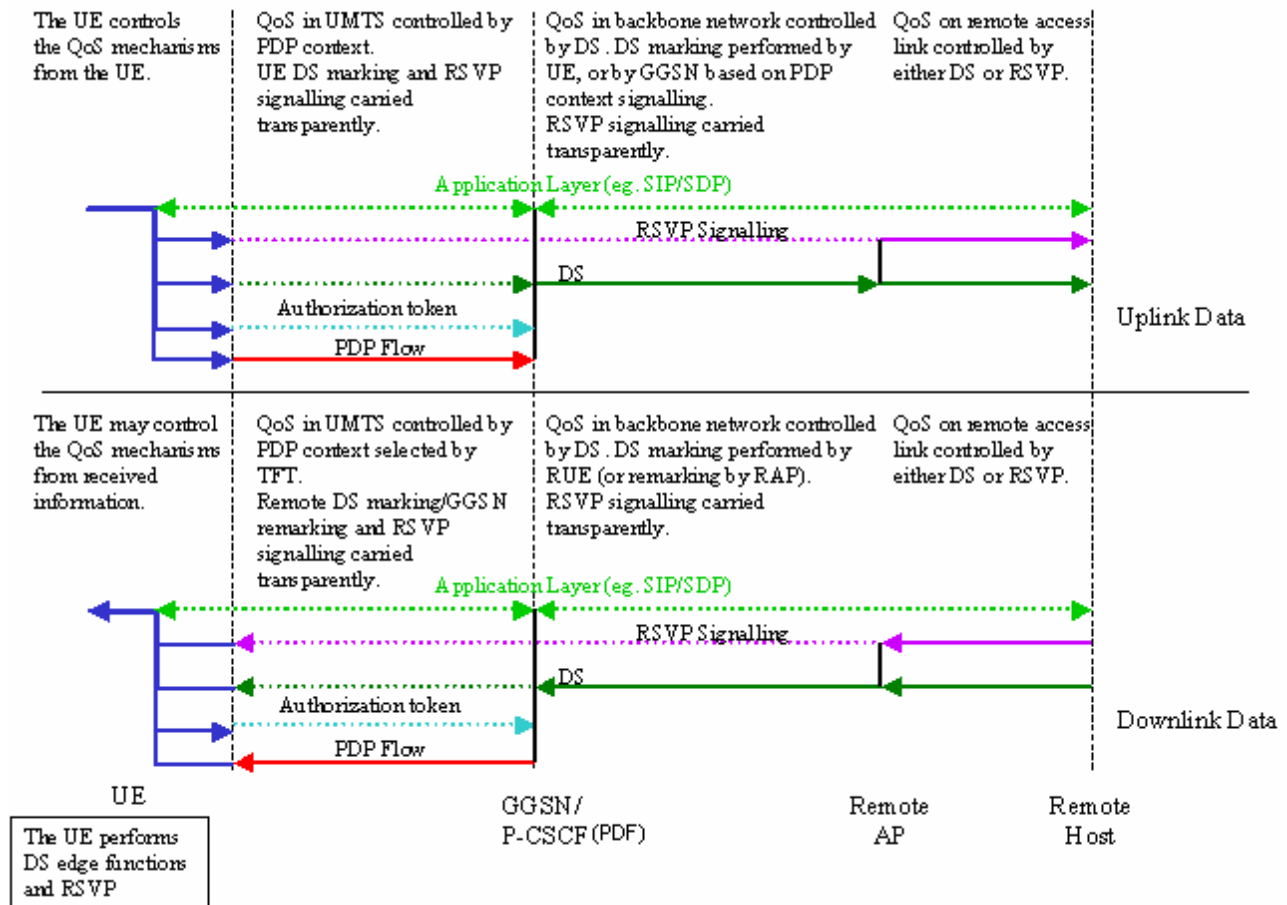
The end-to-end QoS is provided by a local mechanism in the UE, the PDP context over the UMTS access network, DiffServ through the backbone IP network, and DiffServ in the remote access network in the scenario shown in the figure below. The RSVP signalling may control the QoS at both the local and remote accesses. This function may be used to determine the characteristics for the PDP context, so the UE may perform the interwork between the RSVP signalling and PDP context.

The UE provides control of the DiffServ (although this may be overwritten by the GGSN), and in effect, determines the appropriate interworking between the PDP context and DiffServ.



**Figure A.4: Local UE supports RSVP signalling with IntServ semantics, and DiffServ; without service based policy**

The GGSN provides the interworking between the PDP context and the DiffServ function. The application layer signalling may be processed in the local network at an application server such as the P-CSCF in the case of SIP signalling. Interworking between the GGSN and the application layer is shown as a vertical line where applicable. This interworking is for policy control and is between the GGSN and the PDF policy function co-located in the P-CSCF, as shown in the figure below.



**Figure A.5: Local UE supports RSVP signalling with IntServ semantics, and DiffServ; where service based policy is applied**

### A.2.4 Scenario 4

The UE performs an IP BS function which enables end-to-end QoS using IP layer signalling towards the remote end. However, the UE relies on this end-to-end communication being utilised by at least the access point (GGSN) in order to provide the end-to-end QoS.

This scenario assumes that the UE and GGSN support RSVP signalling which may control the QoS directly, or interwork with DiffServ. The backbone IP network is RSVP and/or DiffServ enabled.

The application layer (e.g. SIP/SDP) between the end hosts identifies the QoS requirements. The QoS requirements from application layer (e.g. TS 23.228 [4] describes interworking from SIP/SDP to QoS requirements) are mapped down to create an RSVP session. The UE shall establish the PDP context suitable for support of the RSVP session. The authorisation token from the application layer shall be mapped to the PDP context parameters, and may also be mapped to the RSVP signalling.

In this scenario, the terminal supports signalling via the RSVP protocol to control the QoS across the end-to-end path. The GGSN also supports the RSVP signalling, and uses this information rather than the PDP context to control the QoS through the backbone IP network. The control of the QoS through the core is expected to be supported through interworking with DiffServ at the GGSN, although it may optionally be supported by per flow resource reservation. The RSVP signalling protocol may be used for different services. It is only expected that only RSVP using the Integrated Services (IntServ) semantics would be supported, although in the future, new service definitions and semantics may be introduced. The entities that are supporting the RSVP signalling may fully support the specifications for IntServ and IntServ/DiffServ interwork. If not, they are expected to set the break bit.

In this scenario, the control of the QoS over the UMTS access network (from the UE to the GGSN) may be performed either from the terminal using the PDP context signalling. Alternatively, subscription data accessed by the SGSN may override the QoS requested via signalling from the UE (according to the procedures specified in TS 23.060 [19]).

QoS for the IP layer is performed at two levels. The end-to-end QoS is controlled by the RSVP signalling. Although RSVP signalling occurs end-to-end in the QoS model, it is not necessarily supported by all intermediate nodes. DiffServ is used to provide the QoS throughout the backbone IP network, although optionally each node may support RSVP signalling and allocation of resources per flow. An authorisation token may be included in the RSVP signalling and the PDP context establishment/modification. The GGSN may authorise the RSVP session and configure the DiffServ classifier functionality.

The GGSN supports the RSVP signalling and acts as the interworking point between RSVP and DiffServ. Intermediate QoS domains may apply QoS according to either the RSVP or DiffServ mechanisms.

The end-to-end QoS is provided by a local mechanism in the UE, the PDP context over the UMTS access network, DiffServ through the backbone IP network, and RSVP in the remote access network in the scenario shown in the figure below. The RSVP signalling may control the QoS at the local access. This function may be used to determine the characteristics for the PDP context, so the UE may perform the interwork between RSVP and the PDP context.

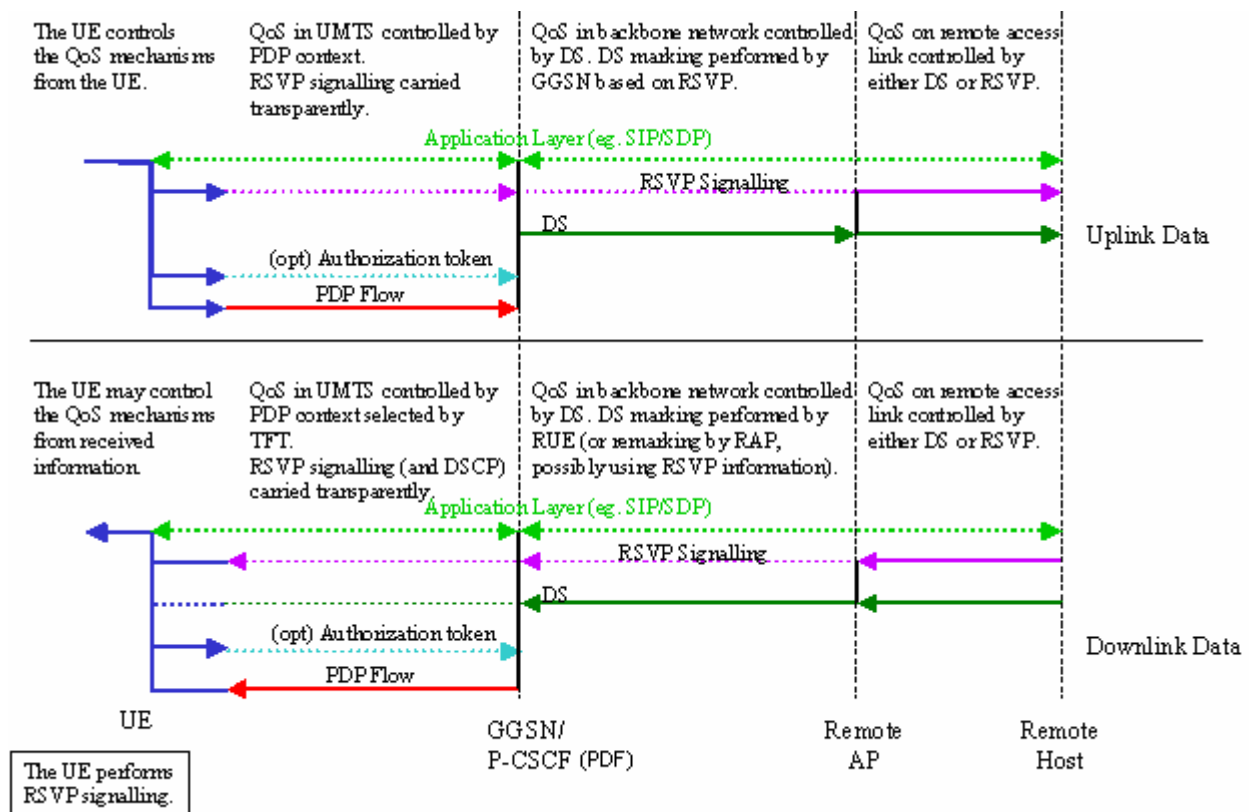


Figure A.6: Local UE supports RSVP signalling using IntServ Semantics

### A.2.5 Scenario 5

The UE performs an IP BS function which enables end-to-end QoS without IP layer signalling and negotiation towards the IP BS function in the GGSN, or the remote host. The P-CSCF provides the authorization token to the UE during the SIP session setup process, and the UE provides the authorization token to the GGSN in the PDP context activation/modification message. The GGSN uses the authorization token to obtain a policy decision from the P-CSCF(PDF). This is done via the standardized interface between the PDF and GGSN. Even if the interface is an open interface where all information elements are standardized, the actual usage of the information is operator specific.

The scenario assumes that the GGSN support DiffServ edge functions, and that the backbone IP network is DiffServ enabled.

The application layer (e.g. SIP/SDP) between the end hosts identifies the QoS needs. The QoS requirements from application layer (e.g. TS 23.228 [4] describes interworking from SIP/SDP to QoS requirements) are mapped down to the IP layer and further down to the PDP context parameters in the UE. The authorisation token from the application layer is included in the PDP context parameters by the UE.



In this scenario, the control of the QoS over the UMTS access network (from the UE to the GGSN) may be performed from the terminal using the PDP context signalling. Alternatively, subscription data accessed by the SGSN may override the QoS requested via signalling from the UE (according to the procedures specified in TS 23.060 [19]).

The QoS for the downlink direction is controlled by the remote host from the remote network to the GGSN. The PDP context controls the UMTS level QoS between the GGSN and the UE. The QoS in the uplink direction is controlled by the PDP context up to the GGSN. The GGSN configures the DiffServ Edge function to interwork with the backbone IP network and control the IP QoS bearer service towards the remote -host.

The end-to-end QoS is provided by a local mechanism in the UE, the PDP context over the UMTS access network, DiffServ through the backbone IP network, and DiffServ in the remote access network. Note that DiffServ control at the Remote Host is shown in this example. However, other mechanisms may be used at the remote end, as demonstrated in the other scenarios.

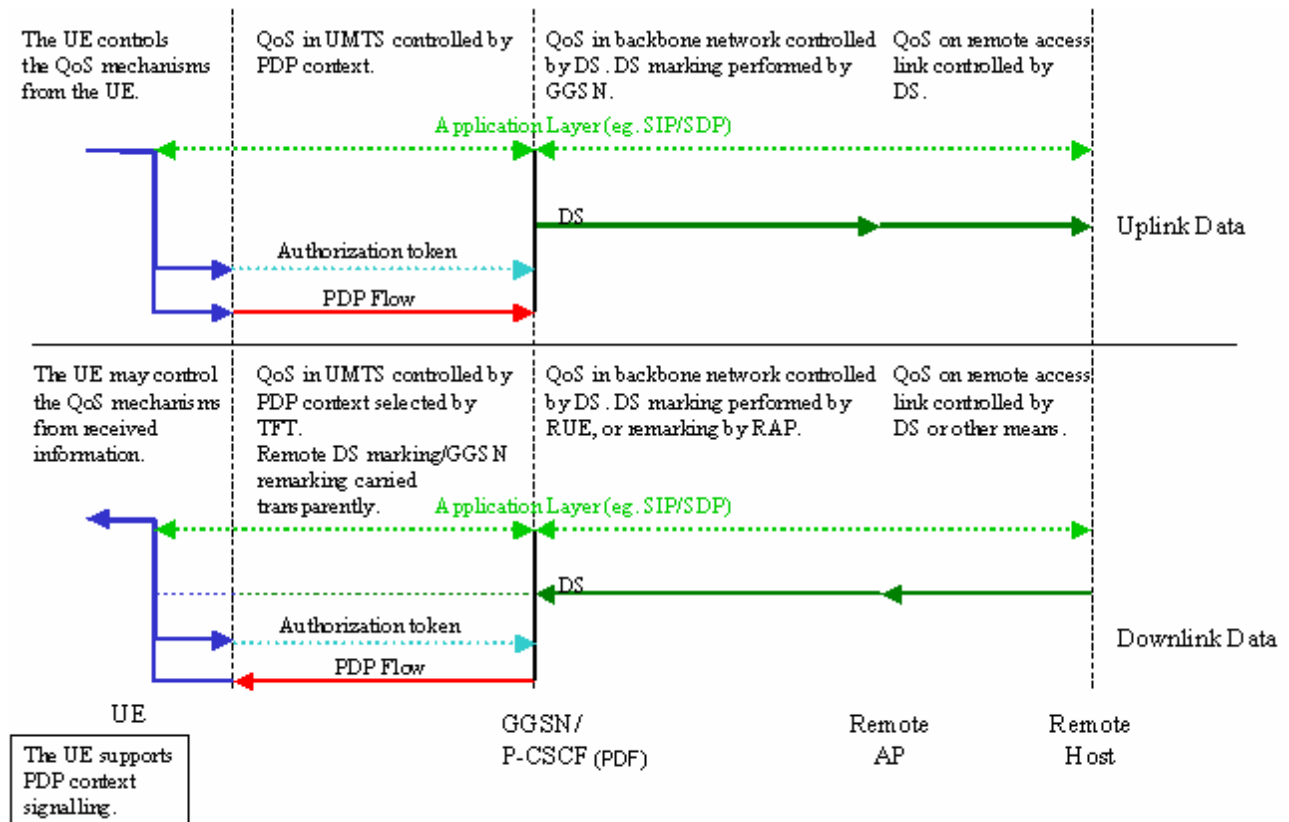


Figure A.7: Local UE provides authorization token in PDP context activation/modification message and GGSN provides interworking with DiffServ

Annex B (informative):  
(void)

## Annex C (informative): Sample Mapping of SDP Descriptions Into QoS Authorization

The QoS requirement for a session depends on the media and codec information for the session. Initial session establishment in the IM Subsystem must determine a common codec (or set of common codecs for multimedia sessions) that will be used for the session. This is done through an end-to-end message exchange to determine the complete set of common codecs, and then the session initiator makes the decision as to the initial set of codecs for the media flows.

The session initiator includes an SDP in the SIP INVITE message that lists every codec that the originator is willing to support for this session. When the message arrives at the destination endpoint, it responds with the subset that it is also willing to support for the session by selectively accept or decline those media types in the original list. When multiple media codecs are listed, the caller and called party's media fields must be aligned—that is, there must be the same number, and they must be listed in the same order. QoS authorization is performed for this common subset. The P-CSCF(PDF) shall use the SDP contained in the SIP signalling to calculate the proper authorization. The authorization shall include limits on IP resources, and restrictions on IP packet flows, and may include restrictions on IP destinations. These restrictions are expressed as a data rate and QoS class for the combined set of IP flows, and a set of filter specs.

The QoS authorization for a session shall include an Authorization-Token, which shall be assigned by the P-CSCF(PDF). The Authorization-Token shall contain information that identifies the P-CSCF(PDF) that generated the token. Each authorized session may include several flow authorizations. Each flow authorization may include an authorization for one or more flows. The authorization shall contain the following information:

- Filter Specs (IP flow 5-tuples that identify the set of flows)
- Data rate and QoS class that describes the authorized resource for the set of flows
- The IP flow 5-tuples includes Source Address, Source Port, Destination Address, Destination Port and Protocol ID. Note that some fields may be wildcarded.

A typical SDP description consists of a session-level description (details that apply to the whole session and all media flows) and the several media-level descriptions (details that apply to a single media flow). The four critical components for mapping an SDP description into a QoS authorization are the media announcements ("m="), the connection data ("c="), the attributes ("a=") and the bandwidth ("b=").

The media announcements field contains information about the type of media session, and is of the form:

m=<media> <port> <transport> <fmt list>

The attributes field contains attributes of the preceding media session, and is of the form:

a=<attribute><value>

The connection data field contains information about the media connection, and is of the form:

c=<network type> <address type> <connection address>

The optional bandwidth field contains information about the bandwidth required, and is of the form:

b=<modifier>:<bandwidth-value>

An example SDP description from the session originator in the SIP INVITE message:

```
v=0
o=hshieh 2890844526 2890842807 IN IP4 saturn.attws.com
s=-
c=IN IP4 192.141.10.188
t=0 0
```

```

b=AS:64
m=audio 29170 RTP/AVP 3 96 97
a=rtpmap:96 G726-32/8000
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
m=video 51372 RTP/AVP 34
a=fmtp 34 SQCIF=2/MaxBitRate=500/SAC AP
m=application 32416 udp text_chat

```

The called party answers the call and returns the following SDP description in the SIP 183 message:

```

v=0
o=johndoe 2890844526 2890842807 IN IP4 uranus.solar.com
s=-
c=IN IP4 204.142.180.111
t=0 0
b=AS:64
m=audio 31160 RTP/AVP 3 97
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=recvonly
m=video 61000 RTP/AVP 31
a=fmtp 34 SQCIF=2/MaxBitRate=500/SAC AP
m=application 33020 udp text_chat
a=sendonly

```

Upon receiving the above SDP, the originator's P-CSCF will authorize QoS resource for the originator UE with the following media flows:

#### A uplink audio flow:

The following IP 5-tuples identify the flow:

SrcAddress	SrcPort	DestAddress	DestPort	ProtocolID
192.141.10.188	*	204.142.180.111	31160	17

Since the conversational audio is very sensitive to delay, the maximum QoS class corresponding to conversational traffic class would be set. The b parameter is used to determine the maximum authorised data rate.

**An uplink video flow:**

The following IP 5-tuples identify the flow:

SrcAddress	SrcPort	DestAddress	DestPort	ProtocolID
192.141.10.188	*	204.142.180.111	61000	17

The video flow may be assigned a maximum QoS class corresponding to streaming traffic class. The b parameter is used to determine the data rate.

**A downlink video flow:**

The following IP 5-tuples identify the flow:

SrcAddress	SrcPort	DestAddress	DestPort	ProtocolID
204.142.180.111	*	192.141.10.188	51372	17

The video flow may be assigned a maximum QoS class corresponding to streaming traffic class. The b parameter is used to determine the maximum authorised data rate.

**A downlink udp flow:**

The following IP 5-tuples identify the flow:

SrcAddress	SrcPort	DestAddress	DestPort	ProtocolID
204.142.180.111	*	192.141.10.188	32416	17

The udp application flow may be assigned a maximum QoS class corresponding to interactive. The b parameter is used to determine the data rate.

NOTE: The sample mappings in this section are for illustration purpose only. The actual mapping of media codec to QoS resource requirement is specified in TS 29.208 [4b].

---

## Annex D (informative): Resource reservation and end-to-end RSVP

### D.1 Resource reservation with end-to-end RSVP

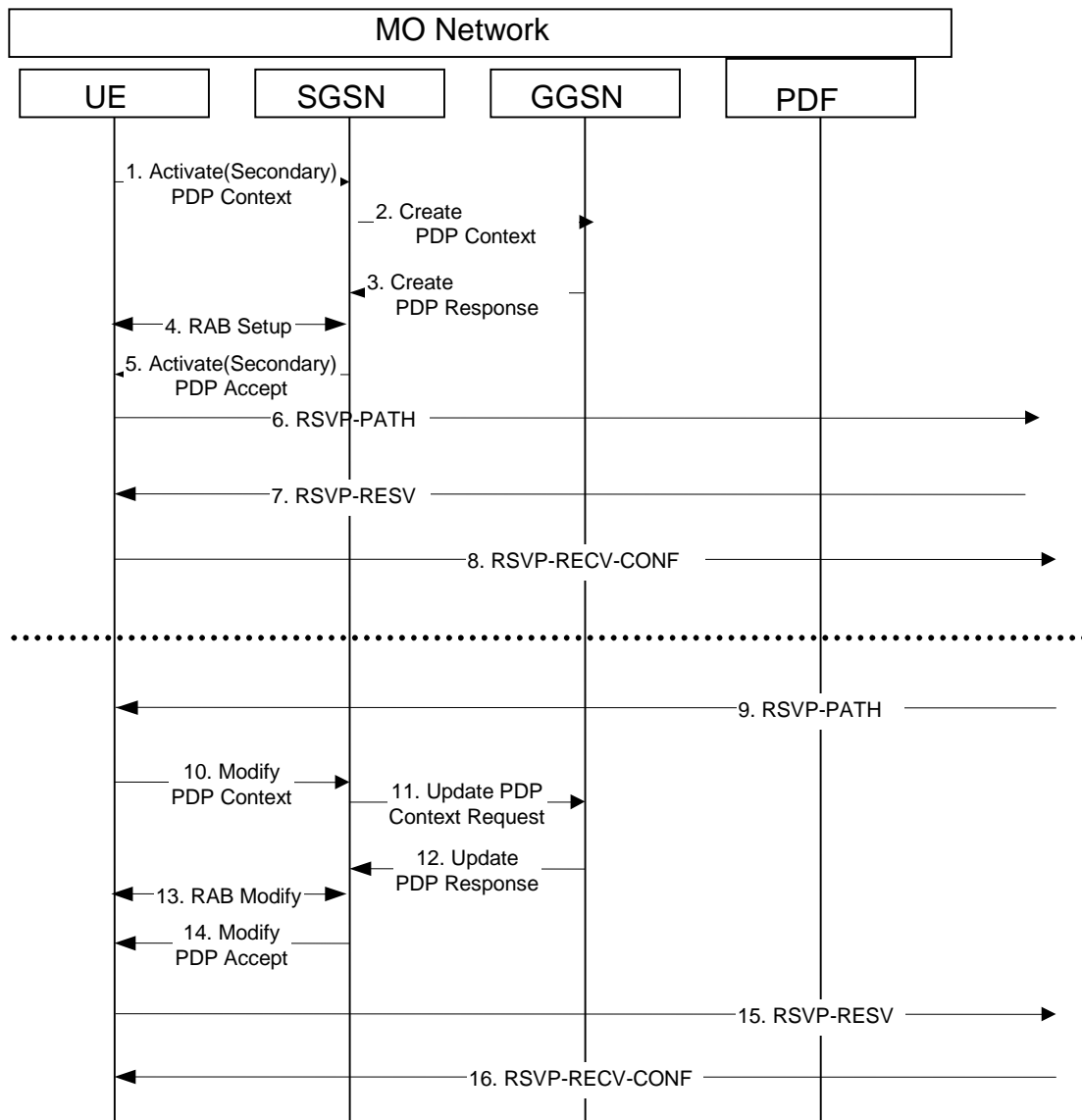
For this case, RSVP is added to the GPRS bearer establishment procedures specified in TS 23.060 [19], with no Service-based local policy.

NOTE: The diagrams in this subsection depict one possible signalling sequence, however, the alternative signalling sequences below are possible:

- to trigger the Create PDP Context Request message after the PATH message.
- to trigger the Create PDP Context Request message after the RESV message.
- to trigger only one PDP context after all RSVP exchanges have completed.

NOTE: The diagrams in this subsection depict the case when the GGSN is not RSVP aware, however, the alternative of GGSN being RSVP aware is also possible.

The following figure is applicable to the Mobile Originating (MO) side.



**Figure D.1: MO Resource Reservation with End-to-End RSVP**

NOTE: There is no timing relationship between the set of flows for the uplink (above the line) and the downlink (below the line).

- 1) The UE sends an Activate (Secondary) PDP Context message to the SGSN with the UMTS QoS parameters.
- 2) The SGSN sends the corresponding Create PDP Context message to the GGSN.
- 3) The GGSN authorizes the PDP context activation request according to the local operator's IP bearer resource based policy, the local operator's admission control function and the GPRS roaming agreements and sends a Create PDP Context Response message back to the SGSN.
- 4) RAB setup is done by the RAB Assignment procedure.
- 5) The SGSN sends an Activate (Secondary) PDP Context Accept message to UE.
- 6) UE sends an RSVP PATH message to the next hop, through the GGSN. The GGSN does not process the RSVP PATH message. Alternatively, the GGSN may process the RSVP PATH message and forward it to the next hop.
- 7) The UE receives the RSVP RESV message in the downlink direction, through the GGSN. The GGSN does not process the RSVP RESV message. Alternatively, the GGSN may process the RSVP RESV message and forward it to the UE.

- 8) The UE sends a RSVP RESV-CONF message to the next hop. The use of the RESV-CONF message is optional.
- 9) The UE receives a RSVP PATH message in the downlink direction, through the GGSN. The GGSN does not process the RSVP PATH message. Alternatively, the GGSN may process the incoming RSVP PATH message and forward it to the UE.
- 10) The UE may send a Modify PDP Context message to the SGSN with the necessary modification to UMTS QoS parameters according to the received RSVP PATH message.
- 11) The SGSN sends the corresponding Update PDP Context Request message to the GGSN.
- 12) The GGSN authorizes the PDP context modification according to the local operator's IP bearer resource based policy, the local operator's admission control function and the GPRS roaming agreements and sends an Update PDP Context Response message back to the SGSN.
- 13) The radio access bearer modification may be performed by the RAB Assignment procedure.
- 14) The SGSN sends a Modify PDP Context Accept message to UE.
- 15) UE sends the RSVP RESV message to the next hop, through the GGSN. The GGSN does not process the RSVP RESV message. Alternatively, the GGSN may process the RSVP RESV message and forward it to the next hop.
- 16) The UE receives the RSVP RESV-CONF message in the downlink direction. The use of the RESV-CONF message is optional.

The following figure is applicable to the Mobile Terminating (MT) side. As the flow is the mirror of the Mobile Originating (MO) side, the step-by-step description is omitted.



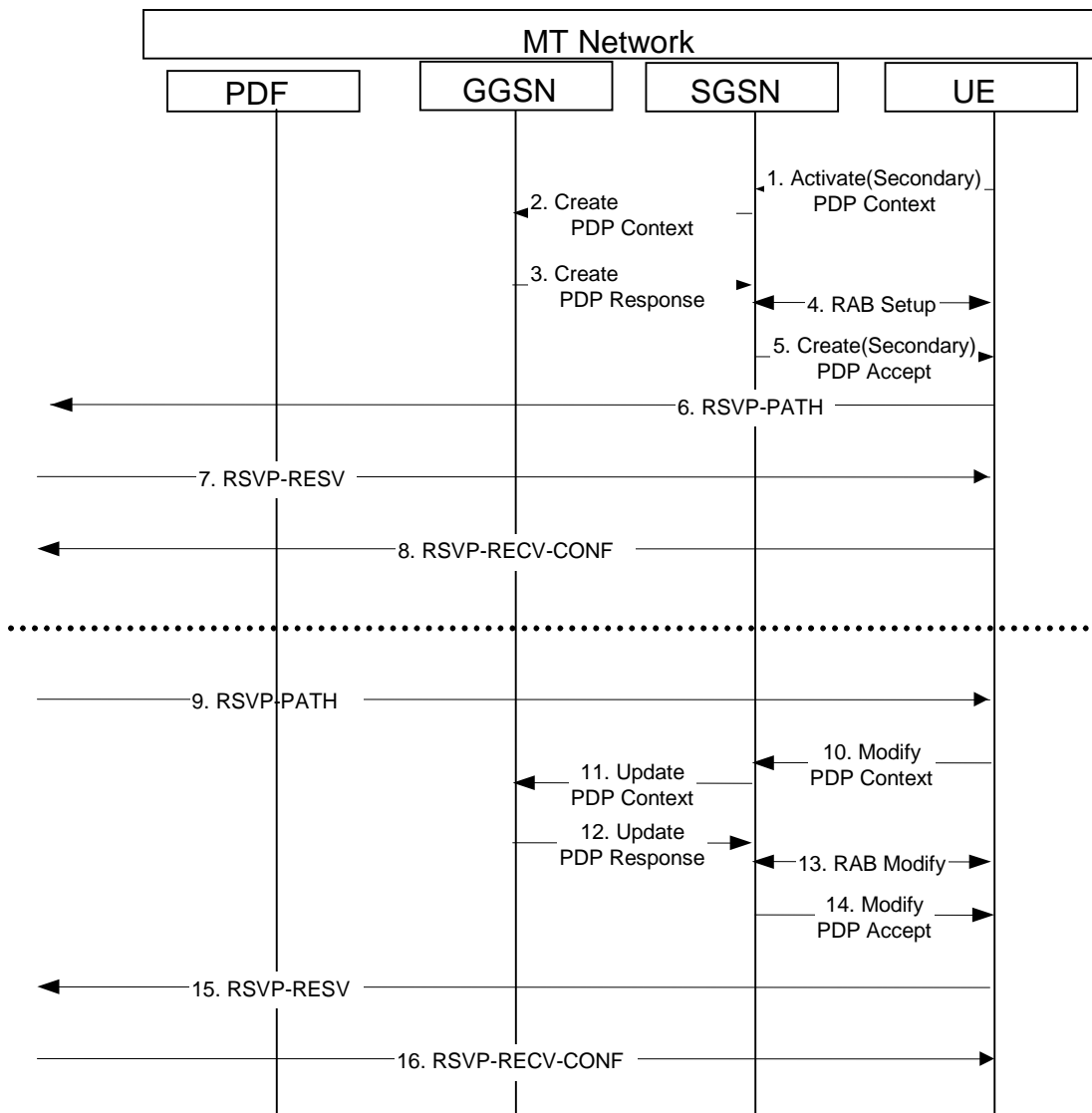


Figure D.2: MT Resource Reservation with End-to-End RSVP

NOTE: There is no timing relationship between the set of flows for the uplink (above the line) and the downlink (below the line).

## D.2 Resource Reservation with End-to-End RSVP and Service-based Local Policy

For this case, Service-based Local Policy and RSVP are added to the GPRS bearer establishment procedures specified in TS 23.060 [19].

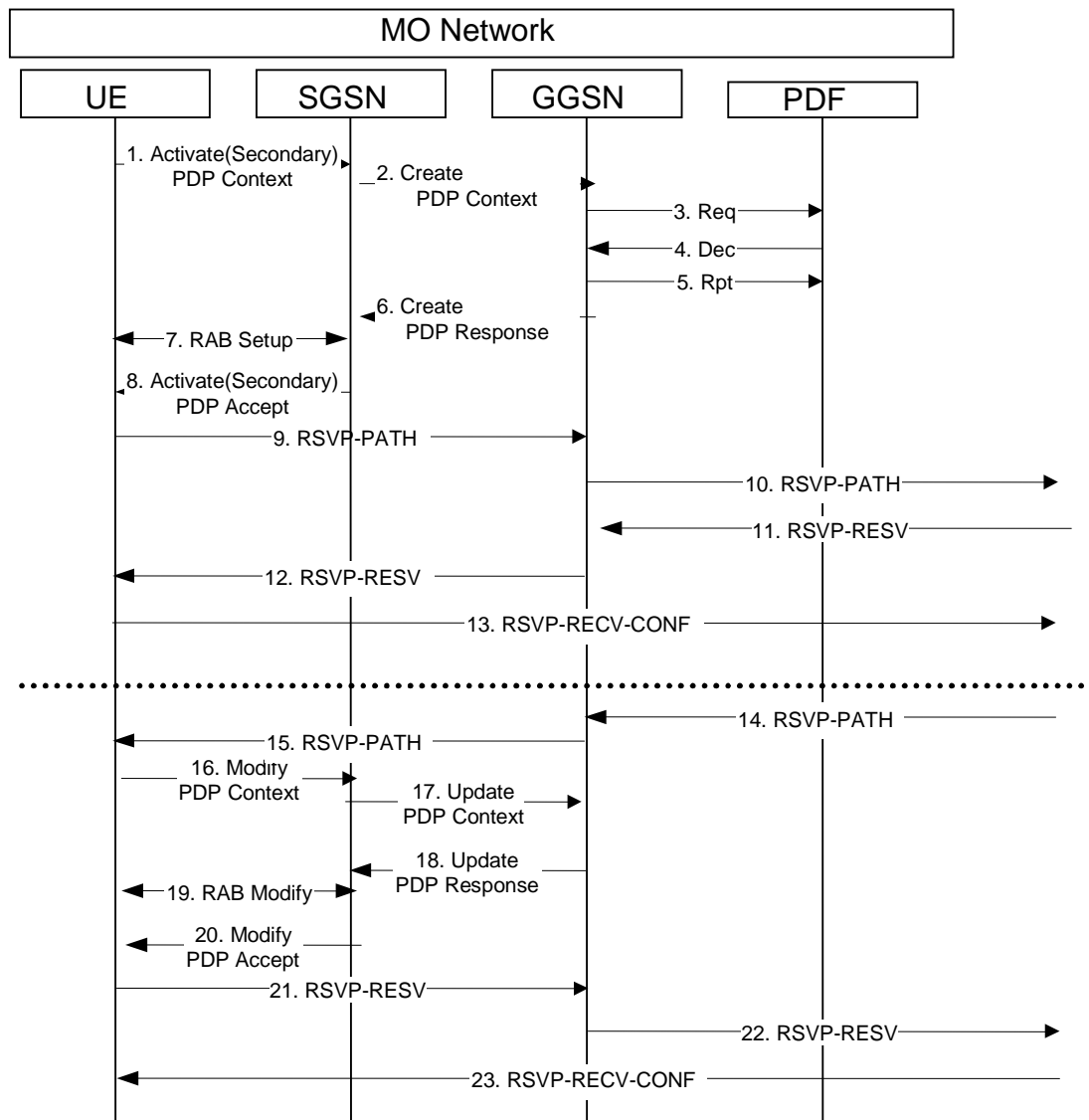
NOTE: The diagrams in this subsection depict one possible signalling sequence, however, the alternative signalling sequences below are possible:

- to trigger the Create PDP Context Request message after the PATH message.
- to trigger the Create PDP Context Request message after the RESV message.
- to trigger only one PDP context after all RSVP exchanges have completed.

NOTE: The diagrams in this subsection depict the case when the GGSN is RSVP aware, however, the alternative of GGSN not being RSVP aware is also possible.

This section provides the flows for bearer establishment, resource reservation and policy control with RSVP.

The following figure is applicable to the Mobile Originating (MO) side.



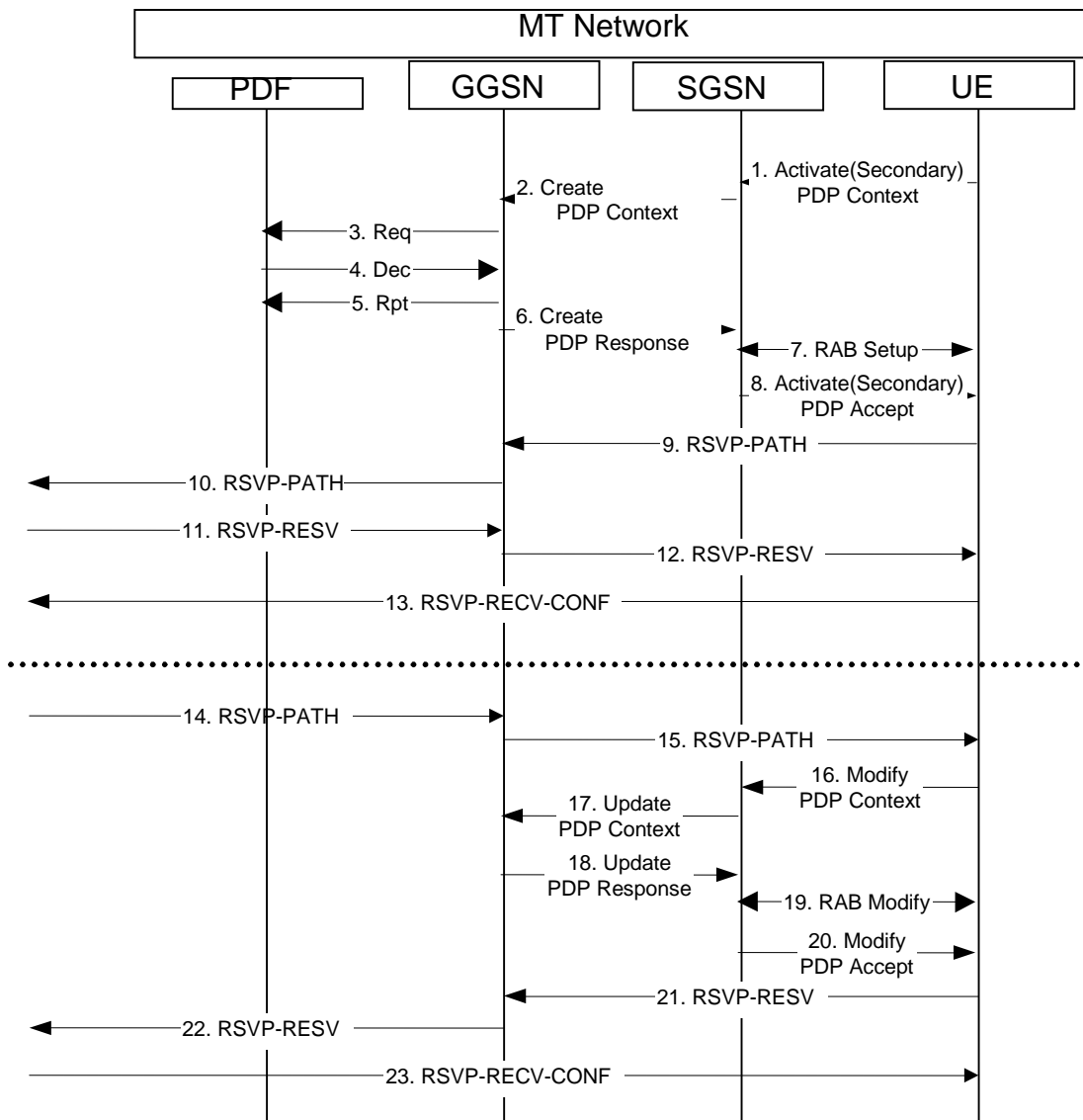
**Figure D.3: MO Resource Reservation with End-to-End RSVP and Service-based Local Policy**

NOTE: There is no timing relationship between the set of flows for the uplink (above the line) and the downlink (below the line).

- 1) The UE sends an Activate (Secondary) PDP Context message to the SGSN with the UMTS QoS parameters. The UE includes the Binding Information in the Activate PDP Context message.
- 2) The SGSN sends the corresponding Create PDP Context message to the GGSN.
- 3) The GGSN sends a COPS REQ message with the Binding Information to the PDF in order to obtain relevant policy information.
- 4) The PDF sends a COPS DEC message back to the GGSN.
- 5) The GGSN sends a COPS RPT message back to the PDF.
- 6) The GGSN maps IP flow based policy information into PDP context based policy information and uses the PDP context based policy information to accept the PDP activation request, and sends a Create PDP Context Response message back to SGSN. The GGSN may cache the policy information.

- 7) RAB setup is done by the RAB Assignment procedure.
  - 8) The SGSN sends an Activate (Secondary) PDP Context Accept message to UE.
  - 9) UE sends a RSVP PATH message to GGSN. The UE includes the Binding Information.
- NOTE: If the decision was previously cached locally at the GGSN, it may not be necessary to query the PDF again. Otherwise the GGSN may have to query the PDF.
- 10) The GGSN uses the policy information to accept the RSVP PATH message, and forwards the RSVP PATH message to the next hop.
  - 11) The GGSN receives the RSVP RESV message in the downlink direction.
- NOTE: If the decision was previously cached locally at the GGSN, it may not be necessary to query the PDF again. Otherwise the GGSN may have to query the PDF.
- 12) The GGSN uses the policy information to accept the RSVP RESV message, and forwards the RSVP RESV message to the UE.
  - 13) The UE sends a RSVP RESV-CONF message to the next hop. The use of the RESV-CONF message is optional.
  - 14) The GGSN receives a RSVP PATH message in the downlink direction.
  - 15) The GGSN forwards the RSVP PATH message to the UE.
  - 16) The UE may send a Modify PDP Context message to the SGSN with the necessary modification to UMTS QoS parameters according to the received RSVP PATH message. The UE includes the Binding Information in the Modify PDP Context message.
  - 17) The SGSN sends the corresponding Update PDP Context message to the GGSN.
- NOTE: If the decision was previously cached locally at the GGSN, it may not be necessary to query the PDF again. Otherwise the GGSN may have to query the PDF.
- 18) The GGSN uses the policy information to accept the PDP modification request, and sends a Update PDP Context Response message back to SGSN.
  - 19) The radio access bearer modification may be performed by the RAB Assignment procedure.
  - 20) The SGSN sends a Modify PDP Context Accept message to UE.
- NOTE: Steps 16 to 20 are optional if the existing PDP context already satisfies the QoS requirements.
- 21) The UE sends a RSVP RESV message to the GGSN. The UE includes the Binding Information in the RSVP RESV message.
- NOTE: If the decision was previously cached locally at the GGSN, it may not be necessary to query the PDF again. Otherwise the GGSN may have to query the PDF.
- 22) The GGSN uses the policy information to accept the RSVP RESV message, and forwards the RSVP RESV message to the next hop.
  - 23) The UE receives the RSVP RESV-CONF message in the downlink direction. The use of the RESV-CONF message is optional.

The following figure is applicable to the Mobile Terminating (MT) side. As the flow is the mirror of the Mobile Originating (MO) side, the step-by-step description is omitted.



**Figure D.4: MT Resource Reservation with End-to-End RSVP and Service-based Local Policy**

NOTE: There is no timing relationship between the set of flows for the uplink (above the line) and the downlink (below the line).

## Annex E (informative): Change history

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Cat	Old	New
2001-06	SP-12	SP-010337	-	-	Raised to Version 5. Same technical content as version 2.0.0	-	2.0.0	5.0.0
2001-10	SP-13	SP-010513	0003	1	Session Flow: QoS Interaction Procedures	F	5.0.0	5.1.0
2001-10	SP-13	SP-010513	0004	1	COPS Usage for Go Interface	F	5.0.0	5.1.0
2001-10	SP-13	SP-010513	0002	-	Token generation at the PCF	F	5.0.0	5.1.0
2001-10	SP-13	SP-010513	0005	1	P-CSCF and PCF Clarifications	F	5.0.0	5.1.0
2002-01	SP-14	SP-010711	0001	3	PDP Context Used for Application Level Signalling	B	5.1.0	5.2.0
2002-01	SP-14	SP-010711	0006	2	P-CSCF notification of PDP context modification	C	5.1.0	5.2.0
2002-01	SP-14	SP-010711	0008	3	QoS Scenarios Considerations	F	5.1.0	5.2.0
2002-01	SP-14	SP-010711	0009	1	Session Flow: QoS Interaction Procedures	B	5.1.0	5.2.0
2002-01	SP-14	SP-010711	0010	-	COPS Usage for Go Interface	B	5.1.0	5.2.0
2002-01	SP-14	SP-010711	0012	-	Mapping IP flow based policy information into PDP context based policy information in the GGSN	F	5.1.0	5.2.0
2002-01	SP-14	SP-010711	0013	1	New event for P-CSCF notification of PDP context modification	C	5.1.0	5.2.0
2002-03	SP-15	SP-020134	0014	1	Removal of packet handling action from PCF decision	F	5.2.0	5.3.0
2002-03	SP-15	SP-020134	0017	1	Authorization of QoS Resources	F	5.2.0	5.3.0
2002-03	SP-15	SP-020134	0019	-	Number of media components per PDP Context	B	5.2.0	5.3.0
2002-03	SP-15	SP-020134	0020	-	Incorrect Place of the RAB Procedures in Section 6.3.2	F	5.2.0	5.3.0
2002-03	SP-15	SP-020134	0021	1	Editorial Corrections of QoS Interaction Procedures Flows	D	5.2.0	5.3.0
2002-03	SP-15	SP-020134	0022	1	Corrections of the Indication of PDP Context Release Procedure	F	5.2.0	5.3.0
2002-03	SP-15	SP-020134	0023	1	Corrections in 6.3 Session Flow: QoS Interaction Procedures	F	5.2.0	5.3.0
2002-03	SP-15	SP-020153	0025	-	Correction of references to obsolete SIP RFC 2543 IETF Specification	F	5.2.0	5.3.0
2002-06	SP-16	SP-020315	0028	2	Alignment of TS 23.207	F	5.3.0	5.4.0
2002-06	SP-16	SP-020315	0027	1	Clarifications to TS 23.207	F	5.3.0	5.4.0
2002-06	SP-16	SP-020315	0030	-	Correct miss-match between figure and explanatory texts	F	5.3.0	5.4.0
2002-06	SP-16	SP-020315	0034	3	Number of media components per PDP Context	F	5.3.0	5.4.0
2002-09	SP-17	SP-020532	0036	1	Modification of IMS Signalling PDP context	F	5.4.0	5.5.0
2002-09	SP-17	SP-020532	0037	2	SBLP Handling and TFT Processing	F	5.4.0	5.5.0
2002-09	SP-17	SP-020532	0039	1	Policy control procedures on PDP context modification	F	5.4.0	5.5.0
2002-09	SP-17	SP-020532	0040	4	Source IP address filtering for Service Based Local Policy	F	5.4.0	5.5.0
2002-09	SP-17	SP-020532	0043	1	Alignment with stage 3	F	5.4.0	5.5.0
2002-09	SP-17	SP-020532	0045	-	Alignment with stage 3- RSVP	F	5.4.0	5.5.0
2002-12	SP-18	SP-020774	0046	2	Clarifications on Go interface	F	5.5.0	5.6.0
2002-12	SP-18	SP-020774	0048	1	Consistency of stage 2 - RSVP proxy	F	5.5.0	5.6.0
2002-12	SP-18	SP-020774	0051	-	PCF to PDF Changes	F	5.5.0	5.6.0
2002-12	SP-18	SP-020774	0049	4	Mobile IP and Service Based Local Policy interactions	F	5.5.0	5.6.0
2002-12	SP-18	SP-020819	0044	4	Alignment with stage 3 - DS control over Go	F	5.5.0	5.6.0
2003-03	SP-19	SP-030119	0055	-	Removal of editors notes	F	5.6.0	5.7.0
2003-06	SP-20	SP-030302	0057	1	Handling of IMS signalling information in QoS and PCO IEs at GGSN	F	5.7.0	5.8.0
2003-09	SP-21	SP-030378	0060	1	Functional additions for the Gq interface	B	5.8.0	6.0.0
2003-12	SP-22	SP-030656	0061	3	Procedures in the AF	B	6.0.0	6.1.0
2003-12	SP-22	SP-030656	0062	1	Information exchanged via Gq interface	B	6.0.0	6.1.0
2003-12	SP-22	SP-030656	0063	1	Procedures in the PDF	B	6.0.0	6.1.0
2003-12	SP-22	SP-030656	0064	-	Editorial corrections to 23.207	D	6.0.0	6.1.0
2004-01	SP-22	SP-030656	0065	2	Gq-related updates to the signalling flows	B	6.0.0	6.1.0
2004-01	SP-22	SP-030656	0066	3	Requirements for IM CN Subsystem signalling flag	B	6.0.0	6.1.0
2004-01	SP-22	SP-030656	0067	-	Defintion of the Application Function	F	6.0.0	6.1.0
2004-03	SP-23	SP-040035	0074	1	Update of Authorization on Gq	B	6.1.1	6.2.0
2004-03	SP-23	SP-040035	0068	1	Mapping amendment to PDF procedures	B	6.1.1	6.2.0
2004-03	SP-23	SP-040035	0069	2	Mapping amendment to AF procedures	B	6.1.1	6.2.0
2004-03	SP-23	SP-040035	0073	1	SBLP implications of bundling different IMS sessions to the same PDP Context	B	6.1.1	6.2.0
2004-03	SP-23	SP-040035	0075	1	Service information	B	6.1.1	6.2.0
2004-06	SP-24	SP-040317	0077	3	Authorisation Reject Procedure by the PDF	B	6.2.0	6.3.0
2004-06	SP-24	SP-040317	0079	1	AF capabilities	F	6.2.0	6.3.0
2004-06	SP-24	SP-040317	0080	2	General corrections	B	6.2.0	6.3.0

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Cat	Old	New
2004-06	SP-24	SP-040317	0081	1	Intra-domain Gq for IMS	F	6.2.0	6.3.0
2004-06	SP-24	SP-040317	0083	-	Condition for update authorization procedure	B	6.2.0	6.3.0
2004-09	SP-25	SP-040521	0084	1	SBLP and non-realtime PDP Contexts	F	6.3.0	6.4.0
2004-09	SP-25	SP-040521	0085	-	Generation of multiple tokens	F	6.3.0	6.4.0
2005-06	SP-28	SP-050337	0087	-	Update of binding information handling	F	6.4.0	6.5.0
2005-09	SP-29	SP-050337	0088	1	Correction of reference to non-existent/obsolete document	A	6.5.0	6.6.0

---

## History

<b>Document history</b>		
V6.4.0	September 2004	Publication
V6.5.0	June 2005	Publication
V6.6.0	September 2005	Publication