Technical Specification Group Services and System Aspects ***TSGS#18(02)0774***

Meeting #18, New Orleans, U.S.A., 9-12 December 2002

Source: **TSG SA WG2**
Title: **CRs on 23.207**
Agenda Item: **7.2.3**

The following Change Requests (CRs) have been approved by TSG SA WG2 and are requested to be approved by TSG SA plenary #18.
Note: the source of all these CRs is now S2, even if the name of the originating company(ies) is still reflected on the cover page of all the attached CRs.

Tdoc #	**Title**	**Spec**	**CR #**	**cat**	**Version in**	**REL**	**WI**	**S2 meeting**
S2-023060	Clarifications on Go interface	23.207	046rev2	F	5.5.0	5	IMS-CCR	S2-27
S2-023063	Clarification of Diffserv functions in 23.207 without Go control	23.207	050rev1	F	5.5.0	5	E2EQoS	S2-27
S2-023064	Alignment with stage 3 – DS control over Go	23.207	044rev3	F	5.5.0	5	E2EQoS	S2-27
S2-023065	Consistency of stage 2 – RSVP proxy	23.207	048rev1	F	5.5.0	5	E2EQoS	S2-27
S2-023269	PCF to PDF Changes	23.207	051	F	5.5.0	5	IMS-CCR	S2-28
S2-023535	Definition of QoS Class	23.207	052rev1	F	5.5.0	5	E2EQoS	S2-28
S2-023538	Mobile IP and Service Based Local Policy interactions	23.207	049rev4	F	5.5.0	5	E2EQoS	S2-28

3GPP TSG-SA2 Meeting #27
Beijing, China, 14 – 18 October

Tdoc S2 –~~022707~~023060rev1

CR-Form-v7

CHANGE REQUEST

⌘ **23.207** **CR** **046** ⌘**rev** **2** ⌘ Current version: **5.5.0** ⌘

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

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

Title:	⌘	Clarifications on Go interface
Source:	⌘	NEC Corporation
Work item code:	⌘	IMS-CCR
Date:	⌘	7/10/2002
Category:	⌘	**F**
Release:	⌘	Rel-5

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

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	The description of the type of charging related information across the Go interface is not accurate. In clauses 5.4 and 5.5, there is inappropriate sentences as requirement level.
Summary of change:	⌘	1. The nature of charging related information passed on the Go interface is clarified. 2. It is proposed to change the sentence appropriately in 5.4.5.5.
Consequences if not approved:	⌘	Misalignment remains between 23.207 and stage3 as well as 23.228.

Clauses affected:	⌘	2, 5.3, 5.4, 5.5

		Y	N		
Other specs affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	

Other comments:	⌘	

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

Start of first change

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 22.288: "Service requirements for the IP Multimedia – 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".

[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".

End of first change

Start of second change

5.3 Go interface (PCF – 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 Control Function (PCF). The Go interface provides information to support the following functions in the GGSN:

- Control of Diffserv inter-working
-
- 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 Control Function (PCF). 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 PCF 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 PCF.

5.3.2 Information Elements 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 PCF. The information elements specific to UMTS would be standardized and carried in the 3GPP Go specific interactions between the PCF and the GGSN.

A **Request** (REQ) message from the GGSN to the PCF shall allow the GGSN to request SBLP policy information for the IP flow(s) identified by binding information (described below).

Binding information associates the PDP context to the ~~IMS session and~~ IP flow(s) of an IMS session, and is used by the GGSN to request SBLP policy information from the PCF. The binding information includes 1) an authorization token sent by the P-CSCF to the UE during SIP signalling, and 2) one or more flow identifiers used by the UE, GGSN and PCF to uniquely identify the IP media flow(s).

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 PCF 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 PCF 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 PCF 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 PCF. 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~~Event generation information (e.g. charging identity)~~

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 wild-carded.

The authorized QoS information provides an upper bound on the resources that can be reserved or allocated for the IP flow(s). 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 29.207.

The packet handling action defines the packet handling that should be accorded to in-profile and out-of-profile packets matching the packet classifier. In-profile traffic is defined as traffic that is within the authorized QoS information. The packet handling action may be ignored by the GGSN.

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 PCF 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

~~Event generation~~Charging correlation information contains information used to correlate usage records (e.g. CDRs) of the GGSN with IMS session records from the P-CSCF. ~~The PCF shall send the ICID provided by the P-CSCF as part of the authorisation (Install) decision. The~~ For this purpose, the GGSN shall send the GCID of the PDP context and the GGSN address to the PCF 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).

5.4 QoS Parameters

~~Note that the details for this section are specified in~~See stage 3 specification 3GPP TS 29.207[4a].

5.5 QoS Parameter Mapping

~~Note that the details for this section are specified in~~See stage 3 specification 3GPP TS 29.208[4b].

End of second change

3GPP TSG-SA2 Meeting #28
Bangkok, Thailand, 11-15 October 2002

S2-023538 ⌘

CR-Form-v7

CHANGE REQUEST

⌘ **23.207** **CR** **49** ⌘**rev** **4** ⌘ Current version: **5.5.0** ⌘

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

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Use of MobileIPv6 route optimisation and Service Based Local Policy
Source:	⌘	Nortel Networks
Work item code:	⌘	E2E-QoS
Date:	⌘	11/11/2002
Category:	⌘	**F**
Release:	⌘	Rel-5

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

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	Standard IPv6 nodes may support the procedures for Route Optimisation when communicating with a node using MobileIPv6 ('Correspondant Node procedures'). Use of MIPv6 Route Optimisation is not compatible with IMS Service Based Local Policy.
Summary of change:	⌘	Add clarification that MIPv6 Route Optimisation will not operate effectively because packets direct to the Care Of Address may not be allowed by Service Based Local Policy
Consequences if not approved:	⌘	Possible failure of IMS sessions if MIPv6 Route Optimisation requests are accepted and Service Based Local Policy is applied.

Clauses affected:	⌘	6.1.2

	Y	N		
Other specs affected: ⌘		X	Other core specifications	⌘
		X	Test specifications	
		X	O&M Specifications	

Other comments: ⌘

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

---------- First Modified Section ----------

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. If the UE received the Authorization Token in SIP signalling, the UE shall include the Authorization Token in the PDP Context Activation request for the PDP Context(s) that are activated to carry the media flows of the IMS session.

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. If the UE received the Authorization Token in SIP signalling, the UE shall include the Authorization Token in the PDP Context Activation request for the PDP Context(s) that are activated to carry the media flows of the IMS session.

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

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

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

---------- End of Modifications ----------

3GPP TSG-S2#27
Bangkok, Thailand. 11th - 15th November. 2002

Tdoc ⌘ S2-023535

CR-Form-v7

CHANGE REQUEST

⌘ **TS 23.207** **CR** **52** ⌘ **rev** 1 ⌘ Current version: **5.5.0** ⌘

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

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

Title:	⌘	Definition of QoS Class
Source:	⌘	Ericsson
Work item code:	⌘	E2EQoS
Date:	⌘	2002-10-15
Category:	⌘	**F**
Release:	⌘	REL-5

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

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	The term QoS class has been used in TS 23.207, but it is not described what this term means. At last SA2 meeting Ericsson took action to provide a definition for this term consistent with stage 3 functions. The term is clarified.
Summary of change:	⌘	A definition for QoS class is provided.
Consequences if not approved:	⌘	Some terminology is unclear.

Clauses affected:	⌘	5.2.1

		Y	N		
Other specs affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	

Other comments: ⌘

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

First amended section

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 [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 configured on the GGSN or derived from PDP context parameters.

RSVP/IntServ Function

[Editor's note: Detailed functional description of RSVP/IntServ Function is FFS]

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 PCF 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 TS23.228 are to control and manage media flows based on policy, and are under the control of PCF. 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.

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 PCF associated with the IP flow(s). In order to allow SBLP policy information to be "pulled" from the PCF, the binding information shall allow the GGSN to determine the address of the PCF to be used.

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.

3GPP TSG-SA2 Meeting #28
Bangkok, Thailand, November 11, 2002

Tdoc ⌘ S2-023269

CR-Form-v7

CHANGE REQUEST

⌘ **23.207** **CR** **51** ⌘**rev** **-** ⌘ Current version: **5.5.0** ⌘

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

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

Title:	⌘	PCF to PDF Change
Source:	⌘	Lucent Technologies
Work item code:	⌘	IMS-CCR
Date:	⌘	11.11.2002
Category:	⌘	**F**
Release:	⌘	Rel-5

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

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	It was agreed to use the Policy Decision Function teminology for compatibiltiy with other access networks.
Summary of change:	⌘	Replace the term Policy Control Function with Policy Decision Function throughout the document.
Consequences if not approved:	⌘	Confusion between the 3GPP and other architectures.

Clauses affected:	⌘	3.2, 5.1, 5.1.1.1, 5.1.2.1, 5.2, 5.2.1, 5.2.3, 5.3, 5.3.1, 5.3.2, 6.1.1, 6.1.3, 6.2, 6.3.1, 6.3.2.1, 6.3.2.2, 6.3.2.3, 6.3.3, 6.3.4, 6.3.5, 6.3.6, 6.3.6a, 6.3.7, A.2.3, A.2.4, A.2.5,			
		Y	**N**		
Other specs affected:	⌘	**X**		Other core specifications	⌘ 23.002, 23.228, 24.228, 24.229, 29.207, 29.208
				Test specifications	
				O&M Specifications	
Other comments:	⌘				

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

**********First Change**********

3.2 Abbreviations

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

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
~~PCF~~PDF	~~Policy Control Function~~Policy Decision Function
PEP	Policy Enforcement Point
PHB	Per Hop Behavior
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

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 99.
- 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 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 Control Function~~Policy Decision Function (~~PCF~~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 Control Function**~~**Policy Decision Function (~~PCF~~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 [RFC2753] "A Framework for Policy-based Admission Control" where the ~~PCF~~PDF is effectively a Policy Decision Point (PDP). The ~~PCF~~PDF makes decisions in regard to SBLPusing policy rules, and communicates these decisions to the IP BS Manager in the GGSN, which is the IP Policy Enforcement Point (PEP).

The ~~Policy Control Function~~Policy Decision Function (~~PCF~~PDF) is a logical entity of the P-CSCF. If the ~~PCF~~PDF is implemented in a separate physical node, the interface between the ~~PCF~~PDF and P-CSCF is not standardized.

The interface between the ~~PCF~~PDF and GGSN is specified within 3GPP, named Go interface, and is included in the Reference Architecture depicted in TS23.002. The protocol interface between the ~~PCF~~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 ~~PCF~~PDF makes policy decisions based on information obtained from the P-CSCF. In the P-CSCF(~~PCF~~PDF), the application level parameters (e.g., SDP) are mapped into IP QoS parameters. The P-CSCF(~~PCF~~PDF) is in the same domain as the GGSN.

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

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 and be able to shape upstream traffic. 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.

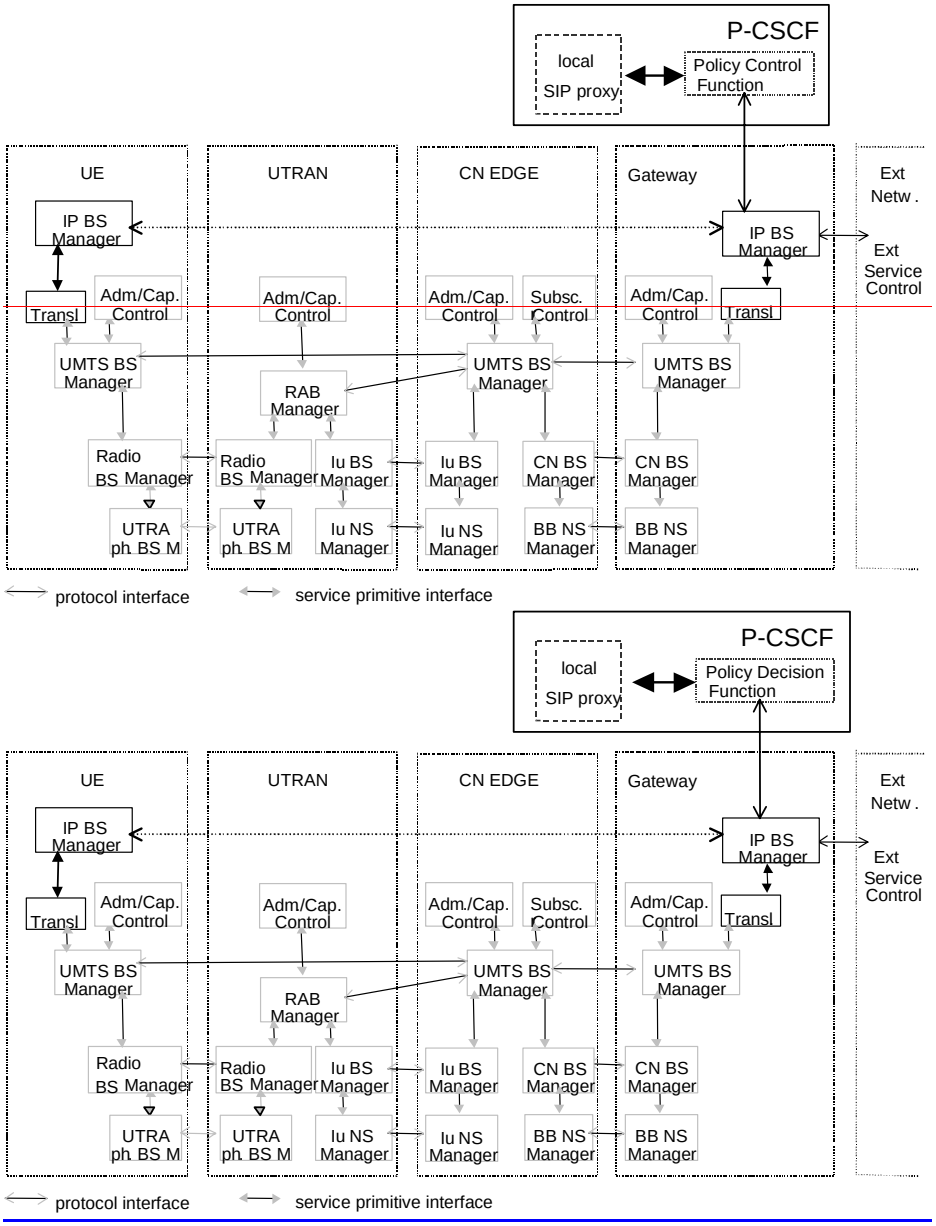


Figure 2: QoS management functions for UMTS bearer service in the control plane and QoS management functions for end-to-end IP QoS

NOTE: The dimmed boxes in Figure 2 are clarified in TS23.107.

NOTE: The following will be revisited in the Release 6 timeframe: - the possible reuse of the protocols in the Go interface between the GGSN and other application servers, and possible interfaces between the ~~PCF~~PDF and the P-CSCF, and between the ~~PCF~~PDF and other application servers.

[Editor's note: Figure 2 and this chapter shows UE only as a combined element. This TS also need to consider the case where the TE and MT are split. A section providing the split and the distribution of functionality need to be added to this TS and is for further study. Standardization of the interface between the TE and MT is the responsibility of the 3GPP working group TSG T2, and is outside the scope of this TS.]

5.2 Capabilities of Functional Elements

This section provides functional descriptions of capabilities in GGSN, UE, and P-CSCF(~~PCF~~PDF).

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. The IETF Differentiated Services architecture will be used to provide QoS for the external bearer service.

RSVP/IntServ Function

[Editor's note: Detailed functional description of RSVP/IntServ Function is FFS]

The **Service-based Local Policy Enforcement Point** controls the quality of service that is provided to a set of IP packets (or IP "flows") defined by a packet classifier. The policy enforcement function includes policy-based admission control that is applied to the IP bearers associated with the flows, and configuration of the packet handling and 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 IP flow 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 an IP flow. The authorized resources may be expressed as an Intserv-style Flowspec. 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 ~~PCF~~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 TS23.228 are to define the control and to manage media flows based on policy, and are under the control of ~~PCF~~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, a gate status (open/closed), a traffic metering function, and user plane actions to be taken for the set of packets matching the classifier. When a gate is open, the packets in a flow are subject to the Diffserv edge treatment (policing or marking) as determined by traffic metering and user plane actions. 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.

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. It is possible for a set of packets to match more than one classifier. When this happens, the sequence of actions associated with the gates are executed in sequence. Packets that are marked by a gate may not be (re)marked by a subsequent gate to a Diffserv Code Point corresponding to a better service class.

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 ~~PCF~~PDF associated with the IP flow(s). In order to allow SBLP policy information to be "pulled" from the ~~PCF~~PDF, the binding information shall allow the GGSN to determine the address of the ~~PCF~~PDF to be used.

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 RFC2475, 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 authorization token may also be used to bind a RSVP session with a SIP session by including the authorization token and flow identifier(s) in RSVP messages. For IMS services, the authorization token is provided to the UE by the P-CSCF during SIP session establishment.

The manner in which QoS preconditions for a SIP session shall be met are as stated in TS 23.228. The functionality shall be compliant to the IETF specification on Integration of Resource Management and SIP.

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 P-CSCF(~~PCF~~PDF)

This clause provides functional descriptions of capabilities in P-CSCF(~~PCF~~PDF). Determination of exactly which functions are required to support interoperator and multi-vendor aspects are not addressed in this clause.

Service-based Local Policy Decision Point

- Authorize QoS resources (bandwidth, etc.) for the session. The P-CSCF (~~PCF~~PDF) shall use the SDP contained in the SIP signaling message 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 IP packet flows and restrictions on IP destination address and port. For bi-directional media flows, the P-CSCF(~~PCF~~PDF), 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 P-CSCF(~~PCF~~PDF) assumption would be determined by operator policy in order to reduce the possibilites of bearer misuse In the filters supplied by the ~~PCF~~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.

- The P-CSCF (~~PCF~~PDF) shall be able to enforce the behaviour of the UE in 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 IMS network using the indications described in Sections 4.2.5.1 of [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 P-CSCF/~~PCF~~PDF shall take care that such a PDP context would be rejected by the GGSN. To do so, the P-CSCF/~~PCF~~PDF uses the Go interface.

- The P-CSCF (~~PCF~~PDF) shall be able to decide if new QoS authorization (bandwidth, etc.) is needed due to the 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 ~~PCF~~PDF functions as a Policy Decision Point for the service-based local policy control.

- The ~~PCF~~PDF shall exchange the authorization information with the GGSN via the Go interface.
- ~~PCF~~PDF provides final policy decisions controlling the allocated QoS resources for the authorized media stream. The decision shall be transferred from the ~~PCF~~PDF to the GGSN.
- At IP multimedia session release, the ~~PCF~~PDF shall revoke the QoS resource authorization for the session.

Binding Mechanism Handling

- The ~~PCF~~PDF generates an authorization token for each SIP session and the P-CSCF sends the authorization token to the UE in SIP signalling. The authorization token may contain information that identifies its generator. 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.

5.3 Go interface (~~PCF~~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 Control Function~~Policy Decision Function (~~PCF~~PDF). The Go interface provides information to support the following functions in the GGSN:

- Control of Diffserv inter-working
-
- 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 Control Function~~Policy Decision Function (~~PCF~~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 ~~PCF~~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 ~~PCF~~PDF.

5.3.2 Information Elements 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 ~~PCF~~PDF. The information elements specific to UMTS would be standardized and carried in the 3GPP Go specific interactions between the ~~PCF~~PDF and the GGSN.

A **Request** (REQ) message from the GGSN to the ~~PCF~~PDF shall allow the GGSN to request SBLP policy information for the IP flow(s) identified by binding information (described below).

Binding information associates the PDP context to the IMS session and IP flows, and is used by the GGSN to request SBLP policy information from the ~~PCF~~PDF. The binding information includes 1) an authorization token sent by the P-CSCF to the UE during SIP signalling, and 2) one or more flow identifiers used by the UE, GGSN and ~~PCF~~PDF to uniquely identify the IP media flow(s).

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 ~~PCF~~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 ~~PCF~~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 ~~PCF~~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 ~~PCF~~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
- Event generation information (e.g. charging identity)

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 wild-carded.

The authorized QoS information provides an upper bound on the resources that can be reserved or allocated for the IP flow(s). 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 29.207.

The packet handling action defines the packet handling that should be accorded to in-profile and out-of-profile packets matching the packet classifier. In-profile traffic is defined as traffic that is within the authorized QoS information. The packet handling action may be ignored by the GGSN.

Event generation information contains information used to correlate usage records (e.g. CDRs) of the GGSN with IMS session records from the P-CSCF. The ~~PCF~~PDF shall send the ICID provided by the P-CSCF as part of the authorisation (Install) decision. The GGSN shall send the GCID of the PDP context and the GGSN address to the ~~PCF~~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).

5.4 QoS Parameters

Note that the details for this section are specified in stage 3 specification TS 29.207.

5.5 QoS Parameter Mapping

Note that the details for this section are specified in stage 3 specification TS 29.208.

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 signaling 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 IP level information (e.g., addressing 5-tuple) provided by service based local policy according to the authorization token to configure the DiffServ classifier 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 GGSN may use IP level information provided by service based local policy according to authorization token to authorize the RSVP session and configure the DiffServ classifier functionality. The authorization token may be included in the RSVP signaling 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 and optionally (dependent on operator policy) RSVP messages that are subject to service based local policy by sending an authorization request to the ~~PCF~~PDF. Alternatively, the GGSN may authorize PDP context activation/modification messages and optionally (dependent on operator policy) RSVP 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.

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. If the UE received the Authorization Token in SIP signalling, the UE shall include the Authorization Token in the PDP Context Activation request for the PDP Context(s) that are activated to carry the media flows of the IMS session.

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. If the UE received the Authorization Token in SIP signalling, the UE shall include the Authorization Token in the PDP Context Activation request for the PDP Context(s) that are activated to carry the media flows of the IMS session.

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

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

6.1.3 Procedures in the P-CSCF(~~PCF~~PDF)

The QoS procedures in P-CSCF(~~PCF~~PDF) are related to service based local policy control.

The authorize QoS resources procedure is triggered by the P-CSCF receiving a SIP message containing SDP information. The SDP contains sufficient information about the session, such as the end-points, bandwidth requirements and the characteristics of the media exchange. The P-CSCF initiates a policy setup in ~~PCF~~PDF for the IMS session. The ~~PCF~~PDF shall authorize the required QoS resources and install the IP bearer level policy for the IMS session.

The Authorization-Token is generated by the ~~PCF~~PDF and sent to the UE by the P-CSCF. For the originating UE, the Authorization-Token shall be included in the first available reliable SIP message (e.g. 183 Session Progress)) from P-CSCF to the UE. For the terminating UE, the Authorization-Token shall be included in the SIP Invite message from P-CSCF to the UE.

The P-CSCF also generates and forwards an indication to the UE to assist the UE in deciding whether it can assign multiple media components to the same PDP Context, or separate PDP Contexts have to be used. This mechanism is described in Section 4.2.5.1 in [4].

Upon receiving the bearer authorization request from the GGSN, the ~~PCF~~PDF shall authorize the request according to the stored SBLP for the session.

The ~~PCF~~PDF makes a final decision to enable the allocated QoS resource for the authorized IP flows. This may be triggered by the receipt of the SIP 200 OK (Invite Response) message to the P-CSCF. QoS resources may also be enabled at the time they are authorised by the ~~PCF~~PDF.

During the mid-call SIP signaling for media or codec change, the ~~PCF~~PDF shall be able to decide if new QoS authorization is needed. 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 flow changed.

At IMS session release, the ~~PCF~~PDF shall 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 binding information in PDP Context Activation and Modification messages to associate the PDP context bearer with policy information . The binding information includes 1) an Authorization Token sent by the P-CSCF to the UE during SIP signaling, and 2) one or more Flow Identifiers which are used by the UE, GGSN and ~~PCF~~PDF to uniquely identify the IP media flow(s). It is assumed that only one binding information is carried within PDP context Activation/Modification messages in this Release.

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 ~~PCF~~PDF, the authorization token shall allow the GGSN to determine the address of the ~~PCF~~PDF to be used.

6.3 Session Flow: QoS Interaction Procedures

This section highlights possible additions to the GPRS bearer establishment procedures specified in TS23.060 for support of IM Services, and describes the QoS interactions involved within the sub-procedure blocks for Authorize QoS Resources, Resource Reservation with Service-based Local Policy, Approval of QoS Commit, Removal of QoS Commit, Revoke Authorization for GPRS and IP Resources, Indication of PDP Context Release, Authorization of PDP Context Modification and Indication of PDP Context Modification in Chapter 5: 'IP multimedia subsystem procedures' of TS23.228. 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 TS23.060 without the additions described in this section.

For cases where Service-based Local Policy is not used, the Authorize QoS Resources,the Resource Reservation with Service-based Local Policy, the Approval of QoS Commit, the Removal QoS Commit, 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 TS23.228 are not applied.

For the flow sequences involving RSVP, the following are assumed:

- the successful setup of RSVP signalling.
-

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: Whether 'gate' corresponds to a single IP flow or multiple IP flows is FFS.

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

The Authorize QoS Resources procedure is triggered by the P-CSCF receiving a SIP message containing SDP information. An offer-answer pair of SDP payloads contain sufficient information about the session, such as the end-points, bandwidth requirements, and the characteristics of the media exchange.

The ~~PCF~~PDF shall authorize the required QoS resources for the session and install the IP bearer level policy based on information from the P-CSCF.

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

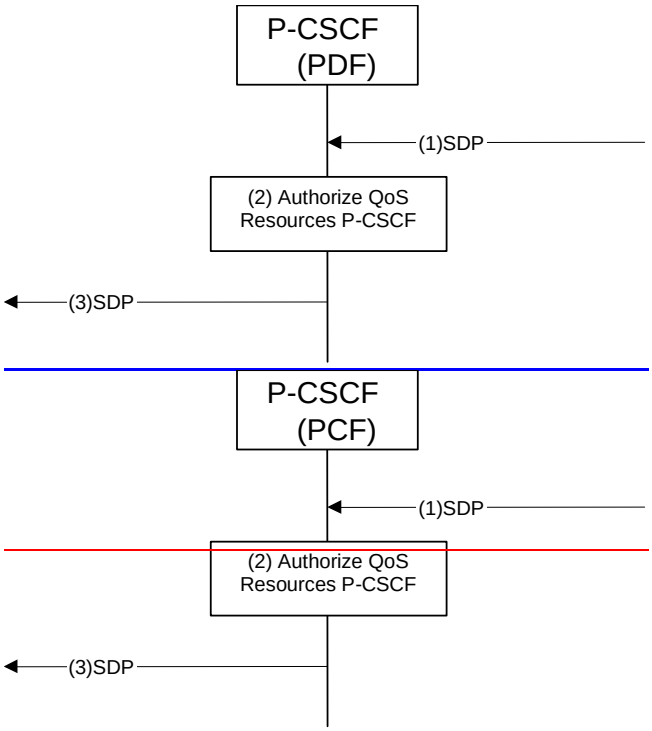


Figure 3: Authorize QoS Resources

1) A SIP message containing SDP payload is received by the P-CSCF.

2) The ~~PCF~~PDF shall authorize the required QoS resources for the session and install the IP bearer level policy based on information from the P-CSCF.

3) Upon successful authorization of the session, the P-CSCF forwards the SDP payload to the UE for the originating side. For the terminating side, the P-CSCF forwards the SDP payload to the terminating S-CSCF.

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 TS23.060.

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.

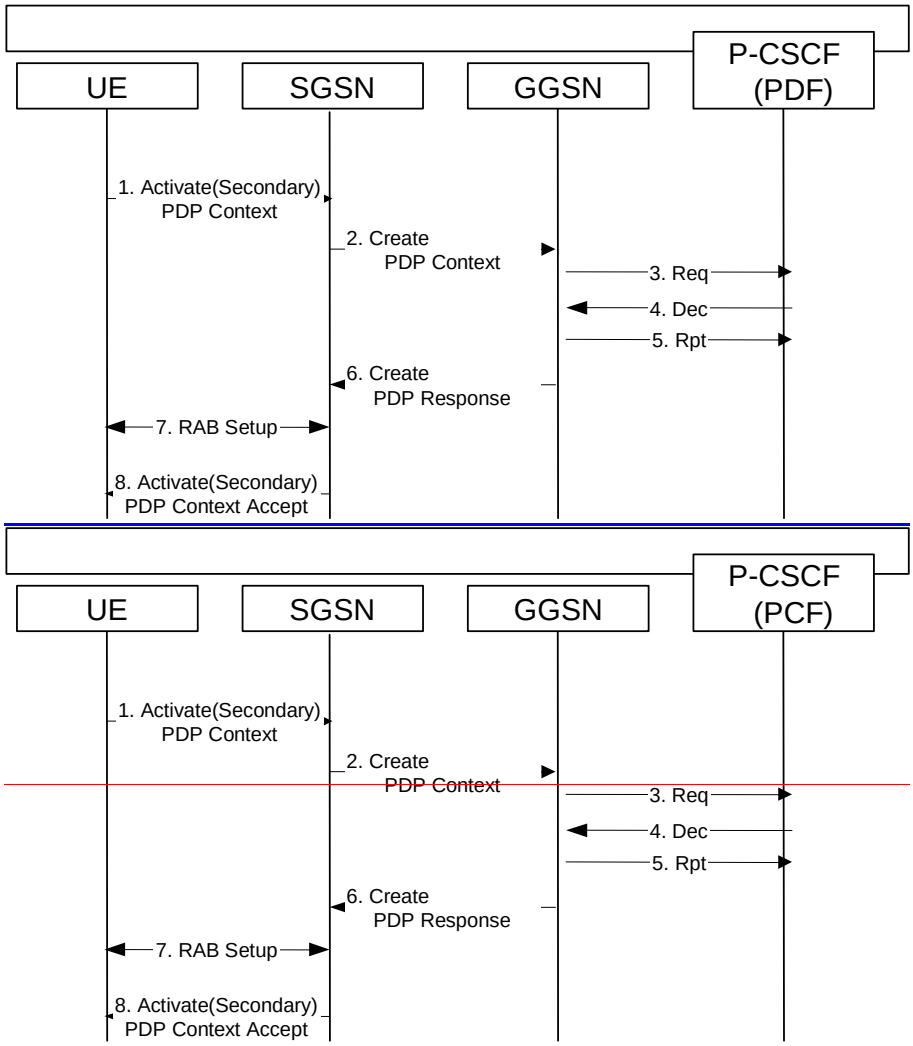


Figure 4: Resource Reservation with Service-based Local Policy

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 ~~PCF~~PDF in order to obtain relevant policy information.

4) The ~~PCF~~PDF sends a COPS DEC message back to the GGSN.

5) The GGSN sends a COPS RPT message back to the ~~PCF~~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.

7) RAB setup is done by the RAB Assignment procedure.

8) The SGSN sends an Activate (Secondary) PDP Context Accept message to UE.

6.3.2.2 Resource Reservation with End-to-End RSVP

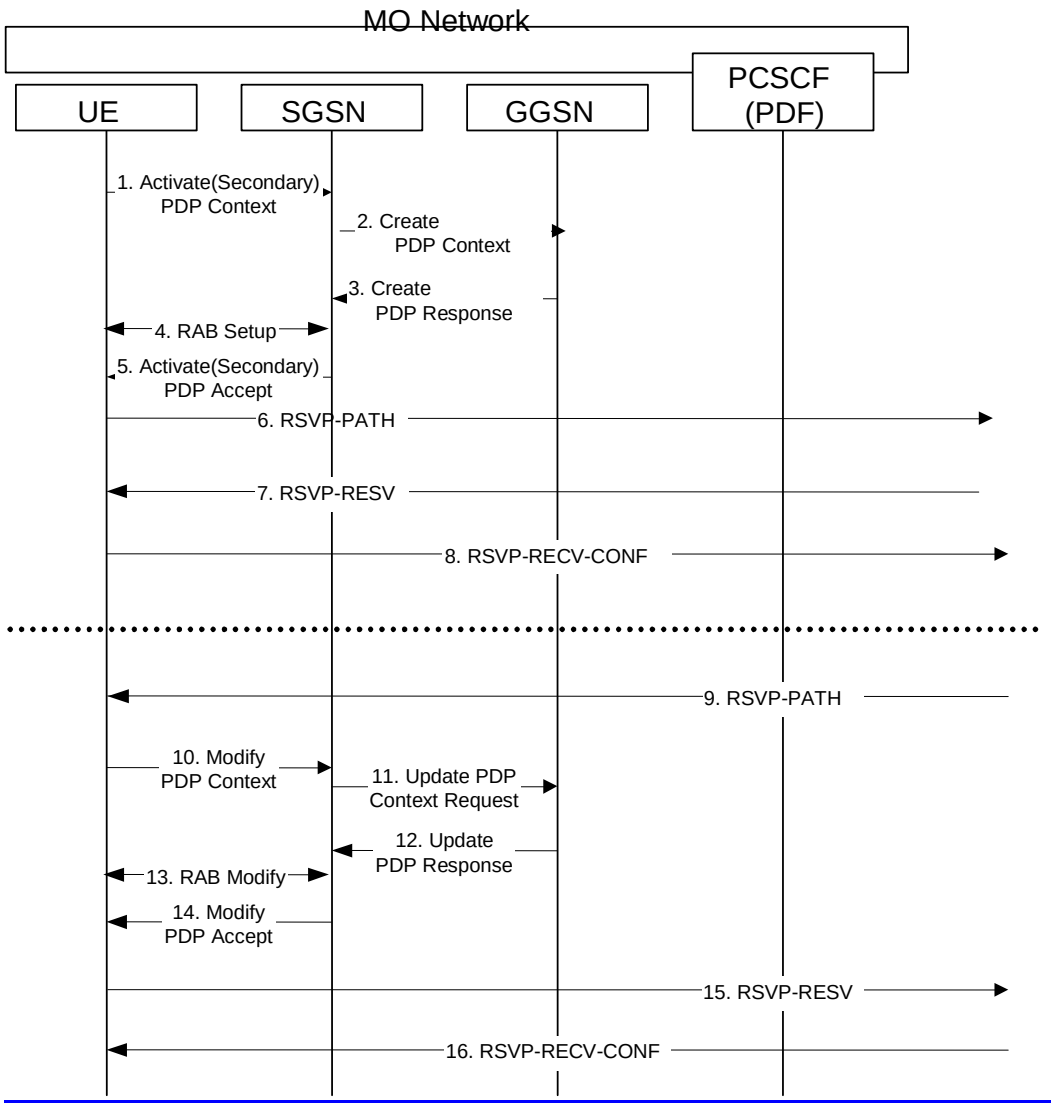
For this case, RSVP is added to the GPRS bearer establishment procedures specified in TS23.060, with no Service-based local policy.

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.


MO Network
UE
SGSN
GGSN
PCSCF (PDF)
1. Activate(Secondary) PDP Context
2. Create PDP Context
3. Create PDP Response
4. RAB Setup
5. Activate(Secondary) PDP Accept
6. RSVP-PATH
7. RSVP-RESV
8. RSVP-RECV-CONF
9. RSVP-PATH
10. Modify PDP Context
11. Update PDP Context Request
12. Update PDP Response
13. RAB Modify
14. Modify PDP Accept
15. RSVP-RESV
16. RSVP-RECV-CONF

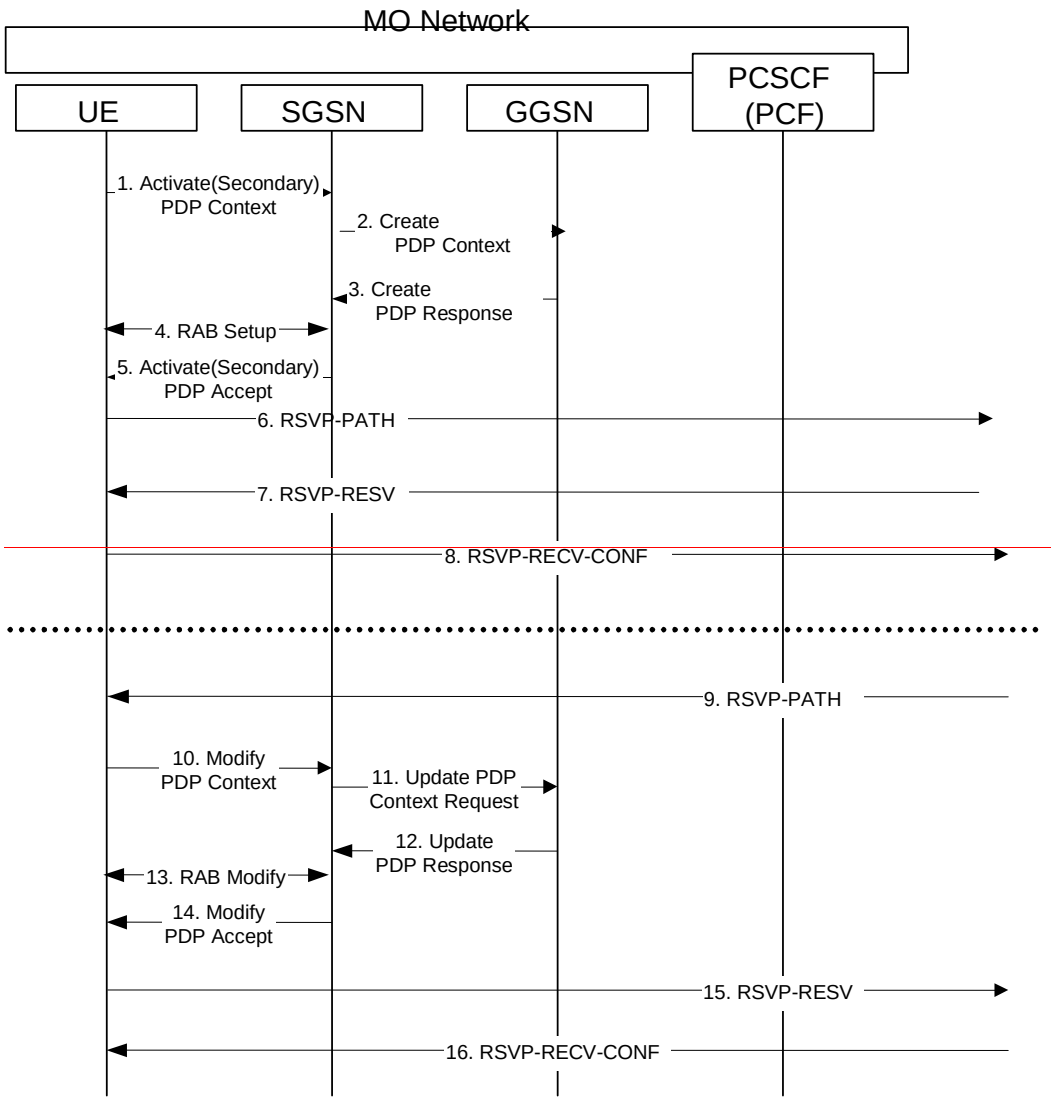


Figure 5: MO Resource Reservation with End-to-End RSVP

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.

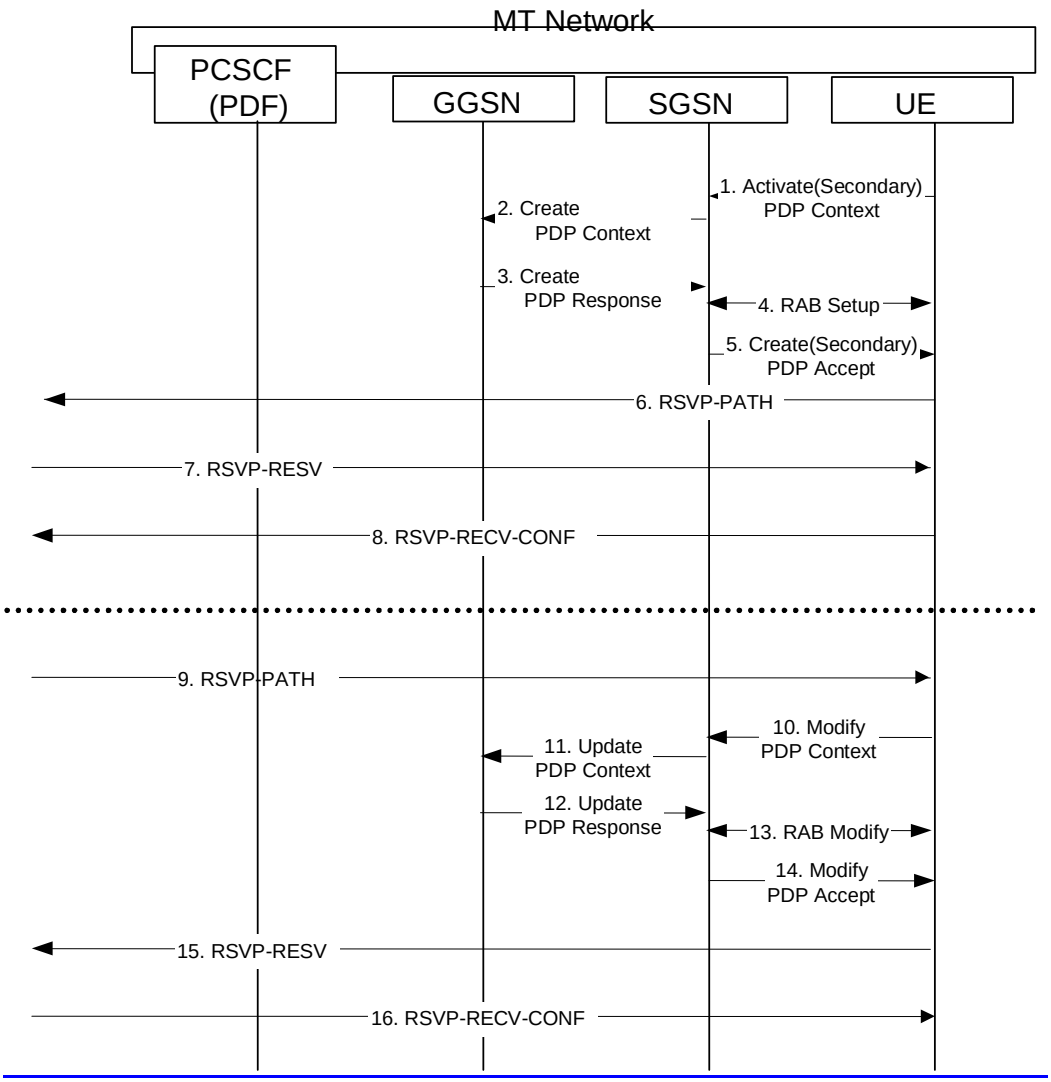
13) The radio access bearer modification may be performed by the RAB Assignment procedure.

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.


MT Network
PCSCF (PDF)
GGSN
SGSN
UE
1. Activate(Secondary) PDP Context
2. Create PDP Context
3. Create PDP Response
4. RAB Setup
5. Create(Secondary) PDP Accept
6. RSVP-PATH
7. RSVP-RESV
8. RSVP-RECV-CONF
9. RSVP-PATH
10. Modify PDP Context
11. Update PDP Context
12. Update PDP Response
13. RAB Modify
14. Modify PDP Accept
15. RSVP-RESV
16. RSVP-RECV-CONF

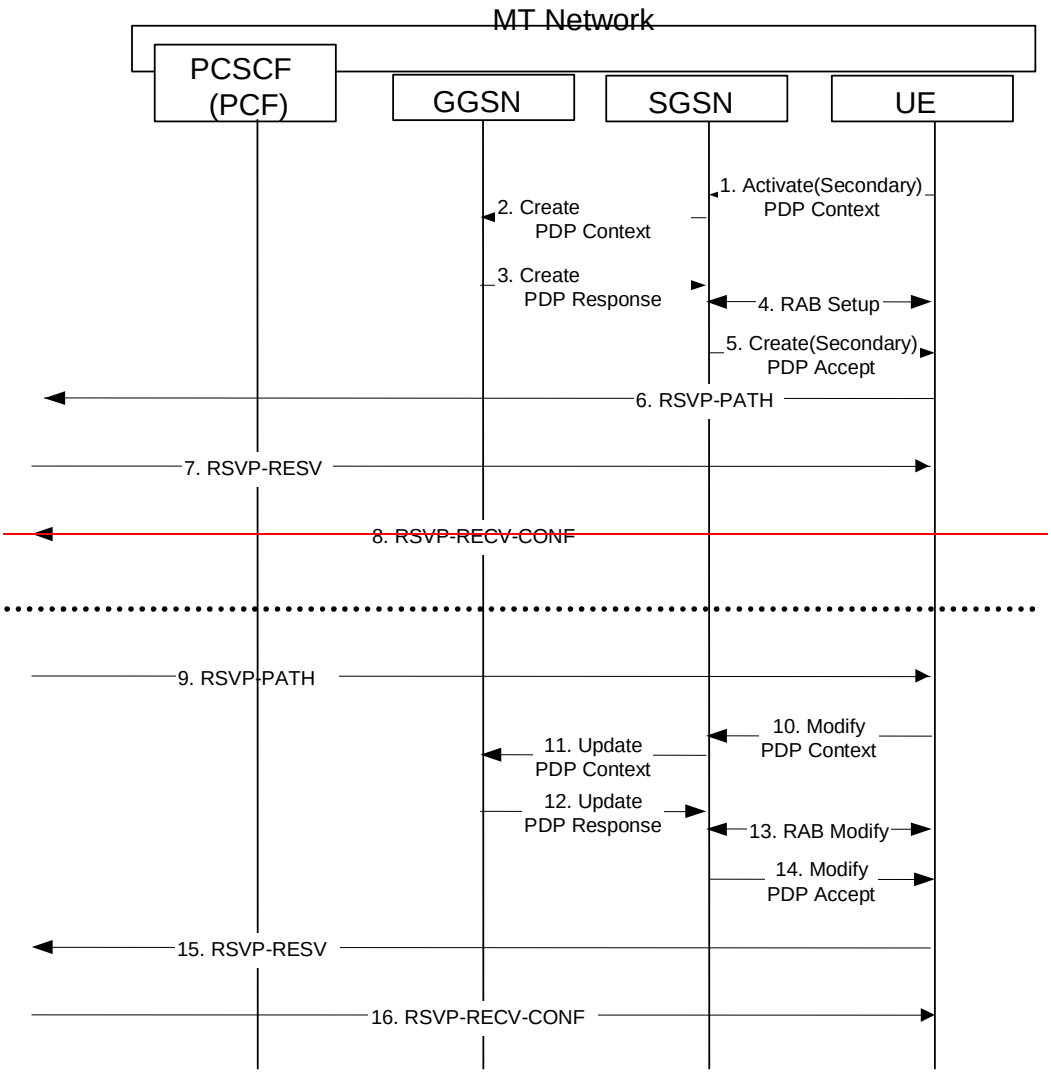


Figure 6: MT Resource Reservation with End-to-End RSVP

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

6.3.2.3 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 TS23.060.

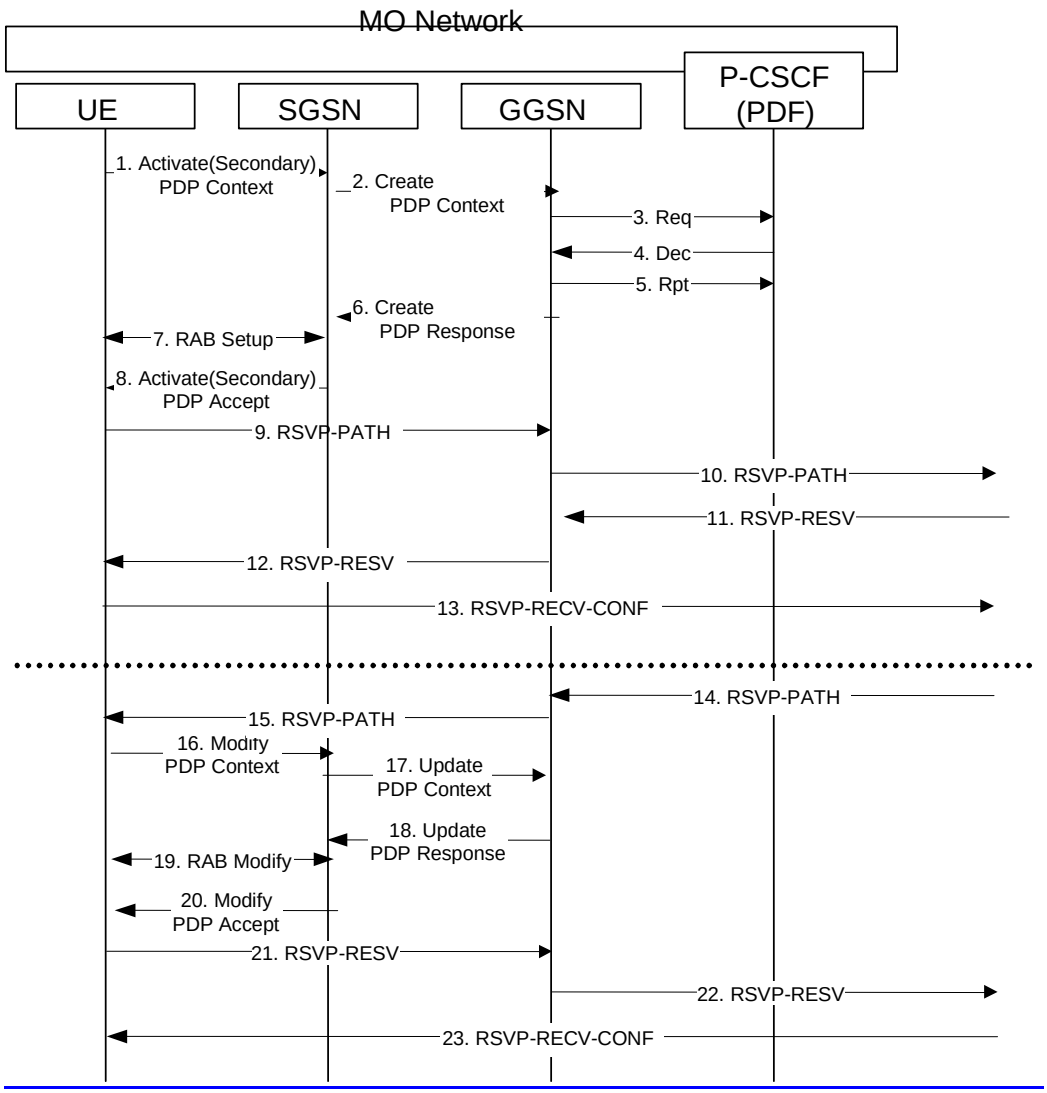
NOTE: The diagrams in this subsection depict one possible signalling sequence, however, the alternative signalling sequences below are possible:

- 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.


MO Network
UE
SGSN
GGSN
P-CSCF (PDF)
1. Activate(Secondary) PDP Context
2. Create PDP Context
3. Req
4. Dec
5. Rpt
6. Create PDP Response
7. RAB Setup
8. Activate(Secondary) PDP Accept
9. RSVP-PATH
10. RSVP-PATH
11. RSVP-RESV
12. RSVP-RESV
13. RSVP-RECV-CONF
14. RSVP-PATH
15. RSVP-PATH
16. Modify PDP Context
17. Update PDP Context
18. Update PDP Response
19. RAB Modify
20. Modify PDP Accept
21. RSVP-RESV
22. RSVP-RESV
23. RSVP-RECV-CONF

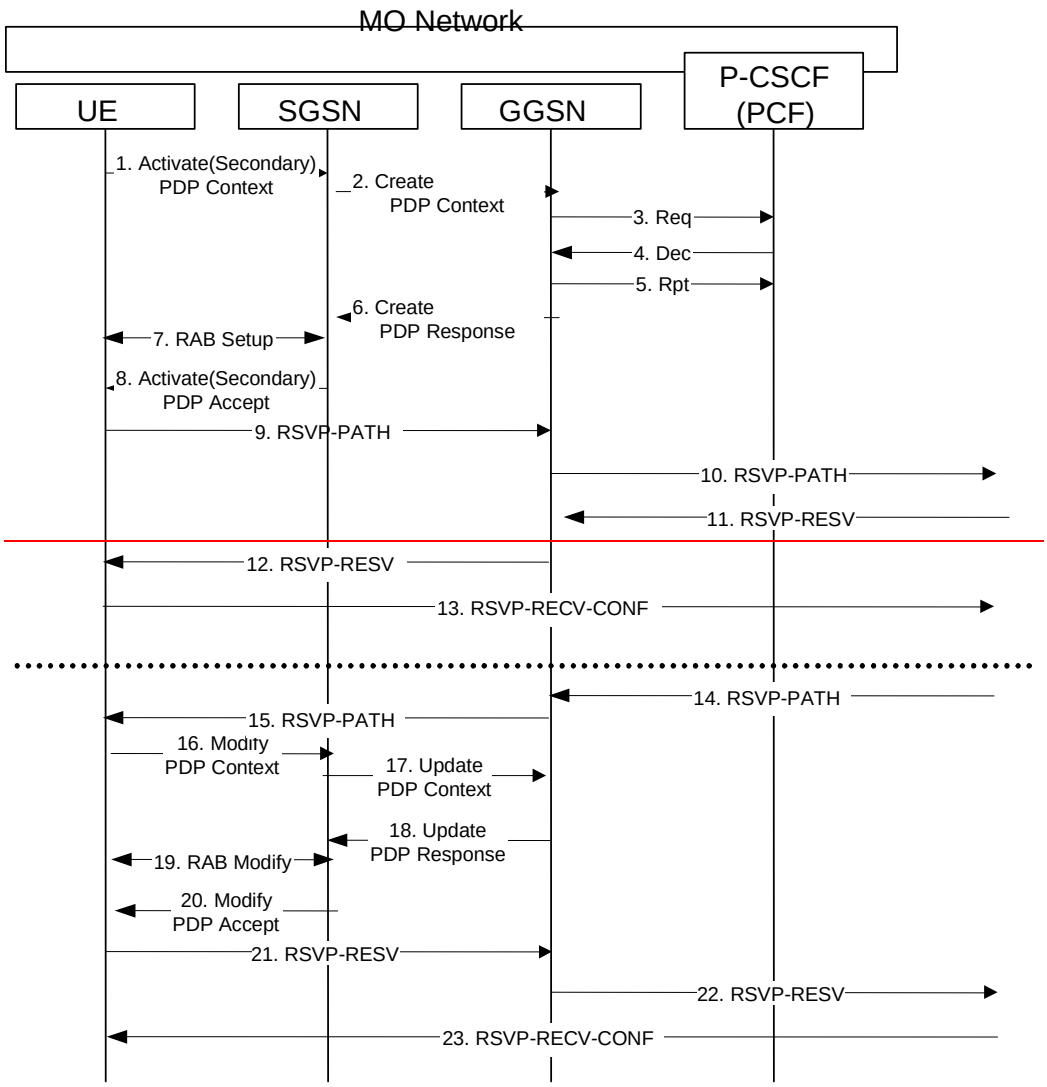


Figure 7: MO Resource Reservation with End-to-End RSVP and Service-based Local Policy

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 ~~PCF~~PDF in order to obtain relevant policy information.

4) The ~~PCF~~PDF sends a COPS DEC message back to the GGSN.

5) The GGSN sends a COPS RPT message back to the ~~PCF~~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 ~~PCF~~PDF again. Otherwise the GGSN may have to query the ~~PCF~~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 ~~PCF~~PDF again. Otherwise the GGSN may have to query the ~~PCF~~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 ~~PCF~~PDF again. Otherwise the GGSN may have to query the ~~PCF~~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.

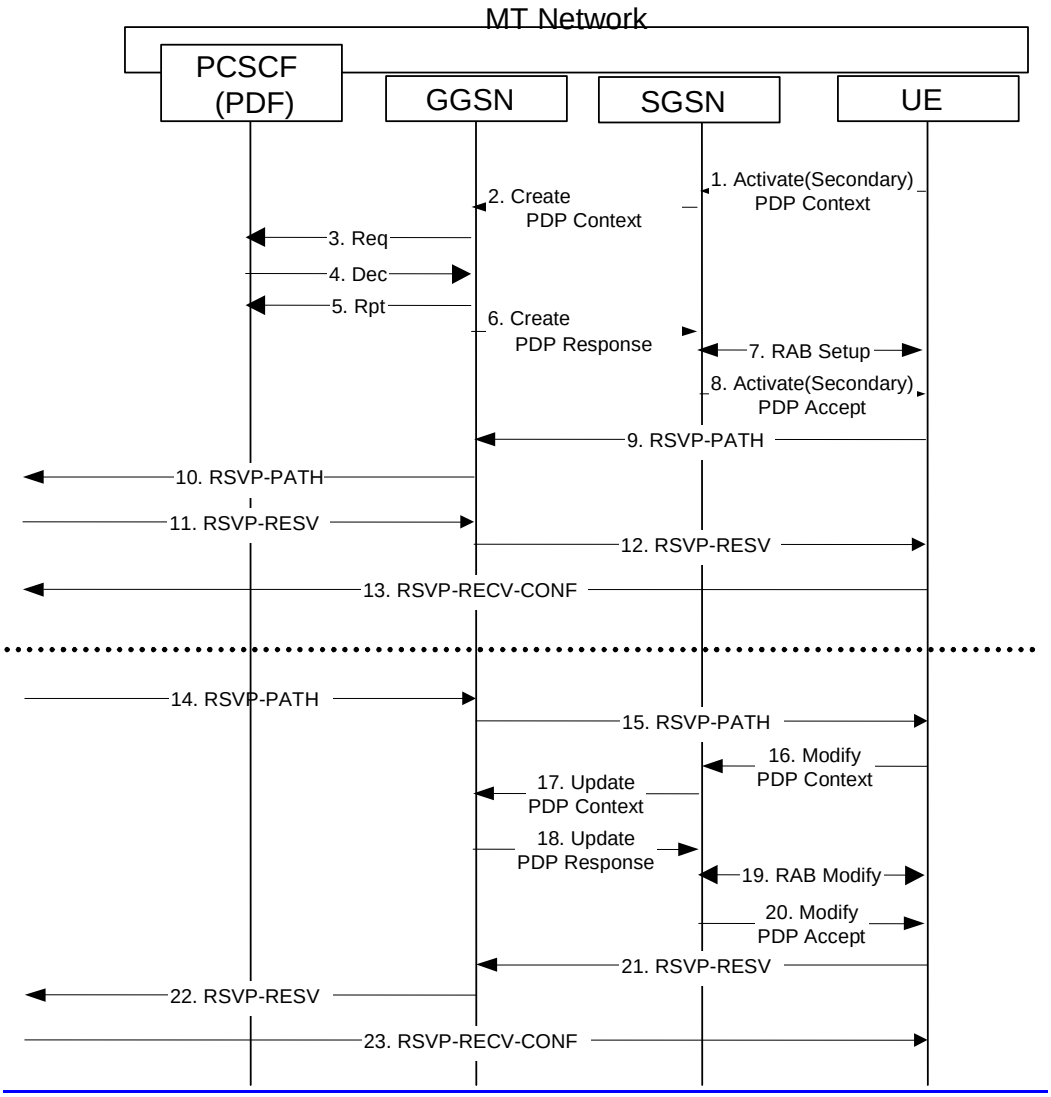
21) The UE sends a RSVP RESV message to the GGSN. The UE includes the Binding Information in the RSVP RESV message.

NOTE: If the decision was previously cached locally at the GGSN, it may not be necessary to query the ~~PCF~~PDF again. Otherwise the GGSN may have to query the ~~PCF~~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.


MT Network
PCSCF (PDF)
GGSN
SGSN
UE
1. Activate(Secondary) PDP Context
2. Create PDP Context
3. Req
4. Dec
5. Rpt
6. Create PDP Response
7. RAB Setup
8. Activate(Secondary) PDP Accept
9. RSVP-PATH
10. RSVP-PATH
11. RSVP-RESV
12. RSVP-RESV
13. RSVP-RECV-CONF
14. RSVP-PATH
15. RSVP-PATH
16. Modify PDP Context
17. Update PDP Context
18. Update PDP Response
19. RAB Modify
20. Modify PDP Accept
21. RSVP-RESV
22. RSVP-RESV
23. RSVP-RECV-CONF

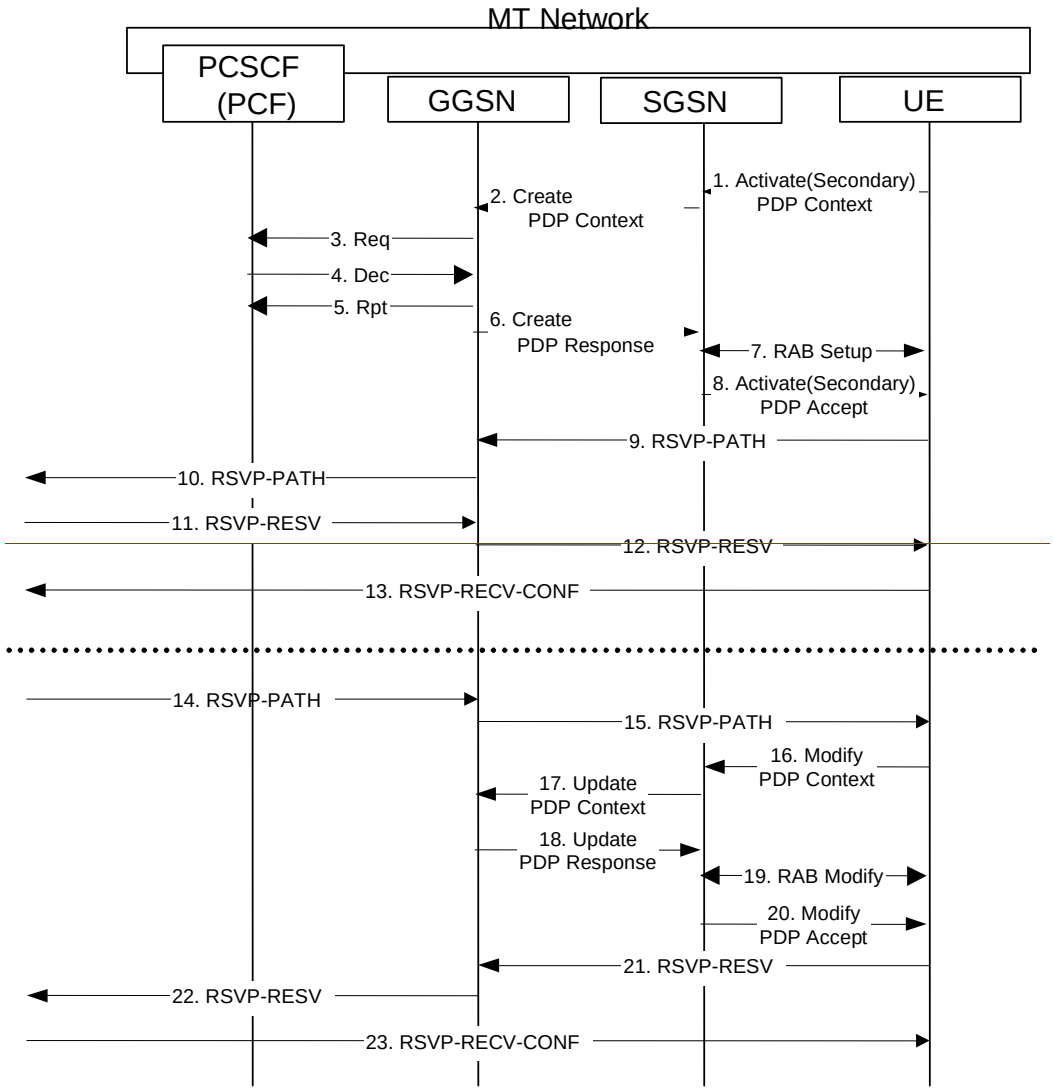


Figure 8: MT Resource Reservation with End-to-End RSVP and Service-based Local Policy

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

6.3.2.4 (void)

6.3.3 Approval of QoS Commit

The Approval of QoS Commit procedure is triggered by the P-CSCF receiving a 200 OK response to the INVITE request.

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

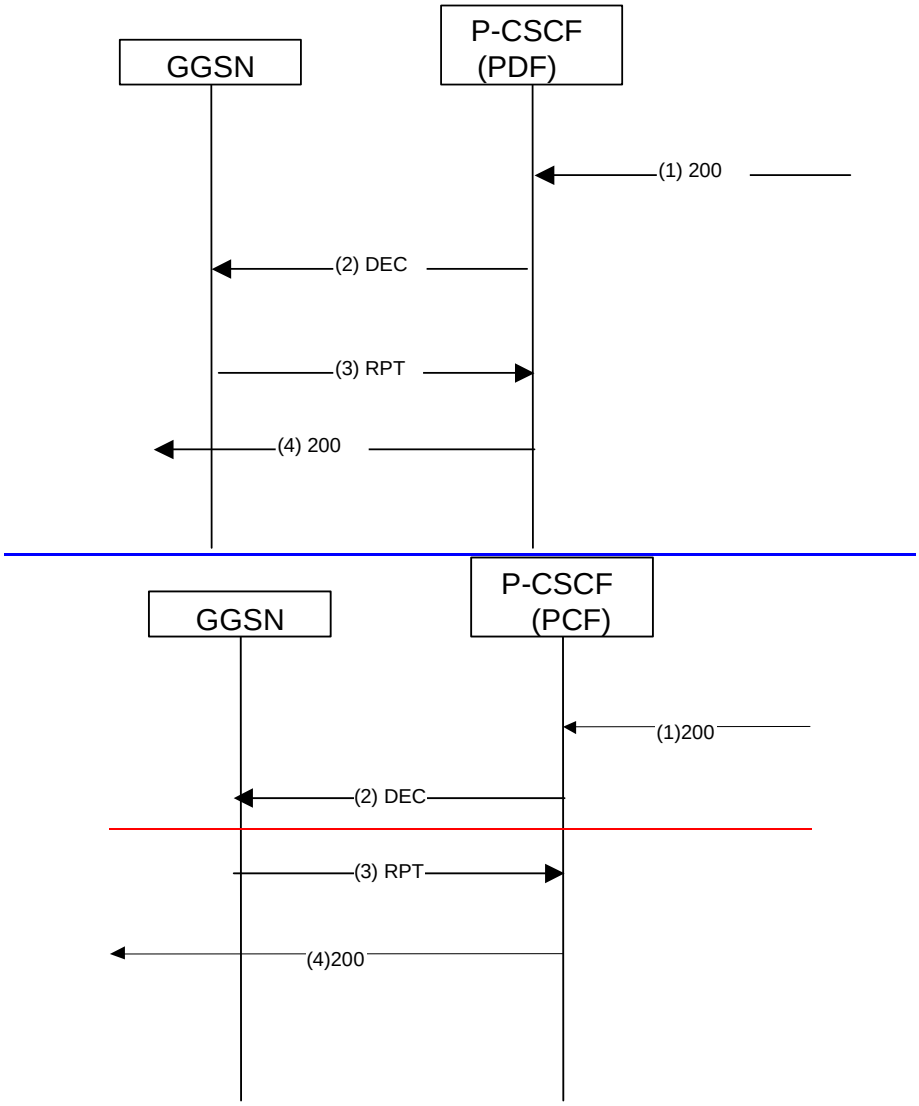


Figure 11: Approval of QoS Commit

1) The P-CSCF receives the 200 OK response to the INVITE request. ~~PCF~~PDF approves the QoS Commit based on local policy.

2) The ~~PCF~~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.

3) 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 ~~PCF~~PDF.

4) 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 Removal of QoS Commit

The "Removal of QoS commit" procedure is used e.g. when a media component of a session is put on hold (e.g. in case of a media re-negotiation or call hold). The P-CSCF (~~PCF~~PDF) provides final decision on removal of QoS commit for the authorized media stream to the GGSN. The ~~PCF~~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.

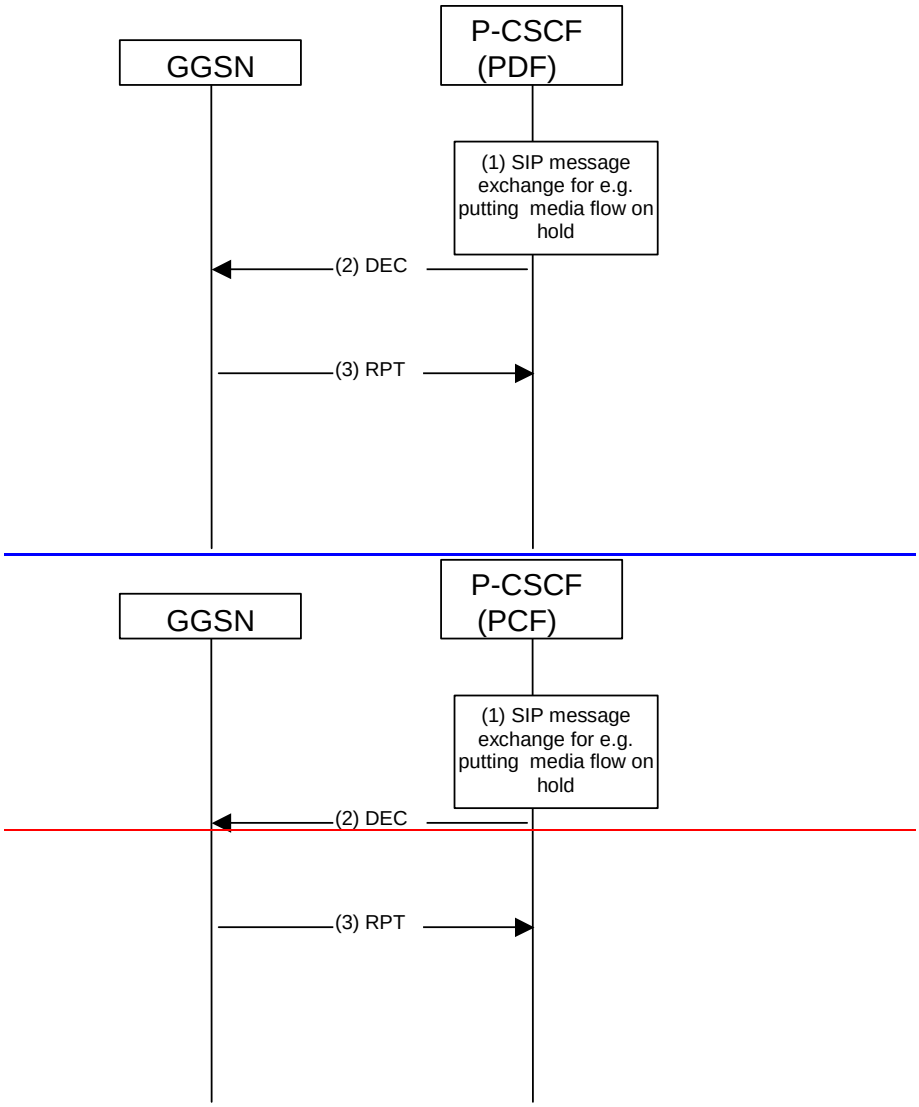


Figure 12: Removal of QoS commit

1) SIP message exchanges for e.g., putting a media flow on hold are carried out.
2) The ~~PCF~~PDF shall send a COPS DEC message to the GGSN to close the 'gate'.
3) The GGSN receives the COPS DEC message, closes the gate, and sends a COPS RPT message back to the ~~PCF~~PDF.

6.3.5 Revoke Authorization for GPRS and IP Resources

The "Revoke Authorization for GPRS and IP resources" procedure is used e.g. upon IMS session release. The ~~PCF~~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).

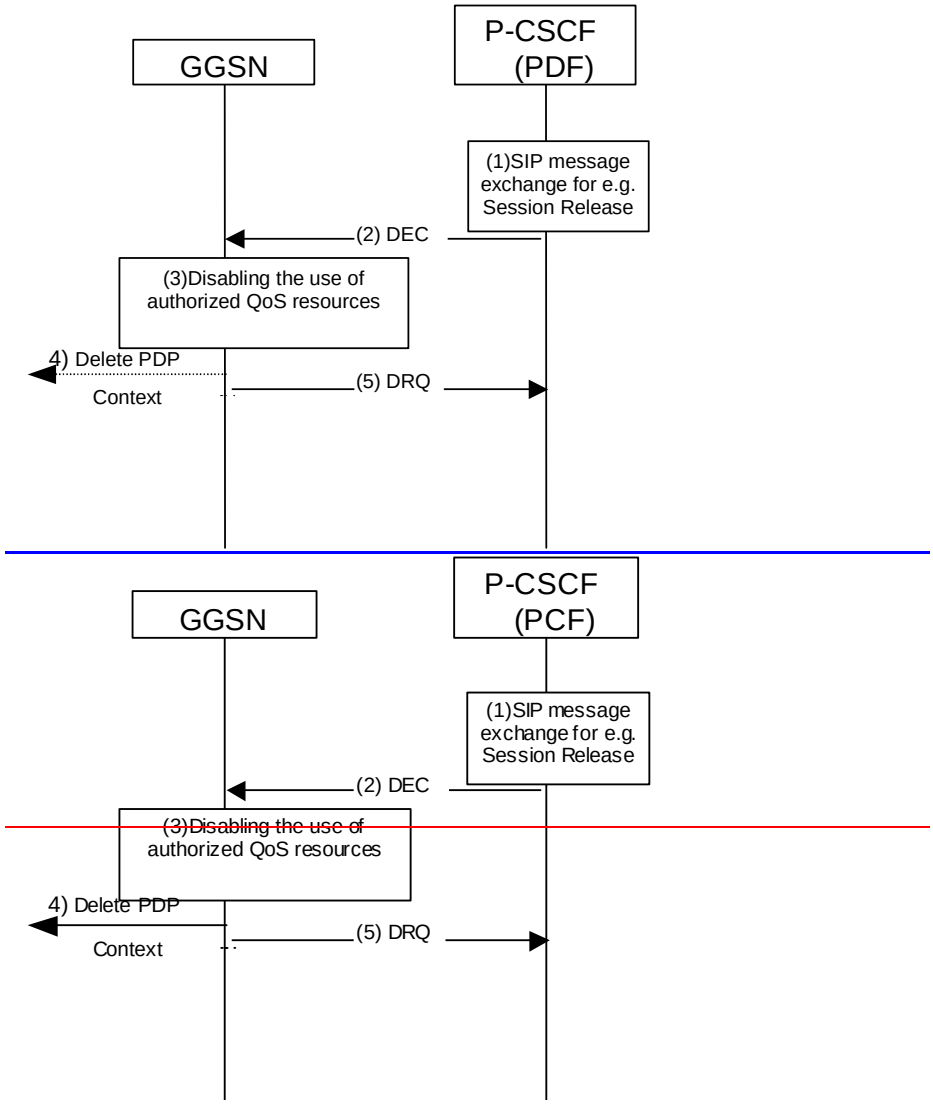


Figure 13: Revoke Authorization for GPRS and IP Resources

1) SIP message exchanges for e.g. session release are carried out.

2) The ~~PCF~~PDF shall send a COPS DEC (Decision) message containing revoke command to the GGSN. 3) The GGSN receives the COPS DEC message, and disables the use of the authorized QoS resources.

4) The GGSN initiates deactivation of the PDP context used for the IP multimedia session, in case the UE has not done it before.

5) Upon deactivation of the PDP Context, the GGSN sends a COPS DRQ (Delete Request State) message back to the ~~PCF~~PDF.

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 ~~PCF~~PDF.

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

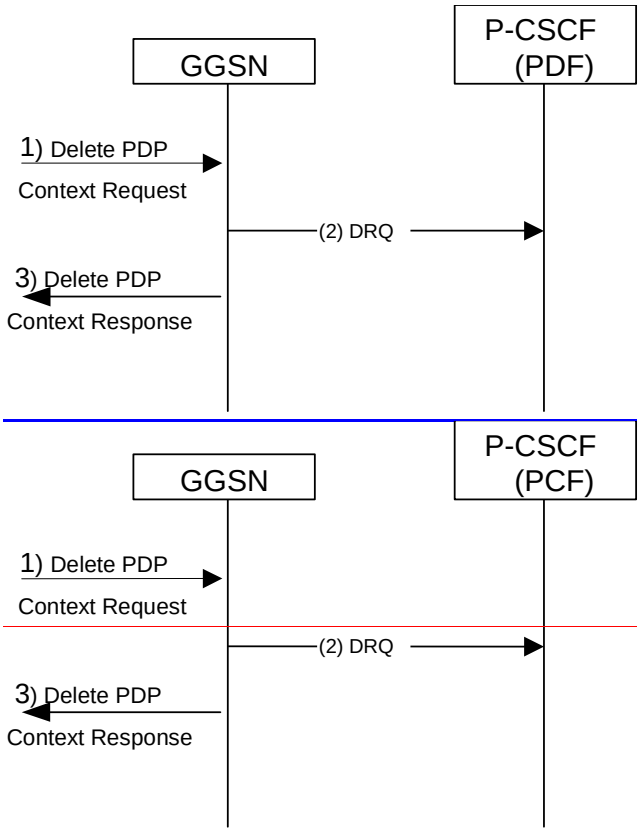


Figure 14: Indication of PDP Context Release

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 P-CSCF(~~PCF~~PDF).
3) 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 ~~PCF~~PDF as described below. The following figures present the "Authorization of PDP Context Modification" procedure.

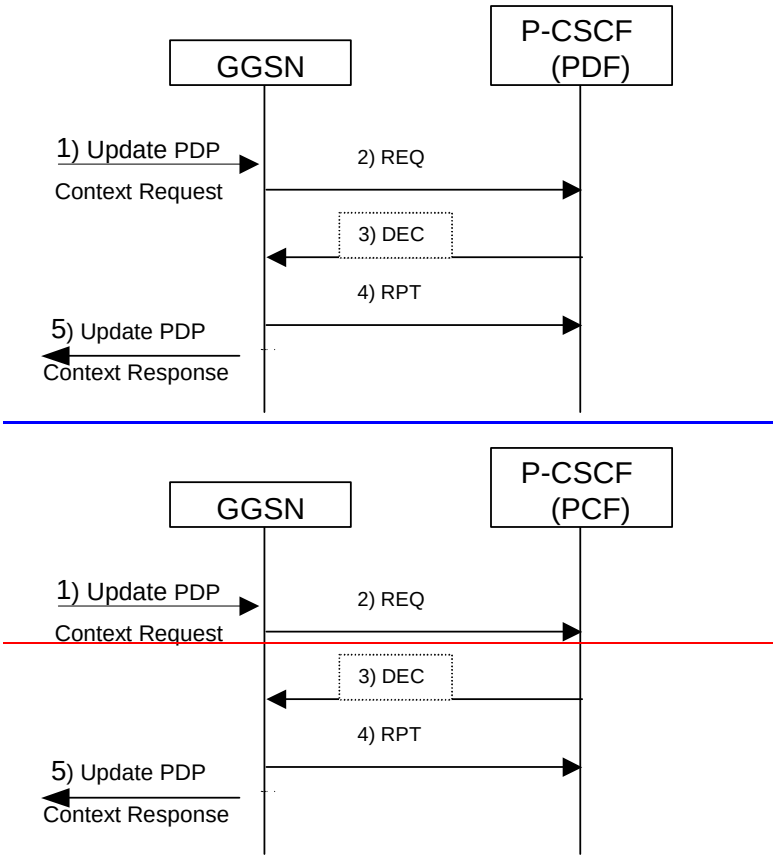


Figure 14a: Authorization of PDP Context Modification

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 P-CSCF(~~PCF~~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 P-CSCF(~~PCF~~PDF).

3) The P-CSCF(~~PCF~~PDF) receives the COPS REQ message, notes the requested modification and informs the GGSN of the authorization decision.

4) The GGSN sends a COPS RPT message back to the P-CSCF(~~PCF~~PDF).

5) If the P-CSCF(~~PCF~~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 ~~PCF~~PDF as described below. The following figures present the “Indication of PDP Context Modification” procedure.

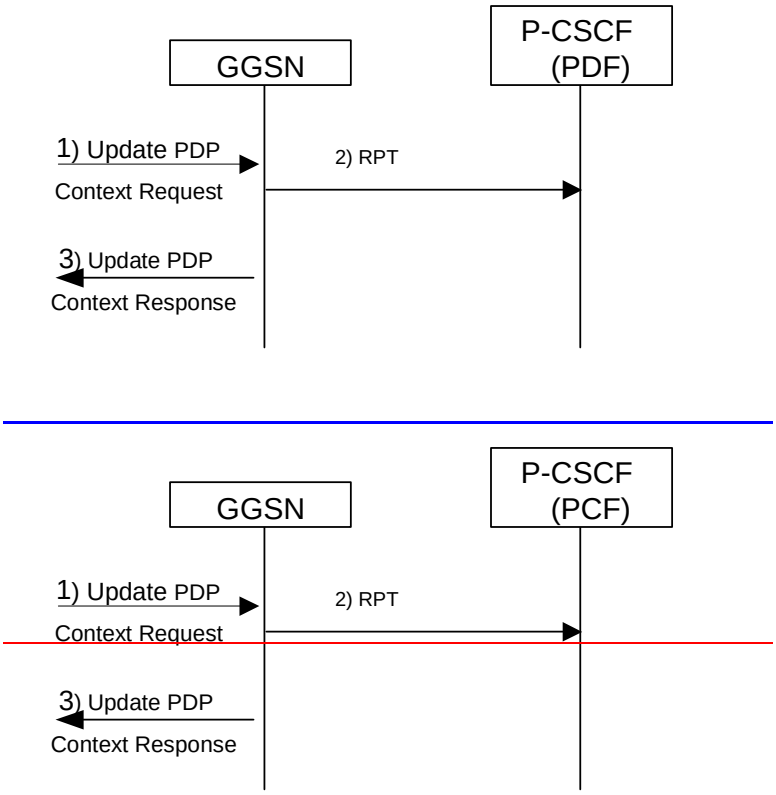


Figure 15: Indication of PDP Context Modification

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 P-CSCF(~~PCF~~PDF) to indicate the state changes of the PDP context.

3) The GGSN sends the Update PDP Context Response message to the SGSN to acknowledge the PDP context modification.

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 signalling flag shall be a standardised static information.

In the case of IMS, the signalling flag is used to reference rules and restrictions on the PDP context used for application level signalling, as described in 23.228 section 4.2.6.

The signalling flag and the QoS profile parameters detailed in TS23.107 may be used independently of each other.

**********Next Change**********

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. TS23.228 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 corresponding RSVP signalling parameters as well as the PDP context parameters.

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).

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.

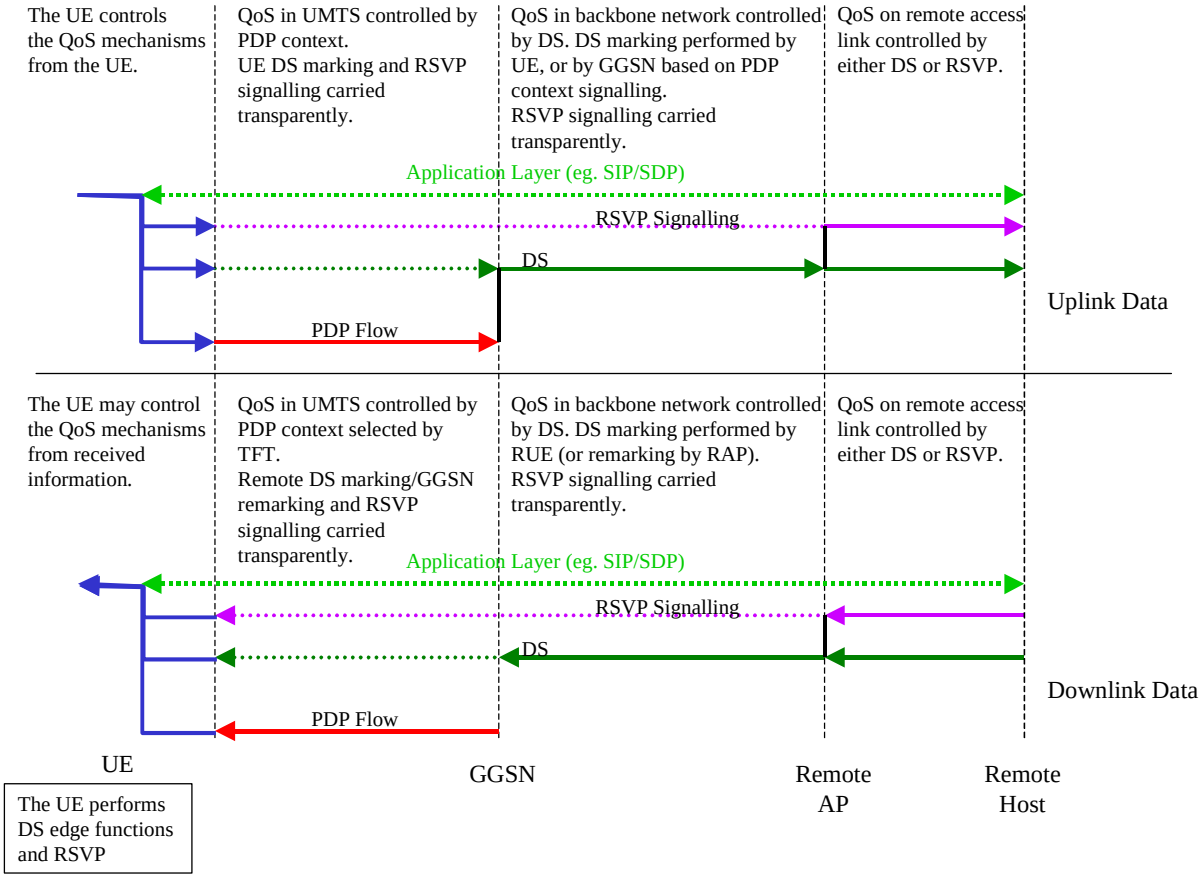
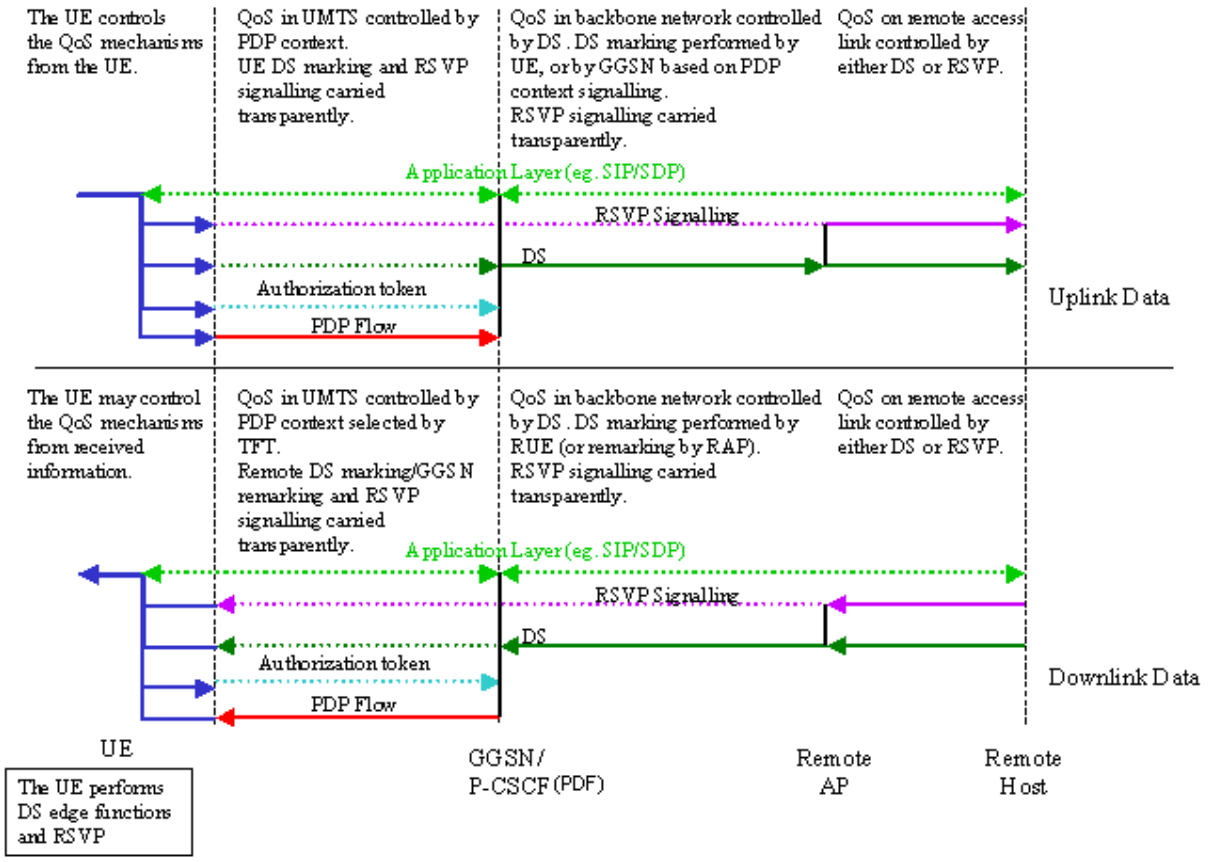


Figure A.4: Local UE supports RSVP signalling with IntServ semantics, and DiffServ; without service based policy

When the authorisation token is included in the PDP context establishment/modification (as per section 5.1.1.2.3), the GGSN may use IP level information provided by service based local policy according to the authorisation token to configure the DiffServ classifier functionality. The information can also be used for DiffServ class admission control, e.g., the requested end-to-end bandwidth from the UE for a particular flow may be informed to the GGSN beforehand for the GGSN DiffServ edge to determine if the flow can be allowed to a certain DiffServ class or to/from an ingress/egress point.

The application layer signaling may be processed in the local network at an application server such as the P-CSCF in the case of SIP signaling. 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 ~~PCF~~PDF policy function co-located in the P-CSCF, as shown in the figure below.


The UE controls the QoS mechanisms from the UE.
QoS in UMTS controlled by PDP context.
UE DS marking and RSVP signalling carried transparently.
QoS in backbone network controlled by DS. DS marking performed by UE, or by GGSN based on PDP context signalling.
RSVP signalling carried transparently.
QoS on remote access link controlled by either DS or RSVP.
Application Layer (eg. SIP/SDP)
RSVP Signalling
DS
Authorization token
PDP Flow
Uplink Data
The UE may control the QoS mechanisms from received information.
QoS in UMTS controlled by PDP context selected by TFT.
Remote DS marking/GGSN remarking and RSVP signalling carried transparently.
QoS in backbone network controlled by DS. DS marking performed by RUE (or remarking by RAP).
RSVP signalling carried transparently.
QoS on remote access link controlled by either DS or RSVP.
Application Layer (eg. SIP/SDP)
RSVP Signalling
DS
Authorization token
PDP Flow
Downlink Data
UE
GGSN/ P-CSCF (PDF)
Remote AP
Remote Host
The UE performs DS edge functions and RSVP

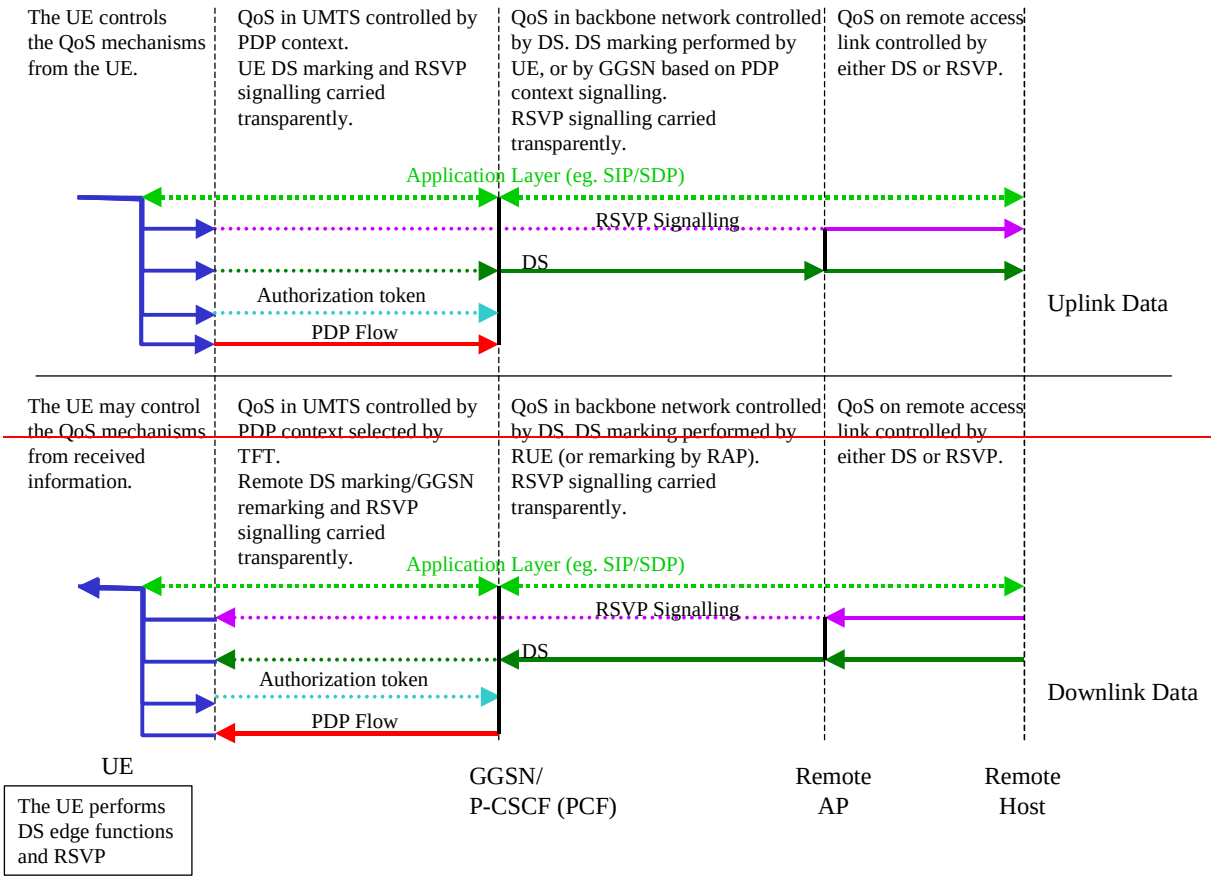

The UE controls the QoS mechanisms from the UE.
QoS in UMTS controlled by PDP context.
UE DS marking and RSVP signalling carried transparently.
QoS in backbone network controlled by DS. DS marking performed by UE, or by GGSN based on PDP context signalling.
RSVP signalling carried transparently.
QoS on remote access link controlled by either DS or RSVP.
Application Layer (eg. SIP/SDP)
RSVP Signalling
DS
Authorization token
PDP Flow
Uplink Data
The UE may control the QoS mechanisms from received information.
QoS in UMTS controlled by PDP context selected by TFT.
Remote DS marking/GGSN remarking and RSVP signalling carried transparently.
QoS in backbone network controlled by DS. DS marking performed by RUE (or remarking by RAP).
RSVP signalling carried transparently.
QoS on remote access link controlled by either DS or RSVP.
Application Layer (eg. SIP/SDP)
RSVP Signalling
DS
Authorization token
PDP Flow
Downlink Data
UE
GGSN/ P-CSCF (PCF)
Remote AP
Remote Host
The UE performs DS edge functions and RSVP

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. TS23.228 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 corresponding RSVP signalling parameters and the PDP context parameters.

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).

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 use IP level information provided by service based local policy according to the authorisation token to authorise the RSVP session and configure the Diffserv classifier functionality. The information may also be used in conjunction with a Diffserv aggregate to enable DiffServ class admission control, e.g., the requested end-to-end bandwidth from the UE for a particular flow may be informed to the GGSN beforehand for the GGSN DiffServ edge to determine if the flow can be allowed to a certain DiffServ class or to/from an ingress/egress point.

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.

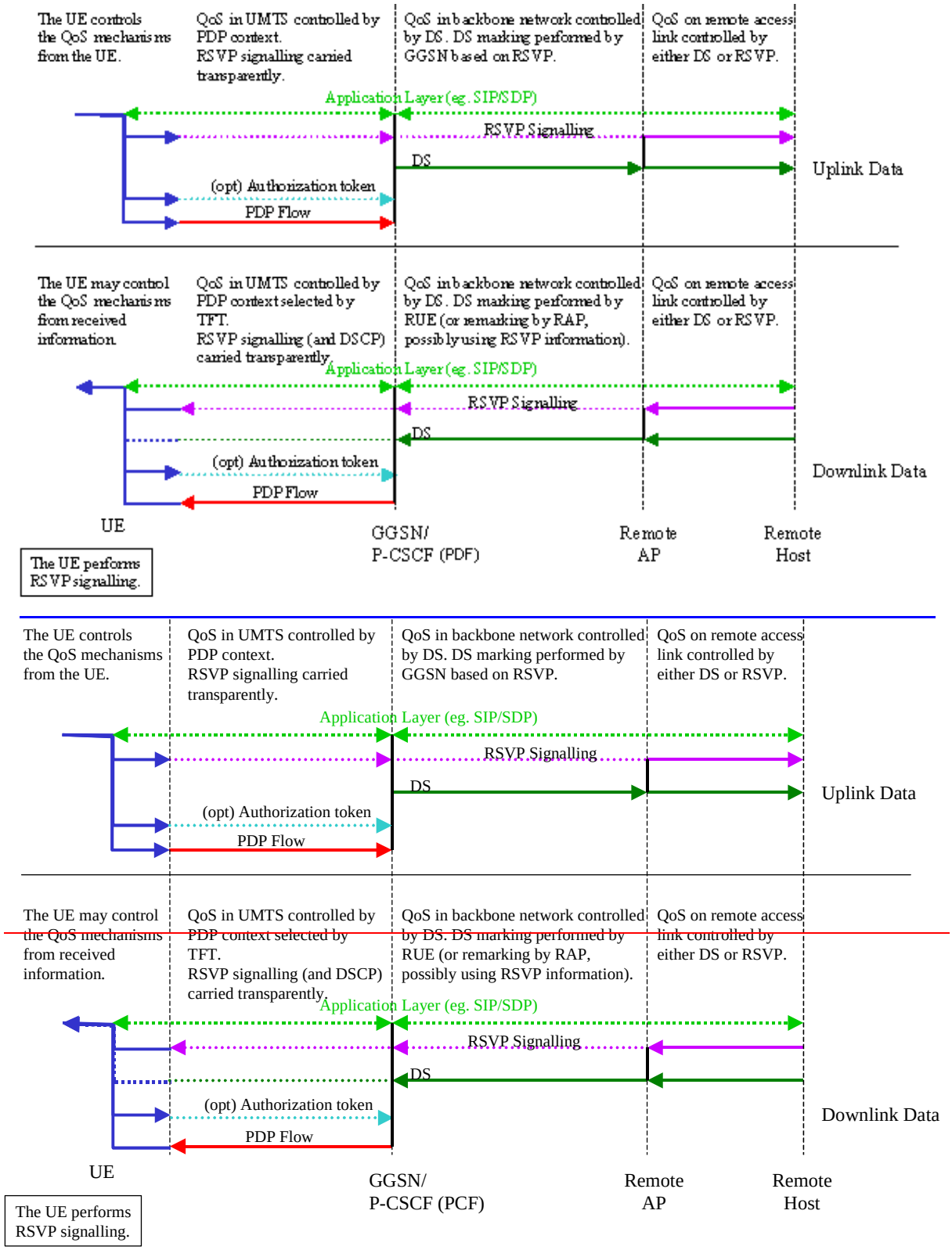


Figure A.6: Local UE supports RSVP signalling using IntServ Semantics

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, to enhance the interworking options to the DiffServ edge function of the GGSN. The GGSN uses the authorization token to obtain a policy decision from the P-CSCF(~~PCF~~PDF) which will be used to derive IP level information. This is done via the standardized interface between the ~~PCF~~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.

In addition, IP level information may also be derived from PDP context (e.g. QoS parameters).

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. TS23.228 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.

The GGSN DiffServ edge function may use the IP level information (e.g., 5-tuple combination of source and destination IP address, source and destination port number, and the protocol identifier) provided by service based local policy according to the authorisation token to configure the DiffServ classifier functionality. The information can be used for DiffServ class admission control, e.g., for the GGSN DiffServ edge to determine if the flow can be allowed to a certain DiffServ class or to/from an ingress/egress point. As a result, the GGSN may select the appropriate DiffServ setting to apply. This is shown in the figure below.

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).

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 uses the IP level information to interwork with DiffServ in 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.

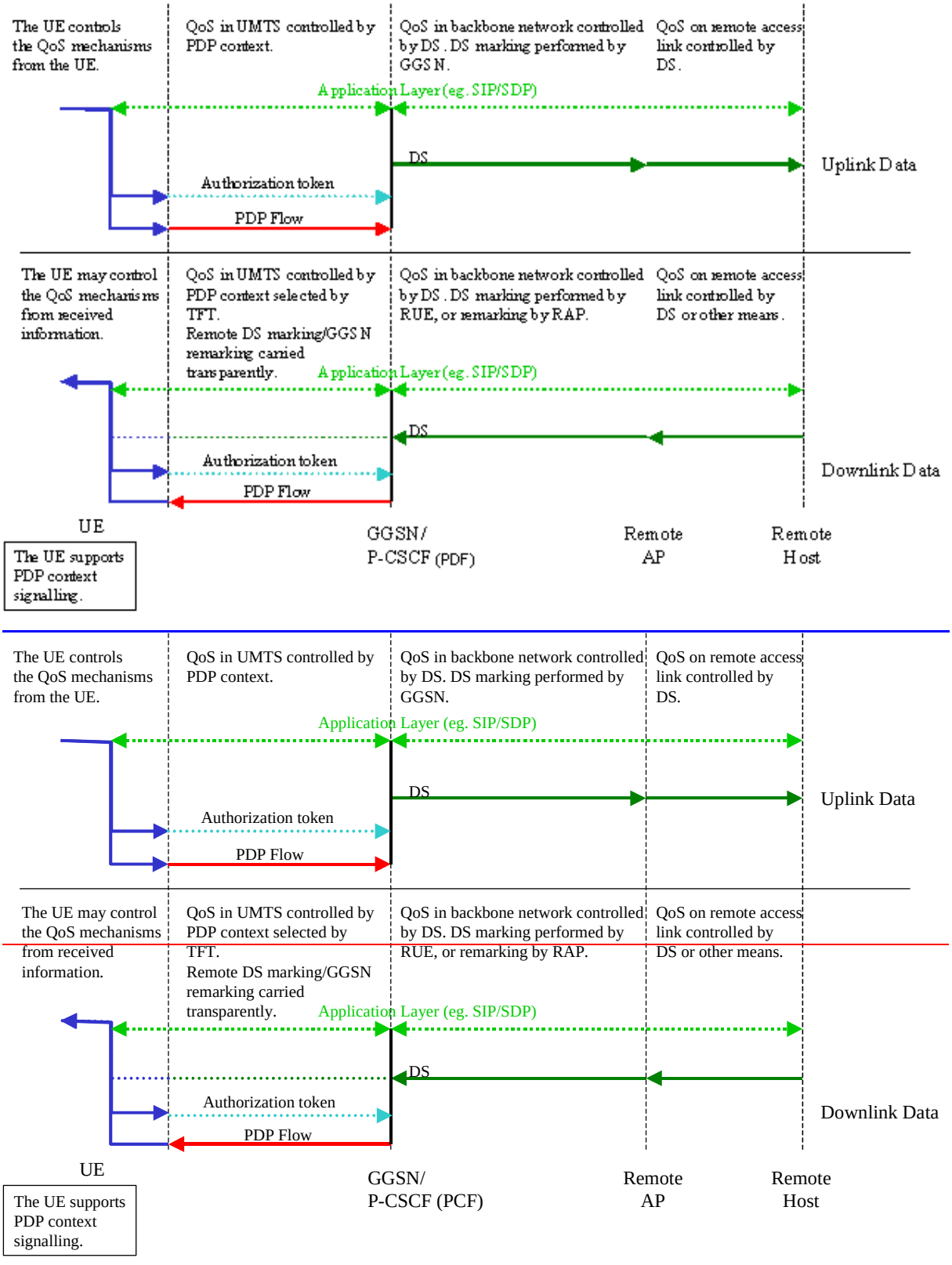


Figure A.7: Local UE provides authorization token in PDP context activation/modification message and GGSN provides interworking with DiffServ

3GPP TSG-S2#27
Beijing, China, 14th – 18th October 2002

Tdoc ⌘ S2-023065

CR-Form-v7

CHANGE REQUEST

⌘ **TS 23.207** **CR** **48** ⌘ **rev** **1** ⌘ Current version: **5.5.0** ⌘

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

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

Title:	⌘	Consistency of stage 2 – RSVP proxy
Source:	⌘	Nortel Networks
Work item code:	⌘	E2EQoS
Date:	⌘	11/10/2002
Category:	⌘	**F**
Release:	⌘	REL-5

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

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	S2-022293 (CR 45 to 23.207) removed the stage 2 items related to scenario 6 in appendix A and the functionality related to the RSVP proxy capability. However, references to the scenario 6 are still present in the spec.
Summary of change:	⌘	Removing references to scenario 6 (RSVP proxy).
Consequences if not approved:	⌘	The stage 2 specification is inconsistent.

Clauses affected:	⌘	A.1, A.2

		Y	N		
Other specs affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	

Other comments:	⌘	

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

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 UTMS 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 ~~and 6~~ 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. ~~Scenario 6 has been postponed to a future release.~~

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

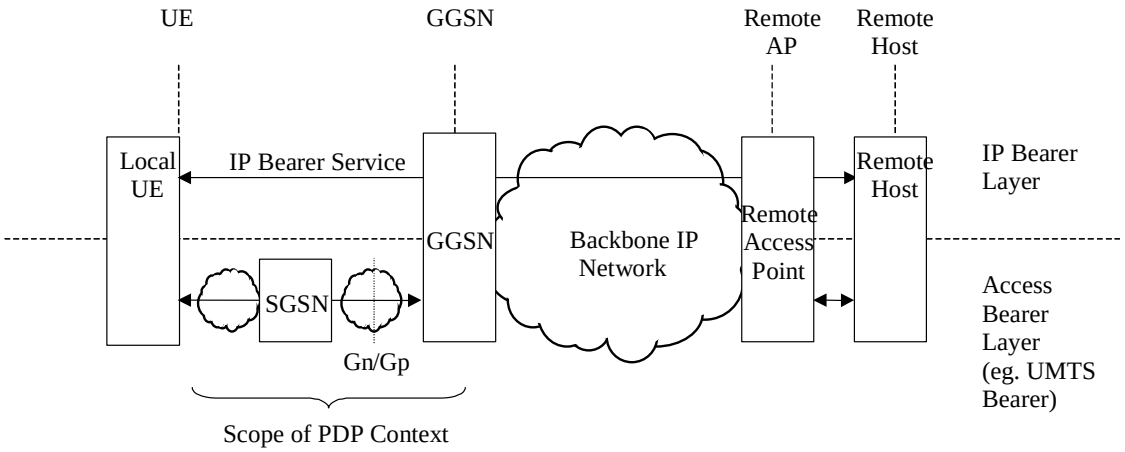


Figure A.1: Network Architecture for QoS Conceptual Models

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

[Editor's NOTE: the precedence and sequence of the different phases of session / bearer establishment need further study.]

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~~s~~ 5 ~~and 6~~). 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~~6~~.

NOTE: Scenario 5 ~~and 6~~ is reserved for the IP multimedia services involving, e.g., SIP signalling , IP policy control, and subscription checking.

3GPP TSG-S2#27
Beijing, China, October 14th – 18th, 2002

Tdoc ⌘ S2-023064

CR-Form-v7

CHANGE REQUEST

⌘ **TS 23.207** **CR** **044** ⌘**rev** **3** ⌘ Current version: **5.5.0** ⌘

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

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

Title:	⌘	Alignment with stage 3 – DS control over Go
Source:	⌘	Ericsson, Nokia
Work item code:	⌘	E2EQoS
Date:	⌘	2002-10-15
Category:	⌘	**F**
Release:	⌘	REL-5

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

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	This contribution aligns TS 23.207 with the stage 3 specification TS 29.207.
Summary of change:	⌘	QoS information is only provided for the combined set of flows requested by the GGSN.
Consequences if not approved:	⌘	The stage 2 specification is not aligned with the stage 3 specification.

Clauses affected:	⌘	5.1.1.3, 5.2.1, 5.2.3, 5.3.1, 5.3.2, 6.1.1, A.2.3, A.2.5, C

Other specs affected:	Y	N		
⌘		X	Other core specifications	⌘
		X	Test specifications	
		X	O&M Specifications	

Other comments:	⌘	

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

First amended section

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 ~~and be able to shape upstream traffic~~. 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.

Next amended section

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 [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 configured on the GGSN or derived from PDP context parameters.

RSVP/IntServ Function

[Editor's note: Detailed functional description of RSVP/IntServ Function is FFS]

The **Service-based Local Policy Enforcement Point** controls the quality of service that is provided to a combined set of IP flows~~packets (or IP "flows") defined by a packet classifier~~. The policy enforcement function includes policy-based admission control that is applied to the ~~IP~~ bearer~~s~~ associated with the flows, and configuration of the ~~packet handling and~~ 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 ~~an~~the set of IP flows. The authorized resources are~~may be~~ expressed as a maximum authorised bandwidth and QoS class~~an Intserv-style Flowspec~~. 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 PCF 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 TS23.228 are to ~~define the~~ control and ~~to~~ manage media flows based on policy, and are under the control of PCF. 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)~~, a traffic metering function, and user plane actions to be taken for the set of packets matching the classifier~~. When a gate is open, the packets in a flow are accepted, and are thus subject to the Diffserv edge treatment ~~(policing or marking) as determined by traffic metering and user plane actions~~. 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.

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. ~~It is possible for a set of packets to match more than one classifier. When this happens, the sequence of actions associated with the gates are executed in sequence. Packets that are marked by a gate may not be (re)marked by a subsequent gate to a Diffserv Code Point corresponding to a better service class.~~

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 PCF associated with the IP flow(s). In order to allow SBLP policy information to be "pulled" from the PCF, the binding information shall allow the GGSN to determine the address of the PCF to be used.

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.

Next amended section

5.2.3 P-CSCF(PCF)

This clause provides functional descriptions of capabilities in P-CSCF(PCF). Determination of exactly which functions are required to support interoperator and multi-vendor aspects are not addressed in this clause.

Service-based Local Policy Decision Point

- Authorize QoS resources (bandwidth, etc.) for the session. The P-CSCF (PCF) shall use the SDP contained in the SIP signaling message 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 ~~packet~~ flows and restrictions on individual IP flows (eg. destination address and port).

  ~~-~~For bi-directional media flows, the P-CSCF(PCF), 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 P-CSCF(PCF) assumption

would be determined by operator policy in order to reduce the possibilites of bearer misuse In the filters supplied by the PCF 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.

- The P-CSCF (PCF) shall be able to enforce the behaviour of the UE in 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 IMS network using the indications described in Sections 4.2.5.1 of [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 P-CSCF/PCF shall take care that such a PDP context would be rejected by the GGSN. To do so, the P-CSCF/PCF uses the Go interface.

- The P-CSCF (PCF) shall be able to decide if new QoS authorization (bandwidth, etc.) is needed due to the 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 PCF functions as a Policy Decision Point for the service-based local policy control.

- The PCF shall exchange the authorization information with the GGSN via the Go interface.

- PCF provides final policy decisions controlling the allocated QoS resources for the authorized media stream. The decision shall be transferred from the PCF to the GGSN.

- At IP multimedia session release, the PCF shall revoke the QoS resource authorization for the session.

Binding Mechanism Handling

- The PCF generates an authorization token for each SIP session and the P-CSCF sends the authorization token to the UE in SIP signalling. The authorization token may contain information that identifies its generator. 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.

Next amended section

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 Control Function (PCF). The Go interface provides information to support the following functions in the GGSN:

~~- Control of Diffserv inter working~~

~~-~~

- 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 Control Function (PCF). 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 PCF 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 PCF.

Next amended section

5.3.2 Information Elements 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 PCF. The information elements specific to UMTS would be standardized and carried in the 3GPP Go specific interactions between the PCF and the GGSN.

A **Request** (REQ) message from the GGSN to the PCF shall allow the GGSN to request SBLP policy information for ~~the~~a set of IP flow~~(s)~~ identified by binding information (described below).

Binding information associates the PDP context to the IMS session and IP flows, and is used by the GGSN to request SBLP policy information from the PCF. The binding information includes 1) an authorization token sent by the P-CSCF to the UE during SIP signalling, and 2) one or more flow identifiers used by the UE, GGSN and PCF to uniquely identify the IP media flow(s).

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 PCF 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 PCF 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 PCF 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 PCF. 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
- Event generation information (e.g. charging identity)

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 wild-carded.

The authorized QoS information provides an upper bound on the resources that can be reserved or allocated for the combined set of IP flow~~(s)~~. 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 29.207.

The packet handling action defines the packet handling that should be accorded to ~~in-profile and out-of-profile~~ packets matching the packet classifier. ~~In-profile traffic is defined as traffic that is within the authorized QoS information. The packet handling action may be ignored by the GGSN.~~ The packet handling action (gate status) shall result in packets being passed (gate open), or silently discarded (gate closed).

Event generation information contains information used to correlate usage records (e.g. CDRs) of the GGSN with IMS session records from the P-CSCF. The PCF shall send the ICID provided by the P-CSCF as part of the authorisation (Install) decision. The GGSN shall send the GCID of the PDP context and the GGSN address to the PCF 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).

Next amended section

6.1.1 Procedures in the GGSN

The QoS procedures in the GGSN are triggered by the QoS signaling 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~~IP~~ level information ~~(e.g., addressing 5-tuple) provided by service based local policy according to the authorization token~~ to configure the DiffServ edge~~classifier~~ 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 GGSN may use IP level information provided by service based local policy according to authorization token to authorize the RSVP session and configure the DiffServ classifier functionality.~~ The authorization token may be included in the RSVP signaling 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 ~~and optionally (dependent on operator policy) RSVP messages~~ that are subject to service based local policy by sending an authorization request to the PCF. Alternatively, the GGSN may authorize PDP context activation/modification messages ~~and optionally (dependent on operator policy) RSVP 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.

Next amended section

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. TS23.228 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 corresponding RSVP signalling parameters as well as~~ 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).

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.

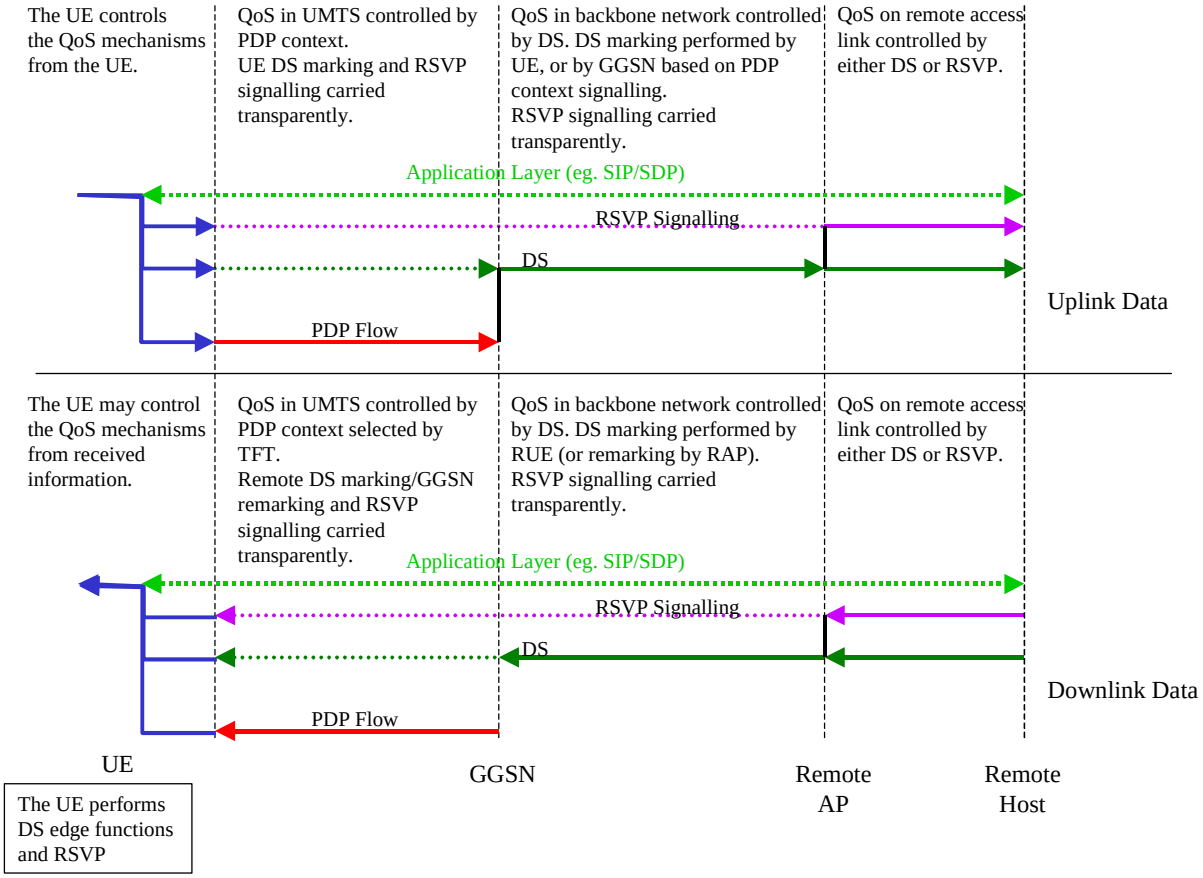


Figure A.4: Local UE supports RSVP signalling with IntServ semantics, and DiffServ; without service based policy

~~When the authorisation token is included in the PDP context establishment/modification (as per section 5.1.1.2.3), the GGSN may use IP level information provided by service based local policy according to the authorisation token to configure the DiffServ classifier functionality. The information can also be used for DiffServ class admission control, e.g., the requested end-to-end bandwidth from the UE for a particular flow may be informed to the GGSN beforehand for the GGSN DiffServ edge to determine if the flow can be allowed to a certain DiffServ class or to/from an ingress/egress point.~~ The GGSN provides the interworking between the PDP context and the DiffServ function

The application layer signaling may be processed in the local network at an application server such as the P-CSCF in the case of SIP signaling. 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 PCF policy function co-located in the P-CSCF, as shown in the figure below.

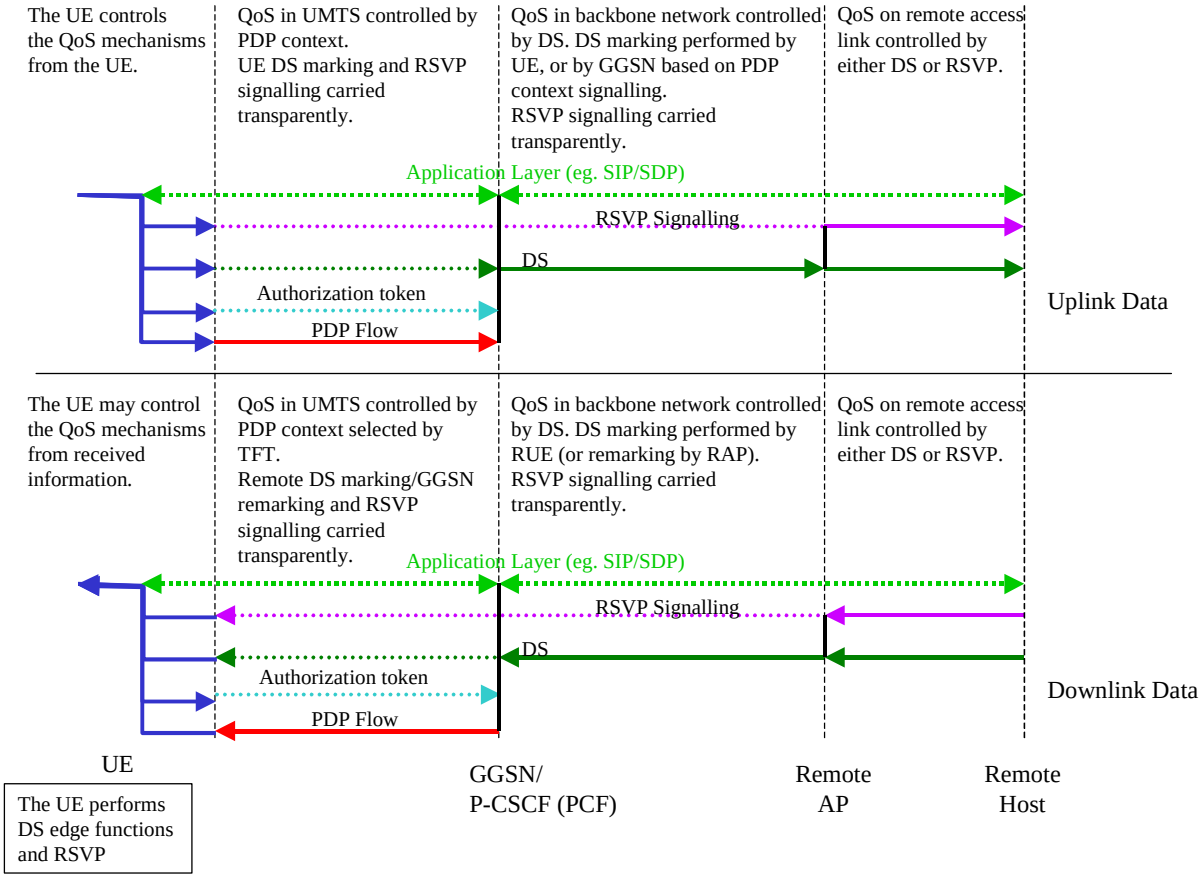


Figure A.5: Local UE supports RSVP signalling with IntServ semantics, and DiffServ; where service based policy is applied

Next amended section

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. TS23.228 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 corresponding RSVP signalling parameters and~~ 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).

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 ~~use IP level information provided by service based local policy according to the authorisation token to~~ authorise the RSVP session and configure the Diffserv classifier functionality. ~~The information may also be used in conjunction with a Diffserv aggregate to enable DiffServ class admission control, e.g., the requested end-to-end bandwidth from the UE for a particular flow may be informed to the GGSN beforehand for the GGSN DiffServ edge to determine if the flow can be allowed to a certain DiffServ class or to/from an ingress/egress point.~~

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.

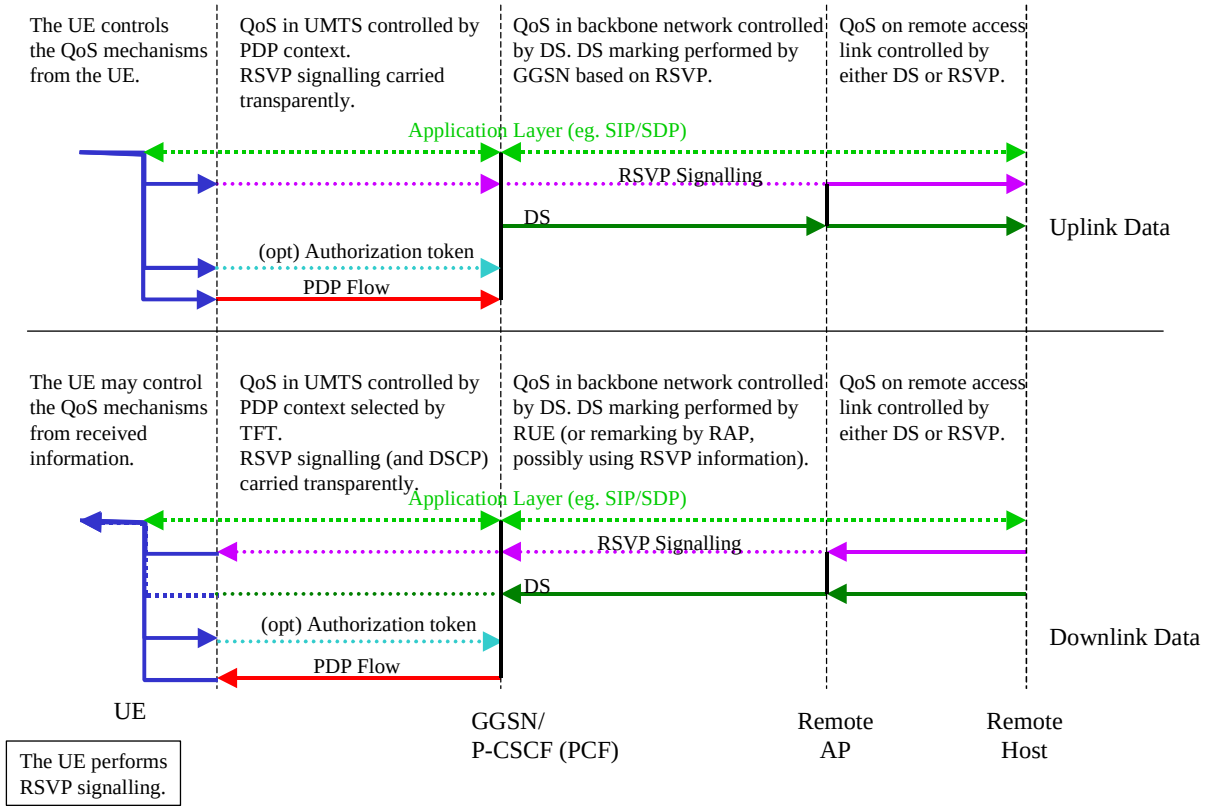


Figure A.6: Local UE supports RSVP signalling using IntServ Semantics

Next amended section

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~~, to enhance the interworking options to the DiffServ edge function of the GGSN~~. The GGSN uses the authorization token to obtain a policy decision from the P-CSCF(PCF) ~~which will be used to derive IP level information~~. This is done via the standardized interface between the PCF 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.

~~In addition, IP level information may also be derived from PDP context (e.g. QoS parameters).~~

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. TS23.228 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.

~~The GGSN DiffServ edge function may use the IP level information (e.g., 5-tuple combination of source and destination IP address, source and destination port number, and the protocol identifier) provided by service based local policy according to the authorisation token to configure the DiffServ classifier functionality. The information can be used for DiffServ class admission control, e.g., for the GGSN DiffServ edge to determine if the flow can be allowed to a certain DiffServ class or to/from an ingress/egress point. As a result, the GGSN may select the appropriate DiffServ setting to apply. This is shown in the figure below.~~

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).

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~~uses the IP level information~~ to interwork with~~ DiffServ in~~ 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.

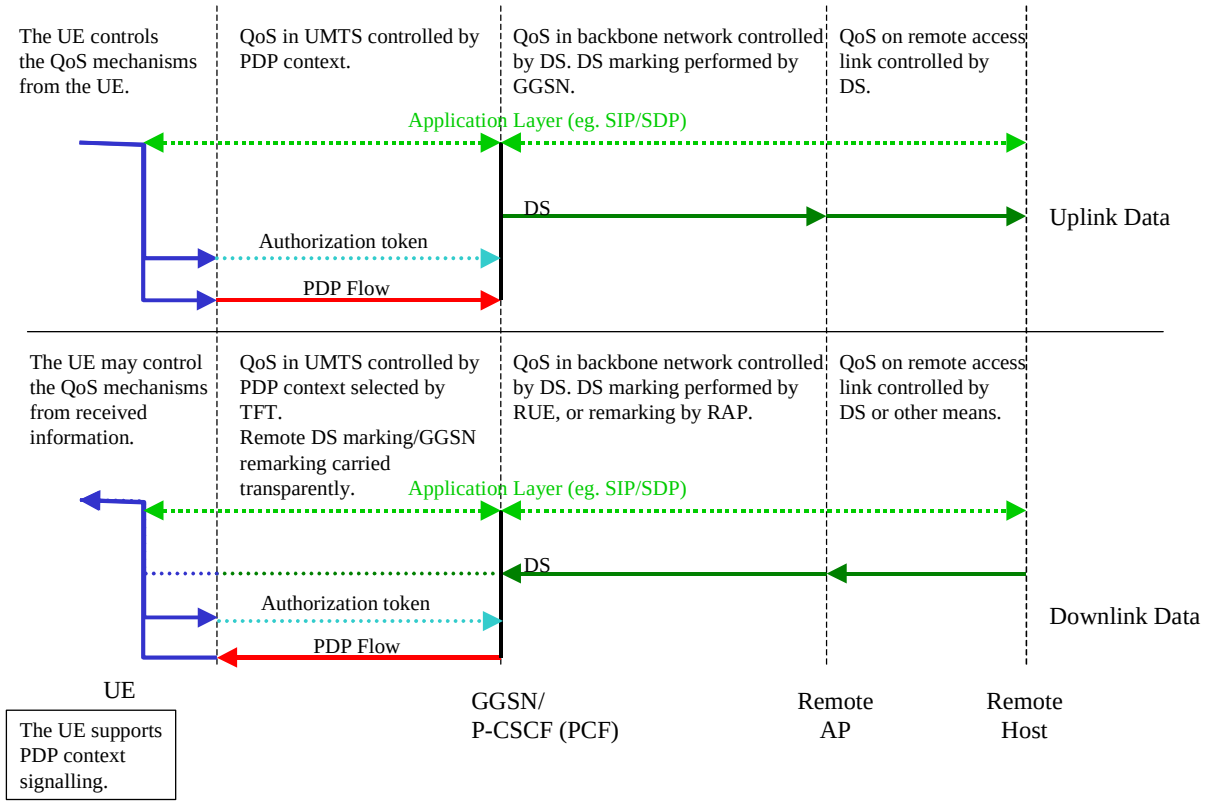


Figure A.7: Local UE provides authorization token in PDP context activation/modification message and GGSN provides interworking with DiffServ

Next amended section

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(PCF) shall use the SDP contained in the SIP signaling 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 ~~may take the form of a flowspec and~~ filter specs.

The QoS authorization for a session shall include an Authorization-Token, which shall be assigned by the P-CSCF(PCF). The Authorization-Token shall ~~may~~ contain information that identifies the P-CSCF(PCF) 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~~ies~~ the set of flows)
- Data rate and QoS class~~FLOWSPEC~~ that describes the authorized resource for the set of flows

~~- DSCP that identifies the assigned DiffServ PHB the flow~~

~~-~~The IP flow 5-tuples includes Source Address, Source Port, Destination Address, Destination Port and Protocol ID. Note that some fields may be wildcarded.~~The FLOWSPEC includes the following elements:~~

~~- Token rate [r]~~

~~- Bucket depth [b]~~

~~- Peak rate [p]~~

~~- Minimum policed unit [m]~~

- ~~Maximum packet size [M]~~

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**

~~This audio flow uses either AMR or GSM FR codec and the authorized resource envelope can be expressed as a FLOWSPEC as follow:~~

~~**b**~~	~~**m**~~	~~**M**~~	~~**r**~~	~~**p**~~
~~**72.5 bytes**~~	~~**52 bytes**~~	~~**72.5 bytes**~~	~~**3625 bytes/s**~~	~~**3625 bytes/s**~~

~~*See Note 1 for the mapping calculation~~

Since the conversational audio is very sensitive to delay, the ~~DiffServ EF class will be used for the flow, e.g., DSCP = 101110~~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 uses H.263 SQCIF codec with 15frame/s. Let's assume the average bit rate and peak bit rate for the encoded video are 28kb/s and 40kb/s respectively. The authorized resource envelope can be expressed as a FLOWSPEC as follow:~~

~~b~~	~~m~~	~~M~~	~~r~~	~~p~~
~~373 bytes~~	~~273 bytes~~	~~373 bytes~~	~~4095 bytes/s~~	~~5595 bytes/s~~

~~*See Note 2 for the mapping calculation~~

The video flow may be assigned a ~~DiffServ AF class with DSCP = 001010~~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 uses H.263 SQCIF codec with 15frame/s. Let's assume the average bit rate and peak bit rate for the encoded video are 28kb/s and 40kb/s respectively. The authorized resource envelope can be expressed as a FLOWSPEC as follow:~~

~~b~~	~~M~~	~~M~~	~~r~~	~~p~~
~~373 bytes~~	~~273 bytes~~	~~373 bytes~~	~~4095 bytes/s~~	~~5595 bytes/s~~

~~*See Note 2 for the mapping calculation~~

The video flow may be assigned a ~~DiffServ AF class with DSCP = 001010~~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

~~Assuming a typing speed of 1 char to 50 chars a second, the authorized resource envelope may be expressed as a FLOWSPEC as follow:~~

~~b~~	~~m~~	~~M~~	~~R~~	~~p~~
~~90 bytes~~	~~41 bytes~~	~~90 bytes~~	~~41 bytes/s~~	~~90 bytes/s~~

~~*See Note 3 for the mapping calculation~~

The udp application flow may be assigned a ~~DiffServ AF class with DSCP = 010100~~maximum QoS class corresponding to interactive. The b parameter is used to determine the data rate.

~~Note 1: With AMR or GSM FR codec, the authorization shall use the maximum rate of the two, i.e., 13kb/s. With 20ms frames, there are 50 frames per second and each frame has 260 bits or 32.5 bytes payload. With IP/UDP/RTP overhead of 40 bytes, each packet is 72.5 bytes. The token rate and peak rate for the session (i.e., r and p) are 72.5 x 50 = 3625 bytes /s. The bucket depth and Maximum packet size (i.e., b and M) are 72.5 bytes. The minimum AMR rate of 4.75kb/s is used to calculate the minimum policed unit m. At that rate, each frame has 95 bits or 16 byes. With the overhead of 40 bytes, we have m equals to 52 bytes.~~

~~Note 2: With variable video codec h.263, we assume an average rate at 28kb/s and peak rate at 40kb/s. The average rate is used to calculate r and m. With 15 frames a second, each frame has 1867 bits or 233 bytes. Each packet is 273 bytes, so the r is 273x15=4095 bytes/s and the m is 273 bytes. The peak rate is used to calculate b, M and p. With 40kb/s and 15 frames/s, each frame has 2667 bits or 333 bytes. Each packet is 373 bytes, so the p is 373x15=5595 bytes/s and the b and M are 373 bytes.~~

~~Note 3: The calculation is the same as in Note 2 with average rate of 1 byte/s and peak rate of 50 bytes/s.~~

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.

~~[Editorial note: The sample mappings in this section are for illustration purpose only. The actual mapping of media codec to QoS resource requirement, e.g., FLOWSPEC, is for further study.]~~

3GPP TSG-CN3 Meeting #27
Beijing, China, 14-18 October 2002

S2-023063

CR-Form-v7

CHANGE REQUEST

⌘ **23.207** **CR** **50** ⌘**rev** **1** ⌘ Current version: **5.5.0** ⌘

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

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

Title:	⌘	Clarification of Diffserv functions in 23.207 without Go control
Source:	⌘	Nortel Networks
Work item code:	⌘	E2E-QOS
Date:	⌘	15/10/2002
Category:	⌘	**F**
Release:	⌘	Rel-5

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

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	Policy-based (Go) control of Diffserv Edge Functions at the GGSN was not included in Release 5. However Diffserv Edge Functions are introduced to the GGSN in Release 5 at the IP Bearer Service layer for the first time. Some description of how these are configured is required.
Summary of change:	⌘	Clarification of the Diffserv Edge Function Functional Components that can be installed on the basis of PDP Context parameters and on the basis of static configuration is added.
Consequences if not approved:	⌘	The Diffserv Edge Functions introduced in release 5 will be poorly defined.

Clauses affected:	⌘	5.2.1			
Other specs affected:	⌘	**Y**	**N**		
			N	Other core specifications	⌘
			N	Test specifications	
			N	O&M Specifications	
Other comments:	⌘				

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

First amended section

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 [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.

End of amendment