Source: **TSG SA WG2**
Title: **CRs on 23.207 (End to End QoS)**
Agenda Item: **7.2.3**

The following Change Request has been approved by TSG SA WG2 and is requested to be approved by TSG SA plenary #24.
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.

S2 doc #	Title	Spec	CR #	cat	Version in	REL	WI	S2 meeting	Clauses affected
S2-041625	Authorisation Reject Procedure by the PDF	23.207	077r3	B	6.2.0	6	QoS1	S2 #39	5.2.3, 5. 2.4, 6.1.3, 6.3.1, 6.3.2
S2-041492	AF capabilities	23.207	079r1	F	6.2.0	6	QoS1	S2 #39	5.2.4, 5.3a
S2-042119	General corrections	23.207	080r2	B	6.2.0	6	QoS1	S2 #40	3.1, 5.2.1, 6.1.3, 6.1.4, A.2.5, Annex C
S2-041489	Intra-domain Gq for IMS	23.207	081r1	F	6.2.0	6	QoS1	S2 #39	2, 5.1.1.1
S2-042120	Condition for update authorization procedure	23.207	083	B	6.2.0	6	QoS1	S2 #40	6.3.8

3GPP TSG-SA2 Meeting #39
ShenZhen, China, 19th – 23rd April 2004

Tdoc ⌘S2-041625

CR-Form-v7

CHANGE REQUEST

⌘ **23.207** **CR** **077** ⌘ **rev** **3** ⌘ Current version: **6.2.0** ⌘

*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 **X**

Title:	⌘	Authorisation Reject Procedure by the PDF
Source:	⌘	SA2 (Orange)
Work item code:	⌘	QoS1
Date:	⌘	13/04/2004
Category:	⌘	**B**
Release:	⌘	Rel-6

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

Use one of the following releases:

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:	⌘	There were still an open issue in TR 23.917 regarding the procedure used when the PDF rejects an authorisation request. There were two options listed in the TR: a) The PDF rejects the authorisation request with an indication of what could have been accepted b) The PDF authorizes lower QoS resources with an indication of what has been authorised. This contribution proposes to adopt option a) and reflect this in TS 23.207
Summary of change:	⌘	The text in 23.207 is changed to reflect the possiblity for the PDF to reject the authorisation request
Consequences if not approved:	⌘	There will still be an unsolved issue on the Gq interface procedures.

Clauses affected:	⌘	5.2.3, 5.2.4, 6.1.3, 6.3.1, 6.3.2

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 MODIFIED SECTION** ----------

5.2.3 PDF

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

Service-based Local Policy Decision Point

- The PDF shall check if the policy set-up information received from the AF is consistent with operator policy rules defined in the PDF.
- Authorize QoS resources (bandwidth, etc.) for the AF session. The PDF shall use the policy set-up information received from the AF to calculate the proper authorization. The authorization shall be expressed in terms of the IP resources to be authorized. The authorization shall include limits on QoS for the set of IP flows and restrictions on individual IP flows (e.g. destination address and port).
- In the filters supplied by the PDF for bi-directional flows, the source address prefix for downstream packets may be identified as the same as the destination address prefix for the upstream. Similarly, the source address prefix for the upstream packets may be identified as the same as the destination address prefix for the downstream.

- In case of IMS, the PDF shall be able to enforce the behaviour of the UE with respect to the assignment of IMS media components to the same PDP Context or to separate PDP Contexts. This behaviour of the UE is controlled by the AF (i.e. the P-CSCF) using the indications described in Section E.2.2.1 of [4]. In case the UE violates this indication, and attempts to carry multiple IMS media components in a single PDP context despite of an indication that mandated separate PDP contexts, the PDF shall take care that such a PDP context would be rejected by the GGSN. To do so, the PDF uses the Go interface.

- The PDF shall be able to decide if new QoS authorization (bandwidth, etc.) is needed due to a mid-call media or codec change. A new authorization shall be required when the resources requested by the UE for a flow exceeds previous authorization, or a new flow is added, or when elements of the packet classifier(s) for authorized flows change.
- The PDF functions as a Policy Decision Point for the service-based local policy control.
- The PDF shall exchange the authorization information with the GGSN via the Go interface.
- PDF provides final policy decisions controlling the allocated QoS resources for the authorized media stream. The decision shall be transferred from the PDF to the GGSN.
- At AF session release, the PDF shall revoke the QoS resource authorization for the AF session.

Binding Mechanism Handling

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

5.2.4 Application Function (AF)

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

Service Based Local Policy related functions

- The AF shall use Gq interface to exchange service based policy set-up information with the PDF. This applies both during session establishment, as well as upon a mid-session modification effecting the media (e.g. addition of a new media in mid-session).
- The AF shall indicate to the PDF whether or not the PDF should contact the AF at UE resource reservation.

- For bi-directional media flows, the AF, according to operator policy, may assume that the 64-bit IPv6 address prefix of the source address for downstream packets is the same as the prefix of the destination address for upstream packets of the same media flow. The implementation of this AF assumption would be determined by operator policy in order to reduce the possibilities of bearer misuse.

Binding Mechanism Handling

- The AF requests authorization token(s) from the PDF. The following are possible:

    1. The PDF authorizes QoS resources usage for that application for a particular session and user. The authorization token is only valid for the duration of the session for the specific user.
    2. The AF requests multiple authorization tokens. The PDF provides the requested number of authorization tokens. Each of these tokens may later be allocated to a session, and then used for subsequent QoS resource usage authorization procedures for the duration of the session for the specific user.
    3. The PDF rejects the authorisation because the service information is not consistent with the operator policy rules defined in the PDF. No token is sent to the AF. The PDF shall also indicate in the authorisation reject the service information that could be accepted by the PDF.

- For AF sessions to and from the same UE, the AF(s) shall request authorization tokens from the same PDF.

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

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

---------- **SECOND MODIFIED SECTION** ----------

6.1.3 Procedures in the PDF

In case of applying Service based local policy:

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

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

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

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

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

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

When the PDF receives updated service information, the AF sends an update for service information to the PDF. The 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.

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

---------- **THIRD MODIFIED SECTION** ----------

6.3.1 Authorize QoS Resources, AF session establishment

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

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

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

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

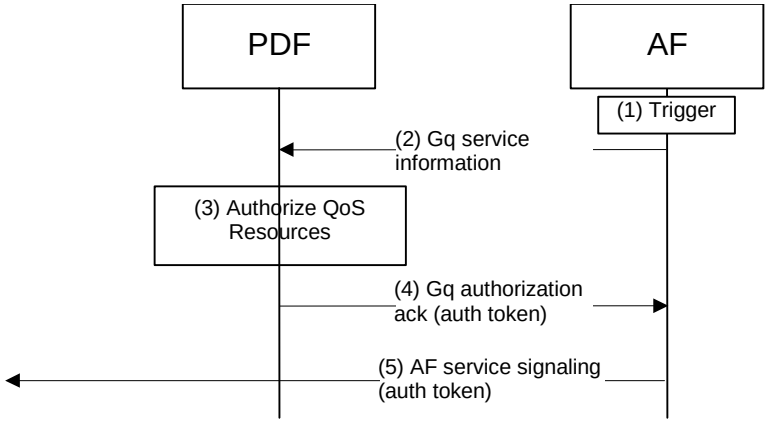

Figure 3: Authorize QoS Resources, AF session establishment

1) An AF session signaling message is received at or generated by the AF, or an internal action at the AF triggers the need for an authorization request.

2) The Application Function sends a request for authorization token to the PDF with service information, which may include session description information based on the AF session signaling. Some services may require further interaction between the AF and the PDF to provide the full service information, e.g. for IMS session establishment (mobile terminated).
Note that it is also possible that the AF initiates a request for multiple authorization tokens to use for future sessions, in which case the PDF can generate multiple authorization tokens.

3) If the PDF has received AF session description in the service information in Step 2, the PDF shall authorize the required QoS resources for the AF session if the session description is consistent with the operator policy rules defined in the PDF, and install the IP bearer level policy based on information received from the AF. If the service information was not received in Step 2 above, the QoS authorisation is deferred.
The PDF generates an authorization token for the AF session.

4) The PDF sends the authorisation token to the AF.

5) The AF forwards the AF session signaling message containing the session description. The AF shall include the authorization token in this AF session signaling message.

6.3.2 Resource Reservation Message Flows

6.3.2.1 Resource Reservation with Service-based Local Policy

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

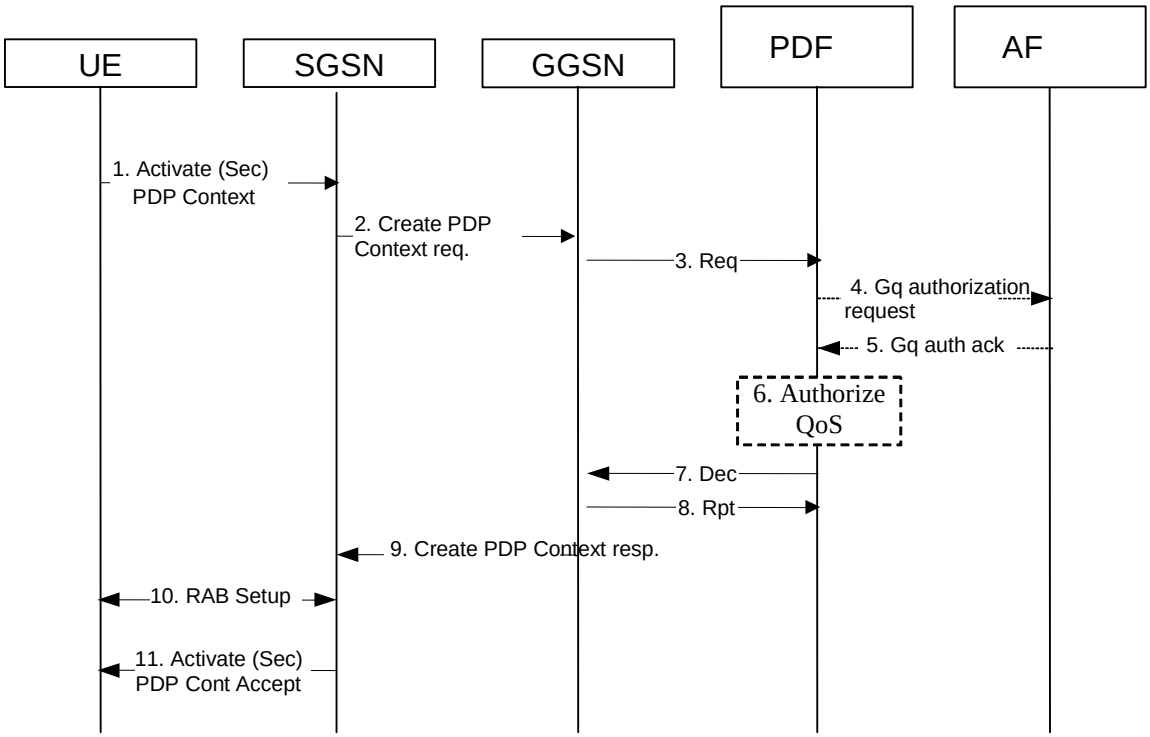

Figure 4: Resource Reservation with Service-based Local Policy

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 PDF in order to obtain relevant policy information.

4) A PDF generated authorization token enables the PDF to identify the authorisation status information. If the previous PDF interaction with that AF had requested this, or if the previous interaction with the AF did not include service information, the PDF sends an authorisation request to that Application Function.

6) The AF sends the service information to the PDF.

7) The PDF shall authorize the required QoS resources for the AF session if the session description is consistent with the operator policy rules defined in the PDF, and install the IP bearer level policy in its internal database. This is based on information from the Application Function.

7) The PDF sends a COPS DEC message back to the GGSN.

8) The GGSN sends a COPS RPT message back to the PDF, which may also trigger a report message to be sent from the PDF to the AF.

9) The GGSN maps IP flow based policy information into PDP context based policy information and uses the PDP context based policy information to accept the PDP activation request, and sends a Create PDP Context Response message back to SGSN.

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

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

---------- END OF MODIFIED SECTION ----------

3GPP TSG-SA2 Meeting #39
Shenzhen, China, 19th – 23rd April, 2004

Tdoc ⌘ S2-041492

CR-Form-v7

CHANGE REQUEST

⌘ **23.207** **CR** **079** ⌘ **rev** **1** ⌘ Current version: **6.2.0** ⌘

*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:	⌘	AF capabilities
Source:	⌘	SA2 (Siemens)
Work item code:	⌘	QoS1
Date:	⌘	19/04/2004
Category:	⌘	**F**
Release:	⌘	Rel-6

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

Use one of the following releases:

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:	⌘	A part of the AF capabilities have not been included into 23.207 yet, especially the ability of the AF to give instructions to the PDF how to execute the different SBLP procedures for a concrete AF session.
Summary of change:	⌘	The AF capabilities to instruct the PDF are completed. The description of the information exchanged via the Gq interface is updated accordingly. The missing bearer modification indication is added. Furthermore, some rewording is proposed to improve the understanding.
Consequences if not approved:	⌘	The AF capabilities and the Gq information would be incomplete. The AF would not be able to instruct the PDF appropriately depending on the requirements of the service.

Clauses affected:	⌘	5.2.4, 5.3a

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.

Start of modified section

5.2.4 Application Function (AF)

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

Service Based Local Policy related functions

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

Binding Mechanism Handling

- The AF requests authorization token(s) from the PDF. The following are possible:
    1. The AF requests a single authorization token. The PDF authorizes QoS resources usage for that application for a particular session and user. The authorization token is only valid for the duration of the session for the specific user.
    2. The AF requests multiple authorization tokens. The PDF provides the requested number of authorization tokens. Each of these tokens may later be allocated to a session, and then used for subsequent QoS resource usage authorization procedures for the duration of the session for the specific user.
- For AF sessions to and from the same UE, the AF(s) shall request authorization tokens from the same PDF.

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

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

End of modified section

Start of modified section

5.3a Gq Interface (PDF - AF)

5.3a.1 Gq Functional Requirements

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

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

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

5.3a.2 Information Exchanged via Gq interface

Service information:

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

a) Description of session: the AF may provide one or more of the following information when describing the session (the set of information that needs to be sent in different cases depends on ~~a~~the service for which the media authorisation is required):

- Application identifier: identifies the particular service that the session belongs to. This information may be used by the PDF to differentiate QoS for different application services. For example application identifier may be used as additional information together with the indication of the type of service information when QoS class for the bearer authorisation in Go interface is decided. The application identifier may be used also to complete the QoS authorisation with application specific default settings in the PDF if the AF does not provide all or any of the following information.
- Information defining the media stream
  - Media stream Id (to uniquely identify the media stream within the session)
  - Information defining the IP flows of the media stream.
    - direction (bi-directional, uplink / downlink)
    - 5-tuple (source/destination address and port number, protocol Id)
    - indication of the maximum and/or mean bandwidth required
  - An indication of the requested type of service information per service-flow, e.g., conversational voice or video, streaming voice or video

b) Resource Reservation Policy: Definition of whether PDF shall contact the AF at resource reservation during the session even if policy set-up information is already available in the PDF.

c) ~~Install Gating~~ Media Control Policy: Definition of whether ~~gating~~ explicit AF media control is used or not in the session. If ~~gating~~ explicit AF media control is not used, the AF does not explicitly enable or disable the media. At bearer authorization the PDF shall install~~opens~~ the gates in the GGSN and derive their state (open/close) based on the information defining the media stream~~at the bearer authorisation~~.

d) Revoke Policy: Definition of whether the PDF itself may initiate a revoke of authorization.

e) Indication Forwarding Policy: Definition of whether the PDF shall forward bearer indications (e.g. bearer release indication).

Authorisation token:

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

Charging correlation related information:

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

~~Gate~~ Media control ~~indications~~commands:

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

Bearer reservation indication:

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

Bearer release indication:

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

Bearer modification indication:

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

Revoke authorisation command:

The AF determines when ~~all authorisations related to~~ an authorization token and all related authorizations need to be removed e.g. due to the AF session release, and shall instruct the PDF to remove the authorizations and to enforce the removal~~e~~ of the resources previously authorised for the AF session. The revoke authorisation command may contain information about the reason of the revoking.

End of modified section

3GPP TSG-SA2 Meeting #40
Sophia Antipolis, 17th – 21st May, 2004

Tdoc ⌘ S2-042119

CR-Form-v7

CHANGE REQUEST

⌘ **23.207** **CR** **080** ⌘ **rev** **2** ⌘ Current version: **6.2.0** ⌘

*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:	⌘	General corrections
Source:	⌘	SA2 (Siemens)
Work item code:	⌘	QoS1
Date:	⌘	12/05/2004
Category:	⌘	**B**
Release:	⌘	Rel-6

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

Use one of the following releases:

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:	⌘	Some sections of 23.207 contain obsolete abbreviations or descriptions.
Summary of change:	⌘	A number of general corrections and rewordings are proposed, like: - replacement of PCF with PDF - rewording of PDF action in case of an update of service information - addition of “AF” to “session”. The PDF actions in case of an update of service information have been extended to reflect the possibility for the PDF to reject the update of service information if the service information received from the AF is not consistent with the operator policy rules defined in the PDF. In addition the PDF shall indicate in the response to the AF the service information that could be accepted by the PDF.
Consequences if not approved:	⌘	The specification would be inconsistent and could be misunderstood.

Clauses affected:	⌘	3.1, 5.2.1, 6.1.3, 6.1.4, A.2.5, Annex 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.

Start of 1st modified section

3.1 Definitions

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

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

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

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

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

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

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

End of 1st modified section

Start of 2nd modified 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.

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

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

In the user plane, policy enforcement is defined in terms of a "gate" implemented in the GGSN. A gate is a policy enforcement function that interacts through Go interface with PDF as the Policy Decision Point for QoS resource authorisation at the IP BS level for a unidirectional flow of packets. Gate operations as defined in TS23.228 are to control and 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, 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~~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.

End of 2nd modified section

Start of 3rd modified section

6.1.3 Procedures in the PDF

In case of applying Service based local policy:

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

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

When the PDF received service information from the AF, the PDF shall authorize the QoS resources, and stores the SBLP for the AF session based on the service information received from the AF.

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

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

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

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

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

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

End of 3rd modified section

Start of 4th modified section

6.1.4 Procedures in the AF

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

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

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

- If the AF indicates to the PDF that it wishes to be contacted upon berarer resource reservation, the service information shall be passed during the Gq interaction upon bearer resource reservation. Alternatively, if the initial AF session signalling message contains session description information, such as the end-point addresses, bandwidth requirements and the characteristics of the media exchange, the AF shall forward this information to the PDF as part of the service information at the same time with the authorisation token request.

- The AF generates the information (e.g. service information) conveyed over the Gq interface from the application specific media description (e.g. SDP media description).

- The PDF shall use the service information for the QoS policy set up for the AF session. During an AF session change, the AF shall send an update for service information to the PDF based on the new session description information exchanged within AF session signalling.

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

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

End of 4th modified section

Start of 5th modified 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. The GGSN uses the authorization token to obtain a policy decision from the P-CSCF(~~PCF~~PDF). 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.

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.

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 to interwork with the backbone IP network and control the IP QoS bearer service towards the remote -host.

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

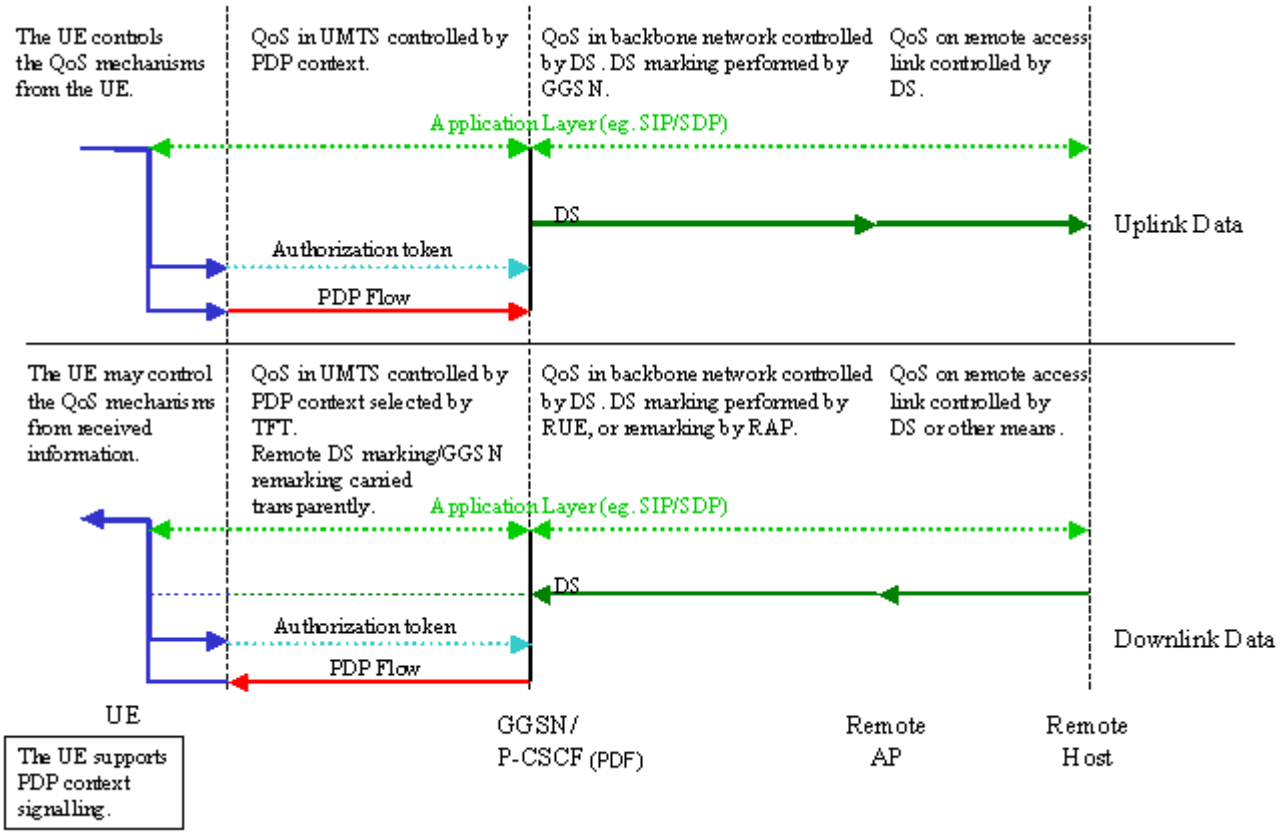

Figure A.7: Local UE provides authorization token in PDP context activation/modification message and GGSN provides interworking with DiffServ

End of 5th modified section

Start of 6th modified 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~~PDF) 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 filter specs.

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

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

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

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

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

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

a=<attribute><value>

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

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

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

b=<modifier>:<bandwidth-value>

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

v=0

o=hshieh 2890844526 2890842807 IN IP4 saturn.attws.com

s=-

c=IN IP4 192.141.10.188

t=0 0

b=AS:64

m=audio 29170 RTP/AVP 3 96 97

a=rtpmap:96 G726-32/8000

a=rtpmap:97 AMR

a=fmtp:97 mode-set=0,2,5,7; maxframes=2

m=video 51372 RTP/AVP 34

a=fmtp 34 SQCIF=2/MaxBitRate=500/SAC AP

m=application 32416 udp text_chat

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

v=0

o=johndoe 2890844526 2890842807 IN IP4 uranus.solar.com

s=-

c=IN IP4 204.142.180.111

t=0 0

b=AS:64

m=audio 31160 RTP/AVP 3 97

a=rtpmap:97 AMR

a=fmtp:97 mode-set=0,2,5,7; maxframes=2

a=recvonly

m=video 61000 RTP/AVP 31

a=fmtp 34 SQCIF=2/MaxBitRate=500/SAC AP

m=application 33020 udp text_chat

a=sendonly

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

A uplink audio flow:

The following IP 5-tuples identify the flow:

SrcAddress	SrcPort	DestAddress	DestPort	ProtocolID
192.141.10.188	*****	**204.142.180.111**	**31160**	**17**

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

An uplink video flow:

The following IP 5-tuples identify the flow:

SrcAddress	SrcPort	DestAddress	DestPort	ProtocolID
192.141.10.188	*****	**204.142.180.111**	**61000**	**17**

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

A downlink video flow:

The following IP 5-tuples identify the flow:

SrcAddress	SrcPort	DestAddress	DestPort	ProtocolID
204.142.180.111	*****	**192.141.10.188**	**51372**	**17**

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

A downlink udp flow:

The following IP 5-tuples identify the flow:

SrcAddress	SrcPort	DestAddress	DestPort	ProtocolID
204.142.180.111	*****	**192.141.10.188**	**32416**	**17**

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

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

End of 6th modified section

3GPP TSG-SA2 Meeting #39
Shenzhen, China, 19-23 April 2004

Tdoc ⌘S2-041489

CR-Form-v7

CHANGE REQUEST

⌘ **23.207** **CR** **081** ⌘**rev** **1** ⌘ Current version: **6.2.0** ⌘

*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:	⌘	Intra-domain Gq for IMS
Source:	⌘	SA2 (Nortel Networks)
Work item code:	⌘	QoS1
Date:	⌘	19/04/2004
Category:	⌘	**F**
Release:	⌘	Rel-6

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

Use one of the following releases:
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:	⌘	Gq supports inter-domain relationships from PDF to AFs for trusted networks. However in the particular of IMS, P-CSCF and GGSN are in the same domain so Gq is in fact intra-domain.
Summary of change:	⌘	Add note that for IMS, P-CSCF and GGSN are in the same domain.
Consequences if not approved:	⌘	Generic text on Gq could be misinterpreted to allow GGSN and P-CSCF in different networks in the case the Gq is for IMS.

Clauses affected:	⌘	2, 5.1.1.1

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.

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".

[4c] 3GPP TS 29.xxx: “Policy control over Gq interface”.

[5] 3GPP TS 22.105: "Vocabulary for 3GPP Specifications".

[6] RFC 2475: "An Architecture for Differentiated Services (DiffServ)".

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

[8] RFC 2748: "Common Open Policy Service protocol (COPS)".

[9] RFC 2205: "Resource ReSerVation Protocol (RSVP)".

[10] RFC 2209: "Resource ReSerVation Protocol (RSVP) Message Processing Rules".

[11] RFC 2210: "The use of RSVP with IETF integrated Services".

[12] RFC 1633: "Integrated Services in the Internet Architecture: an Overview".

[13] RFC 3261: "SIP: Session Initiation Protocol".

[14] RFC 2327: "Session Description Protocol".

[15] RFC 2998: "A Framework For Integrated Services Operation Over DiffServ Networks".

[16] RFC 2750: "RSVP Extensions for Policy Control".

[17] RFC 2474: "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers".

[18] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[19] 3GPP TS 23.060: “General Packet Radio Service (GPRS) Service description; Stage 2”

[20] 3GPP TS 23.221: "Architecture requirements".

NEXT CHANGE

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

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

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

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

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

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

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

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

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

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

Policy Decision Function (PDF) is a logical policy decision element which uses standard IP mechanisms to implement Service Based Local Policy (SBLP) in the IP bearer layer. These mechanisms may be conformant to, for example, the framework defined in IETF [RFC2753] "A Framework for Policy-based Admission Control" where the PDF is effectively a Policy Decision Point (PDP). The PDF makes decisions in regard to SBLP using policy rules, and communicates these decisions to the IP BS Manager in the GGSN, which is the IP Policy Enforcement Point (PEP).

The interface between the PDF and the Application Function (AF) is the Gq interface specified in 3GPP TS 23.002 [2].

The interface between the PDF and GGSN is specified within 3GPP, named Go interface, and is included in the Reference Architecture depicted in TS23.002. The interface between the PDF and

GGSN supports the transfer of information and policy decisions between the policy decision point and the IP BS Manager in the GGSN.

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

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

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

3GPP TSG-SA2 Meeting #40
Sophia Antipolis, 17th – 21st May, 2004

Tdoc ⌘ S2-042120

CR-Form-v7

CHANGE REQUEST

⌘ **23.207** **CR** **083** ⌘ **rev** **-** ⌘ Current version: **6.2.0** ⌘

*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 **X**

Title:	⌘	Condition for update authorization procedure
Source:	⌘	SA2 (Siemens)
Work item code:	⌘	QoS1
Date:	⌘	12/05/2004
Category:	⌘	**B**
Release:	⌘	Rel-6

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

Use one of the following releases:
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:	⌘	At the last meeting the possibility for the PDF to reject a QoS authorization procedure was introduced. Such rejection might happen when the session description is not consistent with the local operator policy rules of the PDF. After a successful session establishment conformable to the local operator policies a session modification could take place. The update authorization procedure is used to trigger the PDF to align the authorization. The modified session description could be not consistent with the local operator policies of the PDF but the PDF cannot reject the authorization of the modification.
Summary of change:	⌘	The update authorization procedure is extended by a condition. The procedure is only successfully executed if the session description is consistent with the local operator policy rules defined in the PDF.
Consequences if not approved:	⌘	Although the PDF can reject the QoS authorisation procedure due to local policies any later update could not be rejected by the PDF. Thus it would be possible to circumvent the local operator policies of the PDF.

Clauses affected:	⌘	6.3.8			
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.

6.3.8 Update Authorization procedure

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

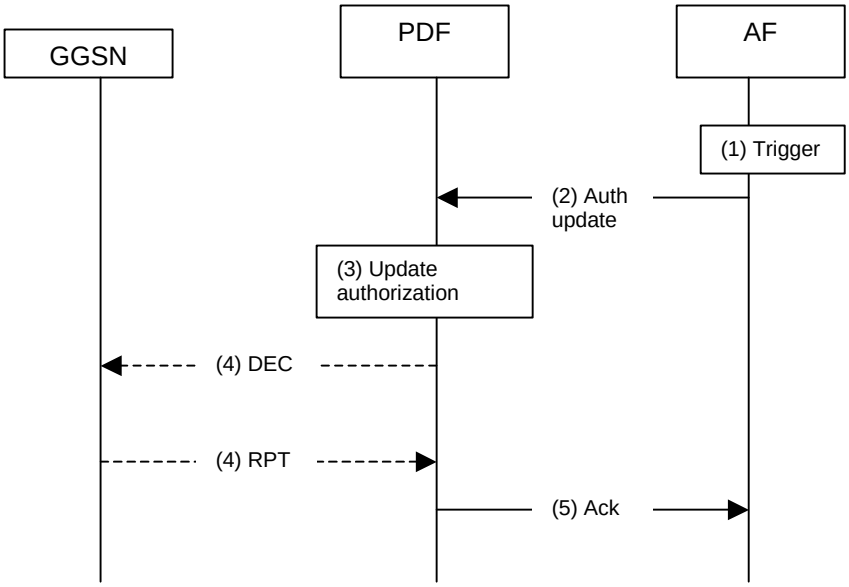

Figure 16: Update Authorization for the session

1. The AF is triggered to give updated service information to the PDF (e.g. as a result of the modification of the session at session control level).

2. The AF gives the updated service information to the PDF.

3. The PDF updates the authorization for the session if the session description is consistent with the operator policy rules defined in the PDF. In case the session modification requires enhancing the reserved resources, the PDF may decide not to send an updated decision authorizing the enhanced QoS to the GGSN, but would rather wait for a new authorization request from the GGSN.

4. In case the session modification affects the authorized resources, the PDF sends a COPS DEC message to the GGSN to enforce authorization according to the session modification. The GGSN updates the authorization. If the QoS of the PDP context exceeds the updated authorized QoS and the UE does not modify the PDP context accordingly, the GGSN shall perform a network initiated PDP context modification to reduce the QoS to the authorized level. The GGSN sends a COPS RPT message back to the PDF.

5. The PDF sends an acknowledgement to the AF.