Presentation of Specification to TSG or WG

Presentation to:	**TSG CN Plenary Meeting #24**
Document for presentation:	**TS 29.209, Version 1.0.0**
Presented for:	**Information**

Abstract of document:

The TS defines the Gq interface specifying the policy control procedures between the Application Function (AF) and the Policy Decision Function (PDF)

Changes since last presentation to Meeting #:

The document has not been presented to CN Plenary before.

Outstanding Issues:

- Some updates to AF and PDF procedures to fully align them with the CN3#32 agreed Gq interface encoding (clause 5)
- Final checking that generally textual descriptions are aligned with each other and the Gq interface encoding (clauses 5 and 6)
- Final checking that the new TS 29.209 is fully aligned with the Gq interface related changes (CRs) to TS 29.207 and TS 29.208 (clause 5)
- Final checking that error procedures are complete (clauses 5 and 6)
- Possible minor updates to procedure section due to SA2 discussed IMS messaging (clause 5)

Contentious Issues:

-

3GPP TS 29.209 V1.0.0 (2004-5)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Core Network; Policy control over Gq interface (Release 6)

Keywords
UMTS, QoS

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

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

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

Version x.y.z

where:

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

1 Scope

The present document provides the stage 3 specification of the Gq interface. The functional requirements and the stage 2 specifications of the Gq interface are contained in 3GPP TS 23.002 [2] and 3GPP TS 23.207 [3]. The Gq interface is used for session based policy set-up information exchange between the Policy Decision Function (PDF) and the Application Function (AF).

Whenever it is possible the present document specifies the requirements for the protocol by reference to specifications produced by the IETF within the scope of Diameter. Where this is not possible, extensions to Diameter are defined within the present document.

2 References

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

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications ".

[2] 3GPP TS 23.002: "Network architecture".

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

[4] 3GPP TS 29.207: "Policy control over Go interface".

[5] 3GPP TS 29.208: "End-to-end Quality of Service (QoS) signalling flows".

[6] IETF RFC 3588: "Diameter Base Protocol"

[7] draft-ietf-aaa-diameter-nasreq-14.txt: "Diameter Network Access Server Application [8] IETF RFC 2234: "Augmented BNF for syntax specifications: ABNF"

[9] IETF RFC 3520: "Session Authorization Policy Element"

[10] 3GPP TS 33.210: "3G Security; Network Domain Security (NDS); IP network layer security "

3 Definitions and abbreviations

3.1 Definitions

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

Application Function (AF): element offering applications that require the control of IP bearer resources.

The AF is capable of communicating with the PDF to transfer dynamic QoS-related application information. One example of an AF is the P-CSCF of the IM CN subsystem.

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

One example of an application session is an IMS session.

AF session signalling: used to control the AF session.

One example of AF session signalling is SIP/SDP.

Attribute-Value Pair (AVP): see RFC 3588 [6], corresponds to an Information Element in a Diameter message.

3.2 Abbreviations

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

AAA	AA-Answer
AAR	AA-Request
AF	Application Function
ASA	Abort-Session-Answer
ASR	Abort-Session-Request
AVP	Attribute-Value Pair
GCID	GPRS Charging Id
PDF	Policy Decision Function
RAA	Re-Auth-Answer
RAR	Re-Auth-Request
SBLP	Service Based Local Policy
SDI	Session Description Information
STA	Session-Termination-Answer
STR	Session-termiantion-Request

4 Gq interface

4.1 Overview

The Gq interface is used for the service-based policy set-up information exchange between the Policy Decision Function (PDF) and the Application Function (AF), e.g. the P-CSCF. As defined in the stage 2 specifications (3GPP TS 23.207 [3]), this information is used by the PDF for the service based local policy decisions. The PDF exchanges the policy information with the GGSN as specified in 3GPP TS 29.207 [4].

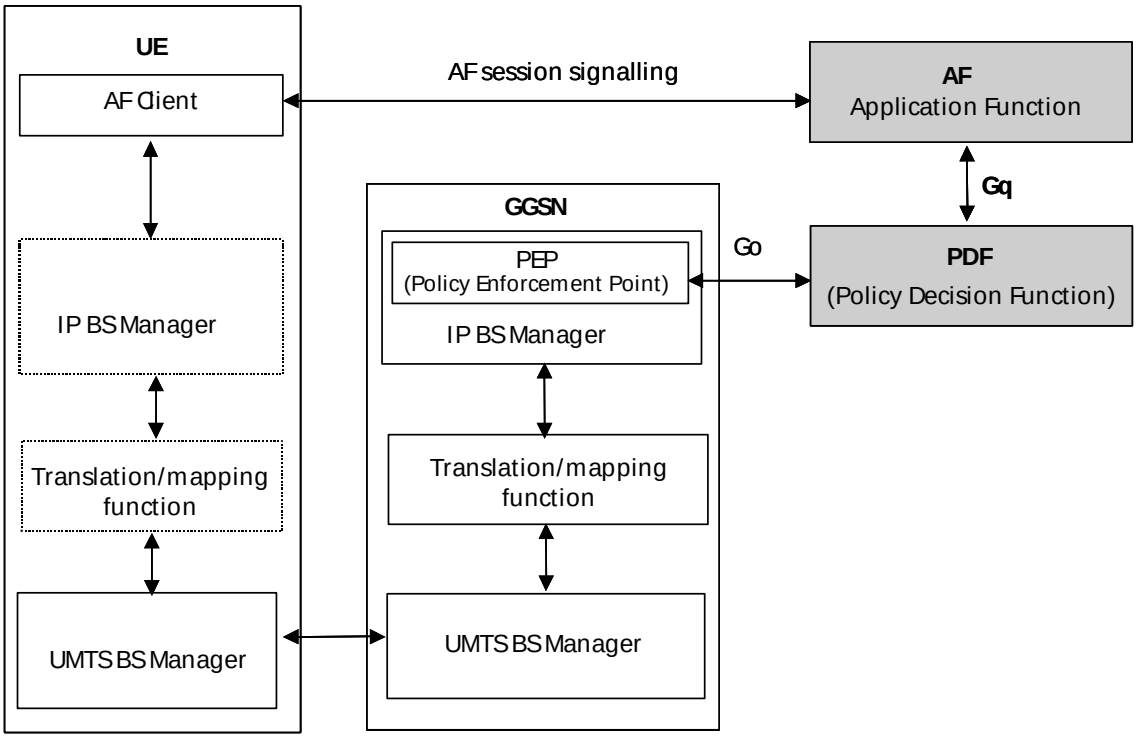
The Gq interface may be an intra- or inter-domain interface. One PDF shall be able to serve more than one AF and one given AF may interact with a number of PDFs, although on an AF session basis, it shall interact with only a single PDF.

Signalling flows related to the Gq interface are specified in 3GPP TS 29.208 [5].

4.2 Gq reference model

The Gq interface is defined between the PDF and the AF. The Gq interface may be an intra- or inter-domain interface. The PDF is in the same PLMN as the GGSN.

The relationships between the different functional entities involved are depicted in figure 4.1.



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

Figure 4.1: Gq interface architecture model

4.3 Functional elements and capabilities

4.3.1 Policy Decision Function (PDF)

The Policy Decision Function (PDF) acts as a Policy Decision Point for service based local policy control. The PDF makes the policy decisions based on the session and media related information obtained from the AF via the Gq interface. The PDF shall exchange the decision information with the GGSN via the Go interface.

4.3.2 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. The AF shall use the Gq interface to exchange service based policy information with the PDF.

5 Policy control procedures

5.1 PDF

5.1.1 Initial authorization of QoS resources

When receiving an initial AA-Request from the AF, the PDF allocates Authorisation-Token(s). The PDF shall store the Diameter base protocol Session-Id received in the AA-Request message for the Authorisation-Token(s). If the AA-

Request contains the Media-Component-Description AVP(s) the PDF shall authorize the required QoS resources and store the SBLP for the session based on the service information. If the AA-Request contains Flow-Grouping AVP(s), the PDF shall only authorize the QoS if the IP flows are distributed to PDP contexts in a way that is allowed by the Flow-Grouping AVP(s). The PDF sends the allocated token(s) in the Authorisation-Token AVP to the AF in the AA-Answer message.

5.1.2 Resource reservation

When receiving the bearer authorization request from the Go interface, the PDF shall authorize the request according to the stored SBLP for the session, if available. If the SBLP is not available for the session, or if the AF has instructed the PDF to do so, the PDF shall send the Re-Auth_Request message with the SERVICE_INFORMATION_REQUEST indication in the Gq-Specific-Action AVP to the AF to request the service information. When receiving the Media-Component-Description AVP(s) in the Re-Auth-Answer message the PDF shall authorize the required QoS resources and stores the SBLP for the session. If SBLP is available for the session but the requested bearer resources exceed it, and the AF has not instructed the PDF to contact it at bearer authorization, the PDF shall deny the resources without contacting the AF.

After the bearer authorization the PDF may send an access network charging identifiers (e.g. GCID) received from the GGSN to the AF for charging correlation purposes. The PDF does this by sending the Re-Auth_Request message with the CHARGING_CORRELATION_EXCHANGE indication in the Gq-Specific-Action AVP to the AF.

5.1.3 Gate function

The AF shall indicate to the PDF as part of the Media-Component-Description AVP(s) whether the media IP flow(s) should be enabled or disabled at the bearer authorization. The PDF may receive a separate AA-Request message(s) from the AF to enable or disable specified IP flows. The PDF shall reply with an AA-Answer and shall include the Access-Network-Charging-Identifier(s) available at this moment. The PDF makes the final decision to enable or disable the authorized IP flows.

5.1.4 Session modification

The PDF may receive the AA-Request message from the AF with modified service information. The PDF shall store the SBLP for the session based on the new service information. The PDF shall acknowledge the session modification by issuing an AA-Answer back to the AF and shall include the Access-Network-Charging-Identifier(s) available at this moment.

5.1.5 Bearer modification

The bearer authorization for the session- or bearer-initiated modification is performed as specified in 3GPP TS 29.207 [4].

If the AF has requested a notification at the loss of a bearer, and the PDF receives a notification that a PDP context is modified to the bandwidth of 0 kbit via the Go interface, the PDF shall send a Re-Auth_Request with the value for the Gq-Specific-Action set to AVP INDICATION_OF_LOSS_OF_BEARER and shall indicate the affected IP flows with the Flows AVP(s) if not all IP flows within an AF session are affected.

If the AF has requested a notification at the recovery of a bearer, and the PDF receives a notification that a PDP context is modified from the bandwidth of 0 kbit to a higher value via the Go interface, the PDF shall send a Re-Auth_Request with the value for the Gq-Specific-Action AVP set to INDICATION_OF_RECOVERY_OF_BEARER and shall indicate the affected IP flows with the Flows AVP(s) if not all IP flows within an AF session are affected.

5.1.6 Revoke authorization

When receiving the Session-Termination-Request message from the AF, the PDF shall revoke the bearer authorization.

5.1.7 Indication of bearer release

When the GGSN informs the PDF of the PDP context release, the PDF shall inform the AF about this event by sending the Abort-Session-Request message with the appropriate Session-Abort-Cause AVP value.

5.2 AF

5.2.1 Initial authorization of QoS resources

When receiving an AF session signalling message initiating a new AF session, the AF requests an authorization for the session from the PDF by sending the AA-Request message. The AF shall include the corresponding Media-Component-Description AVP(s) into the message if the SDI is already available at the AF. The AF may include the Flow-Grouping AVP(s) to request a particular way on how the IP flows described within the service description are distributed to PDP contexts. The AF may also include the AF-Charging-Identifier AVP into the message for the charging correlation purposes.

The AF receives the Authorisation-Token AVP from the PDF in the AA-Answer message. The usage of Authorisation-Token(s) is application dependent.

5.2.2 Resource reservation

The PDF may contact the AF at the UE resource reservation by sending the Re-Auth-Request message with request for the service information. The AF shall respond with the Re-Auth-Answer message containing the Media-Component-Description AVP(s). The information in the Media-Component-Description AVP(s) may be based on the session description information negotiated within the AF session signaling. The receiving of session description request does not trigger the sending of a new authorization request back to the PDF. The AF may include the Flow-Grouping AVP(s) to request a particular way on how the IP flows described within the service description are distributed to PDP contexts.

The AF may receive an access network charging identifier (e.g. GCID) for charging correlation purposes from the PDF in a separate Re-Auth-Request message after the bearer has been authorized. The receiving of charging correlation information from the PDF does not trigger the sending of a new authorization request back to the PDF.

5.2.3 Gate function

The AF shall indicate to the PDF as part of the Media-Component-Description whether the media IP flow(s) should be enabled or disabled at the bearer authorization. Depending on the application, the AF may instruct the PDF also during the session when the IP flow(s) are to be enabled or disabled to pass through the access network. The AF does this by sending the AA-Request message containing the Media-Component- Description AVP(s) that contains the flow status information for the flows to be enabled or disabled.

5.2.4 Session modification

During the AF session modification, the AF shall send an update for the session description information to the PDF based on the new SDI exchanged within the AF session signalling. The AF does this by sending the AA-Request message containing the Media-Component-Description AVP(s) containing the updated service information. The AF may include the Flow-Grouping AVP(s) to request a particular way on how the IP flows described within the service description are distributed to PDP contexts.

The PDF acknowledges the session modification by issueing an AA-Answer back to the AF.

5.2.5 Revoke authorization

When AF session is terminated the AF shall revoke the corresponding bearer authorization by the sending Session-Termination-Request message to the PDF.

6 Gq protocol

6.1 Protocol support

The Diameter Base Protocol as specified in RFC 3588 [6] shall apply except as modified by the defined Gq application specific procedures and AVPs. Unless otherwise specified, the procedures (including error handling and unrecognized information handling) are unmodified.

In addition to the AVPs defined within the sub-clause 6.5, the Diameter AVPs from the Diameter base application [6] are reused within the Diameter messages of the Gq application. The support of AVPs from the Diameter Network Access Server Application (NASREQ) [7] is not required from Diameter implementations that conform to the present document.

Accounting functionality (Accounting Session State Machine, related command codes and AVPs) is not used in the Gq interface.

The Gq application is defined as an IETF vendor specific Diameter application, where the vendor is 3GPP. The vendor identifier assigned by IANA to 3GPP (http://www.iana.org/assignments/enterprise-numbers) is 10415.

Editor's note: The application id needs to be allocated from IANA.

With regard to the Diameter protocol defined over the Gq interface, the PDF acts as a Diameter server, in the sense that it is the network element that handles authorization requests for a particular realm. The AF acts as the Diameter Client, in the sense that is the network element requesting authorization to use bearer path network resources.

The support of Diameter agents between the PDF and the AF, is optional for the IMS, where the Gq is intra operator i.e. GGSN, PDF and P-CSCF are all in the same network.

6.1.1 Advertising application support

The AF and the PDF shall advertise the support of the Gq specific Application by including the value of the application identifier in the Auth-Application-Id AVP and the value of the 3GPP (10415) in the Vendor-Id AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands. The Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands are specified in the Diameter Base Protocol.

6.2 Securing Diameter messages

For secure transport of Diameter messages, see 3GPP TS 33.210 [10].

6.3 Gq messages

Existing Diameter command codes from the Diameter base protocol RFC 2588 [6] and the NASREQ Diameter application (draft-ietf-aaa-diameter-nasreq-14.txt [7]) are used with the Gq specific AVPs. A Gq specific Auth-Application id is used together with the command code to identify the Gq messages.

NOTE: The notion of NAS (Network Access Server) is not used here, NASREQ is just used for protocol purposes, not for its functional meaning.

6.3.1 AA-Request (AAR) command

The AAR command, indicated by the Command-Code field set to 265 and the 'R' bit set in the Command Flags field, is sent by an AF to the PDF in order to request the authorization for the bearer usage for the AF session.

Message Format:

```
<AA-Request> ::= < Diameter Header: 265, REQ, PXY >
                 < Session-Id >
                 { Auth-Application-Id }
                 { Origin-Host }
```

```
                { Origin-Realm }
                { Destination-Realm }
               *[ Media-Component-Description ]
               *[ Flow-Grouping ]
                [ AF-Charging-Identifier ]
               *[ Gq-Specific-Action ]
               *[ Proxy-Info ]
               *[ Route-Record ]
               *[ AVP ]
```

6.3.2 AA-Answer (AAA) command

The AAA command, indicated by the Command-Code field set to 265 and the 'R' bit cleared in the Command Flags field, is sent by the PDF to the AF in response to the AAR command.

Message Format:

```
<AA-Answer> ::=  < Diameter Header: 265, PXY >
                 < Session-Id >
                 { Auth-Application-Id }
                 { Origin-Host }
                 { Origin-Realm }
                 [ Result-Code ]
                 [ Experimental-Result ]
                *[ Authorization-Token ]
                *[ Access-Network-Charging-Identifier ]
                 [ Error-Message ]
                 [ Error-Reporting-Host ]
                *[ Failed-AVP ]
                *[ Proxy-Info ]
                *[ AVP ]
```

6.3.3 Re-Auth-Request (RAR) command

The RAR command, indicated by the Command-Code field set to 258 and the 'R' bit set in the Command Flags field, is sent by the PDF to the AF in order to indicate Gq specific action.

Message Format:

```
<RA-Request> ::= < Diameter Header: 258, REQ, PXY >
                 < Session-Id >
                 { Origin-Host }
                 { Origin-Realm }
                 { Destination-Realm }
                 { Destination-Host }
                 { Auth-Application-Id }
                *{ Gq-Specific-Action }
                *[ Access-Network-Charging-Identifier ]
                *[ Flows ]
                 [ Origin-State-Id ]
                *[ Proxy-Info ]
                *[ Route-Record ]
                *[ AVP]
```

6.3.4 Re-Auth-Answer (RAA) command

The RAA command, indicated by the Command-Code field set to 258 and the 'R' bit cleared in the Command Flags field, is sent by the AF to the PDF in response to the RAR command.

Message Format:

```
<RA-Answer> ::=  < Diameter Header: 258, PXY >
                 < Session-Id >
                 { Auth-Application-Id }
                 { Origin-Host }
                 { Origin-Realm }
                 [ Result-Code ]
                 [ Experimental-Result ]
                *[ Media-Component-Description ]
                *[ Flow-Grouping ]
                 [ Origin-State-Id ]
                 [ Error-Message ]
                 [ Error-Reporting-Host ]
                *[ Failed-AVP ]
                *[ Proxy-Info ]
```

```
                *[ AVP ]
```

6.3.5 Session-Termination-Request (STR) command

The STR command, indicated by the Command-Code field set to 275 and the 'R' bit set in the Command Flags field, is sent by the AF to inform the PDF that an authorized session shall be terminated.

Message Format:

```
<ST-Request> ::= < Diameter Header: 275, REQ, PXY >
                 < Session-Id >
                 { Origin-Host }
                 { Origin-Realm }
                 { Destination-Realm }
                 { Auth-Application-Id }
                 { Termination-Cause }
                 [ Destination-Host ]
                *[ Class ]
                 [ Origin-State-Id ]
                *[ Proxy-Info ]
                *[ Route-Record ]
                *[ AVP ]
```

6.3.6 Session-Termination-Answer (STA) command

The STA command, indicated by the Command-Code field set to 275 and the 'R' bit cleared in the Command Flags field, is sent by the PDF to the AF in response to the STR command.

Message Format:

```
<ST-Answer>  ::= < Diameter Header: 275, PXY >
                 < Session-Id >
                 { Origin-Host }
                 { Origin-Realm }
                 { Auth-Application-Id }
                 [ Result-Code ]
                 [ Experimental-Result ]
                 [ Error-Message ]
                 [ Error-Reporting-Host ]
                *[ Failed-AVP ]
                 [ Origin-State-Id ]
                *[ Redirect-Host ]
                 [ Redirect-Host-Usase ]
                 [ Redirect-Max-Cache-Time ]
                *[ Proxy-Info ]
                 [ AVP ]
```

6.3.7 Abort-Session-Request (ASR) command

The ASR command, indicated by the Command-Code field set to 274 and the 'R' bit set in the Command Flags field, is sent by the PDF to inform the AF that bearer resources for the authorized session are no longer available.

Message Format:

```
<AS-Request>  ::= < Diameter Header: 274, REQ, PXY >
                  < Session-Id >
                 { Origin-Host }
                 { Origin-Realm }
                 { Destination-Realm }
                 { Destination-Host }
                 { Auth-Application-Id }
                 { Session-Abort-Cause }
                 [ Origin-State-Id ]
                *[ Proxy-Info ]
                *[ Route-Record ]
                 [ AVP ]
```

6.3.8 Abort-Session-Answer (ASA) command

The ASA command, indicated by the Command-Code field set to 274 and the 'R' bit cleared in the Command Flags field, is sent by the AF to the PDF in response to the ASR command.

Message Format:

```
<AS-Answer>  ::=  < Diameter Header: 274, PXY >
                   < Session-Id >
                   { Origin-Host }
                   { Origin-Realm }
                   [ Result-Code ]
                    [ Experimental-Result ]
                   [ Origin-State-Id ]
                   [ Error-Message ]
                   [ Error-Reporting-Host ]
                  *[ Failed-AVP ]
                  *[ Redirected-Host ]
                   [ Redirected-Host-Usage ]
                   [ Redirected-Max-Cache-Time ]
                  *[ Proxy-Info ]
                  *[ AVP ]
```

6.4 Gq Experimental-Result-Code AVP values

This subclause defines the Gq specific values of the Experimental-Result-Code AVP:

DIAMETER_INVALID_SERVICE_INFORMATION (5001)

The PDF cannot authorize the bearer with the service information provided by the AF.

DIAMETER_GATE_NOT_MATCH (5002)

The PDF cannot associate the gate specified in the gate control request from the AF to any existing IP flow filters.

6.5 Gq specific AVPs

The table 6.5.1 describes the Diameter AVPs defined for the Gq interface protocol, their AVP Code values, types, possible flag values and whether or not the AVP may be encrypted. The Vendor-Id header of all AVPs defined in the present document shall be set to 3GPP (10415).

Table 6.5.1: Gq specific Diameter AVPs

				AVP Flag rules (note 1)				
Attribute Name	AVP Code	Clause defined	Value Type (note 2)	Must	May	Should not	Must not	May Encr.
Access-Network-Charging-Identifier		6.5.1	Grouped	M,V	P			Y
Access-Network-Charging-Identifier-Value		6.5.2	OctetString	M,V	P			Y
AF-Application-Identifier		6.5.3	OctetString	M,V	P			Y
AF-Charging-Identifier		6.5.4	OctetString	M,V	P			Y
Authorization-Token		6.5.5	OctetString	M,V	P			Y
Flow-Description		6.5.6	IPFilterRule	M,V	P			Y
Flow-Grouping		6.5.7	Grouped	M,V	P			Y
Flow-Number		6.5.8	Unsigned32	M,V	P			Y
Flows		6.5.9	Grouped	M,V	P			Y
Flow-Status		6.5.10	Enumerated	M,V	P			Y
Gq-Specific-Action		6.5.11	Enumerated	M,V	P			Y
Max-Requested-Bandwidth		6.5.12	Unsigned32	M,V	P			Y
Max-Requested-Bandwidth-DL		6.5.13	Unsigned32	M,V	P			Y
Max-Requested-Bandwidth-UL		6.5.14	Unsigned32	M,V	P			Y
Media-Component-Description		6.5.15	Grouped	M,V	P			Y
Media-Component-Number		6.5.16	Unsigned32	M,V	P			Y
Media-Type		6.5.18	Enumerated	M,V	P			Y
RR-Bandwidth		6.5.19	Unsigned32	M,V	P			Y
RS-Bandwidth		6.5.20	Unsigned32	M,V	P			Y
RTCP-Flows		6.5.21	Grouped	M,V	P			Y
Session-Abort-Cause		6.5.22	Enumerated	M,V	P			Y

NOTE 1: The AVP header bit denoted as 'M', indicates whether support of the AVP is required. The AVP header bit denoted as 'V', indicates whether the optional Vendor-ID field is present in the AVP header. For further details, see RFC 3588 [6].
NOTE 2: The value types are defined in IETF RFC 3588 [6].

6.5.1 Access-Network-Charging-Identifier AVP

The Access-Network-Charging-Identifier AVP (AVP code x) is of type Grouped, and contains a charging identifier (e.g. GCID) within the Access-Network-Charging-Identifier-Value AVP along with information about the flows transported within the corresponding bearer within the Flows AVP. If no Flows AVP is provided, the Access-Network-Charging-Identifier-Value applies for all flows within the AF session.

The Access-Network-Charging-Identifier AVP may be sent from the PDF to the AF. The AF may use this information for charging correlation with session layer.

AVP Format:

```
Access-Network-Charging-Identifier ::= < AVP Header: x >
                    { Access-Network-Charging-Identifier-Value}
                    *[ Flows ]
```

6.5.2 Access-Network-Charging-Identifier-Value AVP

The Access-Network-Charging-Identifier-Value AVP (AVP code 1) is of type OctetString, and contains a charging identifier (e.g. GCID).

6.5.3 AF-Application-Identifier AVP

The AF-Application-identifier AVP (AVP code x) is of type OctetString, and it contains information that identifies the particular service that the AF service session belongs to. This information may be used by the PDF to differentiate QoS for different application services. For example the AF-Application-Identifier may be used as additional information together with the Media-Type AVP when the QoS class for the bearer authorisation at the Go interface is selected. The AF-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 full Session-Component-Description information.

Editor's Note: If a similar AVP is required for the entire session is FFS.

6.5.4 AF-Charging-Identifier AVP

The AF-Charging-Identifier AVP (AVP code 2) is of type OctetString, contains the AF Charging Identifier that is sent from the AF to the PDF. The PDF may use this information for charging correlation with bearer layer.

6.5.5 Authorization-Token AVP

The Authorization-Token AVP (AVP code 3) is of type OctetString, and contains the Authorization Token defined in the RFC 3520 [9].

6.5.6 Flow-Description AVP

The Flow-Description AVP (AVP code 4) is of type IPFilterRule, and defines a packet filter for an IP flow with the following information:

- Direction (in or out)
- Source and destination IP address (possibly masked)
- Protocol
- Source and destination port (list or ranges)

The IPFilterRule type shall be used with the following restrictions:

- Only the Action "permit" shall be used.
- No "options" shall be used.
- The invert modifier "!" for addresses shall not be used.
- The keyword "assigned" shall not be used.
- For direction "out", an IPv4 destination IP address shall not be wildcarded. For direction "out", the 64 kbits network prefix of an IPv6 destination IP address shall not be wildcarded.

Editor's note: The error handling if any of these rules is not observed is FFS.

The Flow description AVP shall be used to describe a single IP flow.

The direction "in" refers to uplink IP flows, and the direction "out" refers to downlink IP flows.

6.5.7 Flow-Grouping AVP

The Flow-Grouping AVP (AVP code x) is of type Grouped, and it indicates that no other IP Flows shall be transported together with the listed IP Flows in the same PDP context(s).

AVP Format:

Flow-Grouping ::= < AVP Header: x >
1*{Flows}

6.5.8 Flow-Number AVP

The Flow-Number AVP (AVP code x) is of type Unsigned32, and it contains the ordinal number of the IP flow(s), assigned according to the rules in Annex C of TS 29.207 [4].

6.5.9 Flows AVP

The Flows AVP (AVP code x) is of type Grouped, and it indicates IP flows via their flow identifiers.

If no Flow-Number AVP(s) are supplied, the Flows AVP refers to all Flows matching the media component number.

AVP Format:

Flows::= < AVP Header: x >
{ Media-Component-Number}
*[Flow-Number]

6.5.10 Flow-Status AVP

The Flow-Status AVP (AVP code 5) is of type Enumerated, and describes whether the IP flow(s) are enabled or disabled. The following values are defined:

ENABLED-UPLINK (0)

This value shall be used to enable associated uplink IP flow(s) and to disable associated downlink IP flow(s).

ENABLED-DOWNLINK (1)

This value shall be used to enable associated downlink IP flow(s) and to disable associated uplink IP flow(s).

ENABLED (2)

This value shall be used to enable all associated IP flow(s) in both directions.

DISABLED (3)

This value shall be used to disable all associated IP flow(s) in both directions.

REMOVED (4)

The IP Filters for the associated IP flow(s) shall be removed.

6.5.11 Gq-Specific-Action AVP

The Gq-Specific-Action AVP (AVP code 7) is of type Enumerated, and determines the type of the Gq action within the PDF initiated request.

Within an initial AA request the AF may use the Gq-Specific-Action AVP to request specific actions from the PDF at the bearer authorization and to limit the contact at bearer authorization to such bearer authorization events where this action is required. If the Gq-Specific-Action AVP is omitted within the initial AA request, no notification of any of the events defined below is requested.

The following values are defined:

SERVICE_INFORMATION_REQUEST (0)

This value shall be used when the PDF requests the service information from the AF for the bearer authorization. In the AAR, this value indicates that the AF requests the PDF to demand service information at each bearer authorization

CHARGING_CORRELATION_EXCHANGE (1)

This value shall be used when the PDF reports the access network charging identifier to the AF. The PDF shall include the Access-Network-Charging-Identifier AVP within the request. In the AAR, this value indicates that the AF requests the PDF to provide an access network charging identifier to the AF at each bearer authorization, when a new access network charging identifier becomes available.

INDICATION_OF_LOSS_OF_BEARER (2)

This value shall be used when the PDF reports a loss of a bearer (PDP context bandwidth modification to 0 kbit) to the AF. In the AAR, this value indicates that the AF requests the PDF to provide a notification at the loss of a bearer.

INDICATION_OF_RECOVERY_OF_BEARER (3)

This value shall be used when the PDF reports a recovery of a bearer (PDP context bandwidth modification from 0 kbit to another value) to the AF. In the AAR, this value indicates that the AF requests the PDF to provide a notification at the recovery of a bearer.

6.5.12 Max-Requested-Bandwidth AVP

The Max-Requested-Bandwidth AVP (AVP code x) is of type Unsigned32, and it indicates the maximum requested bandwidth in bits per second for an uplink or downlink IP flow.

6.5.13 Max-Requested-Bandwidth-DL AVP

The Max-Requested-Bandwidth-DL AVP (AVP code x) is of type Unsigned32, and it indicates the maximum requested bandwidth in bits per second for a downlink IP flow.

6.5.14 Max-Requested-Bandwidth-UL AVP

The Max -Bandwidth-UL AVP (AVP code x) is of type Unsigned32, and it indicates the maximum requested bandwidth in bits per second for an uplink IP flow.

6.5.15 Media-Component-Description AVP

The Media-Component-Description AVP (AVP code x) is of type Grouped, and it contains service information for a single media component within an AF session. It may be based on the SDI exchanged between the AF and the AF client in the UE. The information is used by the PDF to determine authorized QoS and IP flow classifiers for bearer authorization.

Within one Gq message, a single IP flow shall not be described by more than one Session-Component-Description AVP.

If a Media-Component-Description AVP is not supplied, or if optional AVP(s) within a Media-Component-Description AVP are omitted, but corresponding information has been provided in previous Gq messages, the previous information for the corresponding IP flow(s) remains valid. A Media-Component-Description AVP is disabled by supplying a Flow Status AVP with value "REMOVED".

Editor´s Note: The usage of several AVPs on media component level requires further explanatory text.

AVP format:

```
Media-Component-Description ::= < AVP Header: ?>
                                { Media-Component-Number } ; Ordinal number of the media comp.
                               *[ Media-Sub-Component ]        ; Set of flows for one flow identifier
                                [ AF-Application-Identifier ]
                                [ Media-Type ]
                                [ Max-Requested-Bandwidth ]
                                [ Flow-Status ]
                                [ RTCP-Flows ]
                                [ RS-Bandwidth ]
                                [ RR-Bandwidth ]
```

6.5.16 Media-Component-Number AVP

The Media-Component-Number AVP (AVP code x) is of type Unsigned32, and it contains the ordinal number of the media component, assigned according to the rules in Annex C of TS 29.207 [4].

6.5.17 Media-Sub-Component AVP

The Media-Sub-Component AVP contains the requested QoS and filters for the set of IP flows identified by their common Flow-Identifier. The Flow-Identifier is defined in 3GPP TS 29.207[4].

AVP format:

```
Media-Sub-Component ::= < AVP Header: ?>
                        { Flow-Number }      ; Ordinal number of the IP flow
                     1*2[ Flow-Description ]        ; UL and/or DL
                        [ Flow-Status ]
                        [ Max-Requested-Bandwidth-UL ]
                        [ Max-Requested-Bandwidth-DL ]
```

6.5.18 Media-Type AVP

The Media-Type AVP (AVP code x) is of type Enumerated, and it determines the media type of a session component. The following values are defined:

AUDIO (0)

VIDEO (1)

DATA (2)

APPLICATION (3)

CONTROL (4)

6.5.19 RR-Bandwidth AVP

The RR-Bandwidth AVP (AVP code x) is of type Unsigned32, and it indicates the maximum required bandwidth in bits per second for RTCP receiver reports within the session component, as specified in RFC 3556 [x].

6.5.20 RS-Bandwidth AVP

The RS-Bandwidth AVP (AVP code x) is of type Unsigned32, and it indicates the maximum required bandwidth in bits per second for RTCP sender reports within the session component, as specified in RFC 3556 [x].

6.5.21 RTCP-Flows AVP

The RTCP-Flows AVP (AVP code x) is of type Grouped, and provides Flow Numbers of IP Flows within a media component used to transport RTCP.

AVP Format:

```
RTCP-Flows ::= < AVP Header: x >
        1*{Flow-Number}
```

6.5.22 Session-Abort-Cause AVP

The Session-Abort-Cause AVP (AVP code x) is of type Enumerated, and determines the cause of the session abort request. The following values are defined:

PDP_CONTEXT_RELEASED (0)

This value is used when the PDP context has been deactivated as a result from normal PDP context signalling handling.

INSUFFICIENT_PDF_RESOURCES (1)

This value is used to indicate that the PDF is overloaded and needs to abort the session.

INSUFFICIENT_BEARER_RESOURCES (2)

This value is used when the PDP context has been deactivated due to insufficient bearer resources at the GGSN.

Editor's note: More values are to be defined later as needed.

Annex A:

Editor's note: Normative and informative annexes are included as needed.

Annex B (informative): Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
29-08-03					Presented to CN3#29 for information		001
02-03-04					CN3#31 agreed contributions amended	001	002
22-04-04					CN3#31bis agreed contributions amended	002	010
18-05-04					CN3#32 agreed contributions amended. The version is submitted for information for the CN Plenary.	010	100