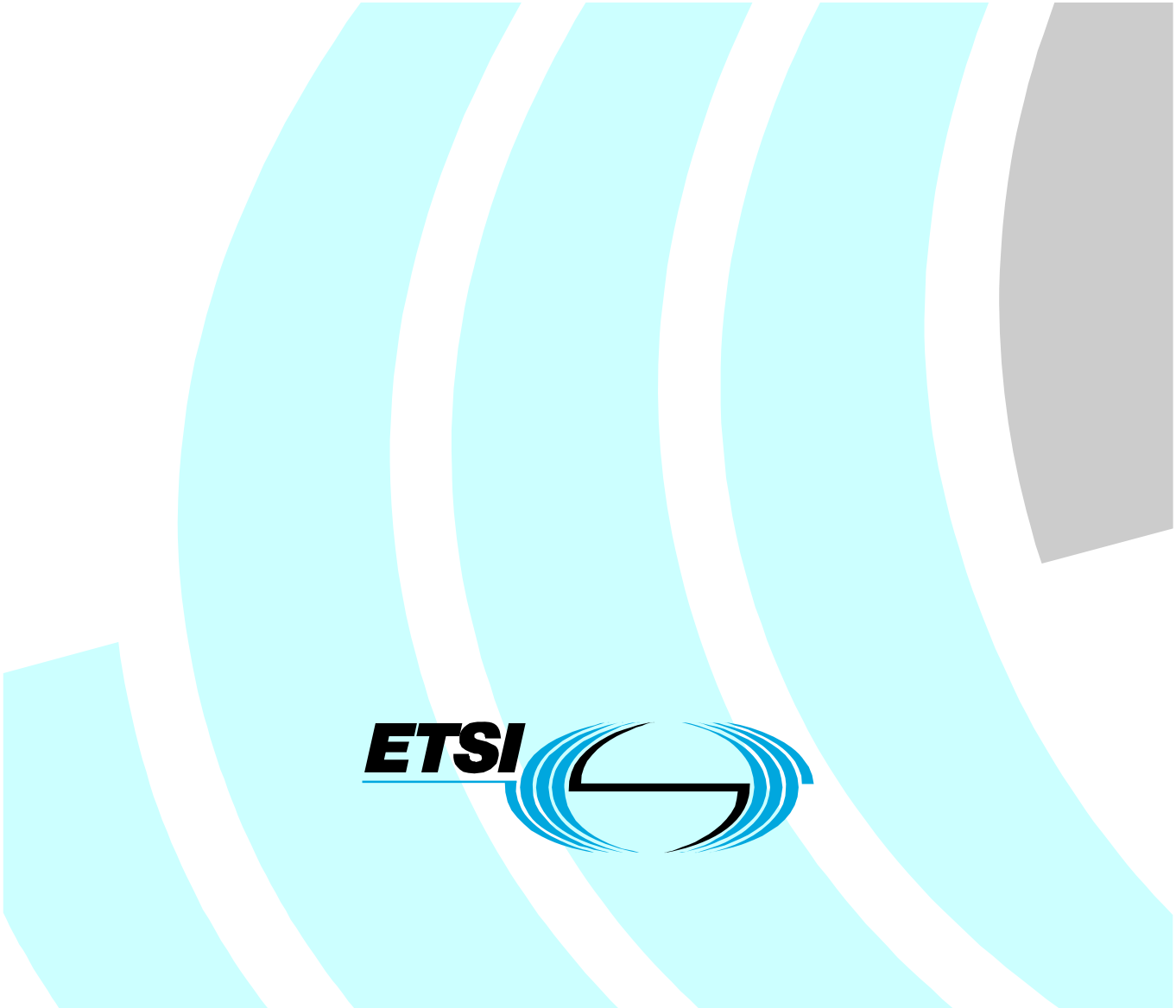
ETSI TS 183 017 V1.4.0 (2007-08)

Technical Specification

Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control: DIAMETER protocol for session based policy set-up information exchange between the Application Function (AF) and the Service Policy Decision Function (SPDF); Protocol specification



Reference
RTS/TISPAN-03076-NGN-R1

Keywords
interface, stage 3

ETSI

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

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

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

Contents

Intellectual Property Rights

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

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

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

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 ES 282 001 [1] and ES 282 003 [2]. The Gq' interface is the interface between the Application Function (AF) and the Service Policy Decision Function (SPDF) and is used for session based policy set-up information exchange between the SPDF and the AF.

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.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

[1] ETSI ES 282 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture Release 1".

[2] ETSI ES 282 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control Sub-system (RACS); Functional Architecture".

[3] IETF RFC 3588: "Diameter Base Protocol".

[4] ETSI TS 129 209: "Universal Mobile Telecommunications System (UMTS); Policy control over Gq interface (3GPP TS 29.209 Release 6)".

[5] IETF RFC 4005: "Diameter Network Access Server Application".

[6] ETSI TS 133 210: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Network Domain Security (NDS); IP network layer security (3GPP TS 33.210 Release 7)".

[7] ETSI TS 283 003: "TISPAN Release 1 Endorsement of 3GPP TS 24.229: IP Multimedia Call Control Protocol based on SIP and SDP; Stage 3".

[8] ETSI ES 283 018: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control: H.248 Profile for controlling Border Gateway Functions (BGF) in the Resource and Admission Control Subsystem (RACS); Protocol specification".

[9] IETF RFC 4566: "SDP: Session Description Protocol".

[10] IETF RFC 2960: "Stream Control Transmission Protocol".

[11] IETF RFC 3309: "SCTP Checksum Change".

[12] ETSI TS 129 207: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Policy control over Go interface (3GPP TS 29.207 Release 6)".

[13] ETSI ES 283 035: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment Sub-System (NASS); e2 interface based on the DIAMETER protocol".

[14] ETSI ES 283 026: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control; Protocol for QoS reservation information exchange between the Service Policy Decision Function (SPDF) and the Access-Resource and Admission Control Function (A-RACF) in the Resource and Protocol specification".

[15] ETSI ES 283 034: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment Sub-System (NASS); e4 interface based on the DIAMETER protocol".

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

[17] IETF RFC 3388: "Grouping of Media Lines in the Session Description Protocol (SDP)".

[18] IETF RFC 3524: "Mapping of Media Streams to Resource Reservation Flows".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

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

NOTE: The AF is capable of communicating with the SPDF to transfer dynamic QoS-related application information. One example of an AF is the P-CSCF of the IMS.

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

NOTE: One example of an application session is an IMS session.

AF session signalling: used to control the AF session

NOTE: One example of AF session signalling is SIP/SDP.

Attribute-Value Pair (AVP): Information Element in a Diameter message

NOTE: See RFC 3588 [3].

hard-state reservation: type of reservation whereby the requested resources are reserved without time limit

NOTE: Hard-state reservations are terminated when the DIAMETER session is terminated.

soft-state reservation: type of reservation whereby the requested resources are reserved for a finite amount of time

NOTE: Soft-state reservations are terminated if the DIAMETER session is terminated.

3.2 Abbreviations

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

A-RACF	Access-RACF
AAA	AA-Answer
AAR	AA-Request
AF	Application Function

ASA	Abort-Session-Answer
ASR	Abort-Session-Request
AVP	Attribute-Value Pair
BGF	Border Gateway Function
CER	Capabilities-Exchange-Request
CEA	Capabilities-Exchange-Answer
IANA	Internet Assigned Numbers Authority
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IP-CAN	IP-Connectivity Access Network
NAPT	Network Address and Port Translation
NASREQ	Network Access Server Application
P-CSCF	Proxy - Call Session Control Function
PDF	Policy Decision Function
QoS	Quality of Service
RAA	Re-Auth-Answer
RACF	Resource and Admission Control Function
RACS	Resource and Admission Control Subsystem
RAR	Re-Auth-Request
RTP	Real Time Protocol
SDI	Session Description Information
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SPDF	Service-based Policy Decision Function
STA	Session-Termination-Answer
STR	Session-Termination-Request
UDP	User Datagram Protocol
UE	User Equipment
UL AVP	Up Link Attribute Value Pair

4 Gq' interface

4.1 Overview

The Gq' interface is used for the service-based policy set-up information exchange between the SPDF and the AF, e.g. the P-CSCF. As defined in the stage 2 specification (ES 282 003 [2]), this information is used by the SPDF for the Service Based Policy decisions.

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

4.2 Gq' reference model

The Gq' interface is defined between the AF and the SPDF. Within the present release, the Gq' interface is used for requesting transport plane resources and admission control for fixed broadband access networks (e.g. xDSL).

When supporting a GPRS IP-CAN, the AF shall apply the procedures specified in TS 129 209 [4].

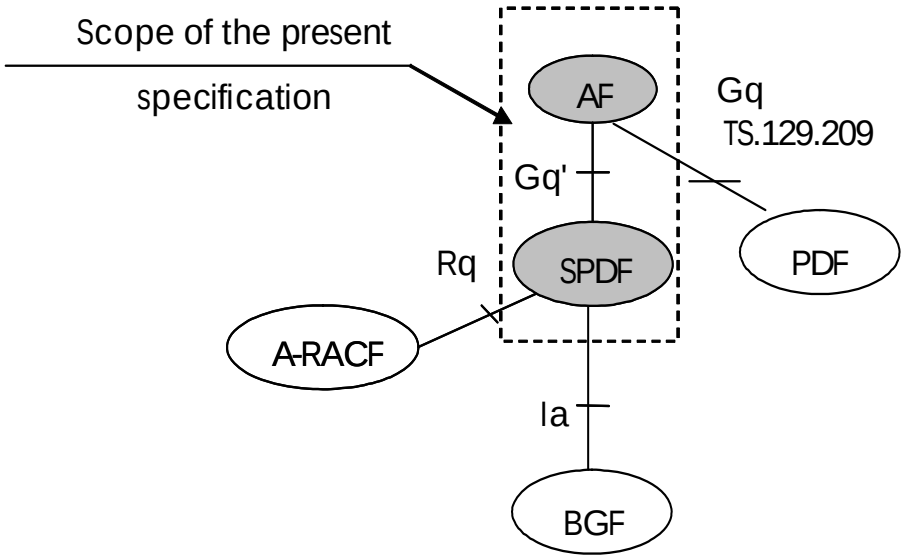


Figure 1: Gq' reference model

4.3 Functional elements and capabilities

4.3.1 Service-based Policy Decision Function (SPDF)

The SPDF is a functional element that coordinates the resource reservation requests received from the AF. The SPDF makes policy decisions using policy rules and forwards the session and media related information obtained from the AF to the A-RACF for admission control purposes. Additionally, based on information received on the Gq' interface and on configuration data, the SPDF may request the instantiation of a border gateway function (BGF) via the Ia interface. The functionality of the SPDF is further detailed in ES 282 003 [2].

4.3.2 Application Function (AF)

The AF is a functional element offering applications that request and use IP bearer resources. The AF shall use the Gq' interface to exchange session and media related information with the SPDF. One example of an application function is the P-CSCF of the IMS.

5 Procedures descriptions

5.1 Procedures at the AF

5.1.1 Initial reservation for a session

Upon receipt of an AF session signalling message initiating a new AF session, the AF shall request an authorization for the session from the SPDF by sending the AA-Request message. This AA-Request message shall contain a new Session-Id.

NOTE: As specified in RFC 3588 [3], the Session-Id is globally unique and is meant to uniquely identify a user session without reference to any other information. The Session-Id begins with the sender's identity encoded in the DiameterIdentity type.

The AA-Request message may contain an Authorization-Lifetime AVP as a hint of the maximum lifetime that it is requesting. When requesting for Hard-state reservation, the AF shall not include an Authorization-Lifetime AVP.

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 for the IP flows described within the service description to be distributed to IP-CAN bearers.

When providing a given Media-Component-Description AVP in the initial AA-Request, the AF may request the SPDF to Commit the requested resources by setting the Flow-Status AVP to the value ENABLED, ENABLED-UPLINK or ENABLED-DOWNLINK. Alternatively, the AF may perform this in two phases in using separate reserve and commit operations. When using the two phases method, the Flow-Status AVP value of the initial AA-Request message shall be set to DISABLED.

The AF may also include the AF-Charging-Identifier AVP into the message for the charging correlation purposes.

Based on local configuration data, the AF determines that address translation needs to occur on the user plane (e.g. a BGF on the media path performs NAPT, IP version interworking or hosted NAPT procedures), upon receipt of SDI pointing towards the endpoint served by the AF (e.g. for IMS, in case the P-CSCF receives an SDP offer sent by the served UE), the AF shall include the Binding-Information AVP with the Input-List AVP. The Input-List AVP shall be populated based on the received SDI as follows:

- for each IP-flow information within the received SDI, the AF shall set the V6-Transport-Address AVP or V4-Transport-Address AVP with the corresponding IP address and port number.

If required (e.g. the received SDI is sent by a served endpoint with hosted-NAPT configuration), the AF may also include the Latching-Indication AVP set to "LATCH".

For the purpose of access profile correlation in the A-RACF, the AF shall include within the AA-Request a correlation identifier in the form:

- either of the User-Name AVP; and/or
- the Globally-Unique-Address AVP.

The above AVPs are defined in [13] and their contents are made available to the AF via the e2 interface.

The mapping of information element names defined in [2] and Diameter AVPs used in this document is given in table 5.1.1.1.

Table 5.1.1.1: Mapping of information element names to Diameter AVPs

Information element name	Mapping to Diameter AVP	Cat.
Subscriber ID	User-Name	O
Globally Unique IP Address	Globally-Unique-Address	O
Requestor Name	AF-Application-Identifier	O
Service Class	Service-Class	O
Media Type	Media-Type	O
Reservation Class	Reservation-Class	O
Transport Service Class	Transport-Class	O

The AF may specify the Reservation-Priority AVP at request level in the AA-Request in order to assign a priority to the request. The AF may further specify the Reservation-Priority AVP in Media-Component-Description AVP(s) in order to assign priority to individual media. If the Reservation-Priority AVP is not specified the requested priority is DEFAULT (0).

The AF may specify the Specific-Action AVP in the AA-Request with the events of which it wants to be informed.

The AF shall store the contents of the Output-List AVP received within the Binding-Information AVP contained in the AA-Answer message for future use.

The behaviour when the AF does not receive the AA-Answer, or when it arrives after the internal timer waiting for it has expired, or when it arrives with an indication different than DIAMETER_SUCCESS, is outside the scope of the present document.

5.1.2 Session modification

During the AF session modification, the AF shall send an update for the session description information to the SPDF based on the new SDI exchanged within the AF session signalling. The AF does this by sending the AA-Request message with an existing Session-Id and Media-Component-Description AVP(s) containing the updated service information. When refreshing an existing session, the AF may issue an AA-Request without any Media-Component-Description AVP. The AF may include the Flow-Grouping AVP(s) to request a particular way for the IP flows described within the service description to be distributed to IP-CAN bearers.

The AF SHALL NOT use the RAA to modify the session service information. As an option, the AF MAY send an AAR command following an RAA to update the session service information.

The AF may perform the following operations:

- Add a new IP flow within an existing media component - provide a new Media-Sub-Component AVP within the corresponding Media-Component-Description AVP.
- Add a new IP flow within a new media component - provide a new Media-Component-Description AVP.
- Modify a media component - update the corresponding Media-Component-Description AVP (e.g. increase or decrease the allocated bandwidth).
- Modify an existing IP flow within a media component - update the corresponding Media-Sub-Component AVP.
- Modify the commit status - change the Flow-Status AVP of the corresponding Media-Component-Description AVP and/or Media-Sub-Component to one of the values ENABLED-UPLINK (0), ENABLED-DOWNLINK (1) or ENABLED (2), according to the direction in which the resources are to be committed.
- Release a media component - provide the corresponding Media-Component-Description AVP with the Flow-Status AVP set to the value REMOVED (4).
- Release an IP flow within a media component - provide the corresponding Media-Sub-Component AVP with the Flow-Status AVP set to the value REMOVED (4).
- Refresh a soft-state reservation - provide an Authorization-Lifetime AVP in the AA-Request as a hint of the maximum lifetime that it is requesting.

In case any of the Specific-Action AVP, the AF-Charging-Identifier AVP, the Flow-Grouping AVP, the Service-Class AVP, the User-Name AVP, or the Globally-Unique-Address AVP was provided in an initial AA-Request, the provided AVP(s) shall have the same value if provided also in a modifying AA-Request.

If present, the Reservation-Priority AVP associated with a reservation request or a media component shall not be modified by the AF.

The AF may also, if updated SDI pointing towards the endpoint served by the AF is available with updated addressing information pointing to the served endpoint, and that it determines that address translation needs to occur on the user plane (e.g. BGF on the media path performs NAPT, IP version interworking or hosted NAPT procedures), the AF shall include the Binding-Information AVP with the Input-List AVP set based on the received SDI. The Input-List AVP shall contain addressing information for the entire set of IP flows (i.e. modified and non modified).

The AF shall store the contents of the Output-List AVP received within the Binding-Information AVP contained in the AA-Answer message for future use.

If required (e.g. in cases where the served endpoint is behind a hosted-NAPT), and updated addressing information pointing towards the served endpoint is available, the AF shall include the Latching-Indication AVP set to "RELATCH".

The behaviour when the AF does not receive the AA-Answer, or when it arrives after the internal timer waiting for it has expired, or when it arrives with an indication different than DIAMETER_SUCCESS, are outside the scope of the present document.

5.1.3 Session termination

When the AF session is terminated, the AF shall terminate the Diameter session by sending a Session-Termination-Request message to the SPDF.

5.2 Procedures at the SPDF

5.2.1 Initial reservation for a session

Upon receipt of an initial AA-Request, the SPDF determines based on local policy whether a BGF and/or an A-RACF need to be involved in the AF session. If this is the case, the SPDF determines the address of the BGF and A-RACF using local policy.

If the AA-Request contains the Media-Component-Description AVP(s), the SPDF shall trigger the Resource Reservation procedure towards the A-RACF. If the AA-Request contains the User-Name AVP and/or the Globally-Unique-IP-Address AVP, the SPDF uses this information as part of the resource reservation procedure performed on the Rq interface.

Additionally, based on the contents of the AA-Request (e.g. the AA-Request may contain AVPs such as the Reservation-Class AVP and/or Binding-Information AVP) and on local policy rules, the SPDF may request BGF services.

The SPDF shall wait for the result of the above interaction(s) with the A-RACF and/or the BGF before returning, in a single AA-Answer message, the result of those interactions to the AF. The contents of the AA-Answer shall be derived as follows:

- If the resource reservation procedure succeeds and if the requested binding information was received via the Ia interface, the AA-Answer message sent by the SPDF to the AF shall contain the Binding-Output-List AVP.
- If the resource reservation procedure fails (i.e. the SPDF receives a reservation failure notification via the Rq interface), the SPDF shall return the Experimental-Result-Code AVP with the value INSUFFICIENT_RESOURCES in the AA-Answer.
- If the resource reservation procedure succeeds but the SPDF did not succeed in getting a binding via the Ia interface, the SPDF shall return the Experimental-Result-Code AVP with the value BINDING_FAILURE in the AA-Answer.
- If the SPDF fails in finding an appropriate A-RACF or BGF instance needed to serve the resource reservation request, the SPDF may return the Result-Code with the value UNABLE_TO_DELIVER in the AA-Answer.

Once the SPDF recognizes, based on the contents of an AA-Request and possibly on configuration data, that BGF services are requested on the transport plane, the SPDF shall use the contents of the AA-Request in order to enforce any service needed over the Ia interface. The detailed procedures are as specified in [8].

5.2.2 Session modification

The SPDF may receive the AA-Request message from the AF with modified service information. Based on the contents of the AA-Request, the SPDF shall coordinate any required modifications to existing resource reservation over the Rq interface and/or to existing BGF settings instancied via the Ia interface. As described in clause 5.2.1, the SPDF shall acknowledge the session modification by issuing an AA-Answer back to the AF only after all actions taken upon the Rq and/or Ia interfaces are achieved.

Depending on the value of the Flow-Status AVP received from the AF, the SPDF may interpret the session modification as a commitment of requested resources.

Once the SPDF recognizes, based on the contents of an AA-Request and possibly on configuration data, that BGF functions are requested on the transport plane or that BGF functions are already in use and need to be configured, the SPDF shall use the contents of the AA-Request in order to enforce any functions needed over the Ia interface. The detailed procedures are as specified in [8].

5.2.3 Session termination

Upon receipt of a Session-Termination-Request message from the AF, the SPDF shall trigger the session termination procedure over the Rq interface and revoke any transport plane functions enforced over the Ia interface as a result of this session.

5.2.4 SPDF notifications

The Gq' interface supports facilities for indicating, on request basis, relevant events like revocation of established resource reservations. The SPDF shall send unsolicited RA-Request messages to the AF. Such messages are implicitly requested through policies established in the AF via the Specific-Action AVP (see 7.3.23) of the initial AA-Request message.

If one of the events supported at the Gq' interface occurs, the SPDF shall send an unsolicited RAR message to the AF:

- The value of the Specific-Action AVP, indicating the event that occurred.
- Optionally, the appropriate Abort-Cause AVP value.

5.3 IMS related P-CSCF procedures

5.3.1 Provisioning of service information at the P-CSCF

The P-CSCF shall send service information to the SPDF upon every SIP message that includes an SDP answer payload.

NOTE: The present clause assumes that the SDP payload is not encrypted when received in a SIP message.

The service information shall be derived both from the SDP offer and the SDP answer. This ensures that the SPDF receives proper information for all possible IMS session set-up scenarios, and that the SPDF is also capable of handling session modifications.

All media components in the SDP shall be sent. Therefore, the P-CSCF shall derive a media component within the session information from every SDP media component, as detailed in annex B. The SDP contains sufficient information about the session, such as the end-points' IP address and port numbers and bandwidth requirements.

The P-CSCF shall derive the Flow-Description AVP within the service information from the SDP as follows:

- An uplink Flow-Description AVP shall be formed as follows: The destination address and port number shall be taken from the connection information parameter of the SDP received by the P-CSCF in the downlink direction, while the source IP address may be formed from the address present in the SDP received by the P-CSCF in the uplink direction, and the source port number shall be wildcarded. For example, assuming UE A sends an SDP to UE B, the SPDF of UE B uses the address present in this SDP for the destination address of UE B's uplink Flow-Description AVP, while the SPDF of the UE A uses the same address for the source address of UE A's uplink Flow-Description AVP. If the source address is not formed from the 64 bit prefix, the source address shall be wild carded.

- A downlink Flow-Description AVP shall be formed as follows: the destination address and port number shall be taken from the connection information parameter of the SDP received by the P-CSCF in the uplink direction, while the source IP address may be formed (in order to reduce the possibilities of bearer misuse) from the destination address in the SDP received by the P-CSCF in the downlink direction (taking into account only the 64 bit prefix of the IPv6 address) and the source port number shall be wildcarded. For example, assuming UE A sends an SDP to UE B, the SPDF of UE a uses the address present in this SDP for the destination address of UE A's downlink Flow-Description AVP, while the SPDF of UE B uses the 64 bit prefix of the same address for the source address of UE B's downlink Flow-Description AVP. If the source address is not formed from the 64 bit prefix, the source address shall be wild carded.

The P-CSCF shall derive the bandwidth information within the service information, from the "b=AS" SDP parameter, as detailed in annex B. For the possibly associated RTCP IP flows, the P-CSCF shall use the SDP "b=RR" and "b=RS" parameters, if present, as specified in annex B. The "b=AS", "b=RR" and "b=RS" parameters in the SDP contain all the overhead coming from the IP-layer and the layers above, e.g. IP, UDP, RTP and RTCP payload, or IP, UDP and RTCP.

5.3.2 Enabling IP flows at the P-CSCF

Prior to the completion of the SIP session set-up, i.e. until the 200 OK(INVITE) is received, the P-CSCF may enable or disable media IP flows depending on operator policy, thus allowing or forbidding early media in forward and/or backward directions. If early media is to be disabled, the P-CSCF may modify the values of the Flow-Status AVPs derived from SDP according to table B.1 of annex B. If the P-CSCF chooses to modify the values, the P-CSCF shall store the last received SDP.

When the 200 OK is received, the P-CSCF shall enable all media IP flows according to the direction attribute within the last received SDP, as specified in annex B. When the 200 OK is received and the P-CSCF previously provided modified values of the Flow-Status AVPs in the session information, the P-CSCF shall provide service information with values of the Flow-Status AVPs corresponding to the last received SDP.

If the P-CSCF receives SDP answers after the completion of the SIP session set-up, i.e. after the 200 OK(INVITE) is received, the P-CSCF shall provide the Flow-Status AVPs as derived from the SDP according to annex B.

6 Use of the Diameter base protocol

With the clarifications listed in the following clauses the Diameter Base Protocol defined by RFC 3588 [3] shall apply.

6.1 Securing Diameter messages

For secure transport of Diameter messages, see TS 133 210 [6].

6.2 Accounting functionality

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

6.3 Use of sessions

The Session-Termination-Request (STR) and Session-Termination-Answer (STA) commands defined in RFC 3588 [3] shall be used in order to terminate the sessions.

6.4 Transport protocol

Diameter messages over the Gq' interface shall make use of SCTP RFC 2960 [10] and shall utilize the new SCTP checksum method specified in RFC 3309 [11].

6.5 Routing considerations

This clause specifies the use of the Diameter routing AVPs Destination-Realm and Destination-Host.

The AF obtains the contact address of the SPDF for a given user via the e2 interface (ES 283 035 [13]). Both the Destination-Realm and Destination-Host AVPs shall be present in the request.

6.6 Advertising application support

The Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands are specified in the Diameter Base Protocol (RFC 3588 [3]).

The AF and the SPDF shall advertise the support of the Gq specific Application by including the value 16777222 of the application identifier in the Auth-Application-Id AVP within the Vendor-Specific-Application-Id grouped AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands.

The vendor identifier value of 3GPP (10415) shall be included in the Vendor-Id AVP within the Vendor-Specific-Application-Id grouped AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands.

The Vendor-Id AVP included in Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands that is not included in the Vendor-Specific-Application-Id AVPs as described above shall indicate the manufacturer of the Diameter node as per RFC 3588 [3].

Additionally, the AF and SPDF shall advertise the support of additional Vendor-ID AVPs by including the value ETSI (13019) and 3GPP (10415) in two different Supported-Vendor-Id AVPs of the CER and CEA commands.

7 DIAMETER application

The Diameter Base Protocol as specified in RFC 3588 [3] is used to support information transfer on the Gq' interface. RFC 3588 [3] shall apply except as modified by the additional support of the methods and the additional support of the commands and Attribute-Value-Pairs (AVPs), and result and event codes specified in this document. Unless otherwise specified, the procedures of RFC 3588 [3] (including error handling and unrecognized information handling) are unmodified.

In addition to the AVPs defined within the clause 7.3, the Diameter AVPs from the Diameter base application (RFC 3588 [3]) are reused within the Diameter messages sent over the Gq' interface.

The present document re-uses the Diameter application defined for the 3GPP Gq interface. The Gq Diameter application is defined as an IETF vendor specific Diameter application with application ID 16777222, where the vendor is 3GPP. The vendor identifier assigned by IANA to 3GPP (http://www.iana.org/assignments/enterprise-numbers) is 10415.

Due to the definition of the commands used over the Gq' interface, there is no possibility to skip the Auth-Application-Id AVP and use the Vendor-Specific-Application-Id AVP instead. Therefore the Gq application identifier shall be included in the Auth-Application-Id AVP.

With regards to the Diameter protocol defined over the Gq' interface, the SPDF 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 SPDF and the AF, may not be necessary where the Gq' is intra-operator (for example IMS).

7.1 Commands

Existing Diameter command codes from the Diameter base protocol RFC 3588 [3] and the NASREQ Diameter application (RFC 4005 [5]), are used. The Gq specific Auth-Application id is used together with the command code within those 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.

7.1.1 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 SPDF 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 ]
                 [ SIP-Forking-Indication ]
                *[ Specific-Action ]
                 [ User-Name ]
                 [ Binding-Information ]
                 [ Latching-Indication ]
                 [ Reservation-Priority ]
                 [ Globally-Unique-Address ]
                 [ Service-Class ]
                 [ Authorization-Lifetime ]
                *[ Proxy-Info ]
                *[ Route-Record ]
                *[ AVP ]
```

7.1.2 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 SPDF 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 ]
                 [ Binding-Information ]
                 [ Reservation-Priority ]
                 [ Error-Message ]
                 [ Error-Reporting-Host ]
                 [ Authorization-Lifetime ]
                 [ Auth-Grace-Period ]
                *[ Failed-AVP ]
                *[ Proxy-Info ]
                *[ AVP ]
```

7.1.3 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 SPDF to the AF in order to indicate a specific action.

However, application-specific authentication and/or authorization messages are not mandated for the Gq application in response to an RAR command.

The values INDICATION_OF_RELEASE_OF_BEARER, INDICATION_OF_SUBSCRIBER_DETACHMENT, INDICATION_OF_RESERVATION_EXPIRATION and INDICATION_OF_LOSS_OF_BEARER, INDICATION_OF_RECOVERY_OF_BEARER and INDICATION_OF_RELEASE_OF_BEARER of the Specific-Action AVP shall not be combined with each other in an Re-Auth-Request.

Message Format:

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

7.1.4 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 SPDF in response to the RAR command.

Message Format:

```
<RA-Answer> ::= < Diameter Header: 258, PXY >
                 < Session-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 ]
```

7.1.5 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 SPDF that an authorized session shall be terminated.

Message Format:

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

7.1.6 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 SPDF to the AF in response to the STR command.

Message Format:

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

7.1.7 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 SPDF to inform the AF that all bearer resources for the authorized session have become unavailable.

Message Format:

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

7.1.8 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 SPDF 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 ]
```

7.2 Experimental-Result-Code AVP values

7.2.1 Experimental-Result-Code AVP values imported from TS 129 209

This clause list the specific values of the Experimental-Result-Code AVP imported from [4] (vendor-id is 3GPP):

- INVALID_SERVICE_INFORMATION (5061)
  - The service information provided by the AF is invalid or insufficient for the server to perform the requested action.
- FILTER_RESTRICTIONS (5062)
  - The Flow_Description AVP(s) cannot be handled by the server because restrictions defined in clause 7.3.17 are not observed.

7.2.2 Experimental-Result-Code AVP values imported from ES 283 026

This clause defines the specific values of the Experimental-Result-Code AVP imported from [14] (vendor-id is ETSI):

- INSUFFICIENT_RESOURCES (4041):
  - The A-RACF or BGF indicates insufficient resources to perform the requested action.
- COMMIT_FAILURE (4043):
  - The A-RACF or BGF indicates that the resources reservation could not be committed.
- REFRESH_FAILURE (4044):
  - The A-RACF indicates that the lifetime of a reservation could not be extended.
- QOS_PROFILE_FAILURE (4045):
  - The A-RACF indicates that the request did not match the QoS profile.
- ACCESS_PROFILE_FAILURE (4046):
  - The A-RACF indicates that the request did not match any access profile.
- PRIORITY_NOT_GRANTED (4047):
  - The A-RACF or BGF indicates that the priority level of the request is not accepted at media or request level.
- MODIFICATION_FAILURE (5041):
  - The A-RACF or BGF indicates that the resources reservation could not be modified.

7.2.3 Experimental-Result-Code AVP values defined in this document

This clause defines the specific values of the Experimental-Result-Code AVP (vendor-id is ETSI):

- BINDING_FAILURE (5021):
  - The requested address binding could not be provided.

7.3 AVPs

The following tables summarize the AVPs used in this document, beyond those defined in the Diameter Base Protocol RFC 3588 [3].

Table 7.3.1 describes the Diameter AVPs defined in this document, their AVP Code values, types, possible flag values and whether the AVP may or not be encrypted. The Vendor-Id header of these AVPs shall be set to ETSI (13019).

Table 7.3.1: Diameter AVPs defined in this document

				AVP Flag rules (note 1)				
Attribute Name	**AVP Code**	**Clause defined**	**Value Type (note 2)**	**Must**	**May**	**Should not**	**Must not**	**May Encr.**
Binding-information	450	7.3.1	Grouped	V			M	Y
Binding-input-list	451	7.3.2	Grouped	V			M	Y
Binding-output-list	452	7.3.3	Grouped	V			M	Y
V6-transport-address	453	7.3.4	Grouped	V			M	Y
V4-transport-address	454	7.3.5	Grouped	V			M	Y
Port-number	455	7.3.6	Unsigned32	V			M	Y
Reservation-class	456	7.3.7	Unsigned32	V			M	Y
Latching-indication	457	7.3.8	Enumerated	V			M	Y
Reservation-priority	458	7.3.9	Enumerated	V			M	Y
Service-Class	459	7.3.33	UTF8String	V			M	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 [3]. NOTE 2: The value types are defined in RFC 3588 [3].								

Table 7.3.2 describes the Diameter AVPs imported from ES 283 035 [13]. The Vendor-Id header of these AVPs shall be set to ETSI (13019).

Table 7.3.2: Diameter AVPs imported from e4 interface ES 283 034 [15]

				AVP Flag rules				
Attribute Name	**AVP Code**	**Clause defined**	**Value Type**	**Must**	**May**	**Should not**	**Must not**	**May Encrypt**
Globally-Unique-Address	300	7.3.10	Grouped	V			M	Y
Address-Realm	301	7.3.11	Octet String	V			M	Y
Transport-Class	311	7.3.34	Unsigned32	V	M			Y
NOTE: 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 TS 133 210 [6].								

Table 7.3.3 describes the Diameter AVPs imported from the Gq interface protocol [4]. The Vendor-Id header of these AVPs shall be set to 3GPP (10415). This document modifies the syntax of certain Grouped AVPs defined in [4] by adding one or more optional AVP(s) to the syntax specified in [4]. AVPs defined in [4].but not listed in the following table should not be sent by a Diameter application conforming to this document and shall be ignored by receiving entities.

Table 7.3.3: Diameter AVPs imported from TS 29 209 [4]

Attribute Name	AVP Code	Clause defined	Value Type (note 2)	AVP Flag rules (note 1)				May Encr.
				Must	May	Should not	Must not	
Abort-Cause	500	7.3.14	Enumerated	M,V	P			Y
AF-Application-Identifier	504	7.3.15	Octet String	M,V	P			Y
AF-Charging-Identifier	505	7.3.16	Octet String	M,V	P			Y
Flow-Description	507	7.3.17	IPFilterRule	M,V	P			Y
Flow-Grouping	508	7.3.18	Grouped	M,V	P			Y
Flow-Number	509	7.3.19	Unsigned32	M,V	P			Y
Flows	510	7.3.20	Grouped	M,V	P			Y
Flow-Status	511	7.3.21	Enumerated	M,V	P			Y
Flow-Usage	512	7.3.22	Enumerated	M,V	P			Y
Specific-Action	513	7.3.23	Enumerated	M,V	P			Y
Max-Requested-Bandwidth-DL	515	7.3.24	Unsigned32	M,V	P			Y
Max-Requested-Bandwidth-UL	516	7.3.25	Unsigned32	M,V	P			Y
Media-Component-Description	517	7.3.26 (note 3)	Grouped	M,V	P			Y
Media-Component-Number	518	7.3.27	Unsigned32	M,V	P			Y
Media-Sub-Component AVP	519	7.3.28	Grouped	M,V	P			Y
Media-Type	520	7.3.29	Enumerated	M,V	P			Y
RR-Bandwidth	521	7.3.30	Unsigned32	M,V	P			Y
RS-Bandwidth	522	7.3.31	Unsigned32	M,V	P			Y
SIP-Forking-Indication	523	7.3.32	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 [3].
NOTE 2: The value types are defined in RFC 3588 [3].
NOTE 3: The AVP was initially defined in the Gq specification TS 129 209 [4]. This document provides updated syntax to some of those AVP in the form of optional AVPs that have been added to the Grouped AVP syntax.

Table 7.3.4 describes the Diameter AVPs defined for the NASREQ application (RFC 4005 [5]) and used in this document, their AVP Code values, types, possible flag values and whether the AVP may or not be encrypted. Flags values are described in the context of this document rather than in the context of the application where they are defined. AVPs defined in RFC 4005 [5] but no listed in the following table should not be sent by a Diameter application conforming to this document and shall be ignored by receiving entities. No Vendor-Id header shall be included in these AVPs.

Table 7.3.4: Diameter AVPs imported from RFC 4005 [5]

Attribute Name	AVP Code	Clause defined	Value Type	AVP Flag rules				May Encrypt
				Must	May	Should not	Must not	
Framed-IP-Address	8	See [5]	Octet String				V,M	Y
Framed-IPv6-Prefix	97	See [5]	Octet String				V,M	Y

7.3.1 Binding-information AVP

The Binding-Information AVP (AVP code 450) is of type Grouped and is sent between the AF and the SPDF in order to convey binding information required for NA(P)T, hosted NA(P)T and NA(P)T-PT control.

AVP format:

```
Binding-information ::= < AVP Header: 450 13019>
             { Binding-Input-List }    ;
             [ Binding-Output-List ]    ;
```

7.3.2 Binding-input-list AVP

The Binding-Input-List AVP (AVP code 451) is of type Grouped and contains a list transport addresses for which a binding is requested. The AF constructs the Binding-Input-List using SDI information.

AVP format:

```
Binding-Input-List ::= < AVP Header: 451 13019>
             *[ V6-Transport-Address ]    ;
                         *[ V4-Transport-Address ]        ;
```

7.3.3 Binding-output-list AVP

The Binding-Output-List AVP (AVP code 452) is of type Grouped and contains a list of transport addresses which is the result of the binding operation performed by the transport plane functions.

AVP format:

```
Binding-Output-List ::= < AVP Header: 452 13019>
             *[ V6-Transport-Address ]    ;
                         *[ V4-Transport-Address ]       ;
```

7.3.4 V6-Transport-address AVP

The V6-Transport-Address AVP (AVP code 453) is of type Grouped and contains a single IPv6 address and a single port number.

AVP format:

```
Transport-Address ::= < AVP Header: 453 13019>
                     { Framed-IPv6-Prefix }  ;
             { Port-Number }    ;
```

7.3.5 V4-Transport-address AVP

The V4-Transport-Address AVP (AVP code 454) is of type Grouped and contains a single IPv4 address and a single port number.

AVP format:

```
Transport-Address ::= < AVP Header: 454 13019>
                     { Framed-IP-Address }  ;
             { Port-Number }    ;
```

7.3.6 Port-number AVP

The Port-Number AVP (AVP code 455) is of type Unsigned32 and contains the end point port number.

7.3.7 Reservation-Class AVP

The Reservation-class AVP (AVP code 456) is of type Unsigned32 and contains an integer used as an index pointing to the traffic characteristic of the flow (e.g. burstiness and packet size).

7.3.8 Latching-indication AVP

The Latching-Indication AVP (AVP code 457) is of type Enumerated.

The following values are defined:

- LATCH (0)
- RELATCH (1)

7.3.9 Reservation-priority AVP

The Reservation-Priority AVP (AVP code 458) is of type Enumerated. The following values are specified:

DEFAULT (0): This is the lowest level of priority. If no Reservation-Priority AVP is specified in the AA-Request, this is the priority associated with the reservation.

- PRIORITY-ONE (1)
- PRIORITY-TWO (2)
- PRIORITY-THREE (3)
- PRIORITY-FOUR (4)
- PRIORITY-FIVE (5)
- PRIORITY-SIX (6)
- PRIORITY-SEVEN (7)

7.3.10 Globally-unique-address AVP

The Globally-Unique-Address AVP (AVP code 300) is of type Grouped (see ES 283 034 [15]).

AVP Format:

```
Globally-Unique-Address ::= < AVP Header: 300 13019 >
    [Framed-IP-Address]
    [Framed-IPv6-Prefix]
    [Address-Realm]
```

7.3.11 Address-realm AVP

The Address-Realm AVP (AVP code 301) is of type Octet String (see ES 283 034 [15]).

7.3.12 Framed-IP-address AVP

The Framed-IP-Address AVP is defined in the NASREQ application (see RFC 4005 [5]).

7.3.13 Framed-IPv6-prefix AVP

The Framed-IPv6-Prefix AVP is defined in the NASREQ application (see RFC 4005 [5]).

7.3.14 Abort-cause AVP

The Session-Abort-Cause AVP (AVP code 500) is of type Enumerated, and determines the cause of a session abort request or of an RAR indicating a IP-CAN bearer release. The following values are defined:

- BEARER_RELEASED (0)
  - This value is used when the bearer has been deactivated as a result from normal signalling handling. For xDSL, the bearer may refer to an ATM VC.
- INSUFFICIENT_SERVER_RESOURCES (1)
  - This value is used to indicate that the server is overloaded and needs to abort the session.
- INSUFFICIENT_BEARER_RESOURCES (2)
  - This value is used when the bearer has been deactivated due to insufficient bearer resources at a transport gateway (e.g. RCEF for xDSL).

7.3.15 AF-application-identifier AVP

The AF-Application-identifier AVP (AVP code 504) is of type Octet String, and it contains information that identifies the RACS client requesting the resources (e.g. name of an ASP or group of ASPs). This information is used by the SPDF over the Rq interface (see ES 283 026 [14]).

7.3.16 AF-charging-identifier AVP

The AF-Charging-Identifier AVP (AVP code 505) is of type Octet String, contains the AF Charging Identifier that is sent by the AF. This information may be used for charging correlation between AF and the RACS functional entities.

7.3.17 Flow-description AVP

The Flow-Description AVP (AVP code 507) 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 b 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.

If any of these restrictions is not observed by the AF, the server shall send an error response to the AF containing the Experimental-Result-Code AVP with value FILTER_RESTRICTIONS.

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.

7.3.18 Flow-grouping AVP

The Flow-Grouping AVP (AVP code 508) is of type Grouped, and it indicates that no other IP Flows shall be transported together with the listed IP Flows in the same IP-CAN bearer.

If Flow-Grouping AVP(s) have been provided in earlier service information, but are not provided in subsequent service information, the old flow grouping remains valid.

If Flow-Grouping AVP(s) have been provided in earlier service information, and new Flow-Grouping AVP(s) are provided, the new flow grouping information replaces the previous information. Previous flow grouping information is invalidated even if the new Flow-Grouping AVP(s) affect other IP flows.

A Flow-Grouping AVP containing no Flows AVP may be used to invalidate flow grouping information provided in earlier service information. A Flow-Grouping AVP containing no Flows AVP shall not be supplied together with other Flow-Grouping AVP(s).

If earlier service information has already been provided, flow grouping information in subsequent service information shall not restrict the flow grouping further for IP flows already described in the previous service information. However, new IP flows described for the first time in the subsequent service information may be added to existing flow groups or in new flow groups.

AVP Format:

```
Flow-Grouping ::= < AVP Header: 508 >
    *[Flows]
```

7.3.19 Flow-number AVP

The Flow-Number AVP (AVP code 509) 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 129 207 [12].

7.3.20 Flows AVP

The Flows AVP (AVP code 510) 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]
```

7.3.21 Flow-status AVP

The Flow-Status AVP (AVP code 511) 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). If any downlink RTCP IP flow(s) are identified by the Flow_Usage AVP(s), those flow(s) shall be enabled.
- ENABLED-DOWNLINK (1):
  - This value shall be used to enable associated downlink IP flow(s) and to disable associated uplink IP flow(s). If any uplink RTCP IP flow(s) are identified by the Flow_Usage AVP(s), those flow(s) shall be enabled.
- 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. If any RTCP IP flow(s) are identified by the Flow_Usage AVP(s), those flow(s) shall be enabled.
- REMOVED (4):
  - This value shall be used to remove all associated IP flow(s). The IP Filters for the associated IP flow(s) shall be removed. The associated IP flows shall not be taken into account when deriving the authorized QoS.

7.3.22 Flow-usage AVP

The Flow-Usage AVP (AVP code 512) is of type Enumerated, and provides information about the usage of IP Flows. The following values are defined:

- NO_INFORMATION (0):
  - This value is used to indicate that no information about the usage of the IP flow is being provided.

- RTCP (1):
  - This value is used to indicate that an IP flow is used to transport RTCP.
- NO_INFORMATION is the default value.

NOTE: An AF may choose not to identify RTCP flows, e.g. in order to avoid that RTCP flows are always enabled by the server.

7.3.23 Specific-action AVP

The Specific-Action AVP (AVP code 513) is of type Enumerated.

Within a SPDF initiated Re-Authorization Request, the Specific-Action AVP determines the type of the action.

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

The following values from TS 129 209 [4] are used:

- INDICATION_OF_LOSS_OF_BEARER (2):
  - Within a RAR, this value shall be used when the server reports a loss of a bearer (e.g. the bandwidth detected in the BGF is 0 kbit) to the AF. In the AAR, this value indicates that the AF requests the server to provide a notification at the loss of a bearer.
- INDICATION_OF_RECOVERY_OF_BEARER (3):
  - Within a RAR, this value shall be used when the server reports a recovery of a bearer (e.g. the bandwidth detected by the BGF is modified from 0 kbit to another value) to the AF. In the AAR, this value indicates that the AF requests the server to provide a notification at the recovery of a bearer.
- INDICATION_OF_RELEASE_OF_BEARER (4):
  - In the AAR, this value indicates that the AF requests the SPDF to provide a notification at the removal of an IP-CAN bearer. In a RAR message, the SPDF indicates to the AF that a transport layer error has occurred.

In addition, this document defines two new values:

- INDICATION_OF_SUBSCRIBER_DETACHMENT (6):
  - In the AAR, this value indicates that the AF requests the SPDF to provide a notification at the detachment of a subscriber. In a RAR message, the SPDF indicates to the AF that the subscriber has been detached.
- INDICATION_OF_RESERVATION_EXPIRATION (7):
  - In the AAR, this value indicates that the AF requests the SPDF to provide a notification when the reservation is about to expire. In a RAR message, the SPDF indicates to the AF that the reservation is about to expire.

Other values from TS 129 209 [4] are not relevant at the Gq' interface and are not used. If received by the SPDF, these values are ignored.

7.3.24 Max-requested-bandwidth-DL AVP

The Max-Requested-Bandwidth-DL AVP (AVP code 515) is of type Unsigned32, and it indicates the maximum requested bandwidth in bits per second for a downlink IP flow. The bandwidth contains all the overhead coming from the IP-layer and the layers above, e.g. IP, UDP, RTP and RTP payload.

7.3.25 Max-requested-bandwidth-UL AVP

The Max -Bandwidth-UL AVP (AVP code 516) is of type Unsigned32, and it indicates the maximum requested bandwidth in bits per second for an uplink IP flow. The bandwidth contains all the overhead coming from the IP-layer and the layers above, e.g. IP, UDP, RTP and RTP payload.

7.3.26 Media-component-description AVP

The Media-Component-Description AVP (AVP code 517) 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 may be used by the server to determine authorized QoS and IP flow classifiers for bearer authorization and charging rule selection.

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

Bandwidth information and Flow-Status information provided within the Media-Component-Description AVP applies to all those IP flows within the media component, for which no corresponding information is being provided within Media-Sub-Component AVP(s).

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 Diameter messages, the previous information for the corresponding IP flow(s) remains valid.

All IP flows within a Media-Component-Description AVP are permanently disabled by supplying a Flow Status AVP with value "REMOVED". The server may delete corresponding filters and state information.

AVP format:

```
Media-Component-Description ::= < AVP Header: 517 >
                                { 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-UL ]
                                    [ Max-Requested-Bandwidth-DL ]
                                      [ Flow-Status ]
                                    [ RS-Bandwidth ]
                                  [ RR-Bandwidth ]
                                      [ Reservation-Class ]
                                      [ Reservation-Priority ]
                                      [ Transport-Class ]
```

7.3.27 Media-component-number AVP

The Media-Component-Number AVP (AVP code 518) is of type Unsigned32, and it contains the ordinal number of the media component, assigned according to the rules in annex C of TS 129 207 [12].

7.3.28 Media-sub-component AVP

The Media-Sub-Component AVP (AVP code 519) is of type Grouped, and it contains the requested QoS and filters for the set of IP flows identified by their common Flow-Identifier. The Flow-Identifier is defined in TS 129 207 [12].

Possible Bandwidth information and Flow-Status information provided within the Media-Sub-Component AVP takes precedence over information within the encapsulating Media Component Description AVP. If a Media-Sub-Component- AVP is not supplied, or if optional AVP(s) within a Media-Sub-Component AVP are omitted, but corresponding information has been provided in previous Diameter messages, the previous information for the corresponding IP flow(s) remains valid, unless new information is provided within the encapsulating Media-Component-Description AVP. If Flow-Description AVP(s) are supplied, they replace all previous Flow-Description AVP(s), even if a new Flow-Description AVP has the opposite direction as the previous Flow-Description AVP.

All IP flows within a Media-Sub-Component- AVP are permanently disabled by supplying a Flow Status AVP with value "REMOVED". The server may delete corresponding filters and state information.

AVP format:

```
Media-Sub-Component ::= < AVP Header: 519 >
                    { Flow-Number }   ; Ordinal number of the IP flow
              0*2[ Flow-Description ]    ; UL and/or DL
               [ Flow-Status ]
                           [ Flow-Usage ]
                         [ Max-Requested-Bandwidth-UL ]
                           [ Max-Requested-Bandwidth-DL ]
```

7.3.29 Media-type AVP

The Media-Type AVP (AVP code 520) is of type Enumerated, and it determines the media type of a session component. The media types indicate the type of media in the same way as the SDP media types with the same names defined in [11]. The following values are defined:

- AUDIO (0)
- VIDEO (1)
- DATA (2)
- APPLICATION (3)
- CONTROL (4)
- TEXT (5)
- MESSAGE (6)
- OTHER (0xFFFFFFFF)

7.3.30 RR-bandwidth AVP

The RR-Bandwidth AVP (AVP code 521) 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 [16]. The bandwidth contains all the overhead coming from the IP-layer and the layers above, i.e. IP, UDP and RTCP.

7.3.31 RS-bandwidth AVP

The RS-Bandwidth AVP (AVP code 522) 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 [16]. The bandwidth contains all the overhead coming from the IP-layer and the layers above, i.e. IP, UDP and RTCP.

7.3.32 SIP-forking-indication AVP

The SIP_Forking AVP (AVP code 523) is of type Enumerated, and describes if several SIP dialogues are related to one Diameter session:

- SINGLE_DIALOGUE (0)
  - This value is used to indicate that the Diameter session relates to a single SIP dialogue. This is the default value applicable if the AVP is omitted.
- SEVERAL_DIALOGUES (1)
  - This value is used to indicate that the Diameter session relates to several SIP dialogues.

7.3.33 Service-Class AVP

The Service-Class AVP (AVP code 459) is of type UTF8String, and it contains the service class requested by the AF. The service class is to be checked against local policies in the SPDF.

7.3.34 Transport-Class AVP

The Transport-Class AVP (AVP code 311) is of type Unsigned32, and it contains an integer used as an index pointing to a class of transport services to be applied (e.g. forwarding behaviour).

7.4 Use of namespaces

This clause contains the namespaces that have either been created in this document, or the values assigned to existing namespaces managed by IANA.

7.4.1 AVP codes

This document assigns the AVP values from the AVP Code namespace managed by ETSI for its Diameter vendor-specific applications. See clause 7.3.

7.4.2 Experimental-result-code AVP values

This document assigns the Experimental-Result-Code AVP values from the AVP Code namespace managed by ETSI for its Diameter vendor-specific applications. See clause 7.2.

7.4.3 Command code values

This document does not assign command code values but uses existing command defined by 3GPP and IETF.

7.4.4 Application-ID value

This document re-uses the value 16777217 allocated by IANA to the 3GPP Gq interface application.

Annex A (normative): Support for SIP forking

A.1 Support for SIP forking

The P-CSCF shall be able to handle forking.

A.1.1 Authorization of resources for early media for forked responses

When a SIP session has been originated by a connected UE, the P-CSCF may receive multiple provisional responses due to forking before the first final answer is received.

The UE and the P-CSCF become aware of the forking only when the second provisional response arrives. For this, and any subsequent provisional response, the P-CSCF shall use an AA request within the existing Diameter session containing the SIP-Forking-Indication AVP with value SEVERAL_DIALOGUES and include the service information derived from the latest provisional response.

When receiving an AA request containing the SIP-Forking-Indication AVP with value SEVERAL_DIALOGUES, the SPDF shall identify the existing authorization information for that Diameter session. The SPDF shall authorize any additional media components and any increased QoS requirements for the previously authorized media components, as requested within the service information. The SPDF shall authorize the maximum bandwidth required by any of the dialogues, but not the sum of the bandwidths required by all dialogues. Thus, the QoS authorized for a media component is equal to the highest QoS requested for that media component by any of the forked responses. The SPDF shall also send additional packet classifiers as required by the Flow Description AVPs within the session information to the GGSN.

A.1.2 Updating the authorization information at the final answer

The P-CSCF shall store the SDP information for each early dialogue separately till the first final SIP answer is received. Then the related early dialogue is progressed to an established dialogue to establish the final SIP session. All the other early dialogues are terminated. The authorization information for the SIP session is updated to match the requirements of the remaining early dialogue only.

When receiving the first final SIP response, the P-CSCF shall send an AA request without the SIP-Forking-Indication AVP and include the service information derived from the SDP corresponding to the dialogue of the final response.

When receiving an AA request with no SIP-Forking-Indication AVP or with a SIP-Forking-Indication AVP with value SINGLE_DIALOGUE, the SPDF shall. update authorization information and packet classifiers to match only the requirements of the service information within this AA request.

Annex B (normative): QoS parameter mapping for IMS

Within the IMS, session establishment and modification involves an end-to-end message-exchange using SIP/SDP with negotiation of media attributes (e.g. codecs) as defined in TS 283 003 [7]. The P-CSCF shall provide service information derived from the relevant SDP information to the SPDF via the Gq' interface. The P-CSCF shall apply the mapping rules in this annex to derive service information from SDP.

B.1 SDP to service information mapping in AF

The mapping described in this clause is mandatory for the P-CSCF and should also be applied by other AFs if the SDI is SDP.

When a session is initiated or modified the P-CSCF shall use the mapping rules in table B.1 for each SDP media component to derive a Media-Component-Description AVP from the SDP Parameters. Furthermore, the P-CSCF shall map information about the grouping of media lines into resource reservation flows into the Flow-Grouping AVP as specified in table B.3.

Table B.1: Rules for derivation of service information within Media-Component-Description AVP from SDP media component

service information per Media-Component-Description AVP (see notes 1 and 7)	Derivation from SDP Parameters (see note 2)
Media-Component-Number	ordinal number of the position of the "m=" line in the SDP
AF-Application-Identifier	The AF-Application-Identifier AVP may be supplied or omitted, depending on the application. For IMS, if the AF-Application-Identifier AVP is supplied, its value should not demand application specific bandwidth or QoS class handling. However, if an IMS application is capable of handling a QoS downgrading, the AF-Application-Identifier AVP may be used to demand application specific bandwidth or QoS class handling.
Media-Type	The Media Type AVP shall be included with the same value as supplied for the media type in the "m=" line.

Flow-Status	IF port in m-line = 0 THEN
	  Flow-Status:= REMOVED;
	ELSE
	  IF a=recvonly THEN
	  IF <SDP direction> = mobile originated THEN
	  Flow-Status := ENABLED_DOWNLINK; (NOTE 4)
	  ELSE /* mobile terminated */
	  Flow-Status := ENABLED_UPLINK; (NOTE 4)
	  ENDIF;
	  ELSE
	  IF a=sendonly THEN
	  IF <SDP direction> = mobile originated THEN
	  Flow-Status := ENABLED_UPLINK; (NOTE 4)
	  ELSE /* mobile terminated */
	  Flow-Status := ENABLED_DOWNLINK; (NOTE 4)
	  ENDIF;
	  ELSE
	  IF a=inactive THEN
	  Flow-Status :=DISABLED;
	  ELSE /* a=sendrecv or no direction attribute */
	  Flow-Status := ENABLED (NOTE 4)
	  ENDIF;
	  ENDIF;
	  ENDIF;
	ENDIF;
	(NOTE 5)

service information per Media-Component-Description AVP (see notes 1 and 7)	Derivation from SDP Parameters (see note 2)

Max-Requested-Bandwidth-UL	IF <SDP direction> = mobile terminated THEN
	  IF b=AS:<bandwidth> is present THEN
	  Max-Requested-Bandwidth-UL:= <bandwidth> * 1000; /* Unit is bit/s
	  ELSE
	  Max-Requested-Bandwidth-UL:= <Operator specific setting>,
	  or AVP not supplied;
	  ENDIF;
	ELSE
	  Consider SDP in opposite direction
	ENDIF
	(Note 8)

Max-Requested-Bandwidth-DL	IF <SDP direction> = mobile originated THEN
	  IF b=AS:<bandwidth> is present THEN
	  Max-Requested-Bandwidth-DL:= <bandwidth> * 1000; /* Unit is bit/s
	  ELSE
	  Max-Requested-Bandwidth-DL:= <Operator specific setting>,
	  or AVP not supplied;
	  ENDIF;
	ELSE
	  Consider SDP in opposite direction
	ENDIF
	(Note 8)

RR-Bandwidth	IF b=RR:<bandwidth> is present THEN
	  RR-Bandwidth:= <bandwidth>;
	ELSE
	  AVP not supplied
	ENDIF;
	(NOTE 3; NOTE 6)

RS-Bandwidth	IF b=RS:<bandwidth> is present THEN
	  RS-Bandwidth:= <bandwidth>;
	ELSE
	  AVP not supplied
	ENDIF;
	(NOTE 3: NOTE 6)

Media-Sub-Component	Supply one AVP for each Flow Identifier within the media component. The Flow identifiers are derived according to Annex D of TS 129 207 [13]. The encoding of the AVP is described in Table B.2

NOTE 1: The encoding of the service information is defined in this document.
NOTE 2: The SDP parameters are described in RFC 4566 [9].
NOTE 3: The "b=RS:" and "b=RR:" SDP bandwidth modifiers are defined in RFC 3556 [16].
NOTE 4: As an operator policy to disable forward and/or backward early media, the Flow-Status may be downgraded before a SIP dialogue is established, i.e. until a 200 OK(INVITE) is received. The Value "DISABLED" may be used instead of the Values "ENABLED_UPLINK" or "ENABLED_DOWNLINK". The Values "DISABLED", "ENABLED_UPLINK" or "ENABLED_DOWNLINK" may be used instead of the Value "ENABLED"
NOTE 5: If the SDP answer is available when the session information is derived, the direction attributes and port number from the SDP answer shall be used to derive the flow status. However, to enable interoperability with SIP clients that do not understand the inactive SDP attribute, if a=inactive was supplied in the SDP offer, this shall be used to derive the flow status. If the SDP answer is not available when the session information is derived, the direction attributes from the SDP offer shall be used.
NOTE 6: Information from the SDP answer is applicable, if available.
NOTE 7: The AVPs may be omitted if they have been supplied in previous service information and have not changed.
NOTE 8: TS 183 048 provides rules to be used by the P-CSCF in deriving the bandwidth to request from RACS in the case an operator specific setting is to be used to populate the Max Requested Bandwidth DL and the Max Requested Bandwidth UL AVPs.

Table B.2: Rules for derivation of Media-Sub-Component AVP from SDP media component

Gq' service information per Media-Sub-Component AVP (see notes 1 and 5)	Derivation from SDP Parameters (see note 2)
Flow-Number	derived according to annex C of TS 129 207 [12]
Flow-Status	AVP not supplied
Max-Requested-Bandwidth-UL	AVP not supplied
Max-Requested-Bandwidth-DL	AVP not supplied

Flow-Description	For uplink and downlink direction, a Flow-Description AVP shall be provided unless no IP Flows in this direction are described within the media component.
	The SDP direction attribute (NOTE 4) indicates the direction of the media IP flows within the media component as follows:
	IF a=recvonly THEN (NOTE 3)
	IF <SDP direction> = mobile originated THEN
	Provide only downlink Flow-Description AVP
	ELSE /* mobile terminated */
	Provide only uplink Flow-Description AVP
	ENDIF;
	ELSE
	IF a=sendonly THEN (NOTE 3)
	IF <SDP direction> = mobile originated THEN
	Provide only uplink Flow-Description AVP
	ELSE /* mobile terminated */
	Provide only downlink Flow-Description AVP
	ENDIF;
	ELSE /* a=sendrecv or a=inactive or no direction attribute */
	Provide uplink and downlink Flow-Description AVPs
	ENDIF;
	ENDIF;
	For RTCP IP flows uplink and downlink Flow-Description AVPs shall be provided irrespective of the SDP direction attribute.
	
	The uplink destination address shall be copied from the "c=" line of downlink SDP. (see note 6)
	The uplink destination port shall be derived from the "m=" line of downlink SDP. (see note 6)
	The downlink destination address shall be copied from the "c=" line of uplink SDP. (see note 6)
	The downlink destination port shall be derived from the "m=" line of uplink SDP. (note 6)
	Uplink and downlink source addresses shall either be derived from the prefix of the destination address or be wildcarded by setting to "any", as specified in this document.
	Source ports shall not be supplied.
	Proto shall be derived from the transport of the "m=" line. For "RTP/AVP" proto is 17(UDP).

Flow-Usage	The Flow-Usage AVP shall be supplied with value "RTCP" if the IP flow(s) described in the Media-Sub-Component AVP are used to transport RTCP. Otherwise the Flow-Usage AVP shall not be supplied. [10] specifies how RTCP flows are described within SDP.

NOTE 1: The encoding of the service information is defined in this document.
NOTE 2: The SDP parameters are described in [9].
NOTE 3: If the SDP direction attribute for the media component negotiated in a previous offer-answer exchange was sendrecv, or if no direction attribute was provided, and the new SDP direction attribute sendonly or recvonly is negotiated in a subsequent SDP offer-answer exchange, uplink and downlink Flow-Description AVPs shall be supplied.
NOTE 4: If the SDP answer is available when the session information is derived, the direction attributes from the SDP answer shall be used to derive the flow description. However, to enable interoperability with SIP clients that do not understand the inactive SDP attribute, if a=inactive was supplied in the SDP offer, this shall be used. If the SDP answer is not available when the session information is derived, the direction attributes from the SDP offer shall be used.
NOTE 5: The AVPs may be omitted if they have been supplied in previous service information and have not changed, as detailed in this document.
NOTE 6: If the session information is derived from an SDP offer, the required SDP may not yet be available. The corresponding Flow Description AVP shall nevertheless be included and the unavailable fields (possibly all) shall be wildcarded.

Table B.3: Rules for mapping SDP information about the grouping of media lines into resource reservation flows into the Flow Grouping AVP

Flow-Grouping AVP (see note 1)	Derivation from SDP Parameters (see note 2)
Flow Grouping	For each SDP "a=group:SRF" SDP line, a Flow Grouping AVP shall be generated. (NOTE 3)
Flows	For each identification tag within "a=group:SRF" SDP line, a Flows AVP containing a Media-Component-Number AVP identifying the corresponding m-line shall be generated. (NOTE 3) No Flow-Number AVP shall be supplied within the Flows AVP.

NOTE 1: The encoding of the service information is defined in this document.
NOTE 2: The SDP parameters are described in [9].
NOTE 3: The SDP "group" attribute is defined in RFC 3388 [17]. The "SRF" semantics attribute within this grouping framework is defined in RFC 3524 [18].

Annex C (informative): Bibliography

ETSI TS 182 006: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Stage 2 description (3GPP TS 23.228 version 7.2.0, modified)".

ETSI TS 183 048: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Resource & Admission Control System (RACS) stage 3; Protocol Signalling flows specification; RACS Stage 3".

History

Document history		
V1.1.1	March 2006	Publication
V1.4.0	August 2007	Publication