ETSI TS 129 214 V14.3.0 (2017-04)

Universal Mobile Telecommunications System (UMTS);
LTE;
Policy and charging control over Rx reference point
(3GPP TS 29.214 version 14.3.0 Release 14)

Reference
RTS/TSGC-0329214ve30

Keywords
LTE,UMTS

ETSI

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

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

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

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 (https://ipr.etsi.org/).

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

Foreword

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

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

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

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

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 Rx reference point for the present release. The functional requirements and the stage 2 specifications of the Rx reference point are contained in 3GPP TS 23.203 [2]. The Rx reference point lies between the Application Function and the Policy and Charging Rule Function. The Rx interface which is based on RESTful HTTP and XML is specified in 3GPP TS 29.201 [37].

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 23.203: "Policy and Charging Control architecture".

[3] Void.

[4] Void.

[5] 3GPP TS 29.209: "Policy control over Gq interface", latest Rel-6 version.

[6] Void.

[7] 3GPP TS 29.211: "Rx Interface and Rx/Gx signalling flows", latest Rel-6 version.

[8] 3GPP TS 29.212: "Policy and Charging Control (PCC); Reference points".

[9] 3GPP TS 29.213: "Policy and Charging Control signalling flows and Quality of Service (QoS) parameter mapping".

[10] Void.

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

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

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

[14] IETF RFC 4006: "Diameter Credit Control Application".

[15] ETSI TS 183 017 v3.2.1: "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".

[16] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[17] 3GPP TS 24.229: "IP Multimedia Call Control Protocol based on SIP and SDP; Stage 3".

[18] IETF RFC 3264: "An Offer/Answer Model with the Session Description Protocol (SDP)".

[19] Void.

[20] IETF RFC 3162: "Radius and IPv6".

[21] IETF RFC 5031: "A Uniform Resource Name (URN) for Emergency and Other Well-Known Services".

[22] Void.

[23] 3GPP TS 32.240: "Telecommunication management; Charging management; Charging architecture and principles".

[24] 3GPP TS 32.299: "Telecommunication management; Charging management; Diameter charging applications".

[25] 3GPP TS 29.229: "Cx and Dx interfaces based on the Diameter protocol; Protocol details"

[26] 3GPP TS 24.292: "IP Multimedia (IM) Core Network (CN) subsystem Centralized Services (ICS); Stage 3".

[27] IETF RFC 3959 (December 2004): "The Early Session Disposition Type for the Session Initiation Protocol (SIP)".

[28] 3GPP TS 23.380: "IMS Restoration Procedures".

[29] Void.

[30] Void.

[31] 3GPP TS 22.153: "Multimedia Priority Service".

[32] Void.

[33] 3GPP TS 29.274: "3GPP Evolved Packet System. Evolved GPRS Tunnelling Protocol for EPS (GTPv2)".

[34] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)".

[35] IETF RFC 7683: "Diameter Overload Indication Conveyance".

[36] 3GPP TS 23.468: "Group Services and System Aspects; Group Communication System Enablers for LTE (GCSE LTE)".

[37] 3GPP TS 29.201: "Representational State Transfer (REST) reference point between Application Function (AF) and Protocol Converter (PC)".

[38] 3GPP TS 23.003: "Numbering, addressing and identification".

[39] 3GPP TS 29.273: "3GPP EPS AAA interfaces".

[40] 3GPP TS 23.682: "Architecture enhancements to facilitate communications with packet data networks and applications".

[41] 3GPP TS 26.114: "IP Multimedia Subsystem (IMS); Multimedia telephony; Media handling and interaction".

[42] IETF RFC 5761: "Multiplexing RTP Data and Control Packets on a Single Port".

[43] IETF RFC 7944: "Diameter Routing Message Priority".

[44] 3GPP TS 23.179: "Functional architecture and information flows to support mission critical communication services".

[45] IETF draft-holmberg-dispatch-mcptt-rp-namespace-05(January 2017) "Resource-Priority Namespace for Mission Critical Push To Talk service".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[46] 3GPP TS 23.303: "Proximity-based services (ProSe); Stage 2".

[47] 3GPP TS 29.154: "Service capability exposure functionality over Nt reference point".

[48] IETF RFC 5009: "Private Header (P-Header) Extension to the Session Initiation Protocol (SIP) for Authorization of Early Media".

[49] IETF RFC 3948: "UDP Encapsulation of IPsec ESP Packets".

[50] 3GPP TS 24.302: "Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; stage 3".

[51] IETF draft-ietf-dime-load-03: "Diameter Load Information Conveyance".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[52] IETF RFC 6733: "Diameter Base Protocol".

[53] 3GPP TS 23.167: "IP Multimedia Subsystem (IMS) emergency sessions".

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 application(s) that use IP bearer resources

NOTE: One example of an AF is the P-CSCF of the IM CN subsystem.

AF Session: application level 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.

Attribute-Value Pair (AVP): See ETF RFC 6733 [52], corresponds to an Information Element in a Diameter message.

Binding: PCRF process of associating IP flows described in AF Service Information with IP-CAN bearers.

IP-CAN bearer: IP transmission path of defined capacity, delay and bit error rate, etc.
See 3GPP TR 21.905 [1] for the definition of bearer.

IP-CAN session: association between a UE and an IP network (for GPRS, APN).
The association is identified by one UE Ipv4 address and/or one Ipv6 prefix together with a UE identity information, if available, and a PDN represented by a PDN ID (e.g. an APN). An IP-CAN session incorporates one or more IP-CAN bearers. Support for multiple IP-CAN bearers per IP-CAN session is IP-CAN specific. An IP-CAN session exists as long as the related UE Ipv4 address and/or Ipv6 prefix are assigned and announced to the IP network.

IP flow: unidirectional flow of IP packets with the same source IP address and port number and the same destination IP address and port number and the same transport protocol
Port numbers are only applicable if used by the transport protocol.

MPS session: A session for which priority treatment is applied for allocating and maintaining radio and network resources to support the Multimedia Priority Service (MPS). MPS is defined in 3GPP TS 22.153 [31].

Packet flow: A specific user data flow carried through the PCEF. A packet flow can be an IP flow.

PCC rule: set of information enabling the detection of a service data flow and providing parameters for policy control and/or charging control.

RESTful HTTP: is an architectural style consisting of a coordinated set of architectural constraints applied to components, connectors, and data elements, within a distributed hypermedia system applied to the development of web services.

service information: set of information conveyed from the AF to the PCRF over the Rx interface to be used as a basis for PCC decisions at the PCRF, including information about the AF session (e.g. application identifier, type of media, bandwidth, IP address and port number).

service data flow: An aggregate set of packet flows.

3.2 Abbreviations

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

ADC	Application Detection and Control
AF	Application Function
AS	Application Server
ASP	Application Service Provider
AVP	Attribute Value Pair
CRF	Charging Rules Function
DRMP	Diameter Routing Message Priority
DSCP	Differentiated Services Code Point
GCS	Group Communication Service
GCS AS	Group Communication Service Application Server
IP-CAN	IP Connectivity Access Network
MPS	Multimedia Priority Service
PCC	Policy and Charging Control
PCEF	Policy and Charging Enforcement Function
PCRF	Policy and Charging Rule Function
PDF	Policy Decision Function
P-CSCF	Proxy-Call Session Control Function
PSAP	Public Safety Answering Point
RCAF	RAN Congestion Awareness Function
QoS	Quality of Service
SCEF	Service Capability Exposure Function
SCS	Service Capability Server
SDF	Service Data Flow
SPR	Subscriber Profile Repository
TDF	Traffic Detection Function
UDC	User Data Convergence
UE	User Equipment
UDR	User Data Repository
XML	Extensible Markup Language

4 Rx reference point

4.1 Overview

The Rx reference point is used to exchange application level session information between the Policy and Charging Rules Function (PCRF) and the Application Function (AF). As defined in the stage 2 specifications (3GPP TS 23.203 [2]), this information is part of the input used by the PCRF for the Policy and Charging Control (PCC) decisions. The PCRF exchanges the PCC rules with the Policy and Charging Enforcement Function (PCEF) and QoS rules with the Bearer Binding and Event Reporting Function (BBERF) as specified in 3GPP TS 29.212 [8].

Signalling flows related to the both Rx and Gx interfaces are specified in 3GPP TS 29.213 [9].

Refer to Annex G of 3GPP TS 29.213 [9] for Diameter overload control procedures over the Rx interface.

Refer to Annex J of 3GPP TS 29.213 [9] for Diameter message priority mechanism procedures over the Rx interface.

Refer to Annex K of 3GPP TS 29.213 [9] for Diameter load control procedures over the Rx interface.

4.2 Rx reference model

The Rx reference point is defined between the PCRF and the AF. The relationships between the different functional entities involved are depicted in figure 4.2.1. The overall PCC architecture is depicted in subclause 3a of 3GPP TS 29.213 [9].

Figure 4.2.1: Rx reference model

Figure 4.2.2: Void

4.3 Functional elements

4.3.1 AF

The AF is an element offering applications that require the Policy and Charging Control of traffic plane resources (e.g. UMTS PS domain/GPRS domain resources). One example of an application function is the P-CSCF. The AF shall use the Rx reference point to provide session information to the PCRF.

NOTE: The AFs may be deployed by the same operator offering the IP-CAN or may be provided by external third party service provider.

4.3.2 PCRF

The PCRF (Policy Control and Charging Rules Function) is a functional element that encompasses policy control decision and flow based charging control functionalities. These 2 functionalities are the heritage of the release 6 logical entities PDF and CRF respectively. The PCRF provides network control regarding the service data flow detection, gating, QoS and flow based charging (except credit management) towards the PCEF. The PCRF receives session and media related information from the AF and informs AF of traffic plane events.

The PCRF may check that the service information provided by the AF is consistent with the operator defined policy rules before storing the service information. The service information shall be used to derive the QoS for the service. The PCRF may reject the request received from the AF and as a result the PCRF shall indicate, in the response to the AF, the service information that can be accepted by the PCRF.

The PCRF may temporarily not be able to provide the service delivery that AF requested (e.g. due to RAN user plane congestion). In this case, the PCRF may send a re-try interval information to the AF. The re-try interval indicates when service delivery may be retried by the AF over Rx.

NOTE 1: Additionally, existing bandwidth limitation parameters (e.g. Max-Requested-Bandwidth-DL AVP, Max-Requested-Bandwidth-UL AVP within the Acceptable-Service-Info AVP) provided by the PCRF to the AF in AA-Answer command during the Rx session establishment are available in order to mitigate RAN user plane congestion.

The PCRF may use the subscription information as basis for the policy and charging control decisions. The subscription information may apply for both session based and non-session based services. The subscription specific information for each service may contain e.g. max QoS class and max bit rate.

If the AF requests it, the PCRF shall report IP-CAN session events (including bearer events and events on AF signalling transport) to the AF via the Rx reference point.

The PCRF PCC/QoS Rule decisions may be based on one or more of the following:

- the session and media related information obtained from the AF via the Rx reference point;
- the bearer and subscriber related information obtained from the PCEF over the Gx reference point;
- the bearer and subscriber related information obtained from the BBERF over the Gxx reference point;
- subscriber and service related data the PCRF may be aware of by configuration or through the Sp reference point;
- pre-configured information in the PCRF.

NOTE 2: The details associated with the Sp reference point are not specified in this Release. The SPR's relation to existing subscriber databases is not specified in this Release.

The PCRF shall provision PCC/QoS Rules to the PCEF/BBERF via the Gx/Gxx reference point.

4.4 PCC procedures over Rx reference point

4.4.1 Initial Provisioning of Session Information

When a new AF session is being established and media information for this AF session is available at the AF and the related media require PCC supervision, the AF shall open an Rx Diameter session with the PCRF for the AF session using an AA-Request command, unless an Rx session has already been established for the AF session (e.g. as per clause 4.4.6.7). If an Rx Diameter session already exists for the AF session, the AF uses the existing Rx Diameter session. The AF shall provide the full IP address of the UE using either Framed-IP-Address AVP or Framed-Ipv6-Prefix AVP, and the corresponding Service Information within Media-Component-Description AVP(s). The AF shall not include circuit-switched bearer related media in the service information sent to the PCRF. The AF shall indicate to the PCRF as part of the Media-Component-Description whether the media IP flow(s) should be enabled or disabled with the Flow-Status AVP.

NOTE 1: The AF does not need to open an Rx Diameter session with the PCRF, if the SDP payload is only proposing to use a circuit-switched bearer (i.e. "c=" line set to "PSTN" and an "m=" line set to "PSTN", refer to 3GPP TS 24.292 [26]).

NOTE 2: The Rx Diameter session used for an AF session is different from the Rx Diameter session possibly used for the notifications of the status of the AF signalling transmission path. A new Rx Diameter session is established for each new AF session.

The AF may include the AF-Application-Identifier AVP into the AA-Request in order to indicate the particular service that the AF session belongs to. This AVP can be provided at both AF session level, and Media-Component-Description level. When provided at both levels, the AF-Application Identifier provided within the Media-Component-Description AVP will have precedence. The AF may also include an AF application identifier within the AF-Application-Identifier AVP at the AF session level to trigger the PCRF to indicate to the PCEF/TDF to perform the application detection based on the operator's policy as defined in 3GPP TS 29.212 [8].

The AF may include the AF-Charging-Identifier AVP into the AA-Request for charging correlation purposes. The AF may also include the Specific-Action AVP to request notification for certain user plane events, e.g. bearer termination.

The AF may include the Service-URN AVP in order to indicate that the new AF session relates to emergency traffic and additionally it may include the AF-Requested-Data AVP to indicate the information required by the AF. If the PCRF receives the Service-URN AVP indicating an emergency session, the PCRF may apply special policies, for instance prioritising service flows relating to the new AF session or allowing these service flows free of charge. If the Service-URN AVP indicates that the new AF session relates to emergency traffic and the AF-Requested-Data AVP is received, the PCRF shall provide the requested available user information as part of the AA-Answer command.

The AF may include the MPS-Identifier AVP in order to indicate that the new AF session relates to an MPS session. If the PCRF receives the MPS-Identifier AVP indicating an MPS session, the PCRF may take specific actions on the corresponding IP-CAN to ensure that the MPS session is prioritized as specified in 3GPP TS 29.212 [8]. For Multimedia Priority Sevice handling, see Annex A.9.

The AF may include the MCPTT-Identifier AVP in order to indicate that the new AF session relates to an MCPTT session with priority call. If the PCRF receives the MCPTT-Identifier AVP related to that MCPTT session, the PCRF may take specific actions on the corresponding IP-CAN to ensure that the MCPTT session is prioritized. For the handling of MCPTT session with priority call, see Annex A.13.

The AF may include the Priority-Sharing-Indicator AVP set to PRIORITY_SHARING_ENABLED within the Media-Component-Description AVP in order to indicate to the PCRF that the related media flow is allowed to use the same Allocation and Retention Priority (ARP) as media flows belonging to other AF sessions as described in subclause 4.4.8. In this case, if the MCPTT-Preemption is supported, the AF may also include the Pre-emption-Capability AVP containing the suggested pre-emption capability value and the Pre-emption-Vulnerability AVP containing the suggested pre-emption vulnerability value within the Media-Component-Description AVP for the PCRF to determine the ARP values. The AF may also include the Pre-emption-Control-Info AVP containing the pre-emption control information at the AAR command level for the PCRF to perform the pre-emption control as defined in subclause 4.5.27 or 4a.5.17 of 3GPP TS 29.212 [8].

The AF may include the Sharing-Key-UL and/or Sharing-Key-DL AVP within the Media-Component-Description AVP in order to indicate that the related media of the new AF session may share resources with other media components in the related direction that include the same value for the Sharing-Key-UL AVP and/or Sharing-Key-DL AVP.

When the AF is a GCS AS, it may include the GCS-Identifier AVP at command level and Reservation-Priority AVP at command level or media component level in order to indicate that the new AF session relates to a prioritized Group Communication session. Based on this information, the PCRF may take specific actions on the corresponding IP-CAN to ensure that the Group Communication session is prioritized as specified in 3GPP TS 29.212 [8].

If the AF provides service information that has been fully negotiated (e.g. based on the SDP answer), the AF may include the Service-Info-Status AVP set to FINAL_SERVICE_INFORMATION. In this case the PCRF shall authorize the session and provision the corresponding PCC/QoS rules to the PCEF/BBERF.

The AF may additionally provide preliminary service information not fully negotiated yet (e.g. based on the SDP offer) at an earlier stage. To do so, the AF shall include the Service-Info-Status AVP with the value set to PRELIMINARY SERVICE INFORMATION. Upon receipt of such preliminary service information, the PCRF shall perform an early authorization check of the service information. For GPRS, the PCRF shall not provision PCC rules towards the PCEF unsolicitedly. However, the PCRF may authorize a PCC/QoS rule request received from the PCEF/BBERF as per 3GPP TS 29.212 [8]. Further, if the AF requests the PCRF to report the access network information together with preliminary service information, the PCRF shall immediately configure the PCEF (or BBERF) to provide the access network information.

For sponsored data connectivity and if SponsoredConnectivity is supported, the AF shall provide the application service provider identity and the sponsor identity to the PCRF byincluding the Application-Service-Provider-Identity AVP and the Sponsor-Identity AVP in the Sponsored-Connectivity-Data AVP in the AA-Request. Additionally if SponsorChange is supported the AF shall provide an indication whether to enable or not enable sponsored data connectivity to the PCRF by including the Sponsoring-Action AVP set to the applicable value.

NOTE 3: The relationship between the AF and Sponsor is out of scope of this specification. A single AF can serve multiple ASPs and multiple sponsors, An ASP can also be a sponsor.

To support the usage monitoring of sponsored data connectivity, the AF may also include the Granted-Service-Unit AVP in the Sponsored-Connectivity-Data AVP and the Specific-Action AVP set to the value USAGE_REPORT in the AA-Request to request notification when the usage threshold has been reached.

NOTE 4: If the AF is in the user plane, the AF can handle the usage monitoring and therefore it is not required to provide a usage threshold to the PCRF as part of the sponsored data connectivity information.

When SponsoredConnectivity is supported or when SponsorChange is supported and the AF indicated to enable sponsored data connectivity, the following procedures apply:

- If the UE is roaming with the visited access case and the AF is located in the HPLMN or roaming with the home routed case and operator policies do not allow accessing the sponsored data connectivity with this roaming case, the H-PCRF shall reject the service request indicating UNAUTHORIZED_SPONSORED_DATA_CONNECTIVITY to the AF.

- If the UE is roaming with the visited access case and the AF is located in the VPLMN, the V-PCRF shall reject the service request indicating UNAUTHORIZED_SPONSORED_DATA_CONNECTIVITY to the AF.

When SponsoredConnectivity is supported or when SponsorChange is supported and the AF indicated to enable sponsored data connectivity, if the UE is in the non-roaming case or roaming with the home routed case and the operator policies allow accessing the sponsored data connectivity with this roaming case, the following procedures apply:

- If the PCEF/TDF does not support sponsored connectivity and the required reporting level for that service indicates a sponsored connectivity level according to 3GPP TS 29.212 [8], then the PCRF shall reject the request indicating REQUESTED_SERVICE_NOT_AUTHORIZED.

- If the PCEF/TDF supports sponsored data connectivity feature or the required reporting level is different from sponsored connectivity level as described in 3GPP TS 29.212 [8], then the PCRF, based on operator policies, shall check whether it is required to validate the sponsored connectivity data. If it is required, it shall perform the authorizations based on sponsored data connectivity profiles. If the authorization fails, the PCRF responds to the AF with an AA-Answer including the Experimental-Result-Code AVP set to the value UNAUTHORIZED_SPONSORED_DATA_CONNECTIVITY. The profile may include a list of Application Service Providers and their applications per sponsor.

NOTE 5: If the AF is in the operator's network and is based on the OSA/Parlay-X GW, the PCRF is not required to verify that a trust relationship exists between the operator and the sponsors.

When the PCRF receives an initial AA-Request from the AF, the PCRF shall perform session binding as described in 3GPP TS 29.213 [9]. To allow the PCRF to identify the IP-CAN session for which this request applies, the AF shall provide either the Framed-IP-Address or the Framed-Ipv6-Prefix containing the full IP address applicable to an IP flow or IP flows towards the UE. In case of private IP address being used, the AF may provide PDN information if available in the Called-Station-Id AVP for session binding. The AF may provide the domain identity in the IP-Domain-Id AVP for session binding.

NOTE 6: The IP-Domain-Id AVP is helpful in the following scenario: Within a PLMN, there are several separate IP address domains, with PCEF(s) that allocate Ipv4 IP addresses out of the same private address range to UEs. The same IP address can thus be allocated to UEs served by PCEFs in different address domains. If one PCRF controls several PCEFs in different IP address domains, the UE IP address is thus not sufficient for the session binding. An AF can serve UEs in different IP address domains, either by having direct IP interfaces to those domains, or by having interconnections via NATs in the user plane between PCEFs and the AF. If a NAT is used, the AF obtains the IP address allocated to the UE via application level signalling and supplies it for the session binding as Framed-IP-Address to the PCRF. The AF supplies an IP-Domain-Id value denoting the IP address domain behind the NAT in addition. The AF can derive the appropriate value from the source address (allocated by the NAT) of incoming user plane packets. The value provided in the IP-Domain-Id AVP is operator configurable.

NOTE 7: When the scenario described in NOTE 6 applies and the AF is a P-CSCF it is assumed that the P-CSCF has direct IP interfaces to the different IP address domains and that no NAT is located between P-GW and P-CSCF. How a non-IMS AF obtains the UE private IP address to be provided to the PCRF is out of scope of the present release; it is unspecified how to support applications that use a protocol that does not retain the original UE's private IP address.

If the PCRF fails in executing session binding, the PCRF responds to the AF with an AA-Answer including the Experimental-Result-Code AVP set to the value IP-CAN_SESSION_NOT_AVAILABLE. Further details on how the PCRF identifies suitable IP-CAN sessions can be found in the binding mechanism described in 3GPP TS 29.213 [9].

If the request contains Media-Component-Description Attribute-Value Pair(s) (AVP(s)) the PCRF shall store the received Service Information. The PCRF shall process the received Service Information according to the operator policy and may decide whether the request is accepted or not. The PCRF may take the priority information within the Reservation-Priority AVP into account when making this decision.

For an IP-CAN session associated to a dedicated APN for the purpose of offering services to remote UEs via a ProSe UE-to-network relay UE, as defined in 3GPP TS 23.303 [46], the PCRF shall validate the service information based on the service/roaming agreement and the operator policies related to that PDN information.

NOTE 8: The PCRF is not required to be aware of the remote UE.

If the service information provided in the AA-Request command is rejected (e.g. the subscribed guaranteed bandwidth for a particular user is exceeded), the PCRF shall indicate in the AA-Answer command the cause for the rejection with the Experimental-Result-Code AVP set to the value REQUESTED_SERVICE_NOT_AUTHORIZED. If the service information provided in the AA-Request command is rejected by the PCRF due to a temporary condition in the network (e.g. the user plane in the cell the user is located is congested), the PCRF may indicate in the AA-Answer the cause for the rejection with the Experimental-Result-Code AVP set to the value REQUESTED_SERVICE_TEMPORARILY_NOT_AUTHORIZED (4261). The PCRF may also provide a retry-interval within the Retry-Interval AVP in the AA-Answer command to the AF. When the AF receives the re-try interval within the Retry-Interval AVP, the AF shall not send the same service information to the PCRF again (for the same IP-CAN session) until the re-try interval has elapsed. The PCRF may additionally provide the acceptable bandwidth within the Acceptable-Service-Info AVP in AA-Answer command.

NOTE 9: How the PCRF derives the re-try interval is up to implementation.

To allow the PCRF and PCEF to perform PCC rule authorization and bearer binding for the described service IP flows, the AF shall supply both source and destination IP addresses and port numbers within the Flow-Description AVP, if such information is available.

NOTE 10: In SDP source port information is usually not available.

The AF may specify the ToS-Traffic-Class AVP for the described service data flows together with the Flow-Description AVP.

NOTE 11: The ToS-Traffic-Class AVP can be useful when another packet filter attribute is needed to differentiate between flows. For example, (when EPS bearers are used for group communication services) flows encapsulated and encrypted by a tunneling protocol and thus having their IP five-tuple attributes obscured can be differentiated by the Type of Service (or Traffic Class) value of the outer header.

NOTE 12: The use of ToS-Traffic-Class AVP by the AF assumes that no DSCP re-marking is applied from the application to the PGW.

The AF may specify the Reservation-Priority AVP at request level in the AA-Request in order to assign a priority to the AF Session as well as specify the Reservation-Priority AVP at the media-component-description AVP level to assign a priority to the IP flow. The presence of the Reservation-Priority in both levels does not constitute a conflict as they each represent different types of priority. Specifically the Reservation-Priority at the AA-Request level provides the relative priority for a session while the Reservation-Priority at the media-component-description level provides the relative priority for an IP flow within a session. If the Reservation-Priority AVP is not specified the requested priority is DEFAULT (0).

The AF may request notifications of specific IP-CAN session events through the usage of the Specific-Action AVP in the AA-Request command. The PCRF shall make sure to inform the AF of the requested notifications in the event that they take place.

The AF may include the Rx-Request-Type AVP set to INITIAL_REQUEST in the AAR.

The AF may include a Reference Id within the Reference-Id AVP related to a transfer policy negotiated for background data transfer via the Nt reference point as described in 3GPP TS 29.154 [47]. The PCRF shall retrieve the corresponding transfer policy from the SPR based on the Reference Id. If the PCRF can not retrieve the transfer policy, the PCRF shall include in the AA-Answer the Service-Authorization-Info AVP with the bit 0 set to indicate that the transfer policy is unknown. If the time window of the received transfer policy has expired, the PCRF shall include in the AA-Answer the Service-Authorization-Info AVP with the bit 1set to indicate that the transfer policy has expired. Otherwise, if the time window of the received transfer policy has not yet occurred, the PCRF shall include in the AA-Answer the Service-Authorization-Info AVP with the bit 2 set to indicate that the time window of the transfer policy has not yet occurred.

NOTE 13: In the case that the PCRF can not retrieve the transfer policy or the transfer policy expired, the PCRF makes the decision without considering the transfer policy.

The PCRF shall check whether the received Service Information requires PCC/QoS Rules to be created and provisioned and/or authorized QoS to be provisioned as specified in 3GPP TS 29.213 [9]. Provisioning of PCC/QoS Rules and Authorized QoS to the PCEF/BBERF shall be carried out as specified at 3GPP TS 29.212 [8].

If the Sharing-Key-UL AVP and/or Sharing-Key-DL AVP are provided within the Media-Component-Description AVP, the PCRF may apply the mechanisms for resource sharing as specified at 3GPP TS 29.212 [8].

The PCRF shall reply with an AA-Answer to the AF. The acknowledgement towards the AF should take place before or in parallel with any required PCC Rule provisioning towards the PCEF and shall include the Access-Network-Charging-Identifier(s) and may include the Access-Network-Charging-Address AVP, if they are available. The AA-Answer message shall also include the AN-GW-Address AVP, if the PCRF has previously requested to be updated with this information in the PCEF. The AA-Answer message shall also include the PLMN identifier within the 3GPP-SGSN-MCC-MNC AVP if the PCRF has previously requested to be updated with this information in the PCEF/BBERF. The AA-Answer message shall also include the IP-CAN-Type AVP. if the PCRF has previously requested to be updated with this information in the PCEF/BBERF. In that case, the AA-Answer message shall also include the RAT type information within the RAT-Type AVP and AN-Trusted AVP when applicable for the specific IP-CAN Type. In addition, if IP flow mobility applies to service data flows as specified in 3GPP TS 29.212 [8], such that a subset of the flows within the AF session are affected, the PCRF shall also include IP-CAN-type and RAT type information (if applicable) to IP flow mobility related flows, if such information is available. The IP flow mobility affected service data flows are included within the Flows AVP at command level. If the PCRF needs to terminate the Rx session before it has sent the AA Answer, the PCRF shall send the AA Answer immediately and before the AS Request.

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 this specification and based on operator policy.

If the PCRF fails in installing PCC/QoS rules based on the provided service information due to resource allocation failure as specified in 3GPP TS 29.212 [8] and if requested by the AF, the PCRF shall send an RAR command to the AF with the Specific-Action AVP set to the value INDICATION_OF_FAILED_RESOURCES_ALLOCATION to report the resource allocation failure, the Flows AVP containing the service data flows corresponding to the resources that could not be allocated, and the content version within the Content-Version AVP if it was included when the corresponding media component was provisioned. The AF shall send an RAA command to acknowledge the RAR command.

4.4.2 Modification of Session Information

The AF may modify the session information at any time (e.g. due to an AF session modification or internal AF trigger) by sending an AA-Request command to the PCRF containing the Media-Component-Description AVP(s) with the updated Service Information. The AF shall send an AA-Request command to the PCRF, only after the previous AA-Request has been acknowledged.

If the AF provides service information that has been fully negotiated (e.g. based on the SDP answer), the AF may include the Service-Info-Status AVP set to FINAL_SERVICE_INFORMATION. In this case the PCRF shall authorize the session and provision the corresponding PCC rules to the PCEF.

The AF may additionally provide preliminary service information not fully negotiated yet (e.g. based on the SDP offer) at an earlier stage. To do so, the AF shall include the Service-Info-Status AVP with the value set to PRELIMINARY SERVICE INFORMATION. Upon receipt of such preliminary service information, the PCRF shall perform an early authorization check of the service information. For GPRS, the PCRF shall not provision PCC rules towards the PCEF unsolicitedly. However, the PCRF may authorize a PCC/QoS rule request received from the PCEF/BBERF as per 3GPP TS 29.212 [8]. Further, if the AF requests the PCRF to report the access network information together with preliminary service information, the PCRF shall immediately configure the PCEF (or BBERF) to provide the access network information.

The AF may include the Rx-Request-Type AVP set to UPDATE_REQUEST in the AAR.

The AF may include a Reference Id within the Reference-Id AVP related to a transfer policy negotiated for background data transfer via the Nt reference point as described in 3GPP TS 29.154 [47]. The AF shall retrieve the corresponding transfer policy from the SPR based on the Reference Id. If the PCRF can not retrieve the transfer policy, the PCRF shall include in the AA-Answer the Service-Authorization-Info AVP with the bit 0 set to indicate that the transfer policy is unknown. If the time window of the received transfer policy has expired, the PCRF shall include in the AA-Answer the Service-Authorization-Info AVP with the bit 1set to indicate that the transfer policy has expired. Otherwise, if the time window of the received transfer policy has not yet occurred, the PCRF shall include in the AA-Answer the Service-Authorization-Info AVP with the bit 2 set to indicate that the time window of the transfer policy has not yet occurred.

NOTE 1: In the case that the PCRF can not retrieve the transfer policy or the transfer policy expired, the PCRF makes the decision without considering the transfer policy.

The AF may include the MPS-Identifier AVP in order to indicate that the modified AF session relates to an MPS session. If the PCRF receives the MPS-Identifier AVP, it may take specific actions on the corresponding IP-CAN to

ensure that the MPS session is prioritized as defined in 3GPP TS 29.212 [8]. For Multimedia Priority Sevice handling, see Annex A.9.

The AF may include the MCPTT-Identifier AVP in order to indicate that the modified AF session relates to the priority adjustment of an MCPTT session. If the PCRF receives the MCPTT-Identifier AVP related to that MCPTT session, the PCRF may take specific actions on the corresponding IP-CAN to ensure that the MCPTT session is prioritized. For the handling of MCPTT session with priority call, see Annex A.13.

The AF may include the Priority-Sharing-Indicator AVP set to PRIORITY_SHARING_ENABLED within the Media-Component-Description AVP in order to indicate to the PCRF that the related media flow is allowed to use the same Allocation and Retention Priority (ARP) as media flows belonging to other AF sessions as described in subclause 4.4.8. In this case, if the MCPTT-Preemption is supported, the AF may also include the Pre-emption-Capability AVP containing the suggested pre-emption capability value and the Pre-emption-Vulnerability AVP containing the suggested pre-emption vulnerability value within the Media-Component-Description AVP for the PCRF to determine the ARP values. The AF may also include the Pre-emption-Control-Info AVP containing the pre-emption control information at the AAR command level for the PCRF to perform the pre-emption control as defined in subclause 4.5.27 or 4a.5.17 of 3GPP TS 29.212 [8].

The AF may include the Sharing-Key-UL AVP and/or Sharing-Key-DL AVP within the Media-Component-Description AVP in order to indicate that the related media of the modified AF session may share resources with other media components in the related direction that include the same Sharing-Key-UL and or Sharing-Key-DL AVP. The AF may modify the conditions for resource sharing by including a new value of the Sharing-Key-UL AVP and/or Sharing-Key-DL AVP for that media component.

When the AF is a GCS AS, it may include the GCS-Identifier AVP at command level and Reservation-Priority AVP at command level or media component level in order to modify the priority of an AF session that relates to a prioritized Group Communication session. Based on this information, the PCRF may take specific actions on the corresponding IP-CAN to ensure that the Group Communication session is prioritized as specified in 3GPP TS 29.212 [8].

For sponsored data connectivity and if SponsoredConnectivity is supported, the AF shall provide the application service provider identity and the sponsor identity to the PCRF by including Application-Service-Provider-Identity AVP and the Sponsor-Identity AVP in the Sponsored-Connectivity-Data AVP in the AA-Request.

If SponsorChange is supported and the AF requests to enable sponsored data connectivity the AF shall provide the application service provider identity, the sponsor identity and an indication to enable sponsored data connectivity to the PCRF by including Application-Service-Provider-Identity AVP, the Sponsor-Identity AVP and the Sponsoring-Action AVP set to the value ENABLE_SPONSORING (1) in the Sponsored-Connectivity-Data AVP in the AA-Request.

If the AF requests to disable sponsored data connectivity the AF shall provide an indication to disable sponsored data connectivity to the PCRF by including the Sponsoring-Action AVP set to the value DISABLE_SPONSORING (0) in the Sponsored-Connectivity-Data AVP in the AA-Request.

To support the usage monitoring of sponsored data connectivity, the AF may also include the Granted-Service-Unit AVP in the Sponsored-Connectivity-Data AVP in the AA-Request.

NOTE 2: If the AF is in the user plane, the AF can handle the usage monitoring and therefore it is not required to provide a usage threshold to the PCRF as part of the sponsored data connectivity information.

When sponsored data connectivity is requested to be enabled the following procedures apply:

- If the UE is roaming with the visited access case and the AF is located in the HPLMN or roaming with the home routed case and operator policies do not allow accessing the sponsored data connectivity with this roaming case, the H-PCRF shall reject the service request indicating UNAUTHORIZED_SPONSORED_DATA_CONNECTIVITY to the AF.

- If the UE is roaming with the visited access case and the AF is located in the VPLMN, the V-PCRF shall reject the service request indicating UNAUTHORIZED_SPONSORED_DATA_CONNECTIVITY to the AF.

When sponsored data connectivity is requested to be enabled, if the UE is in the non-roaming case or roaming with the home routed case and the operator policies allow accessing the sponsored data connectivity with this roaming case, the following procedures apply:

- If the PCEF/TDF does not support sponsored connectivity and the required reporting level for that service indicates a sponsored connectivity level according to 3GPP TS 29.212 [8], then the PCRF shall reject the request indicating REQUESTED_SERVICE_NOT_AUTHORIZED.

- If the PCEF/TDF supports sponsored data connectivity feature or the required reporting level is different from sponsored connectivity level as described in 3GPP TS 29.212 [8], then the PCRF, based on operator policies, shall check whether it is required to validate the sponsored connectivity data. If it is required, it shall perform the authorizations based on sponsored data connectivity profiles. If the authorization fails, the PCRF responds to the AF with an AA-Answer including the Experimental-Result-Code AVP set to the value UNAUTHORIZED_SPONSORED_DATA_CONNECTIVITY. The profile may include a list of Application Service Providers and their applications per sponsor.

NOTE 3: If the AF is in the operator's network and is based on the OSA/Parlay-X GW, the PCRF is not required to verify that a trust relationship exists between the operator and the sponsors.

The AF may include an AF application identifier within the AF-Application-Identifier AVP at the session level to trigger the PCRF to indicate to the PCEF/TDF to perform the application detection based on the operator's policy as defined in 3GPP TS 29.212 [8].

The PCRF shall process the received Service Information according the operator policy and may decide whether the request is accepted or not. If the updated Service Information is not acceptable (e.g. subscribed guaranteed bandwidth for a particular user is exceeded), the PCRF shall indicate in the AA-Answer command the cause for the rejection with the Experimental-Result-Code AVP set to the value REQUESTED_SERVICE_NOT_AUTHORIZED. If the service information provided in the AA-Request command is rejected by the PCRF due to a temporary condition in the network (e.g. the user plane in the cell the user is located is congested), the PCRF may indicate in the AA-Answer the cause for the rejection with the Experimental-Result-Code AVP set to the value REQUESTED_SERVICE_TEMPORARILY_NOT_AUTHORIZED (4261). The PCRF may also provide a retry-interval within the Retry-Interval AVP in the AA-Answer command to the AF. When the AF receives the re-try interval within the Retry-Interval AVP, the AF shall not send the same service information to the PCRF again (for the same IP-CAN session) until the re-try interval has elapsed. The PCRF may additionally provide the acceptable bandwidth within the Acceptable-Service-Info AVP in the AA-Answer command.

NOTE 4: How the PCRF derives the re-try interval is up to implementation.

If accepted, the PCRF shall update the Service Information with the new information received. Due to the updated Service Information, the PCRF may need to create, modify or delete the related PCC rules as specified in 3GPP TS 29.213 [9] and provide the updated information towards the PCEF following the corresponding procedures specified at 3GPP TS 29.212 [8]. The procedures to update the Authorized QoS for the affected IP-CAN bearer are also specified at 3GPP TS 29.212 [8].

If the Sharing-Key-UL AVP and/or Sharing-Key-DL AVP are provided within the Media-Component-Description AVP, the PCRF may apply the mechanisms for resource sharing as specified at 3GPP TS 29.212 [8].

The PCRF shall reply with an AA-Answer to the AF. The acknowledgement towards the AF should take place before or in parallel with any required PCC Rule provisioning towards the PCEF and shall include the Access-Network-Charging-Identifier(s) and may include the Access-Network-Charging-Address AVP, if they are available at this moment and have not been yet supplied earlier to the AF. The AA-Answer message shall include the AN-GW-Address AVP if the PCRF has previously requested to be updated with this information in the PCEF. The AA-Answer message shall also include the PLMN identifier within the 3GPP-SGSN-MCC-MNC AVP if the PCRF has previously requested to be updated with this information in the PCEF/BBERF. The AA-Answer message shall also include the IP-CAN-Type AVP if the PCRF has previously requested to be updated with this information in the PCEF/BBERF . In that case, the AA-Answer message shall also include the RAT type information within the RAT-Type AVP and AN-Trusted AVP when applicable for the specific IP-CAN Type. In addition, if IP flow mobility applies to service data flows as specified in 3GPP TS 29.212 [8], such that a subset of the flows within the AF session are affected, the PCRF shall also include IP-CAN-type and RAT type information (if applicable) to IP flow mobility related flows, if the PCRF has previously requested to be updated with this information in the PCEF. The IP flow mobility affected service data flows are included within the Flows AVP at command level. If the PCRF needs to terminate the Rx session before it has sent the AA Answer, the PCRF shall send the AA Answer immediately and before the AS Request. If the PCRF does not have an existing session for the Rx session being modified (such as after a PCRF failure), the PCRF may reject the request with an AA-Answer with the result code set to DIAMETER_UNKNOWN_SESSION_ID.

If the PCRF installs PCC/QoS rules or modifies existing PCC/QoS rules based on the updated service information and the installation or modification fails due to resource allocation failure as specified in 3GPP TS 29.212 [8] and if requested by the AF, the PCRF shall send an RAR command to the AF with the Specific-Action AVP set to the value INDICATION_OF_FAILED_RESOURCES_ALLOCATION to report the modification failure, the Flows AVP containing the service data flows corresponding to the resources that could not be allocated, and the content version(s) within the Content-Version AVP(s) if it was included when the corresponding media component was provisioned. If the

modification of the existing PCC/QoS rules fails, the PCRF may also provide the status of the service information within the Media-Component-Status AVP. The AF shall send an RAA command to acknowledge the RAR command.

NOTE 5: The PCRF will report the Media-Component-Status AVP according to the status reported for the related PCC/QoS rules when the modification fails over the Gx/Gxx reference points as described in 3GPP TS 29.212 [8].

4.4.3 Gate Related Procedures

Depending on the application, in the Service Information provision, the AF may instruct the PCRF when the IP flow(s) are to be enabled or disabled to pass through the IP-CAN. The AF does this by sending the AA-Request message containing the Media-Component- Description AVP(s) that contains the flow status information (in the Flow-Status AVP) for the flows to be enabled or disabled.

In response to this action the PCRF shall set the appropriate gate status for the corresponding active PCC rule(s).

If a Media-Sub-Component AVP under a Media-Component-Description AVP contains a Flow-Usage AVP with the value RTCP, then the corresponding RTCP IP Flows in both directions shall be enabled even if the Flow-Status AVP under the Media-Sub-Component AVP is set to ENABLED-UPLINK, ENABLED-DOWNLINK, ENABLED, or DISABLED.

The PCRF shall reply with an AA-Answer and shall include the Access-Network-Charging-Identifier(s) available at this moment. The PCRF forwards the AF decision to enable or disable the authorized IP flows.

The behaviour when the AF does not receive the AAA, 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 this specification and based on operator policy.

4.4.4 AF Session Termination

When an AF session is terminated, if the AF had received a successful AA-Answer for the initial AA-Request, the AF shall send a Session-Termination-Request command to the PCRF. Otherwise, the AF shall wait for the initial AA-Answer to be received prior to sending the Session-Termination-Request command to the PCRF.

When the PCRF receives a ST-Request from the AF, indicating an AF session termination, it shall acknowledge that request by sending a ST-Answer to the AF. Afterwards, it shall free the resources allocated for the corresponding Service Data Flow(s). In order to do that, the PCRF shall initiate the request for the removal of any related PCC/QoS rules from the PCEF/BBERF and for the update of the Authorized QoS for the affected IP-CAN bearer following the corresponding procedures specified at 3GPP TS 29.212 [8]. However, if the AF requests the reporting of access network information within the ST-Request or if the AF provided a threshold for the sponsored data connectivity, the PCRF shall defer sending the ST-Answer.

If the AF session being terminated corresponds to an MPS session, the PCRF may revoke the actions related to the prioritization of the MPS session in the corresponding IP-CAN as defined in 3GPP TS 29.212 [8]. For Multimedia Priority Service handling, see Annex A.9.

If the AF session being terminated corresponds to the last Group Communication session for the IP-CAN session, the PCRF may revoke the actions related to the prioritization of the Group Communication session as specified in 3GPP TS 29.212 [8].

If the AF session being terminated corresponds to a session that included the Priority-Sharing-Indicator AVP set to PRIORITY_SHARING_ENABLED within the Media-Component-Description AVP, the PCRF should readjust the Allocation and Retention Priority for the remaining services sharing priority as described in subclause 4.4.8.

For sponsored data connectivity, and if a usage threshold was provided for the sponsored data connection at initial provisioning of session information (clause 4.4.1) or modification of session information (clause 4.4.2) procedures, the PCRF shall provide the usage consumed to the AF. For such purpose, the PCRF shall initiate the IP-CAN session modification procedure according 3GPP TS 29.212 [8] in order to obtain the consumed usage. The PCRF shall send then the ST-Answer to the AF including the Used-Service-Unit AVP for reporting accumulated usage within the Sponsored-Connectivity-Data AVP.

If the AF requires access network information at this step, the AF shall include the Required-Access-Info AVP within the ST-Request command, indicating the required information. In this case, the PCRF shall initiate the IP-CAN session

modification procedure according to 3GPP TS 29.212 [8]. The PCRF shall send then the ST-Answer to the AF including the required data within the 3GPP-User-Location-Info AVP (if available), TWAN-Identifier AVP (if available), User-Location-Info-Time AVP (if available), UE-Local-IP-Address AVP (if available), UDP-Source-Port AVP (if available), TCP-Source-Port AVP (if available), 3GPP-SGSN-MCC-MNC AVP (if location info is not available) and/or 3GPP-MS-TimeZone AVP (if available).

If the RAN-NAS-Cause feature is supported and the AF initiated the termination of the AF session, upon reception of the ST-Request command, the PCRF shall initiate the IP-CAN session modification procedure according to 3GPP TS 29.212 [8].

If the RAN-NAS-Cause feature is supported , in all the AF session termination cases , t he PCRF shall send the ST-Answer to the AF including the access network information within the 3GPP-User-Location-Info AVP (if available), TWAN-Identifier (if available and Netloc-Trusted-WLAN feature is supported) User-Location-Info-Time AVP (if available), 3GPP-SGSN-MCC-MNC AVP (if location info is not available) and/or 3GPP-MS-TimeZone AVP (if available). Additionally, if the PCRF received from the PCEF the RAN cause and/or NAS cause, TWAN cause or untrusted WLAN cause, the PCRF shall provide the received cause(s) in the RAN-NAS-Release-Cause AVP in the ST-Answer command.

NOTE: The PCRF will apply the procedures described in 3GPP TS 29.212 [8] to get updated about the outcome of the resource release over Gx reference point in order to get the location and failure cause(s) when applicable.

4.4.5 Subscription to Notification of Signalling Path Status

An AF may subscribe to notifications of the status of the AF Signalling transmission path. To do so, the AF shall open an Rx Diameter session with the PCRF for the AF signalling using an AA-Request command. The AF shall provide the UE's IP address (using either the Framed-IP-Address AVP or the Framed-Ipv6-Prefix AVP) and the Specific-Action AVP requesting the subscription to "INDICATION_OF_LOSS_OF BEARER" and/or "INDICATION_OF_RELEASE_OF_BEARER". The AF shall additionally provide a Media-Component-Description AVP including a single Media-Sub-Component AVP with the Flow-Usage AVP set to the value "AF_SIGNALLING". The Media-Component-Description AVP shall contain the Media-Component-Number AVP set to "0".

If the procedures in Clause 4.4.5a are not applied, the Media-Sub-Component AVP shall contain the Flow-Number AVP set to "0", and the rest of AVPs within the Media-Component-Description and Media-Sub-Component AVPs shall not be used in this case.

When the PCRF receives an AA-Request as described in the preceding paragraph from the AF, the PCRF shall perform session binding as described in 3GPP TS 29.213 [9] and acknowledges the AAR command by sending an AA-Answer command to the AF.

PCC/QoS Rules related to AF Signalling IP Flows should be provisioned to PCEF/BBERF using the corresponding procedures specified at 3GPP TS 29.212 [8] at an earlier stage (e.g. typically at the establishment of the IP-CAN bearer dedicated for AF Signalling IP Flows). The PCRF may install the corresponding dynamic PCC/QoS rule for the AF signalling IP flows if none has been installed before.

NOTE 1: Well-known ports (e.g. 3GPP TS 24.229 [17] for SIP) or wildcard ports can be used by PCRF to derive the dynamic PCC/QoS rule for the AF signalling IP flows.

If the Rx Diameter Session is only used for subscription to Notification of Signalling Path Status, the AF may cancel the subscription to notifications of the status of the AF Signalling transmission path. In that case, the AF shall use a Session-Termination-Request (STR) command to the PCRF, which shall be acknowledged with a Session-Termination-Answer (STA) command.

NOTE 2: The Rx Diameter Session created for the AF signalling can also be used when the AF requests notifications of IP-CAN type change, PLMN change and/or when the AF provisions AF Signalling Flow Information.

4.4.5a Provisioning of AF Signalling Flow Information

This clause is applicable when IMS restoration is supported according to supported feature ProvAFsignalFlow as described in clause 5.4.1.

An AF may provision information about the AF signalling IP flows between the UE and the AF. To do so, the AF shall make use of an Rx Diameter session already opened with the PCRF if an Rx Diameter session related to the AF signalling is already established. The AF may modify an already open Rx Diameter session related to the AF signalling (e.g. an Rx Diameter session established for the purpose of subscription to notification of signalling path status as described in 4.4.5) or it may open a new Rx Diameter session related to the AF signalling if none exists.

To provision the AF signalling flow information the AF shall provide the UE's IP address using either Framed-IP-Address AVP or Framed-Ipv6-Prefix AVP. The AF shall additionally provide a Media-Component-Description AVP including one or more Media-Sub-Component AVP(s) representing the AF signalling IP flows. The Media-Component-Description AVP shall contain the Media-Component-Number AVP set to "0". Each Media-Sub-Component AVP representing an AF signalling IP flow shall contain the Flow-Number AVP set according to the rules described in Annex B and one or two Flow-Description AVP(s) set to the IP flows of the AF signalling. Additionally, the Media-Sub-Component AVP shall include the Flow-Usage AVP set to the value "AF_SIGNALLING", the Flow-Status AVP set to "ENABLED" and the AF-Signalling-Protocol AVP set to the value corresponding to the signalling protocol used between the UE and the AF.

When the PCRF receives from the AF an AA-Request as described in the preceding paragraph, the PCRF shall perform session binding as described in 3GPP TS 29.213 [9] and shall acknowledge the AAR command by sending an AA-Answer command to the AF.

PCC/QoS Rules related to the AF signalling IP flows could have been provisioned to PCEF/BBERF using the corresponding procedures specified in 3GPP TS 29.212 [8] at an earlier stage (e.g. typically at the establishment of the IP-CAN bearer dedicated for AF Signalling IP Flows). The PCRF shall install the corresponding dynamic PCC/QoS rule for the AF signalling IP flows.

The AF may de-provision the information about the AF signalling IP flows at any time. To do that, if the Rx Diameter session is only used to provide information about the AF Signalling IP flows, the AF shall close the Rx Diameter session by sending a Session-Termination-Request (STR) command to the PCRF, which shall be acknowledged with a Session-Termination-Answer (STA) command. Otherwise, the AF shall remove the IP flows within the Media-Sub-Component AVP by supplying the Flow-Status AVP with value "REMOVED". In both cases, the PCRF shall remove the corresponding dynamic PCC/QoS rule for the AF signalling IP flows.

4.4.6 Traffic Plane Events

4.4.6.1 IP-CAN Session Termination

When an IP-CAN session is terminated, the PCRF shall inform the AF about the IP-CAN session termination by sending an ASR (abort session request) command to the AF on each active Rx Diameter session.

When the AF receives the ASR command, it shall acknowledge the command by sending an ASA (abort session answer) command to the PCRF. After that the AF shall initiate an AF session termination procedure as defined in subclause 4.4.4.

Signalling flows for IP-CAN session termination cases are presented in 3GPP TS 29.213 [9].

4.4.6.2 Service Data Flow Deactivation

It may happen that one or more PCC/QoS Rules (i.e. Service Data Flows) are deactivated at the PCEF/BBERF at a certain time, either permanently or temporarily. When the PCRF gets the knowledge that one or more SDFs have been deactivated, (e.g. due to a bearer release or loss of bearer or out of credit condition), the PCRF shall inform the AF accordingly if the AF has previously subscribed using the Specific-Action AVP in the AAR command.

When not all the service data flows within the AF session are affected, the PCRF shall inform the AF by sending an RAR (re-authorization request) command. The RAR command shall include the deactivated IP Flows encoded in the Flows AVP, the cause encoded in the Specific-Action AVP and the content version of a media component within the Content-Version AVP if it was included when the media component was provisioned.

If the RAN-NAS-Cause feature is supported and the PCRF received the access network information from the PCEF/BBERF due to bearer termination, the PCRF shall include in the RAR command the access network information within the 3GPP-User-Location-Info AVP (if available), TWAN-Identifier (if available and Netloc-Trusted-WLAN feature is supported) User-Location-Info-Time AVP (if available), 3GPP-SGSN-MCC-MNC AVP (if location info is not available) and/or 3GPP-MS-TimeZone AVP (if available). Additionally, if the PCRF received from the PCEF the

RAN cause and/or NAS cause, TWAN cause or untrusted WLAN cause due to bearer termination, the PCRF shall provide the received cause(s) in the RAN-NAS-Release-Cause AVP in the RAR command.

When the AF receives the RAR command, it shall acknowledge the command by sending an RAA (re-authorization answer) command to the PCRF. The AF may also update the session information by sending an AAR (AA-request) command to the PCRF.

If the PCRF receives the AAR command, it shall acknowledge the command by sending an AAA (AA-answer) command to the AF.

When all the service data flows within the AF session are affected, the PCRF shall inform the AF by sending an ASR command on the Rx Diameter session related to the AF session. When the AF receives the ASR command, it shall acknowledge the command by sending an ASA (abort session answer) command to the PCRF. After that the AF shall initiate an AF session termination procedure as defined in clause 4.4.4.

Signalling flows for Service Data Flow Deactivation cases are presented in 3GPP TS 29.213 [9].

4.4.6.3 Notification of Signalling Path Status

In the event that the PCRF is notified of the loss or release of resources associated to the PCC/QoS Rules corresponding with AF Signalling IP Flows, the PCRF shall inform the AF about the Loss of the Signalling Transmission path by sending a Re-Authorization Request (RAR) command to the AF. The RAR shall include the Specific-Action AVP set to the value "INDICATION_OF_LOSS_OF_BEARER" or "INDICATION_OF_RELEASE_OF_BEARER" and the deactivated IP Flow encoded in the Flows AVP.

NOTE: According to the standardized QCI characteristics as defined in 3GPP TS 23.203 [2], the IMS signalling specific PCC rules include a QCI corresponding to a non-GBR bearer. When these guidelines are followed, the INDICATION_OF_LOSS_OF_BEARER will not be reported.

If the RAN-NAS-Cause feature is supported and the PCRF received the access network information from the PCEF/BBERF due to bearer termination, the PCRF shall include in the RAR command the access network information within the 3GPP-User-Location-Info AVP (if available), TWAN-Identifier (if available and Netloc-Trusted-WLAN feature is supported) User-Location-Info-Time AVP (if available), 3GPP-SGSN-MCC-MNC AVP (if location info is not available) and/or 3GPP-MS-TimeZone AVP (if available). Additionally, if the PCRF received from the PCEF the RAN cause and/or NAS cause, TWAN cause or untrusted WLAN cause due to bearer termination, the PCRF shall provide the received cause(s) in the RAN-NAS-Release-Cause AVP in the RAR command.

When the AF receives the RAR command, it shall acknowledge the command by sending an RAA command to the PCRF.

The AF may then decide to terminate the Rx Diameter session used for the notification of the status of the AF Signalling transmission path. The AF may also decide to terminate any other active Rx Diameter session with the PCRF related to the AF Signalling which is not available any longer. In that case, the AF shall then initiate the AF Termination procedure towards the PCRF as defined in clause 4.4.4.

4.4.6.4 IP-CAN type change Notification

If the AF has successfully subscribed to change notifications in UE's IP-CAN type and RAT type, the PCRF shall send an RAR command when the corresponding event occurs, i.e. when the UE's IP-CAN type or RAT type changes or becomes available. In this case the RAR from the PCRF shall include the Specific-Action AVP for the subscribed event and include the IP-CAN-Type AVP, RAT-Type AVP (if applicable) and AN-Trusted AVP (if applicable) and AN-GW-Address AVP (if applicable) for the UE's new IP-CAN/RAT. If the PCRF is informed of an IP-CAN type change due to IP flow mobility as specified in 3GPP TS 29.212 [8], where a subset of the flows within the AF session are affected, the PCRF shall include IP-CAN type and RAT type information (if applicable) to IP flow mobility affected service data flows. The IP flow mobility affected service data flows are included within the Flows AVP at command level.

4.4.6.5 Access Network Charging Information Notification

If the AF has subscribed to a notification about Access Network Charging Information, the PCRF shall provide the Access Network Charging Information in the response, if already known by the PCRF. If not available, the PCRF shall provide the Access Network Charging Information by sending a Re-Authorization-Request (RAR) command when the Access Network Charging Information is received from the PCEF. If different Access Network Charging Information is applicable to the IP-CAN session, the PCRF shall notify the AF about the Access Network Charging Information that

applies to each authorized flow. The RAR shall include the Specific-Action AVP set to the value "CHARGING_CORRELATION_EXCHANGE" and shall include the assigned Access-Network-Charging-Identifier(s) and may include the Access-Network-Charging-Address AVP.

4.4.6.6 Reporting Usage for Sponsored Data Connectivity

When SponsoredConnectivity is supported or when SponsorChange is supported and the AF indicated to enable sponsored data connectivity and the AF provided usage monitoring thresholds for such sponsor to the PCRF when the Rx Diameter session was established or modified, the PCRF shall report accumulated usage to the AF, when

- the PCRF detects that the usage threshold provided by the AF has been reached; or
- the AF session is terminated by the AF;
- the AF disables the sponsored data connectivity; or
- the AF session is terminated by the PCRF due to the IP-CAN session termination, the termination of all the service data flows of the AF session or the home operator policy disallowing the UE accessing the sponsored data connectivity in the roaming case.

When the PCRF detects that the usage threshold has been reached or the AF disables the sponsored data connectivity, the PCRF shall report the accumulated usage as provided by the PCEF/TDF to the AF in a RA-Request (RAR) command with the Specific-Action AVP set to the value USAGE_REPORT; Otherwise, when the AF session is terminated by the AF or the PCRF, the PCRF shall report the accumulated usage as provided by the PCEF/TDF to the AF in ST-Answer (STA) command. The accumulated usage reported by the PCRF corresponds to the usage since the last report to the AF.

The accumulated usage shall be reported in the Used-Service-Unit AVP within the Sponsored-Connectivity-Data AVP.

If the AF receives a RAR command indicating the usage threshold is reached, the AF may terminate the AF session or provide a new usage threshold in the Granted-Service-Unit AVP within the Sponsored-Connectivity-Data AVP to the PCRF in the AAR command. Alternatively, the AF may allow the session to continue without providing new usage threshold in the AAR command.

NOTE: After the PCRF reports the accumulated usage to the AF, the AF can provide a new usage threshold to the PCRF. The monitoring will not start until the PCRF receives the new threshold from the AF and provide it to the PCEF

4.4.6.7 Reporting Access Network Information

If the AF requests the PCRF to report the access network information (i.e. user location and/or user timezone information), the AF shall subscribe to the "ACCESS_NETWORK_INFO_REPORT" within the Specific-Action AVP and shall include the required access network information within the Required-Access-Info AVP. The AF may request the PCRF to report the access network information in conjunction with providing the PCRF with the AF session information, refer to clause 4.4.1. Optionally, the AF may request the PCRF to report the access network information without providing service information (see clause A.10.2). In the latter case the AF establishes an Rx session for the AF session upon requesting the access network information from the PCRF with an AA-Request command, containing information required for the session binding in the Framed-IP-Address AVP, the Framed-Ipv6-Prefix AVP Subscription-Id AVP, the Called-Station-Id AVP and/or the IP-Domain-Id AVP.

The AF may also request the PCRF to report the access network information at Rx session termination. To do so, the AF shall include the required access network information within the Required-Access-Info AVP in the corresponding ST-Request.

When the PCRF receives a request to report the access network information from the AF in an AAR command or in an STR command triggered by the AF, if the PCRF determines that the access network does not support the access network information reporting based on the currently used IP-CAN type or the values of the RAT-Type AVP or the PCEF/BBERF does not support the access network information reporting based on the Supported-Feature AVP, the PCRF shall respond to AF with an AAA or STA command including the NetLoc-Access-Support AVP set to the value of 0 (NETLOC_ACCESS_NOT_SUPPORTED); otherwise, it shall immediately configure the PCEF or BBERF to provide such access network information.

When the PCRF then receives the access network information from the PCEF/BBERF, the PCRF shall provide the corresponding access network information to the AF within the 3GPP-User-Location-Info AVP (if available), TWAN-Identifier AVP (if available), User-Location-Info-Time AVP (if available), UE-Local-IP-Address AVP (if available), UDP-Source-Port AVP (if available), TCP-Source-Port AVP (if available), 3GPP-SGSN-MCC-MNC AVP (if location info is not available) and/or 3GPP-MS-TimeZone AVP in the RAR command if the Rx session is not being terminated or in the STA command if the Rx session is being terminated. If the information is provided in the RAR command, PCRF shall also provide the ACCESS_NETWORK_INFO_REPORT within Specific-Action AVP.

NOTE 1: The PCRF receives the access network information from the PCEF/BBERF if it is requested by the AF previously or the IP-CAN bearer/IP-CAN session is terminated.

When the PCRF receives the NetLoc-Access-Support AVP set to the value of 0 (NETLOC_ACCESS_NOT_SUPPORTED) from the PCEF/BBERF, the PCRF shall send a RAR command including the Specific-Action AVP set to INDICATION_OF_ACCESS_NETWORK_INFO_REPORTING_FAILURE and the NetLoc-Access-Support AVP set to the value of 0 (NETLOC_ACCESS_NOT_SUPPORTED) if the AF requested the access network information in an AAR command or send an STA command including the NetLoc-Access-Support AVP set to the value of 0 (NETLOC_ACCESS_NOT_SUPPORTED) if the AF requested the access network information in an S3GPP TR command.

NOTE 2: The 3GPP GPRS, 3GPP EPS, Untrusted WLAN and Trusted WLAN support access network information reporting in this release.

The PCRF shall not send an RAR command with the ACCESS_NETWORK_INFO_REPORT value within a Specific-Action AVP to report any subsequently received access network information to the AF, unless the AF sends a new request for access network information.

4.4.6.8 Temporary Network Failure handling

If the PCRF detects that a temporary network failure has occurred (e.g. the SGW has failed for 3GPP-EPS access as defined in clause B.3.14 of 3GPP TS 29.212 [8]) and the AF requests an AF session establishment or modification in an AA-Request command, the PCRF shall respond to the AF with an AA-Answer including the Experimental-Result-Code AVP set to the value TEMPORARY_NETWORK_FAILURE.

If the PCRF detects that a temporary network failure has occurred (e.g. the SGW has failed for 3GPP-EPS access) and the AF requests an AF session termination in a ST-Request command, the PCRF shall respond with successful Result-Code AVP to the AF.

NOTE 1: If the AF includes the Required-Access-Info AVP in the ST-Request command to request the access network information, the PCRF will not include the access network information in the ST-Answer command.

NOTE 2: Actions over Gx/Gxx reference point when there is a temporary network failure are described in 3GPP TS 29.212 [8]. For example, for S-GW Restoration procedures the PCRF will wait for the SGW recovery before deleting the corresponding PCC/QoS rules,according to clause B.3.14 in that specification.

If the PCRF detects that the PCC/QoS rules related to an AF session cannot be installed or modified because there is a temporary network failure (e.g. SGW failed according to clause B.3.14 in 3GPP TS 29.212 [8]) and if requested by the AF, the PCRF shall send a RA-Request command to the AF with the Specific-Action AVP set to INDICATION_OF_FAILED_RESOURCES_ALLOCATION and the content version of a media component within the Content-Version AVP if it was included when the media component was provisioned. If the modification of the PCC/QoS rules fails, the PCRF may provide the status of the related service information within the Media-Component-Status AVP.

4.4.6.9 PLMN information change Notification

If the AF has successfully subscribed to PLMN_CHANGE notification, the PCRF shall send an RAR command when the corresponding event occurs, i.e. when the PLMN where the UE is located has been updated or becomes available. In this case the RAR from the PCRF shall include the Specific-Action AVP set to PLMN_CHANGE and include the 3GPP-SGSN-MCC-MNC AVP for the PLMN where the UE is located.

4.4.7 P-CSCF Restoration Enhancement Support

This clause is applicable when the PCRF-based P-CSCF Restoration Enhancement, as defined in 3GPP TS 23.380 [28], is supported by both P-CSCF and PCRF.

The P-CSCF acting as AF shall send an AAR command including the Rx-Request-Type AVP set to the value PCSCF_RESTORATION (2) to the PCRF in the case P-CSCF Restoration needs to be performed. This AAR shall include the following information required by the DRA or PCRF to find the corresponding IP-CAN session:

- The UE's IP address as applicable in the Framed-IP-Address AVP or in the Framed-Ipv6-Prefix AVP. If the IP address is not unique (e.g. private IPv4 case), the P-CSCF shall also include the IP-Domain-ID AVP if available.

- If the IP address is not available or if the IP address is not unique and the IP-Domain-ID is not available, the P-CSCF shall include the IMSI in the Subscription-Id AVP and the APN in the Called-Station-Id AVP.

The AF shall also include the Auth-Session-State AVP set to the value NO_STATE_MAINTAINED (1) in the AAR command, as described in IETF RFC 6733 [52]. As a consequence, the PCRF shall not maintain any state information about this session.

The PCRF shall acknowledge the AAR command by sending an AAA command to the P-CSCF acting as AF and shall include the Auth-Session-State AVP set to NO_STATE_MAINTAINED (1). The PCRF shall send a request for P-CSCF Restoration to the PCEF for the corresponding IP-CAN session.

4.4.8 Priority Sharing Request

If PrioritySharing feature is supported, the AF may include the Priority-Sharing-Indicator AVP set to PRIORITY_SHARING_ENABLED within the Media-Component-Description AVP in order to indicate to the PCRF that the related media flow is allowed to use the same Allocation and Retention Priority as media flows which are assigned the same QCI in the PCRF belonging to other AF sessions for the same IP-CAN session that also contain the Priority-Sharing-Indicator AVP set to PRIORITY_SHARING_ENABLED. If the MCPTT-Preemption feature is supported, the AF may also include the Pre-emption-Capability AVP containing the suggested pre-emption capability value and the Pre-emption-Vulnerability AVP containing the suggested pre-emption vulnerability value within the Media-Component-Description AVP and include the Pre-emption-Control-Info AVP containing the pre-emption control information at the AAR command level to the PCRF for ARP decision and pre-emption control. Upon reception of this information, the PCRF shall behave as described in 3GPP TS 29.212 [8], subclauses 4.5.27 and 4a.5.17. For the handling of MCPTT sessions, see Annex A.13.

NOTE 1: Service data flow deactivation procedures will apply according to subclause 4.4.6.2.

NOTE 2: This enhancement avoids the risk that a bearer establishment request is rejected if the maximum number of active bearers is exceeded.

If the AF earlier has indicated a media flow priority sharing to the PCRF by setting the Priority-Sharing-Indicator AVP to PRIORITY_SHARING_ENABLED, the AF may include the Priority-Sharing-Indicator AVP set to PRIORITY_SHARING_DISABLED within the Media-Component-Description AVP in order to indicate to the PCRF that the related media flow shall not be part of the mechanism for sharing the Allocation and Retention Priority with other media flows any longer.
If this media flow was in priority sharing with other media flows the PCRF should readjust the Allocation and Retention Priority for the remaining services sharing priority as described in 3GPP TS 29.212 [8], subclauses 4.5.27 and4a.5.17 and handle the media flow excluded from priority sharing according to normal PCC/QoS rule provisioning procedures described in 3GPP TS 29.212 [8], subclauses 4.5.2 and 4a.5.2.

If the AF earlier has indicated media flow priority sharing to the PCRF by setting the Priority-Sharing-Indicator AVP to PRIORITY_SHARING_ENABLED for media flows and the AF indicates to remove one or more of the media flows in priority sharing with other media flows, the PCRF should readjust the Allocation and Retention Priority for the remaining services sharing priority as described in 3GPP TS 29.212 [8], subclauses 4.5.27 and 4a.5.17 and handle the media flow removed according to normal PCC/QoS rule provisioning procedures described in 3GPP TS 29.212 [8], subclauses 4.5.2 and 4a.5.2.

If the AF session being terminated corresponds to a session that included the Priority-Sharing-Indicator AVP set to PRIORITY_SHARING_ENABLED within the Media-Component Description AVP, if the related media flow(s) was in priority sharing with other media flows the PCRF should readjust the Allocation and Retention Priority for the remaining services sharing Allocation and Retention Priority as described in 3GPP TS 29.212 [8] , subclauses 4.5.27

and 4a.5.17 and handle the media flow removed according to normal PCC/QoS rule provisioning procedures described in 3GPP TS 29.212 [8], subclauses 4.5.2 and 4a.5.2.

4.4.9 Support for media component versioning

The support of the media component versioning is optional. When the MediaComponentVersioning feature is supported, the AF and the PCRF shall comply with the procedures specified in this subclause.

If required by operator policies, the AF shall assign a content version to the media component related to certain service and provide the PCRF within the Content-Version AVP as part of the Media-Component-Description AVP. Upon each media component modification, if the content version was assigned to a media component, the AF shall assign a new content version. In this case, all the content related to that media component shall be included. The content version shall be unique for the lifetime of the media component.

NOTE 1: The AF will include all the content of the media component in each media component modification in order to ensure that the media component is installed with the proper information regardless of the outcome of the bearer procedure related to previous interactions that are not reported to the PCRF yet.

If the PCRF receives the Content-Version AVP including an content version for certain media component, the PCRF will follow the procedures described in 3GPP TS 29.212 [8], subclause 4.5.28 and subclause 4a.5.18.

When the PCRF is notified about the outcome of the resource allocation related to one content version of a media component as described in subclause 4.5.28 or subclause 4a.5.18 in 3GPP TS 29.212 [8] and if the PCRF is required to notify the AF, the PCRF shall provide the content version of the media component within the Content-Version AVP corresponding to the value of content version of the PCC/QoS rule and the status of the media component within the Media-Component-Status AVP corresponding to the status of the PCC/QoS rule to the AF as part of the Flows AVP.

The PCRF shall include more than one Content-Version AVPs for the same media component within the Flows AVP in a RAR command if it has received multiple content versions as described in subclause 4.5.28 or subclause 4a.5.18 in 3GPP TS 29.212 [8].

NOTE 2: The AF will use the content version to identify the media component version that failed or succeed when multiple provisions of the same media component occur in a short period of time. How the AF handles such situations is not specified.

5 Rx protocol

5.1 Protocol support

The Rx interface in the present release is based on Rx and Gq protocols defined for Release 6 as specified in 3GPP TS 29.211 [7] and 3GPP TS 29.209 [5] respectively. However, to be able to separate the policy and charging rules function (PCRF) of the present release from the policy decision function (PDF) and charging rules function (CRF) of Release 6, the Rx application in the present release has an own vendor specific Diameter application.

The Rx application is defined as an IETF vendor specific Diameter application, where the vendor is 3GPP and the Application-ID for the Rx application in the present release is 16777236. The vendor identifier assigned by IANA to 3GPP (http://www.iana.org/assignments/enterprise-numbers) is 10415.

NOTE: A route entry can have a different destination based on the application identification AVP of the message. Therefore, Diameter agents (relay, proxy, redirection, translation agents) must be configured appropriately to identify the 3GPP Rx application within the Auth-Application-Id AVP in order to create suitable routeing tables.

Tthe Rx application identification shall be included in the Auth-Application-Id AVP.

With regard to the Diameter protocol defined over the Rx reference point, the PCRF acts as a Diameter server, in the sense that it is the network element that handles AF session authorization requests for a particular realm. The AF acts as the Diameter client, in the sense that is the network element requesting the authorization of resources for an AF session.

5.2 Initialization, maintenance and termination of connection and session

The initialization and maintenance of the connection between each AF and PCRF pair is defined by the underlying protocol. Establishment and maintenance of connections between Diameter nodes is described in IETF RFC 6733 [52].

After establishing the transport connection, the PCRF and the AF shall advertise the support of the Rx 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 Vendor-Specific-Application-Id AVP contained in 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 (IETF RFC 6733 [52]).

The termination of the Diameter user session is specified in IETF RFC 6733 [52] in clauses 8.4 and 8.5. The description of how to use of these termination procedures in the normal cases is embedded in the procedures description (clause 4.4).

5.3 Rx specific AVPs

5.3.0 General

Table 5.3.0.1 describes the Diameter AVPs defined for the Rx interface protocol, their AVP Code values, types, possible flag values, whether or not the AVP may be encrypted and which supported feature the AVP is applicable to. The Vendor-Id header of all AVPs defined in the present document shall be set to 3GPP (10415).

NOTE: Most of these AVPs have already been defined in 3GPP TS 29.209 [5] for Rel-6. Their definition is based on the one used for Rel-6 with some possible modifications to be applied to the Rel-7 protocols.

Table 5.3.0.1: Rx 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.**	**Applicability (Note 3)**
Abort-Cause	500	5.3.1	Enumerated	M,V	P			Y	
Access-Network-Charging-Address	501	5.3.2	Address	M,V	P			Y	
Access-Network-Charging-Identifier	502	5.3.3	Grouped	M,V	P			Y	
Access-Network-Charging-Identifier-Value	503	5.3.4	OctetString	M,V	P			Y	
Acceptable-Service-Info	526	5.3.24	Grouped	M,V	P			Y	
AF-Application-Identifier	504	5.3.5	OctetString	M,V	P			Y	
AF-Charging-Identifier	505	5.3.6	OctetString	M,V	P			Y	
AF-Requested-Data	551	5.3.50	Unsigned32	V	P		M	Y	
AF-Signalling-Protocol	529	5.3.26	Enumerated	V	P		M	Y	ProvAFsignalFlow
Application-Service-Provider-Identity	532	5.3.29	UTF8String	V	P		M	Y	SponsoredConnectivity
Pre-emption-Control-Info	553	5.3.51	Unsigned32	V	P		M	Y	MCPTT-Preemption
Codec-Data	524	5.3.7	OctetString	M,V	P			Y	
Content-Version	552	5.3.49	Unsigned64	V	P		M	Y	MediaComponentVersioning
Flow-Description	507	5.3.8	IPFilterRule	M,V	P			Y	
Flow-Number	509	5.3.9	Unsigned32	M,V	P			Y	
Flows	510	5.3.10	Grouped	M,V	P			Y	
Flow-Status	511	5.3.11	Enumerated	M,V	P			Y	
Flow-Usage	512	5.3.12	Enumerated	M,V	P			Y	
GCS-Identifier	538	5.3.36	OctetString	V	P		M	Y	GroupComService
IP-Domain-Id	537	5.3.35	OctetString	V	P		M	Y	
Max-Requested-Bandwidth-DL	515	5.3.14	Unsigned32	M,V	P			Y	
Max-Requested-Bandwidth-UL	516	5.3.15	Unsigned32	M,V	P			Y	
Max-Supported-Bandwidth-DL	543	5.3.41	Unsigned32	V	P		M	Y	E2EQOSMTSI
Max-Supported-Bandwidth-UL	544	5.3.42	Unsigned32	V	P		M	Y	E2EQOSMTSI
MCPTT-Identifier	547	5.3.45	OctetString	V	P		M	Y	MCPTT
Media-Component-Description	517	5.3.16	Grouped	M,V	P			Y	
Media-Component-Number	518	5.3.17	Unsigned32	M,V	P			Y	
Media-Component-Status	549	5.3.48	Unsigned32	V	P		M	Y	
Media-Sub-Component	519	5.3.18	Grouped	M,V	P			Y	
Media-Type	520	5.3.19	Enumerated	M,V	P			Y	
MPS-Identifier	528	5.3.30	OctetString	V	P		M	Y	Rel10
Min-Desired-Bandwidth-DL	545	5.3.43	Unsigned32	V	P		M		E2EQOSMTSI
Min-Desired-Bandwidth-UL	546	5.3.44	Unsigned32	V	P		M		E2EQOSMTSI
Min-Requested-Bandwidth-DL	534	5.3.32	Unsigned32	V	P		M	Y	Rel10
Min-Requested-Bandwidth-UL	535	5.3.33	Unsigned32	V	P		M	Y	Rel10
Priority-Sharing-Indicator	550	5.3.47	Enumerated	V	P		M	Y	PrioritySharing
RR-Bandwidth	521	5.3.20	Unsigned32	M,V	P			Y	
RS-Bandwidth	522	5.3.21	Unsigned32	M,V	P			Y	
Service-Authorization-Info	548	5.3.46	Unsigned32	V	P		M	Y	
Service-URN	525	5.3.23	OctetString	M,V	P			Y	
Service-Info-Status	527	5.3.25	Enumerated	M,V	P			Y	
Sharing-Key-DL	539	5.3.37	Unsigned32	V	P		M	Y	ResShare
Sharing-Key-UL	540	5.3.38	Unsigned32	V	P		M	Y	ResShare
Specific-Action	513	5.3.13	Enumerated	M,V	P			Y	
SIP-Forking-Indication	523	5.3.22	Enumerated	M,V	P			Y	
Sponsor-Identity	531	5.3.28	UTF8String	V	P		M	Y	SponsoredConnectivity
Sponsored-Connectivity-Data (NOTE 4)	530	5.3.27	Grouped	V	P		M	Y	SponsoredConnectivity SCTimeBasedUM
Sponsoring-Action	542	5.3.40	Enumerated	V	P		M	Y	SponsorChange
Required-Access-Info	536	5.3.34	Enumerated	V	P		M	Y	NetLoc
Rx-Request-Type	533	5.3.31	Enumerated	V	P		M	Y	

Retry-Interval	541	5.3.39	Unsigned32	V	P		M	Y	DeferredService
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 IETF RFC 6733 [52].									
NOTE 2: The value types are defined in IETF RFC 6733 [52].									
NOTE 3: AVPs marked with a supported feature (e.g. "ProvAFsignalFlow", "SponsoredConnectivity", "Rel10" or "NetLoc") are applicable as described in subclause 5.4.1									
NOTE 4: Volume Usage monitoring control functionality is applicable for SponsoredConnectivity supported feature. Time Based Usage monitoring control is applicable for SCTimeBasedUM supported feature.									

5.3.1 Abort-Cause AVP

The Abort-Cause AVP (AVP code 500) is of type Enumerated, and determines the cause of an abort session request (ASR) or of a RAR indicating a 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 GPRS the bearer refers to the PDP Context.

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. GGSN for GPRS).

PS_TO_CS_HANDOVER (3)

This value is used when the bearer has been deactivated due to PS to CS handover.

SPONSORED_DATA_CONNECTIVITY_ DISALLOWED (4)

This value is used in the ASR when the PCRF needs to initiates the AF session termination due to the operator policy (e.g. disallowing the UE accessing the sponsored data connectivity in the roaming case).

5.3.2 Access-Network-Charging-Address AVP

The Access-Network-Charging-Address AVP (AVP code 501) is of type Address, and it indicates the IP Address of the network entity within the access network performing charging (e.g. the GGSN IP address). The Access-Network-Charging-Address AVP should not be forwarded over an inter-operator interface.

5.3.3 Access-Network-Charging-Identifier AVP

The Access-Network-Charging-Identifier AVP (AVP code 502) 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 can be sent from the PCRF to the AF. The AF may use this information for charging correlation with session layer.

AVP Format:

```
Access-Network-Charging-Identifier ::= < AVP Header: 502 >
                     { Access-Network-Charging-Identifier-Value}
                    *[ Flows ]
```

5.3.4 Access-Network-Charging-Identifier-Value AVP

The Access-Network-Charging-Identifier-Value AVP (AVP code 503) is of type OctetString, and contains a charging identifier (e.g. GCID).

5.3.5 AF-Application-Identifier AVP

The AF-Application-identifier AVP (AVP code 504) 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 PCRF 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 authorization at the Gx interface is selected. The AF-Application-Identifier may be used also to complete the QoS authorization with application specific default settings in the PCRF if the AF does not provide full Session-Component-Description information.

The AF-Application-Identifier AVP may also be used to trigger the PCRF to indicate to the PCEF/TDF to perform the application detection based on the operator's policy.

5.3.6 AF-Charging-Identifier AVP

The AF-Charging-Identifier AVP (AVP code 505) is of type OctetString, contains the AF Charging Identifier that is sent by the AF. This information may be used for charging correlation with bearer layer.

5.3.7 Codec-Data AVP

The Codec-Data AVP (AVP code 524) is of type OctetString.

The Codec-Data AVP shall contain codec related information known at the AF. This information shall be encoded as follows:

- The first line of the value of the Codec-Data AVP shall consist of either the word "uplink" or the word "downlink" (in ASCII, without quotes) followed by a new-line character. The semantics of these words are the following:
  - "uplink" indicates that the SDP was received from the UE and sent to the network.
  - "downlink" indicates that the SDP was received from the network and sent to the UE.

NOTE 1: The first line indicates the direction of the source of the SDP used to derive the information. The majority of the information within the Codec-Data AVP indicating "downlink" describes properties, for instance receiver capabilities, of the sender of the SDP, the network in this case and is therefore applicable for IP flows in the uplink direction. Similarly, the majority of the information within the Codec-Data AVP indicating "uplink" describes properties, for instance receiver capabilities, of the sender of the SDP, the UE in this case and is therefore applicable for IP flows in the downlink direction.

- The second line of the value of the Codec-Data AVP shall consist of either the word "offer" or the word "answer", or the word "description" (in ASCII, without quotes) followed by a new-line character. The semantics of these words are the following:
  - "offer" indicates that SDP lines from an SDP offer according to RFC 3264 [18] are being provisioned in the Codec-Data AVP;
  - "answer" indicates that SDP lines from an SDP answer according to RFC 3264 [18] are being provisioned in the Codec-Data AVP;
  - "description" indicates that SDP lines from a SDP session description in a scenario where the offer-answer mechanism of RFC 3264 [18] is not being applied are being provisioned in the Codec-Data AVP. For instance, SDP from an RTSP "Describe" reply may be provisioned.
- The rest of the value shall consist of SDP line(s) in ASCII encoding separated by new-line characters, as specified in IETF RFC 4566 [13]. The first of these line(s) shall be an "m" line. The remaining lines shall be any

available SDP "a" and "b" lines related to that "m" line. However, to avoid duplication of information, the SDP "a=sendrecv", "a=recvonly ", "a=sendonly", "a=inactive", "a=bw-info", "b:AS", "b:RS" and "b:RR" lines do not need to be included.

NOTE 2: For backwards compatibility, it is expected that the codec algorithms in the PCRF described in 3GPP TS 29.213 [9] allow the introduction of new SDP lines without rejecting the request when Codec-Data AVP is provided as part of the Media-Component-Description AVP. The QoS derivation in that case will not take the new SDP line(s) into account.

5.3.8 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). The direction "in" refers to uplink IP flows, and the direction "out" refers to downlink IP flows.
- Source and destination IP address (possibly masked).
- Protocol.
- Source and destination port.

The IPFilterRule type shall be used over Rx interface with the following restrictions:

- The Source Port may be omitted to indicate that any source port is allowed. Lists or ranges shall not be used.
- 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.

NOTE: For TCP protocol, destination port can also be omitted.

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.

For the Rx interface, the Flow description AVP shall be used to describe a single IP flow.

5.3.9 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 B.

5.3.10 Flows AVP

The Flows AVP (AVP code 510) is of type Grouped, and it indicates IP flows via their flow identifiers.

When reporting an out of credit condition, the Final-Unit-Action AVP indicates the termination action applied to the impacted flows.

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

When reporting a resource allocation failure related to the modification of session information, the Media-Component-Status AVP may be included to report the status of the PCC/QoS rules related to the media component.

The Content-Version AVP(s) shall be included if it was included in the Media-Component-Description AVP when the corresponding media component was provisioned.

AVP Format:

```
Flows::= < AVP Header: 510 >
```

```
 {Media-Component-Number}
*[Flow-Number]
*[ Content-Version ]
 [Final-Unit-Action]
 [Media-Component-Status]
*[AVP]
```

5.3.11 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).

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)

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.

NOTE 1: The interpretation of values for the RTCP flows in the Rx interface is described within the procedures in clause 4.4.3.

NOTE 2: The interpretation of values for IMS flows when SIP Forking is supported is described within the procedures in Annex A.3.1.

5.3.12 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.

AF_SIGNALLING (2)

This value is used to indicate that the IP flow is used to transport AF Signalling Protocols (e.g. SIP/SDP).

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.

5.3.13 Specific-Action AVP

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

Within a PCRF 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 any 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 at this time.

For one time specific actions, as identified in the value descriptions below, the AF may also provide the Specific-Action AVP with the applicable one-time-specific-action value(s) in subsequent AA-Requests. Non-one-time-specific-action value(s) may only be provided in the initial AA-Request and shall then be applicable for the entire lifetime of the Rx session.

NOTE 1: One time specific actions are reported once the required action is fulfilled and are not reported again unless the AF sends a new request.

NOTE 2: Unless otherwise stated in the definition of the specific action value, when the AF requests specific actions in the initial AA-Request, the PCRF reports that action whenever new related information is available during the lifetime of the Rx session.

NOTE 2a: Whether the PCRF decides to report INDICATION_OF_RELEASE_OF_BEARER (4) or INDICATION_OF_FAILED_RESOURCES_ALLOCATION (9) upon receipt of a bearer failure from the PCEF is left to the implementation.

The following values are defined:

Void (0)

CHARGING_CORRELATION_EXCHANGE (1)

Within a RAR, this value shall be used when the server reports the access network charging identifier to the AF. The Access-Network-Charging-Identifier AVP shall be included within the request. In the AAR, this value indicates that the AF requests the server to provide the access network charging identifier to the AF for each authorized flow, when the access network charging identifier becomes known at the PCRF.

INDICATION_OF_LOSS_OF_BEARER (2)

Within a RAR, this value shall be used when the server reports a loss of a bearer (in the case of GPRS PDP context bandwidth modification to 0 kbit for GBR bearers) to the AF. The SDFs that are deactivated as a consequence of this loss of bearer shall be provided within the Flows AVP. 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 (in the case of 3GPP-GPRS or 3GPP-EPS when PGW interoperates with a Gn/Gp SGSN, PDP context bandwidth modification from 0 kbit to another value for GBR bearers) to the AF. The SDFs that are re-activated as a consequence of the recovery of bearer shall be provided within the Flows AVP. 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)

Within a RAR, this value shall be used when the server reports the release of a bearer (e.g. PDP context removal for 3GPP-GPRS or bearer/PDP context removal for 3GPP-EPS) to the AF. The SDFs that are deactivated as a consequence of this release of bearer shall be provided within the Flows AVP. In the AAR, this value indicates that the AF requests the server to provide a notification at the removal of a bearer. The content version corresponding to the affected media component may be provided in the Content-Version AVP included within the Flows AVP.

Void (5)

IP-CAN_CHANGE (6)

This value shall be used in RAR command by the PCRF to indicate a change in the IP-CAN type or RAT type (if applicable). When used in an AAR command, this value indicates that the AF is requesting subscription to IP-CAN change and RAT change notification. When used in RAR it indicates that the PCRF generated the request because of an IP-CAN or RAT change. IP-CAN-Type AVP, RAT-Type AVP (if applicable) ,AN-Trusted AVP

(if applicable) and AN-GW-Address AVP (if applicable) shall be provided in the same request with the new/valid value(s).

If an IP-CAN type or RAT type change is due to IP flow mobility and a subset of the flows within the AF session is affected, the affected service data flows shall be provided in the same request.

INDICATION_OF_OUT_OF_CREDIT (7)

Within a RAR, this value shall be used when the PCRF reports to the AF that SDFs have run out of credit, and that the termination action indicated by the corresponding Final-Unit-Action AVP applies (3GPP TS 32.240 [23] and 3GPP TS 32.299 [24]. The SDFs that are impacted as a consequence of the out of credit condition shall be provided within the Flows AVP. In the AAR, this value indicates that the AF requests the PCRF to provide a notification of SDFs for which credit is no longer available. Applicable to functionality introduced with the Rel8 feature as described in clause 5.4.1.

INDICATION_OF_SUCCESSFUL_RESOURCES_ALLOCATION (8)

Within a RAR, this value shall be used by the PCRF to indicate that the resources requested for particular service information have been successfully allocated. The SDFs corresponding to the resources successfully allocated shall be provided within the Flows AVP and the content version within the Content-Version AVP as included when the corresponding media component was provisioned.

In the AAR, this value indicates that the AF requests the PCRF to provide a notification when the resources associated to the corresponding service information have been allocated.

Applicable to functionality introduced with the Rel8 feature as described in clause 5.4.1.

NOTE 3: This value applies to applications for which the successful resource allocation notification is required for their operation since subscription to this value impacts the resource allocation signalling overhead towards the PCEF/BBERF.

INDICATION_OF_FAILED_RESOURCES_ALLOCATION (9)

Within a RAR, this value shall be used by the PCRF to indicate that the resources requested for a particular service information cannot be successfully allocated. The SDFs corresponding to the resources that could not be allocated shall be provided within the Flows AVP. In case of session modification failure, the status of the related service information may be reported in the Media-Component-Status AVP included within the Flows AVP and the content version within the Content-Version AVP as included when the corresponding media component was provisioned.

In the AAR, this value indicates that the AF requests the PCRF to provide a notification when the resources associated to the corresponding service information cannot be allocated. Applicable to functionality introduced with the Rel8 feature as described in clause 5.4.1.

NOTE 4: This value applies to applications for which the unsuccessful resource allocation notification is required for their operation since subscription to this value impacts the resource allocation signalling overhead towards the PCEF/BBERF.

INDICATION_OF_LIMITED_PCC_DEPLOYMENT (10)

Within a RAR, this value shall be used when the PCRF reports the limited PCC deployment (i.e. dynamically allocated resources are not applicable) as specified at Annex K and Annex L in 3GPP TS 23.203 [2] to the AF. In the AAR, this value indicates that the AF requests the PCRF to provide a notification for the limited PCC deployment. Applicable to functionality introduced with the Rel8 feature as described in clause 5.4.1.

USAGE_REPORT (11)

In the RA-Request (RAR), this value shall be used by the PCRF to report accumulated usage volume and/or time of usage when the usage threshold provided by the AF has been reached.

In the AA-Request (AAR), this value indicates that the AF requests PCRF to report accumulated usage volume and /or time of usage when it reaches the threshold.

Applicable to functionality introduced with the SponsoredConnectivity feature for volume usage reporting and with SCTimeBased UM feature for time usage reporting as described in clause 5.4.1.

ACCESS_NETWORK_INFO_REPORT (12)

In the RA-Request (RAR), this value shall be used by the PCRF to report access network information (i.e.user location and/or user timezone information) when the PCRF receiving an Access Network Information report corresponding to the AF session from the PCEF/BBERF.

In the AA-Request (AAR), this value indicates that the AF requests PCRF to report one time access network information when the PCRF receives the first Access Network Information report corresponding to the AF session from the PCEF/BBERF after the AF request for the access network information. The required access information is provided within the Required-Access-Info AVP. Applicable to functionality introduced with the NetLoc feature as described in clause 5.4.1.

The Specific-Action AVP with this value indicates a one time specific action.

INDICATION_OF_RECOVERY_FROM_LIMITED_PCC_DEPLOYMENT (13)

Within a RAR, this value shall be used when the PCRF reports the recovery from limited PCC deployment (i.e. the UE moves from the VPLMN to the HPLMN as specified at Annex K in 3GPP TS 23.203 [2]) to the AF. In the AAR, this value indicates that the AF requests the PCRF to provide a notification for the recovery from limited PCC deployment. Applicable to functionality introduced with the Rel8 feature as described in clause 5.4.1.

NOTE 5: This value is optional and only applicable to the scenario where PCC is deployed in the HPLMN but not in the VPLMN and dynamic policy provisioning only occurs in the home routed roaming cases if no BBERF is employed.

INDICATION_OF_ACCESS_NETWORK_INFO_REPORTING_FAILURE (14)

In the RAR, this value shall be used when the PCRF reports the access network information reporting failure. When applicable, the NetLoc-Access-Support AVP may be provided as well to indicate the reason for the access network information reporting failure. This specific action does not require to be provisioned by the AF. Applicable to functionality introduced with the NetLoc feature as described in clause 5.4.1.

INDICATION_OF_TRANSFER_POLICY_EXPIRED (15)

In the RAR, this value shall be used when the PCRF determines that the transfer policy has expired. This specific action does not require to be provisioned by the AF.

PLMN_CHANGE (16)

In the AA-Request (AAR), this value indicates that the AF requests PCRF to report changes of PLMN. In the RA-Request (RAR), this value shall be used by the PCRF to indicate that there was a change of PLMN. 3GPP-SGSN-MCC-MNC AVP shall be provided in the same RAR command with the new value. Applicable to functionality introduced with the PLMNInfo feature as described in subclause 5.4.1.

5.3.14 Max-Requested-Bandwidth-DL AVP

The Max-Requested-Bandwidth-DL AVP (AVP code 515) is of type Unsigned32, and it indicates the maximum 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.

When provided in an AA-Request, it indicates the maximum requested bandwidth. When provided in an AA-Answer, it indicates the maximum bandwidth acceptable by PCRF.

5.3.15 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.

When provided in an AA-Request, it indicates the maximum requested bandwidth. When provided in an AA-Answer, it indicates the maximum bandwidth acceptable by PCRF.

5.3.16 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 or the AF signalling information. The service information may be based on the SDI exchanged between the AF and the AF session client in the UE. The information may be used by the PCRF to determine authorized QoS and IP flow classifiers for bearer authorization and PCC 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 by the AF, 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.

Reservation-Priority provided within the Media-Component-Description AVP in the request from the AF applies to all those IP flows within the media component and describes the relative importance of the IP flow as compared to other IP flows. The PCRF may use this value to implement priority based admission. If the Reservation-Priority AVP is not specified the IP flow priority is DEFAULT (0).

Each Media-Component-Description AVP shall contain either zero, or one, or two Codec-Data AVPs. In the case of conflicts, information contained in other AVPs either within this Media-Component-Description AVP, or within the corresponding Media-Component-Description AVP in a previous message, shall take precedence over information within the Codec-Data AVP(s). The AF shall provision all the available information in other applicable AVPs in addition to the information in the Codec-Data AVP, if such other AVPs are specified.

If the SDP offer-answer procedures of IETF RFC 3264 [18] are applicable for the session negotiation between the two ends taking part in the communication (e.g. for IMS), the following applies:

- The AF shall provision information derived from an SDP answer and shall also provision information derived from the corresponding SDP offer.

- If the Media-Component-Description AVP contains two Codec-Data AVPs, one of them shall represent an SDP offer and the other one the corresponding SDP answer.

- If the Media-Component-Description AVP contains one Codec-Data AVP, and this AVP represents an SDP offer, the AF shall provision the corresponding SDP answer information in a Codec-Data AVP within a subsequent Rx message.

NOTE 1: Some SDP parameters for the same codec in the SDP offer and answer are independent of each other and refer to IP flows in opposite directions, for instance some MIME parameters conveyed within "a=fmtp" SDP lines and the packetization time within the "a=ptime" line. Other parameters within the SDP answer take precedence over corresponding parameters within the SDP offer.

If SDP is applied without using the offer-answer procedures, zero or one Codec-Data AVP shall be provisioned.

Sharing-Key-DL AVP and/or Sharing-Key-UL AVP provided within the Media-Component-Description AVP indicates that the media components that include the same value of the Sharing-Key-UL AVP and/or Sharing-Key-DL AVP may share resources in the related direction.

NOTE 2: RTCP traffic is not subject to resource sharing.

The Content-Version AVP may be included in order to indicate the content version of a media component.

The Priority-Sharing-Indicator AVP may be included to indicate that the media component can use the same Allocation and Retention Priority as media flows which are assigned the same QCI in the PCRF belonging to other AF sessions for the same IP-CAN session that also contain the Priority-Sharing-Indicator AVP.

The Pre-emption-Capability AVP and Pre-emption-Vulnerability AVP may be included together with Priority-Sharing-Indicator AVP for PCRF Allocation and Retention Priority decision and pre-emption control.

The PCRF may provide the Media-Component-Description AVP(s) within the Acceptable-Service-Info AVP in the AA-Answer command if the service information received from the AF is rejected. For this usage, the Media-Component-Description AVP shall only include the appropriate Media-Component-Number AVP and the Max-Requested-Bandwidth-UL and/or Max-Requested-Bandwidth-DL AVPs indicating the maximum acceptable bandwidth.

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 ]
                             [ Max-Supported-Bandwidth-UL ]
                             [ Max-Supported-Bandwidth-DL ]
                             [ Min-Desired-Bandwidth-UL ]
                             [ Min-Desired-Bandwidth-DL ]
                             [ Min-Requested-Bandwidth-UL ]
                             [ Min-Requested-Bandwidth-DL ]
                             [ Flow-Status ]
                             [ Priority-Sharing-Indicator ]
                             [ Pre-emption-Capability ]
                             [ Pre-emption-Vulnerability ]
                             [ Reservation-Priority ]
                             [ RS-Bandwidth ]
                             [ RR-Bandwidth ]
                            *[ Codec-Data ]
                             [ Sharing-Key-DL ]
                             [ Sharing-Key-UL ]
                             [ Content-Version ]
                            *[ AVP ]
```

5.3.17 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 B.

When this AVP refers to AF signalling, this is indicated by using the value 0 according to the rules in Annex B.

5.3.18 Media-Sub-Component AVP

The Media-Sub-Component AVP (AVP code 519) is of type Grouped, and it contains the requested bitrate and filters for the set of IP flows identified by their common Flow-Identifier. The Flow-Identifier is defined in Annex B.

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. The AF may also include the ToS-Traffic-Class AVP for requesting Type of Service or Traffic Class (for IPv4 and IPv6 respectively) based packet filter for the related flow.

The AF-Signalling-Protocol AVP may be included only if the Flow-Usage AVP has a value of ‘AF_SIGNALLING’.

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 ]
                    [ AF-Signalling-Protocol ]
                    [ ToS-Traffic-Class ]
                   *[ AVP ]
```

5.3.19 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 RFC 4566 [13]. The following values are defined:

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

5.3.20 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 IETF RFC 3556 [11]. The bandwidth contains all the overhead coming from the IP-layer and the layers above, i.e. IP, UDP and RTCP.

5.3.21 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 [11]. The bandwidth contains all the overhead coming from the IP-layer and the layers above, i.e. IP, UDP and RTCP.

5.3.22 SIP-Forking-Indication AVP

The SIP-Forking-Indication 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.

5.3.23 Service-URN AVP

The Service-URN AVP (AVP code 525) is of type OctetString, and it indicates that an AF session is used for emergency traffic.

It contains values of the service URN including subservices, as defined in [21] or registered at IANA. The string "urn:service:" in the beginning of the URN shall be omitted in the AVP and all subsequent text shall be included. Examples of valid values of the AVP are "sos", "sos.fire", "sos.police" and "sos.ambulance".

5.3.24 Acceptable-Service-Info AVP

The Acceptable-Service-Info AVP (AVP code 526) is of type Grouped, and contains the maximum bandwidth for an AF session and/or for specific media components that will be authorized by the PCRF. The Max-Requested-Bandwidth-DL AVP and Max-Requested-Bandwidth-UL AVP directly within the Acceptable-Service-Info AVP indicate the acceptable bandwidth for the entire AF session. The Max-Requested-Bandwidth-DL AVP and Max-Requested-Bandwidth-UL AVP within a Media-Component-Description AVP included in the Acceptable-Service-Info AVP indicate the acceptable bandwidth for the corresponding media component.

If the acceptable bandwidth applies to one or more media components, only the Media-Component-Description AVP will be provided. If the acceptable bandwidth applies to the whole AF session, only the Max-Requested-Bandwidth-DL AVP and Max-Requested-Bandwidth-UL AVP will be included.

```
Acceptable-Service-Info::= < AVP Header: 526 >
                         *[ Media-Component-Description]
                          [ Max-Requested-Bandwidth-DL ]
                          [ Max-Requested-Bandwidth-UL ]
                         *[ AVP ]
```

5.3.25 Service-Info-Status-AVP

The Service-Info-Status AVP (AVP code 527) is of type Enumerated, and indicates the status of the service information that the AF is providing to the PCRF. If the Service-Info-Status AVP is not provided in the AA request, the value FINAL SERVICE INFORMATION shall be assumed.

FINAL SERVICE INFORMATION (0)

This value is used to indicate that the service has been fully negotiated between the two ends and service information provided is the result of that negotiation.

PRELIMINARY SERVICE INFORMATION (1)

This value is used to indicate that the service information that the AF has provided to the PCRF is preliminary and needs to be further negotiated between the two ends (e.g. for IMS when the service information is sent based on the SDP offer).

5.3.26 AF-Signalling-Protocol-AVP

The AF-Signalling-Protocol AVP (AVP code 529) is of type Enumerated, and indicates the protocol used for signalling between the UE and the AF. If the AF-Signalling-Protocol AVP is not provided in the AA-Request, the value NO_INFORMATION shall be assumed.

NO_INFORMATION (0)

This value is used to indicate that no information about the AF signalling protocol is being provided.

SIP (1)

This value is used to indicate that the signalling protocol is Session Initiation Protocol.

5.3.27 Sponsored-Connectivity-Data AVP

The Sponsored-Connectivity-Data AVP (AVP code 530) is of type Grouped, and contains the data associated with the sponsored data connectivity.

The Sponsor-Identity AVP identifies the sponsor. It shall be included by the AF in the Sponsored-Connectivity-Data AVP except for the case of disabling sponsored data connectivity.

The Application-Service-Provider-Identity AVP identifies the application service provider. It shall be included by the AF in the Sponsored-Connectivity-Data AVP except for the case of disabling sponsored data connectivity.

The Granted-Service-Unit AVP shall be used by the AF to provide usage threshold to the PCRF if the volume and/or time of traffic allowed during the sponsored data connectivity is to be monitored.

The Used-Service-Unit AVP shall be used by the PCRF to provide the measured usage to the AF. Reporting shall be done, as requested by the AF, in CC-Total-Octets, CC-Input-Octets, CC-Output-Octets or CC-Time of the Used-Service-Unit AVP.

Sponsoring-Action AVP shall be used by the AF to provide the indication to the PCRF if sponsored data connectivity is to be enabled or disabled.

AVP format:

```
Sponsored-Connectivity-Data::= < AVP Header: 530 >
                              [ Sponsor-Identity ]
                              [ Application-Service-Provider-Identity ]
                              [ Granted-Service-Unit ]
                              [ Used-Service-Unit ]
                              [ Sponsoring-Action ]
                             *[ AVP ]
```

5.3.28 Sponsor-Identity AVP

The Sponsor-Identity AVP (AVP code 531) is of type UTF8String and is used for sponsored data connectivity purposes as an identifier of the sponsor.

5.3.29 Application-Service-Provider-Identity AVP

The Application-Service-Provider-Identity AVP (AVP code 532) is of type UTF8String and is used for sponsored data connectivity purposes as an identifier of the application service provider.

5.3.30 MPS-Identifier AVP

The MPS-Identifier AVP (AVP code 528) is of type OctetString, and it indicates that an AF session relates to an MPS session. It contains the national variant for MPS service name (e.g., NGN GETS).

5.3.31 Rx-Request-Type AVP

The Rx-Request-Type AVP (AVP code 533) is of type Enumerated, and contains the reason for sending the AA-Request message.

The following values are defined:

INITIAL_REQUEST (0)

An initial request is used to initiate an Rx session and contains information that is relevant to initiation.

UPDATE_REQUEST (1)

An update request is used to update an existing Rx session.

PCSCF_RESTORATION (2)

A P-CSCF Restoration is requested. This value is only applicable to the PCSCF-Restoration-Enhancement feature defined in clause 5.4.1.

5.3.32 Min-Requested-Bandwidth-DL AVP

The Min-Requested-Bandwidth-DL AVP (AVP code 534) is of type Unsigned32, and it indicates the minimum 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, TCP, UDP, HTTP, RTP and RTP payload.

When provided in an AA-Request, it indicates the minimum requested bandwidth.

5.3.33 Min-Requested-Bandwidth-UL AVP

The Min-Requested-Bandwidth-UL AVP (AVP code 535) is of type Unsigned32, and it indicates the minimum 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, TCP, UDP, HTTP, RTP and RTP payload.

When provided in an AA-Request, it indicates the minimum requested bandwidth.

5.3.34 Required-Access-Info AVP

The Required-Access-Info AVP (AVP code 536) is of type Enumerated, and contains the access network information required for that AF session.

The following values are defined:

USER_LOCATION (0)

Indicates that the user location information shall be reported, the PCRF shall report the user location information within the 3GPP-User-Location-Info AVP (if available), the serving PLMN identifier within the 3GPP-SGSN-MCC-MNC AVP (if available), the user location information within the TWAN-Identifier (if available) , UE-Local-IP-Address AVP (if available) , UDP-Source-Port AVP (if available), TCP-Source-Port AVP (if available) and User-Location-Info-Time AVP (if available).

MS_TIME_ZONE (1)

Indicates that the user timezone information shall be reported, the PCRF shall report the user timezone information within the 3GPP-MS-TimeZone AVP.

5.3.35 IP-Domain-Id AVP

The IP-Domain-Id AVP (AVP code 537) is of type (OctetString), and indicates the domain information which assists session binding.

5.3.36 GCS-Identifier AVP

The GCS-Identifier AVP (AVP code 538) is of type OctetString, and it indicates that an AF session relates to a Group Communication session that requires prioritization.The values that identify the Group Communication session are not specified.

5.3.37 Sharing-Key-DL AVP

The Sharing-Key-DL AVP (AVP code 539) is of type Unsigned32 and is used to identify what media components may share resource in the downlink direction.

The Sharing-Key-DL AVP shall be used as follows:

- If resource sharing applies between media components across AF sessions for the same user, the same value of the Sharing-Key-DL AVP shall be used;
- If resource sharing does not apply between media components across AF sessions for the same user, a different value of the Sharing-Key-DL AVP shall be used for each media component.

5.3.38 Sharing-Key-UL AVP

The Sharing-Key-UL AVP (AVP code 540) is of type Unsigned32 and is used to identify what media components may share resource in the uplink direction.

The Sharing-Key-UL AVP shall be used as follows:

- If resource sharing applies between media components across AF sessions for the same user, the same value of the Sharing-Key-UL AVP shall be used;

- If resource sharing does not apply between media components across AF sessions for the same user, a different value of the Sharing-Key-UL AVP shall be used for each media component.

5.3.39 Retry-Interval AVP

The Retry-Interval AVP (AVP code 541) is of type Unsigned32, and it indicates a time interval in seconds to wait until which the AF retries to send the same service information to the PCRF (for the same IP-CAN session) when the service information is temporarily rejected by the PCRF (e.g. due to the detected congestion status of the cell the user is located in).

5.3.40 Sponsoring-Action AVP

The Sponsoring-Action AVP (AVP code 542) is of type Enumerated, and contains the indication whether to enable or disable/not enable sponsored data connectivity.

The following values are defined:

DISABLE_SPONSORING (0)

Disable sponsored data connectivity or not enable sponsored data connectivity

ENABLE_SPONSORING (1)

Enable sponsored data connectivity.

NOTE: The use of value DISABLE_SPONSORING (0) to "not enable" sponsored data connectivity is used at initial provisioning of session information to provide sponsor information but not enable it at that point in time and to "disable" sponsored data connectivity is used at modification of session information when disabling sponsored data connectivity previously enabled.

5.3.41 Max-Supported-Bandwidth-DL AVP

The Max-Supported-Bandwidth-DL AVP (AVP code 543) is of type Unsigned32, and it indicates the maximum supported bandwidth in bits per second for a downlink IP flow as defined in 3GPP TS 26.114 [41]. The bandwidth contains all the overhead coming from the IP-layer and the layers above, e.g. IP, UDP, RTP and RTP payload.

5.3.42 Max-Supported-Bandwidth-UL AVP

The Max-Supported-Bandwidth-UL AVP (AVP code 544 is of type Unsigned32, and it indicates the maximum supported bandwidth in bits per second for an uplink IP flow as defined in 3GPP TS 26.114 [41]. The bandwidth contains all the overhead coming from the IP-layer and the layers above, e.g. IP, UDP, RTP and RTP payload.

5.3.43 Min-Desired-Bandwidth-DL AVP

The Min-Desired-Bandwidth-DL AVP (AVP code 545) is of type Unsigned32, and it indicates the minimum desired bandwidth in bits per second for a downlink IP flow as defined in 3GPP TS 26.114 [41]. The bandwidth contains all the overhead coming from the IP-layer and the layers above, e.g. IP, UDP, RTP and RTP payload.

5.3.44 Min-Desired-Bandwidth-UL AVP

The Min-Desired-Bandwidth-DL AVP (AVP code 546) is of type Unsigned32, and it indicates the minimum desired bandwidth in bits per second for an uplink IP flow as defined in 3GPP TS 26.114 [41]. The bandwidth contains all the overhead coming from the IP-layer and the layers above, e.g. IP, UDP, RTP and RTP payload.

5.3.45 MCPTT-Identifier AVP

The MCPTT-Identifier AVP (AVP code 547) is of type OctetString, and it includes either one of the namespace values used for MCPTT (see draft-holmberg-dispatch-mcptt-rp-namespace [45]) and it may include the name of the MCPTT service provider.

5.3.46 Service-Authorization-Info AVP

The Service-Authorization-Info AVP (AVP code 548) is of type Unsigned32, it shall contain a bit mask and indicatethe result of the authorization for the service request from the AF. The bit 0 shall be the least significant bit. For example, to get the value of bit 0, a bit mask of 0x0001 should be used. The meaning of the bits shall be as defined below:

Table 5.3.46: Service-Authorization-Info

Bit	Name	Description
0	The transfer policy is known/unknown.	This bit, when set, indicates that the transfer policy is unknown.
1	The transfer policy has expired/has not expired	This bit, when set, indicates that the transfer policy has expired.
2	The time window of the transfer policy has occurred/has not yet occurred	This bit, when set, indicates that the time window of the transfer policy has not yet occurred.

5.3.47 Priority-Sharing-Indicator AVP

The Priority-Sharing-Indicator AVP (AVP code 550) is of type Enumerated and is used to indicate that the related media component can use the same Allocation and Retention Priority as media component(s) which are assigned the same QCI in the PCRF belonging to other AF sessions for the same IP-CAN session that also contain the Priority-Sharing-Indicator AVP set to PRIORITY_SHARING_ENABLED.

The following values are defined:

PRIORITY_SHARING_ENABLED (0)

This value indicates that the related media component is allowed to share the Allocation and Retention Priority with media components belonging to other AF sessions that have also indicated that priority sharing is enabled.

PRIORITY_SHARING_DISABLED (1)

This value indicates that the related media component is not allowed to share the Allocation and Retention Priority with media components belonging to other AF sessions. This is the default value applicable if this AVP is not supplied.

5.3.48 Media-Component-Status AVP

The Media-Component-Status AVP (AVP code 549) is of type Unsigned32, and it describes the status of the PCC/QoS rule(s) related to a media component.

The following values are defined in this specification:

0 (ACTIVE):

This value shall be used to indicate that the PCC/QoS rule(s) related to certain media component are active.

1 (INACTIVE):

This value shall be used to indicate that the PCC/QoS rule(s) related to certain media component are inactive. This is the default value applicable if this AVP is not supplied.

NOTE: It is assumed that the AF considers the PCC/QoS rule(s) related to the media component(s) for which the Media-Component-Status AVP(s) are not received as inactive when the Specific-Action AVP set to INDICATION_OF_FAILED_RESOURCES_ALLOCATION (9) is received.

5.3.49 Content-Version AVP

The Content-Version AVP (AVP code 552) is of type Unsigned64, and it indicates the version of some content, e.g. of the content of a media component included within the Media-Component-Description AVP. The content version shall be unique for the content and for the lifetime of that content.

NOTE: The method of assigning content versions within the Content-Version AVPs is implementation specific. Example implementations are a monotonically increasing number or a value based on a timestamp.

5.3.50 AF-Requested-Data AVP

The AF-Requested-Data AVP (AVP code 551) is of type Unsigned32 and indicates the information that the AF requested to be exposed, it shall contain a bit mask. The bit 0 shall be the least significant bit. For example, to get the value of bit 0, a bit mask of 0x0001 should be used. The meaning of the bits shall be as defined below:

Table 5.3.50.1: AF-Requested-Data

Bit	Name	Description
0	EPC-level identities required	This bit, when set, indicates that the AF requests the PCRF to provide the EPC-level identities (MSISDN, IMSI, IMEI(SV)) available for that IP-CAN session.

5.3.51 Pre-emption-Control-Info AVP

The Pre-emption-Control-Info (AVP code 553) is of type Unsigned32, it shall contain a bit mask and indicate that how the PCRF to perform pre-emption among multiple potential media flow candidates of same priority. Pre-emption-Control-Info AVP is provided at the AAR command level and the latest provided value within the Pre-emption-Control-Info AVP shall be applied to all potential media flow candidates.The bit 0 shall be the least significant bit. For example, to get the value of bit 0, a bit mask of 0x0001 should be used. The meaning of the bits shall be as defined below:

The following values are defined:

Table 5.3.z: Pre-emption-Control-Info

Bit	Name	Description
0	Most recent added flow is pre-empted/not pre-empted.	This bit, when set, indicates that the most recent added flow is pre-empted.
1	Least recent added flow is pre-empted/not pre-empted	This bit, when set, indicates that the least recent added flow is pre-empted.
2	Highest bandwidth flow is pre-empted/not pre-empted	This bit, when set, indicates that the highest bandwidth flow is pre-empted.

5.4 Rx re-used AVPs

5.4.0 General

Table 5.4.0.1 lists the Diameter AVPs re-used by the Rx reference point from existing Diameter Applications, including a reference to their respective specifications and when needed, a short description of their usage within the Rx reference point. Other AVPs from existing Diameter Applications, except for the AVPs from Diameter Base Protocol, do not need to be supported. The AVPs from Diameter Base Protocol are not included in table 5.4.0.1, but they are re-used for the Rx protocol. Unless otherwise stated, re-used AVPs shall maintain their 'M', 'P' and 'V' flag settings. Where 3GPP Radius VSAs are re-used, unless otherwise stated, they shall be translated to Diameter AVPs as described in RFC 4005 [12] with the exception that the 'M' flag shall be set and the 'P' flag may be set.

Table 5.4.0.1: Rx re-used Diameter AVPs

Attribute Name	Reference	Comments	Applicability (notes 1, 2)
3GPP-MS-TimeZone	3GPP TS 29.061 [34]	Indicates the offset between universal time and local time in steps of 15 minutes of where the MS currently resides. This AVP shall have the 'M' bit cleared.	NetLoc RAN-NAS-Cause
3GPP-SGSN-MCC-MNC	3GPP TS 29.061 [34]	Indicates the serving core network operator ID. For GPRS accesses the MCC and the MNC of the SGSN. For EPS the MCC and the MNC provided by the SGW or TWAG. This AVP shall have the 'M' bit cleared.	NetLoc, Netloc-Trusted-WLAN RAN-NAS-Cause
3GPP-User-Location-Info	3GPP TS 29.061 [34]	Indicates details of where the UE is currently located (e.g. SAI or CGI), Coding shall be done as defined in 3GPP TS 29.274 [33]. This AVP shall have the 'M' bit cleared.	NetLoc RAN-NAS-Cause
AN-GW-Address	3GPP TS 29.212 [8]	Carries the IP address of the ePDG used as IPSec tunnel endpoint with the UE. This AVP shall have the ‘M’ bit cleared.	
AN-Trusted	3GPP TS 29.273 [39]	Indicates whether the access network is trusted or untrusted for the Non-3GPP access network. This AVP shall have the 'M' bit cleared.	
Called-Station-Id	IETF RFC 4005 [12]	The PDN the user is connected to. For GPRS and EPS the APN. When used to contain the APN, the APN is composed of the APN Network Identifier only, or the APN Network Identifier and the APN Operator Identifier as specified in TS 23.003 [38], clause 9.1. The inclusion of the APN Operator Identifier can be configurable.	Rel8
DRMP	IETF RFC 7944 [43]	Allows Diameter endpoints to indicate the relative priority of Diameter transactions.	
Final-Unit-Action	IETF RFC 4006 [14]	The action applied by the PCEF when the user’s account cannot cover the service cost.	Rel8
Framed-IP-Address	IETF RFC 4005 [12]	The valid routable Ipv4 address that is applicable for the IP Flows towards the UE at the PCEF. The PCRF shall use this address to identify the correct IP-CAN session (session binding). For example, the IP address may actually be that of the network interface of a NAT device between the UE and the GW. The values 0xFFFFFFFF and 0xFFFFFFFE are not applicable as described in RFC 4005 [12].	
Framed-Ipv6-Prefix	IETF RFC 4005 [12]	A valid full Ipv6 address that is applicable to an IP flow or IP flows towards the UE at the PCEF. The PCRF shall use this address to identify the correct IP-CAN session (session binding, refer to TS 29.213 [9]). For example, the IP address may actually be that of the network interface of a NAT device between the UE and the GW. The encoding of the value within this Octet String type AVP shall be as defined in RFC 3162 [20], clause 2.3. The "Reserved", "Prefix-Length" and "Prefix" fields shall be included in this order. The AF shall set the "Prefix Length" to 128 and encode the Ipv6 address of the UE within the "Prefix" field.	
Granted-Service-Unit (NOTE 3)	IETF RFC 4006 [14]	The volume and/or time thresholds for sponsored data connectivity. Only CC-Total-Octets, one of the CC-Input-Octets and CC-Output-Octets, or CC-Time AVPs are reused. This AVP shall have the ‘M’ bit cleared.	SponsoredConnectivity, SCTimeBasedUM
IP-CAN-Type	3GPP TS 29.212 [8]	IP-CAN type of the user.	
Load	IETF draft-ietf-dime-load [51]	The AVP used to convey load information between Diameter nodes. This AVP and all AVPs within this grouped AVP shall have the 'M' bit cleared.	
NetLoc-Access-Support	3GPP TS 29.212 [8]	Indicates the level of support for NetLoc procedures provided by the current access network.	NetLoc

Attribute Name	Reference	Comments	Applicability (notes 1, 2)
OC-OLR	IETF RFC 7683 [35]	Contains the necessary information to convey an overload report	
OC-Supported-Features	IETF RFC 7683 [35]	Defines the support for the Diameter overload indication conveyence by the sending node	
Pre-emption-Capability	3GPP TS 29.212 [8]	Indicates whether a service data flow can get resources that were already assigned to another service data flow with a lower priority level.	MCPTT-Preemption
Pre-emption-Vulnerability	3GPP TS 29.212 [8]	Indicates whether a service data flow can lose the resources assigned to it in order to admit a service data flow with higher priority level.	MCPTT-Preemption
RAN-NAS-Release-Cause	3GPP TS 29.212 [8]	Indicates RAN and/or NAS release cause code information. TWAN release cause code information or untrusted WLAN release cause code information.	RAN-NAS-Cause
RAT-Type	3GPP TS 29.212 [8]	Indicate which Radio Access Technology is currently serving the UE.	Rel8
Reference-Id	3GPP TS 29.154 [47]	Indicates the transfer policy stored in the SPR.	
Reservation-Priority	3GPP TS 183.017 [15]	The vendor-id shall be set to ETSI (13019) [15]. The support of this AVP shall be advertised in the capabilities exchange mechanisms (CER/CEA) by including the ETSI parameter in the Supported-Vendor-Id AVP.	
Subscription-Id	IETF RFC 4006 [14]	The identification of the subscription (IMSI, MSISDN, etc.)	
Supported-Features	3GPP TS 29.229 [25]	If present, this AVP informs the destination host about the features that the origin host requires to successfully complete this command exchange.	Rel8
TCP-Source-Port	3GPP TS 29.212 [8]	Contains the TCP source port number in the case that a NAT and firewall are detected and the IKEv2 messages exchanged between the UE and the ePDG are transported using the firewall traversal tunnel as described in 3GPP TS 24.302 [50].This AVP shall have the 'M' bit cleared.	NetLoc-Untrusted-WLAN
TWAN-Identifier	3GPP TS 29.061 [34]	Indicates the UE location in a Trusted WLAN or Untrusted WLAN Access Network. This AVP shall have the 'M' bit cleared.	Netloc-Trusted-WLAN RAN-NAS-Cause NetLoc-Untrusted-WLAN
ToS-Traffic-Class	3GPP TS 29.212 [8]	Indicates the DSCP code to be used for packet filter. The first octet contains the DSCP code and the second octet contains the mask field set to 11111100.	DSCP
UDP-Source-Port	3GPP TS 29.212 [8]	Contains the UDP source port number in the case that NAT is detected and the IKEv2 messages exchanged between the UE and the ePDG are encapsulated in the UDP messages according to IETF RFC 3948 [49]. This AVP shall have the 'M' bit cleared.	NetLoc-Untrusted-WLAN
UE-Local-IP-Address	3GPP TS 29.212 [8]	Indicates the local IP address of the UE. This AVP shall have the 'M' bit cleared.	NetLoc-Untrusted-WLAN
Used-Service-Unit (NOTE 3)	IETF RFC 4006 [14]	The measured volume and/or time for sponsored data connectivity. Only CC-Total-Octets, one of the CC-Input-Octets and CC-Output-Octets, or CC-Time AVPs are reused. This AVP shall have the 'M' bit cleared.	SponsoredConnectivity SCTimeBasedUM
User-Equipment-Info	IETF RFC 4006 [14]	The identification and capabilities of the terminal (IMEISV, etc.) When the User-Equipment-Info-Type is set to IMEISV(0), the value within the User-Equipment-Info-Value shall be a UTF-8 encoded decimal.	

Attribute Name	Reference	Comments	Applicability (notes 1, 2)
User-Location-Info-Time	3GPP TS 29.212 [8]	Indicates the time the UE was last known to be in the location.	NetLoc RAN-NAS-Cause NetLoc-Untrusted-WLAN
NOTE 1: AVPs marked with "Rel8" are applicable as described in clause 5.4.1. NOTE 2: AVPs marked with "SponsoredConnectivity" are applicable for sponsored data connectivity. NOTE 3: Volume Usage monitoring control functionality is applicable for SponsoredConnectivity supported feature. Time Based Usage monitoring control is applicable for SCTimeBasedUM supported feature.			

5.4.1 Use of the Supported-Features AVP on the Rx reference point

The Supported-Features AVP is used during session establishment to inform the destination host about the required and optional features that the origin host supports. The client shall, in the first request of a Diameter session indicate the set of supported features. The server shall, in the first answer within the Diameter session indicate the set of features that it has in common with the client and that the server shall support within the same Diameter session. Any further command messages shall always be compliant with the list of supported features indicated in the Supported-Features AVPs during session establishment. Features that are not advertised as supported shall not be used to construct the command messages for that Diameter session. Unless otherwise stated, the use of the Supported-Features AVP on the Rx reference point shall be compliant with the requirements for dynamic discovery of supported features and associated error handling on the Cx reference point as defined in clause 7.2.1 of 3GPP TS 29.229 [25].

The base functionality for the Rx reference point is the 3GPP Rel-7 standard and a feature is an extension to that functionality. If the origin host does not support any features beyond the base functionality, the Supported-Features AVP may be absent from the Rx commands. As defined in clause 7.1.1 of 3GPP TS 29.229 [25], when extending the application by adding new AVPs for a feature, the new AVPs shall have the M bit cleared and the AVP shall not be defined mandatory in the command ABNF.

As defined in 3GPP TS 29.229 [25], the Supported-Features AVP is of type grouped and contains the Vendor-Id, Feature-List-ID and Feature-List AVPs. On the Rx reference point, the Supported-Features AVP is used to identify features that have been defined by 3GPP and hence, for features defined in this document, the Vendor-Id AVP shall contain the vendor ID of 3GPP (10415). If there are multiple feature lists defined for the Rx reference point, the Feature-List-ID AVP shall differentiate those lists from one another.

On receiving an initial request application message, the destination host shall act as defined in clause 7.2.1 of 3GPP TS 29.229 [25]. The following exceptions apply to the initial and stateless AAR/AAA command pair:

- If the AF supporting post-Rel-7 Rx functionality is able to interoperate with a PCRF supporting Rel-7, the AAR shall include the features supported by the AF within Supported-Features AVP(s) with the ‘M’ bit cleared. Otherwise, the AAR shall include the supported features within the Supported-Features AVP(s) with the M-bit set.

NOTE 1: One instance of Supported-Features AVP is needed per Feature-List-ID.

- If the AAR command does not contain any Supported-Features AVP(s) and the PCRF supports Rel-7 Rx functionality, the AAA command shall not include the Supported-Features AVP. In this case, both AF and PCRF shall behave as specified in the Rel-7 version of this document.

- If the AAR command contains the Supported-Features AVP(s), the PCRF shall include the Supported-Features AVP(s) in the AAA command, with the ‘M’ bit cleared, indicating only the features that both the PCRF and AF support.

NOTE 2: The client will always declare all features that are supported according to table 5.4.1.1. When more than one feature identifying a release is supported by both AF and PCRF, the AF will work according to the latest common supported release.

Once the PCRF and AF have negotiated the set of supported features during session establishment, the set of common features shall be used during the lifetime of the Diameter session.

The table below defines the features applicable to the Rx interfaces for the feature list with a Feature-List-ID of 1.

Table 5.4.1.1: Features of Feature-List-ID 1 used in Rx

Feature bit	Feature	M/O	Description
0	Rel8	M	This feature indicates the support of the base 3GPP Rel-8 functionality, including the AVPs and corresponding procedures supported by the base 3GPP Rel-7 Rx standard, but excluding those features represented by separate feature bits. AVPs introduced with this feature are marked with "Rel8" in Table 5.4.0.1.
1	Rel9	M	This feature indicates the support of the base 3GPP Rel-9 functionality, including the AVPs and corresponding procedures supported by the Rel8 feature bit, but excluding those features represented by separate feature bits.
2	ProvAFsignalFlow	O	This indicates support for the feature of provisioning of AF signalling flow information as described in clause 4.4.5a. If the PCRF supports this feature the AF may provision AF signalling flow information. NOTE: This feature is used by the IMS Restoration Procedures to provide to the PDN-Gateway the address of the P-CSCF selected by the UE, refer to TS 23.380 [28].
3	SponsoredConnectivity	O	This feature indicates support for sponsored data connectivity feature. If the PCRF supports this feature, the AF may provide sponsored data connectivity to the subscriber.
4	Rel10	M	This feature indicates the support of the base 3GPP Rel-10 functionality, including the AVPs and corresponding procedures supported by the Rel8 and Rel9 feature bit, but excluding those features represented by separate feature bits. AVPs introduced with this feature are marked with "Rel10" in table 5.3.0.1.
5	NetLoc	O	This feature indicates the support of the Access Network Information Reporting.
6	ExtendedFilter	O	This feature indicates the support for the local (i.e. UE) address and mask being present in filters signalled between network and UE.
7	SCTimeBasedUM	O	This feature indicates support for sponsored data connectivity feature with time-based usage monitoring control required. If the PCRF supports this feature, the AF may provide time threshold for the usage monitoring control.
8	Netloc-Trusted-WLAN	O	This feature indicates the support for the Trusted WLAN access.It requires that NetLoc feature is also supported.
9	RAN-NAS-Cause	O	This feature indicates the support for the release cause code information (NOTE 1) from the access network.
10	GroupComService	O	This feature indicates the support of Group Communication services as described in TS 23.468 [36] for unicast services.
11	ResShare	O	This feature indicates the support of resource sharing among several AF sessions.
12	DeferredService	O	This feature indicates the support of deferred transfer of service information from the AF.
13	DSCP	O	This feature indicates that the AF may provide a DSCP value when describing a service flow by supplying the ToS-Traffic-Class AVP.
14	SponsorChange	O	This feature indicates that the AF provides information on whether it wants to enable or disable/not enable sponsoring a service. It requires that SponsoredConnectivity is also supported.
15	E2EQOSMTSI	O	This feature indicates that the AF supports QoS End-to-end MTSI extensions as defined in 3GPP TS 26.114 [41]
16	NetLoc-Untrusted-WLAN	O	This feature indicates the support of the Untrusted WLAN access as described in 3GPP TS 23.203 [2]. It requires that NetLoc feature is also supported.
17	MCPTT	O	This feature indicates the support of Mission Critical Push To Talk services as described in 3GPP TS 23.179 [44]
18	PrioritySharing	O	This feature indicates that Priority Sharing is supported as described in 3GPP TS 23.203 [2], subclause 6.1.19.
19	PLMNInfo	O	This feature indicates that reporting on changes of PLMN info is supported.
20	MediaComponentVersioning	O	This feature indicates the support of media component versioning as defined in subclause 4.4.9.
21	MCPTT-Preemption		This feature indicates the support of service pre-emption based on the information provided by the AF. It requires that MCPPT feature is also supported.

Feature bit: The order number of the bit within the Feature-List AVP where the least significant bit is assigned number "0".
Feature: A short name that can be used to refer to the bit and to the feature, e.g. "EPS".
M/O: Defines if the implementation of the feature is mandatory ("M") or optional ("O").
Description: A clear textual description of the feature.
NOTE 1: In this release, the release cause code information from the access network can include RAN/NAS release cause(s), a TWAN release cause or an untrusted WLAN release cause.

Table 5.4.1.2: Features of Feature-List-ID 2 used in Rx

Feature bit	Feature	M/O	Description
0	PCSCF-Restoration-Enhancement	O	This feature indicates support of P-CSCF Restoration Enhancement. It is used for the PCRF and the P-CSCF to indicate if they support P-CSCF Restoration Enhancement.

Feature bit: The order number of the bit within the Feature-List AVP where the least significant bit is assigned number "0".
Feature: A short name that can be used to refer to the bit and to the feature, e.g. "EPS".
M/O: Defines if the implementation of the feature is mandatory ("M") or optional ("O").
Description: A clear textual description of the feature.

5.5 Rx specific Experimental-Result-Code AVP values

5.5.1 Permanent Failures

Errors that fall within the Permanent Failures category shall be used to inform the peer that the request failed, and should not be attempted again.

IETF RFC 6733 [52] specifies the Experimental-Result AVP containing Vendor-ID AVP and Experimental-Result-Code AVP. The Experimental-Result-Code AVP (AVP Code 298) is of type Unsigned32 and contains a vendor-assigned value representing the result of processing a request. The Vendor-ID AVP shall be set to 3GPP (10415).

Specific values of the Rx specific Experimental-Result-Code AVP are:

INVALID_SERVICE_INFORMATION (5061)

The PCRF rejects new or modified service information the service information provided by the AF is invalid or insufficient for the server to perform the requested action.

FILTER_RESTRICTIONS (5062)

The PCRF rejects new or modified service information because the Flow-Description AVP(s) cannot be handled by the server because restrictions defined in clause 5.3.7 are not observed.

REQUESTED_SERVICE_NOT_AUTHORIZED (5063)

The PCRF rejects new or modified service information because the requested service, as described by the service information provided by the AF, is not consistent with either the related subscription information, operator defined policy rules and/or the supported features in the IP-CAN network.

DUPLICATED_AF_SESSION (5064)

The PCRF rejects a new Rx session setup because the new Rx session relates to an AF session with another related active Rx session, e.g. if the AF provided the same AF charging identifier for this new Rx session that is already in use for the other ongoing Rx session.

IP-CAN_SESSION_NOT_AVAILABLE (5065)

The PCRF rejects a new Rx session setup when it fails to associate the described service IP flows within the session information received from the AF to an existing IP-CAN session.

UNAUTHORIZED_NON_EMERGENCY_SESSION (5066)

The PCRF rejects a new Rx session setup because the session binding function associated a non-Emergency IMS session to an IP-CAN session established to an Emergency APN.

UNAUTHORIZED_SPONSORED_DATA_CONNECTIVITY (5067)

The PCRF rejects a new Rx session setup because the PCRF can't authorize the sponsored data connectivity based on the sponsored data connectivity profile or the operator policy (e.g. the sponsored data connectivity not authorized in the roaming case).

TEMPORARY_NETWORK_FAILURE (5068)

The PCRF rejects new or modified service information because there is a temporary failure in the access network (e.g. the SGW has failed).

5.5.2 Transient Failures

Errors that fall within the transient failures category are used to inform a peer that the request could not be satisfied at the time it was received, but may be able to satisfy the request in the future.

The Result-Code AVP values defined in Diameter Base IETF RFC 6733 [52] are applicable. Also the following specific Rx Experimental-Result-Code value is defined for transient failures:

REQUESTED_SERVICE_TEMPORARILY_NOT_AUTHORIZED (4261)

The PCRF temporarily rejects new or modified service information because the network is temporarily not able to provide the service delivery that the AF requested, e.g. due to the service information is not consistent with the operator defined policy rules for the congestion status of the user.

5.6 Rx messages

5.6.0 General

Existing Diameter command codes from the Diameter base protocol IETF RFC 6733 [52] and the NASREQ Diameter application (RFC 4005 [12]) are used with the Rx specific AVPs. An Rx specific Auth-Application id is used together with the command code to identify the Rx messages.

NOTE 1: The notion of NAS (Network Access Server) is not used here, NASREQ is just used for protocol purposes, not for its functional meaning.

NOTE 2: Some of the AVPs included in the messages formats below are in bold to highlight that these AVPs are used by this specific protocol and do not belong to the original Diameter Base Protocol IETF RFC 6733 [52].

NOTE3: Multiple instances of the Subscription-Id AVP in the AAR or RAR command correspond to multiple types of identifier for the same subscriber, for example IMSI and MSISDN.

5.6.1 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 PCRF in order to provide it with the Session Information.

Message Format:

```
<AA-Request> ::= < Diameter Header: 265, REQ, PXY >
                 < Session-Id >
                 [ DRMP ]
                 { Auth-Application-Id }
                 { Origin-Host }
                 { Origin-Realm }
                 { Destination-Realm }
                 [ Destination-Host ]
                 [ IP-Domain-Id ]
                 [ Auth-Session-State ]
                 [ AF-Application-Identifier ]
```

```
                *[ Media-Component-Description ]
                 [ Service-Info-Status ]
                 [ AF-Charging-Identifier ]
                 [ SIP-Forking-Indication ]
                *[ Specific-Action ]
                *[ Subscription-Id ]
                 [ OC-Supported-Features ]
                *[ Supported-Features ]
                 [ Reservation-Priority ]
                 [ Framed-IP-Address ]
                 [ Framed-Ipv6-Prefix ]
                 [ Called-Station-Id ]
                 [ Service-URN ]
                 [ Sponsored-Connectivity-Data ]
                 [ MPS-Identifier ]
                 [ GCS-Identifier ]
                 [ MCPTT-Identifier ]
                 [ Rx-Request-Type ]
                *[ Required-Access-Info ]
                 [AF-Requested-Data ]
                 [ Reference-Id ]
                 [ Pre-emption-Control-Info ]
                 [ Origin-State-Id ]
                *[ Proxy-Info ]
                *[ Route-Record ]
                *[ AVP ]
```

5.6.2 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 PCRF to the AF in response to the AAR command.

Message Format:

```
<AA-Answer> ::=  < Diameter Header: 265, PXY >
                 < Session-Id >
                 [ DRMP ]
                 { Auth-Application-Id }
                 { Origin-Host }
                 { Origin-Realm }
                 [ Result-Code ]
                 [ Experimental-Result ]
                 [ Auth-Session-State ]
                *[ Access-Network-Charging-Identifier ]
                 [ Access-Network-Charging-Address ]
                 [ Acceptable-Service-Info ]
                 [ AN-GW-Address ]
                 [ AN-Trusted ]
                 [ Service-Authorization-Info ]
                 [ IP-CAN-Type ]
                 [ NetLoc-Access-Support ]
                 [ RAT-Type ]
                *[ Flows ]
                 [ OC-Supported-Features ]
                 [ OC-OLR ]
                *[ Supported-Features ]
                *[ Subscription-Id ]
                 [ User-Equipment-Info ]
                 [ 3GPP-SGSN-MCC-MNC ]
                *[ Class ]
                 [ Error-Message ]
                 [ Error-Reporting-Host ]
                 [ Failed-AVP ]
                 [ Retry-Interval ]
                 [ Origin-State-Id ]
                *[ Redirect-Host ]
                 [ Redirect-Host-Usage ]
                 [ Redirect-Max-Cache-Time ]
                *[ Proxy-Info ]
                *[ Load ]
                *[ AVP ]
```

5.6.3 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 PCRF to the AF in order to indicate an Rx specific action.

Message Format:

```
<RA-Request> ::= < Diameter Header: 258, REQ, PXY >
                 < Session-Id >
                 [ DRMP ]
                 { Origin-Host }
                 { Origin-Realm }
                 { Destination-Realm }
                 { Destination-Host }
                 { Auth-Application-Id }
                *{ Specific-Action }
                 [ OC-Supported-Features ]
                *[ Access-Network-Charging-Identifier ]
                 [ Access-Network-Charging-Address ]
                 [ AN-GW-Address ]
                 [ AN-Trusted ]
                *[ Flows ]
                *[ Subscription-Id ]
                 [ Abort-Cause ]
                 [ IP-CAN-Type ]
                 [ NetLoc-Access-Support ]
                 [ RAT-Type ]
                 [ Sponsored-Connectivity-Data ]
                 [ 3GPP-User-Location-Info ]
                 [ User-Location-Info-Time ]
                 [ 3GPP-MS-TimeZone ]
                *[ RAN-NAS-Release-Cause ]
                 [ 3GPP-SGSN-MCC-MNC ]
                 [ TWAN-Identifier ]
                 [ TCP-Source-Port ]
                 [ UDP-Source-Port ]
                 [ UE-Local-IP-Address ]
                 [ Origin-State-Id ]
                *[ Class ]
                *[ Proxy-Info ]
                *[ Route-Record ]
                *[ AVP ]
```

5.6.4 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 PCRF in response to the RAR command.

Message Format:

```
<RA-Answer> ::=  < Diameter Header: 258, PXY >
                 < Session-Id >
                 [ DRMP ]
                 { Origin-Host }
                 { Origin-Realm }
                 [ Result-Code ]
                 [ Experimental-Result ]
                 [ OC-Supported-Features ]
                 [ OC-OLR ]
                *[ Media-Component-Description ]
                 [ Service-URN ]
                 [ Origin-State-Id ]
                *[ Class ]
                 [ Error-Message ]
                 [ Error-Reporting-Host ]
                *[ Redirect-Host ]
                 [ Redirect-Host-Usage ]
                 [ Redirect-Max-Cache-Time ]
                 [ Failed-AVP ]
                *[ Proxy-Info ]
                *[ AVP ]
```

5.6.5 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 PCRF that an established session shall be terminated.

Message Format:

```
<ST-Request> ::= < Diameter Header: 275, REQ, PXY >
                 < Session-Id >
```

```
                [ DRMP ]
                { Origin-Host }
                { Origin-Realm }
                { Destination-Realm }
                { Auth-Application-Id }
                { Termination-Cause }
                [ Destination-Host ]
                [ OC-Supported-Features ]
               *[ Required-Access-Info ]
               *[ Class ]
                [ Origin-State-Id ]
               *[ Proxy-Info ]
               *[ Route-Record ]
               *[ AVP ]
```

5.6.6 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 PCRF to the AF in response to the S3GPP TR command.

Message Format:

```
<ST-Answer>  ::= < Diameter Header: 275, PXY >
                 < Session-Id >
                 [ DRMP ]
                 { Origin-Host }
                 { Origin-Realm }
                 [ Result-Code ]
                 [ Error-Message ]
                 [ Error-Reporting-Host ]
                 [ OC-Supported-Features ]
                 [ OC-OLR ]
                 [ Failed-AVP ]
                 [ Sponsored-Connectivity-Data ]
                 [ Origin-State-Id ]
                 [ 3GPP-User-Location-Info ]
                 [ User-Location-Info-Time ]
                 [ 3GPP-MS-TimeZone ]
                *[ RAN-NAS-Release-Cause ]
                 [ 3GPP-SGSN-MCC-MNC ]
                 [ TWAN-Identifier ]
                 [ TCP-Source-Port ]
                 [ UDP-Source-Port ]
                 [ UE-Local-IP-Address ]
                 [ Netloc-Access-Support ]
                *[ Class ]
                *[ Redirect-Host ]
                 [ Redirect-Host-Usage ]
                 [ Redirect-Max-Cache-Time ]
                *[ Proxy-Info ]
                *[ Load ]
                *[ AVP ]
```

5.6.7 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 PCRF to inform the AF that bearer for the established session is no longer available.

Message Format:

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

5.6.8 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 PCRF in response to the ASR command.

Message Format:

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

Annex A (normative): IMS Related P-CSCF Procedures over Rx

A.1 Provision of Service Information at P-CSCF

The P-CSCF shall send service information to the PCRF upon every SIP message that includes an SDP answer payload for the purpose of authorizing the IP flows and the QoS resources required for a negotiated IMS session, unless the SDP payload only relates to a circuit-switched bearer (i.e. "c=" line set to "PSTN" and an "m=" line set to "PSTN", refer to 3GPP TS 24.292 [26]). The service information shall be derived both from the SDP offer and the SDP answer. This ensures that the PCRF receives proper information to perform media authorization for all possible IMS session set-up scenarios, and that the PCRF is also capable of handling session modifications. The P-CSCF may include the Service-Info-Status AVP with the value set to FINAL_SERVICE_INFORMATION.

Additionally, the P-CSCF may send service information to the PCRF when receiving a SIP message that includes an SDP offer payload for the purpose of performing an early bandwidth authorization check, or for enabling pre-authorization for a UE terminated IMS session establishment or modification with UE initiated resource reservation, or for the retrieval of network provided access network information (see clause A.10.2). The P-CSCF shall send service information to the PCRF when receiving a SIP message that includes an SDP offer payload when the IMS session is an MPS session that requires priority treatment. For a UE terminated session the P-CSCF may send the service information derived from the SDP offer when the SDP offer either does not include any preconditions information or includes preconditions information indicating that the local preconditions (i.e. the preconditions related to the remote peer) are already met. In this case, the P-CSCF shall derive the service information only from the SDP offer and shall include the Service-Info-Status AVP with the value set to PRELIMINARY SERVICE INFORMATION.

NOTE 1: For a UE terminated session setup, when the SDP offer either does not include any preconditions information or includes preconditions information indicating that the local preconditions (i.e. the preconditions related to the remote peer) are already met, the terminating UE can request a resource modification prior to sending the SDP answer. Even if the IP address and port information in the session information derived from the SDP offer can be insufficient for PCC rule authorization, the policy to handle such UE initiated requests at the PCRF can take into account the fact that an IMS session establishment is ongoing, for instance in deciding whether to authorize the request and in selecting an appropriate charging key and a gating policy.

The P-CSCF shall derive 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 shall be taken from the SDP information received by the P-CSCF in downlink direction, while the source IP address may be formed from the address present in the SDP received by the P-CSCF in uplink direction (taking into account only the 64 bit prefix of the Ipv6 address) Source and destination ports shall be derived according to rules provided in 3GPP TS 29.213 [9] clause 6.2.

EXAMPLE 1: Assuming UE A sends an SDP to UE B, the PCRF of UE B uses the address present in this SDP for the destination address of UE B's uplink Flow-Description AVP, while the PCRF of the UE A uses the 64 bit prefix of 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 wildcarded.

- A downlink Flow-Description AVP shall be formed as follows: The destination address shall be taken from the SDP information received by the P-CSCF in 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 downlink direction (taking into account only the 64 bit prefix of the Ipv6 address) Source and destination ports shall be derived according to rules provided in 3GPP TS 29.213 [9] clause 6.2.

EXAMPLE 2: Assuming UE A sends an SDP to UE B, the PCRF of UE A uses the address present in this SDP for the destination address of UE A's downlink Flow-Description AVP, while the PCRF 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 wildcarded.

The P-CSCF shall derive the bandwidth information within the service information, from the "b=AS" SDP parameter and "a=bw-info" SDP parameter, if available and if the E2EMTSIQOS feature is supported. If "a=bw-info" is used for bandwidth derivation, the P-CSCF shall use the SDP attribute line that contains the bandwidth properties for the IP version used by the UE, as detailed in 3GPP TS 29.213 [9] clause 6.2. If the received "a=bw-info" SDP attribute line(s) contain only bandwidth properties for an IP version that is not used by the UE, the P-CSCF shall re-compute the bandwidth properties for the used IP version and use that value for the bandwidth derivation as defined in 3GPP TS 26.114 [41].

NOTE 2: If no IP version is included for any of the "a=bw-info" SDP attribute lines related to a certain payload type and direction then IPv6 is assumed for all bandwidth properties related to the same direction and payload type, on all of the related "a=bw-info" SDP attribute lines, see clause 19 of 3GPP TS 26.114 [41].

If "a=bw-info" is used for bandwidth derivation and it includes both known and unknown bandwidth properties, the P-CSCF shall only consider the known bandwidth properties to derive the bandwidth information and ignore the unknown ones. If the" a=bw-info" line is received with an unknown directionality, then the entire "a=bw-info" line shall be ignored.

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 3GPP TS 29.213 [9] clause 6.2. 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.

For multiplexed RTP/RTCP flows (as negotiated using the"a=rtcp-mux" SDP attribute defined in IETF RFC 5761 [42], a P-CSCF supporting RTP/RTCP transport multiplexing shall derive the bandwidth information within the service information as specified in 3GPP TS 29.213 [9] subclause 6.2.

However, if service information is received containing the "b=TIAS" SDP parameter that corresponds to an SDP answer payload, and if the P-CSCF supports this parameter, the P-CSCF may derive the bandwidth from this parameter rather than from the "b=AS" SDP parameter, as detailed in 3GPP TS 29.213 [9] clause 6.2.

When available, the P-CSCF shall also indicate to PCRF, as a complement to the Service Information, the IMS Communication Service Identifier within the AF-Application-Identifier AVP. The originating P-CSCF shall take the IMS Communication Service Identifier value from the SIP response. The terminating P-CSCF shall take the IMS Communication Service Identifier value from the SIP request. Otherwise, the P-CSCF may not be able to provide an IMS Communication Service Identifier value to the PCRF. The format and specific headers where IMS communication service identifiers are transported within SIP are defined in 3GPP TS 24.229 [17].

NOTE 3: In order to indicate the IMS Communication Service Identifier to the PCRF, the originating P-CSCF sets the AF-Application-Identifier AVP to the ICSI contained in the topmost occurance of the "+g.3gpp.icsi-ref" header field parameter of the Feature-Caps header field(s) of 18x or 2xx SIP response (Feature-Caps: *;+g.3gpp.icsi-ref=”urn%Aurn-7%A3gpp-service.ims.icsi.mmtel”) and the terminating P-CSCF sets the AF-Application-Identifier AVP to the ICSI of the P-Asserted-Service header information received in the SIP request (e.g. P-Asserted-Service: urn:urn-7:3gpp-service.ims.icsi.mmtel). Since the headers and the format of the ICSI can vary depending on the case, the PCRF has to be prepared to accept the complete ICSI information received in different formats, as described in subclause 7.2A.8.2 in 3GPP TS 24.229 [17].

Additionally, the P-CSCF may include the Sharing-Key-DL AVP and/or Sharing-Key-UL AVP within the Media-Component-Description AVP in order to indicate the PCRF that resource sharing should apply for the media components in the related direction with the same value for the Sharing-Key-DL AVP and/or Sharing-Key-UL AVP.

Additionally, if PrioritySharing feature is supported, the P-CSCF may provide the Priority-Sharing-Indicator AVP within the Media-Component-Description AVP as described in subclause 4.4.47.

NOTE 4: The P-CSCF obtains this information from the Application Server as described in 3GPP TS 23.228 [16], subclause 5.4.7.9.

NOTE 5: RTCP flows are not subject to resource sharing. This requirement cannot be met for multiplexed RTP/RTCP flows as in this case there is no mechanism in the current release to distinguish between RTP and RTCP flows.

If the Service-URN AVP does not include an emergency service URN, i.e. a top-level service type of "sos" as specified in IETF RFC 5031 [21] and possibly additional sub-service information on the type of the emergency service and the PCRF binds the IMS service session to an IP-CAN session established to an Emergency APN, the PCRF shall return an AAA command with Experimental-Result-Code AVP set to the value UNAUTHORIZED_NON_EMERGENCY_SESSION to the P-CSCF. Upon receiving an AAA with Experimental-Result-Code AVP set to the value UNAUTHORIZED_NON_EMERGENCY_SESSION the P-CSCF shall apply the procedures defined in 3GPP TS 24.229 [17].

NOTE 6: The PCRF determines whether an IP-CAN session is established to an Emergency APN based on the information received over Gx and operator configuration.

If the AF-Requested-Data AVP is provided in the AA-Request command indicating "EPC-level Identities required", the PCRF shall provide the available user information for the IP-CAN session within the Subscription-Id AVP (s) and/or User-Equipment-Info AVP.

NOTE 7: The user information received within the User-Equipment-Info AVP and/or Subscription-Id AVP can be used to support authentication of roaming users in deployments with no IMS-level roaming interfaces or to support PSAP callback functionality for anonymous IMS emergency sessions. See 3GPP TS 23.167 [53] for futher information.

The PCRF may decide not to authorize requested service information. The PCRF will indicate it to the P-CSCF by sending an AA-Answer with Experimental-Result-Code AVP set to the value REQUESTED_SERVICE_NOT_AUTHORIZED. Upon receiving an AA-Answer with Experimental-Result-Code AVP set to the value REQUESTED_SERVICE_NOT_AUTHORIZED the P-CSCF shall apply the procedures defined in 3GPP TS 24.229 [17].

A.2 Enabling of IP Flows

A.2.0 General

Prior to the completion of the SIP session set-up, i.e. until the 2xx response to the INVITE request 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 direction. The P-CSCF may set the values of the Flow-Status AVPs derived from the SDP direction attributes as defined in 3GPP TS 29.213 [9] clause 6.2 or set the values of the Flow-Status AVPs considering the em-param of the P-Early-Media header field according to subclause A.2.1 or downgrade the values of the Flow-Status AVPs derived from the SDP direction attribute based on the configuration in the P-CSCF according to subclause A.2.2. However for multiplexed RTP/RTCP flows (as negotiated using the "a=rtcp-mux" SDP attribute defined in IETF RFC 5761 [42]), a P-CSCF supporting RTP/RTCP transport multiplexing shall set the Flow-Status set to "ENABLED" to prevent that RTCP is blocked. If the P-CSCF chooses to modify the values of the Flow-Status AVPs as received from the SDP direction attribute, the P-CSCF shall store the last received SDP.

When a 2xx response is received, the P-CSCF shall enable all media IP flows according to the direction attribute within the last received SDP, as specified in 3GPP TS 29.213 [9] clause 6.2. When a 2xx response is received and the P-CSCF previously provided the values of the Flow-Status AVPs different from the value derived from the SDP direction attribute in the session information, the P-CSCF shall provide service information with values of the Flow-Status AVPs corresponding to the last received SDP.

NOTE: In most cases a 2xx response is a 200 (OK) response.

If the P-CSCF receives SDP answers after the completion of the SIP session set-up, i.e. after the 2xx response to the INVITE request is received, the P-CSCF shall provide the Flow-Status AVP, based on the last received SDP answer. The Flow-Status AVP shall be derived from the SDP according to 3GPP TS 29.213 [9] clause 6.2.

A.2.1 Gate control procedures considering the P-Early-Media header field

Prior to the completion of the SIP session set-up, the P-CSCF may use the em-param of the P-Early-Media header field defined in IETF RFC 5009 [48] in order to enable or disable early media in forward and/or backward direction. If the P-CSCF uses the em-param of the P-Early-Media header field for the gate control of early media, the P-CSCF shall perform the following procedures.

In the terminating P-CSCF, when a SIP message with the P-Early-Media header field is received from the UE and the policies configured in the P-CSCF indicate that the UE is authorized to send early media, then:

1) the P-CSCF shall set the Flow-Status AVP to "ENABLED" if:

   - the received em-param(s) in the P-Early-Media header field includes "sendrecv" and the last received SDP direction attribute from the UE is "sendrecv" or no SDP direction attribute has been received; or

2) the P-CSCF shall set the Flow-Status AVP to "ENABLED-UPLINK" if:

   - the received em-param(s) in the P-Early-Media header field includes "sendrecv" and the last received SDP direction attribute from the UE is "sendonly"; or

   - the received em-param(s) in the P-Early-Media header field includes "sendonly" and the last received SDP direction attribute from the UE is "sendrecv" or "sendonly" or no SDP direction attribute has been received; or

3) the P-CSCF shall set the Flow-Status AVP to "ENABLED-DOWNLINK" if:

   - the received em-param(s) in the P-Early-Media header field includes "sendrecv" and the last received SDP direction attribute from the UE is "recvonly"; or

   - the received em-param(s) in the P-Early-Media header field includes "recvonly" and the last received SDP direction attribute from the UE is "sendrecv" or "recvonly" or no SDP direction attribute has been received; or

4) the P-CSCF shall set the Flow-Status AVP to "DISABLED" if either the received em-param(s) in the P-Early-Media header field or the last received SDP direction attribute from the UE includes "inactive"; or

5) the P-CSCF may set the Flow-Status AVP to "DISABLED" or apply the rules defined in subclause A.2.2 if the received em-param(s) in the P-Early-Media header field includes "sendonly" or "recvonly" and the last received SDP direction attribute from the UE is "recvonly" or "sendonly" respectively.

NOTE 1: If the UE is authorized to send early media, the P-CSCF will not remove or modify the P-Early-Media header field according to 3GPP TS 24.229 [17].

When a SIP message with the P-Early-Media header field is received from the functional entity within the trust domain, and if:

- the P-Early-Media header field includes the "gated" parameter, then the P-CSCF may decide not to perform the gate control of early media; or

- the P-Early-Media header field does not include the "gated" parameter, then the P-CSCF shall perform the following procedures:

  1) the P-CSCF shall set the Flow-Status AVP to"ENABLED" if:

     - the received em-param(s) in the P-Early-Media header field includes "sendrecv" and the last received SDP direction attribute from the functional entity is "sendrecv" or no SDP direction attribute has been received; or

  2) the P-CSCF shall set the Flow-Status AVP to "ENABLED-DOWNLINK" if:

     - the received em-param(s) in the P-Early-Media header field includes "sendrecv" and the last received SDP direction attribute from the functional entity is "sendonly"; or

     - the received em-param(s) in the P-Early-Media header field includes "sendonly" and the last received SDP direction attribute from the functional entity is "sendrecv" or "sendonly" or no SDP direction parameter has been received; or

3) the P-CSCF shall set the Flow-Status AVP to "ENABLED-UPLINK" if:

   - the received em-param(s) in the P-Early-Media header field includes "sendrecv" and the last received SDP direction attribute from the functional entity is "recvonly"; or

   - the received em-param(s) in the P-Early-Media header field includes "recvonly"and the last received SDP direction attribute from the functional entity is "sendrecv" or "recvonly" or no SDP direction parameter has been received ; or

4) the P-CSCF shall set the Flow-Status AVP to "DISABLED" if either the received em-param(s) in the P-Early-Media header field or the last received SDP direction attribute from the functional entity includes "inactive"; or

5) the P-CSCF may set the Flow-Status AVP to "DISABLED" or apply the rules defined in subclause A.2.2 if the received em-param(s) in the P-Early-Media header field includes "sendonly" or "recvonly" and the last received SDP direction attribute from the functional entity is "recvonly" or "sendonly" respectively.

NOTE 2: According to IETF RFC 5009 [48], the non-direction parameter "gated" can be included after the direction parameter (e.g. "sendrecv") in the parameter list. The proxy performing gating of early media can add the parameter before forwarding the SIP message.

When a SIP message without the P-Early-Media header field is received from either the functional entity within the trust domain or the UE that is authorized to send early media, then the P-CSCF may set the Flow-Status AVP to "DISABLED" or apply the rules defined in subclause A.2.2 or apply the rules defined in 3GPP TS 29.213 [9] clause 6.2.

NOTE 3: As indicated in IETF RFC 5009 [48] the applicable preconditions need to be met in order to allow early media in a particular direction.

When a SIP message is received from the functional entity other than the functional entity within the trust domain or the UE that is authorized to send early media, then the P-CSCF shall not use the received em-param(s) in the P-Early-Media header field and may apply the rules defined in subclause A.2.2 or apply the rules defined in 3GPP TS 29.213 [9] clause 6.2.

NOTE 4: The P-CSCF will remove or modify the P-Early-Media header field in the above case.

A.2.2 Gate control procedures based on the configuration in the P-CSCF

Prior to the completion of the SIP session set-up, the P-CSCF may downgrade the values of the Flow-Status AVPs derived from the SDP direction attributes based on the configuration in the P-CSCF. If the P-CSCF has the configuration for the gate control of early media, the P-CSCF shall perform the following procedures.

NOTE: The gate control of early media can be configured in the P-CSCF per UE basis.

When the Flow-Status AVP derived from the SDP direction attribute is "ENABLED", then the P-CSCF may downgrade the value of the Flow-Status AVP to the value "DISABLED", "ENABLED_UPLINK", or "ENABLED_DOWNLINK" based on the configuration in the P-CSCF.

When the Flow-Status AVP derived from the SDP direction attribute is "ENABLED_UPLINK" or "ENABLED_DOWNLINK", then the P-CSCF may downgrade the value of the Flow-Status AVP to the value "DISABLED" based on the configuration in the P-CSCF.

A.3 Support for SIP forking

The P-CSCF shall be able to handle forking when PCC is applied. Forking can occur as specified in 3GPP TS 23.228 [16]. The related UE procedures are described in 3GPP TS 24.229 [17].

A.3.1 PCC rule provisioning 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. Multiple early media session may be established during this process.

The UE and the P-CSCF become aware of the forking only when a subsequent provisional response arrives for a new early dialogue. After the first early media session is established, for each subsequent provisional response establishing an additional early media session,, 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.

The P-CSCF shall also provision the service information derived from any subsequent SDP offer-answer exchange within an early dialogue (e.g. in PRACK and OK(PRACK), or UPDATE and OK(UPDATE)) using an AA request within the existing Diameter session containing the SIP-Forking-Indication AVP with value SEVERAL_DIALOGUES and the derived service information.

When receiving an AA request containing the SIP-Forking-Indication AVP with value SEVERAL_DIALOGUES, the PCRF shall identify the existing authorization information for that AF session. The PCRF shall send additional PCC Rules or individual service data flow filters to already provide PCC rules as required by the Flow Description AVPs within the session information to the PCEF. The PCRF shall authorize any additional media components and any increased QoS requirements for the previously authorized media components, as requested within the service information. The PCRF 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 PCRF shall open or close the gates for service flows depending on the flow status that is being provisioned. However, if a flow ID has been enabled in uplink or downlink direction or both way within previous service information, it shall remain enabled even if the PCRF receives service information that disable this flow ID within an AA request containing the SIP-Forking-Indication AVP with value SEVERAL_DIALOGUES.

If the P-CSCF provides one or more Media-Component-Description AVP with the Flow-Status AVP set to "REMOVED" for previously authorized media component(s) the media component shall remain as authorized and the PCRF shall not take any action on that media component(s).

NOTE: There can be cases where a forked response could not support some of the media components included in the SDP Offer (e.g. when early session disposition SDP as described in Annex A.7 applies, the forked response related to the early session could include the port set to zero for those media components not related to the early session or when a subsequent SDP Offer-Answer to indicate that some media is disabled). For those cases the P-CSCF will indicate the PCRF about the removal of the corresponding media component. However this media component is already supported by other UEs and the PCRF needs to maintain the corresponding PCC rules until the final SDP answer is received in the P-CSCF in order to avoid the release of resources in the network.

A.3.2 Updating the provisioned PCC rules 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 service 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. The P-CSCF shall provision the full service information including the applicable Flow-Description AVP(s) and Flow-Status AVP(s).

When receiving an AA request with no SIP-Forking-Indication AVP or with a SIP-Forking-Indication AVP with value SINGLE_DIALOGUE, the PCRF shall update installed PCC Rules information and Authorized-QoS information to match only the requirements of the service information within this AA request. The PCRF should immediately remove PCC Rule(s) or individual service data flow filters not matching IP flow(s) in the updated Service Information, to reduce the risk for initial clipping of the media stream, and to minimize possible misuse of resources. The PCRF shall also open or close the gates for service flows according to the flow status in the received service information.

A.4 Notification of AF Signalling Transmission Path Status

When the P-CSCF receives an initial REGISTER SIP message from an attached UE, the P-CSCF may subscribe to notifications of the status of the AF Signalling transmission path using the procedures specified in clause 4.4.5. Once the P-CSCF has subscribed, the P-CSCF may receive notifications from the PCRF according to clause 4.4.6.3.

NOTE 1: When the Standardised QCI characteristics as defined in 3GPP TS 23.203 [2] are followed, the QCI for IMS signalling will correspond to a non-GBR bearer. In this case, the P-CSCF will not receive notifications related to the Specific-Action with value "INDICATION_OF_LOSS_OF_BEARER".

NOTE 2: This procedure is not applicable for IMS registrations for Emergency sessions.

The P-CSCF shall cancel the subscription to notification of the status of the AF Signalling transmission path when the AF Signalling to that particular user is terminated (i.e. when the user is de-REGISTERED from the IM CN subsystem).

When the P-CSCF receives a notification of loss of signalling connectivity from the PCRF, the P-CSCF shall behave as defined in 3GPP TS 24.229 [17].

A.5 Indication of Emergency Session

A SIP INVITE request can contain a service URN as defined in IETF RFC 5031 [21] within the request URI. If the service within this URN is "sos", possibly with additional sub-service information, the P-CSCF shall provision this service and sub-service information within the Service-URN AVP towards the PCRF. The P-CSCF may also provision possible information about other services received within the service URN.

A.6 Notification IP-CAN Type Change

When the P-CSCF receives an initial REGISTER SIP message or an INVITE SIP message from an attached UE, the P-CSCF may request from the PCRF the information about the type of IP-CAN the UE is attached to using the procedure specified in clause 4.4.1.

NOTE 1: This procedure is not applicable for IMS registrations for Emergency sessions.

NOTE 2: The P-CSCF can request information about the type of IP-CAN as part of the SIP session setup when it is only interested in the related information when the IMS session is ongoing.

If the P-CSCF requests information about the type of IP-CAN, the P-CSCF shall also subscribe within the same AAR command operation to notifications for changes of the IP-CAN type used by the UE. The P-CSCF shall include a Specific-Action AVP in the AAR that is set to the value of IP-CAN_CHANGE.

When the P-CSCF receives the AA-Answer or RA-Request from the PCRF, the P-CSCF stores the IP-CAN type information received within the IP-CAN-Type AVP and the RAT type information received within the RAT-Type AVP and AN-Trusted AVP (if also provided by the PCRF) and behaves as defined in 3GPP TS 24.229 [17].

The P-CSCF may receive notifications for changes of the IP-CAN type from the PCRF according to clause 4.4.6.4. When the P-CSCF receives a notification of the change of the IP-CAN used by the UE, the P-CSCF stores the new IP-CAN type information and RAT type information and behaves as defined in 3GPP TS 24.229 [17].

NOTE 3: The subscription to receive information about the type of IP-CAN will be cancelled when the corresponding Rx session is terminated by the AF (i.e. when the UE is de-REGISTERED or the related SIP call is torn down).

A.7 Support for Early Session disposition SDP

A.7.1 General

As a network option, the P-CSCF may support the PCC procedures in the present Clause to handle "early session" disposition type SDP, as standardised in IETF RFC 3959 [27].

A.7.2 Service Information Provisioning for Early Media

The P-CSCF can receive "early session" disposition SDP in addition to "session" disposition SDP in SIP early dialogues.

The P-CSCF shall then provision service information derived both from the "early session" disposition SDP and "session" disposition SDP applying the procedures in Clauses A.1, A.2, and A.3, and in the present Clause.

The P-CSCF shall apply the mapping rules in Annex B.1.2.2.2 to derive the flow identifiers from "early session" disposition SDP.

If a single media line with one media type (e.g. "audio" or "video") is contained in "early session" disposition SDP and a single media line with the same media type is contained in the "session" disposition SDP of the same SIP dialogue, and both media lines describe service flows of the same directionality (uplink, downlink, or bidirectional), the P-CSCF should describe those SDP media lines in the same session information media component (with the same flow ID).

The "early session" disposition SDP can also contain media lines of a type not included in the "session" disposition SDP, or several media lines of the same type. Such media components shall be described in own media components in the service information.

If the P-CSCF desires to invoke special policies or separate event notifications for an "early session" disposition media line, it may choose to provision a separate session information media component even if a media line with the same media type and directionality is contained in "session" disposition SDP.

NOTE 1: A PCRF is then likely to supply separate PCC rules for early media and the corresponding final media. This may lead to an over provisioning of resources during call establishment and a subsequent reconfiguration of the radio bearer, or even to a call failure if the extra resources are not authorized or available.

If the P-CSCF receives "early session" disposition SDP before any "session" disposition SDP and supplies service information derived from the "early session" disposition SDP at this point of time, it shall use dedicated media components relating only to the "early session" disposition SDP in the service information.

NOTE 2: The "session" disposition SDP offer will frequently occur before the "early session" disposition SDP offer, but can also occur in parallel or in exceptional cases afterwards. The "session" disposition SDP answer can be contained in the same SIP message as the "early session" disposition SDP offer, or can be sent in a 200 OK (INVITE), i.e. after the "early session" disposition SDP answer.

If the P-CSCF includes any media component relating both to "early session" disposition SDP and "session" disposition SDP in the service information, the P-CSCF shall:

- provision the service information derived from "early session" disposition SDP and the service information derived from "session" disposition SDP in separate Rx AA-Requests, and shall send a new Rx AA-Request only after any previous Rx AA-Request has been acknowledged; and

- provision the first service information (either derived from "early session" disposition SDP or "session" disposition SDP) without the SIP-Forking-Indication AVP, or with the SIP-Forking-Indication AVP with value SINGLE_DIALOGUE; and

- provision all subsequent service information during ongoing call establishment with the SIP-Forking-Indication AVP with value SEVERAL_DIALOGUES; and

- if an SDP answer has been received and Codec-Data AVPs are provisioned within a Media-Component-Description AVP, provision a Codec-Data AVP derived from the corresponding offer together with a Codec-Data AVP derived from the SDP answer.

NOTE 3: The P-CSCF needs to provision the service information derived from "early session" disposition SDP and the service information derived from "session" disposition SDP in separate Rx AA-Requests because the encoding of the media-component does not allow for the simultaneous provisioning of two corresponding filters.

NOTE 4: The PCRF will treat service information containing the SIP-Forking-Indication AVP as described in Clause A.3.

A.7.3 Updating the Provisioned Service Information when Dialogue is established

The P-CSCF shall store the SDP information for the "session" disposition type until the first final SIP answer is received. Then the early media described in the "early session" disposition type SDP are terminated.

The P-CSCF shall then update the service information to match the requirements of the media described in the "session" disposition type SDP only:

- If the P-CSCF included any media component relating both to "early session" disposition SDP and "session" disposition SDP in the service information, the P-CSCF shall send an AA request without the SIP-Forking-Indication AVP or with a SIP-Forking-Indication AVP with value SINGLE_DIALOGUE and shall include the service information derived from the "session" disposition SDP. The P-CSCF shall provision the full service information including the applicable Flow-Description AVP(s) and Flow-Status AVP(s).

- The P-CSCF shall disable any media component(s) in the service information that relate to early media only by setting their flow status to "removed".

A.8 Provision of Signalling Flow Information at P-CSCF

When the P-CSCF has successfully concluded the initial registration of an attached UE, i.e., when the P-CSCF has sent to the UE a SIP 200 (OK) response to the SIP REGISTER request, the P-CSCF may provision information about the SIP signalling flows between the UE and itself using the procedure specified in clause 4.4.5a. If the P-CSCF already has an open Rx Diameter session with the PCRF related to the signalling with the UE, e.g. one that has been opened according to the procedure described in clause A.6 and/or in clause A.4, the P-CSCF shall reuse the already open session to provision the SIP Signalling IP Flow information.

NOTE: This procedure is not applicable for IMS registrations for Emergency sessions.

If the P-CSCF provisions information about SIP signalling flows, the P-CSCF shall ensure that for each signalling IP flow information it provides, the Flow-Description AVP shall accurately reflect the IP flow information as seen in the IP header ‘on the wire’. The P-CSCF shall set the value of the AF-Signalling-Protocol AVP to ‘SIP’.

When the P-CSCF de-registers the UE and terminates SIP Signalling to the UE, the P-CSCF shall de-provision the SIP Signalling IP flow information from the PCRF as described in clause 4.4.5a.

A.9 Handling of MPS Session

When the P-CSCF receives an authorised Resource-Priority header field or a temporarily authorised Resource-Priority header field containing an appropriate namespace and priority value in SIP signaling, and recognizes the need for priority treatment as specified in 3GPP TS 24.229 [17], the P-CSCF shall include the MPS-Identifier AVP and Reservation-Priority AVP in the AAR command towards the PCRF. The MPS-Identifier AVP shall contain the national variant for MPS service name indicating an MPS session. The Reservation-Priority AVP shall include the priority value of the related priority service. The Reservation-Priority AVP shall be populated with a default value if the priority value is unknown.

NOTE 1: Various mechanisms can be applied to recognize the need for priority treatment in the P-CSCF (e.g., based on the dialled digits), according to national regulation and network configuration, as stated in 3GPP TS 24.229 [17].

NOTE 2: Lowest user priority value is mapped in the corresponding lowest enumerated value of the Reservation-Priority AVP.

If the P-CSCF supports the Diameter message priority mechanism for an MPS session, it shall include the DRMP AVP towards the PCRF as described in 3GPP TS 29.213 [9], Annex J.

NOTE 3: If the P-CSCF supports the Diameter message priority mechanism for an MPS session, it includes the DRMP AVP with a priority value equivalent to the Reservation-Priority AVP priority value. Highest user priority value is mapped in the corresponding lowest enumerated value of the DRMP AVP.

Upon reception of a request that requires MPS treatment, the PCRF shall derive the PCC/QoS Rules corresponding to the MPS session, as appropriate. The PCRF shall take specific actions on the corresponding IP-CAN to ensure that the MPS session is prioritized, as described in 3GPP TS 29.212 [8], clause 4.5.19.1.3.

When the P-CSCF terminates the MPS session, the PCRF shall delete the PCC/QoS Rules corresponding to the MPS session. The PCRF shall revoke the actions related to the prioritization of the MPS session in the corresponding IP-CAN, as described in 3GPP TS 29.212 [8], clause 4.5.19.1.3.

A.10 Retrieval of network provided location information

A.10.1 General

According to Annex E.7 of 3GPP TS 23.228 [16], the P-CSCF can use PCC to retrieve network provided location information. Information flows related to the distribution of network provided location information within the IMS are provided in Annex R of 3GPP TS 23.228 [16].

This sublause provides optional PCC procedures to support the retrieval of network provided location information.

The originating P-CSCF can, depending on operator policy, retrieve the user location and/or UE Time Zone information either before sending the INVITE towards the terminating side or upon reception of the SDP answer from the terminating side.

A.10.2 Retrieval of network provided location information at originating P-CSCF for inclusion in SIP Request

If the originating P-CSCF is required by operator policy to retrieve network provided location information before forwarding a SIP INVITE request, upon reception of an INVITE/UPDATE request, the P-CSCF shall send an AA-Request according to clause 4.4.1 (SIP INVITE request) or 4.4.2 (SIP INVITE/UPDATE request) including:

- the "ACCESS_NETWORK_INFO_REPORT" value within the Specific-Action AVP; and
- the required access network information within the Required-Access-Info AVP.

If the SIP INVITE request is an initial SIP INVITE request, the P-CSCF shall establish an Rx session for the new SIP session with the AA-Request according to clause 4.4.6.7 (if no session information is included) or 4.4.1 (if preliminary session information is included).

The P-CSCF will receive the access network information from the PCRF in an RAR, and should include this access network information in the SIP INVITE/UPDATE requests that it forwards. When the retrieved access network information corresponds to the TWAN-Identifier AVP, the P-CSCF may also map the retrieved access network information to a Geographical Identifier for routing, as specified in Annex E.8 of 3GPP TS 23.228 [16].

A.10.3 Retrieval of network provided location information at originating P-CSCF for inclusion in SIP response confirmation

If an originating P-CSCF is required by operator policy to retrieve network provided location information before forwarding an SDP answer, the P-CSCF shall apply the following procedures:

Upon reception of an SDP offer, the P-CSCF may send an AA-Request to the PCRF according to clause A.1 and may include in this AA-request:

- the "ACCESS_NETWORK_INFO_REPORT" value within the Specific-Action AVP; and
- the required access network information within the Required-Access-Info AVP.

Upon reception of an SDP answer, the P-CSCF will send an AA-Request to the PCRF according to clause A.1. If the P-CSCF has not requested access network information upon reception of the SDP offer, the P-CSCF shall include in this AA-request:

- the "ACCESS_NETWORK_INFO_REPORT" value within the Specific-Action AVP; and
- the required access network information within the Required-Access-Info AVP.

The P-CSCF will receive the access network information from the PCRF in an RAR, and should include this access network information in the SIP message with the response confirmation before forwarding it. When the retrieved access network information corresponds to the TWAN-Identifier AVP, the P-CSCF may also map the retrieved access network information to a Geographical Identifier for routing, as specified in Annex E.8 of 3GPP TS 23.228 [16].

A.10.4 Retrieval of network provided location information at terminating P-CSCF

If a terminating P-CSCF is required by operator policy to retrieve network provided location information at session establishment and/or modification, the P-CSCF shall apply the following procedures:

The terminating P-CSCF may retrieve network provided location information upon reception of a SIP INVITE request containing an SDP offer by sending an AA-Request including:

- the "ACCESS_NETWORK_INFO_REPORT" value within the Specific-Action AVP;
- the required access network information within the Required-Access-Info AVP;
- service information derived from the SDP offer; and
- the Service-Info-Status AVP with the value set to PRELIMINARY SERVICE INFORMATION.

Upon reception of a SIP response that requires the inclusion of access network information and includes an SDP answer, the P-CSCF will send an AA-Request to the PCRF according to clause A.1. If the P-CSCF has not already retrieved network provided location information upon reception of the corresponding SIP INVITE request including an SDP offer, the P-CSCF shall include in this AA-request:

- the "ACCESS_NETWORK_INFO_REPORT" value within the Specific-Action AVP; and
- the required access network information within the Required-Access-Info AVP.

Upon reception of a SIP response that requires the inclusion of access network information and includes no SDP answer, if the P-CSCF has not already retrieved network provided location information upon reception of the corresponding SIP INVITE request including an SDP offer, the P-CSCF shall send an AA-Request including:

- the "ACCESS_NETWORK_INFO_REPORT" value within the Specific-Action AVP; and
- the required access network information within the Required-Access-Info AVP.

The P-CSCF may also include in the AA-Request

- service information derived from an SDP offer within the SIP response; and
- the Service-Info-Status AVP with the value set to PRELIMINARY SERVICE INFORMATION.

If the SIP INVITE request is an initial SIP INVITE request, the P-CSCF shall establish an Rx session for the new SIP session with the AA-Request according to clause 4.4.6.7 (if no session information is included) or 4.4.1 (if preliminary session information is included).

If an Rx session related to service data has not yet been established, the P-CSCF shall establish an Rx session for the new SIP session with the AA-Request according to clause 4.4.6.7 (if no session information is included) or 4.4.1 (if preliminary session information is included).

The P-CSCF will receive the access network information from the PCRF in an RAR, and should include this access network information in the SIP response before forwarding it. When the retrieved access network information corresponds to the TWAN-Identifier AVP, the P-CSCF may also map the retrieved access network information to a Geographical Identifier for routing, as specified in Annex E.8 of 3GPP TS 23.228 [16].

A.10.5 Provisioning of network provided location information at SIP session release

If a P-CSCF is required by operator policy to include network provided location information in SIP session release signalling, the P-CSCF shall apply the following procedures:

Upon reception of a SIP session release request that requires the inclusion of network provided location information, the P-CSCF will send an ST-Request and shall include in this request the required access network information within the Required-Access-Info AVP.

The P-CSCF will receive the access network information from the PCRF in the corresponding ST-Answer, and should include this access network information either in the SIP session termination request (at the originating side) or a reply to the SIP session termination request (at the terminating side). When the retrieved access network information corresponds to the TWAN-Identifier AVP, the P-CSCF may also map the retrieved access network information to a Geographical Identifier for routing, as specified in Annex E.8 of 3GPP TS 23.228 [16].

A.11 Handling of RAN/NAS release cause values

If the P-CSCF is required by operator policy to provide the RAN/NAS release cause information, it includes this information in the corresponding SIP message as specified in 3GPP TS 24.229 [17] when received from the PCRF (see clause 4.4.4, 4.4.6.1, 4.4.6.2, 4.4.6.3 and 4.4.6.7).

A.12 Resource Sharing

The P-CSCF may indicate to the PCRF that media of an AF session may share resources with media belonging to other AF sessions according to 3GPP TS 23.228 [16].

If the P-CSCF determines that resource sharing is possible, it may at establishment of a new AF session, include the Sharing-Key-UL AVP and/or Sharing-Key-DL AVP indicating that media resources may be shared in the related direction. The P-CSCF shall assign a distinct value for the Sharing-Key-UL AVP and/or Sharing-Key-DL AVP for each media component identified by the Media-Component-Description AVP for the AF session.

NOTE 1: When resource sharing applies to both directions for a certain media component, the P-CSCF can assign the same value for Sharing-Key-UL AVP and Sharing-Key-DL AVP within the same media component.

The P-CSCF shall not include the Sharing-Key-UL AVP and/or Sharing-Key-DL AVP within the Media-Component-Description AVP when the AF session relates to an Emergency Session.

The PCRF shall not include the Sharing-Key-DL AVP and/or Sharing-Key-UL AVP for those PCC/QoS Rules related to the RTCP traffic.

Trigger conditions that require applying or stopping resource sharing are described in 3GPP TS 24.229 [17].

NOTE 2: When P-CSCF needs to stop sharing according to the procedures described in 3GPP TS 24.229 [17], the P-CSCF will provide new values for the Sharing-Key-UL AVP and/or Sharing-Key-DL AVP that are not being used by any other AF sessions for the same user.

A.13 Handling of MCPTT priority call

A.13.1 General

Within the framework of MCPTT, when the SIP Core (3GPP TS 23.179 [44]) is implemented by an IMS core network, if the P-CSCF receives a SIP request message including a Resource-Priority header field with a namespace field and priority value defined for MCPTT for adjusting the priority of an MCPTT session, the P-CSCF shall provide the Reservation-Priority AVP and the MCPTT-Identifier AVP in the AA-Request command as defined in subclause A.13.2 to allow the PCRF to set the corresponding PCC rule(s) according to the prioritized MCPTT service. Additionally, if PrioritySharing feature is supported, the P-CSCF may provide the Priority-Sharing-Indicator AVP within the Media-Component-Description AVP as described in subclause A.1. For MCPTT the service priority and the priority sharing indicator are defined in 3GPP TS 23.179 [44].

NOTE 1: The process of adjusting priority may occur several times during the course of one session, e.g. a normal MCPTT group call elevated to an MCPTT emergency group call, returned to a normal priority MCPTT group call, elevated to an MCPTT imminent peril group call and returned to a normal priority MCPTT group call.

NOTE 2: Upon reception of a request that requires the adjustment of the MCPTT priority, the PCRF is expected to derive the PCC Rules corresponding to the this MCPTT session, as appropriate according to operator policies.

NOTE 3: The PCRF can identify an MCPTT call using the IMS Communication Service Identifier specific to MCPTT, which is provided by the P-CSCF in the AF-Application-Identifier AVP in the AA-Request sent to PCRF.

A.13.2 Determination of MCPTT priority parameter values

When the P-CSCF receives an authorized Resource-Priority header field containing an appropriate namespace and priority value used for MCPTT in SIP signaling, the P-CSCF shall include the MCPTT-Identifier AVP and Reservation-Priority AVP in the AAR command towards the PCRF.

The MCPTT-Identifier AVP shall include the namespace defined for MCPTT as received within the Resource-Priority header field.

NOTE: Two different values are defined for the MCPTT-Identifier AVP, one for each namespace value defined for MCPTT (see draft-holmberg-dispatch-mcptt-rp-namespace-00.txt [45]).

The Reservation-Priority AVP shall contain the priority value of the Resource-Priority header; the lowest priority shall be mapped to to DEFAULT (0), the next after the lowest to PRIORITY-ONE (1), and so on up to the highest priority which shall be mapped to PRIORITY-FIFTEEN (15).

Additionally, when the P-CSCF receives information about priority sharing from an MCPTT server that supports simultaneous sessions and that needs to share a common priority for several MCPTT sessions and if PrioritySharing feature is supported, the P-CSCF may include the Priority-Sharing-Indicator AVP within the Media-Component-Description AVP in the AAR command. See 3GPP TS 23.179 [44] for further information.

A.14 Notification of PLMN Change

When the P-CSCF receives an initial REGISTER SIP message from an attached UE, the P-CSCF may subscribe to notifications of PLMN ID changes corresponding to the PLMN where the UE is located using the procedure specified in subclause 4.4.6.9.

When the P-CSCF receives the AA-Answer or RA-Request from the PCRF, the P-CSCF stores the PLMN identifier received within 3GPP-SGSN-MCC-MNC AVP and behaves as defined in 3GPP TS 24.229 [17].

The P-CSCF shall cancel the subscription to notification for changes of the PLMN used by the UE when the user is de-registered from the IM CN subsystem.

Annex B (normative): Flow identifiers: Format definition and examples

B.1 Format of a flow identifier

B.1.1 General

A flow identifier is expressed as a 2-tuple as follows:

> <The ordinal number of the position of the media component description in the SDI , The ordinal number of the IP flow(s) within the media component description assigned in the order of increasing downlink port numbers as detailed below >

where both are numbered starting from 1. The encoding of the flow identifier is as indicated in 3GPP TS 24.008 [12].

If UE and AF share an algorithm for a given application, which guarantees that UE and AF assign the same ordinal number to each media component, the ordinal numbers of the IP Flows within a media component shall be assigned according to the following rules:

- All IP flow(s) or bidirectional combinations of two IP flow(s) within the media component, for which a downlink destination port number is available, shall be assigned ordinal numbers in the order of downlink destination port numbers.
- All IP flows, where no downlink destination port number is available, shall be assigned the next higher ordinal numbers in the order of uplink destination port numbers.

The ordinal number of a media component shall not be changed when the session description information is modified.

If no SDI with fixed and unique positions for media components is exchanged between UE and AF, the UE and AF may assign the ordinal numbers of the media components in another application-dependent algorithm which guarantees that UE and AF assign the same ordinal number to each media component.

If UE and AF do not share an algorithm for a given application, which guarantees that UE and AF assign the same ordinal number to each media component, the ordinal number of the media component shall be set to zero and the ordinal number of the IP flows shall be assigned according to the following rules:

1. If ordinal numbers for several IP flows are assigned at the same time, all uplink IP flows shall be assigned lower ordinal number than all downlink IP flows.
2. If ordinal numbers for several IP flows are assigned at the same time, all uplink and all downlink IP flows shall separately be assigned ordinal numbers according to increasing internet protocol number assigned by IANA (e.g. 6 for TCP and 17 for UDP)
3. If ordinal numbers for several IP flows are assigned at the same time, for each internet protocol with a port concept, all uplink and all downlink IP flows of this internet protocol shall separately be assigned ordinal numbers according to increasing port numbers.
4. If IP flows are removed from an existing session, the previously assigned binding info shall remain unmodified for the remaining IP flows.
5. If IP flows are added to an existing session, the previously assigned binding info shall remain unmodified and the new IP flows shall be assigned ordinal numbers following the rules 1. To 3., starting with the first previously unused ordinal number. The numbers freed in step 4. Shall not be reused.

If the IP flows correspond to AF signalling (e.g. SIP signalling IP Flows), and no IP flow information is provided both the ordinal number of the media component and the IP flows shall be set to zero. In the case when the IP flow information of the AF signalling is provided, the ordinal number of the media component will be set to zero, and the ordinal number(s) of the IP flows shall follow the rules set above for the case when the UE and AF do not share an algorithm for a given application.

B.1.2 Derivation of Flow Identifiers from SDP

B.1.2.1 Standard Procedure

The procedure in Table B.1.2.1.1 shall be applied for SDP of "session" disposition type within SIP and for all SDP outside SIP.

Table B.1.2.1.1: Standard Procedure to derive Flow Identifiers from SDP

The ordinal number of the position of the media component	The ordinal number of the IP flow(s) within the media component description
The ordinal number of the position of the "m=" line in the SDP	The ordinal number of the IP flow(s) within the "m=" line assigned in the order of increasing downlink destination port numbers, if downlink destination port numbers are available. For uplink or inactive unicast media IP flows, a downlink destination port number is nevertheless available, if SDP offer-answer according to RFC 3264 is used. The ordinal number of the IP flow(s) within the "m=" line assigned in the order of increasing uplink destination port numbers, if no downlink destination port numbers are available.

B.1.2.2 SDP with "early session" disposition type

The procedure in Table B.1.2.2.1 shall be applied for SDP of "early session" disposition type within SIP. The "early session" disposition type is specified within IETF RFC 3959 [27].

Table B.1.2.2.1: Procedure to derive Flow Identifiers from "early session" disposition SDP

The ordinal number of the position of the media component	The ordinal number of the IP flow(s) within the media component description
If a single media component with one media type (e.g. "audio" or "video") is contained in "early session" disposition SDP and a single media component with the same media type is contained in the "session" disposition SDP of the same SIP dialogue, and if both SDP media components are described in a single Rx service information media component, that Rx service information media component shall obtain the media component number derived from "session" disposition SDP following the rules in table B.1.2.1.1. Otherwise each media component shall obtain the ordinal number of the position of the "m=" line in the "early session" disposition SDP plus 1000 as media component ordinal number.	As in table B.1.2.1.1.

B.2 Example 1

An UE, as the offerer, sends a SDP session description, as shown in table B.2.1, to an application server (only relevant SDP parameters are shown):

Table B.2.1: The values of the SDP parameters sent by the UE in example 1.

V=0 o=ecsreid 3262464865 3262464868 IN IP6 2001:0646:00F1:0045:02D0:59FF:FE14:F33A s=MM01 i=One unidirectional audio media and one unidirectional video media and one bidirectional application

```
media
t=3262377600 3262809600
m=video 50230 RTP/AVP 31
c=IN IP6 2001:0646:00F1:0045:02D0:59FF:FE14:F33A
a=recvonly
m=audio 50330 RTP/AVP 0
c=IN IP6 2001:0646:00F1:0045:02D0:59FF:FE14:F33A
a=sendonly
m=application 50430 udp wb
c=IN IP6 2001:0646:00F1:0045:02D0:59FF:FE14:F33A
a=sendrecv
```

and receives the SDP parameters, as shown in table B.2.2, from the application server:

Table B.2.2: The values of the SDP parameters sent by the application server in example 1.

```
V=0
o=ecsreid 3262464865 3262464868 IN IP6 2001:0646:00F1:0045:02D0:59FF:FE14:F33A
s=MM01
i=One unidirectional audio media and one unidirectional video media and one bidirectional application
media
t=3262377600 3262809600
m=video 51372 RTP/AVP 31
c=IN IP6 2001:0646:000A:03A7:02D0:59FF:FE40:2014
a=sendonly
m=audio 49170 RTP/AVP 0
c=IN IP6 2001:0646:000A:03A7:02D0:59FF:FE40:2014
a=recvonly
m=application 32416 udp wb
c=IN IP6 2001:0646:000A:03A7:0250:DAFF:FE0E:C6F2
a=sendrecv
```

From this offer–answer exchange of SDP parameters the UE and the PCRF each creates a list of flow identifiers comprising the IP flows as shown in table B.2.3:

Table B.2.3: Flow identifiers in example 1.

Order of 'm='-line	Type of IP flows	Destination IP address / Port number of the IP flows	Flow identifier
1	RTP (Video) DL	2001:0646:00F1:0045:02D0:59FF:FE14:F33A / 50230	<1,1>
1	RTCP DL	2001:0646:00F1:0045:02D0:59FF:FE14:F33A / 50231	<1,2>
1	RTCP UL	2001:0646:000A:03A7:02D0:59FF:FE40:2014 / 51373	<1,2>
2	RTP (Audio) UL	2001:0646:000A:03A7:02D0:59FF:FE40:2014 / 49170	<2,1>
2	RTCP DL	2001:0646:00F1:0045:02D0:59FF:FE14:F33A / 50331	<2,2>
2	RTCP UL	2001:0646:000A:03A7:02D0:59FF:FE40:2014 / 49171	<2,2>
3	UDP (application) DL	2001:0646:00F1:0045:02D0:59FF:FE14:F33A / 50430	<3,1>
3	UDP (application) UL	2001:0646:000A:03ª7:0250:DAFF:FE0E:C6F2 / 32416	<3,1>

B.3 Example 2

In the general case, multiple ports may be specified with a "number of ports" qualifier as follows, RFC 2327 [17]:

m=<media> <port>/<number of ports> <transport> <fmt list>

An UE, as the offerer, sends a SDP session description, as shown in table B.3.1, to an application server (only relevant SDP parameters are shown):

Table B.3.1: The values of the SDP parameters sent by the UE in example 2.

```
v=0
o=ecsreid 3262464321 3262464325 IN IP6 2001:0646:00F1:0045:02D0:59FF:FE14:F33A
s=MM02
i=One unidirectional audio media consisting of two media IP flows described by one media
component
t=3262377600 3262809600
m=audio 50330/2 RTP/AVP 0
c=IN IP6 2001:0646:00F1:0045:02D0:59FF:FE14:F33A
a=recvonly
```

and receives the SDP parameters, as shown in table B.3.2, from the application server:

Table B.3.2: The values of the SDP parameters sent by the application server in example 2.

```
v=0
o=ecsreid 3262464321 3262464325 IN IP6 2001:0646:00F1:0045:02D0:59FF:FE14:F33A
s=MM02
i=One unidirectional audio media consisting of two media IP flows described by one media
component
t=3262377600 3262809600
m=audio 49170/2 RTP/AVP 0
c=IN IP6 2001:0646:000A:03A7:02D0:59FF:FE40:2014
a=sendonly
```

From this offer–answer exchange of SDP parameters the UE and the PCRF each creates a list of flow identifiers comprising the IP flows as shown in table B.3.3:

Table B.3.3: Flow identifiers in example 2.

Order of 'm='-line	Type of IP flows	Destination IP address / Port number of the IP flows	Flow identifier
1	RTP (audio) DL	2001:0646:00F1:0045:02D0:59FF:FE14:F33A / 50330	<1,1>
1	RTCP DL	2001:0646:00F1:0045:02D0:59FF:FE14:F33A / 50331	<1,2>
1	RTCP UL	2001:0646:000A:03A7:02D0:59FF:FE40:2014 / 49171	<1,2>
1	RTP (audio) DL	2001:0646:00F1:0045:02D0:59FF:FE14:F33A / 50332	<1,3>
1	RTCP DL	2001:0646:00F1:0045:02D0:59FF:FE14:F33A / 50333	<1,4>
1	RTCP UL	2001:0646:000A:03A7:02D0:59FF:FE40:2014 / 49173	<1,4>

B.4 Example 3 without media components.

The UE and AF do not exchange SDP for an application and do not share an algorithm, which guarantees that UE and AF assign the same ordinal number to each media component.

At the AF session initiation, the UE and AF agree to set up the following IP flows:

- Uplink UDP flow with destination port 100.
- Downlink UDP flow with destination port 100.
- Downlink TCP flow with destination port 100.
- Uplink TCP flow with destination port 100.
- Uplink UDP flow with destination port 200.

The following binding info is assigned to these IP flows.

- Uplink UDP flow with destination port 100: (0, 2)
- Downlink UDP flow with destination port 100: (0, 5)
- Downlink TCP flow with destination port 100: (0, 4)
- Uplink TCP flow with destination port 100: (0, 1)
- Uplink UDP flow with destination port 200: (0, 3)

At a later stage in the session, the TCP IP flows are removed and the following IP flows are added:

- Uplink UDP flow with destination port 150.
- Downlink UDP flow with destination port 50.

The following binding info is assigned to the IP flows existing at this stage:

- Uplink UDP flow with destination port 100: (0, 2)
- Downlink UDP flow with destination port 100: (0, 5)
- Uplink UDP flow with destination port 200: (0, 3)
- Uplink UDP flow with destination port 150: (0, 6)
- Downlink UDP flow with destination port 50: (0, 7)

B.5 Example 4

In this example, the SDP "a=rtcp" attribute defined in IETF RFC 3605 is used.

An UE, as the offerer, sends a SDP session description, as shown in table B.5.1, to an application server (only relevant SDP parameters are shown):

Table B.5.1: The values of the SDP parameters sent by the UE in example 1.

```
V=0
o=ecsreid 3262464865 3262464868 IN IP6 2001:0646:00F1:0045:02D0:59FF:FE14:F33A
s=MM01
i=One unidirectional video media
t=3262377600 3262809600
m=video 50230 RTP/AVP 31
c=IN IP6 2001:0646:00F1:0045:02D0:59FF:FE14:F33A
a=recvonly
a=rtcp: 49320
```

and receives the SDP parameters, as shown in table B.5.2, from the application server:

Table C.5.2: The values of the SDP parameters sent by the application server in example 1.

```
V=0
o=ecsreid 3262464865 3262464868 IN IP6 2001:0646:00F1:0045:02D0:59FF:FE14:F33A
s=MM01
i=One unidirectional video media
t=3262377600 3262809600
m=video 51372 RTP/AVP 31
c=IN IP6 2001:0646:000A:03A7:02D0:59FF:FE40:2014
```

```
a=sendonly
a=rtcp:53020
```

From this offer–answer exchange of SDP parameters the UE and the PCRF each creates a list of flow identifiers comprising the IP flows as shown in table B.5.3:

Table B.5.3: Flow identifiers in example 4.

Order of 'm='-line	Type of IP flows	Destination IP address / Port number of the IP flows	Flow identifier
1	RTP (Video) DL	2001:0646:00F1:0045:02D0:59FF:FE14:F33A / 50230	<1,2>
1	RTCP DL	2001:0646:00F1:0045:02D0:59FF:FE14:F33A / 49320	<1,1>
1	RTCP UL	2001:0646:000A:03A7:02D0:59FF:FE40:2014 / 53020	<1,1>

Annex C (informative):
Void

Annex D (normative): Monitoring Related SCEF Procedures over Rx

D.1 Monitoring events support, using SCEF procedures over Rx

If SCS/AS has requested monitoring of events and operator policies in the SCEF indicate that monitoring shall be performed via PCRF, the SCEF shall initiate the applicable Rx procedures acting as an AF as described in 3GPP TS 23.682 [40].

The following monitoring events are supported;

- Location reporting according to the Access Network Information Report procedures described in clause 4.4.6.7. This functionality requires the support of NetLoc and/or NetLoc-Trusted-WLAN supported features.

- Communication Failure reporting as described in clauses 4.4.4, 4.4.6.1 and 4.4.6.3. This functionality requires the support of RAN-NAS-Cause supported feature.

Annex E (informative): Change history

Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
12-2014	CT-66	CP-140922	0361	1	UPCON related update about definition,abbreviation and achitecture part	12.5.0	13.0.0
12-2014	CT-66	CP-140935	0364	3	Double resource reuse support over Rx	12.5.0	13.0.0
12-2014	CT-66	CP-140934	0365	2	Mitigating RAN user plane congestion over Rx	12.5.0	13.0.0
03-2015	CT-67	CP-150131	0370		Reporting RAN/NAS cause during bearer creation/modification failure scenarious	13.0.0	13.1.0
03-2015	CT-67	CP-150134	0371		Removal of Editor's Note	13.0.0	13.1.0
03-2015	CT-67	CP-150131	0372		Access network information reporting during the IP-CAN session termination	13.0.0	13.1.0
03-2015	CT-67	CP-150136	0373		Introduction of a reference to the Rest-Rx interface	13.0.0	13.1.0
03-2015	CT-67	CP-150131	0374		Inclusion of RAN/NAS cause values into SIP signalling by P-CSCF	13.0.0	13.1.0
03-2015	CT-67	CP-150101	0380		Correction to the usage monitoring control for sponsored data connectivity	13.0.0	13.1.0
03-2015	CT-67	CP-150104	0383	2	Access network information report in case of IP-CAN bearer/IP-CAN session termination	13.0.0	13.1.0
03-2015	CT-67	CP-150136	0386	1	Correction to temporary network failure handling	13.0.0	13.1.0
03-2015	CT-67	CP-150114	0388		TWAN supports access network information report	13.0.0	13.1.0
03-2015	CT-67	CP-150127	0389	2	Uniqueness of Sharing Key for resource sharing over Rx	13.0.0	13.1.0
03-2015	CT-67	CP-150133	0394	2	Add the ToS-Traffic-Class AVP to the Rx to be sent by AF	13.0.0	13.1.0
06-2015	CT-68	CP-150362	0390	3	Clarification of the Called-Station-Id	13.1.0	13.2.0
06-2015	CT-68	CP-150361	0395	1	Removing restrictions to report RAT type to the AF	13.1.0	13.2.0
06-2015	CT-68	CP-150356	0396	2	Alignment with SDP procedures for resource sharing	13.1.0	13.2.0
06-2015	CT-68	CP-150363	0398	1	Adding TWAN and untrusted WLAN release cause	13.1.0	13.2.0
06-2015	CT-68	CP-150356	0399	-	Sharing-Key-UL	13.1.0	13.2.0
06-2015	CT-68	CP-150344	0405	2	Non-3GPP access for 3GPP-SGSN-MCC-MNC	13.1.0	13.2.0
06-2015	CT-68	CP-150362	0406	-	Correcting Hanging Paragraphs	13.1.0	13.2.0
09-2015	CT-69	CP-150485	0401	4	Clarification of the IP-Domain-Id	13.2.0	13.3.0
09-2015	CT-69	CP-150476	0408	2	Corrections to the PCRF-based P-CSCF Restoration Enhancement	13.2.0	13.3.0
09-2015	CT-69	CP-150472	0410	-	AVPs applicability for RAN-NAS-Cause	13.2.0	13.3.0
09-2015	CT-69	CP-150480	0411	1	Events applicability to support monitoring	13.2.0	13.3.0
09-2015	CT-69	CP-150482	0412	2	Change of chargeable party when sponsor connectivity applies	13.2.0	13.3.0
09-2015	CT-69	CP-150476	0415	1	Correction to the P-CSCF restoration enhancement	13.2.0	13.3.0
09-2015	CT-69	CP-150468	0421	2	Fixing Ambiguous Flag Rules for AVPs reused from TS 29.061	13.2.0	13.3.0
12-2015	CT-70	CP-150797	0422	1	Update the PCC architecture figures in 29.214	13.3.0	13.4.0
12-2015	CT-70	CP-150666	0423	1	RTP/RTCP transport multiplexing	13.3.0	13.4.0
12-2015	CT-70	CP-150663	0424	2	Support of new bandwidth information over Rx	13.3.0	13.4.0
12-2015	CT-70	CP-150789	0425	-	Incorrect command name to request access network information	13.3.0	13.4.0
12-2015	CT-70	CP-150631	0427	1	Update the reference of draft-ietf-dime-ovli	13.3.0	13.4.0
12-2015	CT-70	CP-150730	0428	1	Diameter message priority for PCC i	13.3.0	13.4.0
12-2015	CT-70	CP-150668	0432	2	Location report to support emergency service in Untrusted WLAN access	13.3.0	13.4.0

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New**
03-2016	CT#71	CP-160095	0435	2	F	Rx impact for background data transfer	13.5.0
03-2016	CT#71	CP-160101	0436	-	F	ICSI format specification over Rx	13.5.0
03-2016	CT#71	CP-160100	0437	3	A	Reporting of NAS/RAN cause in the STA command	13.5.0
03-2016	CT#71	CP-160101	0438	2	F	RAN-NAS-Cause handling upon unsuccessful bearer termination over Rx	13.5.0
03-2016	CT#71	CP-160092	0441	1	B	UE-to-network relay PCC handling over Rx	13.5.0
03-2016	CT#71	CP-160101	0442	1	F	Support of removed filters when SIP Forking applies over Rx	13.5.0
03-2016	CT#71	CP-160094	0443	-	F	Missing experimental result code value	13.5.0
03-2016	CT#71	CP-160104	0444	-	F	Location reporting for IMS sessions over S2b	13.5.0
03-2016	CT#71	CP-160093	0446	2	B	Reservation-Priority AVP and DRMP AVP Interaction	13.5.0
03-2016	CT#71	CP-160087	0448	2	B	New subclause to Appendix A for the handling of MCPTT emergency calls	13.5.0
06-2016	CT#72	CP-160282	0450	2	F	Support of IP version as part of the enhanced bandwidth mechanisms for MTSI sessions	13.6.0
06-2016	CT#72	CP-160287	0451	4	F	Priority sharing for concurrent sessions	13.6.0
06-2016	CT#72	CP-160271	0453	1	F	Reuse of TWAN-Identifier AVP in the Untrusted WLAN Access	13.6.0
06-2016	CT#72	CP-160275	0455	-	A	Correction to the time-based usage monitoring for sponsored data connectivity	13.6.0
06-2016	CT#72	CP-160251	0456	4	F	Authorization based on transfer policy	13.6.0
06-2016	CT#72	CP-160251	0457	1	F	Correction to the usage monitoring when the sponsoring is disabled	13.6.0
06-2016	CT#72	CP-160251	0458	2	F	Code of Sponsoring-Action AVP	13.6.0
06-2016	CT#72	CP-160263	0459	1	F	Correction to MCPTT priority call handling	13.6.0
06-2016	CT#72	CP-160276	0461	-	F	Inclusion of Transient failure code	13.6.0
06-2016	CT#72	CP-160274	0449	3	B	Clarification on the gate control procedure over Rx interface	14.0.0
06-2016	CT#72	CP-160274	0452	2	B	Report of modification failure over Rx reference point	14.0.0
09-2016	CT#73	CP-160461	0463	2	A	Addition of UDP/TCP port and ePDG address as untrusted WLAN location information	14.1.0
09-2016	CT#73	CP-160445	0467	1	A	Disabling/removing priority sharing for media flow	14.1.0
09-2016	CT#73	CP-160442	0469	-	A	Correction of IETF drmp draft version	14.1.0
09-2016	CT#73	CP-160458	0471	2	A	IP-CAN type and RAT type report over Rx	14.1.0
09-2016	CT#73	CP-160452	0472	-	F	Correction of the reference name for UMTS	14.1.0
09-2016	CT#73	CP-160452	0473	-	F	Gate control procedures based on the configuration in the P-CSCF	14.1.0
09-2016	CT#73	CP-160444	0475	1	A	PCRF authorization when the transfer policy has not been valid	14.1.0
09-2016	CT#73	CP-160444	0477	1	A	Transfer policy expires when the session is ongoing	14.1.0
09-2016	CT#73	CP-160456	0480	1	B	Subscription to notification of PLMN id change over Rx	14.1.0
09-2016	CT#73	CP-160463	0481	1	B	Support of sponsored data connectivity for TDF	14.1.0
12-2016	CT#74	CP-160636	0484	4	A	Remove "same media type" requirement for Priority Sharing	14.2.0
12-2016	CT#74	CP-160615	0487	1	B	Diameter Load Control Mechanism	14.2.0
12-2016	CT#74	CP-160630	0488	1	B	Support for subscription to changes to IP-CAN by P-CSCF for session setup	14.2.0
12-2016	CT#74	CP-160630	0489	5	B	Provision of EPC-level identities for IMS emergency sessions over Rx	14.2.0
12-2016	CT#74	CP-160633	0490	1	F	Inclusion of 3GPP-SGSN-MCC-MNC AVP in the AAA command	14.2.0
12-2016	CT#74	CP-160625	0491	2	B	PCC impacts due to multi-stream multiparty conferencing media handling	14.2.0
12-2016	CT#74	CP-160622	0494	1	A	Reference update draft-holmberg-dispatch-mcptt-rp-namespace	14.2.0
12-2016	CT#74	CP-160628	0495	2	B	AF triggers the activation of PCC/ADC rule with application identifier	14.2.0
12-2016	CT#74	CP-160630	0497	-	F	Enhance the description about Permanent Failures	14.2.0
12-2016	CT#74	CP-160614	0500	-	A	Correction to change IETF drmp draft version to official RFC 7944	14.2.0
12-2016	CT#74	CP-160616	0501	1	F	Diameter base protocol specification update	14.2.0
12-2016	CT#74	CP-160630	0502	6	B	Handling of multiple Rx interactions for the same media component	14.2.0
12-2016	CT#74	CP-160630	0503	1	F	Correction to the usage of Media-Component-Status AVP	14.2.0
03-2017	CT#75	CP-170081	0506	-	A	Reference update draft-holmberg-dispatch-mcptt-rp-namespace	14.3.0
03-2017	CT#75	CP-170076	0507	1	F	Handling of Vendor-Specific-Application-Id AVP	14.3.0
03-2017	CT#75	CP-170086	0509	3	F	Network provided location information retrieval at SDP offer time for mobile terminating call	14.3.0
03-2017	CT#75	CP-170086	0510	2	F	Correction to the Media-Component-Status AVP	14.3.0
03-2017	CT#75	CP-170081	0511	2	C	Pre-emption control for priority sharing	14.3.0
03-2017	CT#75	CP-170076	0512	-	F	Update instance number for the Failed-AVP in answer commands	14.3.0

History

Document history		
V14.3.0	April 2017	Publication