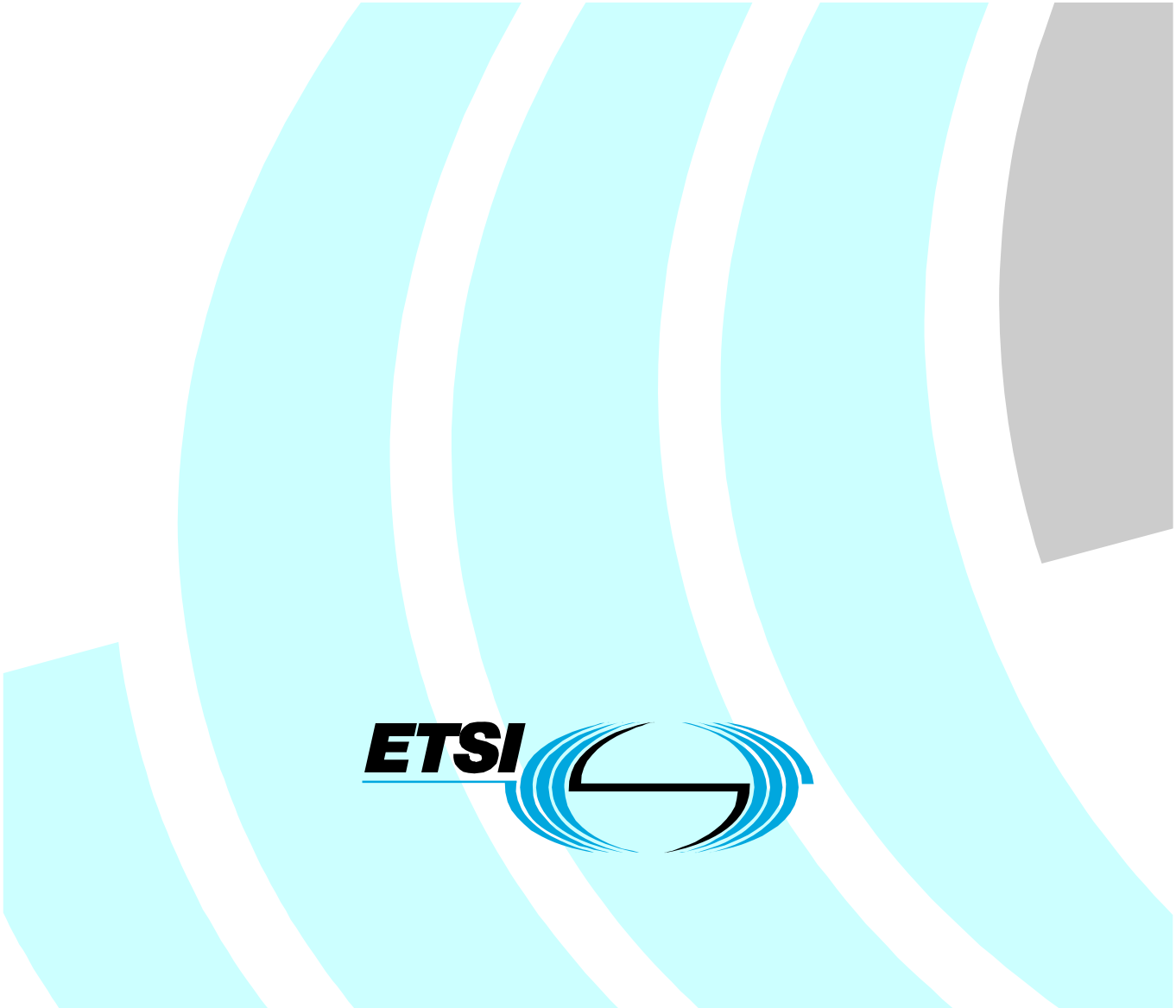
ETSI TS 183 060 V2.1.1 (2009-04)

Technical Specification

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control Subsystem (RACS); Re interface based on the DIAMETER protocol



Reference
DTS/TISPAN-03118-NGN-R2

Keywords
interface, network, system

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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights

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

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

Foreword

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

1 Scope

The present document defines a specification based on DIAMETER for use at the Re Reference Point between the TISPAN NGN Access-Resource Admission Control Function (A-RACF) and the Resource Control Enforcement Function (RCEF).

Whenever it is possible the present document specifies the requirements for this 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

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.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

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

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

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

[1] ETSI ES 282 003 (V2.0.0): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control Sub-System (RACS): Functional Architecture".

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

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

[4] IETF RFC 3309: "Stream Control Transmission Protocol (SCTP) Checksum Change".

[5] IETF RFC 3554: "On the Use of Stream Control Transmission Protocol (SCTP) with IPSec".

[6] ITU-T NGN-GSI/DOC - 127: "ITU-Telecommunication Standardization Sector, Draft Recommendation Q.rcp3.3 - Diameter Alternative Version 0.2.0".

[7] ETSI TS 129 212: "Universal Mobile Telecommunications System (UMTS); LTE; Policy and charging control over Gx reference point (3GPP TS 29.212)".

[8] IETF RFC 4006 (2005): "Diameter Credit-Control Application".

[9] ETSI TS 129 209 (V6.7.0): "Universal Mobile Telecommunications System (UMTS); Policy control over Gq interface (3GPP TS 29.209)".

[10] IETF RFC 4005 (2005): "Diameter Network Access Server Application".

[11] IANA Private Enterprise Numbers.

NOTE: See http://www.iana.org/assignments/enterprise-numbers

[12] ETSI ES 283 026 (V2.4.1): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control; Protocol for QoS reservation information exchange between the Service Policy Decision Function (SPDF) and the Access-Resource and Admission Control Function (A-RACF) in the Resource and Protocol specification" .

[13] IETF RFC 5431 (2009):"Diameter ITU-T Rw Policy Enforcement Interface Application".

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

2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area**.** For non-specific references, the latest version of the referenced document (including any amendments) applies.

[i.1] ITU-T Recommendation Q.3303.3: "Protocol at the interface between the policy decision physical entity (PD-PE) and the policy enforcement physical entity (PE-PE) (Rw interface): Diameter".

[i.2] ETSI TS 129 210: "Universal Mobile Telecommunications System (UMTS); Charging rule provisioning over Gx interface (3GPP TS 29.210)".

3 Definitions and abbreviations

3.1 Definitions

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

activation: operation of binding a Policy-Rule to a Transport Resource based on the transport resource classifier

Attribute-Value Pair (AVP): corresponds to an Information Element in a DIAMETER message

NOTE: See RFC 3588 [3].

deactivation: operation of un-binding a Policy-Rule to a Transport Resource

dynamic policy rule: subcategory of policy rules in which the ownership belongs to the A-RACF and any installation/modification/removal of the policy are performed using Re interface

Explicit Event Subscription: model for Event Subscription in which the A-RACF explicitly subscribes for the notification of particular event(s)

Implicit Event Subscription: model for Event Subscription in which the list of event(s) that needs to be reported to the A-RACF is configured on the RCEF

installation: operation of providing a new, non-existing, Policy-Rule to the RCEF

modification: operation of modifying an existing Policy-Rule(s), providing a new Policy-Rule(s), or removing an existing Policy-Rule associated with a Transport Resource

Policy Rule: QoS Policy which defines how the data traffic should be handled by the RCEF, including:

- cata traffic classification definition;
- traffic forwarding definition based on the classification;
- traffic statistics generation definition based on the classification.

Provisioned Policy Rule: subcategory of policy rules in which the ownership belongs to the provisioning system and any installation/ modification/ removal of the policy can only be triggered by the provisioned system

removal: operation of removing an existing Policy-Rule in the RCEF

Transport Resource: Network Element on which a Policy Rule needs to be activated

Transport Resource Classifier: parameter or set of parameters identifying a given Transport Resource

3.2 Abbreviations

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

ABNF	Augmented Backus-Naur Form
AF	Application Function
A-RACF	Access-Resource and Admission Control Function
AVP	Attribute-Value Pair
CCA	Credit-Control Answer
CCR	Credit-Control Request
CEA	Capabilities-Exchange-Answer
CER	Capabilities-Exchange-Request
IANA	Internet Assigned Numbers Authority
IETF	Internet Engineering Task Force
PIA	Policy-Install-Answer
PIR	Policy-Install-Request
RACF	Resource and Admission Control Function
RACS	Resource and Admission Control Subsystem
RCEF	Resource Control Enforcement Function
RFC	Request For Comments
SCTP	Stream Control Transport Protocol
SPDF	Service-based Policy Decision Function

4 Overview

The Resource Control Enforcement Function (RCEF) defined in ES 282 003 [1] performs policy enforcement functions under control of the A-RACF.

The RCEF main functions are:

- Enforcement of the policies defined by the access provider.
- Opening and closing of gates in order to allow only authorized traffic to flow; marks IP packets in accordance with the filtering criteria received from the A-RACF.

Policing of upstream and downstream traffic to ensure that the traffic remains within the authorized limits.

The traffic policies are provided by the A-RACF to the RCEF through the Re reference point.

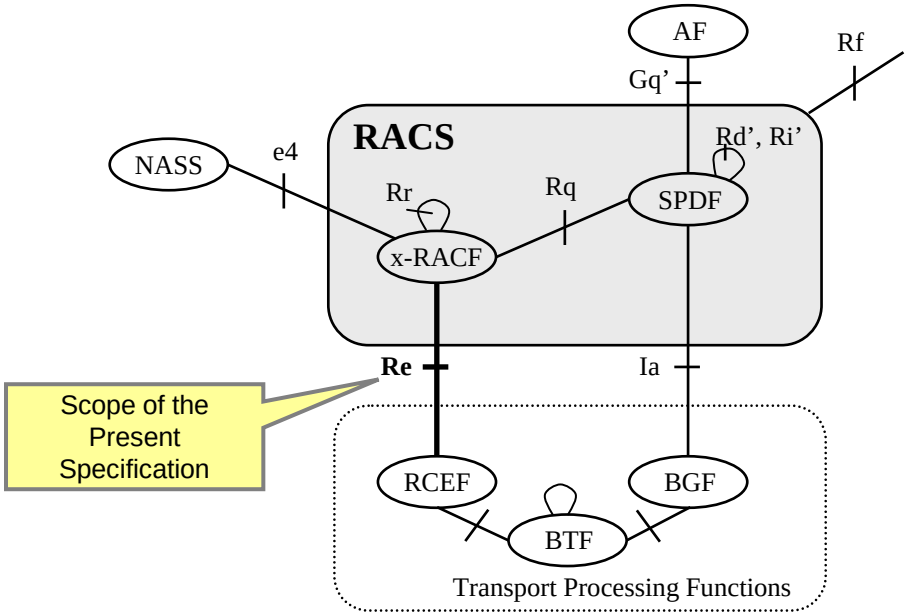


Figure 1: RACS Reference Model

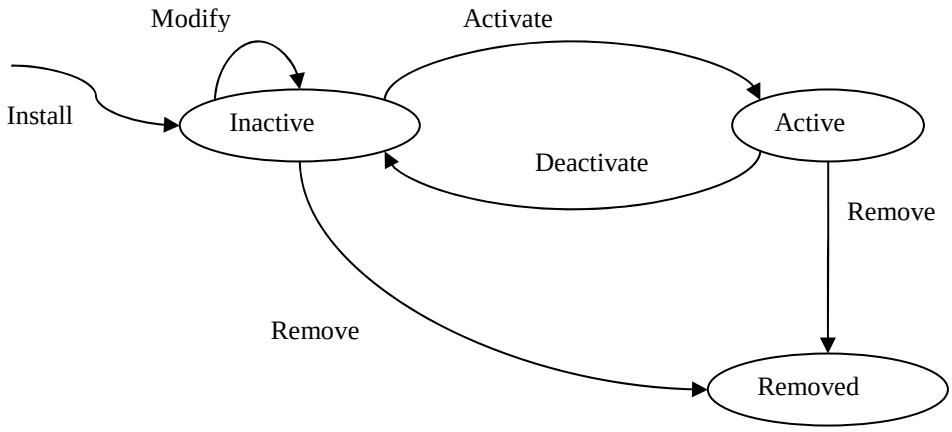
5 Procedure descriptions

5.1 General

The following clauses describe the realization of the functional procedures of the Re Reference Point (defined in the RACS specification ES 282 003 [1]) using the Diameter commands described in clause 7.1. This involves describing a mapping between the Information Elements defined in the RACS specification (ES 282 003 [1]) and DIAMETER AVPs. Procedures across the Re Reference Point can be divided into two categories:

- A-RACF initiated procedures (push mode): Policy operations are initiated by A-RACF. A-RACF decides on the appropriate traffic policies and activates those in RCEF.
- RCEF initiated procedures (pull mode): Policy operations are initiated by RCEF. In response to a request from RCEF, A-RACF shall decide on and activate the appropriate traffic policies in RCEF.

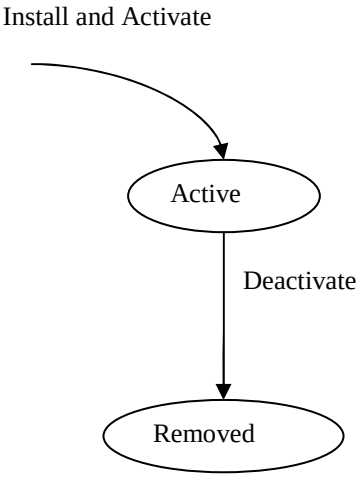
Figure 2 illustrates the policy-rule life cycle for provisioned type of policy-rules and various states the policy-rule may go through.



NOTE 1: Install/Modify/remove transitions may be initiated by the provisioning systems or the network element management system. The details of such interface is outside the scope of the present document.
NOTE 2: Activate/Deactivate transitions are initiated using the Re interface.
NOTE 3: The activation operation may result in applying quality of service [QoS] parameters and procedures defined in the policy rule to the transport resource.
NOTE 4: The deactivation process results in unbinding a policy from the network transport resource.

Figure 2: Policy rule life cycle (Provisioned)

Figure 3 illustrates the policy-rule life cycle for Dynamic type of policy-rules and varies states it may go through.



NOTE 1: Dynamic policy-rule can only exist on the RCEF if and only if it is associated with a transport resource through the interaction between A-RACF and RCEF.
NOTE 2: "Deactivate" a policy rule can be a result of:
- Modifying transport resource applied policy-rules. For detail on modification, see clause 5.2.1.3.
- Terminating the transport resources session.

NOTE 3: The activation operation may result in applying quality of service [QoS] parameters and procedures defined in the policy rule to the transport resource.

Figure 3: Policy rule life cycle [Dynamic]

5.2 A-RACF initiated procedures

5.2.1 Procedures at the A-RACF

5.2.1.1 High level description

The A-RACF is the DIAMETER Server.

The policy operations that the A-RACF may support include the installation, activation, modification, deactivation and removal of Policy Rules on the RCEF:

- In order to activate one or several Policy Rules, or to Install and Activate one or several Policy Rules, the A-RACF sends an initial Policy-Install-Request (PIR) Command containing at least one Policy Rule to the RCEF. The PI-Request-Type AVP contains the value INITIAL_REQUEST. Each Policy Rule is described in the Policy-Rule-Install AVP. The Policy-Rule-Install AVP shall contain a Policy-Rule-Definition AVP. At least one Transport Resource Classifier shall be included in the Policy-Rule-Definition AVP, in order to indicate the Transport Resource Classifier(s) associated with the Policy Rule(s).

- In order to modify Policy Rule(s) previously activated on a given Transport Resource, the A-RACF sends a PIR Command with the PI-Request-Type AVP set to the value UPDATE_REQUEST. During the Modification procedure, a Policy Rule previously activated for the Transport Resource may be modified or deactivated and removed (uninstalled).

- In order to deactivate and remove all Policy Rule(s) previously activated for given Transport Resource Classifier(s), the A-RACF sends a PIR Command to the RCEF, with the PI-Request-Type AVP set to TERMINATION_REQUEST. The Termination Request shall contain the Transport Resource Classifier(s).

The A-RACF may query the RCEF for the currently activated Policy Rules:

- Query of the supported Policy Rules.

- Query of the list of Policy Rules associated with a given Transport Resource.

- Query of the details of particular Policy Rules associated with a given Transport Resource.

5.2.1.2 Initial Policy Installation Request

The Initial Policy Installation Request is a PIR command with the PI-Request-Type AVP set to INITIAL_REQUEST.

The A-RACF shall include the Auth-Session-State AVP with the value NO_STATE_MAINTAINED (1) [3] to indicate implicitly terminated sessions.

The A-RACF may include one or several Event-Trigger AVP(s) in order to subscribe to the notification of particular event(s).

The Policy-Rule-Install AVP is used to describe the Policy Rule(s). The A-RACF shall include at least one Policy-Rule-Install AVP in the Initial PIR:

- In order to install and activate a new Policy Rule, the Policy-Rule-Definition AVP shall be used:

  - Policy-Rule-Name AVP shall be included in the Policy-Rule-Definition AVP.

  - The Flow-Status AVP shall be included in the Policy-Rule-Definition AVP. The value shall be set to ENABLED-UPLINK (0) or ENABLED-DOWNLINK (1) in order to request the activation of the corresponding Policy Rule:

    - ENABLED-UPLINK shall be used to describe a Policy Rule relative to the outgoing direction on the RCEF.

    - ENABLED-DOWNLINK shall be used to describe a Policy Rule relative to the incoming direction on the RCEF.

        - If Policy Rules for each direction need to be specified, several Policy-Rule-Definition AVPs will be included.

    - The QoS-Information AVP may be included in the Policy-Rule-Definition AVP:

        - The Max-Requested-Bandwidth-UL AVP and Traffic-Descriptor-UL AVP may be included in order to describe the bandwidth profile of a Policy-Rule-Definition AVP with a Flow-Status equal to ENABLED-UPLINK.

        - The Max-Requested-Bandwidth-DL AVP and Traffic-Descriptor-DL AVP may be included in order to describe the bandwidth profile of a Policy-Rule-Definition AVP with a Flow-Status equal to ENABLED-DOWNLINK.

        - The ToS-Traffic-Class AVP may be included in order to associate the Policy Rule with a Traffic Class:

            - The same ToS-Traffic-Class is associated with both the uplink and the downlink directions when both directions are used.

    - The Reporting-Level may be included in the Policy-Rule-Definition AVP.

    - The Precedence AVP shall be included in the Policy-Rule-Definition AVP.

- In order to activate a specific Policy Rule predefined at the RCEF, Policy-Rule-Name AVP shall be used as a reference for that Policy Rule.

- In order to activate a group of Policy Rules predefined at the RCEF, the Policy-Rule-Base-Name AVP may be used.

In order to identify the Transport Resources to which the Policy Rule applies, the A-RACF shall include at least one of the following Transport Resource Classifiers within the Policy-Rule-Definition AVP:

- Logical-Access-Id AVP in order to associate the Policy-Rule-Definition AVP(s) with a particular Logical-Access-Id.

- Physical-Access-Id AVP in order to associate the Policy-Rule-Definition AVP(s) with a particular bearer resource upon which the Policies should be enforced.

- Framed-IP-Address AVP in order to associate the Policy-Rule-Definition AVP(s) with a particular IP Session.

    - The Address-Realm AVP may be added if the Framed-IP-Address AVP is also included, in order to associate the Policy-Rule-Definition AVP(s) with a particular Globally Unique IP Address.

- Called-Station-Id AVP in order to associate the Policy-Rule-Definition AVP(s) with a particular Transport Resource on the RCEF.

- The User-Name AVP in order to associate the Policy-Rule-Definition AVP(s) with a particular End User.

- Zero, one or several Flow-Description AVP(s) may be included in the Policy-Rule-Definition AVP, in order to associate a given Policy Rule with IP Flows.

- ToS-Traffic-Class AVP in order to associate the Policy-Rule-Definition AVP(s) with a particular Traffic Class.

- The A-RACF may include one or several of these Transport Resource Classifiers.

    - In case several Transport Resource Classifiers are included, they shall match with each others.

5.2.1.3 Policy modification request

The Policy Modification Request is a PIR Command with the PI-Request-Type AVP with the value UPDATE_REQUEST.

The A-RACF shall include the Auth-Session-State AVP with the value NO_STATE_MAINTAINED (1) [3].

The A-RACF may include one or several Event-Trigger AVP(s) in order to subscribe to the notification of particular event(s). Event-Trigger AVPs that were specified in the corresponding Initial PIR or in previous Policy Modification Requests, remain valid even if they are not specified in the Policy Modification Request.

In order to remove a previously activated Policy Rule(s) associated with the Transport Resource, the A-RACF may include one or several Policy-Rule-Remove AVP(s) as main AVP(s):

- In order to remove a Policy Rule previously activated on the Transport Resource, the A-RACF shall include the Policy-Rule-Name AVP in the Policy-Rule-Remove AVP.
- In order to remove a group of Policy Rules previously activated on the Transport Resource, the A-RACF shall include the Policy-Rule-Base-Name AVP in the Policy-Rule-Remove AVP.

In order to modify Policy Rules previously activated for the Transport Resource, the A-RACF may include one or several Policy-Rule-Install AVP(s) as main AVP(s):

- The A-RACF shall include the Policy-Rule-Definition AVP:
  - The A-RACF shall include a known Policy-Rule-Name AVP.
  - The A-RACF may update the Policy-Rule-Definition.
    - In particular, the A-RACF may instruct the RCEF to deactivate and remove a Policy Rule previously associated with the Transport Resource, by changing the Flow-Status in the Policy-Rule-Definition AVP to REMOVED.

In order to install and activate new Policy Rule(s) on the RCEF, the A-RACF may include one or several Policy-Rule-Install AVP(s) as main AVP(s).

- Each Policy-Rule-Install AVP shall be specified as described in clause 5.2.1.2.
  - In particular, the A-RACF shall include a new Policy-Rule-Name AVP.

In order to activate Policy Rules pre-defined on the RCEF, the A-RACF may include one or several Policy-Rule-Install AVP(s) as main AVP(s). Each Policy-Rule-Install AVP shall be specified as follows:

- Policy-Rule-Name AVP shall be used as a reference for that Policy Rule.
- The Policy-Rule-Base-Name AVP shall not be included if the Policy-Rule-Name AVP is included.

In order to activate a group of Policy Rules pre-defined on the RCEF, the A-RACF may include one or several Policy-Rule-Install AVP(s) as main AVP(s). Each Policy-Rule-Install AVP shall be specified as follows:

- Policy-Rule-Base-Name AVP shall be used as a reference for that group of Policy Rules.
- The Policy-Rule-Name AVP shall not be included if the Policy-Rule-Base-Name AVP is included.

5.2.1.4 Policy termination request

In order to deactivate and remove all Policy Rule(s) previously activated on a Transport Resource, the A-RACF sends a PIR Command to the RCEF, with the PI-Request-Type AVP set to TERMINATION_REQUEST.

The Policy Termination-Request shall include the Transport Resource Classifier of the corresponding Transport Resource.

In the case of pre-defined Policy Rule on the RCEF (e.g. identified by Policy-Rule-Base-Name), the A-RACF may only be authorized to deactivate the pre-defined Policy Rule.

5.2.1.5 Event notification

5.2.1.5.1 Events

Depending on the policy installed, the RCEF may initiate communication with A-RACF to notify certain event occurred on the network element, according to the event A-RACF may decide to modify / remove existing policies, install new policies or escalate the event to higher layer.

Event type is identified within the CCR message according to clause 7.3.3.3.

The following is a list of supported events:

- Loss of bearer.
- Recovery of bearer.
- RCEF malfunction.
- Resource modification.

5.2.1.5.2 Event subscription

Two mechanisms are supported on the Re Reference Point:

- Explicit Event Subscription: The A-RACF may request to be notified of certain events (e.g. bearer failure) by specifying them in the Event-Trigger AVP of the Initial PIR command or of the subsequent Policy Modification Request(s).
- Implicit Event Subscription: Configuration/provisioning at the RCEF indicates which events need to be reported to the A-RACF: as such, the A-RACF may not need to explicitly subscribe for the notification of the occurrence of particular events.

5.2.1.5.3 Event notification

A CCR from the RCEF to the A-RACF indicates the occurrence of particular events (Explicit or Implicit Event Subscription).

As soon as one of the expected AVPs is missing, the A-RACF denies the entire CCR and returns a CCA command with the Result-Code AVP with the value DIAMETER_MISSING_MANDATORY_AVP [3]. This is the case if:

- either the Session-Id AVP is missing;
- or the Service-Context-Id AVP is missing;
- or Auth-Session-State AVP is missing;
- or the CC-Request-Type AVP is missing;
- or the CC-Request-Number AVP is missing;
- or the CCR command does not contain at least one Policy-Rule-Report AVP;
- or the CCR command does not include at least one of Logical-Access-Id AVP, Framed-IP-Address AVP, Called-Station-Id AVP or User-Name AVP;
- or one of Origin-Host AVP, Origin-Realm AVP, Destination-Realm AVP is missing;
- or the Event-Trigger AVP is missing;
- or the Auth-Application-Id AVP is missing.

The A-RACF determines the impacted Policy(ies) from the Policy-Rule-Name AVP or Policy-Rule-Base-Name AVP specified in the Policy-Rule-Report AVP.

The A-RACF determines the subsequent action (e.g. the A-RACF may want to remove a Policy), A-RACF may implement the subsequent action using one of the following methods:

- Respond to the CCR command with CCA command that does not include any policy alteration and then follow up with a PIR command to alter active policies (if needed) as per clause 5.2.
- Include policy alteration request within the CCA command as described below. In the case of any failure during the modification of the active policy, RCEF is required to communicate the failure to A-RACF using Event Notification as per clause 5.2.1.5.2

The A-RACF answers to the RCEF with a CCA command and includes the following AVPs:

- Session-Id, CC-Request-Type, CC-Request-Number AVPs are the same as in the corresponding CCR.
- Result-Code AVP.
- Policy-Rule-Install AVP if a Policy needs to be installed or updated, as a consequence of the event.
- Policy-Rule-Remove AVP if a Policy previously installed needs to be removed.
- Auth-Session-State AVP with the value NO_STATE_MAINTAINED (1) [3].
- In order to identify the Transport Resources to which the Policy Rule applies, the A-RACF shall include at least one of the following Classifiers:
  - Logical-Access-Id AVP in order to associate the Policy-Rule-Definition AVP(s) with a particular Logical-Access-Id.
  - Framed-IP-Address AVP in order to associate the Policy-Rule-Definition AVP(s) with a particular IP Session.
    - The Address-Realm AVP may be included if the Framed-IP-Address AVP is included, in order to associate the Policy Rule with a particular Globally Unique IP Address.
  - Called-Station-Id AVP in order to associate the Policy-Rule-Definition AVP(s) with a particular Transport Resource on the RCEF.
  - The User-Name AVP in order to associate the Policy-Rule-Definition AVP(s) with a particular End User.
  - Zero, one or several Flow-Description AVP(s) may be included in the Policy-Rule-Definition AVP, in order to associate a given Policy Rule with IP Flows.
  - ToS-Traffic-Class AVP in order to associate the Policy-Rule-Definition AVP(s) with a particular Traffic Class.
  - The A-RACF may include one or several of these Transport Resource Classifiers.
    - In case several Transport Resource Classifiers are included, they shall match with each others.

5.2.1.6 Policy Query Request

The Policy Query Request is a PIR command with the PI-Request-Type AVP set to QUERY_REQUEST.

Several Query levels are supported:

- In order to query the RCEF for the list of Policy Rules supported by the RCEF, the A-RACF shall not include any Transport Resource Classifier, and shall not include any Policy Rule.
- In order to query the RCEF for the list of Policy Rules currently associated with a given Transport Resource, the A-RACF shall include the Transport Resource Classifier, and shall not include any Policy Rule.
- In order to query the RCEF for the details about particular Policy Rule(s), the A-RACF shall include the Transport Resource Classifier and the Policy Rule(s) for which details are requested.

5.2.2 Procedures at the RCEF

5.2.2.1 High level description

The RCEF is the DIAMETER Client.

- A PIR Command with the PI-Request-Type AVP set to INITIAL_REQUEST is interpreted by the RCEF as an Initial Policy Install Request.
- A PIR Command with the PI-Request-Type AVP set to UPDATE_REQUEST is interpreted by the RCEF as a Policy Modification Request.
- A PIR Command with the PI-Request-Type AVP set to TERMINATION_REQUEST is interpreted by the RCEF as a Policy Termination Request.
- A PIR Command with the PI-Request-Type AVP set to QUERY_REQUEST is interpreted by the RCEF as a Policy Query Request.

There is no partial granting on the Re interface, i.e. the entire PIR command shall be either granted or denied.

5.2.2.2 Initial policy installation request

The RCEF interprets a PIR command with the PI-Request-Type AVP set to INITIAL_REQUEST as an Initial Policy Installation Request.

As soon as one of the expected AVPs is missing, the RCEF denies the entire PIR and returns a PIA command with the Result-Code AVP with the value DIAMETER_MISSING_MANDATORY_AVP [3]. This is the case if:

- either the Session-Id AVP is missing;
- or Auth-Session-State AVP is missing;
- or the PI-Request-Type AVP is missing;
- or the PI-Request-Number AVP is missing;
- or the PIR command does not contain at least one Policy-Rule-Install AVP;
- or one of Origin-Host AVP, Origin-Realm AVP, Destination-Host AVP, Destination-Realm AVP is missing;
- or the Auth-Application-Id AVP is missing.

If the Auth-Session-State AVP is different from NO_STATE_MAINTAINED, the RCEF returns a PIA command with:

- the Result-Code AVP with the value DIAMETER_INVALID_AVP_VALUE [3];
- a Failed-AVP AVP with a copy of the Auth-Session-State AVP.

If the RCEF can map the specified Transport Resource Classifier(s) to the corresponding Transport Resource, and Policy-Rule(s) is(are) currently active on the Transport Resource, the RCEF shall deactivate and remove all Policy-Rules currently active on the Transport Resource. In other words, the Initial PIR command over-rides anything that is currently configured by other PIR requests for the Transport Resource.

The RCEF should identify the bearer resources according to the Logical-Access-Id or the Physical-Access-Id or combination of them.

The RCEF processes each Policy-Rule-Install AVP:

- If the Policy-Rule-Name AVP is included but the corresponding Policy Rule is not pre-defined on the RCEF, and if the Policy-Rule-Definition corresponding to the Policy-Rule-Name AVP is not included, the RCEF:
  - stops processing the PIR command;
  - denies the entire PIR command and returns a PIA command with:
    - the Experimental-Result-Code AVP UNKNOWN_POLICY_RULE_NAME;
    - a Failed-AVP AVP with a copy of Policy-Rule-Name AVP.
- If the Policy-Rule-Base-Name AVP is included but the corresponding group of Policy Rules is not pre-defined on the RCEF, the RCEF:
  - stops processing the PIR command;
  - denies the entire PIR command and returns a PIA command with:
    - the Experimental-Result-Code AVP UNKNOWN_POLICY_RULE_BASE_NAME;
    - a Failed-AVP AVP with a copy of Policy-Rule-Name AVP.
- If the Policy-Rule-Name AVP is included and the corresponding Policy Rule is pre-defined on the RCEF, the RCEF attempts to activate the pre-defined Policy Rule on the Transport Resource identified by the Transport Resource Classifier.
- If the Policy-Rule-Name AVP is included and the corresponding Policy Rule is not pre-defined on the RCEF, the RCEF attempts to activate the Policy Rule described in the Policy-Rule-Definition AVP corresponding to the Policy-Rule-Name AVP:
  - If no Transport Resource Classifier is specified in the Policy-Rule-Definition AVP, the RCEF:
    - stops processing the PIR command;
    - denies the entire PIR command and returns a PIA command with:
      - the Experimental-Result-Code AVP UNKNOWN_TRANSPORT_RESOURCE;
      - the Failed-AVP AVP containing a copy of the failed Policy-Rule-Definition AVP.
  - If the Flow-Status AVP is missing from the Policy-Rule-Definition AVP, the RCEF:
    - stops processing the PIR command;
    - denies the entire PIR command and returns a PIA command with:
      - the Result-Code AVP with the value DIAMETER_MISSING_MANDATORY_AVP [3];
      - the Failed-AVP AVP with an example of the Flow-Status AVP.
  - If the Flow-Status AVP is included with a value different from ENABLED-UPLINK or ENABLED-DOWNLINK, the RCEF:
    - stops processing the PIR command;
    - denies the entire PIR command and returns a PIA command with:
      - the Result-Code AVP with the value DIAMETER_INVALID_AVP_VALUE [3];
      - the Failed-AVP AVP with a copy of the Flow-Status AVP.

- If the Flow-Status is ENABLED-UPLINK or ENABLED-DOWNLINK, the RCEF attempts to activate the corresponding Policy Rule for the corresponding Transport Resource in the appropriate direction. If this fails, the RCEF:
  - denies the entire PIR command and sends a PIA command to the A-RACF with:
    - the Experimental-Result-Code AVP set to POLICY_ACTIVATION_FAILURE;
    - a Failed-AVP AVP with a copy of Policy-Rule-Name AVP.

- If the processing of a given Policy-Rule-Install AVP fails for a reason not stated above, the RCEF:
  - stops processing the PIR command;
  - denies the entire PIR command and returns a PIA command with:
    - the Result-Code AVP with the value DIAMETER_UNABLE_TO_COMPLY [3];
    - a Failed-AVP AVP with a copy of Policy-Rule-Install AVP.

- If the Policy-Rule-Base-Name is included and the corresponding group of Policies is pre-defined on the RCEF, the RCEF attempts to activate the group of pre-defined Policy Rules for the Transport Resource. If this fails, the RCEF:
  - denies the entire PIR command and sends a PIA command to the A-RACF with:
    - the Experimental-Result-Code AVP set to POLICY_ACTIVATION_FAILURE;
    - a Failed-AVP AVP with a copy of Policy-Rule-Base-Name AVP.

The RCEF may verify if the A-RACF is allowed to perform the requested Policy Installation Request. Depending on the level of authorization of the A-RACF, the RCEF may deny the Policy Installation Request:

- If the A-RACF is not authorized to perform the Policy Installation Request on the RCEF, the RCEF returns a PIA command to the A-RACF with the Result-Code AVP set to DIAMETER_AUTHORIZATION_REJECTED [3].

- If the A-RACF is not authorized to perform the Policy Installation Request for the specified Transport Resource Classifier, the RCEF denies the entire PIR command and returns a PIA command to the A-RACF with:
  - the Experimental-Result-Code AVP set to AUTHORIZATION_REJECTED_FOR_TRANSPORT_RESOURCE;
  - at least one Failed-AVP AVP(s). Each Failed-AVP AVP shall contain a copy of a specified Transport Resource Classifier.

- If the A-RACF is not authorized to perform the Policy Installation Request for the specified Policy-Rule-Name AVP, the RCEF denies the entire PIR command and returns a PIA command to the A-RACF with:
  - the Experimental-Result-Code AVP set to AUTHORIZATION_REJECTED_FOR_POLICY_RULE_NAME;
  - a Failed-AVP AVP with a copy of the specified Policy-Rule-Name AVP.

- If the A-RACF is not authorized to perform the Policy Installation Request for the specified Policy-Rule-Base-Name AVP, the RCEF denies the entire PIR command and returns a PIA command to the A-RACF with:
  - the Experimental-Result-Code AVP set to AUTHORIZATION_REJECTED_FOR_POLICY_RULE_BASE_NAME;
  - a Failed-AVP AVP with a copy of the specified Policy-Rule-Base-Name AVP.

If the Policy Installation Request succeeds, the RCEF:

- returns a PIR command to the A-RACF with the Result-Code AVP set to DIAMETER_SUCCESS [3].

5.2.2.3 Policy modification request

The RCEF interprets a PIR command the PI-Request-Type AVP set to UPDATE_REQUEST as a Policy Modification Request.

As soon as one of the expected AVPs is missing, the RCEF denies the entire PIR and returns a PIA command with the Result-Code AVP with the value DIAMETER_MISSING_MANDATORY_AVP [3]. This is the case if:

- either the Session-Id AVP is missing;
- or Auth-Session-State AVP is missing;
- or the PI-Request-Type AVP is missing;
- or the PI-Request-Number AVP is missing;
- or the PIR command does not include at least one of Transport Resource Classifiers, i.e. one of Logical-Access-Id AVP, Framed-IP-Address AVP, Called-Station-Id AVP or User-Name AVP;
- or the Auth-Application-Id AVP is missing.

The RCEF may perform the following Modification Operations:

- activate a pre-defined Policy Rule for the Transport Resource, not yet activated on the Transport Resource;
- install and activate a new Policy Rule on the Transport Resource;
- modify Policy Rule(s) previously installed and activated on the Transport Resource;
- deactivate and remove the Policy Rule(s) previously activated on the Transport Resource. The removal of the policy shall depend on the policy-rule type [Dynamic / Provisioned] where the A-RACF initiated transactions can only result in removing "dynamic" policy rules.

The RCEF processes each Policy-Rule-Install AVP:

- If the Policy-Rule-Definition is included and if Transport Resource Classifier(s) are included: as soon as the RCEF cannot map one of the specified Transport Resource Classifier(s) to the corresponding Transport Resource, or as soon as specified Transport Resource Classifiers do not match with each others, the RCEF:
  - stops processing the PIR command;
  - denies the entire PIR command and returns a PIA command with:
    - the Experimental-Result-Code AVP UNKNOWN_TRANSPORT RESOURCE.
  - failed-AVP AVP(s) with a copy of the failed Transport Resource Classifier(s).
- If the Policy-Rule-Name AVP is included but the corresponding Policy Rule is not known yet on the RCEF (i.e. not pre-defined on the RCEF and not installed in previous commands, even for other Transport Resources), and if the Policy-Rule-Definition AVP corresponding to the Policy-Rule-Name AVP not included, the RCEF:
  - stops processing the PIR command and falls back to the previously installed state.
  - denies the entire PIR command and returns a PIA command to the A-RACF with:
    - the Experimental-Result-Code AVP UNKNOWN_POLICY_RULE_NAME;
    - a Failed-AVP AVP with a copy of Policy-Rule-Name AVP.

- If the Policy-Rule-Base-Name AVP is included but the corresponding group of Policy Rules is not known yet on the RCEF (i.e. not pre-defined on the RCEF and not installed in previous commands, even for other Transport Resources), the RCEF:
  - stops processing the PIR command and falls back to the previously installed state;
  - denies the entire PIR command and returns a PIA command with:
    - the Experimental-Result-Code AVP UNKNOWN_POLICY_RULE_BASE_NAME;
    - a Failed-AVP AVP with a copy of Policy-Rule-Base-Name AVP.
- If the Policy-Rule-Name AVP is included and the corresponding Policy Rule is activated for the Transport Resource, the RCEF attempts to modify the Policy Rule:
  - If the Flow-Status AVP is missing from the Policy-Rule-Definition AVP, the RCEF:
    - stops processing the PIR command and falls back to the previously installed state;
    - denies the entire PIR command and returns a PIA command to the A-RACF with:
      - the Result-Code AVP with the value DIAMETER_MISSING_MANDATORY_AVP [3];
      - the Failed-AVP AVP with an example of the Flow-Status AVP.
  - If the Flow-Status AVP is different from ENABLED-UPLINK or ENABLED-DOWNLINK or REMOVED, the RCEF:
    - stops processing the PIR command and falls back to the previously installed state;
    - denies the entire PIR command and returns a PIA command to the A-RACF with:
      - the Result-Code AVP with the value DIAMETER_INVALID_AVP_VALUE [3];
      - a Failed-AVP AVP with a copy of the Flow-Status AVP;
      - a Failed-AVP AVP with a copy of the Policy-Rule-Name AVP.
  - If the modification of the Policy Rule fails for a reason not stated above, the RCEF:
    - stops processing the PIR command and falls back to the previously installed state;
    - denies the entire PIR command and returns a PIA command to the A-RACF with:
      - the Experimental-Result-Code AVP with the value POLICY_MODIFICATION_FAILURE;
      - a Failed-AVP AVP with a copy of the Policy-Rule-Name AVP.
  - If the Flow-Status AVP is modified to REMOVED, the RCEF deactivates and removes the corresponding Policy Rule for the Transport Resource.
- If the Policy-Rule-Name AVP is included and the corresponding Policy Rule is not activated yet on the Transport Resource, the RCEF attempts to install and activate the new Policy Rule described in the Policy-Rule-Definition AVP corresponding to the Policy-Rule-Name AVP:
  - Installation of a new policy is described in clause 5.2.2.1.

The RCEF may verify if the A-RACF is allowed to perform the requested Policy Modification Request. Depending on the level of authorization of the A-RACF, the RCEF may deny the Policy Modification Request:

- If the A-RACF is not authorized to perform the Policy Modification Request on the RCEF, the RCEF returns a PIA command to the A-RACF with the Result-Code AVP set to DIAMETER_AUTHORIZATION_REJECTED [3].

- If the A-RACF is not authorized to perform the Policy Modification Request for the specified Transport Resource Classifier, the RCEF returns denies the entire PIR command and a PIA command to the A-RACF with:
  - the Experimental-Result-Code AVP set to AUTHORIZATION_REJECTED_FOR_TRANSPORT_RESOURCE;
  - at least one Failed-AVP AVP(s). Each Failed-AVP AVP shall contain a copy of a specified Resource Classifier.
- If the A-RACF is not authorized to perform the Policy Modification Request for the specified Policy-Rule-Name AVP, the RCEF denies the entire PIR command and returns a PIA command to the A-RACF with:
  - the Experimental-Result-Code AVP set to AUTHORIZATION_REJECTED_FOR_POLICY_RULE_NAME;
  - a Failed-AVP AVP with a copy of the specified Policy-Rule-Name AVP.
- If the A-RACF is not authorized to perform the Policy Modification Request for the specified Policy-Rule-Base-Name AVP, the RCEF denies the entire PIR command and returns a PIA command to the A-RACF with:
  - the Experimental-Result-Code AVP set to AUTHORIZATION_REJECTED_FOR_POLICY_RULE_BASE_NAME;
  - a Failed-AVP AVP with a copy of the specified Policy-Rule-Base-Name AVP.

If the Policy Modification Request fails for one reason not stated above, the RCEF:

- stops processing the PIR command and falls back to the previously installed state;
- denies the entire PIR command and returns a PIA command with:
  - the Result-Code AVP with the value DIAMETER_UNABLE_TO_COMPLY [3].

If the Policy Modification Request succeeds, the RCEF:

- returns a PIR command to the A-RACF with the Result-Code AVP set to DIAMETER_SUCCESS [3].

5.2.2.4 Policy termination request

The RCEF interprets a PIR command with the PI-Request-Type AVP set to TERMINATION_REQUEST as a Policy Termination Request.

If the RCEF cannot map the specified Transport Resource Classifier(s) to the corresponding Transport Resource, or if several Transport Resource Classifiers are specified but they do not match with each others, the RCEF:

- stops processing the PIR command;
- denies the entire PIR command and returns a PIA command with:
  - the Experimental-Result-Code AVP UNKNOWN_TRANSPORT RESOURCE;
  - at least one Failed-AVP AVP. Each Failed-AVP AVP shall contain a copy of one specified Transport Resource Classifier.

Otherwise the RCEF attempts to deactivate and remove all Policy Rules currently activated on the Transport Resource. The removal of the policy shall depend on the policy-rule type [Dynamic/Provisioned] where the A-RACF initiated transactions can only result in removing "dynamic" policy rules.

The RCEF may verify if the A-RACF is allowed to perform the requested Policy Termination Request. Depending on the level of authorization of the A-RACF, the RCEF may deny the Policy Termination Request:

- If the A-RACF is not authorized to perform the Policy Termination Request on the RCEF, the RCEF returns a PIA command to the A-RACF with the Result-Code AVP set to DIAMETER_AUTHORIZATION_REJECTED [3].
- If the A-RACF is not authorized to perform the Policy Termination Request for the specified Transport Resource Classifier, the RCEF returns denies the entire PIR command and a PIA command to the A-RACF with:
  - the Experimental-Result-Code AVP set to AUTHORIZATION_REJECTED_FOR_TRANSPORT_RESOURCE;
  - at least one Failed-AVP AVP(s). Each Failed-AVP AVP shall contain a copy of a specified Transport Resource Classifier.
- If the A-RACF is not authorized to perform the Policy Termination Request for the specified Policy-Rule-Name AVP, the RCEF denies the entire PIR command and returns a PIA command to the A-RACF with:
  - the Experimental-Result-Code AVP set to AUTHORIZATION_REJECTED_FOR_POLICY_RULE_NAME;
  - a Failed-AVP AVP with a copy of the specified Policy-Rule-Name AVP.
- If the A-RACF is not authorized to perform the Policy Termination Request for the specified Policy-Rule-Base-Name AVP, the RCEF denies the entire PIR command and returns a PIA command to the A-RACF with:
  - the Experimental-Result-Code AVP set to AUTHORIZATION_REJECTED_FOR_POLICY_RULE_BASE_NAME;
  - a Failed-AVP AVP with a copy of the specified Policy-Rule-Base-Name AVP.

If the Policy Termination Request fails for a reason not stated above, the RCEF:

- stops processing the PIR command and falls back to the previously installed state;
- denies the entire PIR command and returns a PIA command to the A-RACF with:
  - the Result-Code AVP with the value DIAMETER_UNABLE_TO_COMPLY [3].

If the Policy Termination Request succeeds, the RCEF:

- returns a PIR command to the A-RACF with the Result-Code AVP set to DIAMETER_SUCCESS [3].

5.2.2.5 Event notification

If one of the events implicitly or explicitly subscribed by the A-RACF occurs, the RCEF shall send an unsolicited CCR message to the A-RACF for Event Notification.

- The RCEF shall include the Session-Id AVP of the impacted Policy Session.
- The RCEF shall include the Service-Context-Id AVP with the value 461.

NOTE: Content of the Service-Context-Id AVP should be specified, in compliance with RFC 4006 [8].

- The RCEF shall include the CC-Request-Type with the value UPDATE_REQUEST (2) defined in [8].
- The RCEF shall include the CC-Request-Number with the value 0 as advised in [8].
- The RCEF may include the Transport Resource Classifier (i.e. User-Name AVP, Logical-Access-Id AVP, Framed-IP-Address AVP, Called-Station-Id AVP) in order to identify the impacted Transport Resource.

- The RCEF may include the Event-Timestamp AVP in order to report the moment the event occurred (in seconds since January 1, 1900 00:00 UTC).
- The RCEF shall include at least one Event-Trigger AVP in order to indicate which particular event(s) has (have) occurred.
- The RCEF shall include at least one Policy-Rule-Report AVP in order to indicate which Policy(ies) is (are) impacted by the corresponding Event(s). Multiple instances of Policy-Rule-Report AVPs shall be used in the case it is required to report different Policy-Rule-Status values for different groups of rules within the same DIAMETER command. The Policy-Rule-Report AVP shall be specified as follows:
  - The Policy-Rule-Name AVP shall identify a particular Policy impacted by the event.
  - Policy-Rule-Base-Name AVP shall be used instead of the Policy-Rule-Name AVP if the event impacts a group of policies predefined at the RCEF.
  - The Policy-Rule-Status AVP shall have one of the values specified in clause 7.3.3.3.

5.2.2.6 Policy Query Request

The RCEF interprets a PIR command with the PI-Request-Type AVP set to QUERY_REQUEST as a Policy Query Request.

As soon as one of the expected AVPs is missing, the RCEF denies the entire PIR and returns a PIA command with the Result-Code AVP with the value DIAMETER_MISSING_MANDATORY_AVP [3]. This is the case if:

- either the Session-Id AVP is missing;
- or the PI-Request-Type AVP is missing;
- or the PI-Request-Number AVP is missing;
- or one of Origin-Host AVP, Origin-Realm AVP, Destination-Host AVP, Destination-Realm AVP is missing;
- or the Auth-Application-Id AVP is missing.

The information returned by the RCEF is function of the AVPs specified in the PIR command:

- If no Transport Resource Classifier and no Policy-Rule-Name AVP is included, the RCEF:
  - returns a PIA command to the A-RACF with:
    - the Result-Code AVP set to DIAMETER_SUCCESS [3];
    - the set of Policy-Rule-Name AVPs and Policy-Rule-Base-Name AVPs known by the RCEF.
- If no Transport Resource Classifier is included, but a Policy-Rule-Name AVP is included, the RCEF:
  - stops processing the entire PIR command;
  - denies the entire PIR command and returns a PIA command to the A-RACF with the Experimental-Result-Code AVP set to UNKNOWN_TRANSPORT_RESOURCE.
- If Transport Resource Classifier(s) is(are) specified, but no Policy-Rule-Name or Policy-Rule-Base-Name AVP is included:
  - If the RCEF cannot map the specified Transport Resource Classifier(s) to the corresponding Transport Resource, or if several Transport Resource Classifiers are specified but they do not match with each others, the RCEF:
    - stops processing the PIR command;

        - denies the entire PIR command and returns a PIA command with:
            - the Experimental-Result-Code AVP UNKNOWN_TRANSPORT_RESOURCE;
            - at least one Failed-AVP AVP. Each Failed-AVP AVP shall contain a copy of one specified Transport Resource Classifier.
    - Otherwise, the RCEF returns a PIA command to the A-RACF with:
        - the Result-Code AVP set to DIAMETER_SUCCESS [3];
        - the set of Policy-Rule-Name AVPs and Policy-Rule-Base-Name AVPs currently activated for the corresponding Transport Resource Classifier(s).

- If Transport Resource Classifier(s) is(are) specified, and Policy-Rule-Name AVP(s) or Policy-Rule-Base-Name AVP(s) are included:
    - If the RCEF cannot map the specified Transport Resource Classifier(s) to the corresponding Transport Resource, or if several Transport Resource Classifiers are specified but they do not match with each others:
        - the RCEF stops processing the PIR command;
        - the RCEF denies the entire PIR command and returns a PIA command with:
            - the Experimental-Result-Code AVP UNKNOWN_TRANSPORT RESOURCE;
            - at least one Failed-AVP AVP. Each Failed-AVP AVP shall contain a copy of one specified Transport Resource Classifier.
    - Otherwise, as soon as one of the specified Policy-Rule-Name AVP(s) or one of the specified Policy-Rule-Base-Name AVP(s) is not associated with one of the specified Transport Resource Classifier(s):
        - the RCEF stops processing the PIR command;
        - the RCEF denies the entire PIR command and returns a PIA command with:
            - the Experimental-Result-Code AVP with the value UNKNOWN_POLICY_RULE_FOR_TRANSPORT RESOURCE (for failed Policy-Rule-Name AVP) or UNKNOWN_POLICY_RULE_BASE_NAME_FOR_TRANSPORT RESOURCE (for failed Policy-Rule-Base-Name AVP);
            - a Failed-AVP AVP with a copy of the failed Policy-Rule-Name AVP or Policy-Rule-Base-Name AVP;
            - a Failed-AVP AVP per with a copy of the failed Transport Resource Classifier.
    - Otherwise, the RCEF returns a PIA command to the A-RACF with:
        - the Result-Code AVP set to DIAMETER_SUCCESS [3];
        - The Policy-Rule-Definition AVP(s) corresponding to each Policy-Rule-Name AVP, or to each Policy Rule that is part of a specified Policy-Rule-Base-Name AVP.

The RCEF may verify if the A-RACF is allowed to perform the requested Query. Depending on the level of authorization of the A-RACF, the RCEF may deny the Policy Query Request:

- If the A-RACF is not authorized to Query the RCEF, the RCEF returns a PIA command to the A-RACF with the Result-Code AVP set to DIAMETER_AUTHORIZATION_REJECTED [3].
- If the A-RACF is not authorized to Query for the specified Transport Resource Classifier, the RCEF returns a PIA command to the A-RACF with the Experimental-Result-Code AVP set to AUTHORIZATION_REJECTED_FOR_TRANSPORT_RESOURCE.

- If the A-RACF is not authorized to Query for the specified Policy-Rule-Name AVP, the RCEF returns a PIA command to the A-RACF with the Experimental-Result-Code AVP set to AUTHORIZATION_REJECTED_FOR_POLICY_RULE_NAME.

- If the A-RACF is not authorized to Query for the specified Policy-Rule-Base-Name AVP, the RCEF returns a PIA command to the A-RACF with the Experimental-Result-Code AVP set to AUTHORIZATION_REJECTED_FOR_POLICY_RULE_BASE_NAME.

If the Policy Query Request fails for a reason not stated above, the RCEF:

- stops processing the PIR command and falls back to the previously installed state;

- denies the entire PIR command and returns a PIA command to the A-RACF with:

  - the Result-Code AVP with the value DIAMETER_UNABLE_TO_COMPLY [3].

5.3 RCEF initiated procedures

RCEF initiated procedures ("pull mode") apply when RCEF receives a request for transport resources via transport signalling. RCEF will employ a CC-Request to request a policy operation by A-RACF. A-RACF will respond to a CC-Request with a CC-Answer.

5.3.1 Procedures at the A-RACF

5.3.1.1 High level description

The A-RACF will receive a CCR command from the RCEF in certain circumstances (e.g. Pull mode) to request a resource reservation. The CCR command will also be received in order to modify or terminate this resource reservation:

- A CCR command with the CC-Request-Type AVP set to INITIAL_REQUEST is interpreted as an initial pull reservation request, and is requesting authorization and resource reservation.

- A CCR command with the CC-Request-Type AVP set to UPDATE_REQUEST is interpreted as a session modification of an existing resource reservation.

- A CCR command with the CC-Request-Type AVP set to TERMINATION_REQUEST is interpreted as session termination and release of existing resource reservation.

It is not permitted to partially grant a CCR. The entire CCR shall be granted or denied.

5.3.1.2 Traffic policy activation request

On receipt of a CC-Request from RCEF with CC-Request-type AVP set to "INITIAL_REQUEST", the A-RACF will either create corresponding service control state or associate the request with already existing service control state and initiate the attachment of a traffic policy to the transport resource(s) described by the Transport Resource Classifier(s) contained within the request. Receipt of a CC-Request with CC-Request-type AVP set to "INITIAL_REQUEST" will replace all earlier traffic policies which have been attached to the transport resources described by the Transport Resource Classifier(s).

In response to the initial CC-Request, the A-RACF shall send a CC-Answer command to activate the corresponding traffic policy or policies in RCEF.

5.3.1.3 Traffic policy modification request

On receipt of a CC-Request with the CC-Request-Type AVP set to the value "UPDATE_REQUEST", the A-RACF shall identify the corresponding service control state using the Transport Resource Classifier(s). A-RACF decides on the attachment of the appropriate new or updated traffic policies and sends a CC-Answer command to the RCEF containing the new or updated traffic policies.

Depending on the value of the Flow-Status AVP received from RCEF through the CC-Request, the A-RACF shall interpret the session modification as one of the following:

- modification of requested resources;
- commitment of requested resources;
- removal of requested resources.

The A-RACF shall interpret the presence of the Policy-Update-Request AVP as a request to modify resources associated to the related Policy-Rule. The actual modification depends on the received QoS-information parameters value:

- If the QoS-Information AVP contains a Max-Requested-Bandwidth-DL or Max-Requested-Bandwidth-UL AVP set to zero, the A-RACF interprets the received command as a request to release the associated resources. This has however no impact on the Policy-Rule-Status.
- If the QoS-Information AVP contains a Max-Requested-Bandwidth-DL or Max-Requested-Bandwidth-UL AVP set to FFFFFFFF, the A-RACF interprets the command as a request to modify the current bandwidth and determines the bandwidth to be allocated based on the Policy-Rule-Name.

5.3.1.4 Traffic policy deactivation request

Traffic policy deactivation may be initiated by the RCEF through a CC-Request with CC-Request-Type AVP set to the value "TERMINATION_REQUEST". The A-RACF shall identify the corresponding service control state using the Transport Resource Classifier(s). A-RACF shall respond with a CC-Answer to RCEF including the Policy-Rule-Remove AVP. If a single traffic policy is to be removed, A-RACF shall include the Policy-Rule-Name AVP identifying the appropriate traffic policy to be deactivated within the Policy-Rule-Remove AVP. If multiple traffic policies are to be removed, A-RACF shall include the Policy-Rule-Base-Name AVP identifying the appropriate traffic policies to be deactivated within the Policy-Rule-Remove AVP. After completing the CC-Answer, A-RACF may decide to remove the corresponding service control state.

5.3.2 Procedures at the RCEF

5.3.2.1 High level description

The RCEF will send a CCR command to request a resource reservation from the A-RACF via the Re reference when the RCEF receives a trigger. The CCR indicates that a change of policies may need to be applied to a particular transport resource identified by the logical access id or the user-name.

The RCEF will receive a reply in the CCA command which contains the Policy Rules to be applied.

The policy operations on the RCEF may include the installation, activation, modification, deactivation and removal of traffic policies.

5.3.2.2 Traffic policy activation request

In order to activate one or several traffic policies the RCEF sends an initial CC-Request to A-RACF. The CC-Request-type AVP contains the value "INITIAL_REQUEST". The A-RACF is expected to respond with a CC-Answer. Each traffic policy is described in the Policy-Rule-Install AVP. The Policy-Rule-Install AVP shall contain a Policy-Rule-Definition AVP. At least one Transport Resource Classifier shall be included in the Policy-Rule-Definition AVP, in order to indicate the Transport Resource Classifier(s) associated with the traffic policy. On receipt of the CC-Answer, the RCEF will either:

- activate a pre-defined traffic policy. In this case the Policy-Rule-Name AVP shall contain a reference to the traffic policy to be attached to the resource. The traffic policy shall be known by the RCEF, or
- activate a set of pre-defined traffic policies. In this case the Policy-Rule-Base-Name AVP shall contain a reference to the traffic policies to be attached to the resource. The traffic policies shall be known by the RCEF, or

- activate a traffic policy not previously defined. In this case the Policy-Rule-Definition AVP shall be included within the Policy-Rule-Install AVP. The Policy-Rule-Definition AVP shall contain a QoS-Information AVP describing the QoS parameters of the traffic policy which is to be attached to the resource.

5.3.2.3 Traffic policy modification request

In order to modify traffic policies previously activated on transport resources described by Transport Resource Classifier(s), the RCEF sends a CC-Request Command with the CC-Request-Type AVP set to the value "UPDATE_REQUEST". During the modification procedure, a traffic policy previously activated for a set of Transport Resource Classifier(s) may be modified or deactivated.

5.3.2.4 Traffic Policy Deactivation Request

In order to deactivate all traffic policies previously activated for given Transport Resource Classifier(s), the RCEF sends a CC-Request Command to the A-RACF, with the CC-Request-Type AVP set to "TERMINATION_REQUEST".

On receipt of the CC-Answer, the RCEF will:

- deactivate the traffic policy referenced by the Policy-Rule-Name AVP - if the Policy-Rule-Name AVP is included in the Policy-Rule-Remove AVP of the CC-Answer;

- deactivate the traffic policies referenced by the Policy-Rule-Base-Name AVP - if the Policy-Rule-Base-Name AVP is included in the Policy-Rule-Remove AVP of the CC-Answer.

6 Use of the DIAMETER base protocol

The DIAMETER Base Protocol defined by RFC 3588 [3] shall apply, with the clarifications listed in the present document.

6.1 Securing DIAMETER messages

For secure transport of DIAMETER messages, IPSec may be used. Guidelines on the use of SCTP with IPSec can be found in RFC 3554 [5].

The RCEF may verify the identity of the A-RACF issuing during the Capabilities Exchange Request procedure.

The RCEF may verify if the A-RACF that issues a PIR command is allowed to do so, based on:

- The Identity of the A-RACF.

- The Type of PIR Command.

- The content of the PIR Command.

- Any combination of the above.

6.2 Accounting functionality

Accounting functionality (Accounting Session State Machine, related command codes and AVPs) is not used on the Re Reference Point.

6.3 Use of sessions

DIAMETER sessions are implicitly terminated. As such, the Abort-Session-Request (ASR) and Session-Termination-Request (STR) defined in [3] are not used.

NOTE: The A-RACF and RCEF obviously maintain state, but this state is not associated with the Session-Id.

The A-RACF shall include in its Requests the Auth-Session-State AVPs set to the value NO_STATE_MAINTAINED (1) [3].

The Session-Id AVP is not meaningful on the Re interface. This means that the RCEF shall not maintain associations between the activated Policy Rules and the Session-Id AVP.

For this reason, the RAR/RAA and STR/STA commands defined in the DIAMETER base protocol are not used in the context of the present document.

Anyway, the Session-Id AVP shall be included in all DIAMETER commands that conform to the present document. The value of the Session-Id shall be chosen by the A-RACF.

6.4 Transport protocol

DIAMETER messages over the Re interface shall make use of SCTP RFC 2960 [2] and shall utilize the new SCTP checksum method specified in RFC 3309 [4].

6.5 Routing considerations

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

Both the Destination-Realm and Destination-Host AVPs shall be present in the Request from the A-RACF to the RCEF. The A-RACF may obtain the Destination-Host AVPs to use in Requests towards the RCEF from NASS user location information retrieved from the CLF or from configuration data.

Requests initiated by the RCEF towards an A-RACF may include both Destination-Host and Destination-Realm AVPs. The RCEF may obtain the Destination-Host AVPs to use in Requests towards the A-RACF from Requests received earlier from the A-RACF, or from configuration data.

6.6 Advertising Application support

The Capabilities-Exchange-Request (CER) and Capabilities-Exchange-Answer (CEA) are defined in RFC 3588 [3].

The A-RACF and RCEF shall advertise support of the Re specific application by including the following AVPs:

- Vendor-Specific-Application-Id grouped AVPs containing the following AVPs:
  - Auth-Application-Id AVPs with the value (16777253);
  - Vendor-Id AVPs with the value AVPs (13019).
- Supported-Vendor-Id AVP with the value ETSI (13019) to indicate support of ETSI AVPs.
- Supported-Vendor-Id AVP with the value 3GPP (10415) to indicate support of 3GPP AVPs.
- Supported-Vendor-Id AVP with the value ITU-T (11502) to indicate support of ITU-T AVPs.

NOTE: The Vendor-Id AVPs included in CER and CEA commands that is not included in the Vendor-Specific-Application-Id AVPs as described above indicates the manufacturer of the DIAMETER node as per RFC 3588 [3].

7 DIAMETER application

The DIAMETER Base Protocol as specified in RFC 3588 [3] is used to support information transfer on the Re interface.

RFC 3588 [3] shall apply except as modified by the defined support of the methods and the defined support of the commands and AVPs, result and event codes specified in clause 5. Unless otherwise specified, the procedures (including error handling and unrecognized information handling) are unmodified.

The present document uses the DIAMETER application number (16777253).

7.1 Commands

The following commands are used:

Table 1: Command-Code values

Command-Name	Abbreviation	Code	Defined In	See clause
Policy-Install-Request	PIR	315	[6], [13]	7.1.1
Policy-Install-Answer	PIA	315	[6], [13]	7.1.2
Credit-Control-Request	CCR	272	[8]	7.1.3
Credit-Control-Answer	CCA	272	[8]	7.1.4

AVPs defined in [6] and not used in the present document are not represented in the below clauses. If received, these AVPs shall be ignored by the A-RACF and the RCEF.

AVPs added in the ABNF of the commands are represented in bold.

7.1.1 Policy-Install-Request (PIR) command

The Policy-Install-Request (PIR) command, indicated by the Command-Code field set to 315 and the "R" bit set in the Command Flags field, is sent by the A-RACF to the RCEF in order to install policies in the RCEF. This command is defined in [6] and used with additional AVPs defined in the present document.

Message Format:

```
< Policy-Install-Request > ::=   < Diameter Header: 315, REQ, PXY>
            < Session-Id >
            { Auth-Application-Id }
            { Origin-Host }
            { Origin-Realm }
            { Destination-Realm }
            { Destination-Host }
            { PI-Request-Type }
            { PI-Request-Number }
            [ Origin-State-Id ]
            [ Auth-Session-State ]
        *   [ Event-Trigger ]
        *   [ Policy-Rule-Remove ]
        *   [ Policy-Rule-Install ]
            [ User-Name ]
            [ Logical-Access-Id ]
            [ Framed-IP-Address ]
            [ Address-Realm ]
            [ Called-Station-ID ]
            [ ToS-Traffic-Class ]
        *   [ Proxy-Info ]
        *   [ Route-Record ]
        *   [ AVP ]
```

7.1.2 Policy-Install-Answer (PIA) command

The Policy-Install-Answer (PIA) command, indicated by the Command-Code field set to 315 and the "R" bit cleared in the Command Flags field, is sent by a server in response to Policy-Install-Request command. This command is defined in [6] and used with additional AVPs defined in the present document.

Message Format:

```
<PI-Answer> ::= < Diameter Header: 315, PXY>
            < Session-Id >
            { Origin-Host }
            { Origin-Realm }
            { PI-Request-Type }
            { PI-Request-Number }
            [ Result-Code ]
        *   [ Policy-Rule-Report ]
            [ Experimental-Result ]
            [ Origin-State-Id ]
            [ Error-Message ]
            [ Error-Reporting-Host ]
        *   [ Policy-Rule-Name ]
        *   [ Policy-Rule-Base-Name ]
        *   [ Policy-Rule-Definition ]
        *   [ Failed-AVP ]
        *   [ Proxy-Info ]
        *   [ AVP ]
```

7.1.3 CC-Request (CCR) command

The CCR command, indicated by the Command-Code field set to 272 and the 'R' bit set in the Command Flags field, is sent by the RCEF to the A-RACF in order to report the occurrence of particular event or to request activation, modification, or deactivation of traffic policies. If the Traffic-Flow AVP is used at the command level in the CCR command, the Flow-Description AVP, the Flow-Status AVP and the QoS-Information AVP shall not be used in the CCR command.

Message Format:

```
<CC-Request> ::= < Diameter Header: 272, REQ, PXY >
                 < Session-Id >
                 { Origin-Host }
                 { Origin-Realm }
                 { Destination-Realm }
                 { Auth-Application-Id }
                 { Service-Context-Id }
                 { CC-Request-Type }
                 { CC-Request-Number }
                 [ Destination-Host ]
                 [ User-Name ]
                 [ Origin-State-Id ]
                 [ Event-Timestamp ]
                 [ Auth-Session-State ]
                 [ Termination-Cause ]
                 [ Called-Station-ID ]
                 [ Logical-Access-Id ]
                 [ Physical-Access-ID ]
             *   [ Traffic-Flow ]
             *   [ Flow-Description ]
                 [ Flow-Status ]
                 [ QoS-Information ]
                 [ Framed-IP-Address ]
                 [ Address-Realm ]
             *   [ Policy-Rule-Report]
```

* [Policy-Update-Request]
* [Event-Trigger]
* [Proxy-Info]
* [Route-Record]
* [AVP]

7.1.4 CC-Answer (CCA) Command

The Credit-Control-Answer message (CCA) is indicated by the command-code field being set to 272 and the 'R' bit being cleared in the Command Flags field. It is sent by the A-RACF to the RCEF in answer to the CCR..

Message Format:

<CC-Answer> ::= < Diameter Header: 272, PXY >
< Session-Id >
{ Origin-Host }
{ Origin-Realm }
{ Auth-Application-Id }
{ Result-Code }
{ CC-Request-Type }
{ CC-Request-Number }
[User-Name]
[Framed-IP-Address]
[Address-Realm]
[Called-Station-Id]
[Logical-Access-Id]
[ToS-Traffic-Class]
[Origin-State-Id]
[Event-Timestamp]
[Auth-Session-State]
* [Event-Trigger]
* [Policy-Rule-Remove]
* [Policy-Rule-Install]
* [Failed-AVP]
* [Proxy-Info]
* [Route-Record]
* [AVP]

7.2 Experimental-Result-Code AVP values

Clause 7.2 defines new Experimental-Result-Code values that shall be supported by all DIAMETER implementations that conform to the present document. When one of the Experimental Result Code defined in clause 7.2 is included in a response, it shall be inside an Experimental-Result AVP and the Result-Code AVP shall be absent.

7.2.1 Success

Experimental Result Codes that fall within the Success category are used to inform a peer that a request has been successfully completed.

7.2.2 Transient failures

Experimental Result Codes that fall within the transient failures category are those used to inform a peer that the request could not be satisfied at the time that it was received. The request may be able to be satisfied in the future.

The following values of the Experimental-Result-Code AVP defined in ES 283 026 [12] are reused:

- COMMIT_FAILURE (4043).
  - The RCEF indicates that the Policy could not be committed.

7.2.3 Permanent failures

Experimental Result Codes that fall within the Permanent Failures category are used to inform the peer that the request failed, and should not be attempted again.

The present document defines the following new values of the Experimental-Result-Code AVP:

- UNKNOWN_POLICY_RULE (5061)
  - The RCEF indicates that the specified Policy-Rule-Name AVP in unknown.
- UNKNOWN_POLICY_RULE_BASE_NAME (5062)
  - The RCEF indicates that the specified Policy-Rule-Base-Name AVP in unknown.
- UNKNOWN_POLICY_RULE_FOR_TRANSPORT_RESOURCE (5063)
  - The RCEF indicates a mismatch between the specified combination of Policy-Rule-Name AVP and Transport Resource Classifier.
- UNKNOWN_POLICY_RULE_BASE_NAME_FOR_TRANSPORT_RESOURCE (5064)
  - The RCEF indicates a mismatch between the specified combination of Policy-Rule-Base-Name AVP and Transport Resource Classifier.
- UNKNOWN_TRANSPORT RESOURCE (5065)
  - The RCEF indicates that the specified Transport Resource Classifier(s) do not match with each others, or cannot be mapped to any Transport Resource.
- POLICY_ACTIVATION_FAILURE (5066)
  - The RCEF indicates that a given Policy Rule could not be activated.
- POLICY_MODIFICATION_FAILURE (5067)
  - The RCEF indicates that a given Policy Rule could not be updated.
- AUTHORIZATION_REJECTED_FOR_TRANSPORT_RESOURCE (5068)
  - The RCEF denies the request because the requested operation is not allowed for the specified Transport Resource Classifier.
- AUTHORIZATION_REJECTED_FOR_POLICY_RULE_NAME (5069)
  - The RCEF denies the request because the requested operation is not allowed for the specified Policy Rule.
- AUTHORIZATION_REJECTED_FOR_POLICY_RULE_BASE_NAME (5070)
  - The RCEF denies the request because the requested operation is not allowed for the specified Policy Rule.

7.3 AVPs

Clause 7.3 summarizes the AVP used in the present document, beyond those defined in the DIAMETER Base Protocol.

7.3.1 AVPs Defined in the Present Document

Table 2 describes the new DIAMETER AVPs used in the present document, their AVP Code values, types, possible flag values and whether the AVP may or not be encrypted. The Vendor-Id field in the header for these AVPs shall be set to ETSI (13019).

Table 2: New DIAMETER AVPs

				AVP flag rules				
Attribute name	**AVP Code**	**Clause defined**	**Value type**	**Must**	**May**	**Should not**	**Must not**	**May encrypt**
Policy-Rule-Install	550	7.3.1.1	Grouped	M,V	P			Y
Policy-Rule-Remove	551	7.3.1.2	Grouped	M,V	P			Y
Policy-Rule-Definition	552	7.3.1.3	Grouped	M,V	P			Y
Policy-Rule-Base-Name	553	7.3.1.4	UTF8String	M,V	P			Y
Policy-Rule-Name	554	7.3.1.5	OctetString	M,V	P			Y
Policy-Rule-Report	555	7.3.1.6	Grouped	M,V	P			Y
Policy-Rule-Status	556	7.3.1.7	Enumerated	M,V	P			Y
Traffic-Flow	557	7.3.1.8	Grouped	M,V	P			Y
Policy-Update-Request	558	7.3.1.9	Grouped	M,V	P			Y
NOTE: The AVP header bit denoted as "M" indicates whether support of the AVP is required. The AVP header bit denoted as "V" indicates whether the optional Vendor-ID field is present in the AVP header. The 'P' bit indicates the need for encryption for end-to-end security.								

7.3.1.1 Policy-Rule-Install AVP

The Policy-Rule-Install AVP (AVP code 550) is of type Grouped, and it is used to activate, install or modify Policy Rule as instructed from the A-RACF to the RCEF.

AVP Format:

Policy-Rule-Install ::= < AVP Header: 550 >
* [Policy-Rule-Definition]
* [Policy-Rule-Name]
* [Policy-Rule-Base-Name]
* [AVP]

7.3.1.2 Policy-Rule-Remove AVP

The Policy-Rule-Remove AVP (AVP code 551) is of type Grouped, and it is used to deactivate or remove Policy Rules.

AVP Format:

Policy-Rule-Remove ::= < AVP Header: 551 >
* [Policy-Rule-Name]
* [Policy-Rule-Base-Name]
* [AVP]

7.3.1.3 Policy-Rule-Definition AVP

The Policy-Rule-Definition AVP (AVP code 552) is of type Grouped, and it describes a Policy Rule.

The Policy-Rule-Name AVP uniquely identifies the Policy Rule and it is used to reference to a Policy Rule in communication between the RCEF and the A-RACF.

The Flow-Description AVPs determines the traffic flows that belong to the service flow.

If optional AVP(s) within a Policy-Rule-Definition AVP are omitted, but corresponding information has been provided in previous Re messages, the previous information remains valid. If Flow-Description AVP(s) are supplied, they replace all previous Flow-Description AVP(s).

If Flows AVP(s) are supplied, they replace all previous Flows AVP(s).

AVP Format:

Policy-Rule-Definition ::= < AVP Header: 552 >
{ Policy-Rule-Name }
[Service-Identifier]
[Rating-Group]
[User-Name]
[Logical-Access-Id]
[Framed-IP-Address]
[Address-Realm]
[Called-Station-ID]
[Physical-Access-Id]
* [Flow-Description]
[Flow-Status]
[QoS-Information]
[Reporting-Level]
[Precedence]
* [Flows]
* [AVP]

7.3.1.4 Policy-Rule-Base-Name AVP

The Policy-Rule-Base-Name AVP (AVP code 553) is of type UTF8String, and it indicates the name of a pre-defined group of Policy Rules residing at the RCEF.

7.3.1.5 Policy-Rule-Name AVP

The Policy-Rule-Name AVP (AVP code 554) is of type OctetString, and it defines a name for Policy Rule. For Policy Rules provided by the A-RACF it uniquely identifies a Policy Rule. For Policy Rules pre-defined at the RCEF it uniquely identifies a Policy Rule within the RCEF.

7.3.1.6 Policy-Rule-Report AVP

The Policy-Rule-Report AVP (AVP code 555) is of types Grouped, and it is used to report the status of a particular Policy Rule.

Policy-Rule-Name AVP is a reference for a specific Policy. Policy-Rule-Base-Name AVP is a reference to a group of Policies. The Policy-Rule-Status AVP indicates the action being performed on the Policy rule. The Rule-Failure-Code indicates the reason that the Policy decisions cannot be successfully installed/activated or enforced.

AVP Format:

Policy-Rule-Report ::= < AVP Header: 555 >

* [Policy-Rule-Name]
* [Policy-Rule-Base-Name]
[Policy-Rule-Status]
[Rule-Failure-Code]
* [AVP]

7.3.1.7 Policy-Rule-Status AVP

The Policy-Rule-Status AVP (AVP code 556) is of type Enumerated, and describes the status of one or a group of Policy Rules.

The following values are defined:

ACTIVE (0)

This value is used to indicate that the Policy rule(s) are successfully installed (for those provisioned from A-RACF) or activated (for those pre-provisioned in RCEF).

INACTIVE (1)

This value is used to indicate that the Policy rule(s) are removed (for those provisioned from A-RACF) or inactive (for those pre-provisioned in RCEF).

TEMPORARY INACTIVE (2)

This value is used to indicate that, for some reason (e.g. loss of bearer), already installed or activated Policy rules are temporary disabled.

7.3.1.8 Traffic-Flow AVP

The Traffic-Flow AVP (AVP code 557) is of type Grouped, and it describes the detailed information for a group of flows.

AVP Format:

Traffic-Flow ::= < AVP Header: 557 >

* [Flow-Description]
[Flow-Status]
[QoS-Information]
[User-Name]
[Called-Station-ID]
[Framed-IP-Address]
[Framed-IPv6-Prefix]
[Address-Realm]
[Logical-Access-Id]
[Physical-Access-ID]

7.3.1.9 Policy-Update-Request AVP

The Policy-Update-Request AVP (AVP code 558) is of types Grouped, and it is used to request the update the QoS of a particular Policy Rule.

Policy-Rule-Name AVP is a reference for a specific Policy. Policy-Rule-Base-Name AVP is a reference to a group of Policies.

AVP Format:

Policy-Update-Request ::= < AVP Header: 558 >

* [Policy-Rule-Name]
* [Policy-Rule-Base-Name]
[Policy-Rule-Status]
[QoS-Information]
* [AVP]

7.3.2 AVPs imported from ITU-T NGN-GSI/DOC - 127

The following table describes the DIAMETER AVPs imported from ITU-T NGN-GSI/DOC - 127 [6] and used in the present document, their AVP Code values, types, possible flag values and whether the AVP may or not be encrypted. Flags values are described in the context of the present document rather than in the context of the application where they are defined. AVPs defined in [6] but noy listed in table 3 should not be sent by DIAMETER nodes conforming to the present document and shall be ignored by receiving entities. The Vendor-Id field in the header for these AVPs shall be set to ITU-T (11502).

Table 3: DIAMETER AVPs imported from ITU-T NGN-GSI/DOC - 127

				AVP flag rules				
Attribute name	**AVP Code**	**Clause defined**	**Value type**	**Must**	**May**	**Should not**	**Must not**	**May encrypt**
Traffic-Descriptor-UL	1012	7.3.2.1	Grouped	V	P			Y
Traffic-Descriptor-DL	1013	7.3.2.2	Grouped	V	P			Y
Maximum-Burst-Size	1014	7.3.2.3	Unsigned32	V	P			Y
Committed-Data-Rate	1015	7.3.2.4	Unsigned32	V	P			Y
Committed-Burst-Size	1016	7.3.2.5	Unsigned32	V	P			Y
Excess-Burst-Size	1017	7.3.2.6	Unsigned32	V	P			Y
NOTE: The AVP header bit denoted as "M" indicates whether support of the AVP is required. The AVP header bit denoted as "V" indicates whether the optional Vendor-ID field is present in the AVP header. The 'P' bit indicates the need for encryption for end-to-end security.								

7.3.2.1 Traffic-Descriptor-UL AVP (ITU-T NGN-GSI/DOC - 127)

The Traffic-Descriptor-UL AVP (AVP code 1012) is of type Grouped, and indicates traffic characteristics complementary to the maximum bandwidth. It is used to control the bandwidth of traffic flows in the uplink direction.

AVP Format:

Traffic-Descriptor-UL ::= < AVP Header: 1012 >
[Maximum-Burst-Size]
[Committed-Data-Rate]
[Committed-Burst-Size]
[Excess-Burst-Size]

7.3.2.2 Traffic-Descriptor-DL AVP (ITU-T NGN-GSI/DOC - 127)

The Traffic-Descriptor-DL AVP (AVP code 1013) is of type Grouped, and indicates traffic characteristics complementary to the maximum bandwidth. It is used to control the bandwidth of traffic flows in the downlink direction.

AVP Format:

Traffic-Descriptor-DL::= < AVP Header: 1013 >
[Maximum-Burst-Size]
[Committed-Data-Rate]
[Committed-Burst-Size]
[Excess-Burst-Size]

7.3.2.3 Maximum-Burst-Size AVP (ITU-T NGN-GSI/DOC - 127)

The Maximum-Burst-Size AVP (AVP code 1014) is of type Unsigned32, and indicates the peak burst size in Octets. It is used to provision the peak burst size for the traffic policing.

7.3.2.4 Committed-Data-Rate AVP (ITU-T NGN-GSI/DOC - 127)

The Committed-Data-Rate AVP (AVP code 1015) is of type Unsigned32, and indicates the average bandwidth in Octets per second. It is used to provision the average bandwidth for the traffic policing.

7.3.2.5 Committed-Burst-Size AVP (ITU-T NGN-GSI/DOC - 127)

The Committed-Burst Size AVP (AVP code 1016) is of type Unsigned32, and indicates the committed burst size in Octets.

7.3.2.6 Excess-Burst-Size AVP (ITU-T NGN-GSI/DOC - 127)

The Excess-Burst Size AVP (AVP code 1017) is of type Unsigned32, and indicates the excess burst size in Octets.

7.3.2.7 PI-Request-Type AVP (ITU-T NGN-GSI/DOC - 127)

The PI-Request-Type AVP (AVP Code 1010) is of type Enumerated and contains the reason for sending the Policy-Install-Request command. It shall be present in all Policy-Install-Request messages.

The following values defined in [6] are reused:

INITIAL_REQUEST 1

An Initial Request is used to activate Policy Rule(s) on a particular Transport Resource.

UPDATE_REQUEST 2

An Update Request is used to update Policy Rules previously activated on a given Transport Resource, to add new Policy on a given Transport Resource, or to remove one or several Policy Rule(s) activated on a given Transport Resource.

TERMINATION_REQUEST 3

Termination Request is used to deactivate and remove all Policy Rules previously activated on a given Transport Resource.

The following values are added compared to [6]:

QUERY_REQUEST 4

Query Request is used to query the RCEF about the supported or activated Policy Rules.

7.3.2.8 PI-Request-Number AVP (ITU-T NGN-GSI/DOC - 127)

The PI-Request-Number AVP (AVP Code 1011) is of type Unsigned32 and identifies this request within one session. As Session-Id AVPs are globally unique, the combination of Session-Id and PI-Request-Number AVPs is also globally unique and can be used in matching policy-install messages with confirmations. An easy way to produce unique numbers is to set the value to 0 for a policy-install request of type INITIAL_REQUEST and EVENT_REQUEST and to set the value to 1 for the first UPDATE_REQUEST, to 2 for the second, and so on until the value for TERMINATION_REQUEST is the value of the last UPDATE_REQUEST + 1.

7.3.3 AVPs Imported From TS 129 212

Table 4 describes the DIAMETER AVPs imported from [7] and used in the present document, their AVP Code values, types, possible flag values and whether the AVP may or not be encrypted. Flags values are described in the context of the present document rather than in the context of the application where they are defined. AVPs defined in TS 129 212 [7] but no listed in the following table should not be sent by DIAMETER nodes conforming to the present document and shall be ignored by receiving entities. The Vendor-Id field in the header for these AVPs shall be set to 3GPP (10415).

Table 4: DIAMETER AVPs imported from TS 129 212

Attribute name	AVP Code	Clause defined	Value type	AVP flag rules				
				Must	May	Should not	Must not	May encrypt
QoS-Information	1016	7.3.3.1	Grouped	M,V	P			Y
ToS-Traffic-Class	1019	7.3.3.2	OctetString	M,V	P			Y
Event-Trigger	1006	7.3.3.3	Enumerated	M,V	P			Y
Precedence	1010	7.3.3.4	Unsigned32	M,V	P			Y
Reporting-Level	1011	7.3.3.5	Enumerated	M,V	P			Y
Rule-Failure-Code	1031	7.3.3.6	Enumerated	M,V	P			Y
NOTE: The AVP header bit denoted as "M" indicates whether support of the AVP is required. The AVP header bit denoted as "V" indicates whether the optional Vendor-ID field is present in the AVP header. The 'P' bit indicates the need for encryption for end-to-end security.								

7.3.3.1 QoS-Information AVP (TS 129 212)

The QoS-Information AVP (AVP code 1016) is of type Grouped, and it defines the maximum QoS that is authorized for the corresponding traffic flow(s):

AVP Format:

QoS-Information ::= < AVP Header: 1016>
[Max-Requested-Bandwidth-UL]
[Max-Requested-Bandwidth-DL]
[Traffic-Descriptor-UL]
[Traffic-Descriptor-DL]
[ToS-Traffic-Class]

7.3.3.2 ToS-Traffic-Class AVP (TS 129 212)

The ToS-Traffic-Class AVP (AVP code 1014) is of type OctetString, and it contains an identifier of the Traffic Class.

7.3.3.3 Event-Trigger AVP (TS 129 212)

The Event-Trigger AVP (AVP code 1006) is of type Enumerated. When sent from the A-RACF to the RCEF the Event-Trigger AVP indicates that an event that shall trigger a CC-Request from the RCEF to the A-RACF. When sent from the RCEF to the A-RACF the Event-Trigger AVP indicates that the corresponding event has occurred on the RCEF.

The following values defined in TS 129 212 [7] are reused:

- LOSS_OF_BEARER (5)
  - This value shall be used in PIR commands by the A-RACF to indicate that upon loss of bearer, the RCEF shall inform the A-RACF.
  - When used in a CCR command, this value indicates that the RCEF generated the request because the bearer associated with the Policy indicated by the corresponding Policy-Rule-Report AVP was lost. The Policy-Rule-Status AVP within the Policy-Rule-Report AVP shall have the value INACTIVE or TEMPORARY INACTIVE.
  - The RCEF may provide the Logical-Access-Id AVP, Framed-IP-Address AVP, Framed-IP-Address and Address-Realm AVPs, User-Name AVP or Called-Station-Id AVP to indicate the resource that has been lost.

- RECOVERY_OF_BEARER (6)
  - This value shall be used in PIR commands by the A-RACF to indicate that upon recovery of bearer, the RCEF shall inform A-RACF.
  - When used in a CCR command, this value indicates that the RCEF generated the request because the bearer associated with the Policy indicated by the corresponding Policy-Rule-Report AVP was recovered. The Policy-Rule-Status AVP within the Policy-Rule-Report AVP shall have the value ACTIVE.
  - The RCEF may provide the Logical-Access-Id AVP, Framed-IP-Address AVP, Framed-IP-Address and Address-Realm AVPs, User-Name AVP or Called-Station-Id AVP to indicate the resource that has been recovered.
- RESOURCES_MODIFICATION (101)
  - When used in a CCR command, this value indicates that the RCEF generated the request because an event occurred that may affect resources requirements and require re-evaluation of these requirement by the RACS. The affected policy rules are provided in the Policy-Rule-Report AVP.

Other values defined in TS 129 212 [7] are not used.

The following values are added:

- ANY_EVENT (11)
  - This value shall be used in PIR commands by the A-RACF to indicate that the RCEF shall inform the A-RACF of the occurrence of any event.
- NO_EVENT (12)
  - This value shall be used in PIR commands by the A-RACF to indicate that the RCEF shall not inform the A-RACF anymore of the occurrence of any event.

7.3.3.4 Precedence AVP (TS 129 212)

The Precedence AVP (AVP code 1010) is of type Unsigned32, and it defines the precedence of a Policy Rule in case of overlapping Policy Rules. A Policy Rule with the Precedence AVP with lower value shall take precedence over a Policy Rule with the Precedence AVP with higher value.

7.3.3.5 Reporting-Level AVP (TS 129 212)

The Reporting-Level AVP (AVP code 1011) is of type Enumerated, and it defines on what level the RCEF reports the usage for the related Policy Rule. The following values are defined:

- SERVICE_IDENTIFIER_LEVEL (0)
  - This value shall be used to indicate that the usage shall be reported on service id and rating group combination level.
- RATING_GROUP_LEVEL (1)
  - This value shall be used to indicate that the usage shall be reported on rating group level.

7.3.3.6 Rule-Failure-Code AVP

The Rule-Failure-Code AVP (AVP code 1031) is of type Enumerated. It is sent by the RCEF to the A-RACF within a Policy-Rule-Report AVP to identify the reason a policy decision is being reported.

The following values are defined:

- UNKNOWN_RULE_NAME (1)
  - This value is used to indicate that the pre-provisioned policy decision could not be successfully activated because the Policy-Rule-Name or Policy-Rule-Base-Name is unknown to the RCEF.
- RATING_GROUP_ERROR (2)
  - This value is used to indicate that the policy decision could not be successfully installed or enforced because the Rating-Group specified within the Policy-Rule-Definition AVP by the A-RACF is unknown or, invalid.
- SERVICE_IDENTIFIER_ERROR (3)
  - This value is used to indicate that the policy decision could not be successfully installed or enforced because the Service-Identifier specified within the Policy-Rule-Definition AVP by the A-RACF is invalid, unknown, or not applicable to the service being charged.
- GW/RCEF_MALFUNCTION (4)
  - This value is used to indicate that the policy decision could not be successfully installed (for those provisioned from the A-RACF) or activated (for those pre-provisioned in RCEF) or enforced (for those already successfully installed) due to GW/RCEF malfunction.
- RESOURCES_LIMITATION (5)
  - This value is used to indicate that the policy decision could not be successfully installed (for those provisioned from A-RACF) or activated (for those pre-provisioned in RCEF) or enforced (for those already successfully installed) due to a limitation of resources at the RCEF.
- MAX_NR_BEARERS_REACHED (6)
  - This value is used to indicate that the policy decision could not be successfully installed (for those provisioned from A-RACF) or activated (for those pre-provisioned in RCEF) or enforced (for those already successfully installed) due to the fact that the maximum number of bearers has been reached for the IP-CAN session.

7.3.4 AVPs imported from RFC 4006

Table 5 describes the DIAMETER AVPs imported from RFC 4006 [8] and used in the present document, their AVP Code values, types, possible flag values and whether the AVP may or not be encrypted. Flags values are described in the context of the present document rather than in the context of the application where they are defined. AVPs defined in RFC 4006 [8] but no listed in the following table should not be sent by DIAMETER nodes conforming to the present document and shall be ignored by receiving entities. The Vendor-Id field in the header for these AVPs shall not be included.

Table 5: DIAMETER AVPs imported from RFC 4006

Attribute name	AVP Code	Clause defined	Value type	AVP flag rules				
				Must	May	Should not	Must not	May encrypt
CC-Request-Number	415		Unsigned32	M	P		V	Y
CC-Request-Type	416		Enumerated	M	P		V	Y
Rating-Group	432		Unsigned32	M	P		V	Y
Service-Identifier	439		Unsigned32	M	P		V	Y
Service-Context-Id	461		UTF8String	M	P		V	Y
NOTE: The AVP header bit denoted as "M" indicates whether support of the AVP is required. The AVP header bit denoted as "V" indicates whether the optional Vendor-ID field is present in the AVP header. The 'P' bit indicates the need for encryption for end-to-end security.								

7.3.5 AVPs imported from TS 129 209

Table 6 describes the DIAMETER AVPs imported from TS 129 209 [9] and used in the present document, their AVP Code values, types, possible flag values and whether the AVP may or not be encrypted. Flags values are described in the context of the present document rather than in the context of the application where they are defined. AVPs defined in TS 129 209 [9] but no listed in the following table should not be sent by DIAMETER nodes conforming to the present document and shall be ignored by receiving entities. The Vendor-Id field in the header for these AVPs shall be set to 3GPP (10415).

Table 6: DIAMETER AVPs imported from TS 129 209

Attribute name	AVP Code	Clause defined	Value type	AVP flag rules				
				Must	May	Should not	Must not	May encrypt
Flow-Description	507	7.3.5.1	IPFilterRule	M,V	P			Y
Flow-Number	509	7.3.5.2	Unsigned32	M,V	P			Y
Flow	510	7.3.5.3	Grouped	M,V	P			Y
Flow-Status	511	7.3.5.4	Enumerated	M,V	P			Y
NOTE: The AVP header bit denoted as "M" indicates whether support of the AVP is required. The AVP header bit denoted as "V" indicates whether the optional Vendor-ID field is present in the AVP header. The 'P' bit indicates the need for encryption for end-to-end security.								

7.3.5.1 Flow-Description AVP (TS 129 209)

The Flow-Description AVP (AVP code 507) is of type IPFilterRule, and defines a packet filter for an IP flow with the following information:

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

The following restrictions apply:

- Only the Action "permit" shall be used.
- No "options" shall be used.
- The invert modifier "!" for addresses shall not be used.
- The keyword "assigned" shall not be used.

If any of these restrictions is not observed by the AF, the server shall send an error response to the AF containing the Experimental-Result-Code AVP with value FILTER_RESTRICTIONS. The Flow description AVP shall be used to describe a single IP flow. The direction "in" refers to uplink IP flows, and the direction "out" refers to downlink IP flows.

7.3.5.2 Flow-Number AVP (TS 129 209)

The Flow-Number AVP (AVP code 509) is of type Unsigned32, and it contains the ordinal number of the IP flow(s), assigned according to the rules in annex C of TS 129 207 [14] (3GPP TS 29.207).

7.3.5.3 Flows AVP (TS 129 209)

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

If no Flow-Number AVP(s) is supplied, the Flows AVP refers to all Flows matching the Media-Component-Number.

AVP Format:

Flows::= < AVP Header: 510 >
{ Media-Component-Number}
* [Flow-Number]

7.3.5.4 Flow-Status AVP (TS 129 209)

The Flow-Status AVP (AVP code 511) is of type Enumerated, and describes whether the Policy Rule needs to be activated or not. The following values are defined:

- ENABLED-UPLINK (0)
  - This value shall be used to activate a Policy Rule relative to the outgoing direction on the RCEF.
- ENABLED-DOWNLINK (1)
  - This value shall be used to activate a Policy Rule relative to the incoming direction on the RCEF.
- REMOVED (4)
  - This value shall be used to deactivate and remove a Policy Rule.

7.3.6 AVPs Imported From RFC 4005

The following table describes the DIAMETER AVPs imported from RFC 4005 [10] and used in the present document, their AVP Code values, types, possible flag values and whether the AVP may or not be encrypted. Flags values are described in the context of the present document rather than in the context of the application where they are defined. AVPs defined in [10] but no listed in the following table should not be sent by DIAMETER nodes conforming to the present document and shall be ignored by receiving entities. The Vendor-Id field in the header for these AVPs shall not be included.

Table 7: DIAMETER AVPs imported from RFC 4005

				AVP flag rules				
Attribute name	**AVP Code**	**Clause defined**	**Value type**	**Must**	**May**	**Should not**	**Must not**	**May encrypt**
Called-Station-Id	30	7.3.6.1	UTF8String	M	P		V	Y
Framed-IP-Address	8	7.3.6.2	OctetString	M	P		V	Y
NOTE: The AVP header bit denoted as "M" indicates whether support of the AVP is required. The AVP header bit denoted as "V" indicates whether the optional Vendor-ID field is present in the AVP header. The 'P' bit indicates the need for encryption for end-to-end security.								

7.3.6.1 Called-Station-Id AVP (RFC 4005)

The Called-Station-Id AVP (AVP Code 30) is of type UTF8String and contains the ASCII string describing the layer 2 address of the Transport Resource on the RCEF. For use with IEEE 802 access, the Called-Station-Id MAY contain a MAC address.

NOTE: Further clarification on the use of Called-Station-Id is required in the next release.

7.3.6.2 Framed-IP-Address

The Framed-IP-Address AVP is defined in the NASREQ application RFC 4005 [10].

7.4 Use of namespaces

Clause 7.4 contains the namespaces that have either been created in the present document, or the values assigned to existing namespaces managed by IANA [11].

7.4.1 AVP codes

The present document assigns the AVP values in the range 550 to 599 from the AVP Code namespace managed by ETSI for its DIAMETER vendor-specific applications. See clause 7.3 for the list of AVP values assigned in the present document.

7.4.2 Experimental-Result-Code AVP values

This clause defines new Experimental-Result-Code values that shall be supported by all DIAMETER implementations that conform to the present document. When one of the Experimental-Result-Code values defined in this clause is included in a response, it shall be inside an Experimental-Result AVP.

7.4.3 Command Code values

The present document does not assign command code values but uses existing command defined in ITU-T NGN-GSI/DOC-127 [6].

7.4.4 Application-ID value

The present document uses value 16777253.

Annex A (informative): Differences compared to ITU-T Rw and 3GPP Gx specifications

The protocol used over the Re reference point and defined in the present specification has strong similarities with the Diameter applications used over the 3GPP Gx reference point and ITU-T Rw reference points.
Table A.1 provides a high-level comparison of the three specifications regarding the list of Diameter commands supported.

Table A.1

	TS 183 060 (Re)	TS 129 210 [i.2] (Gx)	ITU-T Recommendation Q.3303.3 [i.1] (Rw)
CC-Request	X	X	X
CC-Answer	X	X	X
Re-Auth-Request		X	X
Re-Auth-Answer		X	X
Policy-Install-Request	X		X
Policy-Install-Answer	X		X

Although the same commands are used by the three specifications, it should be noted that there are significant differences between them regarding the list of AVPs supported.

History

Document history		
V2.1.1	April 2009	Publication