

3GPP2 X.S0053-0
Version 1.0
Date: June 2008



3RD GENERATION
PARTNERSHIP
PROJECT 2
"3GPP2"

All-IP System – MMD Policy Enhancements

COPYRIGHT

3GPP2 and its Organizational Partners claim copyright in this document and individual Organizational Partners may copyright and issue documents or standards publications in individual Organizational Partner's name based on this document. Requests for reproduction of this document should be directed to the 3GPP2 Secretariat at secretariat@3gpp2.org. Requests to reproduce individual Organizational Partner's documents should be directed to that Organizational Partner. See www.3gpp2.org for more information.

Revision History

| Revision | Description | Date |
|-------------|---------------------|-----------|
| Rev. 0 v1.0 | Initial Publication | June 2008 |

All-IP System – MMD Policy Enhancements

CONTENTS

| | | | |
|----|-------|--|----|
| 1 | 1 | Introduction..... | 1 |
| 2 | 2 | References..... | 2 |
| 3 | 2.1 | Normative References..... | 2 |
| 4 | 2.2 | Informative References..... | 2 |
| 5 | 3 | Definitions, Symbols and Abbreviations..... | 3 |
| 6 | 3.1 | Definitions..... | 3 |
| 7 | 3.1.1 | Symbols and Abbreviations..... | 3 |
| 8 | 4 | FUNCTIONAL OVERVIEW..... | 4 |
| 9 | 4.1 | Relationship to SBBC..... | 4 |
| 10 | 4.2 | Descriptions of Enhancements..... | 4 |
| 11 | 4.2.1 | Policy Contexts..... | 4 |
| 12 | 4.2.2 | Admission Control..... | 5 |
| 13 | 4.2.3 | Policy Management..... | 5 |
| 14 | 4.2.4 | Authentication..... | 5 |
| 15 | 4.2.5 | Privacy..... | 6 |
| 16 | 4.3 | Functional Capabilities..... | 6 |
| 17 | 4.3.1 | Types of Policy..... | 7 |
| 18 | 4.3.2 | Types of QoS Resource Reservation Scenarios..... | 7 |
| 19 | 4.3.3 | Mobility Management Policy..... | 7 |
| 20 | 4.3.4 | Coordination of Policy Across Networks..... | 8 |
| 21 | 5 | ARCHITECTURAL MODEL AND REFERENCE POINTS..... | 8 |
| 22 | 5.1 | Functional Model..... | 8 |
| 23 | 5.1.1 | Policy Management Functional Architecture (Non-roaming)..... | 8 |
| 24 | 5.1.2 | Policy Management Functional Architecture (Roaming)..... | 9 |
| 25 | 5.2 | Functional Entity Descriptions..... | 10 |
| 26 | 5.2.1 | Policy & Charging Rules Function (PCRF)..... | 10 |
| 27 | 5.2.2 | Access Gateway..... | 11 |
| 28 | 5.2.3 | Application Function (AF)..... | 11 |
| 29 | 5.2.4 | Local Mobility Anchor (LMA) / Home Agent (HA)..... | 12 |
| 30 | 5.2.5 | Policy Repository..... | 12 |
| 31 | 5.3 | Reference Points..... | 12 |
| 32 | 6 | OPERATIONAL PROCEDURES..... | 14 |
| 33 | 6.1 | Policy Delegation..... | 14 |
| 34 | 6.2 | Mobility Management..... | 15 |
| 35 | 6.3 | Admission Control Management..... | 15 |
| 36 | 6.3.1 | Use of Local Resource Based Policy..... | 15 |
| 37 | 6.3.2 | Authorization for Allocation of Bearer Resources..... | 15 |
| 38 | 6.3.3 | Gating of IP Packets..... | 17 |

| | | |
|-------|---|----|
| | | 1 |
| 6.4 | QoS Management..... | 18 |
| 6.4.1 | Segmented QoS Model..... | 18 |
| 6.4.2 | Resource Reservation..... | 19 |
| 6.4.3 | Binding Mechanism..... | 20 |
| 6.4.4 | Enforcement of QoS Authorization..... | 21 |
| 6.4.5 | Conflict Detection and Resolution..... | 21 |
| 6.5 | Charging Management..... | 21 |
| 6.5.1 | Charging Models..... | 22 |
| 6.5.2 | Charging Rules..... | 23 |
| 6.5.3 | Conflict Detection and Resolution..... | 24 |
| 6.5.4 | Measurements..... | 24 |
| 6.6 | Packet Flow Optimization Management..... | 25 |
| 6.6.1 | Sample PFO Flows..... | 27 |
| 6.7 | Service Interaction Management..... | 30 |
| 6.8 | Privacy Management..... | 30 |
| 6.9 | Authentication Management..... | 30 |
| 6.10 | Network Selection..... | 30 |
| 6.11 | Security Management..... | 30 |
| 7 | INFORMATION FLOWS..... | 31 |
| 7.1 | AF Session Establishment or Modification – Non Roaming..... | 31 |
| 7.2 | AF Session Establishment – Roaming – Home Routed Traffic..... | 33 |
| | | 31 |
| | | 32 |
| | | 33 |
| | | 34 |
| | | 35 |
| | | 36 |
| | | 37 |
| | | 38 |
| | | 39 |
| | | 40 |
| | | 41 |
| | | 42 |
| | | 43 |
| | | 44 |
| | | 45 |
| | | 46 |
| | | 47 |
| | | 48 |
| | | 49 |
| | | 50 |
| | | 51 |
| | | 52 |
| | | 53 |
| | | 54 |
| | | 55 |
| | | 56 |
| | | 57 |
| | | 58 |
| | | 59 |
| | | 60 |

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

LIST OF FIGURES

| | | |
|------------------|---|----|
| <i>Figure 1</i> | Policy Management functional model (non-roaming) | 9 |
| <i>Figure 2</i> | Policy Management functional model (roaming) | 10 |
| <i>Figure 3</i> | Policy Distribution..... | 14 |
| <i>Figure 4</i> | QoS Authorization Entities (Pull)..... | 16 |
| <i>Figure 5</i> | QoS Authorization Entities (Push)..... | 17 |
| <i>Figure 6</i> | PFO within AGW | 25 |
| <i>Figure 7</i> | PFO Separate from AGW | 26 |
| <i>Figure 8</i> | PFO within AGW | 28 |
| <i>Figure 9</i> | Separate PFO Entity | 29 |
| <i>Figure 10</i> | AF Session Establishment or Modification – non Roaming | 31 |
| <i>Figure 11</i> | AF Session Establishment – Roaming – Home Routed Traffic..... | 33 |

LIST OF TABLES

Table 1 PFO Examples26

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

1
2
3 **FOREWORD**
4

5 (This foreword is not part of this Standard.)
6
7

8 “Shall” and “shall not” identify requirements to be followed strictly to conform to this
9 document and from which no deviation is permitted. “Should” and “should not” indicate that
10 one of several possibilities is recommended as particularly suitable, without mentioning or
11 excluding others, that a certain course of action is preferred but not necessarily required, or
12 that (in the negative form) a certain possibility or course of action is discouraged but not
13 prohibited. “May” and “need not” indicate a course of action permissible within the limits of
14 the document. “Can” and “cannot” are used for statements of possibility and capability,
15 whether material, physical or causal.
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

(This page intentionally left blank.)

1 Introduction

This document describes a policy-based approach to resource management, interactions between network services and network resources, and interactions between network services themselves.

Such policies need to be coordinated across various constituent networks, nodes and links. This co-ordination must take into account the requirements of the service and the availability, cost and, often, the characteristics of network resources and subscriber privileges. The objective is to offer a rich spectrum of services, customized to user expectations, device characteristics, geographical location, time of day, and so on. The support for these services needs to be provided across a diverse collection of networking technologies, primarily dictated by access capabilities and cost.

Various network sub-domains and network entities may have specific resources that need to be managed. For a system comprised of a large number of functional elements, the less state information shared between entities, and, the less state information needing to be synchronized makes it easier to alter the overall behavior with a consistent, predictable outcome. Allowing functional elements to have a certain degree of autonomy in managing local resources, the network resource management solution can focus on ensuring that each entity meets identified service level goals. The objectives for resource management at each entity are outcomes of the operational policy for supporting a service end-to-end.

2 References

2.1 Normative References

The references which are applicable to this specification include the following:

- [MMD Part-13] 3GPP2 X.S0013-013, “Service Based Bearer Control – Tx Interface Stage-3”.
- [MMD Part-12] 3GPP2 X.S0013-012, “Service Based Bearer Control – Stage-2”.
- [MMD Part-14] 3GPP2 X.S0013-014, “Service Based Bearer Control – Ty interface Stage-3”.

2.2 Informative References

- [SR0037] 3GPP2 S.R0037-B v1.0, “IP Network Architecture Model for cdma2000 Spread Spectrum Systems,” August 2007.
- [SR0079] 3GPP2 S.R0079-A v1.0, “Support for End-to-End QoS Stage 1 Requirements,” July 2006.
- [SR0120] 3GPP2 S.R0120, “All-IP System – MMD Policy Enhancements –System Requirements” September 2007.
- [RFC3060] IETF RFC 3060, Police Core Information Model - Version 1 Specification, February 2001.
- [RFC3198] IETF RFC 3198, Terminology for Policy-Based Management, November 2001.
- [RFC4566] IETF RFC 4566, SDP: Session Description Protocol, July 2006.

3 Definitions, Symbols and Abbreviations

3.1 Definitions

None.

3.1.1 Symbols and Abbreviations

| | |
|-------|------------------------------------|
| AF | Application Function |
| AGW | Access Gateway |
| ACL | Access Control List |
| AN | Access Network |
| AT | Access Terminal |
| BMF | Bearer Management Function |
| CRF | Charging Rules Function |
| DSL | Data Subscriber Line |
| HA | Home Agent |
| H-NPR | Home NPR |
| HSS | Home Subscriber Server |
| HRPD | High Rate Packet Data |
| LMA | Local Mobility Anchor |
| MMD | Multi-Media Domain |
| NAT | Network Address Translation |
| NPR | Network Policy Repository |
| PCRF | Policy and Charging Rules Function |
| PDP | Policy Decision Point |
| PDSN | Packet Data Service Node |
| PEP | Policy Enforcement Point |
| QoS | Quality of Service |
| SIP | Session Initiation Protocol |
| SLA | Service Level Agreement |
| SPR | Subscriber Policy Repository |
| V-NPR | Visited NPR |

4 FUNCTIONAL OVERVIEW

4.1 Relationship to SBBC

[MMD Part-12] addresses policy control over IP bearer resources for IMS services (e.g., VoIP) and non-IMS services (e.g., streaming services). Specifically, the linkage between session control and bearer level resource control is defined through two interfaces. The Tx interface [MMD Part-13] connects the Policy and Charging Rules Function (PCRF) to an Application Function (e.g., P-CSCF) that is responsible for application level service decisions. The Ty interface [MMD Part-14] connects the PCRF to the AGW (e.g., PDSN) that is responsible for bearer resources policy enforcement. The PCRF acts as a Policy Decision Point from the perspective of policy control.

One of the fundamental objectives for the Tx and Ty interfaces is to encourage flexibility in the engineering and policy control of IP bearer resources, allowing policy control mechanisms for IP bearer resources related to IMS- and non-IMS-based services, as well as their related IP bearer resources, to be controlled either together or separately.

[MMD Part-12] specifies policy control interactions among a set of network elements. This specification is not intended to replace SBBC but incorporates additional functionality and expands on the list of network elements impacted by the policy specifications.

Section 4.2 provides an overview of the enhancements.

4.2 Descriptions of Enhancements

The policy enhancement requirements are categorized in under five main areas:

- Policy Contexts
- Admission Control
- Policy Management
- Authentication
- Privacy

4.2.1 Policy Contexts

Policy contexts are the set of states that policy uses to make decisions. A policy context can be thought of as a set of variables that represent information used by the policy process to make a decision. A policy context includes, at a minimum, the identity of the subscriber, the invoking application, the identity of the AF (Application Function), and the access network serving the subscriber.

Policy contexts span QoS, Accounting, Mobility, Access, Authentication, Network Selection, Traffic Engineering, Resource Selection, Packet Flow Optimization, and Address Translation.

4.2.2 Admission Control

Admission Control refers to restricting access to services based on network resource allocation, service differentiation, and the characteristics of the content being delivered by the service/application (e.g. conversational, streaming, interactive and background).

4.2.3 Policy Management

The following provides a brief overview of the policy management requirements described in [\[SR0120\]](#):

- Define and manage policies for new characteristics and applications
- Provide mechanism for distributing consistent policy in any given administrative domain.
- Provide capability to base policy decisions upon subscription information.
- A policy data repository function can provide a mechanism which allows network elements to be informed about data changes.
- Support for Parental/Enterprise control.
- Support Subscriber Personalities by allowing a subscriber to have multiple sets of policy.

4.2.4 Authentication

Authentication is an essential operation needed to enable access control, trust establishment and accountability. It is performed at several places in the policy architecture.

Authentication occurs at:

- initial access authentication,
- IP mobility services authentication (for mobile IP),
- SIP and other application authentication.

The network supports the capability for the operator to define policies associated with

- Credential distribution across network elements
- Credential expiration and refresh.
- Trust hierarchies and horizontal relationships between network elements requiring secure communications.
- Enabling and disabling exchange of credential information in protocols which support optional authentication procedures.

The following sub-sections identify some of the enhancements to authentication which are addressed in this document.

4.2.4.1 Credential type enumeration

- Identifies the types of credentials which are supported in the system, including fixed network elements and subscriber devices.

- Examples of credential types are X.509 certificates, Pre-shared keys, and User Name/Passwords.

4.2.4.2 Authentication type enumeration

- Identifies the types of authenticators which are supported in the system, including fixed network elements and subscriber devices.
- Identifies if authenticators (and associated authentication procedures) can be enabled or bypassed based on the authentication status (result) of another authenticator (authentication procedure). This supports Single-Sign-On and Single-Sign-Off methods.
- Examples of authentication types are Access Authentication, MIP authentication, and SIP authentication

4.2.4.3 Key Exchange method and Key Derivation method enumeration

- Identifies the types of key exchange methods
- Identifies the types of key derivation methods
- Examples of key derivation methods are AKA and CAVE. Example of key exchange method is IKE.

4.2.4.4 Credential management and Key management

- Expiration period
- Refresh period
- Expiration Actions

4.2.4.5 Authentication Result Actions

- Actions resulting from successful authentications (e.g., authorization assessment, health assessment)
- Actions resulting from unsuccessful authentications (e.g., log event, emit warning message, quarantine device)

4.2.5 Privacy

Privacy policies include those set by the subscriber and ones determined by the service provider that may take other factors into consideration (e.g., without prior user authorization, presence information may be disclosed to other applications in the user's network or networks that their provider has agreements with in order to satisfy legal intercept, application, or other operational requirements).

In roaming and peering contexts, policy determines which asserted user identities may be exported by the network operator to the other network.

4.3 Functional Capabilities

Policy management functions offer MMD providers a rich spectrum of services provided by the underlying IP network, customized to user expectations, device characteristics,

1
2 geographical location, time of day, and so on. These services are to be delivered across a
3 diverse collection of networking technologies and devices, primarily dictated by access
4 capabilities and cost.
5

6 7 **4.3.1 Types of Policy**

8
9 There are two types of policy - Subscriber Policies and Network Policies.

- 10
11 ▪ Subscriber Policies are policies associated to a particular subscriber, which govern
12 the usage of network resources specifically for that subscriber. Different subscribers
13 can have different policies.
- 14
15 ▪ Network Policies specify operator rules across multiple subscribers.

16
17 Network Policies are combined with Subscriber Policies to determine the overall network
18 behavior for a particular subscriber.

19
20 The split of policy into subscriber and network allows for differentiation between subscribers
21 (through the Subscriber Policies), while providing centralized control over the network
22 (through Network Policies).

23
24 Subscriber policies are policies used by the PCRF to define the limits of what that particular
25 subscriber is or is not authorized to do on the network. Network policies define how network
26 resources are generally to be utilized, and may be of higher or lower priority to a particular
27 subscriber priority, as defined by the network operator.

- 28
29 ▪ An example of this dichotomy would be when a user roams into another network; the
30 H-PCRF may be applying subscriber policies in terms of what level of service is
31 granted to a particular flow, where the V-PCRF may be using network policies to
32 determine what level of service a roamer from their particular home network is
33 entitled to.

34 35 **4.3.2 Types of QoS Resource Reservation Scenarios**

36
37 The PCRF concurrently should support the following QoS resource reservation scenarios:

- 38
39 ▪ Network initiated QoS with policy-push: Subscriber terminals do not use QoS
40 signaling protocols (e.g., RSVP or NSIS) for network resource reservation. Instead,
41 whenever a user terminal starts, modifies, or ends an application, it contacts the AF
42 and, then, it is responsibility of the AF to request to the PCRF the appropriate QoS
43 support in the network.
- 44
45 ▪ User-requested QoS with policy-push-pull: Applications in the user terminal are able
46 to request network resources to accommodate their QoS need using native QoS
47 signaling protocols. The requested QoS requires the authorization from the PCRF.
- 48
49 ▪ User-requested QoS with policy-pull: User terminals are capable of sending QoS
50 requests over signaling protocols for their own QoS needs, and do not require prior
51 authorization. Authorization for the user-requested QoS is obtained "on the fly" at
52 the time the request is actually signaled to the AGW and may require a policy pull
53 operation to the PCRF so as to verify AGW resource availability during regular
54 processing of the QoS signaling messages by the AGW.

55 56 **4.3.3 Mobility Management Policy**

57
58 Mobility policy governs mobility management in inter-technology handoffs and roaming. The
59 importance of mobility policy is to integrate operator and network management strategies and
60

policies into the handoff and roaming control in order to accommodate different access technologies and mobility scenarios.

Policy-based mobility management will:

- ensure that the mobile handoff and roaming are managed by mobility management policies;
- control whether or not a mobile handoff or roaming request is allowed (under the conditions of operator domain agreements, network access technologies & configurations, access permissions and resource / bandwidth required, type of mobiles and user services, etc.);
- provide a means of managing the mobile handoff and roaming priority (e.g., in a case of network failures or peak hours of a day).

4.3.4 Coordination of Policy Across Networks

Coordination of policy across networks or policy peering occurs between MMD providers that have agreed to exchange and enforce policy on behalf of each other. Policy peering may happen as a result of a subscriber roaming on another provider's network or as a result of a call.

Policy peering allows the home network provider to be able to apply subscriber specific policy to the use of both the visited and home networks. In this context, policy management in the home network takes the additional role of identifying and forwarding relevant inter-provider policy information to the visited network. Given the relevant information, policy peering enables some level of subscriber specific policy to be installed in the visited network, thus allowing the policy management function in the visited network to act as a "representative" of the corresponding home-network policy management function. The visited network applies its own network policies as well.

In the visited network, network policy defines rules about how resources in the visited network should be available to the roaming subscriber

5 ARCHITECTURAL MODEL AND REFERENCE POINTS

5.1 Functional Model

This section describes the policy management functional architecture and the functional entities impacted by the policy enhancements and the interface reference points.

5.1.1 Policy Management Functional Architecture (Non-roaming)

Figure 1 illustrates the policy architecture for the non-roaming case when a subscriber is located in its home network. Note, only policy related signaling interfaces are shown. No bearer interfaces are shown.

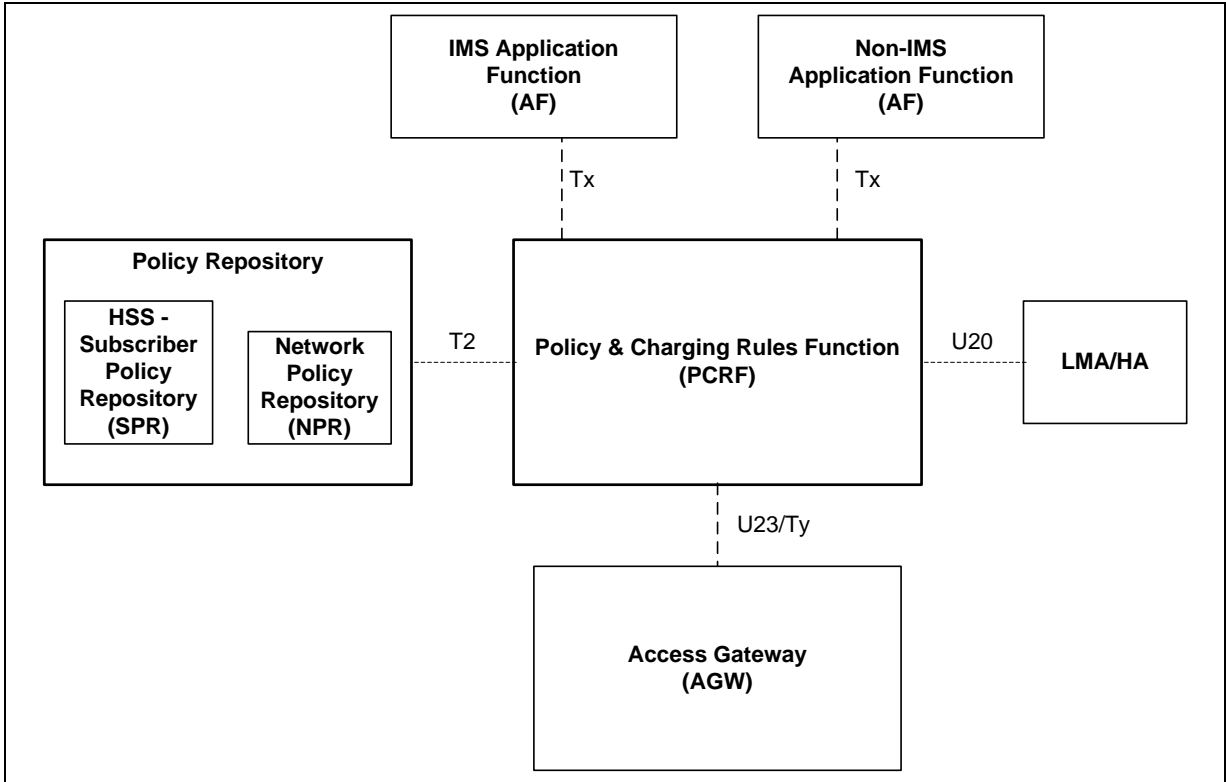


Figure 1 Policy Management functional model (non-roaming)

5.1.2 Policy Management Functional Architecture (Roaming)

Figure 2 illustrates the policy architecture for the roaming case when a subscriber is in a visited network. Note, only policy related signaling interfaces are shown. No bearer interfaces are shown.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

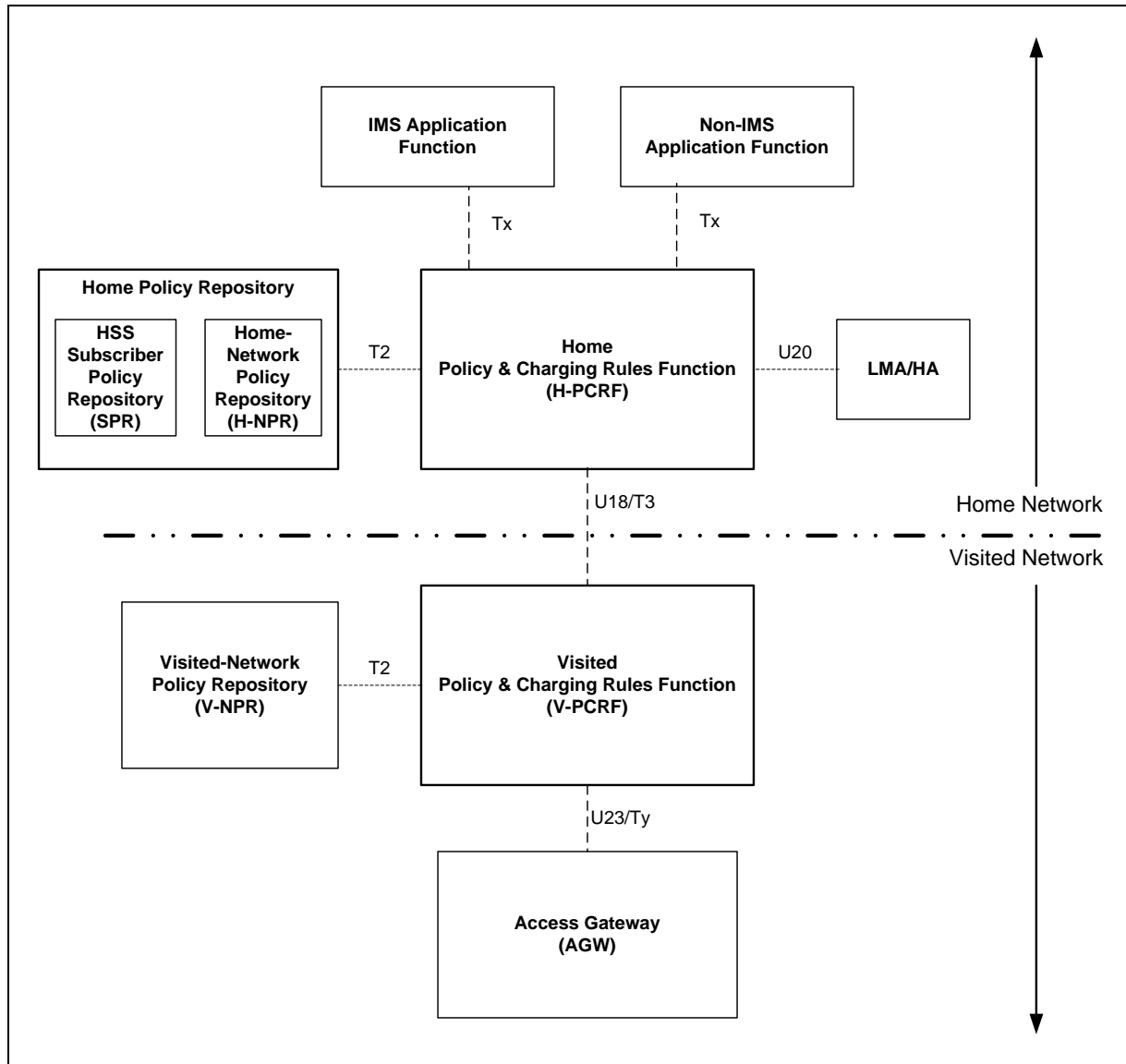


Figure 2 Policy Management functional model (roaming)

5.2 Functional Entity Descriptions

This section describes the functional entities involved in policy management.

5.2.1 Policy & Charging Rules Function (PCRF)

The Policy Charging & Rules Function (PCRF) acts as a Policy Decision Point (PDP) for Service Based QoS Authorization, Local Resource Based Policy (LRBP) control and Mobility Management Policy. The PCRF makes decisions about resource requests based on local network policy.

The PCRF is also responsible for providing, to the Access Gateway (AGW), operator determined dynamic charging rules. The Charging Rules Function (CRF) of the PCRF is responsible for formulating charging rules based on provisioned information, subscription information, input from Application Functions (AF), or operator determined dynamic

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

charging rules, and for providing such charging rules to the Bearer Management Function (BMF) of the AGW, which is a Policy Enforcement Point (PEP).

Some PCRF functions can be associated with a home network for the purpose of representing subscription and home based application function information. Some PCRF functions can be associated with the network of the AGW for purpose of enforcement of local policy. In roaming situations where the AGW is located in a visited network, there may be both a home and a visited PCRF. In this case the visited PCRF may act as a proxy or redirect agent for communications between the Access Gateway and the home PCRF (also see section 5.1.2).

5.2.2 Access Gateway

The Access Gateway (AGW) is a Policy Enforcement Point (PEP) for the following policies:

- Mobility management
- Admission control management
- QoS management
- Charging management
- Packet flow optimization
- Service interaction management
- Privacy management
- Authentication management
- NAT traversal management
- Network management
- Security management

5.2.3 Application Function (AF)

The Application Function (AF) is responsible for requests to the AGW for the purpose of controlling packet flows. The Application Function represents the application or service level intelligence for any service running over the IP bearer, which needs Service Based Authorization. This capability is not limited to IMS based services.

The AF may also provide information to the PCRF to help in the determination of dynamic charging rules for specifically identified service data flows. Such information may include an application identifier, media component descriptions, charging identifier, etc.

5.2.3.1 Types of Application Functions

The enhanced policy architecture considers three distinct types of applications: SIP, non-SIP, and over-the-top.

IMS Application Functions, such as the P-CSCF, interact directly with the PCRF to authorize resources via the Tx reference point. The service QoS characteristics of SIP applications are derived from the Session Description Protocol (SDP) [RFC4566] parameters that are negotiated end-to-end between the end points of the IMS session. These SDP parameters include a media component descriptor giving, for each component, an indication of the type of media, the list of codecs and encoded formats, the required bandwidth per component, and IP flow information, such as IP addresses and ports.

Non-IMS Application Functions may interact directly with the PCRF to authorize resources via the Tx reference point, or interact indirectly via the Service Broker. The service QoS characteristics of non-SIP applications are derived using parameters similar to the SIP applications.

Over-the-top applications do not interact with the PCRF via the Tx reference point. Over-the-top applications may receive differential transport treatment by the network coordinated by the PCRF. For example, the PCRF can push instructions for the AGW to block traffic flow to a given TCP port.

5.2.4 Local Mobility Anchor (LMA) / Home Agent (HA)

Local Mobility Anchor (LMA) / Home Agent (HA) is the Home Agent for the mobile node in the Proxy Mobile IP domain. It is the topological anchor point for the mobile node's home prefix and is the entity that manages the mobile node's reachability state.

5.2.5 Policy Repository

The Policy Repository provides Home Subscriber Server (HSS) / Subscriber Policy Repository (SPR) services, Layer 3 and optional Layer 2 access network policy repository, and supports the Network Policy Repository (NPR) and capabilities related to offline & online charging.

When a subscriber is roaming, there is a Home Policy Repository (with SPR and H-NPR), containing per subscriber policies and home operator network policies. There is also a Visited Network Policy Repository (V-NPR) that contains policies of the visited network (see section 5.1.2).

The Policy Repository can provide the capability of the authorized entity to indirectly update the policy of a particular subscriber or set of subscribers. The authorized entity can create, modify, and delete particular subscriber's policy stored in the Policy Repository.

5.3 Reference Points

This section describes the reference point interfaces involved in policy management.

AF – PCRF (Tx):

The Tx reference point is used to pass policy information between Application Functions (AF) and the PCRF.

Policy Repository – PCRF (T2):

The reference point between the Policy Repository and the PCRF is used to provide the PCRF with the subscriber policies and network policies.

PCRF – AGW (U23/Ty):

The U23/Ty reference point between Access Gateway (AGW) and the PCRF is used to provide the AGW with subscriber policies and network policies.

PCRF – LMA/HA (U20):

1
2 The U20 reference point connects the LMA/HA and the PCRF, and allows (QoS) policy and
3 charging information to be conveyed to the LMA/HA.
4

5 **H-PCRF –V- PCRF (U18/T3):**

7 The U18/T3 reference point between the Home PCRF and the Visited PCRF provides a
8 means for delivering home network and subscriber policies to the visited network so that they
9 may be reconciled with local policies of the visited network.
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

6 OPERATIONAL PROCEDURES

6.1 Policy Delegation

Central management of policies by a policy management function is crucial, as it implies a single point of access for the network operations personnel and higher control over policy integrity and consistency. The outputs of the policy management process are decisions which guide the behavior of the various elements in the network in support of that request.

There are two types of decisions that the policy management function can make:

One is that the component asking the question should take a particular action.

The second is that the component itself executes a policy in order to govern its behavior, this is called sub-delegation.

Figure 3 shows an example where the PCRF is centralizing the management of policies and is interacting with the network element, in this case the AGW.

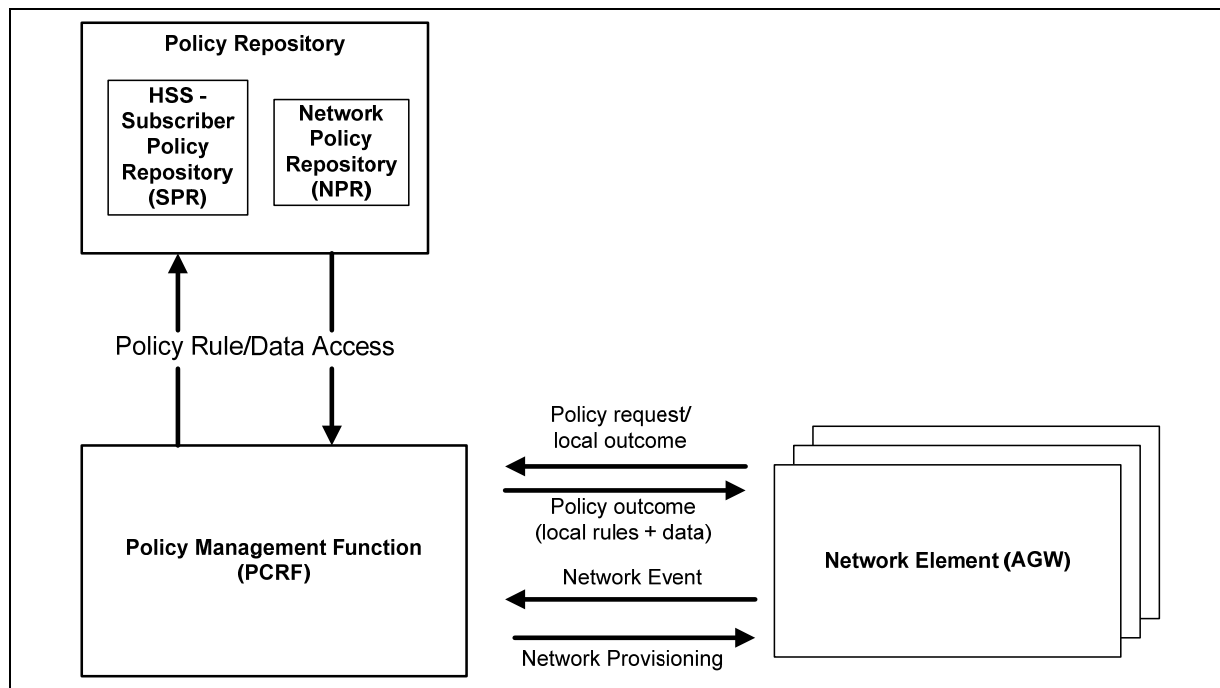


Figure 3 Policy Distribution

The AGW applies service based QoS policy control and/or charging control based on the information it receives from the PCRF or based on some provisioned default. The PCRF may provide service authorized QoS related information, charging rules information, or both in its interactions with the AGW. The AGW applies the information it receives from the PCRF.

6.2 Mobility Management

For further study.

6.3 Admission Control Management

Policy-based admission control ensures that the resources that can be used by a particular set of service data flows are within the “authorized resources” specified via the Tx reference point. Authorization is finding out if the subscriber, once identified, is permitted to have the access to particular network resources and applications. For example, this may be determined by finding out if that customer is a part of a particular group or service plan. In the user plane, admission control is enforced by the gating functionality or QoS can be denied, or the session can be rejected/closed.

6.3.1 Use of Local Resource Based Policy

This specification includes the concept of Local Resource Based Policy (LRBP) and its application during SBBC procedures. The distribution of an operator’s LRBP to a PCRF is outside the scope of this specification. The PCRF is the decision point for LRBP.

LRBP will not be communicated to the AFs for enforcement during service negotiation. LRBP will only be considered during bearer resource authorization procedures.

6.3.2 Authorization for Allocation of Bearer Resources

The AGW is responsible for authorizing access to IP-CAN based on subscription. The PEP (AGW) determines the need for authorization, possibly based on provisioning or based on other attributes of the bearer resource request. The PDP (PCRF) is responsible for LRBP authorization and for assisting (along with the AF) in Service Based Authorization. The PDP will be able to tie the authorization requests back to a specific application that has been invoked by the subscriber. The PDP finds out about IMS applications through the AF, and about non-IMS applications either through the application server itself or through Packet Flow Optimization (PFO) in the AGW. Over-the-top application invocations are determined through PFO in the AGW.

While multiple entities (e.g., AF, PCRF, AAA, AGW) may participate in the process of authorization of a bearer request, all checks must pass if the use of resources is to be allowed. For example, if a particular use would be authorized by a home IP-CAN subscription but is rejected by the visited PCRF based on a local policy check, then the use of resources would not be allowed. The same would be true if the use was authorized by an Application Function but was not allowed based on the IP-CAN subscription check. In this manner, the PCRF always has the last say regarding use of local resources.

The PDP will also use additional parameters, such as the type of access network the subscriber is using, the roaming relationship, ACLs, and even the device type, as well as network conditions in determining the authorized policy for the usage of the application instantiation. In addition, there may also be subscriber policies configured, which are instantiated when the subscriber registers with the network. This authorized policy is then installed into the bearer elements (AGWs) in the form of QoS authorization using either a push model or a pull model.

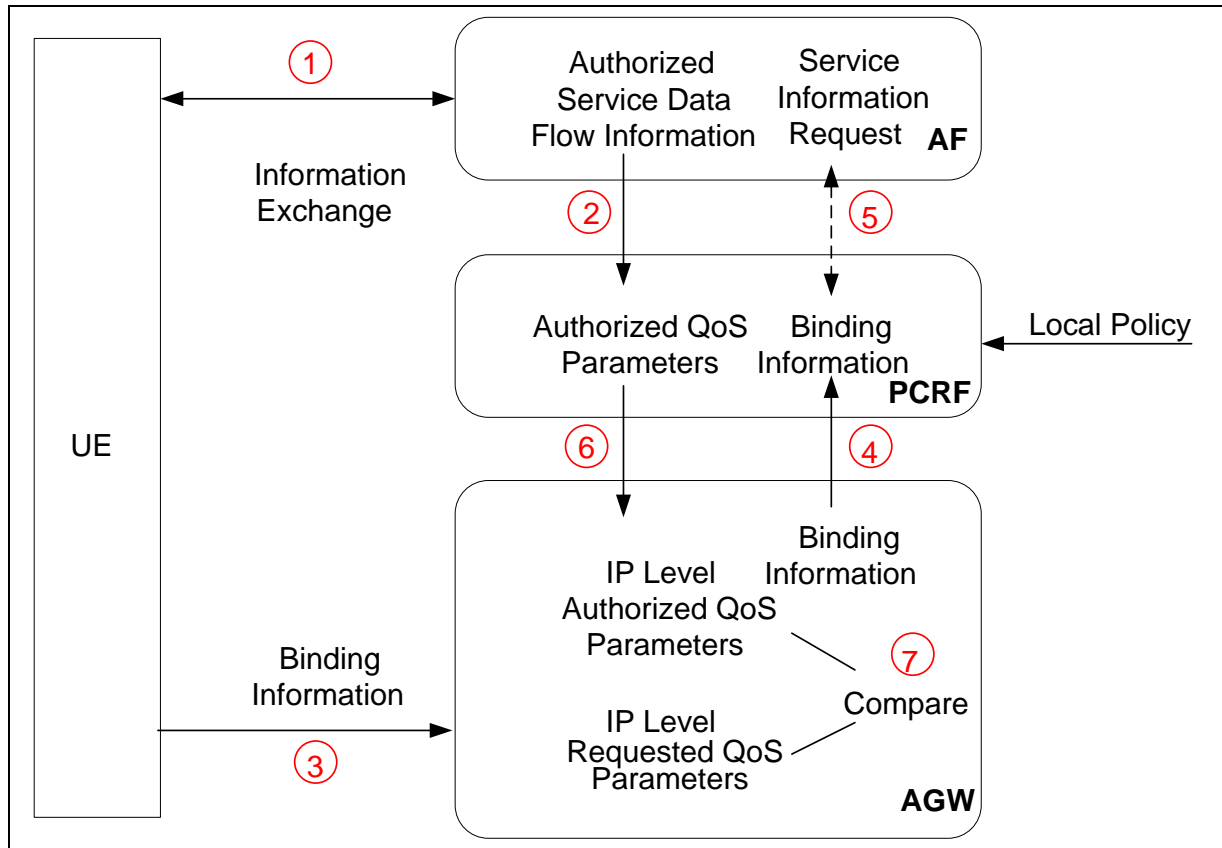


Figure 4 QoS Authorization Entities (Pull)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

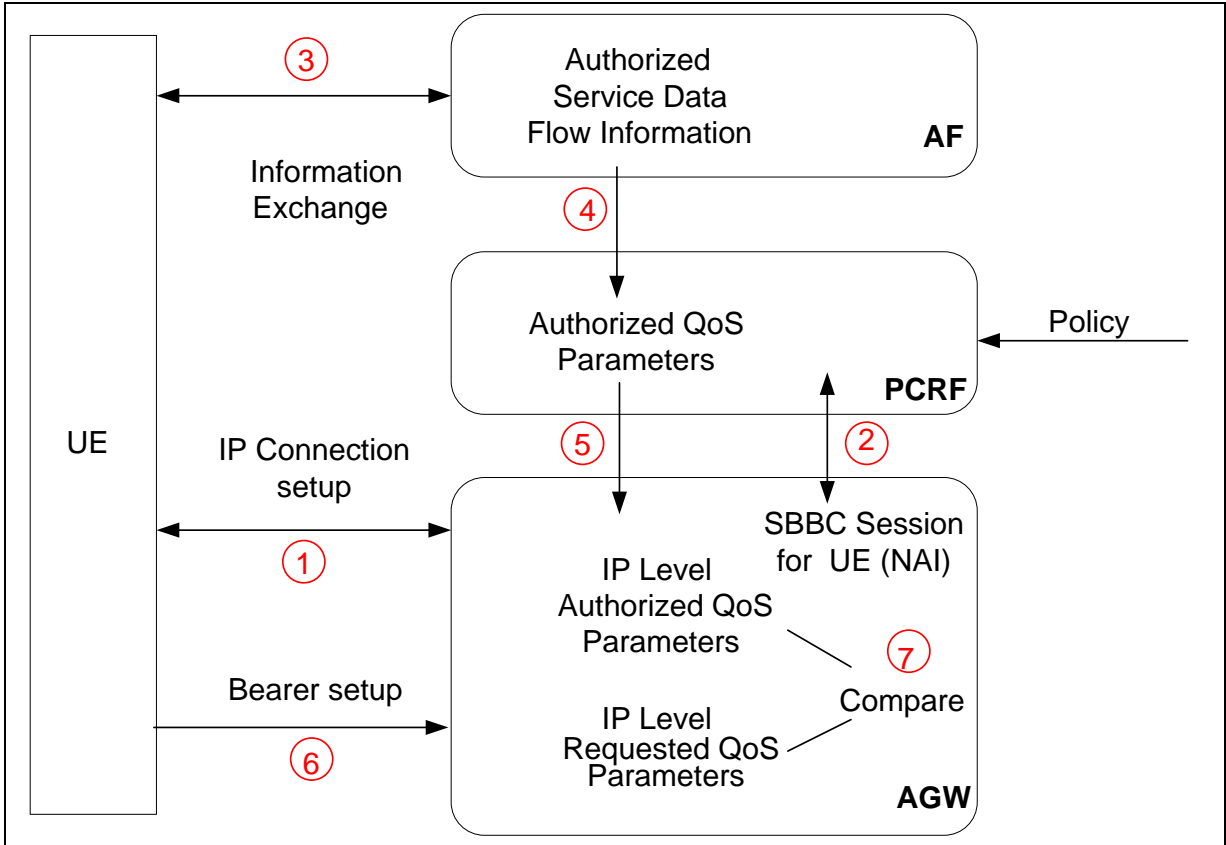


Figure 5 QoS Authorization Entities (Push)

Figure 4 and Figure 5 show the network entities and two different examples of the policy authorization process. Note that the steps in Figure 4 and Figure 5 are not numbered in strict chronological order. In Figure 4, step 1 and step 2 may occur in parallel to the other steps. Step 5 is optional and, when necessary, is invoked by the PCRF after step 4. In Figure 5, step 1 occurs when the UE first attaches to the AGW. The attachment triggers the AGW to establish an SBBC session with the PCRF as shown in step 2. Steps 3 - 5 may happen anytime after step 1.

6.3.3 Gating of IP Packets

The gate is a logical transport-plane function that enables or disables the forwarding of IP packets associated with a packet flow. Therefore, gates provide control points for the connection of the access network to the backbone network. The gates are unidirectional and are managed independently for each packet flow. The gates are implemented by the AGW and are uniquely identified with the respective gate-id identifiers. Gating control should be applied on a per service data flow basis. For each unidirectional packet flow, the associated gate is either opened or closed depending on the flow status and the access control list associated with this flow.

The AF, through the PCRF, authorizes the opening or closing of a gate in the AGW. When the upstream gate is open, the upstream packet filter in the gate allows a flow of packets from a specific IP source address and port number (belonging to the mobile terminal) to a specific IP destination address and port number. When the downstream gate is open, the downstream packet filter in the gate allows a flow of packets, from a specific IP source address and port number to a specific IP destination address and port number (belonging to the mobile

terminal). It should be noted that the source address and port might not always be available. For example, if the application level signaling used is SDP, then the source IP address and source port number may not be known. Hence, these parameters may be specified with a wild card. If a gate is closed, then the IP packets associated with a packet flow are dropped. The gates are closed to any packets that don't match any packet filter of the active PCRF rules.

Besides the flow status, some service data flows can apply the access control lists which are from the PCRF and installed in the AGW. The authorized policy of access control list is only applied when the flow status is enabled. The AGW allows the packets which are allowed by the ACL to pass through and drops any other packets forbidden by the ACL.

6.4 QoS Management

The SBBC architecture supports control of transport reservation procedures (UE-initiated or network-initiated) for IP-CANs to support differentiated QoS in service data flows. This modality of QoS control determines reservation and configuration of IP-CAN bearer resources. Criteria such as the QoS subscription information may be used together with policy rules such as, service-based, subscription-based, IP-CAN-based policies, and/or pre-defined PCRF internal policies to derive the authorized QoS to be enforced for a service data flow. The Policy Enforcement Point (PEP) is the AGW logical function responsible for enforcing the authorized QoS to service data flows in accordance to Policy Decision Point (PDP) decisions. The PDP decisions can be generated at the PCRF or locally at the AGW.

The QoS control mechanism is also responsible for the enforcement of inter-provider Service Level Agreements (SLAs). These SLAs will be part of the peering/roaming agreements between operators. The support of inter-provider QoS brokering and management using policy rules is for further study (FFS).

The QoS control framework in this technical specification accommodates both IMS and non-IMS applications. This allows the service provider to deploy applications regardless of whether they use SIP or not, yet to be able to authorize QoS usage for the applications and their individual flows, on a per-subscriber basis.

The QoS control mechanism necessary to support inter-technology mobility is also FFS. This mechanism shall establish how QoS bindings and reservations for services are transferred between access network technologies so as to preserve negotiated QoS attributes for service data flows.

6.4.1 Segmented QoS Model

Given the complexity of providing end-to-end QoS guarantees, the methodology followed here uses a segmented model comprising three distinct segments: the local access network for the originating side of the session, a backbone network, and the remote access network for the terminating side of the session. This assumption reflects the fact that it is not uncommon that end-to-end service delivery needs to traverse multiple network segments, possibly in distinct administrative domains. The segmented model allows for different techniques to be applied in each segment. The segmented approach also allows for independent controls in a large network, offering a greater degree of flexibility and system stability, but at the same time providing for centralized QoS authorization and end-to-end control. Additionally, the specification assumes QoS control in the access networks with sufficient bandwidth in the backbone network. Specifically, the segmented QoS model exploits the information available from the application signaling protocols (e.g. SIP) to request the appropriate bearer resources on both the local and remote access segments of an end-to-end bearer path. The authorization of bearer resources in the backbone network are outside the scope of this specification. Finally, this specification assumes the controlled network resources are managed on a per packet flow basis.

6.4.2 Resource Reservation

The establishment and modification of a session may involve an end-to-end application-level signaling (e.g. SIP/SDP) with negotiation of media attributes as defined in [MMD part4]. The bearer resource reservation is partitioned into two separate phases, i.e. the reserve phase and the commit phase. At the end of the first phase, bearer resources are reserved but are not yet made available to the mobile terminal. During the first phase, the bearer resource reservation signaling leads to the creation of gates which are used to control the respective packet flows. At the end of the second phase, bearer resources are made available to the mobile terminal (i.e. the gates are opened) and the usage recording is started. However, for some applications, it will be possible to avoid the second phase by committing the bearer resources (i.e. opening the gates) and starting usage recording immediately upon reserving the bearer resources.

The resource reservation parameters may be predefined or dynamically provisioned at establishment and during the lifetime of an IP-CAN session. Predefined resource reservation parameters are necessary when application provided information is unavailable. Gates could be closed or re-opened; packet flows could be created, modified or entirely deleted. In this case, the AF updates the QoS parameters in the PCRF, which in turns updates the AGW.

Details of QoS reservation procedures and mechanisms to prevent cyclic modification of QoS parameters are IP-CAN specific and, as such, not covered in this technical specification.

6.4.2.1 UE-Initiated Requests

During the reservation phase, the mobile terminal requests the reservation of bearer resources from the AGW. The mobile terminal uses the application level service data flow information to derive the QoS parameters for each packet flow. The QoS parameters may represent layer 2 independent descriptions of the traffic characteristics and bearer resource requirements of a packet flow (e.g., flowspecs). To derive the QoS parameters for the application level service data flows, the mobile terminal employs the mapping rules as specified in Annex A of [MMD-013]. Subsequently, the mobile terminal requests from the AGW the bearer resources by specifying the QoS parameters for each packet flow, and includes service binding information (i.e., TFT) in the request. The mechanism by which the application requests QoS and the mechanism for providing the associated QoS parameters from the UE to the AGW is not part of this specification.

If necessary (e.g., the AGW does not already have the policy information), the AGW forwards the service binding information to the PCRF in a request for authorization. The AGW contacts the PCRF based on provisioned information. On receipt of a policy information request from the AGW, the PCRF uses the session identification information (e.g., packet flow) to determine if it already has cached authorized QoS parameters for packet flows relating to this session. If the PCRF is acting as a V-PCRF, the information is routed on to an H-PCRF based on the user transport subscription ID associated with this request. If the PCRF either does not have any information associated with the session, or if the QoS parameters within the policy information request do not fall within the bounds of what is currently authorized for the session, the PCRF may contact the AF using information from an earlier contact. The PCRF authorizes the packet flows by sending to the AGW, the authorized QoS parameters for each packet flow over the Ty interface. Upon receiving the authorization, the AGW creates a gate for each packet flow and informs the mobile terminal that the requested bearer resources have been granted.

6.4.2.2 Network-Initiated Requests

In case of network-initiated requests, the AF acquires service data flow information (e.g., bandwidth, media type) from the application-level signaling (e.g., SDP). The AF caches relevant application-level signaling information for each session. Using the mapping procedures given in [MMD part13], the AF maps the application-level signaling to service

data flows and sends it to a PCRF. An AF may communicate with multiple PCRFs. The AF shall contact the appropriate H-PCRF based on the user-ID associated with this application session (e.g., IMS Private ID). The AF known user-ID must resolve to the same H-PCRF as the user transport subscription ID. The PCRF derives the authorized QoS parameters for each packet flow using the service data flow information received from the AF. The authorized QoS parameters for each packet flow are derived using the rules specified in [MMD-013]. If the AGW has already established an association with the PCRF, the PCRF pushes the authorized QoS parameters for each packet flow to the AGW for policy enforcement. Otherwise, the PCRF saves this information and waits for the AGW to request the information.

6.4.3 Binding Mechanism

Binding is the mechanism that associates a service data flow to the IP-CAN bearer deemed to transport the service data flow. Thus, the binding mechanism associates AF session information with the IP-CAN bearer that is intended to carry its corresponding service data flow(s). The algorithm, employed by the binding mechanism, may contain elements specific for the kind of IP-CAN. Once a data flow is bounded to an IP-CAN bearer, the PCRF can associate the appropriate user and service policy rules to the bearer.

The binding mechanism includes three steps:

1. Session binding, i.e., the PCRF association of the AF session information and applicable policy rules to an IP-CAN session. The IP-CAN session is identified by:
 - The UE IP address of the exact service data flow;
 - The UE identity (of the same kind), if present. Examples of UE identity are: Username (NAI), Calling-Station-ID (MSID), NAS-IP address or NAS-ID, and 3GPP2-Correlation-ID;
 - The information about the Packet Data Network (PDN) the user is accessing.

There could be a 1-to-n mapping between AF session and IP-CAN session (e.g. some IMS session may support different IP addresses for media components). In this case, several IP-CAN session bindings are required for one AF session.

2. QoS authorization, i.e., the selection of a QoS class identifier for each service data flow in the IP-CAN session. QoS authorizations govern packet treatment in the IP-CAN bearers, including bandwidth reservations, packet marking, traffic shaping and policing, authorization envelopes, and gates. The PCRF performs the QoS authorization taking into account the IP-CAN specific restrictions and other policy information available to the PCRF. In case of an aggregation of multiple service data flows, the combination of the authorized QoS information of the individual service data flows is provided as the authorized QoS for this aggregate.
3. Bearer binding, i.e., the association of the QoS authorization to an IP-CAN bearer within that IP-CAN session. For an IP-CAN, limited to a single IP-CAN bearer per IP-CAN session, the bearer is implicit, so finding the IP-CAN session is sufficient for successful binding. Otherwise, the following parameters are used to create the IP-CAN bearer binding for each service data flow:
 - The session binding result;
 - The QoS class identifier of the IP-CAN bearer, if available;
 - The packet-filter information, if available. The filter information includes:

- Destination and Source IP address
- Destination and Source port number
- Protocol ID

Bearer binding is performed by the AGW:

- The QoS class identifier assigned in step 2 above to the service data flow is the main input for this mapping. The AGW evaluates whether it is possible to use one of the existing bearers or not. If that is not possible, the AGW initiates the establishment of a suitable bearer. The binding is created between service data flow(s) and the IP-CAN bearer which have the same QoS class identifier.

For an IP-CAN, where the AGW gains no information on what IP-CAN bearer the UE selects to send an uplink IP flow, the binding mechanism shall assume that, for bi-directional service data flows, both downlink and uplink packets travel on the same IP-CAN bearer.

The enforcement of the authorized QoS of the IP-CAN bearer may lead to a downgrading or upgrading of the requested bearer QoS by the AGW as part of a UE-initiated IP-CAN bearer establishment or modification. Alternatively, the enforcement of the authorized QoS may, depending on operator policy and network capabilities, lead to network initiated IP-CAN bearer establishment or modification.

6.4.4 Enforcement of QoS Authorization

The AGW PEP function enforces QoS-related policies in two different ways:

- QoS class identifier correspondence with IP-CAN specific QoS attributes. The PEP shall be able to convert a QoS class identifier value to IP-CAN specific QoS attribute values (e.g., by defining the appropriate DSCP marking and/or selecting one of a number of pre-configured MPLS LSPs for packet transmission) and determine the QoS class identifier value from a set of IP-CAN specific QoS attribute values.
- IP-CAN bearer QoS enforcement. The PEP controls the QoS that is provided to a combined set of service data flows. The policy enforcement function ensures that the subscription of bearer resources in the IP-CAN is within its established tolerance.

6.4.5 Conflict Detection and Resolution

Service pre-emption priority enables the AGW to resolve conflicts where the activation of all active QoS authorizations for services would result in a cumulative authorized QoS which exceeds the Subscribed Guaranteed bandwidth QoS. The PCRF may resolve the conflict by deactivating those selected authorizations with lower pre-emption priorities and accepting the higher priority service information from the AF. If such a determination cannot be made, the PCRF may reject the service information from the AF.

6.5 Charging Management

The Charging Rules Function (CRF) is the policy decision point responsible for online and/or offline charging control based on charging rules defined by the network operator. Charging rules define service data flows based on packet filtering information, and match service data flows with charging models, methods, and other parameters needed for charging control. The control decision may depend on user subscription data that may apply for both session based and non-session based services, or it may depend on the identity of the network serving the

user (i.e., the same charging rule is applicable to multiple users). Multiple charging rules are supported simultaneously per user and per service data flow.

The Bearer Management Function (BMF) of the AGW is the policy enforcement function for online and/or offline charging rules. Service data flows are identified by the BMF according to filtering information in the charging rules. Any packet associated to a service flow that is subject to charging control can only pass through the BMF if and only if there is a corresponding charging rule associated with it and, if applicable, the online charging system has authorized credit for the service flow.

An exception to the specified charging enforcement behavior is the BMF may let a service data flow pass through the BMF during the course of the credit re-authorization procedure. A credit re-authorization trigger causes the BMF to request re-authorization of the credit to the online charging system. It is up to operator configuration whether the BMF should request credit in conjunction with the charging rule being activated or when the first packet corresponding to the service data flow is detected. The online charging system may either authorize or deny the requested credit.

The charging rules can be either statically pre-provisioned at the BMF or dynamically provided by the CRF. The CRF generates charging rules in order to cover usage scenarios where the filtering information is dynamically negotiated (e.g., negotiated at the application level or to support shared revenue systems). The CRF assigns dynamic charging rules to the BMF at bearer service establishment, modification, and termination.

Upon the initial interaction with the BMF, the CRF may provide charging information containing the address of the online and/or offline charging systems. These shall override any possible predefined addresses at the BMF. The CRF should also provide a default charging method indicating what charging method is to be used in the IP CAN session for every charging rule that omit the charging method and to be applied to data flows associated to over-the-top-applications. During initial interaction the BMF needs to inform the CRF about the existence of predefined charging rules to allow for charging conflict detection and resolution at the CRF level.

6.5.1 Charging Models

The available charging models for Session Based Charging and Flow Based Charging are:

- Volume based charging;
- Time based charging;
- Volume and time based charging;
- Event based charging;
- No charging.

The No charging model is used to indicate to the BMF that charging control is not applicable for a service data flow, i.e., to perform neither accounting nor credit control, and then no online or offline charging information is generated.

The charging rate or charging model applicable to a service data flow may change as a result of events in the service or time of day. For example:

- It should be possible to change the rate based on the time of day.
- The insertion of a paid advertisement within a user requested media stream should result in no charging associated to the user stream. For instance, a video stream may

begin at the start of a session, but the first 30 seconds may include a non-chargeable advertisement.

- The charging rate or charging model applicable to a service data flow may change as a result of having used the service data flow for a certain amount of time and/or volume.
- The user gets to use some services for free after having spent a certain amount of time and/or volume.
- It should be possible to apply a separate rate to a specific service, e.g., allow the user to download a certain volume of data, reserved for the purpose of one service for free, and then continue with a rate causing a charge.
- It should be possible to enforce per-service usage limits for a service data flow using online charging on a per user basis (may apply to prepaid and post-paid users).
- Some services are charged based on activation rather than duration, e.g. 411, or a text message.

The online charging system is responsible for setting and sending the thresholds (time and/or volume based) for the amount of remaining credit to the BMF for monitoring. In case the BMF detects that any of the time based or volume based credit falls below the threshold, the BMF shall send a request for credit re-authorization to the online charging system with the remaining credit (time and/or volume based).

Charging of bearer use of over-the-top applications identified by PFO is charged according to the default charging method installed in the BMF. Since the application is not interacting with the PCRF, no further correlation of accounting records (should the application generate any) can be established directly. Other means of correlating the accounting records may be available, which is considered out of scope for this standard.

6.5.2 Charging Rules

A charging rule shall contain the following parameters:

- Charging Rule Identifier is used between CRF and BMF for referencing charging rules. The charging rule identifiers allocated by the CRF should be unique within the BMF/CRF policy distribution dialogue.
- Charging Key is the reference to the tariff for the service data flow. Any number of charging rules may share the same charging key value. The charging key values for each service shall be operator configurable. Independent credit control for an individual service data flow may be achieved by assigning a unique charging key value for the service data flow in the charging rule.
- Service Identifier identifies the service from the charging rule perspective. Charging rules may share the same service identifier value. The service identifier provides the most detailed identification, specified for flow based charging, of a service data flow. Predefined charging rules may include filters, which support extended capabilities, including enhanced capabilities to identify packets associated with application protocols.
- Charging Rule Precedence is a numeric value establishing a priority ordering of charging rules necessary for the resolution of charging conflicts. The precedence value is used at the BMF to determine the order in which charging rules are to be applied to the service flow.

- Charging Method indicates whether online charging, offline charging, or both are required or the service data flow is not subject to any end user charging. If the charging method identifies that the service data flow is not subject to any end user charging, a Charging Key shall not be included in the charging rule for that service data flow, along with other charging related parameters. If the charging method is omitted the BMF shall apply the default charging method as determined at IP CAN session establishment. The Charging Method is mandatory if there is no default charging method for the IP CAN session.
- Charging Unit indicates, in case of offline charging, whether to record volume- or time-based charging information or both. In case of online charging, the indication of charging unit is passed as a part of credit control.
- Service Identifier Level Reporting indicates whether the BMF shall generate reports per Service Identifier. The BMF shall accumulate the measurements from all charging rules with the same combination of Charging Key/Service Identifier values in a single report.
- Application Function Record Information is an identifier, provided from the AF, to correlate the measurement for the Charging Key/Service Identifier values in a charging rule with application level reports (e.g., IMS).

6.5.3 Conflict Detection and Resolution

Charging rule conflicts can be triggered by overlaps between:

- multiple predefined charging rules in the BMF;
- multiple dynamic charging rules from the CRF;
- charging rules predefined in the BMF and rules from the CRF.

Charging rules conflict should be resolved by applying the charging rule of higher precedence and the following conditions apply:

- When overlap occurs between a dynamically allocated charging rule and a predefined charging rule at the BMF, and they both share the same precedence, then the dynamically allocated charging rule must be applied first.
- It is responsibility of the operator to ensure that overlap between the predefined charging rules can be resolved based on precedence of each predefined charging rule in the BMF.
- It is responsibility of the CRF to ensure that overlap between the dynamically allocated charging rules can be resolved based in precedence of each dynamically allocated charging rule.

6.5.4 Measurements

The Charging Unit field in the charging rule indicates what measurement type is applicable for the service data flow. Admissible measurement types include data volume, duration, combined volume/duration and event based. The BMF measures all the user plane traffic, except traffic that SBBC causes to be discarded. If Service Identifier Level Reporting is mandated in a charging rule, the BMF shall maintain a measurement for the corresponding Charging Key and Service Identifier combination for the service data flow.

6.6 Packet Flow Optimization Management

The role of Packet Flow Optimization (PFO) in the network is to filter IP flows under policy control. PFO policy rules establish which applications the PFO engine should be searching for in an IP flow, and what to do in the event the application is detected. The feature that distinguishes PFO filters over IP flow filters is their additional capability of examining the data part of the IP packets as they pass the inspection point. Once an application is detected, it can be blocked, permitted to proceed, have network resources, such as QoS and packet counters, allocated to it, or otherwise have the network notified of their presence.

PFO functionality may reside in the BMF (e.g. within the LMA/HA, AGW) as shown in Figure 6, or as a separate functional entity from the AGW/BMF as shown in Figure 7. The BMF may be in the serving network, the home network or both. The BMF is an anchor point for bearer traffic, and therefore sees all packets to and from the UE. In both cases (that is, PFO functionality within the AGW or in a separate PFO device), predefined PFO policy rules in the PFO function may include extended service data flow filters, which support enhanced filtering capabilities that cannot be dynamically represented using 5-tuple TFT filters. The syntax and semantics of these extended PFO policy rules is considered outside of the scope of this standard. The PCRF and the PFO shall be able, however, to refer to the PFO rules using simple application identifiers. For instance, the PCRF shall be able to identify the PFO rules related to any given flow profile “A” using an application identifier “A” that can be transferred from the PCRF to the PFO function using either the Tx (in case of an independent PFO device) or an extended version of the Ty reference point (when the PFO functionality is in the AGW).

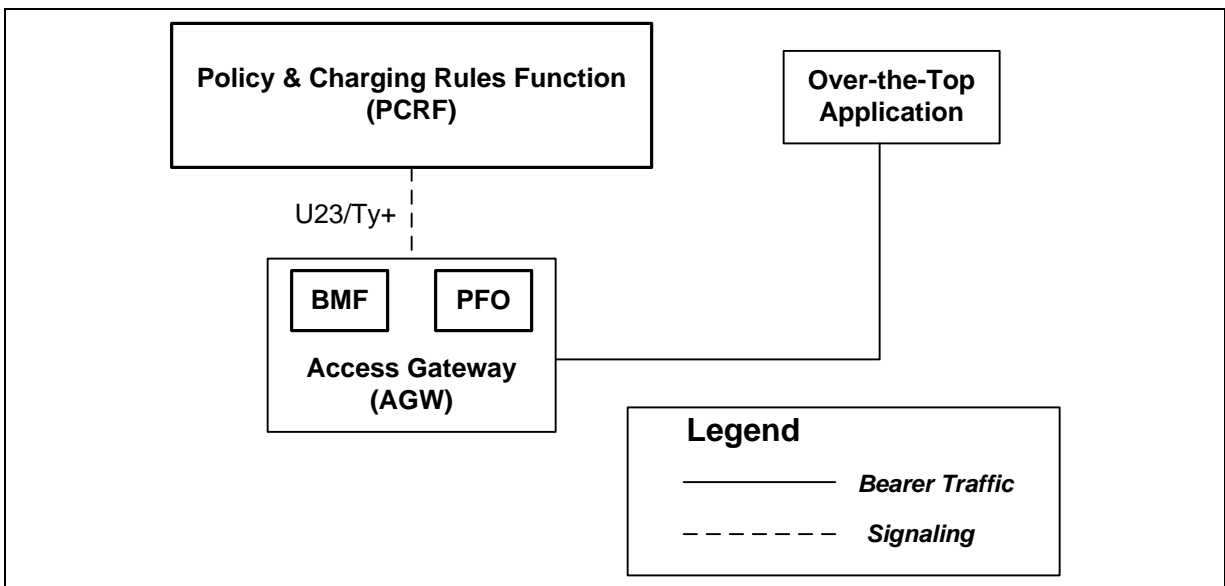


Figure 6 PFO within AGW

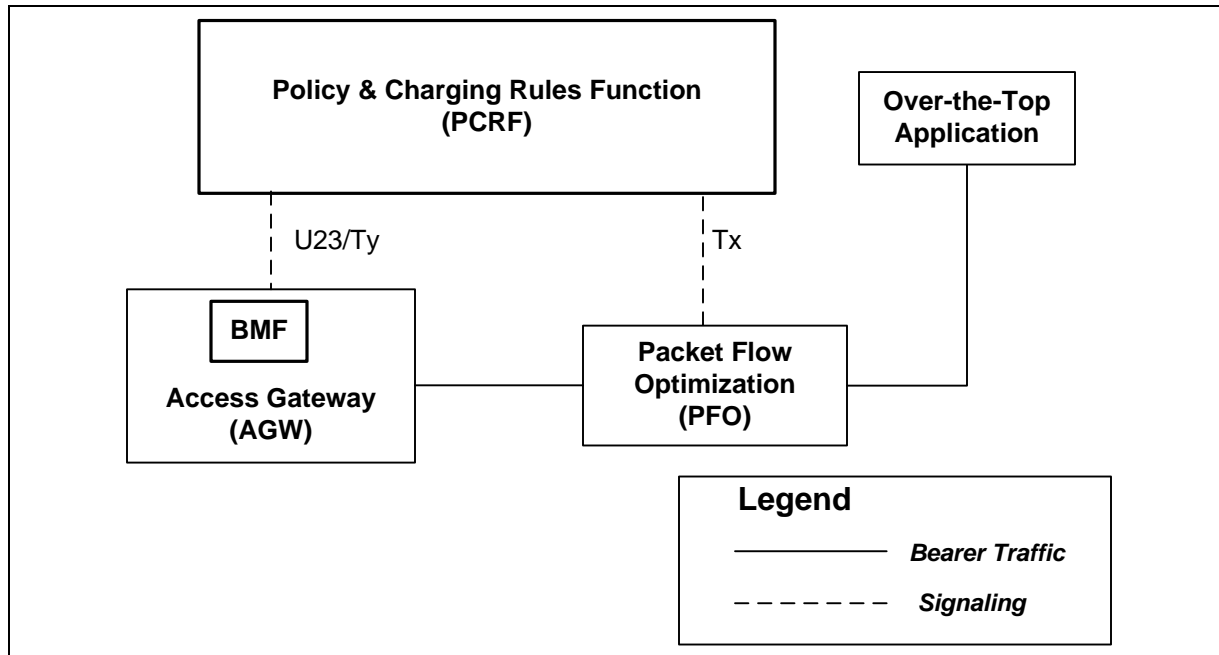


Figure 7 PFO Separate from AGW

By linking PFO with policy, the service provider (e.g. home service provider, visiting service provider or both) gains control over when and why the PFO engine is utilized, and what the BMF should do in the case an application is detected. The action that the PFO engine takes, whenever there is a match with a PFO filter, is to provide the application identity of the IP flow to the PCRF via the Tx or Ty+ interface, depending on where the PFO functionality resides. The PCRF makes a decision about how to proceed with the IP flow, such as to discard the application or permit it. The PCRF may generate or update PCC rules to the PCEF using the Ty+ interface in response to the characteristics provided by the PFO engine. Given the relatively high cost of performing PFO processing, this policy control allows for the operator to use it only when it’s needed. Sample PFO flows are shown in section 6.6.1

A typical application of PFO policy rules is to provide the operator control over, and management of, resources consumed by over-the-top applications running on the network. Table 1 lists other examples of the application of PFO policy rules.

Table 1 PFO Examples

| Example Scenario | Example Policy Applications |
|---|---|
| Subscriber invokes a peer-to-peer file sharing application within an EVDO access network. | Since the handset for this subscriber is capable of supporting file sharing applications, the network policy indicates that PFO is enabled for subscribers with those handsets. Policy is used to reduce the bandwidth allocated to the file sharing application during periods of peak network usage. |
| Subscriber browses a web site with multimedia content. | The service provider can offer more rapid downloads of content from specific sites. The PFO policy is programmed to look for certain URLs, and when one is found, ask for further policy direction. Based on the subscriber identity and usage to date, the user policy can instruct the BMF to allocate additional |

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

| | |
|--|---|
| | bandwidth to this browsing session. |
| Malicious user tries to send files instead of voice RTP packets in their SIP call. | The user policy for this subscriber can indicate that they are a possible malicious user. Network policies indicate that, for possible malicious user, PFO validation of RTP is enabled. At the time of SIP call setup, the BMF is instructed to validate the RTP stream. If it fails validation, the BMF is instructed to generate a flag in the accounting record for the call. |

At the time of Mobile IP registration or IP address allocation, the BMF contacts the PCRF (acting as a policy client). The PCRF, in its response, can activate the predefined charging rules served for the over-the-top application to control the BMF on what applications it should look for, and what to do when that application is detected. The predefined charging rules can tell the BMF to block the app, allow it, or to execute the policy when the app is detected.

The PCRF can also subscribe the application events to the BMF (PEP) at the time of Mobile IP registration, IP address allocation or at some other trigger points, e.g. the policy defined by the operator changes or the deployment of the application changes. By means of the application event subscription, the PCRF can dynamically tell the BMF which PFO rules to activate. When the application is detected, the BMF reports the application event to the PCRF. The PCRF can make the policy decisions based on the current policy contexts and send the policy decisions to the BMF for enforcement.

When an application is invoked, the AF (in the case of a SIP application) or non-SIP application informs the PCRF of this. The PCRF can, at that time, push a PFO policy rule into the BMF to activate it. The purpose of such a policy rule would be to ask the BMF to validate that the bearer traffic for that application matches what the application says it should be. When termination of the application occurs, the AF or non-SIP application informs the PCRF, and the PCRF can remove the PFO policy rule. This allows the service provider to perform PFO for such applications only when they are in use.

Optionally, policy rules may be statically configured in the UE for the non-SIP applications that are defined by a service provider. This optional capability allows the QoS constraints associated with non-SIP applications that are configured, by the service provider, in the UE to be conveyed to the network. The method, for example SIP/SDP, of conveying the QoS constraints, is beyond the scope of this document.

6.6.1 Sample PFO Flows

A sample PFO flow corresponding to the case of PFO functionality residing within the AGW/BMF (as shown in Figure 6) is shown in Figure 8 . A sample PFO flow corresponding to the case of PFO functionality residing within a separate PFO entity (as shown in Figure 7) is shown in Figure 9 . In both cases, we consider that the PCEF is in the AGW. Note, it is also possible for the PCEF to be implemented within the PFO function.

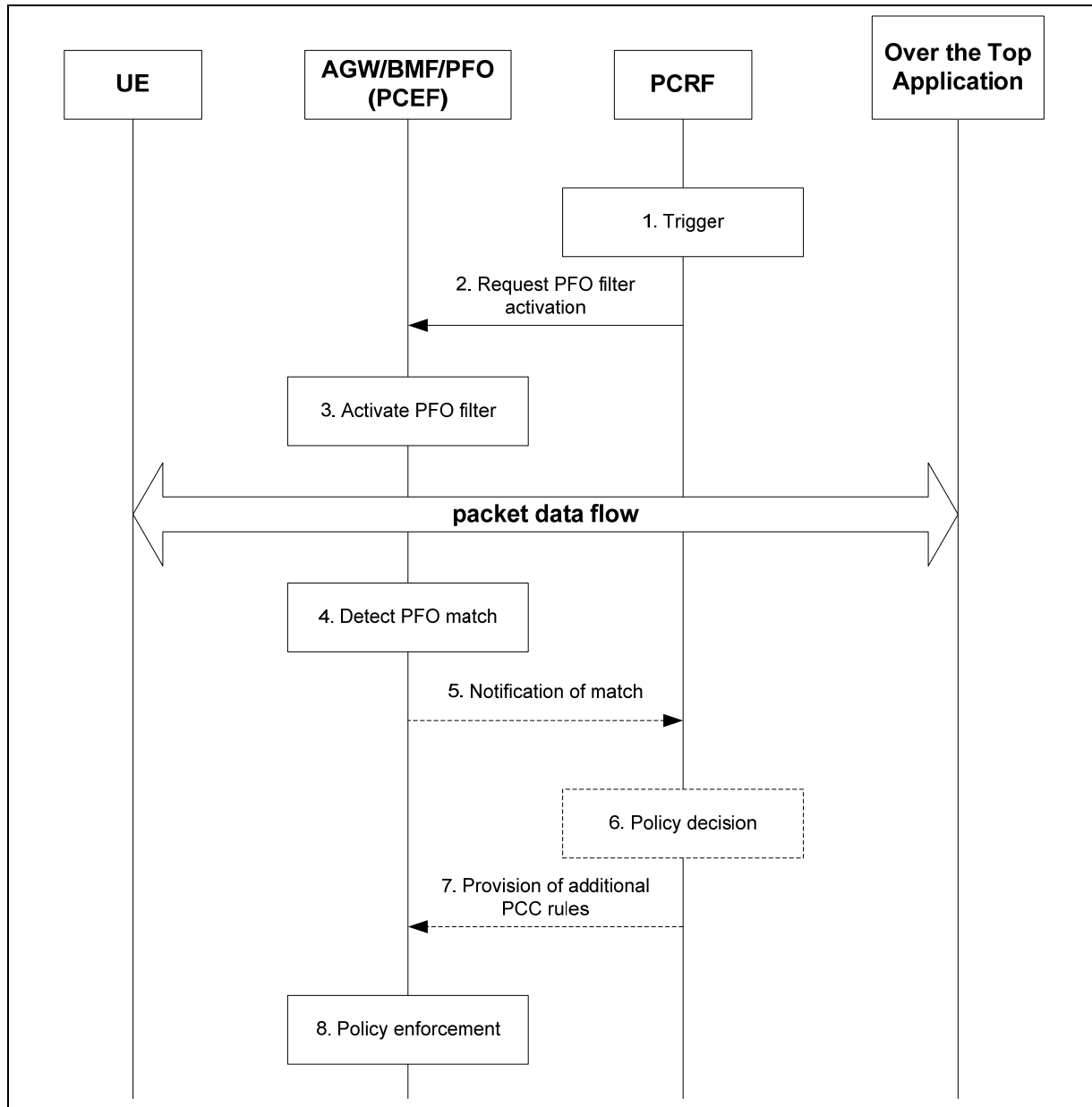


Figure 8 PFO within AGW

1. The PCRF is triggered to deploy PFO filter(s) associated to an (or possibly many) application identifier(s). The trigger event can be a user attachment message, an IP-CAN bearer activation message, or a line command to the PCRF for instance. Before the PCRF is triggered to request PFO filter(s) activation, the PFO function may report the list of application IDs which it supports to PCRF.
2. The PCRF requests the activation of the PFO filter(s) by sending a message to the PFO function with the appropriate application identifier(s). This message traverses the Ty+ interface (i.e., Ty interface enhanced with application identifier).
3. The PFO function selects and activates the requested PFO filter(s) by mapping the application identifier(s) to the corresponding predefined PFO rules.
4. The PFO function detects a data packet that matches an active PFO filter.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

Steps 5 to 7 are conditional since it is possible that the PFO rules already define the enforcement to be made in case of matching packets, e.g., the enforcement can be to drop the matching packets.

5. The PFO function informs the PCRF of the match with the application identifier, application event indicator (e.g., start of the application, termination of the application, etc.) and service data flow information.
6. The PCRF decides which new policy rules should be deployed to deal with the matching flow.
7. The PCRF provisions the new PCC rules to the PCEF (AGW), e.g., establishing a different QoS identifier to the packet, closing the gate, or modifying charging rules.
8. The PCEF enforces the new policy rules associated to the matched PFO filter.

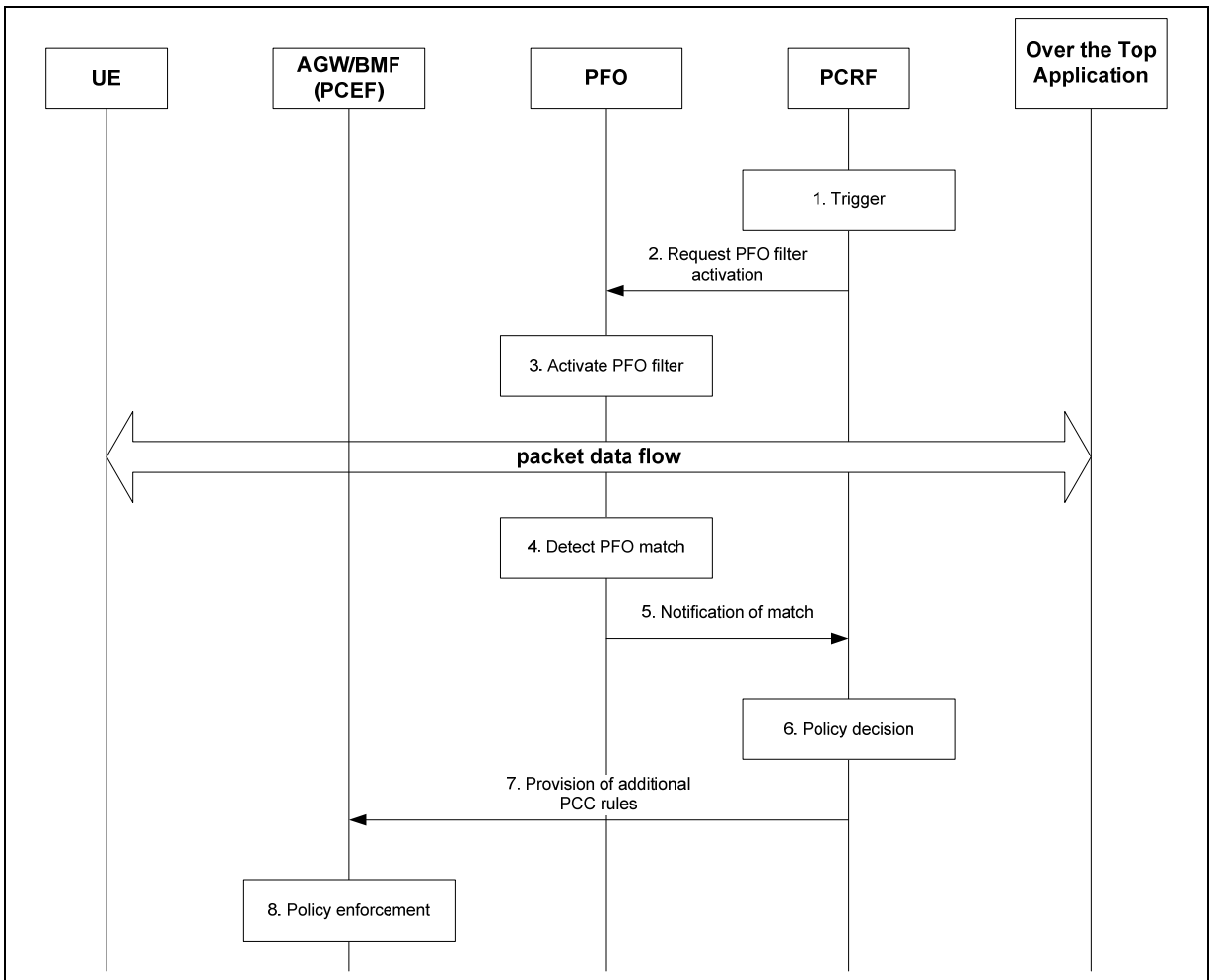


Figure 9 Separate PFO Entity

1. The PCRF is triggered to deploy PFO filter(s) associated to an (or possibly many) application identifier(s). The trigger event can be a user attachment message, an IP-CAN bearer activation message, or a line command to the PCRF for instance. Before the PCRF is triggered to request PFO filter(s) activation, the PFO function may report the list of application IDs which it supports to the PCRF.

2. The PCRF requests the activation of the PFO filter(s) by sending a message to the PFO function with the appropriate application identifier(s). This message traverses the Tx interface.
3. The PFO function selects and activates the requested PFO filter(s) by mapping the application identifier(s) to the corresponding predefined PFO rules.
4. The PFO function detects a data packet that matches an active PFO filter.
5. The PFO function informs the PCRF of the match with the application identifier, application event indicator (e.g., start of the application, termination of the application, etc.) and service data flow information.
6. The PCRF decides which new policy rules should be deployed to deal with the matching flow.
7. The PCRF provisions the new PCC rules to the PCEF (AGW), e.g., establishing a different QoS identifier to the packet, closing the gate, or modifying charging rules.
8. The PCEF enforces the new policy rules associated to the matched PFO filter.

6.7 Service Interaction Management

Service interaction management refers to a broad set of procedures that are necessary to address the impacts of invoking one feature or service upon the invocation of another feature or service. Service interactions can occur between SIP-based features, as well as between non-SIP based features and between SIP-based features and non-SIP-based features.

This broad set of service interactions may involve the interaction of various functional components in the MMD network. The Service Broker (SB), a specialized Application Server (AS), controls the management of the interacting services, based on policies that may put constraints on how different services/features may be invoked simultaneously. The SB may apply the policy constraints, possibly in conjunction with an interaction with the user, and inform the associated application servers.

6.8 Privacy Management

For further study.

6.9 Authentication Management

For further study.

6.10 Network Selection

For further study.

6.11 Security Management

For further study.

7 INFORMATION FLOWS

7.1 AF Session Establishment or Modification – Non Roaming

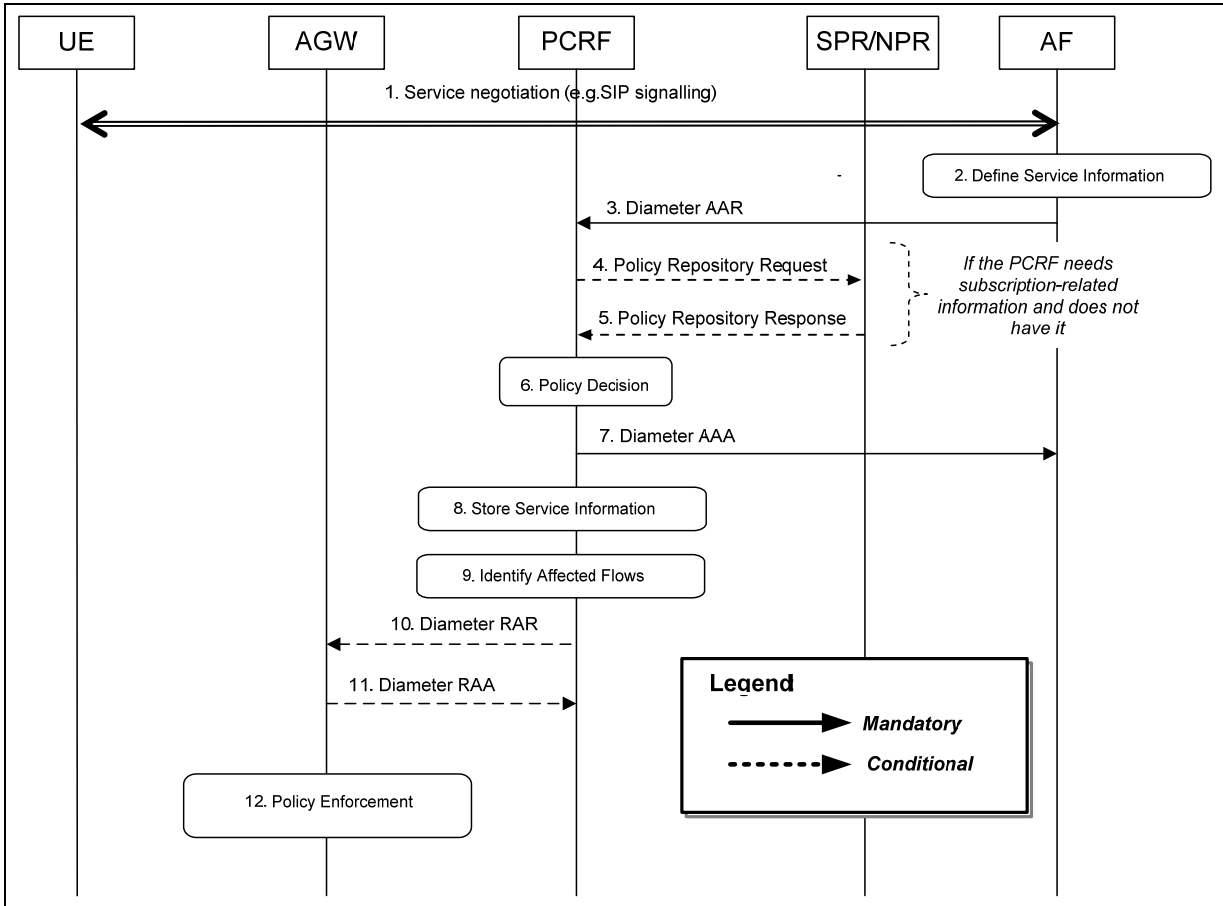


Figure 10 AF Session Establishment or Modification – non Roaming

1. The AF receives an internal or external trigger to provide Service Information, at a set-up of a new AF session or at a modification of an existing AF session.
2. The AF identifies the Service Information needed (e.g. IP address of the IP flow(s), port numbers to be used etc...).
3. The AF provides the Service Information to the PCRF by sending a Diameter AAR for a new Tx Diameter session at set-up of a new AF session, or for the existing Tx Diameter session in case of AF session modification.
4. If the PCRF needs subscription related information it sends policy repository requests to the SPR and/or NPR.
5. The PCRF receives repository response(s) back for any requests it made in step 4.
6. The PCRF makes the policy decision.

7. The PCRF sends a Diameter AAA to the AF. This may be done anytime following step 6, e.g., after step 11.
8. The PCRF stores the received Service Information
9. The PCRF identifies any affected IP flows described in the AF Service Information.
10. If any affected IP flow(s) are identified in step 9, steps 10 through 12 are performed. If there are no IP flow(s) affected, steps 10 through 11 are not executed.
11. The Policy Information is provisioned by the PCRF to the AGW using Diameter RAR. The PCRF may also provide event triggers listing IP flow events for which the PCRF desires Policy Information Requests.
12. The AGW sends RAA to acknowledge the RAR.
13. The AGW enforces Policy based on the rules provided in step 10.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

7.2 AF Session Establishment – Roaming – Home Routed Traffic

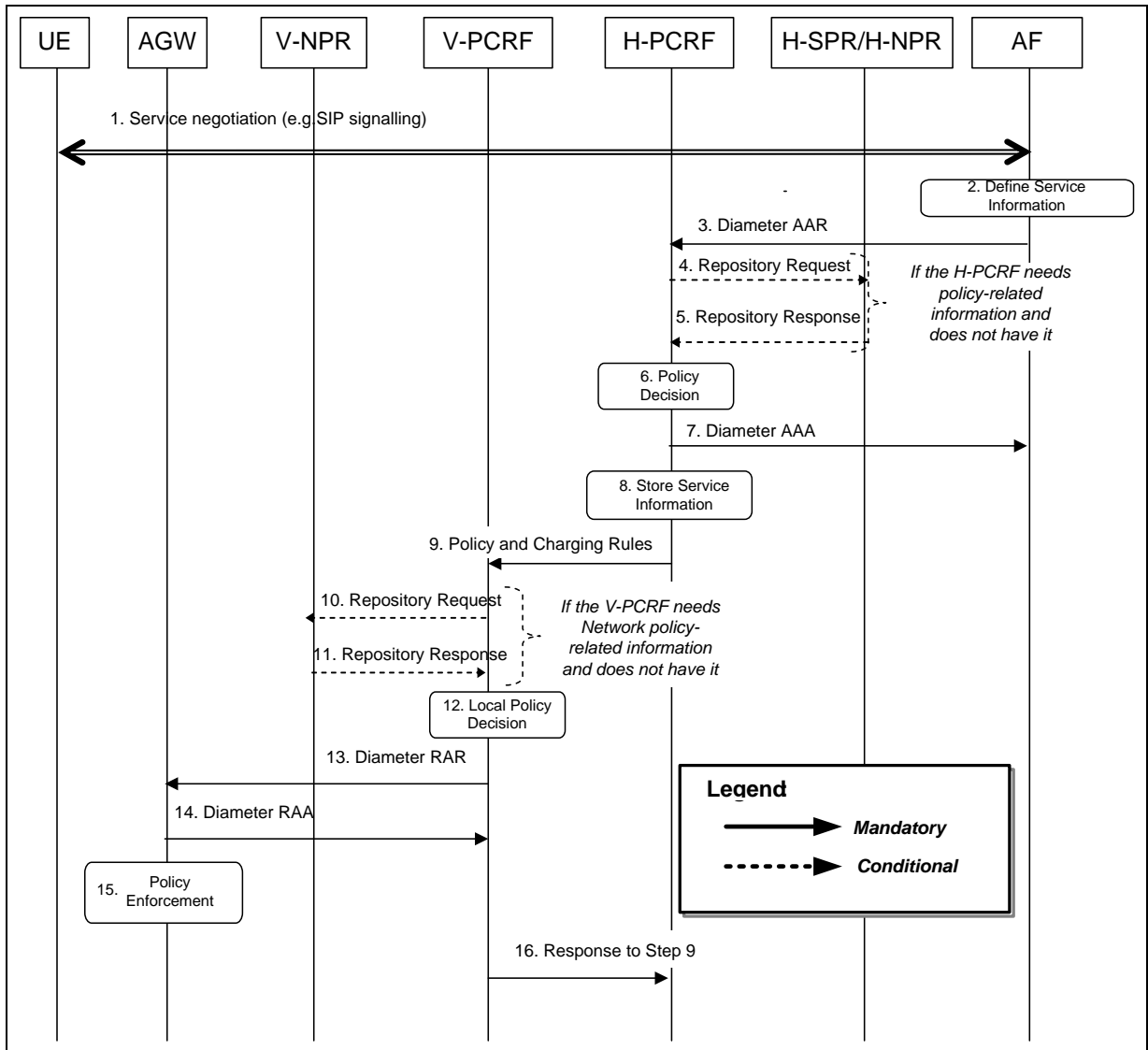


Figure 11 AF Session Establishment – Roaming – Home Routed Traffic

1. The AF receives an internal or external trigger to provide Service Information.
2. The AF identifies the Service Information needed (e.g. IP address of the IP flow(s), port numbers to be used etc...).
3. The AF provides the Service Information to the H-PCRF by sending a Diameter AAR for a new Tx Diameter session at set-up of a new AF session, or for the existing Tx Diameter session in case of AF session modification.
4. If the H-PCRF needs network related policy information it sends policy repository requests to the H-NPR.
5. The H-PCRF receives a repository response back for any request it made in step 4.

6. The H-PCRF makes the authorization and policy decision.
7. The H-PCRF sends a Diameter AAA to the AF. This may be done anytime following step 6 (e.g., after step 16).
8. The H-PCRF stores the service information.
9. The Policy Information is sent by the H-PCRF to the V-PCRF.
10. If the V-PCRF needs network related policy information it sends policy repository requests to the V-NPR.
11. The V-PCRF receives a repository response back for any request it made in step 10.
12. The V-PCRF may modify the policy decision(s) sent by the H-PCRF, for example, based on the roaming agreement between the visited network and the user's home network.
13. The Policy Information is sent by the V-PCRF to the AGW using Diameter RAR. The V-PCRF may also provide event triggers listing IP flow events for which the V-PCRF desires Policy Information Requests.
14. The AGW sends RAA to acknowledge the RAR.
15. The AGW enforces Policy based on the rules provided in step 13.
16. A response to step 9 is sent to the H-PCRF from the V-PCRF.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60