Configuration Guide for Access and Charging Control (Gx)

Ericsson Service-Aware Policy Controller

USER GUIDE

16/1553-CSH 109 215/7 Uen B1

Copyright

© Ericsson España, S.A. 2017. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.

Abstract

This document is a guideline to configure the SAPC for the most typical functions related to Access and Charging Control.

Contents

1 Configure Access and Charging Overview

Next figure, shows the main parts related to configuration and provisioning in the SAPC.

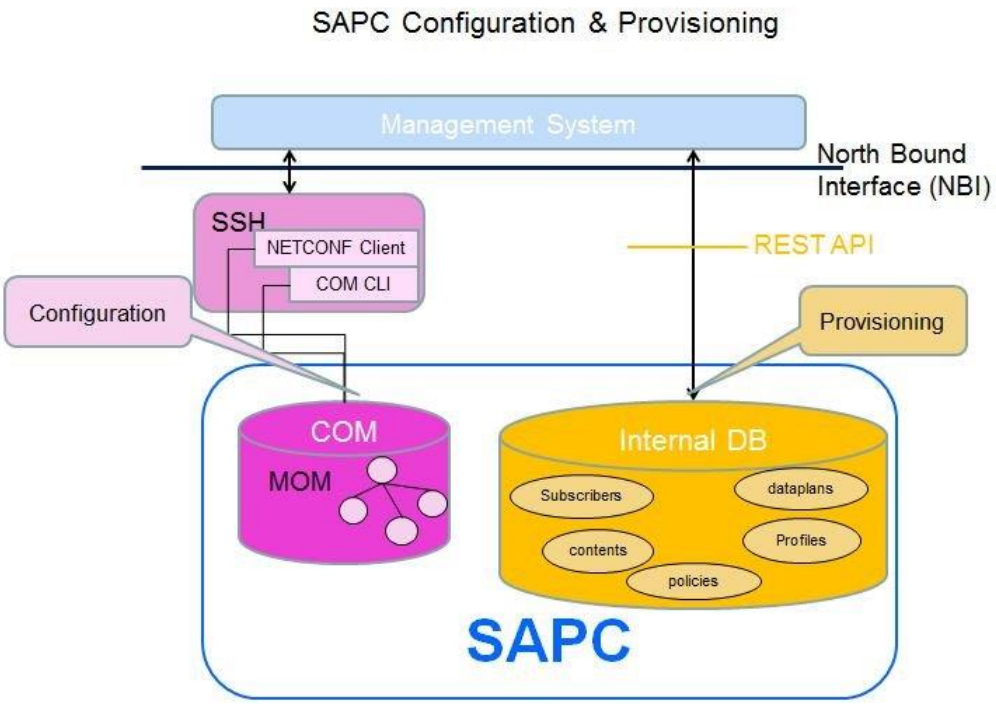


Figure 1 Configuration and Provisioning Overview

The purpose of this document is to provide guidelines to configure the SAPC for Access and Charging Control by providing configuration examples.

This document is not intended as an exhaustive guide to configure the SAPC for every possible scenario.

To understand general provisioning concepts and details regarding subscriptions and policies, refer toConfiguration Guide for Subscription and Policies.

The complete parameter list and details of all configured options of the SAPC are included in separate documents, refer to Managed Object Model (MOM) and Provisioning REST API.

Examples on this document cover the case of data configured in the SAPC internal repository. In case an external repository is used, refer to Database Access.

Next table summarizes the configuration elements in the SAPC related to access and charging control.

Table 1 The SAPC Configuration Elements for Access and Charging

Function		Unconditionally	Dynamically (policies)	Applicable to Diameter Node supporting Protocol
IP-CAN Session Access Control		No	Yes Section 6 on page 21	standard 3GPP Gx Rel9 onwards
Service Access Control	Static Services	Yes	No	standard 3GPP Gx Rel9 onwards
	Preconfigured Services	Yes	No	standard 3GPP Gx Rel9 onwards
	Service Authorization	Yes Section 7 on page 23	Yes Section 7.1 on page 23	standard 3GPP Gx Rel9 onwards
	Rule Spaces	Yes Section 7.4.1 on page 29	No	Ericsson Gx+ interface
	Rule Space Negotiation	No	Yes Section 7.4.2 on page 29	
	One Time Redirect	Yes	No	
Service Charging Control	Static Services	Yes Section 8.1 on page 31	Yes Dynamic Policy Control for Bandwidth Management and Service Charging (Policies for Static Access) Section 7.3 on page 26	Standard PCEF
	Preconfigured Services	Yes Section 8.2 on page 31	Yes Section 8.2 on page 31	Standard PCEF
Subscriber Charging Control		Yes Section 10.4 on page 36	Yes Section 10.5 on page 37	Standard PCEF
Content Filtering Control		Yes Section 11.1 on page 39	Yes Section 11.2 on page 39	Ericsson Gx+ interface

Table 1 The SAPC Configuration Elements for Access and Charging

Function	Unconditionally	Dynamically (policies)	Applicable to Diameter Node supporting Protocol
Header Enrichment	Yes Section 12 on page 41	No	Ericsson Gx+ interface
Event Triggers	Yes Section 5	Yes Section 5	standard 3GPP Gx Rel9 onwards
Presence Reporting Area	Yes Section 13.2 on page 43	Yes Section 13.3 on page 43	standard 3GPP Gx Rel9 onwards

1.1 Other Conventions

This document refers to some configuration and provisioning data.

To clarify which detailed data is managed by COM or by the REST API, this document uses the following conventions:

— Configuration: whenever referring to Managed Object Class (MOC).

The detailed description for the object and attributes can be found in Managed Object Model (MOM).

Example: set `enableReauthsOnSubsChange` attribute in class AppConfig.

The tools or interfaces to manage these data in the SAPC are:

a NETCONF interface, refer to Ericsson NETCONF Interface.

The configuration examples show the NETCONF file contents, using the following syntax:

```
<edit-config>
  ...
  <config>
  <ManagedElement xmlns="urn:com:ericsson:ecim:ComTop">
  <managedElementId>1</managedElementId>
       ...
  </ManagedElement>
  </config>
</edit-config>
```

b Or COM CLI, refer to Ericsson Command-Line Interface.

— Provisioning: mainly subscribers, subscriber groups (dataplans), services (contents), profiles, and policy-related data. The SAPC provides a REST API for them, see Provisioning REST API.

  This document uses the following terminology for them: <resource-name> URI in the provisioning REST API.

  Example: To provision subscriber groups, use the `dataplan` URI in the provisioning REST API.

  And provisioning examples show HTTP operations on REST resources with the following syntax:

  ```
  HTTP-Operation /resource-URI
      {json content}
  ```

  where /resource-URI is the relative URI from the SAPC provisioning base URI detailed in Provisioning REST API.

  Example:

  ```
  PUT /dataplans/Gold
  { "dataplanName" : "Gold",
    "subscribedContents" : [{"contentName" : "HTTP_Streaming",
                             "redirect" : false}]
  }
  ```

  Note: To ease provisioning operations, the SAPC provides an HTTPS CLI client named `resty`, refer to Provisioning Tools.

2 Configuration Prerequisites

Before configuring the SAPC in an operational network, assure that:

— CBA Components are installed.

— The SAPC product software is installed.

— To have a detailed understanding of the function.

3 Configure Gx Diameter Network Data

Note: Origin-Host, Origin-Realm, IP address and diameter port values are set during the SAPC installation procedure. Diameter data related to capabilities exchange (application and vendor identifiers) are provided at installation time, so that no manual procedure is needed.

3.1 Configure Gx PCEFs

The `controls` (for example IP-CAN Session Access Control, Service Access Control) that the SAPC executes when receiving Gx traffic, are configured at PCEF level. To define a PCEF, create a `DiameterNode` instance using the value sent by the PCEF in `Origin-Host` AVP as `diameterNodeId` key.

Note: The SAPC does not execute any default action for a control that is not configured on the Diameter node. The values in `controls` attribute are detailed along SAPC Configuration Guide documents (including this document).

The following example shows a GGSN/PDN-GW configuration supporting IP-CAN Session Access Control, Service Access Control, and Bearer QoS Control:

```
<edit-config>
    <target>
        <running/>
    </target>
    <config>
    <ManagedElement xmlns="urn:com:ericsson:ecim:ComTop">
    <managedElementId>1</managedElementId>
    <dnPrefix>dc=ManagedElement</dnPrefix>
    <networkManagedElementId>1</networkManagedElementId>
    <userLabel>Managed Element</userLabel>
        <PolicyControlFunction xmlns="urn:com:ericsson:ecim:sapcmom">
        <policyControlFunctionId>1</policyControlFunctionId>
            <Network xmlns="urn:com:ericsson:ecim:networkmom">
            <networkId>1</networkId>
                <DiameterNodes>
                <diameterNodesId>1</diameterNodesId>
                    <DiameterNode xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0" nc:operation="merge">
                    <diameterNodeId>ggsnHostname.operator.com</diameterNodeId>
                        <controls>IP_CAN_SESSION_ACCESS</controls>
                        <controls>SERVICE_ACCESS_PCEF_TOD</controls>
                        <controls>BEARER_QOS</controls>
                        <dynamicServiceSupport>true</dynamicServiceSupport>
                    </DiameterNode>
                </DiameterNodes>
            </Network>
         </PolicyControlFunction>
    </ManagedElement>
    </config>
</edit-config>
```

Example 1 PCEF Configuration

3.1.1 Support for interoperability with PCEFs handling Gx Rel9 versions 9.1.0 or 9.0.0

In order to provide support for Gx Rel9 versions 9.1.0 and 9.0.0, the operator can enable the attribute `gxRel910rLowerCompatibility`. This attribute is configured at the `DiameterNode` level of the PCEF configuration.

When this attribute is enabled (set to `true`):

— `Flow-Description` AVP uplink (direction 'in') inside `Flow-Information` is supported.

— `Flow-Direction` AVP is not supported.

3.2 Configure PCEFs for Interworking with Clustered Diameter Systems

A clustered system is a logical system (for example different hardware boards handling the same pool of UE IP addresses) sending Diameter traffic to the SAPC with different `Origin-Host`, but that from the point of view of the SAPC works as a single entity. This way, the SAPC considers a single peer for the incoming Diameter messages coming from the different Diameter peers (different `Origin-Host`) belonging to the same logical cluster and avoids considering the PCEFs as Multiple Gx.

In the same way, PCEFs working in redundancy mode (for example one acting as active, and another one acting in standby), where they send different `Origin-Host` to handle the same pool of UE IP addresses can be grouped in a logical cluster.

To configure the different `Origin-Host` as a single logical system in the SAPC, do the following:

1. Create a single `DiameterNode` instance: the `diameterNodeId` attribute value (key), is the logical cluster identity (that the SAPC internally considers as the PCEF identifier).

2. Set in `clusterPattern` attribute the value of the pattern to be matched with all the received `Origin-Host`.

Example 2 shows a configuration of two clustered PCEFs. On one hand, PCEF nodes sending `Origin-Host` values like `PCEF-D-1.operator.com` and `PCEF-D-2.operator.com` respectively, are grouped as `pcefCluster` from the SAPC point of view, sharing the ending `operator.com` as `clusterPattern` value. On the other hand, nodes sending `Origin-Host` values like `operator-sasn-1.de.com` and `operator-sasn-2.de.com` respectively, are grouped as `sasnCluster`, sharing the beginning `operator-sasn` as `clusterPattern` establishes.

```
<edit-config>
    <target>
        <running/>
    </target>
    <config>
    <ManagedElement xmlns="urn:com:ericsson:ecim:ComTop">
    <managedElementId>1</managedElementId>
        <PolicyControlFunction xmlns="urn:com:ericsson:ecim:sapcmom">
        <policyControlFunctionId>1</policyControlFunctionId>
            <Network xmlns="urn:com:ericsson:ecim:networkmom">
            <networkId>1</networkId>
                <DiameterNodes>
                <diameterNodesId>1</diameterNodesId>
                    <DiameterNode xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0" nc:operation="merge">
                    <diameterNodeId>pcefCluster</diameterNodeId>
                        <controls>IP_CAN_SESSION_ACCESS</controls>
                        <controls>SERVICE_ACCESS_PCEF_TOD</controls>
                        <controls>BEARER_QOS</controls>
                        <clusterPattern>operator.com</clusterPattern>
                    </DiameterNode>
                    <DiameterNode xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0" nc:operation="merge">
                    <diameterNodeId>sasnCluster</diameterNodeId>
                        <controls>IP_CAN_SESSION_ACCESS</controls>
                        <controls>SERVICE_ACCESS_PCEF_TOD</controls>
                        <controls>BEARER_QOS</controls>
                        <clusterPattern>operator-sasn*</clusterPattern>
                    </DiameterNode>
                </DiameterNodes>
            </Network>
        </PolicyControlFunction>
    </ManagedElement>
    </config>
</edit-config>
```

Example 2 PCEF in Cluster Configuration

Note: It is not needed to define a `DiameterNode` instance for each of the `Origin-Host`.

If there are configured several `DiameterNode` instances, one with the complete value of the received `Origin-Host`, and another one as cluster (with the `Origin-Host` value matching with the `clusterPattern` attribute), the SAPC gives precedence to the cluster. The detailed `DiameterNode` instance is not used.

Example: the SAPC receives a Diameter message with `Origin-Host` = node1.myOperator.com, and there are configured the following `DiameterNodes`:

```
DiameterNode=node1.myOperator.com
  controls = ...
  clusterPattern = ""


DiameterNode=clusterMyOperator
  controls = ...
  clusterPattern = "myOperator.com"
```

The SAPC uses the configuration of `DiameterNode` = clusterMyOperator, and ignores the configuration of `DiameterNode` = node1.myOperator.com.

Warning!

If new PCEFs (sending different `Origin-Host` values) are added to a configured logical cluster after ongoing traffic, check that their `Origin-Host` AVP value matches with the `clusterPattern` attribute value of the configured `DiameterNode` instance for that logical cluster.

Otherwise, the SAPC can answer CCR messages with the UNABLE_TO_COMPLY (5012) or DIAMETER_UNKNOWN_SESSION_ID (5002) errors, which can lead to a service outage.

3.3 Configure Multiple Gx Scenario

An IP-CAN session can be controlled by several PCEFs (different `DiameterNode` configured in the SAPC). The typical case for that is that each PCEF enforces a different set of controls. It is needed to configure the `controls` that each PCEF supports. When a Gx request is received, the `controls` supported by the PCEF are checked against what it is configured in the SAPC corresponding `DiameterNode`.

Note: The support for preconfigured and dynamic services has to be enabled only in one of the PCEFs (the one acting as the traffic gateway). Ensure that `dynamicServiceSupport` attribute is set to true in only one `DiameterNode`. Otherwise, Gx traffic related to preconfigured or dynamic PCC rules can malfunction.

The next example shows how some controls are configured for those different PCEFs:

— A Node (`dpiHostname.operator.com`) acting as a Peer to Peer (P2P) services identifier performing Deep Packet Inspection (DPI) that only supports Content Filtering.

— An Ericsson PDN/GW (`ggsnHostname.operator.com`) supporting all controls available in the Ericsson Gx+ interface.

```
<edit-config>
    <target>
        <running/>
    </target>
    <config>
    <ManagedElement xmlns="urn:com:ericsson:ecim:ComTop">
    <managedElementId>1</managedElementId>
        <PolicyControlFunction xmlns="urn:com:ericsson:ecim:sapcmom">
        <policyControlFunctionId>1</policyControlFunctionId>
            <Network xmlns="urn:com:ericsson:ecim:networkmom">
            <networkId>1</networkId>
                <DiameterNodes>
                <diameterNodesId>1</diameterNodesId>
                    <DiameterNode xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0" nc:operation="merge">
                    <diameterNodeId>dpiHostname.operator.com</diameterNodeId>
                        <controls>CONTENT_FILTERING</controls>
                        <dynamicServiceSupport>false</dynamicServiceSupport>
                    </DiameterNode>
                    <DiameterNode xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0" nc:operation="merge">
                    <diameterNodeId>ggsnHostname.operator.com</diameterNodeId>
                        <controls>IP_CAN_SESSION_ACCESS</controls>
                        <controls>BEARER_QOS</controls>
                        <controls>SERVICE_ACCESS_PCEF_TOD</controls>
                        <controls>SERVICE_CHARGING</controls>
                        <controls>SUBSCRIBER_CHARGING</controls>
                        <controls>USAGE_REPORTING</controls>
                        <dynamicServiceSupport>true</dynamicServiceSupport>
                    </DiameterNode>
                </DiameterNodes>
            </Network>
        </PolicyControlFunction>
    </ManagedElement>
    </config>
</edit-config>
```

Example 3 Multiple Gx Configuration

4 Configure Event Triggers Selection

4.1 Provision Unconditionally Event Triggers Selection

To indicate to the PCEFs which are the Gx event triggers at the subscriber level, the subscriber group level, or application level for which the SAPC is interested in receiving CCR Updates, set `eventTriggers` attribute in `subscribers`, `dataplans` or global `dataplans` URI in the provisioning REST API.

Configuring the location change related event triggers (for example RAI change, TAI change, ECGI change, ULI change) at the subscriber or subscriber group level can minimize the network signalling compared to configuring them at the SAPC level.

Example 4 presents the configuration of an event triggers notification at the subscriber level.

```
PUT /subscribers/34610601307

{
 "subscriberId" : "34610601307",
 "eventTriggers": [2,7]
}
```

Example 4 Configuration of Events Notification at the Subscriber Level

In the example above, the SAPC subscribes to RAT change and IP-CAN change event triggers for subscriber "34610601307".

Example 5 presents the configuration of an event trigger at the subscriber group level. In this example, the SAPC subscribes to SGSN change and IP-CAN change event triggers for subscriber group "Gold".

```
PUT /subscribers/34610601307

{
 "subscriberId" : "34610601307",
 "dataplans" :
 [
  {
   "dataplanName" : "Gold"
  }
 ]
}

PUT /dataplans/Gold

{
 "dataplanName" : "Gold",
 "eventTriggers": [0,7]
}
```

Example 5 Configuration of Events Notification at Dataplan Level.

Example 6 presents the configuration of an event notification at the SAPC level. In this example, the SAPC subscribes to SGSN change, RAT change, PLMN change, and successful resource allocation event triggers at application level.

```
PUT /dataplans/global
{
        "dataplanName" : "global",
        "eventTriggers" : [0,2,4,22]
}
```

Example 6 Configuration of Events Notification at SAPC Level

4.2 Provision Event Trigger Selection Policies

To configure event triggers depending on conditions, create the needed policies using:

— For **Global Policy locator**:

`/locators/resources/any/contexts/event-triggers`

— For **Subscriber Group locator:**

`/dataplans/<dataplanName>/locators/resources/any/contexts/event-triggers`

— For **Subscriber locator:**

`/subscribers/<subscriberId>/locators/resources/any/contexts/event-triggers`

— Within the `outputAttributes` object in the `rule`, set:

- `attrName` attribute to `event-triggers`
- `attrValue` to the event triggers list of values, comma separated.

The following example shows a subscriber policy for event triggers selection:

```
PUT /rules/DynamicEventTriggersSubscriber

{
 "condition" : "(AccessData.bearer.accessType==1000)",
 "outputAttributes" :
 [
  {
   "attrName" : "event-triggers",
   "attrValue" : "\"13,48\"",
   "result" : "permit"
  }
 ],
 "ruleName" : "DynamicEventTriggersSubscriber"
}

PUT /policies/DynamicEventTriggersPolicy

{
 "policyName" : "DynamicEventTriggersPolicy",
 "ruleCombiningAlgorithm" : "all-permit",
 "rules" : [ "DynamicEventTriggersSubscriber" ]
}

PUT /subscribers/34610601307/locators/resources/any/contexts/event-triggers

{
 "policies" : [ "DynamicEventTriggersPolicy"]
}
```

Example 7 Dynamic Event Triggers configuration.

4.3 Combining Static Qualification and Policies for Event Triggers

The SAPC combines the event triggers from the dynamic selection and from the static selection together. From the examples above, the SAPC sends the following list of event trigger values:

0, 2, 4, 7, 13, 20, 22, 48

5 Provision Services

The services controlled by the SAPC must be provisioned. To provision services use `contents` URI in the provisioning REST API.

The SAPC supports the following types of services:

— **Static**

  Predefined in the PCEF, activated by the SAPC, and identified in Gx by the `Charging-Rule-Name` AVP or the `Charging-Rule-Base-Name` AVP.

— **Preconfigured**

  Locally set in the SAPC by the operator, downloaded from the SAPC towards the PCEF via Gx using the `Charging-Rule-Definition` AVP.

— **Dynamic**

  Dynamically generated (and modified) in the SAPC from information coming from the Application Function (AF) (by the **Rx Interface**). Dynamic services are downloaded from the SAPC to the PCEF via Gx using the `Charging-Rule-Definition` AVP.

  Covered in Configuration Guide for Dynamic Policy Control (Rx).

The configuration elements related to services provisioning are:

— PCC rules

— Service Charging Data

5.1 Set PCC rules

To set PCC rule for a static or preconfigured service (only a single PCC rule), fill the following attributes in the corresponding `contents` URI in the provisioning REST API:

1. Set `pccRuleName` (unique identifier) attribute
2. **For static PCC rules**

   These PCC rules are identified by a name (`Charging-Rule-Name` AVP) or basename (`Charging-Rule-Basename` AVP). Both the name and basename must be the same as provisioned in the PCEF.

   a When the PCC rule is identified by name, set value `0` in `pccRuleType` attribute

   b When basename is used, set value 1 in `pccRuleType` attribute

For IPv4v6 dual stack IP-CAN sessions, it is necessary to configure some filters in the PCEF to distinguish which PCC rule applies to IPv4 or IPv6.

3. **For preconfigured PCC rules** (identified by `Charging-Rule-Name` AVP)

   1 Set value 2 in `pccRuleType` attribute

   2 To provision the service data flows, use `flows` attribute.

   For IPv4v6 dual stack IP-CAN sessions, it is also possible to define a single PCC rule that contains service data flows for both IPv4 and IPv6.

   3 To set the precedence of a PCC rule compared to other PCC rules running on the same IP-CAN session, set `precedence` attribute.

   The `precedence` attribute can have values from `0` to 2^5-1 meaning the five most significant bits of the priority (lower value means higher precedence). Precedence value is shifted 3 bits and added to the dynamic part.

See Page 18.

Table 2 AVP Precedence

bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
Configurable for preconfigured PCC rules					Dynamic part		

Example 8 provisions different services and PCC rules.

```
PUT /contents/Chat
{
 "contentName" : "Chat",
 "pccRuleName" : "1000",
 "pccRuleType" : 0
}

PUT /contents/Internet
{
 "contentName" : "Internet",
 "pccRuleName" : "2000",
 "pccRuleType" : 1
}

PUT /contents/Skype
{
 "contentName" : "Skype",
 "flows" :
 [
  {
   "destIpAddr" : "any",
   "destPort" : "",
   "direction" : "dl",
   "flowName" : "1",
   "protocol" : "ip",
   "sourceIpAddr" : "10.220.100.1",
   "sourcePort" : "5001"
  },
  {
   "destIpAddr" : "10.220.100.1",
   "destPort" : "5002",
```

```
   "direction" : "ul",
   "flowName" : "2",
   "protocol" : "ip",
   "sourceIpAddr" : "any",
   "sourcePort" : ""
  },
  {
   "destIpAddr" : "any",
   "destPort" : "",
   "direction" : "dl",
   "flowName" : "3",
   "protocol" : "ip",
   "sourceIpAddr" : "2000:1111:2222:4444:5555:ABCD:7777:0002",
   "sourcePort" : "5001-5050"
  },
  {
   "destIpAddr" : "2000:1111:2222:4444:5555:ABCD:7777:0002",
   "destPort" : "5101-5150",
   "direction" : "ul",
   "flowName" : "4",
   "protocol" : "ip",
   "sourceIpAddr" : "any",
   "sourcePort" : ""
  }
 ],
 "pccRuleName" : "5001",
 "pccRuleType" : 2
}

PUT /contents/Streaming
{
 "contentName" : "Streaming",
 "flows" :
 [
  {
   "destIpAddr" : "any",
   "destPort" : "",
   "direction" : "dl",
   "flowName" : "1",
   "protocol" : "ip",
   "sourceIpAddr" : "192.168.1.2",
   "sourcePort" : "5001-5050"
  },
  {
   "destIpAddr" : "any",
   "destPort" : "",
   "direction" : "dl",
   "flowName" : "2",
   "protocol" : "ip",
   "sourceIpAddr" : "192.168.1.2",
   "sourcePort" : "5101-5150"
  }
 ],
 "pccRuleName" : "4033",
 "pccRuleType" : 2,
 "staticQualification" :
 {
  "contentChargingProfileId" : "cp_streaming"
 }
}
```

Example 8 Provisioning of Services

This example provisions the following services:

— A streaming service

  Preconfigured (rule type 2) service, not known by the PCEF, which runs on a set of downlink flows. The streaming server runs on IP address 192.168.1.2,

and uses two different ranges of ports 5001–5050 and 5101–5150. It also has the charging data "cp_streaming".

The id of the PCC rule does not overlap with the ids of the other static PCC rules.

— Skype (Voice over IP) service

Preconfigured service with two different `Charging-Rule-Name` AVPs. This enables two "Skype" service flows, one for IPv4 on "10.220.100.1" IP address, and another for IPv6 on "2000:1111:2222:4444:5555:ABCD:7777:0002" IP address.

— A chat service

Static service known by the PCEF. A static PCC rule identified by name (rule type 0) is sent to the PCEF.

— An internet service

Static service known by the PCEF. A static PCC rule identified by base name (rule type 1) is used. It runs with no specific flows.

6 Configure IP-CAN Session Access Control

To configure IP-CAN session access depending on Conditions, do the following:

1. Configure the `controls` attribute in the `DiameterNode` object class containing value `IP_CAN_SESSION_ACCESS`.
2. Create the needed policies using:
   - For **Global policy locator**:

     `/locators/resources/ip-can-session/contexts/access`

   - For **Subscriber group locator**

     `/dataplans/<dataplanName>/locators/resources/ip-can-session/contexts/access`

   - For **Subscriber locator**

     `/subscribers/<subscriberId>/locators/resources/ip-can-session/contexts/access`

Note: No needed to use `outputAttributes` .

Example 9 describes the provisioning of a policy to accept or reject operations on an IP-CAN session.

```
PUT /rules/IpCanSessionAccessControl_rule
{
 "condition" : "(AccessData.bearer.ipCanType == 5)",
 "ruleName" : "IpCanSessionAccessControl_rule"
}

PUT /policies/IpCanSessionAccessControl_policy
{
 "policyName" : "IpCanSessionAccessControl_policy",
 "ruleCombiningAlgorithm" : "permit-overrides",
 "rules" : [ "IpCanSessionAccessControl_rule" ]
}

PUT /dataplans/Gold/locators/resources/ip-can-session/contexts/access
{
 "policies" : [ "IpCanSessionAccessControl_policy" ]
}

PUT /dataplans/Gold
{
 "dataplanName" : "Gold"
}

PUT /subscribers/34600000001
{
 "dataplans" :
 [

  {
   "dataplanName" : "Gold",
   "priority" : 1
  }
 ],
 "subscriberId" : "34600000001"
}
```

Example 9 Configuration of IP-CAN Session Access Control policy

In this example, the IP-CAN session is allowed if the IP-CAN type is 5 (3GPP-EPS) for the subscriber group with identifier ‘‘Gold’’. Else, the request is rejected.

7 Configure Service Access Control

The services applicable to a Subscriber must be known by the SAPC. These services must be provisioned for the subscriber or the subscriber group in the `subscribedContents` and `deniedContents` attributes of a subscriber or subscriber group.

If time of day (ToD) policies are used for Service Access Control, the PCEF or the PCRF (the SAPC) can be selected as the time controller.

To execute this task in the SAPC, set `controls` attribute (`DiameterNode` object class) only one of the following values:

— `SERVICE_ACCESS_PCEF_TOD`: for PCEFs that support standard ToD procedures (handling of `Revalidation-Time`, `Rule-Activation-Time`, and `Rule-Deactivation-Time` AVPs according to Policy and Charging Control over Gx reference point, 3GPP TS 29.212).

— `SERVICE_ACCESS_PCRF_TOD`: for other cases where the SAPC controls time. The SAPC triggers new reauthorization when time conditions configured in policies are reached.

Set `dynamicServiceSupport` attribute (`DiameterNode` object) to true to enable Gx traffic related to preconfigured or dynamic PCC rules (see example Example 1).

7.1 Provision Policies for Service Authorization

To configure Service Authorization depending on Conditions, create the needed policies using:

— For **Global policy locator**:

```
/locators/resources/<contentName>/contexts/access
```

— For **Subscriber group locator**

```
/dataplans/<dataplanName>/locators/resources/<contentName>/co
ntexts/access
```

— For **Subscriber locator**

```
/subscribers/<subscriberId>/locators/resources/<contentName>/co
ntexts/access
```

Note: No needed to use `outputAttributes`.

Note: Non-authorization codes can be used when the PCEF supports Ericsson Gx+ interface.

To use non-authorization codes in Gx, the condition must follow the following format:

```
#((Condition), non-auth_code)
```

Where condition is the normal condition and the non-auth code is the code that is returned by the SAPC in case that the condition is not fulfilled.

The prioritization of the non-authorization codes can be achieved using the priority of the rules within a policy. If a non-auth code must be returned before any other, the rule that contains the non-auth code must be provisioned in the first place in the rules array.

Next table contains the reason for each of the non authorization codes.

Table 3 Non Authorization Codes

Reason	Code
DENIED_BY_CALENDAR	1
DENIED_BY_ROAMING	2
DENIED_BY_QOS	3
DENIED_BY_BLACK_LISTED	4
DENIED_BY_TERMINAL	5
DENIED_OPERATOR_REASON_ONE	6
DENIED_OPERATOR_REASON_TWO	7
DENIED_OPERATOR_REASON_THREE	8
DENIED_OPERATOR_REASON_FOUR	9
DENIED_OPERATOR_REASON_FIVE	10
DENIED_UNKNOWN_REASON	11
DENIED_USAGE_CONTROL	12

7.1.1 Example of Service Authorization - Global policy for Chat service

A global policy, which applies to all subscribers for Chat service is created in Example 10.

```
# Rule
PUT /rules/SAuth_Chat_Roaming
{
 "condition" : "#((AccessData.subscriber.locationInfo.sgsnAddress == \"172.168.3.4\"),2)",
 "ruleName" : "SAuth_Chat_Roaming"
}

PUT /rules/SAuth_Chat_TerminalBased
{
 "condition" : "#((AccessData.userEquipmentInfo.model==9632),5)",
 "ruleName" : "SAuth_Chat_TerminalBased"
}

PUT /policies/SAuth_ChatPolicy_1
{
 "policyName" : "SAuth_ChatPolicy_1",
 "ruleCombiningAlgorithm" : "deny-overrides",
 "rules" : [ "SAuth_Chat_Roaming", "SAuth_Chat_TerminalBased" ]
}

PUT /locators/resources/Chat/contexts/access
{
 "policies" : [ "SAuth_ChatPolicy_1" ]
}
```

Example 10 Configuration of Service Authorization for Chat service

The “Chat” service is authorized if the SGSN Address is “172.168.3.4” and terminal model is “9632”. If any of the conditions is not fulfilled, the service is not authorized, and the SAPC sends a non-authorization code in the CCA. The priority of non-authorization code “2” is higher than non-authorization code “5”. This is because inside “SAuth_Chat_Policy_1” policy, the rule “SAuth_Chat_Roaming” is evaluated first compared to the rule “Sauth_Chat_TerminalBased”.

7.1.2 Example of Service Authorization - Subscriber policy for Streaming service

```
PUT /rules/SAuth_Internet_AccessBased
{
 "condition" : "#((AccessData.bearer.accessType!=1000),6)",
 "ruleName" : "SAuth_Internet_AccessBased"
}

PUT /policies/SAuth_Internet_Policy_1
{
 "policyName" : "SAuth_Internet_Policy_1",
 "ruleCombiningAlgorithm" : "permit-overrides",
 "rules" : [ "SAuth_Internet_AccessBased" ]
}

PUT /subscribers/34600000001/locators/resources/Internet/contexts/access
{
 "policies" : [ "SAuth_Internet_Policy_1" ]
}

PUT /subscribers/34600000001
{
 "subscriberId" : "34600000001"
}
```

Example 11 Configuration of Service Authorization for Streaming service

The “Internet” service is authorized for the subscriber if access is performed through UMTS Radio Access. If the condition is not fulfilled, the service is not

authorized, and the SAPC includes the non-authorization code 6 (Operator reason 1) in the answer.

7.2 Configure One Time Redirect

This section only applies for authorized static services. To activate or deactivate one time redirect for a service, set `redirect` attribute within `subscribedContents` attribute in a `subscribers` or `dataplans` URI in the provisioning REST API.

7.3 Provision Static Service Policies

Together with the PCEF, the SAPC can assign and change the bandwidth limits and rating group for static services during an IP-CAN session lifetime, depending on flexible conditions for a subscriber or subscriber group.

Some examples of possible use cases are the following:

— Two different ratings can be applied to data services in the Home Network or in roaming for premium and professional subscribers

— Throttle the bandwidth to 128 Kbps for P2P file sharing in rush hours

A static service in the PCEF can be identified by several static service names. Each static service name in the PCEF assigns different characteristics (rating group, service bandwidth, and so on) to the service. The SAPC authorizes the static base name taking into account subscriber information, accumulated use, and roaming (location). The SAPC then selects the right `Charging-Rule-Name` in terms of bandwidth and rating group, depending on the conditions configured in the policies.

To configure Static Services depending on Conditions, create the needed policies using:

— For **Global policy locator**:

```
/locators/resources/<contentName>/contexts/static-access
```

— For **Subscriber group locator**

```
/dataplans/<dataplanName>/locators/resources/<contentName>/cont
exts/static-access
```

— For **Subscriber locator**

```
/subscribers/<subscriberId>/locators/resources/<contentName>/
contexts/static-access
```

— Within the `outputAttributes` object in the `rule` set:

- `attrName` attribute to `pcc-rule-id`.
- `attrValue` to the charging rule name (pccRuleName value).

Table 4 CR-Basename and CR-Names Relation

Service	PccRuleName	PccRuleType	Condition	Charging-Rule-Name
torrent	70	1 (basename)	Limit not surpassed Limit surpassed	70001 70002

Table 5 PCEF Local Data Associated with Downloaded CR-Names

CR-Name	Bandwidth	RatingGroup
70001	1 Mbps	flat rate
70002	128 Kbps	not flat rate

In Example 12, for the ‘‘OneGroup’’ subscriber group, the ‘‘Torrent’’ service is authorized when the subscriber is not roaming. Furthermore, depending on the subscriber consumed volume (details about Fair Usage Control are covered in Configuration Guide for Fair Usage), a different bandwidth and rating group is applied, by sending to the GGSN/PDN-GW either CR-Name = 70001 or CR-Name = 70002.

```
# ------------------------------------------
PUT /rules/rQualify1
{
 "condition" : "not(AccessData.subscriber.accumulatedUsage.reportingGroup[\"total\"].isLimitSurpassed[\"bidirVolu
 "outputAttributes" :
 [
  {
   "attrName" : "pcc-rule-id",
   "attrValue" : "70001",
   "result" : "permit"
  }
 ],
 "ruleName" : "rQualify1"
}

PUT /rules/rQualify2
{
 "condition" : "AccessData.subscriber.accumulatedUsage.reportingGroup[\"total\"].isLimitSurpassed[\"bidirVolume\"]
 "outputAttributes" :
 [
  {
   "attrName" : "pcc-rule-id",
   "attrValue" : "70002",
   "result" : "permit"
  }
 ],
 "ruleName" : "rQualify2"
}

PUT /rules/rule_TorrentAccess
{
 "condition" : "#((AccessData.subscriber.locationInfo.countryCode == 34),2)",
 "ruleName" : "rule_TorrentAccess"
}

PUT /policies/pQualify
```

```
{
 "policyName" : "pQualify",
 "ruleCombiningAlgorithm" : "permit-overrides",
 "rules" : [ "rQualify1", "rQualify2" ]
}

PUT /policies/policy_TorrentAccess
{
 "policyName" : "policy_TorrentAccess",
 "ruleCombiningAlgorithm" : "permit-overrides",
 "rules" : [ "rule_TorrentAccess" ]
}

PUT /dataplans/OneGroup/locators/resources/torrent/contexts/static-access
{
 "policies" : [ "pQualify" ]
}

PUT /dataplans/OneGroup/locators/resources/torrent/contexts/access
{
 "policies" : [ "policy_TorrentAccess" ]
}

PUT /contents/torrent
{
 "contentName" : "torrent",
 "pccRuleName" : "70",
 "pccRuleType" : 1
}

PUT /dataplans/OneGroup
{
 "dataplanName" : "OneGroup",
 "subscribedContents" :
 [
  {
   "contentName" : "torrent",
   "redirect" : false
  }
 ]
}
```

Example 12 Configuration for Qualifying static Charging Rules for PDN-GW

The Access policy composed of “rule_TorrentAccess”, “policy_TorrentAccess”, and `access` context is configured if a flexible condition for the service authorization is needed. These policies are not needed if "torrent" service is always authorized (as it is provisioned in the `subscribedContents` attribute in “OneGroup” subscriber group), and selection of different CR-Names for it depending on the `static-access` policy conditions is the desired behavior.

Bandwidth limits and rating group for static defined services can be also changed depending on time conditions. A specific bandwidth and rating group can be applied in flat hours, and a different bandwidth and rating group for the rest of the time. To achieve that, modify the `condition` attribute of the rules in the previous example. For example:

— for CR-Name = 70002:
`"condition" : "(now.time > "08:00:00") && (now.time < "18:00:01")"`

— and for CR-Name = 70001: the `condition` would be
`"condition" : "(now.time < "8:00:01") || (now.time > "18:00:00")"`

7.4 Rule Spaces

This chapter applies for Ericsson **added-value** (Ericsson Gx+ interface interface).

7.4.1 Provision Rule Spaces

A list of rule spaces and the services (static PCC rules) belonging to that rule space can be configured in the SAPC.

The identifiers and the service definitions of the rule spaces must be the same in the SAPC and in the PCEF.

To define a rule space, create a `rule-space` URI in the provisioning REST API.

Example 13 presents the configuration of a Rule Space.

```
PUT /rule-spaces/RS_Roaming
{
 "contentNames" : [ "Chat", "Internet" ],
 "ruleSpaceName" : "RS_Roaming"
}
```

Example 13 Configuration of Rule Spaces

This example defines the rule space“ RS_Roaming” containing “Chat” and “Internet” services need to be evaluated in case of roaming.

7.4.2 Policies for Rule Space Negotiation

To configure Rule Space Negotiation depending on Conditions, create the needed policies using:

— For **Global policy locator**:

`/locators/resources/service-domain/contexts/access`

— For **Subscriber group locator**

`/dataplans/<dataplanName>/locators/resources/service-domain/contexts/access`

— For **Subscriber locator**

`/subscribers/<subscriberId>/locators/resources/service-domain/contexts/access`

— Within the `outputAttributes` object in the `rule` set:

- `attrName` attribute to `rule-space`
- `attrValue` to the rule space name.

Example 14 presents the configuration of a policy for Rule Space selection.

```
PUT /rules/RSSel_RuleRoaming
{
 "condition" : "AccessData.bearer.accessPoint!=\"OperatorNetwork_1\"",
 "outputAttributes" :
 [
  {
   "attrName" : "rule-space",
   "attrValue" : "\"RS_Roaming\"",
   "result" : "permit"
  }
 ],
 "ruleName" : "RSSel_RuleRoaming"
}

PUT /policies/RSSel_PolicyRoaming
{
 "policyName" : "RSSel_PolicyRoaming",
 "ruleCombiningAlgorithm" : "permit-overrides",
 "rules" : [ "RSSel_RuleRoaming" ]
}

PUT /dataplans/Gold/locators/resources/service-domain/contexts/access
{
 "policies" : [ "RSSel_PolicyRoaming" ]
}
```

Example 14 Configuration of Policy for Rule Space Selection

"Gold" subscribers are explicitly subscribed to the streaming, Skype, and chat services, and indirectly subscribed to the internet service as it is defined in the "Global" subscriber group. The rule space "RS_Roaming" is selected for Gold subscribers, when they access to APNs different than "OperatorNetwork_1".

The rule space "RS_Roaming" contains "Internet" and "Chat" services, so that these are the services considered for authorization.

8 Configure Service Charging Control

To execute this task in the SAPC, set `SERVICE_CHARGING` value in the `controls` attribute (`DiameterNode` object class)

8.1 Static Services

To select different charging data for static services (PCC rules) in the PCEF, the SAPC allows the following options:

a Unconditionally: use `pccRuleName`.

b Depending on conditions, see Section 7.3 on page 26.

8.2 Preconfigured Services

1. Configure Service Charging profiles. The values configured in these Charging Profiles are used to fill charging related AVPs within `Charging-Rule-Definition` AVP. To define a charging profile, create a `content-charging` URI in the provisioning REST API.

2. To unconditionally associate a charging profile with a service:

   In a `content`, set the `contentChargingProfileId` attribute within the `staticQualification` object, with a value according to the `profileId` of a `content-charging` .

3. To configure Service Charging depending on Conditions, create the needed policies using :

   - For **Global policy locator**:

     `/locators/resources/<contentName>/contexts/charging`

   - For **Subscriber group locator**

     `/dataplans/<dataplanName>/locators/resources/<contentName>/contexts/charging`

   - For **Subscriber locator**

     `/subscribers/<subscriberId>/locators/resources/<contentName>/contexts/charging`

   - Within the `outputAttributes` object in the `rule`, set:

     — `attrName` attribute to `charging`

– attrValue to ServiceChargingProfile[\"<chargingProfileId>\"], where chargingProfileId is the profileId of a validcontent-charging

An example for the configuration of Charging Profiles is Example 15.

```
PUT /profiles/content-charging/ChargingType1
{
 "chargingServiceId" : 40000,
 "meteringMethod" : 0,
 "offlineEnabled" : false,
 "onlineEnabled" : true,
 "profileId" : "ChargingType1",
 "ratingGroup" : 1,
 "reportingLevel" : 0
}

PUT /profiles/content-charging/GlobalPrepaid
{
 "chargingServiceId" : 10000,
 "meteringMethod" : 2,
 "offlineEnabled" : false,
 "onlineEnabled" : true,
 "profileId" : "GlobalPrepaid",
 "ratingGroup" : 3,
 "reportingLevel" : 0
}

PUT /profiles/content-charging/TrafficBasedCharging
{
 "chargingServiceId" : 30000,
 "meteringMethod" : 1,
 "offlineEnabled" : true,
 "onlineEnabled" : false,
 "profileId" : "TrafficBasedCharging",
 "ratingGroup" : 4,
 "reportingLevel" : 1
}

PUT /profiles/content-charging/cp_streaming
{
 "meteringMethod" : 0,
 "offlineEnabled" : true,
 "onlineEnabled" : false,
 "profileId" : "cp_streaming",
 "ratingGroup" : 3,
 "reportingLevel" : 0
}
```

Example 15 Configuration of Charging Profiles

Example 8 shows how “Streaming” service is associated with a Charging profile (Service Charging Control is provided): staticQualification contains contentChargingProfileId pointing to “cp_streaming” .

9 Provision Qualification Data for Subscriptions

General concepts on how to Provisioning Subscribers and Subscriber Groups are covered in Configuration Guide for Subscription and Policies.

9.1 Provision Qualification for Subscriber or Subscriber Group Unconditionally

Subscribers or subscriber groups can be qualified for access and charging, by associating a static profile that characterizes them. For example, assigning charging related data. This implies assigning profiles to subscribers or subscriber groups. Static Qos configuration is also part of the Static Qualification for Subscriptions, which are explained in the Configuration Guide for Bearer QoS Control and Bandwidth Management.

To do that:

— Within `subscribers` or `dataplans` URI in the provisioning REST API, set/modify the `staticQualification` object.

Next table contains the particular details for each of the static (qualification data) Subscriber or Subscriber Group Profile

Table 6 Static Subscriber/Subscriber Group Profile

Qualification Data Type	URI in the provisioning REST API	Attribute
Content Filtering (1)	`subscribers` or `dataplans`	`contentFiltering`
Subscriber Charging Information (2)	`subscribers` or `dataplans`	`subscriberChargingProfileId`
Online Charging Information	`subscribers`	`onlineChargingSystemProfileId` (See Configuration Guide for Integration with OCS for Spending Limit Reporting (Sy))
Header Enrichment	`subscribers`	`customerId`
Presence Reporting Area	`subscribers` or `dataplans`	`presenceReportingAreaNames`

(1) To apply this functionality for the PCEF sending Gx requests to the SAPC, configure `controls` attribute within `DiameterNode` object class containing value CONTENT_FILTERING.
(2) To apply this functionality for the PCEF sending Gx requests to the SAPC, configure `controls` attribute within `DiameterNoode` object class containing value SUBSCRIBER_CHARGING.

9.2 Provision Qualification for Subscriber or Subscriber Group Conditionally (depending on policies)

Using policies, it is possible to use conditions to assign profiles to Subscribers or Subscriber Groups. This can be done in addition to static qualification (see Table 6 in chapter 3.4.1).

Set the output attribute of the rule to the desired value for the particular qualification data using the following table:

Table 7 Subscriber Qualification Policies

Qualification Data Type	`resource` **value Within** `locators` **URI in the provisioning REST API**	`context` **value within** `locators` **URI in the provisioning REST API**	`attrName` **attribute within** `outputAttributes` **object**	`attrValue` **attribute within** `outputAttributes` **object**
Content Filtering	`service-domain`	`content-filtering`	`content-filtering`	Content filtering id value
Subscriber Charging Profile (1)	Special value `any`	`charging`	`charging`	`SubsChargingProfile[<subsC`
Presence Reporting Area	Special value `any`	`location`	`presence-area`	`PraProfile[\ "name\"]`

(1) Do not configure time of day conditions within Subscriber Charging policies, as the SAPC does not perform time-based reauthorization.

Combining conditional and unconditional Qualification data

If there are policies configured for a Subscriber, their data prevail over the unconditional qualification data provisioned in the subscriber profile.

If there are policies configured for a Subscriber Group, their data prevail over the unconditional qualification data provisioned in the subscriber group profile.

10 Configure Subscriber Charging Control

1. To execute this task in the SAPC, configure the `controls` attribute in the `DiameterNode` object class with value `SUBSCRIBER_CHARGING`.
2. Provision a Charging System Profile (see Section 10.1 on page 35)
3. Provision Subscriber Charging Profiles (see Section 10.2 on page 35)
4. Configure Subscriber Charging Characteristics Information (see Section 10.3 on page 36)
5. Configure the Charging Information to the subscriber or subscriber group unconditionally (see Section 10.4 on page 36) , conditionally (see Section 10.5 on page 37) or both.

10.1 Provision Charging System Profiles

To provision a Charging System Profile, create a `charging-system` URI in the provisioning REST API.

10.2 Provision Subscriber Charging Profiles

A Subscriber charging profile contains a reference to a charging system and type of charging (online or offline). This charging information can be associated with a subscriber or a subscriber group, and is provided by the SAPC to the PCEF.

To provision a Subscriber Charging Profile, create a `subscriber-charging` URI in the provisioning REST API with the following attributes:

— profileId

— onlineEnabled

— offllineEnabled

— chargingChars (see Section 10.3 on page 36)

— chargingSystemProfileId

Note: The `chargingSystemProfileId` attribute must be set with the `profileId` of a previously provisioned `charging-system` URI in the provisioning REST API.

Example 16 describes the configuration of subscriber charging data.

```
PUT /dataplans/Gold2
{
 "dataplanName" : "Gold2",
 "staticQualification" :
 {
  "subscriberChargingProfileId" : "chargingType01"
 }
}

PUT /profiles/subscriber-charging/chargingType01
{
 "chargingChars" : 987,
 "chargingSystemProfileId" : "ChargingSystem01",
 "offlineEnabled" : false,
 "onlineEnabled" : true,
 "profileId" : "chargingType01"
}

PUT /profiles/charging-system/ChargingSystem01
{
 "primaryOnline" : "primaryChargingHost.ericsson.com",
 "profileId" : "ChargingSystem01",
 "secondaryOnline" : "secondaryChargingHost.ericsson.com"
}
```

Example 16 Configuration of Charging Profiles

This example configures a subscriber charging profile with "chargingType01" identifier and charging characteristic set to "987". This subscriber charging profile configures the subscriber as online in terms of charging. The subscriber charging profile establishes "ChargingSystem01" as the charging system associated with the subscriber. This charging system defines the primary and a secondary host for online charging. The charging profile is associated with the "Gold2" Subscriber Group.

10.3 Configure Charging Characteristics Information

The Charging Characteristics information configured in `chargingChars` attribute within `subscriberCharging` URI in the provisioning REST API is downloaded to the PCEF in the CCA.

The value for charging characteristics is an integer, and if this value is higher than the expected size (65535), its value is truncated to 16 bits.

Charging characteristics data can also be received from the PCEF, and can then be used to evaluate policy conditions for service authorization. Ericsson recommends not to use this value if the charging characteristics for the subscriber have been configured.

Note: This parameter is valid for Ericsson Gx+ interface.

10.4 Provision Unconditional Subscriber Charging Data to Subscriber or Subscriber Groups

To assign an unconditional charging profile to a subscriber or subscriber group, within the `subscribers` or `dataplans` URI in the provisioning

REST API set the `subscriberChargingProfile` attribute with the id of a `subscriber-charging` profile provisioned in the SAPC.

10.5 Provision Conditional Subscriber Charging Data with Policies

To configure Subscriber Charging depending on Conditions, create the needed policies using:

— For **Global policy locator**:

`/locators/resources/any/contexts/charging`

— For **Subscriber group locator**

`/dataplans/<dataplanName>/locators/resources/any/contexts/charging`

— For **Subscriber locator**

`/subscribers/<subscriberId>/locators/resources/any/contexts/charging`

— Within the `outputAttributes` object in the `rule` , set:

- `attrName` attribute to `charging`
- `attrValue` to `SubsChargingProfile[<subsChargingProfileId>` where `subsChargingProfileId` is the id of a valid `subscriber-charging`.

11 Configure Content Filtering Control

To configure Content Filtering Control, do the following:

1. To execute this task in the SAPC, configure the `controls` attribute in the `DiameterNode` object class with value "CONTENT_FILTERING."

2. To associate unconditionally a content filtering profile with a subscriber or subscriber group, see Section 11.1 on page 39)

3. To associate content filtering depending on conditions, see Section 11.2 on page 39)

11.1 Provision Content Filtering for Subscribers or Subscriber Groups.

Set `contentFiltering` attribute within the `staticQualification` object in a `subscribers` or `dataplans` URI in the provisioning REST API.

Example 17 describes how to associate statically a content filtering profile to a subscriber within the `staticQualification` object.

```
PUT /subscribers/34600000001
{
 "dataplans" :
 [
  {
   "dataplanName" : "Gold"
  }
 ],
 "deniedContents" : [ "Chat" ],
 "operatorSpecificInfos" :
 [
  {
   "attributeName" : "age",
   "attributeValue" : "33"
  }
 ],
 "staticQualification" :
 {
  "contentFiltering" : "69"
 },
 "subscriberId" : "34600000001"
}
```

Example 17 Content Filtering Subscriber qualification

This example provisions subscriber "34600000001" belonging to group "Gold" and uses `operatorSpecificInfos` object to indicate the age of the subscriber.

A `contentFiltering` (to be downloaded to the PCEF) set to "69" is also provisioned for the subscriber.

11.2 Provision Content Filtering Policies

To configure Content Filtering depending on Conditions, create the needed policies using :

— For **Global policy locator**:

`/locators/resources/service-domain/contexts/content-filtering`

— For **Subscriber group locator**

`/dataplans/<dataplanName>/locators/resources/service-domain/contexts/content-filtering`

— For **Subscriber locator**

`/subscribers/<subscriberId>/locators/resources/service-domain/contexts/content-filtering`

— Within the `outputAttributes` object in the `rule` , set:

- `attrName` attribute to `content-filtering-id`
- `attrValue` to the content filtering value

Example 18 describes the configuration of a policy to return content filtering profile.

```
PUT /rules/ContentFilteringRule1
{
 "condition" : "(Subscriber.subsAge > 17)",
 "outputAttributes" :
 [
  {
   "attrName" : "content-filtering-id",
   "attrValue" : "9",
   "result" : "permit"
  }
 ],
 "ruleName" : "ContentFilteringRule1"
}

PUT /policies/ContentFilteringPolicy1
{
 "policyName" : "ContentFilteringPolicy1",
 "ruleCombiningAlgorithm" : "permit-overrides",
 "rules" : [ "ContentFilteringRule1" ]
}

PUT /subscribers/34600000001/locators/resources/service-domain/contexts/content-filtering
{
 "policies" : [ "ContentFilteringPolicy1" ]
}
```

Example 18 Configuration of Subscriber Content Filtering Policy

A policy is created for subscriber with identifier “34600000001”, to return as content filtering profile identifier “9” when the age of the subscriber is greater than 17. The age of the subscriber is provisioned in `operatorSpecificInfos` object within the `subscribers` URI in the provisioning REST API.

12 Configure Header Enrichment

The SAPC is able to send towards the GGSN/PDN-GW user-related information to be inserted in the HTTP headers of a particular request so that the service can use this information in its internal logic. One typical application is to provide the third-party applications with a user alias so the MSISDN is not disclosed to them.

The SAPC allows the operator to define any kind of data to be inserted.

This functionality is provided with the Ericsson Gx+ interface and when the SAPC is deployed together with an Ericsson PDN-GW product.

To use Header Enrichment, set `customerId` attribute in the `staticQualificatio n` object of a `subscribers` URI in the provisioning REST API.

13 Configure Presence Reporting Area

The operator can configure presence reporting area selection applicable to a subscriber or subscriber group by using static qualification data or dynamic policies.

When defining the presence reporting area, the identifier is made of 24 bits, where the most significant bit defines the mode (either UE dedicated or CN preconfigured PRA).

Therefore, the most significant bit is 0 (UE dedicated) or 1 (CN preconfigured PRA).

13.1 Provision Presence Reporting Area

To provision a presence reporting area, create a `presence-reporting-area` URI in the provisioning REST API.

```
PUT /profiles/presence-reporting-area/Area1

{
        "name" : "Area1",
        "praId" : 9000001,
        "elementsList":
 {
  "tais" : ["012.45.6789-6791"],
  "macroEnbs" : ["123.456.78901"],
  "homeEnbs" : ["234.567.8901234-8901235"],
  "ecgis" : ["345.678.9012345"],
  "rais" : ["456.789.123.45-46"],
  "sais" : ["567.890.1234.5678"],
  "cgis" : ["678.901.2345.6789-6790"]
 }
}
```

Example 19 Provision Presence Reporting Area

13.2 Provision Unconditional Presence Reporting Area to Subscriber or Subscriber Groups

To assign an unconditional presence reporting area to a subscriber or subscriber group, set the `presenceReportingAreaNames` attribute with the id of a `presence-reporting-area` profile provisioned in the SAPC within the `subscribers` or `dataplans` URI in the provisioning REST API

13.3 Provision Conditional Presence Reporting Area with Policies

To configure Presence Reporting Area depending on conditions, create the needed policies using:

— For **Global Policy locator**:

```
/locators/resources/any/contexts/location
```

— For **Subscriber Group locator:**

```
/dataplans/<dataplanName>/locators/resources/any/contexts/lo
cation
```

— For **Subscriber locator:**

```
/subscribers/<subscriberId>/locators/resources/any/contexts/lo
cation
```

— Within the `outputAttributes` object in the `rule` , set:

- `attrName` attribute to `presence-area`
- `attrValue` to `PraProfile[\"Name\"]`

Example 20 shows the SAPC selecting a presence reporting area for a subscriber using the dynamic policy.

Note: Do not configure time of day conditions in PRA policies, as the SAPC does not perform time of day based reauthorization.

```
PUT /subscribers/34615800304

{
        "subscriberId" : "34615800304",
        "dataplans" :
        [
                {
                        "dataplanName" : "Silver"
                }
        ]
}

PUT /dataplans/Silver

{
        "dataplanName" : "Silver"
}

PUT /rules/PRASelectionGroup_Silver_rule

{
        "condition" : "(AccessData.bearer.accessType==1000)",
        "outputAttributes" :
        [

                {
                        "attrName" : "presence-area",
                        "attrValue" : "PraProfile[\"Area1\"]",
                        "result" : "permit"
                }
        ],
        "ruleName" : "PRASelectionGroup_Silver_rule"
}

PUT /policies/PRASelectionGroup_Silver

{
        "policyName" : "PRASelectionGroup_Silver",
        "ruleCombiningAlgorithm" : "permit-overrides",
        "rules" : [ "PRASelectionGroup_Silver_rule"]
}

PUT /dataplans/Silver/locators/resources/any/contexts/location

{
        "policies" : [ "PRASelectionGroup_Silver" ]
}
```

Example 20 PRA Configuration

In this example, the SAPC defines the presence reporting area "Area1" for subscriber group "Silver" when the "Silver" subscribers access is performed through UTRAN Radio Access.

13.4 Configure Event Triggers for Presence Reporting Area

To subscribe the SAPC to presence area reporting event trigger,the SAPC has to include CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA_REPORT value within Event-Trigger AVP of Gx CCA-initial message.

For details on how to configure event triggers, see Section 4 on page 13.

The following example shows how to configure the presence reporting area event trigger based on access conditions.

```
PUT /policies/DynamicEventTriggersPolicy

{
  "policyName" : "DynamicEventTriggersPolicy",
  "ruleCombiningAlgorithm" : "all-permit",
  "rules" : [ "DynamicEventTriggersRule" ]
}

PUT /rules/DynamicEventTriggersRule

{
  "condition" : "(AccessData.bearer.accessType != 1000)",
  "outputAttributes" :
  [
   {
     "attrName" : "event-triggers",
     "attrValue" : "\"48\"",
     "result" : "permit"
   }
  ],
  "ruleName" : "DynamicEventTriggersRule"
}
```

Example 21 Configuration of Presence Area Reporting Event Trigger based on dynamic conditions

14 Configuration Examples for Use Cases

14.1 Roaming Conditions

Simple conditions to detect roaming have been used in some examples along this document. For example, `AccessData.subscriber.locationInfo.countryCode == 34`.

However, conditions to detect roaming cases can be more complex. For example, some operator may use lists of SGSN-MME IP addresses or multiple PLMN-identifiers.

Next examples shows multiple roaming criteria using Mobile Network Code part of the SGSN PLMN Id (using **Extra Data in internal database** explained in Database Access) and `inRange` function (detailed in Configuration Guide for Subscription and Policies):

```
PUT /operator-specific-infos/Roaming
{
 "infoList" :
  [
   {
    "attributeName" : "networkCodes",
    "attributeValue" : "1-9"
   },
   {
    "attributeName" : "networkCodes",
    "attributeValue" : "12"
   },
   {
    "attributeName" : "networkCodes",
    "attributeValue" : "14-16"
   },
   {
    "attributeName" : "networkCodes",
    "attributeValue" : "21"
   },
   {
    "attributeName" : "networkCodes",
    "attributeValue" : "88"
   }
  ],
 "infoId" : "Roaming"
}
```

Example 22 Roaming criteria as operator-specific-info

```
<edit-config>
  <target>
  <running />
  </target>
  <config>
    <ManagedElement xmlns="urn:com:ericsson:ecim:ComTop">
      <managedElementId>1</managedElementId>
      <dnPrefix>dc=ManagedElement</dnPrefix>
      <networkManagedElementId>1</networkManagedElementId>
      <userLabel>Managed Element</userLabel>
      <PolicyControlFunction xmlns="urn:com:ericsson:ecim:sapcmom">
        <policyControlFunctionId>1</policyControlFunctionId>
        <EntityData xmlns="urn:com:ericsson:ecim:entitydatamom">
          <entityDataId>1</entityDataId>
          <EDSources xmlns="urn:com:ericsson:ecim:edsourcesmom">
            <eDSourcesId>1</eDSourcesId>
            <EDSource xmlns="urn:com:ericsson:ecim:edsourcemom" xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0" nc
             <eDSourceId>Roaming</eDSourceId>
               <definition>
                 def Roaming( argId )
                 {
                   dataSource =
                   {
                     url = "internaldb:";
                     query = "OperatorSpecificInfoPot:{argId}";
                   }
                   fieldDef =
                   {
                     id = dataSourceField("argId");
                     nwCodes = dataSourceField("name:networkCodes");
                  }
                 }
               </definition>
             </EDSource>
            </EDSources>
          </EntityData>
        </PolicyControlFunction>
      </ManagedElement>
  </config>
</edit-config>
```

Example 23 Roaming EDSource

```
PUT /rules/ruleRoaming
{
 "condition" : "inRange(AccessData.subscriber.locationInfo.networkCode,
                        Roaming[\"Roaming\"].nwCodes)",
 "ruleName" : "ruleRoaming"
}
```

Example 24 Complex Roaming Condition

14.2 Cell Congestion

The SAPC can use dynamic subscriber location information in policy decisions, together with cell congestion information provisioned in advanced.

Next figure shows an overview of the configuration schema:

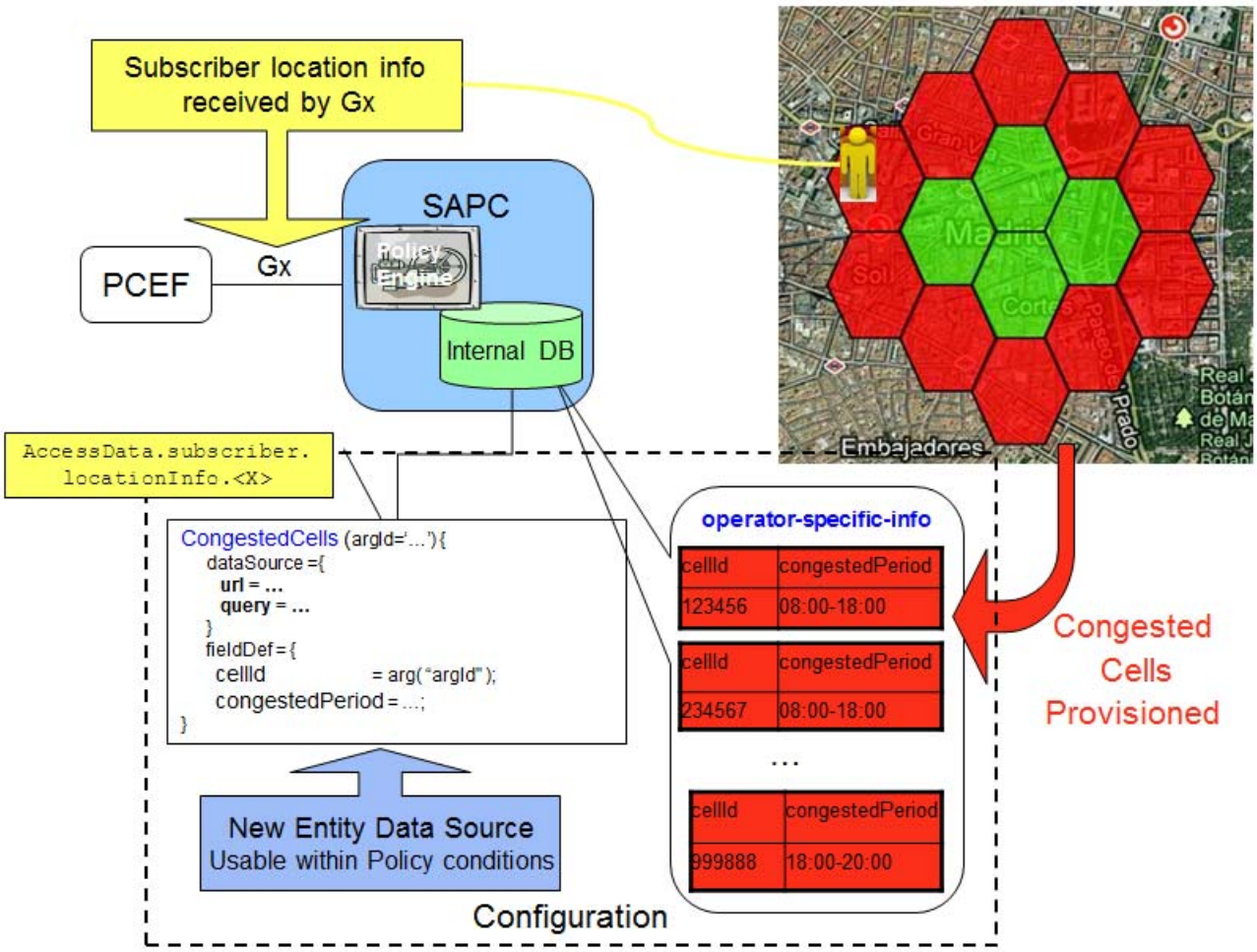


Figure 2 Cell Congestion Configuration

The figure above shows that the subscriber location information received in the SAPC over the Gx interface can be used to verify if the subscriber is in a congested cell. The congested cell identifiers are provisioned in a logical table inside the SAPC internal database, where the period or periods for which the cells are congested can be also set. An Entity Data Source is also needed, so that the information about the congested cells can be used in policy conditions.

To use cell congestion in policies, perform the following steps:

1. To guarantee that the SAPC receives Gx CCR updates when the subscriber is moving, subscribe to the proper location change values of `Event-Trigger` AVP: User Location change, RAI change, TAI change, and ECGI change.

Warning!

The subscription to location change related `Event-Triggers` for all the SAPC subscribers causes a high amount of extra Gx CCR updates signaling in the network. Dimension the SAPC properly or restrict the subscription of location change event triggers only for some subscribers or dataplans. See details in Section 4 on page 13.

2. Configure cell congestion information (at least identities for congested cells) as explained in **Extra Data in internal database** in Database Access:

   a Set the congested cells information, using the `operator-specific-infos` URI in the provisioning REST API

   b Define a new Entity Data Source pointing to the congested cells information.

   Note: The way to locate the configured cell identities, depends on the cellular network plan, and the geographic type information received over Gx, according to `AccessData.subscriber.locationInfo.<tag>` policy tags in Table 10.

   For example:

   - For 2G/3G access, and geographic type CGI, the combination of location area code plus cell identity can be used.
   - For LTE access, E-UTRAN cell identifier for geographic type ECGI can be used.
   - For 3GPP2 access, the cell identifier can be used.

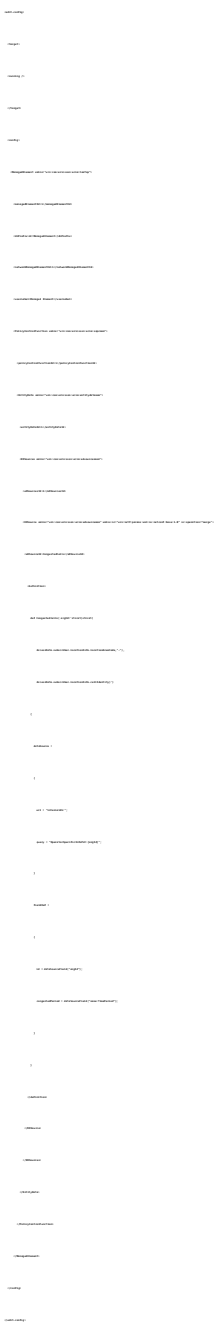
   It is also possible to include periods of time for which the cells are congested, according to the syntax defined in `inPeriod` function, refer to Configuration Guide for Subscription and Policies.

3. Provision a Bearer QoS Control policy containing as `condition` the congested cells information (using Entity Data Source syntax).

   For details about configuration of QoS profiles and Bearer QoS Control, see Configuration Guide for Bearer QoS Control and Bandwidth Management.

Next, the configuration elements examples where some congested cells are defined and used in a policy:

Example 25 Congested Cells as extra data in the SAPC internal database



Example 26 CongestedCells EDSource

The example contains a couple of cells being congested from 08:00 until 18:00 and another one congested from 18:00 until 20:00. The cells are located using the subscriber location information received through Gx. The cell identifiers are composed of Location Area Code and Cell Identity for a 2G/3G 3GPP access.

Example 27 presents that the congested cells (and period of congestion) are considered to assign a lower Bearer QoS Profile. In this, the condition evaluates current time against the congested period of the cell where the subscriber is located. The subscriber location (concatenation of area code and cell identity) is passed to the CellCongestion Entity Data Source as default input argument.

Example 27 Bearer QoS Policy for Congested Cells

14.3 PDN Type and UE IP Address Conditions

The SAPC supports the following IP-CAN session connection types, according to 3GPP Evolved Packet Core (EPC) architecture:

— IP-CAN session Type IPv4, where the UE is allocated an IPv4 address.

— IP-CAN session Type IPv6, where the UE is allocated an IPv6 prefix.

— IP-CAN session Type IPv4v6, where the UE is simultaneously allocated an IPv4 address and IPv6 prefix. This is called dual-stack connectivity.

The preceding information, together with the UE IPv4 address or IPv6 prefix can be used to make policy decisions. Hence, the SAPC provides some policy tags that can be used and configured in the condition of the `rule` URI in the

provisioning REST API: `AccessData.subscriber.ueIpAddress`, `ueIpv6Prefix`, and `ueIpAddressType`.

For example, if the operator wants to evaluate when a subscriber is allocated a particular IPv4 address, use the following expression:

```
(AccessData.subscriber.ueIpAddressType == 0) &&
(AccessData.subscriber.ueIpAddress == "172.40.30.20")
```

To apply a different policy when a subscriber is allocated an IPv6 prefix within a given range, use the following condition expression:

```
(AccessData.subscriber.ueIpAddressType == 1) &&
inRange(AccessData.subscriber.ueIpv6Prefix,
"2001:0DB8:0000:0000:0000:0000:1428:57AB-2001:0DB8::FFFF:FFFF")
```

To identify a dual-stack IP-CAN session connection, use the following expression:

```
(AccessData.subscriber.ueIpAddressType == 2) &&
(AccessData.subscriber.ueIpAddress == "172.40.30.20") &&
(AccessData.subscriber.ueIpv6Prefix == "2001:0DB8:AE56:0034")
```

14.4 Presence Area Status Conditions

14.4.1 Use Case 1: Campus Zone Mobile Broadband

This use case describes a user is assigned to mobile broadband access with high bandwidth when the user enters in his or her campus zone.

The dataplan `Campus_MIT_Group` defines the presence reporting area corresponding to the campus geographical area. When a subscriber enters in the campus zone, it activates `HighBearerQos`, which has a high QoS Profile. When this subscriber leaves the campus zone area, it activates `Qos_default` with a default QoS profile.

```
PUT /subscribers/34600000001

{
        "subscriberId" : "34600000001",
        "eventTriggers": [48],
        "dataplans" :
        [
                {
                        "dataplanName" : "Campus_MIT_Group"
                }
        ]
}

PUT /dataplans/Campus_MIT_Group

{
        "dataplanName" : "Campus_MIT_Group",
        "staticQualification" :
        {
                "presenceReportingAreaNames": ["Campus_MIT"]
        }
}
```

```
PUT /profiles/ip-can-session-qos/Qos_default

{
        "mbrDownlink" : 64,
        "mbrUplink" : 32,
        "profileId" : "Qos_default",
        "qci" : 4
}

PUT /profiles/ip-can-session-qos/HighBearerQos

{
        "mbrDownlink" : 128,
        "mbrUplink" : 64,
        "profileId" : "HighBearerQos",
        "qci" : 5
}

PUT /profiles/presence-reporting-area/Campus_MIT

{
        "name" : "Campus_MIT",
        "praId" : 8388608
}


PUT /rules/PRAQosStatusInCampus_MIT

{
        "condition" : "(AccessData.subscriber.locationInfo.presenceReportingArea[\"Campus_MIT\"].isInArea)",
        "outputAttributes" :
        [

                {
                        "attrName" : "max-qos",
                        "attrValue" : "BearerQosProfile[\"HighBearerQos\"]",
                        "result" : "permit"
                }
        ],
        "ruleName" : "PRAQosStatusInCampus_MIT"
}

PUT /rules/PRAQosStatusOutCampus_MIT

{
        "condition" : "!(AccessData.subscriber.locationInfo.presenceReportingArea[\"Campus_MIT\"].isInArea)",
        "outputAttributes" :
        [

                {
                        "attrName" : "max-qos",
                        "attrValue" : "BearerQosProfile[\"Qos_default\"]",
                        "result" : "permit"
                }
        ],
        "ruleName" : "PRAQosStatusOutCampus_MIT"
}

PUT /policies/PRAQosStatusInPolicy

{
        "policyName" : "PRAQosStatusInPolicy",
        "ruleCombiningAlgorithm" : "permit-overrides",
        "rules" : [ "PRAQosStatusInCampus_MIT", "PRAQosStatusOutCampus_MIT"]
}

PUT /dataplans/Campus_MIT_Group/locators/resources/ip-can-session/contexts/qos

{
        "policies" : [ "PRAQosStatusInPolicy" ]
}
```

Example 28 Configuration of PRA in University Campus

14.4.2 Use Case 2: Home Zone Mobile Broadband

This use case describes a user is assigned to mobile broadband access with high bandwidth when the user enters his or her home zone such as residential area.

`HomeZoneGroup` group is defined as the presence reporting area corresponding to home zone geographical area. When a subscriber enters the home zone area, it activates `HighBearerQos` group, which has a high QoS Profile. When this subscriber leaves the home zone area, it activates `Qos_default`group with a default QoS profile.

```
PUT /subscribers/34600000002
{
  "subscriberId" : "34600000002",
  "eventTriggers": [48],
  "dataplans" :
  [
    {
      "dataplanName" : "HomeZoneGroup"
    }
  ],
  "staticQualification" :
  {
    "presenceReportingAreaNames": ["HomeZone"]
  }
}

PUT /dataplans/HomeZoneGroup
{
  "dataplanName" : "HomeZoneGroup"
}

PUT /profiles/ip-can-session-qos/Qos_default
{
  "mbrDownlink" : 64,
  "mbrUplink" : 32,
  "profileId" : "Qos_default",
  "qci" : 4
}

PUT /profiles/ip-can-session-qos/HighBearerQos
{
  "mbrDownlink" : 128,
  "mbrUplink" : 64,
  "profileId" : "HighBearerQos",
  "qci" : 5
}

PUT /profiles/presence-reporting-area/HomeZone
{
  "name" : "HomeZone",
  "praId" : 1388609,
 "elementsList":
 {
  "tais" : ["012.45.6789-6791"],
  "macroEnbs" : ["123.456.78901"],
  "homeEnbs" : ["234.567.8901234-8901235"],
  "ecgis" : ["345.678.9012345"],
  "rais" : ["456.789.123.45-46"],
  "sais" : ["567.890.1234.5678"],
  "cgis" : ["678.901.2345.6789-6790"]
 }
}

PUT /rules/PRAQosStatusInHomeZone
{
  "condition" : "(AccessData.subscriber.locationInfo.presenceReportingArea[Subscriber.presenceReportingAreaNames].isI
  "outputAttributes" :
  [
    {
      "attrName" : "max-qos",
      "attrValue" : "BearerQosProfile[\"HighBearerQos\"]",
```

```
      "result" : "permit"
    }
  ],
  "ruleName" : "PRAQosStatusInHomeZone"
}

PUT /rules/PRAQosStatusOutHomeZone
{
  "condition" : "!(AccessData.subscriber.locationInfo.presenceReportingArea[Subscriber.presenceReportingAreaNames]
  "outputAttributes" :
  [
    {
      "attrName" : "max-qos",
      "attrValue" : "BearerQosProfile[\"Qos_default\"]",
      "result" : "permit"
    }
  ],
  "ruleName" : "PRAQosStatusOutHomeZone"
}

PUT /policies/PRAQosStatusInPolicy
{
  "policyName" : "PRAQosStatusInPolicy",
  "ruleCombiningAlgorithm" : "permit-overrides",
  "rules" : [ "PRAQosStatusInHomeZone", "PRAQosStatusOutHomeZone"]
}

PUT /dataplans/HomeZoneGroup/locators/resources/ip-can-session/contexts/qos
{
  "policies" : [ "PRAQosStatusInPolicy" ]
}
```

Example 29 Configuration of PRA Home Zone

15 Appendix A. Access and Charging Policy Types

Next figures show the different policy types applicable to access and charging, which can be used in the SAPC.

Access related Policies

Policy Type	Policy Locator			Output Attributes	Comments
	Context	Resource	Subject		
Access Control (Service Authorization) Access	access	<contentId >	<subscriberId> <dataplanId>		Type I = Only policies, no qualification Gx Conditions: Subscriber Data Access Data ToD
Access Control (Static service qualification) Static Access	static-access	<contentId >	<subscriberId> <dataplanId>	permit **pcc-rule-id** "<pccRuleName>"	Type I = Only policies, no qualification Gx Conditions: Subscriber Data Access Data ToD
Rule Space selection Service Domain	access	service-domain	<subscriberId> <dataplanId>	permit **rule-space** "<ruleSpaceName>"	Ericsson Gx+
IP-CAN Sesion Control Access	access	ip-can-session	<subscriberId> <dataplanId>	-	Type I = Only policies, no qualification Gx Conditions: Subscriber Data Access Data ToD

Figure 3 Policy Types (I)

Charging and Content Filtering Policies

Policy Type	Policy Locator			Output Attributes	Comments
	Context	Resource	Subject		
Service Charging	charging	<contentId>	<subscriberId> <dataplanId>	permit **charging** ServiceChargingProfile ["<chargingProfileName>"]	Type II = Mixing policies and qualification Gx Conditions: Access Data Subscriber ToD
Subscriber Charging	charging	any	<subscriber-id> <dataplan-id>	permit **subs-charging** SubsChargingProfile ["<chargingProfileName>"]	Type II = Mixing policies and qualification Gx Conditions: Access Data Subscriber Time conditions (but no ToD reauthorization)
Content Filtering	content-filtering	service-domain	<subscriberId> <dataplanId>	permit **content-filtering-id** "<contentFilteringValue>"	Type II = Mixing policies and qualification Used to return Content-Filtering in Ericsson Gx+

Figure 4 Policy Types (II)

Presence Reporting Area Policy

Policy Type	Policy Locator			Output Attributes	Comments
	Context	Resource	Subject		
Presence Reporting Area Selection	location	any	<subscriberId> <dataplanId> 	permit **presence-area** PraProfile ["<presenceAreaName>"]	Type II = Mixing policies and qualification **Gx** Conditions: Access Data Subscriber Time conditions (but no ToD reauthorization)

Figure 5 Policy Types (III)

Event Triggers Selection Policy

Policy Type	Policy Locator			Output Attributes	Comments
	Context	Resource	Subject		
Event Triggers Selection	event-triggers	any	<subscriberId> <dataplanId> 	permit **event-triggers** "<list of event trigger values>"	Type IV = Mixing AllPermit policies and qualification **Gx** Conditions: Access Data Subscriber Media component (AfData) ToD Algorithms:**all permit** List of event triggers in CSV format

Figure 6 Policy Types (IV)

16 Appendix B. Policy Tags

The following tags related to dynamic information about access and charging data can be used in the `condition` attribute of rules.

Note: There are also some other policy tags applicable to access and charging, which can be found in separate SAPC Configuration Guide documents.

16.1 Time and Date Tags

Time of day conditions can be used in policies. Refer to Configuration Guide for Subscription and Policies for more information.

16.2 Tags Related to Access and Charging

The following tags related to information about IP-CAN session can be used in the policy condition.

For the policy tags obtained from AVPs received in CCR messages (see Comments column), their values are kept during the session lifetime, unless new values of the AVPs are received in subsequent CCR-U/CCR-T messages.

Table 8 Incoming Message Tags

Tag	Return Type	Possible Values	Comments
`AccessData.bearer.accessPoint`	String	any	The Called Station ID. Address where the user is connected to. Network ID + Operator ID

Table 8 Incoming Message Tags

Tag	Return Type	Possible Values	Comments
`AccessData.bearer.accessType`	Integer		Radio Access Technology used: • 0: WLAN • 1000: UTRAN • 1001: GERAN • 1002: GAN • 1003: HSPA_EVOLUTION • 1004: E-UTRAN • 1005: E-UTRAN-NB-IoT • 2000: CDMA2000_1X • 2001: HRPD • 2002: UMB • 2003: EHRPD
`AccessData.bearer.eventTriggers`	Multivalued Integer	any	Received EventTriggers that causes the CCR update. Use this tag together with contains function: `contains(AccessData.bearer.eventTriggers, "<value>")`
`AccessData.bearer.ipCanType`	Integer	0-7	Connectivity access type technology used: • 0: 3GPP-GPRS • 1: DOCSIS • 2: xDSL • 3: WiMAX • 4: 3GPP2 • 5: 3GPP-EPS • 6: Non 3GPP-EPS • 7: FBA
`AccessData.bearer.isAnTrusted`	Boolean	true false	For non-3GPP access networks, indicates if the access is handled as trusted (true) or untrusted (false).

Table 8 Incoming Message Tags

Tag	Return Type	Possible Values	Comments
AccessData. bearer. controlMode	Integer	0-2	Indicates the applied bearer control mode: • 0: UE_ONLY • 2: UE_NW
AccessData. subscriber. chargingChars	Integer	any	Charging Characteristics received from the gateway.(1)
AccessData. subscriber. id	String	any	Subscriber identifier: • Content of the first Subscription-Id AVP received when subsIdType is not configured • AccessData.subscriber.imsi if subsIdType is set to IMSI, or • AccessData.subscriber.msisdn if subsIdType is set to MSISDN.
AccessData. subscriber. imsi	String	any	Subscriber identifier in international IMSI format.
AccessData. subscriber. msisdn	String	any	Subscriber identifier in international E.164 format (MSISDN).
AccessData. subscriber. ueIpAddress	String	any	Subscriber IPv4 address in dot notation format.
AccessData. subscriber. ueIpv6Prefix	String	any	Subscriber IPv6 Prefix, in colon notation, preferred form, without the length part.
AccessData. subscriber. ueIpAddressType	Integer	0-2	Type of UE allocated address: • 0: IPv4 • 1: IPv6 • 2: Dual (IPv4 and IPv6)
AccessData. subscriber. locationInfo. sgsnAddress	IP Address	any	SGSN IP Address

Table 8 Incoming Message Tags

Tag	Return Type	Possible Values	Comments
AccessData. subscriber. locationInfo. anGwIpAddress.v4	IP Address	any	SGW/AGW IPv4 address.
AccessData. subscriber. locationInfo. anGwIpAddress.v6	IP Address	any	SGW/AGW IPv6 address.
AccessData. userEquipmentInfo. model	Integer	any	IMEI-SV Type Allocation Code
AccessData. userEquipmentInfo. serialNr	Integer	any	IMEI-SV Serial Number
AccessData. userEquipmentInfo. version	Integer	any	IMEI-SV Software Version Number

(1) Ericsson recommends not using this value if charging characteristics for the subscriber has been provisioned.

Table 9 Access Policy Tags (II)

Tag	Return Type	Possible Values	Comments
AccessData. bearer. requestType	Integer	1–3	Indicates the request type of the bearer. 1: INITIAL_REQUEST: This value applies for CCR Initial (CC-Request-Type AVP = 1). 2: UPDATE_REQUEST: This value applies for CCR Update (CC-Request-Type AVP = 2). 3: TERMINATION_REQUEST: This value applies for CCR Terminate (CC-Request-Type AVP = 3).
AccessData. host. isPraSupported	Boolean	true false	Indicates if the PCEF supports Presence Reporting Area.
AccessData. host. name	String	any	Origin-Host of the Diameter peer (for example, the PCEF) that sends the message.

Table 10 Subscriber Location Policy Tags

Tag	Return Type	Possible Values	Comments
AccessData. subscriber. locationInfo. cellIdentity	Integer	0-65535 for GPRS, 0-268435455 for EPS	Cell identity where the user currently is registered. For 3GPP-GPRS and 3GPP-EPS access types, the cell identity is obtained from the 3GPP-User-Location-Info AVP. For non-LTE, the cell identity is obtained when geographic location type is Cell Global Identification (CGI). For LTE scenarios, E-UTRAN Cell Identifier (ECI) is obtained when geographic location type is ECGI.
AccessData. subscriber. locationInfo. countryCode	Integer	any	Mobile Country Code (MCC) part of the SGSN PLMN Id. It is obtained from 3GPP-SGSN-MCC-MNC AVP.
AccessData. subscriber. locationInfo. locationAreaCode	Integer	0-65535	Location area code where the user currently is registered, within the geographic location. For 3GPP-GPRS and 3GPP-EPS, the location area code is obtained from 3GPP-User-Location-Info AVP, or if this AVP is not available, the location area code is obtained from RAI AVP.
AccessData. subscriber. locationInfo. networkCode	Integer	any	Mobile Network Code part of the SGSN PLMN Id. It is obtained from 3GPP-SGSN-MCC-MNC AVP.
AccessData. subscriber. locationInfo. presenceReportingArea [“presenceAreaName”]. isInArea	Boolean	true false	PRA status of the UE received from the access network: • true: INSIDE the Area • false: OUTSIDE of the Area It is obtained from the Presence-Reporting-Area-Status AVP.

Table 10 Subscriber Location Policy Tags

Tag	Return Type	Possible Values	Comments
AccessData. subscriber. locationInfo. routingAreaCode	Integer	0-65535	For non-LTE scenarios, the routing area code is the code of routing area where the user currently is registered, within the Routing Area Identification (RAI) geographical location type. The routing area code is obtained from 3GPP-User-Location-Info AVP, or if this AVP is not available, obtained from RAI AVP. For LTE scenarios, the Tracking Area Code (TAC) obtained is from 3GPP-User-Location-Info AVP, when geographic location type is TAI.
AccessData. subscriber. locationInfo. routingAreaIdentity	String	any	RAI of the SGSN where the UE is registered. The RAI is obtained from RAI AVP. The value is encoded as a UTF-8 string on either 11 (if the MNC contains two digits) or 12 (if the MNC contains three digits) octets
AccessData. subscriber. locationInfo. serviceAreaCode	Integer	0-65535	Service area code where the user is registered, within the Service Area Identification (SAI) geographical location type. For 3GPP-GPRS and 3GPP-EPS, it is obtained from 3GPP-User-Location-Info AVP.
AccessData. subscriber. locationInfo. timezone	Integer	Steps of 15 minutes [-48, +56]	Offset between universal time and local time in steps of 15 minutes (900 seconds) of where the UE currently resides.

Reference List

Ericsson Documents

[1] Configuration Guide for Subscription and Policies

[2] System Administrator Guide

Standards

[3] Mobile Radio Interface Layer 3 Core Network Protocols, 3GPP TS 24.008

[4] Policy and Charging Control over Gx reference point, 3GPP TS 29.212