

Configuration Guide for Dynamic Policy Control (Rx)

Ericsson Service-Aware Policy Controller

USER GUIDE

Copyright

© Ericsson España, S.A. 2016. 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 node for the most typical data applicable to Dynamic Policy Control (Rx).



Contents

| | | |
|----------|-------------------------------------------------------------------------------|-----------|
| 1 | Introduction | 1 |
| 1.1 | Document Purpose and Scope | 1 |
| 1.2 | Revision Information | 2 |
| 1.3 | Typographic Conventions | 2 |
| 1.4 | Other Conventions | 3 |
| 2 | Configuration Prerequisites | 5 |
| 3 | Configuration | 7 |
| 3.1 | Configure Gx PCEF Nodes | 8 |
| 3.2 | Provision Dynamic Services | 10 |
| 3.3 | Configure Classification of Dynamic Services | 11 |
| 3.4 | Configure Dynamic Service Authorization | 17 |
| 3.5 | Configure Dynamic Service Qualification | 19 |
| 3.5.1 | Configure Static Qualification for Dynamic Services | 19 |
| 3.5.2 | Configure Dynamic Qualification for Dynamic Services | 20 |
| 3.6 | Configure Bearer QoS Control for Dynamic Services | 24 |
| 3.7 | Configure Access and Charging Policies Based on Dynamic Service Establishment | 24 |
| 3.8 | Configure Event Triggers | 25 |
| 4 | Configuration Examples for Use Cases | 27 |
| 4.1 | Prioritized Video Delivery | 27 |
| 4.2 | Multimedia Telephony over LTE | 29 |
| 5 | Appendix A. Dynamic Policy Types | 35 |
| 6 | Appendix B. Policy Tags | 37 |
| 6.1 | Dynamic Policy Control Tags | 37 |
| 7 | Appendix C. Tags for Output Attributes Used in Policies | 45 |
| 7.1 | QoS and Charging Selection Tags | 45 |
| | Glossary | 47 |
| | Reference List | 49 |





1 Introduction

1.1 Document Purpose and Scope

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

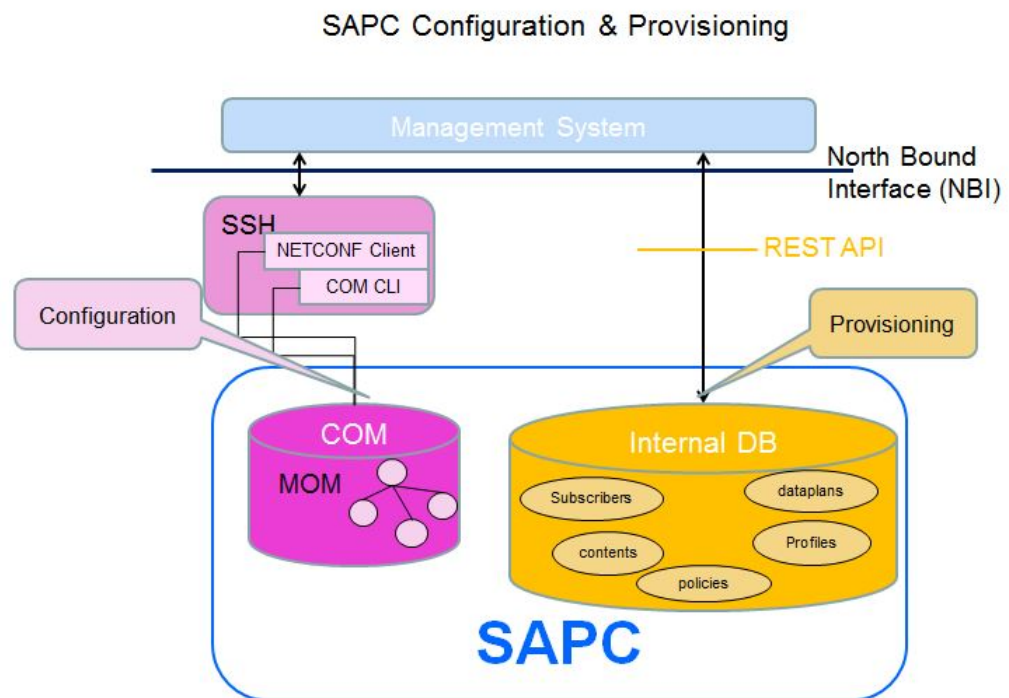


Figure 1 Configuration and Provisioning Overview

The purpose of this document is to provide guidelines and examples to configure Dynamic Policy Control and Rx interface related data in the SAPC node by providing some configuration examples.

This configuration is an extension of the Configuration Guide for Access and Charging Control (Gx).

This document does not intend to be an exhaustive guide for configuring all possibilities related to Dynamic Policy Control in the SAPC.

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.

For general concepts about provisioning of policies, see the Configuration Guide for Subscription and Policies.



This document focuses on the data applicable to the Rx interface and the Dynamic Policy Control function.

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](#).

1.2 Revision Information

Rev. A This is the first release of this document.

Rev. B This document has been revised as follows:
— Added support for IP-Domain-Id.

1.3 Typographic Conventions

This document uses the following typographic conventions:

Table 1 Typographic Conventions

| Convention | Description | Example |
|------------|------------------------|--------------|
| MOC | COM Model Object Class | DiameterNode |



Table 1 Typographic Conventions

| Convention | Description | Example |
|----------------|-----------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NETCONF | SAPC COM configuration | <pre> <edit-config> <target> <running/> </target> <config> <ManagedElement xmlns="urn:com:ericsson:ecim:ComTop"> <managedElementId>1</managedElementId> <PolicyControlFunction xmlns="urn:com:ericsson:ecim:sapc"> <policyControlFunctionId>1</policyControlFunctionId> <Network xmlns="urn:com:ericsson:ecim:networkmom"> <networkId>1</networkId> <DiameterNodes> <diameterNodesId>1</diameterNodesId> <diameterNodeId>ggsnNodeHostname.ggsnNodeHost <controls>IP_CAN_SESSION_ACCESS</control <dynamicServiceSupport>true</dynamicServ </DiameterNode> </DiameterNodes> </Network> </PolicyControlFunction> </ManagedElement> </config> </edit-config> </pre> |
| REST | <p>SAPC provisioning.</p> <p>Exact URI in the Provisioning REST API names, fields, or their corresponding values.</p> | <pre> PUT /subscribers/34620007701 { "subscriberId" : "34620007701" } </pre> |

1.4 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 (dataplan), 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 /dataplan/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 Configuration

To configure the dynamic policy control functionality in the SAPC, perform the following tasks:

- 1 Configure the network protocols: the node data to be able to send and receive messages over the network interfaces such as Gx and Rx.
 - Configure Gx PCEF nodes
- 2 Set provisioning data:
 - Subscribers (refer to [Configuration Guide for Subscription and Policies](#))
 - Subscriber groups (refer to [Configuration Guide for Subscription and Policies](#))
 - Dynamic Services
 - QoS Profiles (refer to [Configuration Guide for Bearer QoS Control and Bandwidth Management](#)) and Charging Profiles (refer to [Configuration Guide for Access and Charging Control \(Gx\)](#))
- 3 Configure the data applicable to dynamic policy control:
 - 1 Configure the rules and policies to identify the services that are dynamically activated through the Rx interface. This procedure is called dynamic service classification.
 - 2 Configure the conditions to authorize or deny subscriber access to the dynamic services. This procedure is called dynamic service authorization.
 - 3 Configure the QoS information and the charging parameters associated with the dynamic services. This procedure is called dynamic service qualification.
 - 4 Configure bearer QoS control for dynamic services (if necessary).
 - 5 Configure Access and Charging Policies based on Dynamic Service Establishment (if necessary).
- 4 In case of integration with an external database, reconfigure the corresponding Entity Data Source, refer to [Database Access](#).

Note: All objects and attributes in this document refer to the default configuration provided at installation time in the SAPC: Entity Data Source pointing to data in the SAPC internal database.



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 PCEF Nodes

The procedure to configure the set of policy controls that the SAPC applies for a PCEF node is detailed in [Configuration Guide for Access and Charging Control \(Gx\)](#). The dynamic policy control function refers to the following controls:

- SERVICE_ACCESS_PCEF_TOD or SERVICE_ACCESS_PCRF_TOD, to authorize dynamic services
- BEARER_QOS, to allocate QoS Information to dynamic services
- SERVICE_CHARGING, to allocate charging information to dynamic services

To enable support for dynamic PCC Rule in the GGSN/PDN-GW, set to true `dynamicServiceSupport` attribute in the corresponding `DiameterNode` MOC.

The following example shows the configuration of a GGSN/PDN-GW node to support dynamic PCC Rules and perform the policy controls IP-CAN session Access Control, Service Access Control, Bearer QoS Control and Service Charging 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">
              <diameterNodeId>ggsnHostname.operator.com</diameterNodeId>
              <controls>IP_CAN_SESSION_ACCESS</controls>
              <controls>SERVICE_ACCESS_PCEF_TOD</controls>
              <controls>BEARER_QOS</controls>
            </DiameterNode>
          </DiameterNodes>
        </Network>
      </PolicyControlFunction>
    </ManagedElement>
  </config>
</edit-config>

```

Example 1 PCEF Configuration

Configure Gx PCEF Nodes using IP-Domain-Id

In scenarios where IP-Domain-Id AVP is received in Rx AAR requests, to configure the mapping between IP-Domain-Id and the corresponding PCEF Origin-Host AVP, do configure the `ipDomainId` attribute of `DiameterNode` object with the IP-Domain-Id AVP value.

Example 2 shows how IP-Domain-Id `ggsn01` is configured for the PCEF with Origin-Host `ggsnNodeHostname.nodeHostRealm.com`.



```

<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">
              <diameterNodeId>ggsnNodeHostname.nodeHostRealm.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>
              <ipDomainId>ggsn01</ipDomainId>
            </DiameterNode>
          </DiameterNodes>
        </Network>
      </PolicyControlFunction>
    </ManagedElement>
  </config>
</edit-config>

```

Example 2 PCEF configuration with ipDomainId.

3.2 Provision Dynamic Services

In addition to the static and preconfigured services handled in the Gx interface, the SAPC supports the following:

- **Dynamic services:** dynamically activated in the SAPC from information coming from the AF (using the Rx interface) and dynamically provisioned towards the GGSN/PDN-GW.

To provision a dynamic service (as for static or preconfigured ones), use the content URI in the Provisioning REST API.

Static or preconfigured services are activated through the Gx interface, while dynamic services are activated by procedures over the Rx reference point. However, static and preconfigured services may be also authorized and installed depending on whether a given dynamic service is running or not. Refer to



Configuration Guide for Access and Charging Control (Gx) provisioning static and preconfigured services.

Next example shows the provisioning of dynamic services:

```
PUT /contents/IMS_IPTV
{
  "contentName" : "IMS_IPTV"
}

PUT /contents/MMTel_audio
{
  "contentName" : "MMTel_audio"
}

PUT /contents/MMTel_video
{
  "contentName" : "MMTel_video"
}

PUT /contents/Video_Conferencing
{
  "contentName" : "Video_Conferencing"
}
```

Example 3 Provisioning of Dynamic Services

The previous example shows the provisioning of the following dynamic services: Video_streaming, MMTel_video, MMTel_audio, IMS_IPTV and Video_Conferencing. The content identifier is used as a reference during service classification and service qualification.

3.3 Configure Classification of Dynamic Services

The SAPC needs to determine a service identifier corresponding to the dynamic service activated by AF events. Mentioned service identifier is relevant to perform afterward Service Authorization (Section 3.4) or Service Qualification (Section 3.5). This section details how to configure the conditions (Dynamic Service Classification policies) to determine such service identifier.

The input information to the classification is the information received from the AF over the Rx interface: the AF application identifier and media pattern (media type, flow direction, and source/destination ports) of the Real Time Protocol (RTP) media components (if present). The output result is the identifier of the service. The association between dynamic services and the information provided by the AF is flexible, and requires a detailed knowledge about the AF-Application-Id or media component data that trigger the activation of dynamic services in the SAPC.

The following video shows how to configure the SAPC for dynamic service classification.



Figure 2

To provision policies for dynamic service classification, use the values summarized in the following figure:

| Policy Type | Policy Locator | | | Output Attributes | Comments |
|--------------------------------|------------------------|-------------|---------|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| | Context | Resource | Subject | | |
| Dynamic Service Classification | service-classification | application | - | service <contentId > | Only policies, no qualification Gx – Rx binding Algorithms: single match, multiple match Conditions: - AfData |

Figure 3 Summary to Configure Classification of Dynamic Services

The result of the service classification is only successful if the SAPC matches all the media components provided in the AA-Request command with the configured rules and policies.

— Use the `/locators/resources/application/contexts/service-classification` URI in the Provisioning REST API containing:

- In the `policies` attribute, put the names of the policies involved in the classification

It is important to assure that the **policies to be evaluated follow the order of the array in the service-classification URI in the Provisioning REST API**, as the first policy that fulfills the conditions is the policy that applies, and no other policy of the array is evaluated. Thus, Ericsson recommends placing the most used policies first.

— For each policy, use the `policies` URI in the Provisioning REST API including:

- Choose one `ruleCombiningAlgorithm` attribute
 - `single-match` means that each rule in the policy can only match one media component in the AF session. Ericsson recommends using it to classify services with known characteristics (number of media components, media type, and so on). Then, do configure one



rule to match each media component and one policy per allowed combination of media components in the AAR command.

- `multiple-match` means that each rule in the policy matches multiple media components in the AF session. Ericsson recommends using it to classify services with variable or unknown number of media components. Then, do configure a single policy with one rule to match all media components that may be received in the AAR command.
- Add in the `rules` attribute the names of the rules for this policy
- For each rule, use the `rules` URI in the Provisioning REST API including:
 - in `condition` attribute the application identifier (and if desired, the media pattern) used to identify the service. The SAPC uses this information to determine whether an evaluated media component matches the rule or not. Use the expression language detailed in [Configuration Guide for Subscription and Policies](#). See appendix B for a complete list of the policy tags that can be used.
 - in `attrValue` attribute inside `outputAttributes`, the service identifier classification result

When all rules in a policy are met, the process returns a list of service identifiers.

Next example shows a global table for dynamic service classification, whose columns contain the input and output information elements mentioned in the video. The rows in the table are evaluated in order, so that the SAPC stops evaluating them when the first one is fulfilled.

Table 2 Dynamic Service Classification

| Application Identifier | Media Pattern | Service Id |
|-----------------------------------------|---------------------------------------------------|----------------------------|
| "urn:urn-7:3gpp-service.ims.icsi.mmtel" | One audio stream with optionally one video stream | MMTel_audio MMTel_video |
| "urn:urn-7:3gpp-service.ims.icsi.iptv" | One media stream on port 554 | IMS_IPTV |
| VisualCon | 1 audio media stream and several video streams | Video_Conferencing |

There are two ways to combine the rules defined in a policy, depending on the value set in the `ruleCombiningAlgorithm` of the policy :

- Single match

For example, the IMS Multimedia Telephony service (MMTel) contains one audio stream with optionally one video stream. Figure 4 shows the required

configuration with two services (MMTel_audio, MMTel_video) and three policies:

- Policy#1: If the AF sends in the AAR-initial message audio and video media components, the SAPC classifies MMTel_audio and MMTel_video services.
- Policy#2: If the AF sends in the AAR-initial message only audio media components, the SAPC classifies MMTel_audio service.
- Policy#3: If the AF sends in the AAR-Update message only video media components, the SAPC classifies MMTel_video service.

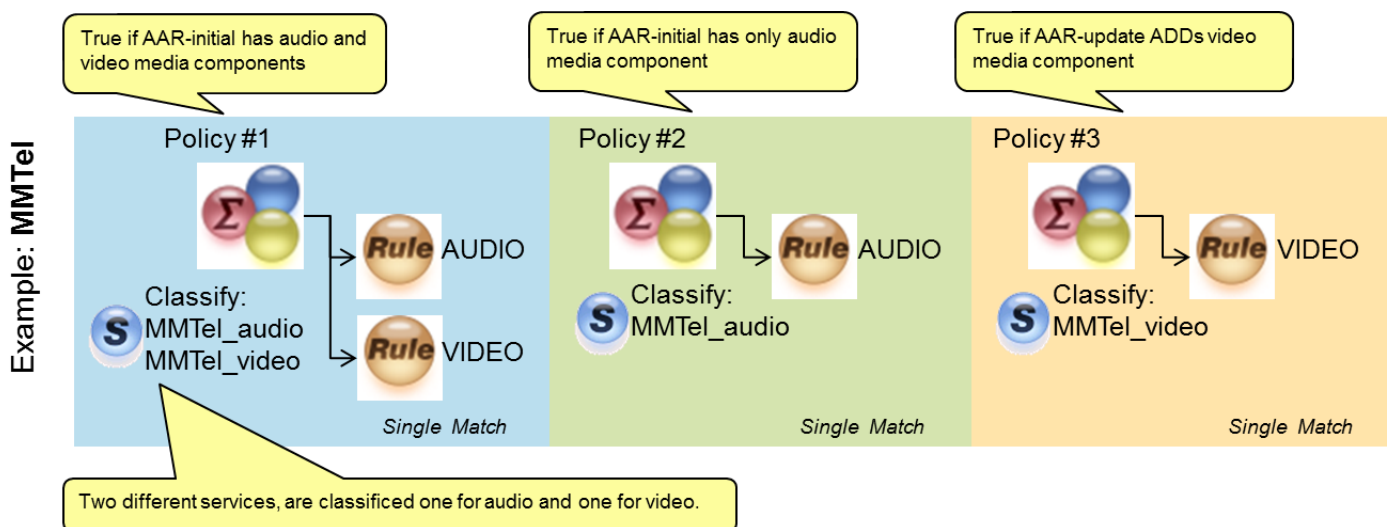


Figure 4 Example configuration to classify the MMTel audio and video service

— Multiple match

For example, a video conference service has several audio and video media streams with different encoding rates. Page 15 shows the required configuration with one service (Video_Conferencing) and one policy:

- Policy#4: If AF sends in AAR command several audio and video media components, the SAPC classifies Video_Conferencing service.

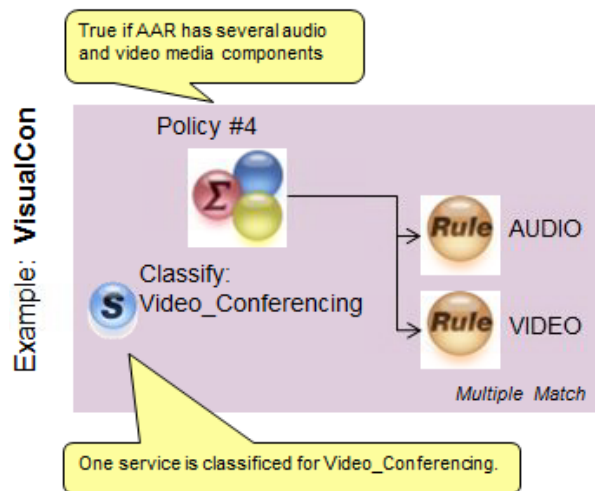


Figure 5 Example configuration to classify the Video_Conferencing

Following example shows the configuration corresponding to the services and conditions described in Table 2:

```
PUT /rules/classifyAudio
{
  "condition" : "(AfData.appId == \"urn:urn-7:3gpp-service.ims.icsi.mmtel\")&
  \"outputAttributes\" :
  [
    {
      \"attrName\" : \"service\",
      \"attrValue\" : \"\\\"MMTel_audio\\\"\",
      \"result\" : \"permit\"
    }
  ],
  \"ruleName\" : \"classifyAudio\"
}

PUT /rules/classifyVideo
{
  \"condition\" : \"(AfData.appId == \"urn:urn-7:3gpp-service.ims.icsi.mmtel\")&
  \"outputAttributes\" :
  [
    {
      \"attrName\" : \"service\",
      \"attrValue\" : \"\\\"MMTel_video\\\"\",
      \"result\" : \"permit\"
    }
  ],
  \"ruleName\" : \"classifyVideo\"
}

PUT /policies/pClassifyMMTel
```



```
{
  "policyName" : "pClassifyMMTel",
  "ruleCombiningAlgorithm" : "single-match",
  "rules" : [ "classifyAudio", "classifyVideo" ]
}

PUT /rules/classifyIPTV
{
  "condition" : "(AfData.appId == \"urn:urn-7:3gpp-service.ims.icsi.iptv\")&&(AfData.appId == \"urn:urn-7:3gpp-service.ims.icsi.iptv\")",
  "outputAttributes" :
  [
    {
      "attrName" : "service",
      "attrValue" : "\"IMS_IPTV\"",
      "result" : "permit"
    }
  ],
  "ruleName" : "classifyIPTV"
}

PUT /policies/pClassifyIPTV
{
  "policyName" : "pClassifyIPTV",
  "ruleCombiningAlgorithm" : "single-match",
  "rules" : [ "classifyIPTV" ]
}

PUT /rules/classifyVideoConferencing
{
  "condition" : "(AfData.appId == \"VisualCon\")",
  "outputAttributes" :
  [
    {
      "attrName" : "service",
      "attrValue" : "\"Video_Conferencing\"",
      "result" : "permit"
    }
  ],
  "ruleName" : "classifyVideoConferencing"
}

PUT /policies/pClassifyVideoConferencing
{
  "policyName" : "pClassifyVideoConferencing",
  "ruleCombiningAlgorithm" : "multiple-match",
  "rules" : [ "classifyVideoConferencing" ]
}

PUT /locators/resources/application/contexts/service-classification
{
  "policies" : [ "pClassifyMMTel", "pClassifyIPTV", "pClassifyVideoConferencing" ]
}
```



```
}
```

Example 4 Configuration of Classification policies for dynamic Services

This configuration example results in the following classification for dynamic Services depending on the data received in the Rx requests:

- MMTEL_video and MMTel_audio: the classification policy uses the combining algorithm `single-match`, meaning that the Rx request contains exactly one media component of type audio and one media component of type video, and all with AF-Application-Id received with the value "urn:urn-7:3gpp-service.ims.icsi.mmtel".
- IMS_IPTV: the classification policy uses the combining algorithm `single-match`, meaning that the Rx request contains exactly one media component of type media and server-side port 554, and all with AF-Application-Id received with the value "urn:urn-7:3gpp-service.ims.icsi.iptv".
- Video_Conferencing: the classification policy uses the combining algorithm `multiple-match`, meaning that the Rx request contains media components (no matters how many of them) with AF-Application-Id received with the value "VisualCon".

Once the dynamic service is classified, a Charging Profile or QoS Profile, or both can be associated by using the dynamic service qualification process.

Quotes included in the Application Identifier

If the AF sends as Application Identifier a string including quotes, the tag `AfData.appId` in the condition should use the expression `substr` (details in [Configuration Guide for Subscription and Policies](#))

If the Application Identifier is this: `+g.3gpp.icsi-ref=\"urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel\"`, the condition to use in the rule should be this:

```
PUT /rules/r_MobileTvAuthorize
{
  "condition" : "(substr(AfData.appId,18,41) == \"urn%3Aurn-7%3A3gpp-
  \"ruleName\" : \"r_MobileTvAuthorize\"
}
```

Example 5 How to use the `AfData.appId` and expression `substr`

3.4 Configure Dynamic Service Authorization

The SAPC offers the possibility to configure whether dynamic services are authorized for a given subscriber or subscriber group, under certain conditions (policies).



Authorization of dynamic services follows the same process as for preconfigured services. For details on how to configure authorization policies, refer to Configuration Guide for Access and Charging Control (Gx)

There are two ways to manage the authorization of dynamic services, by configuring a list of restricted services, or by dynamic policies and conditions.

Dynamic services are by default authorized and do not need to be set within subscribedContents in the group or subscriber profile, to be authorized. Dynamic services can be restricted if set in deniedContents .

Authorization policies for dynamic services can also be used, if restrictions are wanted to be applied (for example not authorizing a particular dynamic service when roaming). This allows the SAPC to use information received from the access network as input for the service authorization decision, such as the Radio Access Type and Subscriber Location Information.

To use policies for dynamic service authorization, create the needed policies using:

— For **global policy locator**:

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

— For **subscriber group locator**:

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

— For **subscriber locator**:

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

Where the <contentName> is the given name of the service to be authorized or not.




| | | | | | |
|--------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|---|--------------------------------------------------------------------------------------------------------|
| Access Control (Dynamic Service Authorization) Access | access  | <contentId >  | <subscriberId> <dataplanId>  | - | Type II = Mixing policies and qualification Conditions: Subscriber Data Access Data ToD |
|--------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|---|--------------------------------------------------------------------------------------------------------|

Figure 6 Summary to Configure Dynamic Service Authorization

In this example, the SAPC authorizes 'VoLTE' dynamic service if the Called Station ID is "ims", IMEI-SV Type Allocation Code is '99000235' and the country code is different from '072' (Botswana)



```

PUT /rules/RUL_TerminalTypeIsValid
{
  "condition" : "(AccessData.userEquipmentInfo.model==99000235) && (AccessDat
  "ruleName" : "RUL_TerminalTypeIsValid"
}

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

PUT /locators/resources/VoLTE/contexts/access
{
  "policies" : [ "POL_TerminalTypeIsValid" ]
}

```

Example 6 Configuration of "VoLTE" Dynamic Service Authorization based on the model and APN given

3.5 Configure Dynamic Service Qualification

Dynamic services can be qualified with QoS or Charging data, or both, either statically or using policy conditions. The SAPC first evaluates the service qualification policies, but if there are not applicable policies, or the policies are not fulfilled, the SAPC obtains the QoS and Charging profile statically assigned to the dynamic service. In both cases, configure the QoS Profile identifier, Charging Profile identifier and related attributes by using the /profiles/content-qos or /profiles/content-charging URI in the Provisioning REST API, or both.

If the QoS profile associated with dynamic services or media components is not complete because some of the attributes in /profiles/content-qos are not present, the SAPC calculates the value of the omitted QoS parameters from the service information received over the Rx interface by using the 3GPP standard procedure defined in TS 29.213, Table 6.3.1. The usual configuration for dynamic services where bandwidth data is received from the AF, is not configuring the bit rate in the QoS Profiles.

3.5.1 Configure Static Qualification for Dynamic Services

The association of a static QoS or charging profile (or both) with a dynamic service follows the same process as for preconfigured services.

- For Charging, refer to Configuration Guide for Access and Charging Control (Gx)



- For QoS, refer to [Configuration Guide for Bearer QoS and Bandwidth Management](#)

The following example shows the allocation of static QoS and charging profiles to a dynamic service:

```
PUT /contents/MMTel_video
{
  "contentName" : "MMTel_video",
  "staticQualification" :
  {
    "contentChargingProfileId" : "Char_MMTel_video",
    "contentQosProfileId" : "QoS_MMTel_video"
  }
}

PUT /profiles/content-qos/QoS_MMTel_video
{
  "arpPriorityLevel" : 7,
  "profileId" : "QoS_MMTel_video",
  "qci" : 2
}

PUT /profiles/content-charging/Char_MMTel_video
{
  "chargingServiceId" : 301,
  "profileId" : "Char_MMTel_video",
  "ratingGroup" : 301,
  "reportingLevel" : 1
}
```

Example 7 Static QoS and Charging assigned to dynamic service

3.5.2 Configure Dynamic Qualification for Dynamic Services

Using policies, it is possible to use dynamic conditions to assign QoS and Charging Profiles to dynamic services.

To use policies for dynamic service qualification, create the needed policies using:

- For **global policy locator**:

```
/locators/resources/<contentName>/contexts/<context type>
```

- For **subscriber group locator**:

```
/dataplan/<dataplanName>/locators/resources/<contentName>/contexts/<context type>
```

- For **subscriber locator**:



/subscribers/<subscriberId>/locators/resources/<contentName>/contexts/<context type>

Where the <contentName> is the given name of the service to be qualified and <context type> is either charging or qos

In addition, to define the conditions that need to be fulfilled to apply a given QoS or Charging Profile, define qualification rules and qualification policies by using the following tables:







| | | | | | |
|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Bearer QoS Control (Dynamic Service Qualification) QoS for Service | qos  | <contentId>  | <subscriberId> <dataPlanId>  | permit qos ServiceQosProfile ["<qosProfileName>"] | Mixing policies and qualification Conditions: media components (AfData) Access Data Subscriber ToD |
| (Dynamic Service Qualification) Service Charging | charging  | <contentId>  | <subscriberId> <dataPlanId>  | permit charging ServiceChargingProfile ["<chargingProfileName>"] | Mixing policies and qualification Conditions: media components (AfData) Access Data Subscriber ToD |

Figure 7 Summary to Configure Dynamic Service Qualification

The next example presents how to assign a QoS Profile depending on policy conditions for a dynamic service “MMTel_audio”:



```
PUT /profiles/content-qos/QosProfile_Default
{
  "arpPci" : false,
  "arpPriorityLevel" : 5,
  "arpPvi" : true,
  "gbrDownlink" : 2000,
  "gbrUplink" : 500,
  "mbrDownlink" : 2500,
  "mbrUplink" : 1000,
  "profileId" : "QosProfile_Default"
}

PUT /rules/qualifyMMTel_audio
{
  "condition" : "(AccessData.bearer.accessPoint == \"internet.network2.operatorX)",
  "outputAttributes" :
  [
    {
      "attrName" : "qos",
      "attrValue" : "ServiceQosProfile[\"QosProfile_Default\"]",
      "result" : "permit"
    }
  ],
  "ruleName" : "qualifyMMTel_audio"
}

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

PUT /locators/resources/MMTel_audio/contexts/qos
{
  "policies" : [ "pQualifyMMTel_audio" ]
}
```

Example 8 Configuration of QoS Profile for dynamic Services

This example configures a QoS Profile named “QosProfile_Default” for the dynamic service “MMTel_audio” when the APN is internet.network2.operatorX.

The next example shows how to assign a Charging data Profile depending on conditions.



```

PUT /profiles/content-charging/ChargingType1
{
  "meteringMethod" : 1,
  "offlineEnabled" : true,
  "onlineEnabled" : false,
  "profileId" : "ChargingType1",
  "ratingGroup" : 4,
  "reportingLevel" : 1
}

PUT /rules/qualifyVoLTE
{
  "condition" : "(AccessData.subscriber.locationInfo.countryCode == \"214\" &
  \"outputAttributes\" :
  [
    {
      \"attrName\" : \"charging\",
      \"attrValue\" : \"ServiceChargingProfile[\"ChargingType1\"]\",
      \"result\" : \"permit\"
    }
  ],
  \"ruleName\" : \"qualifyVoLTE\"
}

PUT /policies/pQualifyVoLTE
{
  \"policyName\" : \"pQualifyVoLTE\",
  \"ruleCombiningAlgorithm\" : \"permit-overrides\",
  \"rules\" : [ \"qualifyVoLTE\" ]
}

PUT /locators/resources/VoLTE/contexts/charging
{
  \"policies\" : [ \"pQualifyVoLTE\" ]
}

```

Example 9 Configuration of Charging Data for dynamic Services

The charging profile “ChargingType1” is configured for the dynamic service “VoLTE” when the user location information indicates MCC=214 and MNC=07.

Note: It is possible to qualify a particular media component (for example to assign a determined charging profile for the video component). This can be done including in the qualification rule condition tags related to the Rx received media components. This is an interesting alternative, in case other dynamic conditions are already used in Dynamic Qualification policies.

An example of rule condition: (expressionX && AfData.media.type == “video”).

3.6 Configure Bearer QoS Control for Dynamic Services

In scenarios where dynamic services do not require a dedicated bearer, but are installed on the default IP-CAN session bearer, it may be required to configure the QoS of the default bearer in relation to the establishment of dynamic services on the IP-CAN session.

Configuration of Bearer QoS Control is described in [Configuration Guide for Bearer QoS and Bandwidth Management](#). In addition, the following specific QoS selection tags are defined in relation to dynamic services:

- `maxDynQosProfile` that returns a QoS profile composed of the highest value for every field in the QoS profile, out of the values obtained for each dynamic PCC Rule running in the IP-CAN session.
- `sumDynQosProfile` that returns a QoS profile composed of the sum of the throughput parameters (GBRs and MBRs) out of the values obtained for each dynamic PCC Rule running in the IP-CAN session, and selecting the highest value in the rest of the QoS parameters.



| Policy Type | Policy Locator | | | Output Attributes | Comments |
|-------------------------------------------------|------------------------------------------------------------------------------------------------|----------------|---------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| | Context | Resource | Subject | | |
| Bearer QoS Control QoS for Bearer | qos  | ip-can-session | <subscriberId> <dataplanId>  | permit max-qos BearerQosProfile ["<qosProfileName>"] or qos_prof_expression permit min-qos BearerQosProfile ["<qosProfileName>"] or qos_prof_expression | Mixing policies and qualification Special functions: - maxQosProfile - maxDynQosProfile - sumQosProfile - sumDynQosProfile |

Figure 8 Summary to Configure QoS for Bearer

3.7 Configure Access and Charging Policies Based on Dynamic Service Establishment

The SAPC can be configured to reevaluate the access and charging policy decisions taken for the IP-CAN session based on the establishment of dynamic services. This is useful when the AF does not provide information about the IP flows required to deliver the service (the media component information is omitted). In this case, for example, a pre-configured PCC Rule can be defined in the SAPC, associated with the activation of a dynamic service, that initiates the establishment of a dedicated bearer.

Configuration of access and charging policy control is described in [Configuration Guide for Access and Charging Control \(Gx\)](#). In addition, the following policy tag is defined in relation to dynamic services:

- `AccessData.subscriber.service["serviceName"].isRunning` that indicates if a dynamic service is running in the IP-CAN session. This allows the SAPC to take policy decision based on whether a given dynamic service is running or not.



3.8 Configure Event Triggers

The following event triggers value can be set in network deployments using Rx interface, if the AF requires to be notified of such events:

- For successful resource allocation, that is, the SAPC requests the PCEF to inform that the resources for a PCC Rule have been successfully allocated: set value `SUCCESSFUL_RESOURCE_ALLOCATION` .
- For access network information report, the SAPC requests the PCEF to report the network location information (NetLoc): set value `ACCESS_NETWORK_INFO_REPORT` .

For details on how to configure event triggers, refer to [Configuration Guide for Access and Charging Control \(Gx\)](#).





4 Configuration Examples for Use Cases

4.1 Prioritized Video Delivery

In this scenario, the operator offers a prioritized video delivery service for a group of premium subscribers. A DPI node (acting as AF) detects the start of a streaming service and reports this event to the SAPC over the Rx interface. Then the SAPC evaluates the applicable policies for the IP-CAN session, and upgrades the QoS of the default bearer.

The following configuration steps are needed:

- Configure a dynamic service classification policy based on the received AF-Application-Id (no media components are received in the Rx Request), giving as output attribute Video_streaming.

```
PUT /rules/ClassifyVideoStreaming
{
  "condition" : "(AfData.appId == \"Video_streaming\")",
  "outputAttributes" :
  [
    {
      "attrName" : "service",
      "attrValue" : "\"Video_streaming\"",
      "result" : "permit"
    }
  ],
  "ruleName" : "ClassifyVideoStreaming"
}

PUT /policies/pClassifyVideoStreaming
{
  "policyName" : "pClassifyVideoStreaming",
  "ruleCombiningAlgorithm" : "single-match",
  "rules" : [ "ClassifyVideoStreaming" ]
}

PUT /locators/resources/application/contexts/service-classification
{
  "policies" : [ "pClassifyVideoStreaming" ]
}
```

Example 10 Define rule and policy for video streaming

- Configure a QoS Profile for the premium subscriber group.



```
PUT /profiles/ip-can-session-qos/QoSPremium
{
  "arpPriorityLevel" : 9,
  "mbrDownlink" : 10000,
  "mbrUplink" : 1000,
  "profileId" : "QoSPremium",
  "qci" : 7
}
```

Example 11 Define Bearer QoS "QoSPremium"

- Configure a QoS Control policy for the premium subscriber group.



```

PUT /rules/rbearerPremium
{
  "condition" : "((AccessData.subscriber.service[\"Video_streaming\"]).isRunni
  "outputAttributes" :
  [
    {
      "attrName" : "max-qos",
      "attrValue" : "BearerQosProfile[\"QoSPremium\"]",
      "result" : "permit"
    },
    {
      "attrName" : "min-qos",
      "attrValue" : "BearerQosProfile[\"QoSPremium\"]",
      "result" : "permit"
    }
  ],
  "ruleName" : "rbearerPremium"
}

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

PUT /dataplan/Premium/locators/resources/ip-can-session/contexts/qos
{
  "policies" : [ "pbearerQoS" ]
}

PUT /dataplan/Premium
{
  "dataplanName" : "Premium"
}

```

Example 12 Define group "Premium", rule and policy for bearer QoS "QoSPremium"

4.2 Multimedia Telephony over LTE

This section shows a configuration example that follows the standard requirements for IMS conversational voice or video, or both services over LTE access. The conversational video service is an extra complement to a conversational voice service in IMS, that can be added or removed by the end user during an ongoing session or can be established together with voice media at initial call establishment. Ericsson recommends to provision two different dynamic

services (VoLTE and ViLTE) that are activated according to the media component information received from the AF.

Next a graphical sketch that explains the needed configuration:

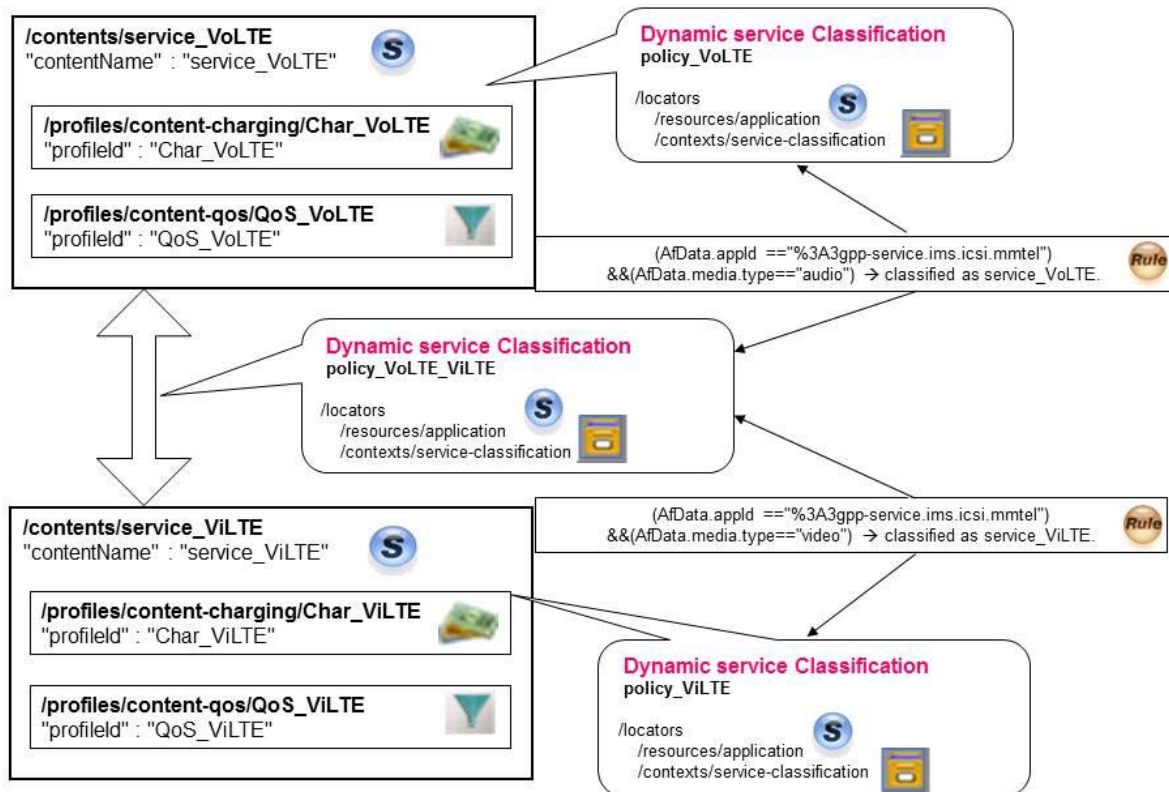


Figure 9 VoLTE/ViLTE scenario

- Define the Charging Profile for the audio and video services, with the appropriate attributes



```
PUT /profiles/content-charging/Char_ViLTE
{
  "chargingServiceId" : 301,
  "profileId" : "Char_ViLTE",
  "ratingGroup" : 301,
  "reportingLevel" : 1
}

PUT /profiles/content-charging/Char_VoLTE
{
  "chargingServiceId" : 302,
  "profileId" : "Char_VoLTE",
  "ratingGroup" : 302,
  "reportingLevel" : 1
}
```

Example 13 Define Charging profile services "Char_VoLTE" and "Char_ViLTE"

- Define the QoS Profile for the audio and video services following the standard recommendations, a dedicated bearer is set up for audio with QCI=1 and another dedicated bearer for video with QCI=2.

```
PUT /profiles/content-qos/QoS_ViLTE
{
  "arpPriorityLevel" : 7,
  "profileId" : "QoS_ViLTE",
  "qci" : 2
}

PUT /profiles/content-qos/QoS_VoLTE
{
  "arpPriorityLevel" : 6,
  "profileId" : "QoS_VoLTE",
  "qci" : 1
}
```

Example 14 Define Qos Profile Services "QoS_VoLTE" and "QoS_ViLTE"

- Define the services and assign statically a different QoS profile and charging profile for each service as it is described in [Configuration Guide for Access and Charging Control \(Gx\)](#)



```

PUT /contents/service_ViLTE
{
  "contentName" : "service_ViLTE",
  "staticQualification" :
  {
    "contentChargingProfileId" : "Char_ViLTE",
    "contentQosProfileId" : "QoS_ViLTE"
  }
}

```

```

PUT /contents/service_VoLTE
{
  "contentName" : "service_VoLTE",
  "staticQualification" :
  {
    "contentChargingProfileId" : "Char_VoLTE",
    "contentQosProfileId" : "QoS_VoLTE"
  }
}

```

Example 15 Define Service "service_VoLTE" and "service_ViLTE"

- Configure policies for dynamic service classification, by making use of the AF-Application-Identifier and Media-Type information received over the Rx interface to identify each service.

```

PUT /rules/rule_ViLTE
{
  "condition" : "((AfData.appId ==\"%3A3gpp-service.ims.icsi.mmtel\") &&(AfData
  "outputAttributes" :
  [
    {
      "attrName" : "service",
      "attrValue" : "\"service_ViLTE\"",
      "result" : "permit"
    }
  ],
  "ruleName" : "rule_ViLTE"
}

```

```

PUT /policies/policy_ViLTE
{
  "policyName" : "policy_ViLTE",
  "ruleCombiningAlgorithm" : "single-match",
  "rules" : [ "rule_ViLTE" ]
}

```

```

PUT /rules/rule_VoLTE
{
  "condition" : "((AfData.appId ==\"%3A3gpp-service.ims.icsi.mmtel\") &&(AfData

```



```

"outputAttributes" :
[
  {
    "attrName" : "service",
    "attrValue" : "\"service_VoLTE\"",
    "result" : "permit"
  }
],
"ruleName" : "rule_VoLTE"
}

PUT /policies/policy_VoLTE
{
  "policyName" : "policy_VoLTE",
  "ruleCombiningAlgorithm" : "single-match",
  "rules" : [ "rule_VoLTE" ]
}

PUT /policies/policy_VoLTE_ViLTE
{
  "policyName" : "policy_VoLTE_ViLTE",
  "ruleCombiningAlgorithm" : "single-match",
  "rules" : [ "rule_VoLTE", "rule_ViLTE" ]
}

PUT /locators/resources/application/contexts/service-classification
{
  "policies" : [ "policy_VoLTE", "policy_ViLTE", "policy_VoLTE_ViLTE" ]
}

```

Example 16 Define rules and policies for "service_VoLTE" and "service_ViLTE"





5 Appendix A. Dynamic Policy Types

Next figures show the different policy types applicable to **dynamic policy control** that can be used.

Dynamic Policy Control (Rx) related Policies












| Policy Type | Policy Locator | | | Output Attributes | Comments |
|---------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| | Context | Resource | Subject | | |
| Dynamic Service Classification | service-classification | application | - | service <contentId > | Only policies, no qualification Gx – Rx binding Algorithms: single match, multiple match Conditions: - AfData |
| Access Control (Dynamic Service Authorization) Access | access  | <contentId >  | <subscriberId> <dataplanId>  | - | Mixing policies and qualification Conditions: Access Data Subscriber ToD |
| Bearer QoS Control (Dynamic Service Qualification) QoS for Service | qos  | <contentId>  | <subscriberId> <dataplanId>  | permit qos ServiceQosProfile ["<qosProfileName>"] | Mixing policies and qualification Conditions: media components (AfData) Access Data Subscriber ToD |
| (Dynamic Service Qualification) Service Charging | charging  | <contentId>  | <subscriberId> <dataplanId>  | permit charging ServiceChargingProfile ["<chargingProfileName>"] | Mixing policies and qualification Conditions: media components (AfData) Access Data Subscriber ToD |
| Bearer QoS Control QoS for Bearer | qos  | ip-can-session | <subscriberId> <dataplanId>  | permit max-qos BearerQosProfile ["<qosProfileName>"] or qos_prof_expression permit min-qos BearerQosProfile ["<qosProfileName>"] or qos_prof_expression | Mixing policies and qualification Conditions: media components (AfData) Access Data Subscriber ToD |

Figure 10 Policy Types for Rx Dynamic Policy Control





6 Appendix B. Policy Tags

6.1 Dynamic Policy Control Tags

The following tags regarding the content of an Rx request, can be used in the classification or qualification of dynamic services, that means when the SAPC receives Rx traffic messages from an AF.

They can be also used in any policy condition evaluated during Gx interactions for dynamic services related policies (that is, policies where the resource is a dynamic service).

Note: The SAPC does not evaluate these policy tags in any other IP-CAN session related policy types (such as IP-CAN Access Control or Subscriber Charging).

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

Table 3 Application (Rx data) Tags

| Tag | Return Type | Possible Values | Comments |
|---------------------------|-------------|-----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AfData. appId | String | any | The application Identifier. Its value can be returned at media component level if present. If not received in any media component, but it is received at command level, the value at command level is returned. If not received neither at media component nor command level, the value returned is ""(empty string). |
| AfData. media. type | String | "audio", "video", "data", "application", "control", "text", "message", "other" | Media component type (1) |



Table 3 Application (Rx data) Tags

| Tag | Return Type | Possible Values | Comments |
|------------------------------------------|-------------|------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AfData. media. typeAsInt | Integer | 0: audio 1: video 2: data 3: application 4: control 5: text 6: message 7: other | Media component type expressed as a number. (1) |
| AfData. media. flowDirection | String | "uplink", "downlink", "bidirectional", "" | The direction of the RTP flow (media subcomponent) of the media component. If no RTP flow is included inside the media component the value equals "". (1) |
| AfData. media.port | Integer | any | The server-side port in the RTP flow from the media component. (1) |
| AfData. media. reservationPriority | Integer | 0-15 | The reservation priority. Its value is returned at media component level if present. If not received in any media component, but it is received at command level, the value at command level is returned. If not received neither at media component nor command level, 0 (lowest priority level) is assumed. (1) |
| AfData. serviceStatus | Integer | 0: final service information 1: preliminary service information | Status of the service information that the AF is providing to the SAPC. If not received, 0 (final service information) is assumed. |

(1) This tag iterates on each media component of the Rx message

The following tags can be used in any policy condition evaluated during Gx interactions according to the characteristics of the dynamic services or media components that are active in the IP-CAN session.

Table 4 Policy Tags Related to Dynamic Services

| Tag | Return Type | Possible Values | Comments |
|--------------------------------------------------------------------|-------------|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AccessData. subscriber. service["serviceName"]. isRunning | Boolean | true false | Indicates if the dynamic service is running on the Gx IP-CAN session. The service name has to correspond to the name used in service classification. |



The following policy tags related to dynamic information about mobile access (IP-CAN session) can also be used in Rx interactions:

Table 5 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 |
| AccessData.bearer.accessType | Integer | | Radio Access Technology used: <ul style="list-style-type: none"> • 0: WLAN • 1000: UTRAN • 1001: GERAN • 1002: GAN • 1003: HSPA_EVOLUTION • 1004: E-UTRAN • 2000: CDMA2000_1X • 2001: HRPD • 2002: UMB • 2003: EHRPD |
| AccessData.bearer.eventTriggers | Multivalued Integer | any | Received <code>EventTriggers</code> that causes the CCR update. Use this tag together with contains function: <code>contains (AccessData.bearer.eventTriggers, "<value>")</code> |
| AccessData.bearer.ipCanType | Integer | 0-7 | Connectivity access type technology used: <ul style="list-style-type: none"> • 0: 3GPP-GPRS • 1: DOCSIS • 2: xDSL • 3: WiMAX • 4: 3GPP2 • 5: 3GPP-EPS • 6: Non 3GPP-EPS • 7: FBA |



Table 5 Incoming Message Tags

| Tag | Return Type | Possible Values | Comments |
|------------------------------------------------|-------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AccessData.bearer.controlMode | Integer | 0-2 | Indicates the applied bearer control mode: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• Content of the first Subscription-Id A VP 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: <ul style="list-style-type: none">• 0: IPv4• 1: IPv6• 2: Dual (IPv4 and IPv6) |
| AccessData.subscriber.locationInfo.sgsnAddress | IP Address | any | SGSN IP Address |



Table 5 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 6 Subscriber Location Policy Tags

| Tag | Return Type | Possible Values | Comments |
|-------------------------------------------------------------|-------------|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AccessData. subscriber. locationInfo. cellIdentity | Integer | 0-65535 for GPRS 0-26843 5455 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. |



Table 6 Subscriber Location Policy Tags

| Tag | Return Type | Possible Values | Comments |
|--------------------------------------------------------------------|-------------|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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. 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 |



Table 6 Subscriber Location Policy Tags

| Tag | Return Type | Possible Values | Comments |
|----------------------------------------------------------------|-------------|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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. |





7 Appendix C. Tags for Output Attributes Used in Policies

7.1 QoS and Charging Selection Tags

The following set of tags may be used in an output attribute element to specify the method to select a QoS profile and Charging profile.

Table 7 QoS and charging Selection Tags

| Tag | Return Type | Format | Comments |
|------------------------|------------------|-------------------------------------------------|------------------------------------------------------------------|
| ServiceChargingProfile | Charging Profile | ServiceChargingProfile ["ChargingProfile Name"] | A Charging profile name previously configured |
| ServiceQosProfile | QoS Profile | ServiceQosProfile ["QosProfile Name"] | A QoS profile name previously configured. |
| maxDynQosProfile | QoS Profile | maxDynQosProfile | Maximum of the QoS Profiles associated to the dynamic PCC rules. |
| sumDynQosProfile | QoS Profile | sumDynQosProfile | Aggregation of QoS profiles of the dynamic PCC rules). |





Glossary

AF

Application Function

EPS

Evolved Packet System

GBR

Guaranteed Bit Rate

GPRS

General Packet Radio Service

IMS

IP Multimedia Subsystem

LTE

Long Term Evolution

MBR

Maximum Bit Rate

MMTEL

Multimedia Telephony

PCC

Policy Charging Control

PCEF

Policy Charging Enforcement Function

PCRF

Policy and Charging Rules Function

QCI

QoS Class Identifier

QoS

Quality of Service

RTP

Real-Time Protocol

RTSP

Real Time Streaming Protocol

SAPC

Ericsson Service-Aware Policy Controller

SGSN

Serving GPRS Support Node

CBA

Component Based Architecture

UE

User Equipment

URN

Uniform Resource Name

VoLTE

Voice Over LTE

ViLTE

Video Over LTE





Reference List

Ericsson Documents

- [1] Configuration Guide for Access and Charging Control (Gx)
- [2] Configuration Guide for Bearer QoS Control and Bandwidth Management
- [3] Configuration Guide for Subscription and Policies