

# Technical Product Description

Ericsson Service-Aware Policy Controller 1

TECHNICAL PRODUCT DESCRIPTION

## 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.

<b>Java</b>	is a registered trademark of Oracle Corporation and/or its affiliates.
<b>VMware</b>	is a registered trademark of VMware Inc.
<b>OpenStack</b>	is a registered trademark of OpenStack Foundation
<b>OpenDaylight</b>	is a registered trademark of The OpenDaylight Project, Inc.

## Abstract

The Technical Product Description describes the architecture, functions, configurations, interfaces, operation, and maintenance of the Ericsson Service-Aware Policy Controller (SAPC) 1.

The SAPC helps fully leverage the Mobile, Fixed and Convergent Broadband solutions by providing the possibility to bring the subscriber dimension into policy decisions that impact traffic. The SAPC is an already proven component in Ericsson Packet Core solutions.



# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Document Purpose and Scope	1
1.2	Disclaimer Note	1
1.3	Revision Information	1
<b>2</b>	<b>Overview</b>	<b>3</b>
<b>3</b>	<b>Reference Architectures</b>	<b>5</b>
3.1	3GPP Policy and Charging Control (PCC) Architecture	5
3.2	Broadband Forum (BBF) Broadband Policy Control Framework Architecture	6
3.3	3GPP and BBF Policy Convergence for Fixed Broadband and Mobile Broadband	7
3.4	ETSI Network Functions Virtualization (NFV) Framework	8
3.5	Naming Conventions	8
<b>4</b>	<b>Solutions</b>	<b>9</b>
4.1	SAPC in Ericsson Virtual Evolved Packet Core (Virtual EPC)	9
4.2	SAPC in Ericsson IMS	9
4.3	SAPC in Ericsson Wi-Fi Calling	9
4.4	SAPC in Ericsson Integrated Policy and Charging	10
4.5	SAPC in Ericsson SDN	10
<b>5</b>	<b>Functions</b>	<b>13</b>
5.1	Policy Management for Mobile, Fix, and Convergent Networks (Gx-based)	13
5.2	Policy Management for Wi-Fi Access	17
5.3	Subscription Management	18
5.4	Dynamic Policy Control	19
5.5	Integrated Policy and Charging - Policy Control Based on Spending Limits	23
5.6	Mobility Based Policy	23
5.7	External SPR Support	24
5.8	Time-Based Authorizations	25
5.9	Notifications to End-Subscribers or to External Systems	25
5.10	Reauthorization Upon Subscription Change	26



5.11	1+1 Geographical Redundancy	26
5.12	Flexible Output Protocol	27
5.13	UE Trace	28
5.14	Policy Studio	28
5.15	Fair Usage Policies	29
5.16	Other Supported Functions	32
<b>6</b>	<b>Interfaces</b>	<b>33</b>
6.1	Reference Model	33
6.2	Statement of Compliance	34
<b>7</b>	<b>SW Architecture</b>	<b>37</b>
<b>8</b>	<b>Operation and Maintenance</b>	<b>39</b>
8.1	Middleware	39
8.2	Provisioning	39
8.3	Node Configuration	39
8.4	Fault Management	39
8.5	Performance Management	39
8.6	Logging	40
8.7	Backup and Restore	40
8.8	Troubleshooting	40
8.9	License Management	40
<b>9</b>	<b>Installation and Deployment</b>	<b>41</b>
9.1	PNF Deployment	41
9.2	VNF Deployment	41
	<b>Glossary</b>	<b>43</b>
	<b>Reference List</b>	<b>47</b>



# 1 Introduction

## 1.1 Document Purpose and Scope

The Technical Product Description document aims to provide a technical and functional description of the Ericsson Service-Aware Policy Controller (SAPC) 1.

The document describes the SAPC 1 role as the Ericsson product providing the policy control element for Mobile, Fixed, and Convergent Broadband networks.

Aspects related to operation and maintenance, internal architecture and deployment are briefly introduced as well.

## 1.2 Disclaimer Note

This document applies to the SAPC 1 main release and all its consecutive SW drops. The delivery dates of the specific functions may diverge. For specific details on General Availability Dates, please check the SAPC Roadmap.

## 1.3 Revision Information

A	This is the first release of this document.
B	Updates on section 9.1.
C	The document is updated with the content included in SAPC 1 Q4 2017.
D	PNF support in section 9 is clarified.





## 2 Overview

The SAPC is the Ericsson Multi-Access Policy Management Framework. It provides policy management for Mobile Broadband Networks, Fixed Broadband Networks, and Fixed-Mobile Convergence (FMC) Broadband Networks. The SAPC enables then the applicability of policy control capabilities based on subscriber and service information. The main enabled policy types are related to service access control, Quality of Service (QoS) control and charging control.

The SAPC is positioned as the advanced solution for the following business drivers:

- **Multiaccess.** The SAPC 1 release provides policy control for both Fixed accesses (like PPP or IPoE) and Mobile accesses (like GSM, UTRAN and E-UTRAN).
- **Convergence.** Users may enter into the Service Network through different type of accesses, and policy control can manage consistently such users across such accesses. With such target, the SAPC 1 provides an FMC policy control solution.
- **Value Added Offerings.** Operators are willing to monetize premium services and obtain more revenues segmenting the subscriber base. The SAPC allows the Operator to define complex offerings and, simultaneously, control the service delivery based on subscriber category, accumulated use, service type, and access conditions.
- **Network Optimization.** Multimedia services are consuming an ever increasing amount of network resources, and subscribers are increasing their use of these services. Operators must manage these services while providing them in a cost effective and reliable way. QoS control ensures that services do not over run the limited network resources and not degrade existing services, Service Level Agreements, and premium subscribers. There is a need to maximize the efficiency of the network from the terminal to the network edge, and the SAPC can control the corresponding parameters setting the right priorities and QoS to the different streams that traverse the transport plane. The output is an optimized network that gives the needed resources based on per subscriber and service policies. And that enables the implementation of voice optimization services, like Voice over Long Term Evolution (VoLTE) or Wi-Fi calling.
- **Smart Traffic Management.** Network architecture is evolving towards Software Defined Network (SDN). Ericsson Service Chaining solution enables operators to manage traffic in a smart way while keeping the focus on cost-driven network optimization. For such purpose, the SAPC provides real-time dynamic policy decisions based on network and subscriber information the SDN-Controller.

The SAPC responds to these challenges by providing an advanced technical solution characterized by:



- **Technology Leaders.** First to market, the SAPC uses state-of-the-art platform technologies, focused in providing excellent characteristics measurements.
- **Easy Integration.** The SAPC can be easily integrated with any gateway supporting the standard 3GPP Gx reference point. The SAPC is deployed in verified in Ericsson end-to-end solutions that requires policy control, interworking then with the Ericsson Evolved Packet Gateway (EPG). In addition, the SAPC can be north-bound integrated with Operation and Maintenance systems through standard interfaces like Simple Network Management Protocol (SNMP), Network Configuration Protocol (NETCONF), or Simple Object Access Protocol (SOAP).
- **High Availability.** The SAPC provides a fully redundant node architecture reaching 5x9's availability, based on a 1+1 Geographical Redundancy solution. Both active-standby and active-active deployment modes are supported.



## 3 Reference Architectures

### 3.1 3GPP Policy and Charging Control (PCC) Architecture

The PCC Architecture is defined in 3GPP TS 23.203 (Reference [5]). It provides the functions for policy, access, and charging control, as well as event reporting for Service Data Flows (SDF).

Figure 1 describes the 3GPP PCC Architecture for the non-roaming case.

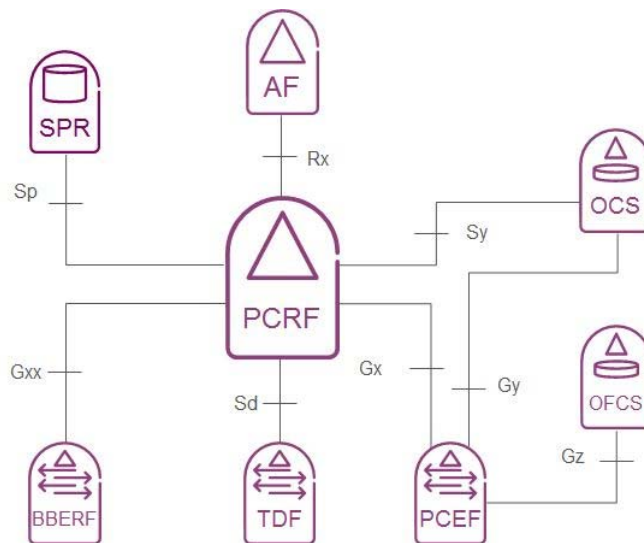


Figure 1 3GPP PCC Architecture

The SAPC, as Policy Server for Mobile Broadband Networks, provides a 3GPP Policy and Charging Rules Function (PCRF) compliant implementation. The 3GPP PCRF is the function responsible for the policy control decision, giving network control regarding the SDF detection, gating, QoS, and flow based charging (except credit management) towards the Policy and Charging Enforcement Function (PCEF) and/or Traffic Detection Function (TDF). Such policy control decision can be based on dynamic service input provided by the Application Function (AF), subscriber profile data managed by the Subscription Profile Repository (SPR), IP-CAN Session data reported by the PCEF, subscriber spending limits reported by the Online Charging System (OCS), or internal PCRF events (for example, timers).

The SAPC 1 provides:

- Gx implementation towards the PCEF. Examples of PCEFs can be a 3GPP Packet Data Networks Gateway (PDN-GW) or a Gi-Box like a Deep Packet Inspection (DPI).
- Rx implementation towards AFs. Examples of AFs can be an IP Multimedia Subsystem (IMS) Proxy Call Session Control Function (P-CSCF) or a Streaming Server.

— Sy implementation towards OCS.

**Note:** The support of the rest of PCRF reference points (Sd and Gxx) is a candidate requirement for future SAPC releases.

## 3.2 Broadband Forum (BBF) Broadband Policy Control Framework Architecture

The BBF TR-134 (Reference [13]) describes an architectural framework to give policy control for Fixed Broadband Multi- Service Networks. The document includes requirements for providing session-based policies, application admission control, bandwidth management, QoS management, security, multicast, routing policies, accounting and charging control, plus use cases related with policy control in Fixed Broadband Networks.

The BBF TR-134 architectural framework is shown in Figure 2.

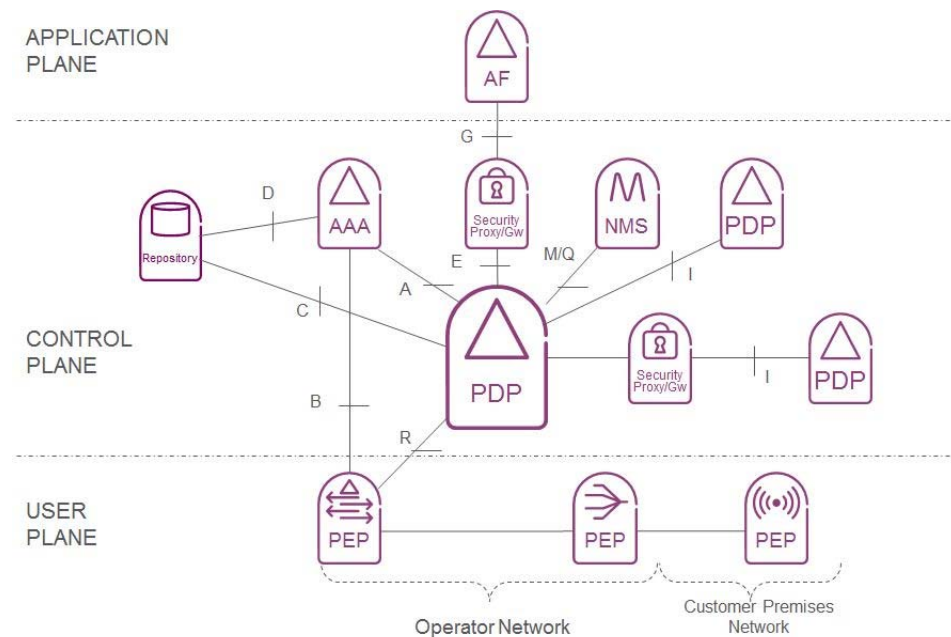


Figure 2 BBF TR-134 Policy Architectural Framework

As Figure 2 depicts, the BBF policy architectural framework contains a Policy Decision Point (PDP) responsible of making policy decisions for different Policy Enforcement Points (PEP) distributed along the User Plane. Such policy decision can be deployed by static activation, or can be dynamically made based on information provided by:

- AFs.
- Control Plane Network Elements, including Authentication, Authorization and Accounting (AAA) Server, a Network Management System (NMS), a data Repository, and even a PDP in the 3GPP domain - that is, a PCRF.



The PDP in Figure 2 is a logical function that can be deployed in four different network elements. None of them is recommended, being then an Operator choice. Such PDP deployment alternatives are listed below:

- Embedded in the Multi Service-Broadband Network Gateway (MS-BNG) or Broadband Remote Access Server (BRAS).
- As part of an NMS.
- As part of the AAA infrastructure.
- As a standalone Policy Server.

The SAPC, as Policy Server for Fixed Broadband Networks, provides a PDP compliant with BBF TR-134 standalone Policy Server deployment.

### 3.3 3GPP and BBF Policy Convergence for Fixed Broadband and Mobile Broadband

The Policy Convergence Architecture, which has been defined as a joint activity between 3GPP and BBF, is an extension of the PCC Architecture commented in Section 3.1 on page 5. It is detailed in 3GPP TS 23.203 Annex S (Reference [5]) and BBF TR-300 (Reference [14]).

Figure 3 displays the Policy Convergence Architecture.

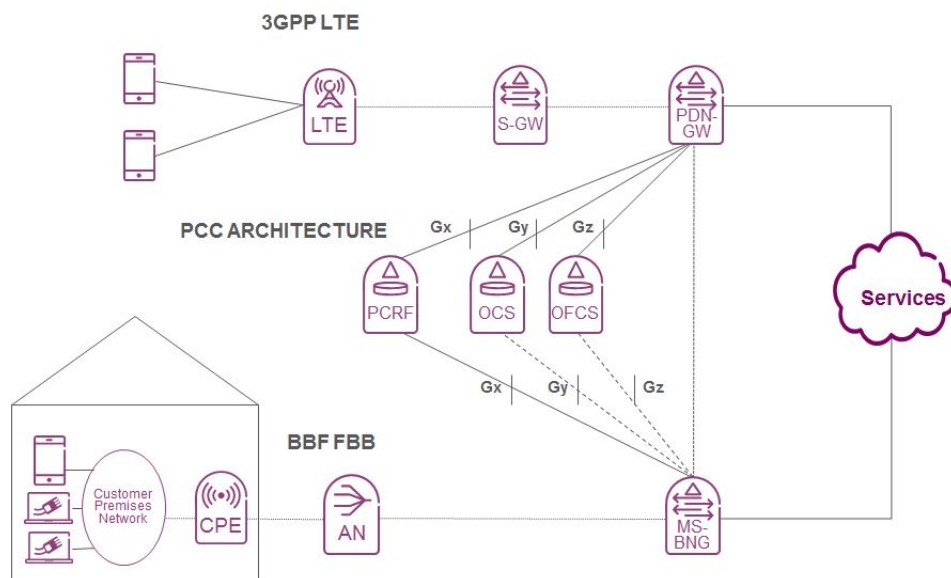


Figure 3 Policy Convergent Architecture

The Policy Convergent Architecture allows the implementation of a convergent control plane, with the PCRF as the convergent policy server. Therefore the same PCRF can make policy decisions to be enforced through Gx at the PCEF in the Mobile Core - for example, PDN-GW -, and at the PCEF in the Fixed Core - the

MS-BNG. So it facilitates the definition of aligned service offerings, guarantees the end-user experience independently of the access technology used, and contributes to control the Operator capital and operational expenditures.

## 3.4 ETSI Network Functions Virtualization (NFV) Framework

ETSI GS NFV 002 (Reference [15]) standardizes the functional architectural framework for virtualized network functions and the supporting infrastructure. The high-level structure of the ETSI NFV framework is displayed in Figure 4.

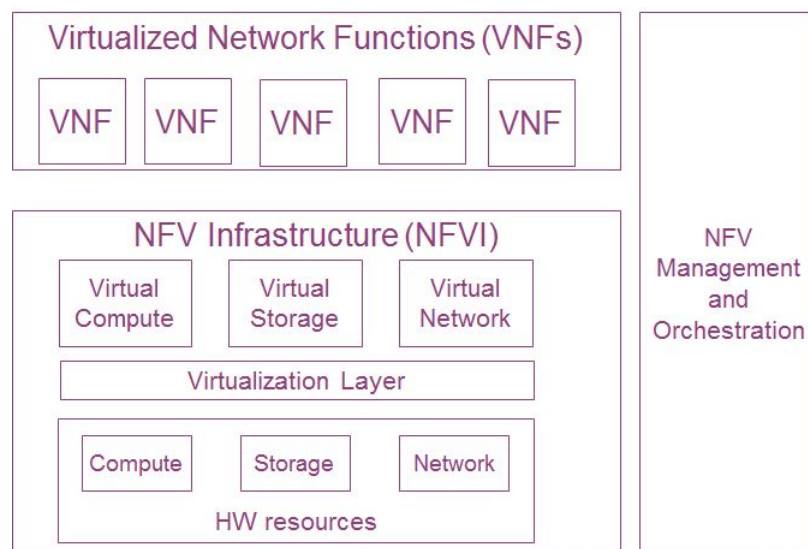


Figure 4 ETSI high-level NFV framework

The SAPC is a cloud-enabled application, being a Virtualized Network Function (VNF) according to Reference [15]. Therefore the SAPC can be deployed on top of a Cloud System as NFV Infrastructure (NFVI).

The SAPC can be orchestrated and instantiated by any Open Virtualization Format (OVF) compliant Management and Orchestration System, like the Ericsson Cloud Manager.

## 3.5 Naming Conventions

The following naming conventions are applied in this document:

- This document considers BRAS capabilities are included in the MS-BNG.



## 4 Solutions

### 4.1 SAPC in Ericsson Virtual Evolved Packet Core (Virtual EPC)

Operators consider NFV and cloud as the next-generation broadband network basis, owing to the flexibility (fast application deployment and automatic scalability on demand) and cost reduction (operational and capital expenditures) NFV and cloud provide. Therefore telecommunication applications are moving from native systems, including software (SW), middleware, and hardware (HW), to virtualized systems (SW-only), becoming then virtual applications.

In such line, Ericsson is virtualizing the complete Ericsson Evolved Packet Core (EPC) portfolio. Therefore a new Ericsson solution has been defined: the Ericsson Virtual EPC. The Ericsson Virtual EPC allows an easier and faster deployment of a dedicated EPC for a Mobile Virtual Network Operator, an Enterprise, or for controlling Internet of Things devices.

The Ericsson Virtual EPC includes the following Ericsson virtual applications: the Virtual EPG, the Virtual SGSN-MME, the Virtual SAPC, and the Virtual Wi-Fi Mobility Gateway (WMG).

### 4.2 SAPC in Ericsson IMS

The IMS consists of a set of functions implementing a Service Network that enables person-to-person and person-to-content communications, in various modes and in a highly personalized and controlled way. Originally designed by 3GPP for delivering IP Multimedia to mobile users, IMS has become a core component within 3G, cable TV, and next generation fixed telecoms networks. The IMS can be used in several different solutions, like VoLTE, PSTN to IP, Visual Communication, and Business Communication.

Ericsson IMS portfolio is the Ericsson state-of-the-art implementation of the IMS, fully virtualized, and ready for cloud deployments. Ericsson IMS is convergent, which enables Operators to run first-line communication services (for example, VoLTE) for both Fixed and Mobile Networks.

The SAPC enhances the Ericsson IMS with policy control for GSM/UTRAN/E-UTRAN accesses. Such policy control includes gating control, charging correlation, resource reservation, and bearer event notification.

### 4.3 SAPC in Ericsson Wi-Fi Calling

The SAPC is integrated in Wi-Fi Calling network architecture by interacting with both the IMS domain and the EPC network. Subscribers can set up then a voice call from an untrusted Wi-Fi network through the IMS domain. So the QoS of

such voice call is controlled through the Operator's EPC. The Ericsson WMG is the key network element for anchoring the data connection from the untrusted Wi-Fi domain to the Operator's EPC.

The SAPC enables to dynamically set or modify the QoS and charging settings for Voice and Video services over Wi-Fi network including Wi-Fi/LTE handover.

## 4.4 SAPC in Ericsson Integrated Policy and Charging

In addition to the 3GPP PCC standard implementation of 3GPP Sy (which is defined for providing policy decisions based on spending limits, see section 5.2.9 in Reference [5]), Ericsson has developed the Integrated Policy & Charging solution. It is an Ericsson enhancement of the 3GPP standard: Ericsson solution enables abstracting the PCRF from the Business Support System (BSS) layer complexity, and to abstract the OCS from the network complexity.

The solution requests the deployment of both the Ericsson Charging System/Mobile Broadband Charging and the Ericsson SAPC. It provides the following improvements on top of the 3GPP standard:

- A unified PCRF and OCS subscription view: 3GPP Sy assumes that PCRF accesses to subscriber data in an SPR using Sp reference point, while OCS holds its own subscriber data. However, Ericsson Integrated Policy & Charging solution considers one single subscription provisioning point: the Ericsson Charging System/Mobile Broadband Charging.
- A uniform PCRF and OCS product catalogue handling for broadband data offers: the 3GPP architecture implies PCRF needs to have detailed information about the broadband data product catalog, and extensive logic to be able to select the applicable product among many overlapping products related to a subscriber. The Ericsson Integrated Policy & Charging solution hides such complexity to the SAPC, because of the needed information is directly reported (when needed) from the Ericsson Charging System/Mobile Broadband Charging.

## 4.5 SAPC in Ericsson SDN

SDN is a network architecture that introduces programmability, centralized intelligence, and abstractions from the underlying network infrastructure. In SDN, the control plane logic is handled by a centralized server and the forwarding plane consists of simplified switching elements that are “programmed” by the centralized controller.

Ericsson SDN solution consists on several functions, including the OpenDaylight® Platform, the Ericsson SDN-Controller, and the Evolved Flow Switch.

The SAPC introduces the subscriber dimension into the Ericsson SDN Service Chaining solution.



#### 4.5.1 SAPC in SDN - Service Chaining

Service Chaining is an SDN application that facilitates the integration of transparent Value-Added Services (VAS) into the Operators' service network. Service Chaining allows dimensioning each transparent VAS based on the traffic demand for such VAS. So Service Chaining solution improves the time to market for new services.

The SAPC provides the subscription-based policy abstractions to the Ericsson Service Chaining SDN solution. The SAPC CAN send real-time policy decisions based on network information and subscriber profile towards the Ericsson SDN-Controller. The SAPC reports then the IP-CAN Session state (PDN connection setup and termination) and the subscriber profile that applies to such IP-CAN Session. And the service chain selection is based on policy evaluation made in the SAPC.

The communication between the SAPC and SDN-Controller is based on SOAP notifications. See section Section 5.9 on page 25 for further details regarding the SAPC SOAP Notifications function.







## 5 Functions

### 5.1 Policy Management for Mobile, Fix, and Convergent Networks (Gx-based)

The SAPC implements 3GPP PCRF according to Reference [5]. It provides then Multi-Access Policy Management to Network Elements implementing 3GPP PCEF in both the Mobile core (for example, PDN-GW, DPI) or Fixed Broadband core (for instance, MS-BNG, DPI) by Gx interface. Gx is a 3GPP standard interface which is based on IETF Diameter Credit Control Application -Reference [17] - and IETF Diameter base protocol (Reference [19]).

Through this function, any User Plane Network Element supporting Gx can request policy information for a given IP session at IP Session establishment and modification.

Policy and Charging control is performed by installing/removing PCC Rules. A PCC Rule is a set of information including:

- Filters that enable the detection of traffic IP flows belonging to a service and allows PCEF to block those packet flows that does not match with the filter.
- Charging data that allows PCEF to apply different charging depending on the service.

The applicable set of PCC Rules to install/remove in the PCEF might be obtained either through the subscriber profile/subscriber group profile or as a result of the evaluation of the applicable control policies.

The following subclauses describe the controls that can be applied.

#### 5.1.1 Bearer QoS Management

The SAPC is the network element that enables a subscriber-based end-to-end QoS control. The SAPC can modify the QoS negotiated in the bearer plane according to local conditions defined by the Operator for 3GPP access. Bearer QoS control in combination with subscriber differentiation allows Operator to offer subscriber groups such as gold, silver, bronze subscriptions, where gold subscribers are favored over other subscribers.

In order to manage the QoS assigned to a specific bearer, the SAPC can act on the parameters that 3GPP defines as part of the QoS information (see Reference [5]). Such parameters include the QoS Class Identifier (QCI), Guaranteed Bit Rate (GBR), Maximum Bit Rate (MBR), Access Point Name - Aggregated Maximum Bit Rate (APN-AMBR), and Allocation Retention Priority (ARP).

With Bearer QoS Management, the Operator can implement different kind of controls like the listed below (not restrictive list):

- Controlling the maximum bandwidth per dedicated bearer and per subscriber.
- Guarantee that the bearer QoS corresponds with the requirements of the service.
- Prioritize a premium service over others that are not profitable in case of congestion.

The SAPC supports Bearer QoS Management for both the default and dedicated bearers. For the default bearer, the SAPC controls the maximum and minimum QoS values, which may depend on subscriber or subscriber group and other parameters configured by policies. These QoS control policies evaluate conditions based on the subscriber profile, User Equipment (UE) information, Radio Access Type (RAT), or location. For example, it enables Operators to control the QoS for subscribers roaming in different networks (Serving Gateway change) or when changing from between different radio technologies - RAT changes. If there is a default bearer modification owing to a network condition change, the SAPC is able to recalculate the QoS bound to the default bearer.

The SAPC allows network-initiated QoS control for dedicated bearers. Dedicated bearers are extra logical transmission paths that have a particular QoS characteristic and a set of filters that define which IP flows are traversing the bearer. By dedicated bearers, an Operator can control the QoS granted for a particular service delivery, depending also on subscriber categorization and state. The SAPC can decide to setup/update/remove a dedicated bearer upon receiving the following events:

- IP-CAN session setup or IP-CAN session modification: The decision of initiating a new bearer might be triggered by policy decisions based on the subscription profile. It means that new bearers are triggered when the UE is establishing the default bearer or when there is a modification in the IP-CAN Session.
- Change of the subscriber profile data by provisioning.
- When the usage limit for the subscriber is surpassed (see Section 5.15 on page 28): The prioritization assigned to a particular service delivery can be removed (that is, remove a dedicated bearer).

**Note:** Bearer QoS Management is not applicable for Fixed Broadband Networks, owing to the bearer concept does not exist in Fixed Broadband.

### 5.1.2 Bandwidth Management

The SAPC provides real-time Bandwidth Management to control the peak throughput on a per service and subscriber basis. This bandwidth control is limited to the enforcement point, not being transmitted to the other nodes in the network (for example, Radio Access Network nodes). So then it is applicable for both Fixed and Mobile Access.

Either PDN-GW, DPI, or MS-BNG reacts on the information received from the SAPC to enforce the requested service throttling. Throttling acts on the single IP



flow (service) independently of the actual congestion in the network and has an immediate impact on the service performance. It tries to avoid that scarce resources are becoming congested.

### 5.1.3 Charging Control

The SAPC provides charging information at two different levels:

- Subscriber level: It includes data like charging method (online/offline) or Charging Systems addresses.
- Service Level: It includes the charging information (rating group) applicable per service.

The charging information might be obtained either through the Subscriber/subscriber group profile or as the result of the evaluation of the Charging Rules within the SAPC Rule Engine.

### 5.1.4 Access Control

The SAPC permits or rejects IP-CAN Session Establishment and Modification operations, according to Operator defined policies. For instance, the SAPC may allow the restriction of the number of IP-CAN Sessions per subscriber and PDN Identifier. The Operator can define specific policies for rejecting the session activation/modification under certain circumstances (for instance, disconnect the IP-CAN Session when modification message has RAT=WLAN).

In addition, the SAPC can provide Access Control per service (thus controlling the authorization of individual services, when a service a set of IP flows), and for a particular user under different access conditions. Service access control functionality decides whether the IP flows are allowed to progress, are dropped, or are redirected to a web portal.

Service Access Control is done in three steps: first the SAPC selects the applicable services to evaluate; then evaluates such selected services to decide which ones are authorized; and finally installs the authorized services in the enforcement node.

### 5.1.5 Multiple PCEF Support

The SAPC can provide the policy decisions to be enforced for a single IP-CAN Session to two or more PCEFs simultaneously. Therefore the SAPC is able to decide what policy control functions can be enforced by each PCEF for that session.

This functionality also enables the SAPC to take into account information received from one PCEF for making a policy decision that is enforced in second PCEF. As an example, Multiple PCEF Support can be used for getting usage reporting

information from a DPI, while the policy decisions based on the accumulated usage (see Section 5.15 on page 28) are enforced in the PDN-GW.

The set of functions to be enforced by each PCEF can be configured by the Operator. The SAPC only executes the controls applicable for the requested PCEF according to the control configuration information. The splitting can be changed during the SAPC live operation.

### 5.1.6 Application Detection and Control (ADC)

The 3GPP ADC function allows the SAPC to be aware of the user plane detection (at the PCEF) of a specific service. Based on such awareness, the SAPC is able to update the IP-CAN Session when either the subscriber actually starts using such service (and then enabling the delivery of such a service on a dedicated bearer), or when the subscriber stops to use it.

The SAPC implements the 3GPP ADC function on the Gx interface.

The function permits to dynamically define the criteria for activating the service reporting or not. Such criteria can be based on the information provided by the PCEF in the Gx, subscription profile data, or Time of Day. In addition, the SAPC can indicate the PCEF to trigger a redirection whenever the services to be controlled are detected.

### 5.1.7 Presence Reporting Area (PRA) Support

Presence Reporting Area (PRA) Support is a 3GPP PCC standard function allowing the implementation of location-based policy control in a multi-vendor Packet Core environment. Reference [5] defines the PRA as an area within 3GPP Packet Domain for the purposes of reporting of UE presence within that area due to policy control and/or charging reasons. There are two types of Presence Reporting Areas: "UE-dedicated Presence Reporting Areas", and "Core Network pre-configured Presence Reporting Areas".

The PRA Support function enables the SAPC dynamic subscription to 3GPP UE presence reporting events from the core network. Then the SAPC can receive the 3GPP UE PRA information whenever the UE attaches or moves into a new MME/SGSN, or the MME/SGSN detects the 3GPP UE has entered or left a PRA. Therefore the SAPC can use PRA into the policy decision.

**Note:** PRA support is not applicable for Fixed Broadband Networks.

### 5.1.8 Advanced Policy Controls (Ericsson Gx+)

Ericsson has extended the standard Gx capabilities in order to implement Advanced Policy Controls. Those Advanced Policy Controls can be only provided by a joint solution provided by either the Ericsson EPG as PCEF, and the SAPC. This is the Ericsson Gx+ reference point. Consequently it is only applicable for Mobile Broadband deployments, and with Ericsson products.



The Advanced Policy Controls are the following:

- **Rule space management:** A Rule Space defines the set of static PCC Rules that might be potentially assigned to a particular subscriber. The Operator may define different Rule Spaces but only one can be active. Once the Rule Space has been selected at IP session setup, it cannot be modified.

At IP-CAN Session Establishment, the Ericsson EPG may suggest a rule space. However, the SAPC may override such suggestion and select a different one. The SAPC is able to select it based on policies whose inputs may be subscription information, date, and time or any data received from the access gateway such as PDN Identifier or RAT.

- **Redirection information for non-authorized services:** The Ericsson EPG may decide whether to redirect or not a service request that is not authorized and to which server based on authorization result codes provided by the SAPC.
- **Content-filtering:** The SAPC provides the applicable content-filtering profile per subscriber to the Ericsson EPG. The Ericsson EPG makes use of this profile to decide whether to allow or not the subscriber to access to a specific URL content. The SAPC obtains the value of the content-filtering profile as the result of Operator defined policies evaluation.
- **Header enrichment:** The SAPC is able to provide subscriber-related information the Ericsson EPG can insert in the HTTP headers of a particular request. Then a third-party application can receive a user alias, so sensitive data like the MSISDN is not disclosed to them. The SAPC allows the Operator to define any kind of data to be inserted.
- **PCRF-Assisted APN Selection:** The Ericsson EPG may request the SAPC to change the APN for the subscriber and the IP-CAN Session by Ericsson Gx+. The SAPC, as the result of a Flexible Output Protocol policy (see Section 5.12 on page 27), introduces the APN to be used for such subscriber IP-CAN Session, plus the DIAMETER-AUTHORIZATION-REJECTED result code. The Ericsson EPG retries then the IP-CAN Session Establishment for the new APN, which is authorized by the SAPC.

The Advanced Policy Controls through Ericsson Gx+ are only applicable to the default IP-CAN Session.

## 5.2 Policy Management for Wi-Fi Access

The SAPC provides policy control decisions to the Ericsson EPG by 3GPP Gx when Wi-Fi access is used. The scenario is the following:

- The SAPC identifies that the subscriber is making use of a Wi-Fi access. This is due to the Gx CCR message for the IP-CAN Session establishment includes the RAT set to WLAN and the IP-CAN-Type set NON-3GPP-EPS.
- The SAPC provides then specific policies per subscriber for such Wi-Fi access, which are enforced by the Ericsson EPG.

The main application of this function is the provisioning of QoS and Charging settings for voice and video services over Wi-Fi (that is, Wi-Fi calling), including the support of Wi-Fi/LTE handover. The SAPC is the responsible for providing Dynamic Policy Control for the Wi-Fi calling as it is described in Section 5.4 on page 19().

## 5.3 Subscription Management

The SAPC logic, upon receiving an input request, uses several data entities to generate the different outputs. The basic data entity is the subscriber profile. The SAPC logic is able to find the subscriber profile upon receiving a traffic identifier, like the Network Access Identifier (NAI)

Once the subscriber has been identified, the applicable profile results from the combination of the subscriber profile associated with such subscriber identifier and the profiles associated for the different subscribing offerings the subscriber belongs to. One subscriber can be associated with multiple service offerings. Each service offering defines the profiles characterizing such subscription. The criteria to decide which offering is applicable at any time is based on the priority level and validity time associated with the relationship between subscriber and the service offering.

The subscriber profile includes data such as:

- Subscriber groups: Group to which the subscriber belongs to.
- Subscribed Services: List of specific services associated with the subscriber.
- Blacklist services: List of specific forbidden services associated with the subscriber.
- Operator Specific Info: Data defined by the Operator that can be used for policy evaluation
- Fair Usage limits can also be defined at subscriber level.

There might be cases where the policy data applicable to a subscriber cannot be obtained using static data because they also depend on dynamic conditions. For example, the service authorization can or not depend on the time of the day. For such cases, the Operator may configure business rules that evaluate the dynamic conditions. The evaluation of such rules gives the applicable data for the current dynamic conditions the subscriber is under.

### 5.3.1 Auto-provisioning

The SAPC allows the automatic creation of a subscriber in the SAPC database when the PCEF requests an IP session establishment. As a result of the auto-provisioning operation, the SAPC assigns a subscriber group to the auto-provisioned subscriber. Such subscriber group may be the auto-provisioning subscriber group (static assignment); or may be dynamically assigned after rule



evaluation (making use of inputs like time, date, or dynamic information received in the Gx queries like the user location).

The auto-provisioning allows the definition of usage control limits as well.

Auto-provisioning avoids the need of performing SAPC subscribers pre-provisioning before starting the SAPC operation - reducing then the SAPC integration costs in Operator networks. From network point of view, auto-provisioning is feasible because of the IP session establishment request is received by the SAPC after the subscriber has been authenticated by the network.

The SAPC also includes a default profile, called Unknown Subscriber Profile, which does not provision any subscriber entry in the SAPC. This Unknown Subscriber Profile enables providing policy control for subscribers that do not need a dedicated management.

## 5.4 Dynamic Policy Control

This function allows the adaptation of the service delivery to the conditions negotiated in the User Plane through introducing the application input into the SAPC policy decision. The application in this context is called AF, and can take the role of the actual application - for example, a streaming server -, or a proxy that has all the service information - like the P-CSCF in IMS.

The AF is able to send service information to the SAPC by the 3GPP Rx interface (Reference [8]). The service information includes the set of IP flows that define a media component: media type (for example, audio, video), Application Identifier, and requested bandwidth.

Based on such service information, the SAPC generates dynamically the PCC Rules that are to be installed in the enforcement point at the User Plane.

Dynamic Policy Control may be used for both IMS (that is, services based on session negotiation) and non-IMS services. The differences are explained in the subclauses below.

### 5.4.1 Dynamic Policy Control for IMS Services (e.g. VoLTE, Wi-Fi Calling)

**Note:** This clause is generally applicable to services that are based on session negotiation, not only to IMS Services.

IMS requires a signaling negotiation between the two peers trying to establish a connection before accessing to a particular service. The reason of such signaling negotiation is to define the characteristics of the bearer where the service is delivered. The involved peers use the Session Description Protocol (SDP) data to negotiate the session parameters, including the media streams to be used (such as video, audio, media codec).

The SAPC is the responsible for binding the agreed session parameters with the PDN connection data. The SAPC ensures that then enough resources are

established in the User Plane to execute the service according to the parameters negotiated in the Application Plane. Therefore only authorized media are executed in the IP-CAN Session.

For such purpose, the AF (that is, P-CSCF in IMS) transfers to the SAPC the set of IP flow that defines a media component, the media type (for example, audio, video), the application identifier, the requested bandwidth, and the rest of the data included in the negotiated SDP. The SAPC uses such data to generate dynamic PCC Rules per each media subcomponent, and to determine their associated QoS. Those dynamic PCC Rules are then sent to the PDN-GW, the responsible of making the actual enforcement.

Dynamic PCC Rules are dynamically generated and/or modified by the SAPC upon reception of Rx messages. Dynamic PCC Rules include information about:

- SDF filters: These filters are used by the PDN-GW to filter the IP traffic within a bearer to determine, at IP flow level granularity, what services are allowed to be passed to the desired end point.
- QoS information: QCI, ARP, MBR and, if applicable, GBR data. These data defines the characteristics of the bearer instantiated or modified. QoS is obtained using Operator defined rules that use as input the Rx application identifier, the media component type, and subscriber profile.
- Gating control data: Upon request from AF, gating control enables or disables temporarily the passing of an SDF through the PDN-GW.
- Charging information for those SDFs: The value of the charging information is calculated by SAPC based on the combination of media information (for example, media type or media flow direction), subscriber associated policies that can evaluate conditions such as date and time, other information received from the PDN-GW (for example, RAT, APN or location information), and subscriber provisioned information.
- Charging Correlation: It makes possible the correlation of the charging information generated by the User Plane and the Application Plane at the Charging System.
- Resource Allocation Notification: The SAPC may indicate the User Plane that confirmation of successfully allocated resources is requested.

Dynamic Policy Control is used for implementing IMS services like VoLTE, where features like path reservation, call termination and the reporting of transmission events to the IMS network request the deployment of a PCRF like the SAPC.

In addition, the SAPC is the enabler of the VoLTE Single Radio Voice Call Continuity (SRVCC) function. SRVCC provides the capability to handover VoLTE calls from the Packet Switch (PS) domain to the Circuit Switch (CS) domain whenever coverage or resources on LTE networks cannot guarantee voice quality.

During the SRVCC procedure, the SAPC receives an indication from the PCEF that one or more PCC Rules cannot be maintained because of PS to CS handover. The





SAPC may then report to the P-CSCF the bearer has been deactivated because of a PS to CS handover. And the call can continue in a seamless way.

#### 5.4.2 Dynamic Policy Control for Non-IMS Services (e.g. IPTV)

Upon an Rx AF reporting regarding the service delivery start, the SAPC is able to trigger an IP-CAN Session modification that may imply the PDN-GW either updates the policies for the default bearer or sets up a dedicated bearer. In the same way, when the AF reports the service delivery has finished, the SAPC performs another IP-CAN Session modification, so the PDN-GW may either downgrade the policies to their first value for the default bearer, or remove the dedicated bearer.

As an example, let us consider a network where the DPI function provides an Rx interface towards the SAPC. In such scenario, the DPI function takes the AF role. The DPI function can be then configured to detect some service flows traversing it (for instance, flows related with IPTV). Therefore the DPI function can report the SAPC when a service delivery begins. Consequently the SAPC is able to update the IP-CAN Session to change the applicable QoS for the default bearer according to the service needs. And once the DPI reports the service delivery has finished, the SAPC modifies the IP-CAN Session. So the default bearer QoS is refreshed to the one assigned before the initial detection of the service.

#### 5.4.3 Network Location (NetLoc)

NetLoc function allows the reporting of the Access Network Information to the Service Layer Domain (e.g. the IMS domain) by the SAPC.

NetLoc is usually requested for VoLTE and ViLTE communications because of regulatory issues. It can be used as well for location based charging of the VoLTE/ViLTE service.

The SAPC provides NetLoc function when EPC-based untrusted WLAN access is used as well.

NetLoc function is activated based on Service Layer request to the SAPC at AF session establishment. It must be provided at any AF session event (for instance, at VoLTE/ViLTE session establishment, update or termination), and at the IP-CAN Session or Bearer termination events that may affect an ongoing AF session.

#### 5.4.4 Emergency Calls

The SAPC is able to handle both IMSI and non-IMSI based emergency calls. Therefore, if the PCEF does not include the Subscription-Id AVP but includes the IMEI within the User-Equipment-Info AVP, the Emergency call proceeds.

The option to accept unauthenticated emergency services with IMEI identifier can be switched on and off by configuration.

### 5.4.5 IP-CAN Type Change Notification

The IP-CAN Type Change Notification is a standard 3GPP PCC function. A PCRF implementing this function reports to the AF a change in the IP-CAN type (e.g. from 3GPP-EPS to 3GPP-GPRS) and/or the RAT type (e.g. from E-UTRAN to WLAN) during the IP-CAN Session lifecycle. This function is used for updating the policies to be enforced considering changes in the access network.

The SAPC implements the 3GPP standard IP-CAN Change Notification function as it is described in 3GPP TS 29.214 (Reference [8]).

**Note:** The SAPC does not support the management of IP Flow mobility routing rules. Therefore the Notification of IP-CAN Type Change due to IP Flow mobility is not implemented.

### 5.4.6 Subscription and Notification of Signalling Path Status

The Subscription and the Notification of the Signalling Path Status function is a standard 3GPP PCC function. It allows the PCRF to report the release of the user plane transmission path to the AF. For such purpose, the AF must be subscribed to such notification at AF session establishment.

In general, the AF subscribes to Notification of Signalling Path Status in a dedicated AF (Rx) session. This AF session is different than the AF sessions created for handling the dynamic services activation/deactivation (i.e. the delivery of the VoLTE/ViLTE communication). So half of the licensed AF sessions capacity can be devoted for delivering the VoLTE/ViLTE communication.

The SAPC implements the Subscription and Notification of Signalling Path Status function as it is described in 3GPP TS 29.214 (Reference [8]).

**Note:** The SAPC does not support the Gxx reference point towards the Bearer Binding and Event Reporting Function (BBERF). Therefore this function is not provided for the Gxx-based Subscription and Notification of the Signalling Path Status at Gxx reference point is not provided.

**Note:** The SAPC does not support the Release Cause Code. The SAPC does not support the INDICATION\_OF\_LOSS\_OF\_BEARER value in the Specific-Action AVP. The Notification of Signalling Path Status for both items is consequently not implemented.

### 5.4.7 IMS Restoration Support: Provisioning of AF Signalling Flow Information

The SAPC implements the support to IMS Restoration based on the 3GPP PCC Provisioning of AF Signalling Flow Information Procedure as it is described in 3GPP TS 29.214 (Reference [8]). This function is used by the IMS Restoration procedures to provide the address of the P-CSCF selected by the 3GPP UE to the PDN-Gateway (seeReference [6]).

For such purpose, and after 3GPP UE registration to the IMS network, the SAPC provides the P-CSCF the 3GPP UE is using for such IMS session to the PDN-GW.



The PDN-GW monitors the P-CSCF status, And if it does not respond, the PDN-GW can update all the 3GPP UEs about it, triggering the discovery for a new P-CSCF.

## 5.5 Integrated Policy and Charging - Policy Control Based on Spending Limits

The SAPC allows the introduction of the spending limits the 3GPP OCS is handling into the policy decision chain. That is the target of the 3GPP Sy interface (Reference [9]), which conveys information about the spending limits status. Being a standard-defined interface, the 3GPP Sy permits the integration of the SAPC with any vendor OCS.

In addition, the SAPC provides Ericsson own enhanced implementation of Sy, called Ericsson Sy, for integration with Ericsson OCS, the Charging System/Mobile Broadband Charging. This is referred as the Ericsson Integrated Policy and Charging solution. See Section 4.4 on page 10 for further details.

The SAPC retrieves the applicable spending limits (Policy Counters according to 3GPP Sy specification, or Policy Groups in Ericsson Sy) from the OCS at IP-CAN Session establishment. This information is used as an input in the policy engine to decide which conditions apply to the subscriber. If there is any change in the spending limit status during the IP-CAN Session, the OCS reports it to the SAPC. And the SAPC can then trigger a reauthorization of the policies enforced into the PDN-GW.

The SAPC caches all the information retrieved through the 3GPP or Ericsson Sy interface for a subscriber during the IP-CAN Session lifetime. This mechanism avoids extra queries towards the OCS, improving the overall performance of the SAPC. The cache is updated at the reception of an OCS report regarding spending limits change

The SAPC can dynamically select the applicable OCS for the 3GPP Sy or Ericsson Sy interaction by policies depending on the provided information in the Gx request (like, for example, the MSISDN/IMSI series or the roaming status).

## 5.6 Mobility Based Policy

The SAPC can provide policy decisions directly to the Ericsson SGSN-MME. This is the purpose of Mobility Based Policy function, and it is achieved by the Ericsson-proprietary Smp reference point. Ericsson Smp is based on a Diameter interface connecting both the SAPC and the Ericsson SGSN-MME.

The function allows the Ericsson SGSN-MME to get subscription-based policy decision from the SAPC. Such policy decisions can consider information provided by the Smp interface (like IMSI, user location, APN) and/or subscription profile data.

The function enables the implementation of the use cases listed below:

- PDN-GW selection function: The SAPC selects the IP address (IPv4 and/or IPv6) and/or Fully-Qualified Domain Name (FQDN) of a list of PDN-GWs for routing the user plane traffic of a 3GPP UE attaching to the network.
- Mobility Management function: The SAPC permits the selection of the Subscriber Profile ID (SPID) for RAT/Frequency Selection Priority based on policies. This is a mean for increasing radio optimization.

The SAPC 1 release provides Mobility Based Policy only at Smp session establishment and termination. The support of a complete Smp session-state machine, including the Smp session modification and reauthorization, is planned for future the SAPC releases.

## 5.7 External SPR Support

The SAPC can be configured to use the subscriber profile information available in an external Lightweight Directory Access Protocol version 3 (LDAPv3) SPR during the policy evaluation and decision process.

An example of external SPR that can be integrated with the SAPC is the 3GPP UDR.

For enabling reading operations towards the external SPR, the SAPC introduces the configuration concept of Entity Data Source. The Entity Data Source contains the specification (in an ad-hoc definition language) about where the data to be fetched is stored. In case such a data requested for policy evaluation cannot be fetched from the external SPR, the SAPC (if configured for) uses the 'unknown subscriber profile' for providing the policy decisions to the PCEF.

In the same way, and for writing operations, the SAPC manages the configuration concept of Entity Data Target. An Entity Data Target defines how to write in the external SPR.

The SAPC can also receive SOAP notifications reporting subscription modifications in the external SPR. Based on that notification, the SAPC can trigger the policy reauthorization process as it is described in Section 5.10 on page 26. Specifically, the SAPC supports the Web Services Description Language (WSDL) data structure defined for the Ericsson Centralized User Database (CUDb) product, permitting an easy integration when Ericsson CUDb is deployed as SPR.

Although nowadays the SAPC supports only external LDAPv3 SPRs, the function may be extended to other database technologies (like HTTP-based or SQL-based ones) with a very short time to market.

### 5.7.1 External SPR 1+1+1 Redundancy Support

The SAPC supports UDC deployments with the Ericsson CUDb in the 1+1+1 geographical redundant setup .



The function implies the SAPC always connects by default to the CUDB instance defined as primary, and automatically addresses the secondary CUDB node in the event of unresponsiveness from the primary. This same behavior applies in case of failure of the secondary node (not being the primary recovered yet) when the SAPC connects to the third alternative.

When the CUDB instances become available again, the SAPC automatically reconnects to the available instance with the highest priority.

## 5.8 Time-Based Authorizations

The SAPC is able to perform the reauthorization of the policies downloaded into the PCEF whenever the validity time for such policy data expires. The SAPC controls internally how long a policy is valid; and once its validity time is over, the SAPC initiates a reauthorization process that might drive to an in-service change of the policy data previously downloaded into the PCEF.

Besides, Time-Based Authorizations are also applied to perform activation/deactivation of any subscriber offering associated with a subscriber. For example, if a subscriber buys a voucher, and such voucher overwrites the subscriber's regular subscription during a certain period, the mechanism triggers the activation/deactivation of the voucher.

### 5.8.1 Minimize Signaling Storms

The Operator may configure policies for Time-Based Authorizations to be applied for a subscriber group. This implies the Time-Based Authorization happens simultaneously for all the active subscribers that belong to such subscriber group. In order to minimize reauthorization message storms towards the PCEF, the SAPC spreads the reauthorization messages in different time windows. The window time duration and the number of messages that can be placed in such window can be configured.

## 5.9 Notifications to End-Subscribers or to External Systems

The SAPC provides the capability of sending Short Messaging System (SMS) notifications and web services-based notifications to the subscriber or to an external system upon certain events.

If SMS notifications are requested and configured, the SAPC sends the SMS notifications to the configured SMS Centers (SMSC) by Short Message Peer-to-Peer (SMPP) protocol. Notifications based on web services use SOAP/XML towards the web service end points, so they are also called SOAP notifications.

SOAP notifications enable the implementation of two policy use cases that are getting track in the industry. They may be configured for providing SAPC statistics and key performance indicators to an Analytics Server (like UE-tracing).

In addition, SOAP notifications are used for reporting the subscriber-related information to the Mobile SDN for service chaining purposes.

The conditions that should be fulfilled to trigger a notification message are configured by notification policies. These policies could be defined per subscriber or subscriber group.

Some possible examples of notifications are listed below:

- The amount of subscribed usage left is lower than a configured threshold.
- Usage limit is surpassed.
- Service access is restricted.
- QoS is downgraded.
- The subscriber is roaming and has consumed 50 MB; and from then on, the subscriber is going to be charged with roaming prices.

The text of the notification message can be configured by the Operator, so the Operator may include different information depending on the notification event. The text of the message uses Unicode characters, allowing then to write the notifications text using Latin or non-Latin characters.

Multiple destinations can be used simultaneously for the same notification.

## 5.10 Reauthorization Upon Subscription Change

The SAPC is able to initiate a reauthorization procedure towards the PCEF when there is a subscriber profile update that implies changes in the policies previously enforced in the PCEF. Once the subscriber profile is modified, the SAPC makes a policy re-evaluation, and sends the new policies to be enforced to the PCEF by Gx RAR.

## 5.11 1+1 Geographical Redundancy

The SAPC provides an 1+1 Geographical Redundancy solution. Such solution allows a robust and high-available the SAPC deployment, enabling seamless service continuation in case of failover. The overall the SAPC system availability reaches a target figure of 99.999%.

The 1+1 Geographical Redundancy implies both the SAPCs in the geographical redundant system are connected through a replication channel. This replication channel is the responsible for the synchronization of the data between the mated pair elements.

Therefore information like the subscriber profile, the available services, or the accumulated consumption are replicated. In addition, the state information the SAPC manages (thus the active IP Sessions for the subscriber) is also replicated.



The SAPC supports two configuration modes for the 1+1 Geographical Redundancy solution:

- Active-Active: Every the SAPC in the 1+1 pair processes the incoming traffic and the provisioning operations. And each the SAPC keeps the state of the other one. Therefore a single the SAPC is ready to process automatically all the incoming traffic and provisioning operations when the other the SAPC cannot handle it.

The solution considers each the SAPC in the 1+1 pair handles a maximum of a 50% of the traffic in normal operation (thus when both the SAPC are available).

The 1+1 Active-Active Geographical Redundant solution is optimized (in performance and response time) when subscriber and session stickiness is implemented at network level. Thus the SAPC Diameter clients must bind all the IP session requests for the same subscriber to the same specific the SAPC instance.

**Note:** The increment in the response time because of the lack of subscriber and session stickiness is estimated in a 300%.

- Active-Standby: Just one of the SAPC in the mated pair (the Active one) is processing the incoming traffic. If the Active SAPC goes down, the control is taken by the other SAPC (the Standby), which becomes the Active one.

The SAPC provisioning is done only in the Active SAPC. The replication channel replicates such provisioning data into the other SAPC.

## 5.12 Flexible Output Protocol

Flexible Output Protocol is the SAPC toolbox enabling the adaptation of the outgoing the SAPC signaling according to its neighbor nodes (e.g. the PCEF) protocol needs. Its main purpose is to facilitate the inter-operation with neighbor nodes that are not fully standard compliant and may manage vendor-specific information. The function then allows the introduction of non-standard vendor-specific attributes, or the modification of the standard one, in the SAPC responses by configuration.

The SAPC applies Flexible Output Protocol depending on the evaluation of dynamic conditions, defined with Flexible Output policies. The function takes the result of the SAPC business logic, and using such policies, enhances the resulting message with the needed information. The message is delivered then afterwards to the neighbor node.

The SAPC 1 provides Flexible Output Protocol only for the Gx reference point. However, this function could be extended in the future for the remaining the SAPC reference points.

## 5.13 UE Trace

UE Trace is the SAPC tool enabling the tracing of any Gx and Rx message the SAPC is managing in real-time, and for a defined set of subscribers. Those subscriber are identified by the IMSI, MSISDN or the SIP-URI (SIP-URI is only applicable for UE tracing of Rx messages).

The UE Trace tool is activated on operator demand. For such purpose, the tool requests the definition of a tracing session, which consists of a unique session identifier and one or several subscribers to be traced.

The data of the UE Trace sessions are stored in XML files, in compliance with 3GPP TS 32.423 (Reference [11]). Such files contain the records of all the active tracing sessions. In addition, a Packet Capture (PCAP) file per UE Trace session is generated once the UE Trace session is stopped. Both the XML files and the PCAP files can be downloaded into an external file system by SFTP.

UE Trace is a tool useful for troubleshooting purposes. It is also a powerful tool in order to provide specific subscriber traffic input for business intelligence purposes.

## 5.14 Policy Studio

The SAPC Policy Studio is a Graphical User Interface (GUI) designed for easing the SAPC business operation and provisioning. The SAPC Policy Studio hides the SAPC data complexity, presenting the information to be provisioned in an understandable and easy-to-operate way.

The SAPC Policy Studio can be deployed in an external Linux server. That allows one SAPC Policy Studio instance can operate several SAPC applications instances.

In addition, the SAPC Policy Studio provides the following functions:

- Import and Export of the configured data.
- Draft/Off-line function.
- Pre-defined workflows (templates) for the SAPC provisioning.
- Single Point of provisioning for several the SAPC instances.
- Management of different Policy Studio users and roles for security purposes, including read only user roles.
- Configuration Guide Section, thus templates providing step-by-step guidance for configuring the SAPC use cases (VoLTE, Mobile Broadband and Integrated Charging).





## 5.15 Fair Usage Policies

Operators around the world are experiencing new customer behaviors based on the Networked Society paradigm - that is people, business and society are using connected devices, no matter the kind of access, to their benefit. One of the consequences of such paradigm is a huge increase of data traffic. This challenges current Operator business models, implying the need of finding new sources of revenues plus the efficient handling of the existing resources.

With such target, Operators are deploying policy management solutions based on usage control (also known as Fair Usage Policies). Based on such Fair Usage Policies, an Operator could, for instance, downgrade the subscriber bandwidth in case it consumes more than 5 GB of data traffic in a monthly period.

The SAPC is the critical network element for the implementation of Fair Usage Policies. The SAPC is the responsible for accumulating the volume consumed by the subscriber, calculating the applicable quotas, and making policy decisions - either access control, bandwidth management, or QoS control policy decisions - based on the accumulation status and the configured volume thresholds.

The solution is founded in 3GPP PCC Architecture (Reference [5]), where the SAPC implements the PCRF. The SAPC provides Fair Usage Policies for controlling volume and/or time usage. The usage control can be performed either at service level, or IP session level (i.e. overall traffic). The volume consumption and time consumption per service or IP session is handled by different counters.

### 5.15.1 Fair Usage Policies Procedure

At IP-CAN Session establishment (i.e. the SAPC receives a Gx Credit Control Request (CCR) message with CC-Request-Type AVP set to the value INITIAL\_REQUEST), the SAPC provides, in addition to the applicable policies for the IP Session, the volume and/or time quotas to be controlled by the PCEF in the Gx Credit Control Answer (CCA). When any of the provided quotas is consumed, the PCEF requests an IP-CAN Session Update to the SAPC (i.e. reception of a Gx CCR message with CC-Request-Type AVP set to the value UPDATE\_REQUEST). The SAPC updates then the usage accumulator, checks its limit, and decides the appropriate policies to be enforced - which are reported to the PCEF in the consecutive Gx CCA message.

At IP-CAN Session termination, the PCEF reports the actual consumption to the SAPC (by Gx CCR message with CC-Request-Type AVP set to the value TERMINATION\_REQUEST). The SAPC can then update the usage accumulator with the actual consumption.

When the reset period is reached (for example, the date ending the monthly Fair Usage Policies subscription), the SAPC automatically resets the usage accumulators, and reports the new applicable policies for the active IP-CAN sessions by a Gx Reauthorization Request (RAR).

### 5.15.2 Life Cycle of Usage Reporting Accumulators

The SAPC may be configured to accumulate the usage in two different types of accumulators:

- Session accumulator: Volume and/or time consumption is stored during the existing IP-CAN Session or IP Session level. The SAPC stores consumption accumulators at session level and reset them every time the user disconnects
- Permanent accumulator: Volume and/or time consumption is stored during a configured period (a month or a configured number of days or hours). In this case, the SAPC stores usage accumulators at subscriber level as they persist across different IP-CAN Sessions or IP Sessions. The configured period might be based on a billing cycle. The SAPC stores usage accumulators during a billing cycle and reset them on the specified billing date.

Both ways may coexist in a SAPC in live operation.

### 5.15.3 Usage Limits

The usage limits are used to trigger the subscriber policy evaluation whenever the usage performed by a subscriber surpasses such usage limits. Usage limits may be defined:

- At subscriber and/or subscriber group level.
- Associated with each particular counter: Different limits for a particular service or group of services or for the total traffic.
- Intermediate limits (that is multiple thresholds) associated with the same usage accumulator. Intermediate limits can be expressed in terms of absolute value, or as a percentage of the final limit.
- Usage limit shared by a number of users (for example, a corporation or members of the same family).

Usage limits can be defined for time control (only applicable to Gx-based Fair Usage Policies), or volume control. In the case of volume usage limits, they can be different for downlink and uplink data traffic. They can also be specified for bidirectional traffic.

### 5.15.4 Conditional Accumulation

The SAPC can perform differentiated control of the volume or time consumption only when certain conditions apply. For instance, to make the control for the accumulated usage only during the rush hours.

Moreover, the SAPC enables the usage of different accumulators for every condition. Then SAPC can take independent decisions, each of them based on the state of each of the specific counters. For example, the Operator might configure two different counters. The first one is for controlling volume consumption during



the rush hour, and the second counter applies only for volume consumption control during weekends. When the first counter surpasses the limit, the SAPC could download a policy decision for bandwidth management. Alternatively, when the second counter surpasses the limit, the SAPC could apply an access control policy.

### **5.15.5 Vouchers Support**

In addition to the application of Fair Usage Policies for normal subscriptions, the SAPC allows the handling of vouchers or promotions. For such purpose, the SAPC associates a voucher to a subscriber including one or several usage limits and an expiry date that is not periodically reset. The SAPC triggers a re-evaluation of subscriber-related policies whenever a limit is surpassed or the expiry date is reached.

The SAPC enables the refill of the voucher by extending the voucher usage limits and/or expiry date.

### **5.15.6 Quota Slicing**

The SAPC allows the configuration of quota slices, that is the split of the whole volume or time quota in smaller pieces. That implies only such smaller quota slices are the ones exchanged between the SAPC and the PCEF.

This functionality enables the SAPC to handle a more updated usage accumulator because of the update period is reduced (the provided quota is consumed earlier than the whole quota). However, there is an increase in the amount of signalling between the SAPC and the PCEF.

### **5.15.7 Reporting Intervals**

The SAPC permits the definition of reporting interval times. It consists of the setup of the maximum time between usage reports from the PCEF, to force the reception of usage information in regular time intervals, independently of the number of bytes consumed by the subscriber.

This function prevents the SAPC from not receiving usage reporting for a long period.

### **5.15.8 Shared Data Plans**

The SAPC permits configuring several subscribers sharing a common usage limit. An example of Shared Data Plan use case is the following: family access to Internet with a maximum usage limit of megabytes; the SAPC is able to control the usage reporting for different members of the family simultaneously. Shared Data Plans are also applicable for corporate users reporting to the same counter to limit the monthly cost

Shared Device Plans is a special application of the Shared Data Plans concept: the SAPC allows the usage control of a common subscription over different devices (multi-SIM).

#### **5.15.9 Access to Accumulated Usage Information**

The volume or time consumed accumulated by the SAPC is stored in the SAPC internal database. A customer care system can access to such information through the Representational State Transfer (REST) API.

It is also possible to reset the stored volume consumed to 0 by REST API.

#### **5.15.10 Advanced Usage Reporting**

The SAPC supports usage reporting capabilities for subscribers with multiple IP sessions. It provides then the handling of a common quota for different IP sessions and it is able to reevaluate and reauthorize (if needed) all the ongoing sessions for the same subscriber once one of the sessions has reported a limit surpassed.

The SAPC also supports different behaviors for the multiple IP sessions, being able to provide conditional accumulation based on the different IP sessions and PDN Identifiers the subscriber is connected to.

### **5.16 Other Supported Functions**

#### **5.16.1 IP Networking**

The SAPC supports IPv4 and IPv6 addresses for transport and user level.

#### **5.16.2 Overload Control and Load Regulation**

The SAPC is a robust telecommunication application, capable of controlling high load on their external interfaces (both signaling and OAM) and overload peaks without crashing.

In addition to that, the SAPC provides a Load Regulation function. Such function enables to reject incoming traffic when the configured thresholds (for both memory or CPU load) are surpassed. The Load Regulation function prevents then the likelihood of an overload situation at the SAPC.

Load Regulation function allows the prioritization of the Emergency Services in case of overload situation.

The SAPC is compliant then with ITU-T, Q543 (Reference [16]).

## 6 Interfaces

### 6.1 Reference Model

A simplified reference model of the SAPC is shown in Figure 5.

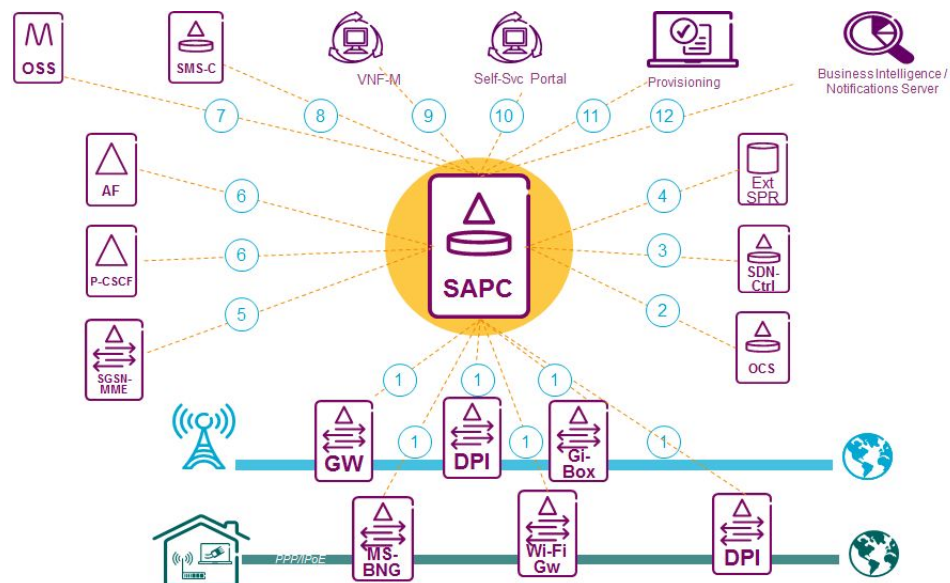


Figure 5 The SAPC Reference Model

The integration points are described as follows:

- 1 The SAPC provides 3GPP Rel-12 & 13 Gx interfaces towards mobile broadband gateways (PDN-GW), Fixed Broadband MS-BNGs, DPIs, Gi-Boxes, or the Ericsson Wi-Fi Gateway.
- 2 The SAPC includes 3GPP Rel-12 & 13 Sy support for getting the spending limits status from the 3GPP OCS. In addition, the SAPC provides Ericsson Sy interface for integration with the Ericsson Online Charging System.
- 3 The SAPC sends the subscriber information towards the SDN-Controller over SOAP notifications.
- 4 The SAPC implements the Sp reference point towards the external SPR. This implementation is compliant with 3GPP Ud protocol. The SAPC reads and writes subscription data from such external SPR by LDAPv3. The SAPC supports SOAP notifications to receive updates regarding subscription changes from the external SPR.
- 5 The SAPC interworks with the Ericsson SGSN-MME by Smp interface for Mobility Based Policy-

- 6 The SAPC provides 3GPP Rel-12 & 13 Rx interfaces for implementing Dynamic Policy Control for IMS services (P-CSCF) and non-IMS services.
- 7 The SAPC offers the following interfaces towards Operations Support Systems (OSS) for configuration, fault management, and statistics:
  - NETCONF for configuration management.
  - SNMP for fault management.
  - Command-Line Interface (CLI).
- 8 The SAPC provides an SMPP interface for sending SMS notifications to end subscribers.
- 9 When the SAPC is deployed on an NFVI, the SAPC delivers the workflows needed by the VNF-M for implementing VNF lifecycle management use cases.
- 10 The SAPC gives a REST API towards self-service Portals for subscriber profile modifications.
- 11 The SAPC offers a REST API for provisioning purposes.
- 12 The SAPC makes use of SOAP notifications for implementing web services-based notifications.

## 6.2 Statement of Compliance

### 6.2.1 Policy Control

- The SAPC implements a Fixed-Mobile Convergent 3GPP PCRF according to Reference [5] and Reference [14]. Therefore the SAPC is compliant with the 3GPP PCRF interface specifications.
  - The SAPC is compliant with 3GPP Rel-12, and Rel-13 Gx interface specifications as it is defined in Reference [7].
  - The SAPC is compliant with 3GPP Rel-12, and Rel-13 Rx interface specifications, described in Reference [8].
  - The SAPC is compliant with 3GPP Rel-12, and Rel-13 Sy interface specifications as in Reference [9].
  - The SAPC is compliant with 3GPP Rel-12, and Rel-13 Ud protocol implementation of the 3GPP Sp reference point, as it is specified in Reference [10].
- The SAPC implements a Fixed Broadband PDP according to Reference [13].



## 6.2.2 Operation & Maintenance

- The SAPC supports NETCONF for configuration purposes according to Reference [18].
- The SAPC is compliant with the Ericsson standard alarm MIBS described in Reference [2].
- The SAPC reports statistics in 3GPP compliant XML report files as defined in Reference [12].





## 7

## SW Architecture

The SAPC main software components are depicted in Figure 6.

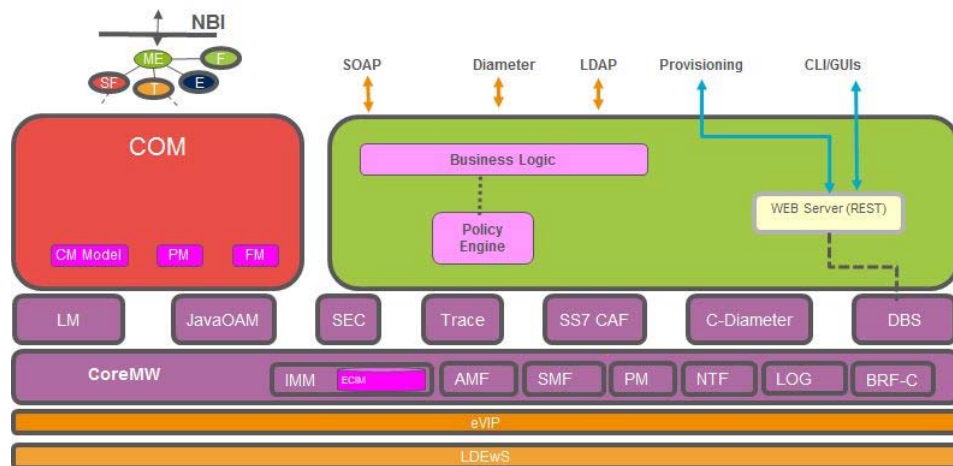


Figure 6 The SAPC SW Architecture

The main architectural software components of the SAPC are the following:

— Protocol interfaces:

- **SOAP:** It provides the SOAP notifications interface.
- **Diameter:** It is the entry point for Diameter-based signalling (for example, Gx).
- **LDAP:** It enables the SAPC interworking with an external SPR.
- **HTTPs:** It is used for the SAPC provisioning by REST resources.

— **Business Logic**

It provides the main core SAPC logic in a protocol independent way.

— **Policy Engine**

This module selects and evaluates the applicable conditions that the business logic needs to consider for making policy decisions.

— **Web Server for REST**

It is the server enabling the REST API provisioning operations.

— **Common Components Framework (Middleware)**

It consists of a set of SW components providing platform capabilities. Such components are provided by Ericsson Component Based Architecture (CBA) platform. The components used are listed below:

- LDE: It is the Linux operating system of the CBA platform.
- eVIP: It provides virtual IP and load balancing.
- CoreMw: It gives a programming framework towards the platform operating system. That framework provides tools for implementing Configuration storage (IMM), Performance Management (PM), High Availability (AMF), SW Management (SMF), Notifications and Alarms (NTF), Logging (LOG), and Backup and Restore (BRF).
- Trace: It contains the tracing framework used for troubleshooting purposes.
- JavaOAM: It is used for executing Java® based SW.
- COM: It implements the Ericsson Common Information Model (ECIM), providing NETCONF interface for Operation and Maintenance purposes.
- DBS: It provides the in-memory database for managing both SPR and state information.
- C-Diameter: It provides the Diameter stack.
- SS7 CAF: It provides the Stream Control Transmission Protocol (SCTP) transport connectivity.
- SEC: It is used for OAM passwords encryption.
- LM: It controls the status of the license keys associated with the commercial licensees.



## 8 Operation and Maintenance

### 8.1 Middleware

The operation, maintenance, deployment, and handling functional area of the SAPC provides cost efficient handling and management support of the node. It covers all phases from factory configuration to normal operation.

The Middleware implements a comprehensive set of network management standards from 3GPP and IETF for communicating network management purposes. Specifically, SNMP, NETCONF, and SOAP are supported.

The SAPC CBA Middleware provides a component called COM that implements a manager-agent architecture. It allows easy integration of the SAPC with OSS and BSS in standards-compliant manner.

### 8.2 Provisioning

The SAPC offers a REST API for provisioning of subscriber and service-related data. This interface handles the creation, retrieval, update, and deletion of the SAPC subscribers, subscriber groups, services, and policies information.

### 8.3 Node Configuration

The SAPC offers a NETCONF interface for configuration of node management data. This interface handles the creation, retrieval, update, and deletion of the SAPC management information. Configuration commands can be logged.

### 8.4 Fault Management

The SAPC provides an SNMP interface for fault management functions to detect and isolate the improper behavior within the node.

### 8.5 Performance Management

The SAPC offers a Performance Management solution that collects and reports the data relevant to the application. The file formatting provided by the SAPC complies with Reference [12]. The supported file formatting is XML.



## 8.6 Logging

The SAPC maintains an application Log, responsible for logging the events related with the SAPC operation (for example, data consumption limit for the subscriber has been reached).

## 8.7 Backup and Restore

Data handled by the SAPC can be persistently stored through the Backup and Restore function. Backups can be ordered manually and either scheduled for specific dates or periodically. Backups can be restored manually.

## 8.8 Troubleshooting

The SAPC provides a state-of-the-art tracing tool for troubleshooting purposes. It is based on Common Trace Format (CTF), and enables the definition of up to 14 tracing levels. It allows tracing on hierarchies of logical trace domains and single trace events.

In addition, it is possible to make tracing by filters (for example, tracing per UE, or Gx message, or IP address).

## 8.9 License Management

The SAPC controls the activation of the commercial licenses by SW keys. For such purpose, the SAPC uses LM Common Component.



## 9 Installation and Deployment

The SAPC can be deployed as VNF, or installed as PNF in a specific HW (Ericsson BSP 8100, or Ericsson NSP 6.1).

**Note:** Although PNF deployment in Commercial of the Self (COTS) is technically possible, the SAPC 1 does not include any specific documentation or scripts for PNF installation on COTS.

### 9.1 PNF Deployment

#### 9.1.1 **BSP 8100**

The SAPC 1 can be installed on BSP 8100 HW. At least BPS 8100 R10B must be used.

See Reference [3] for further details on BSP 8100 HW.

#### 9.1.2 **NSP 6.1**

The SAPC 1 can be installed on NSP 6.1 HW. The BIOS version must be R11A or higher.

See Reference [4] for further details on NSP 6.1

### 9.2 VNF Deployment

The SAPC 1 can be deployed as VNF on top of either OpenStack® or VMware® based NFVI. For detailed information, see Reference [1].





# Glossary

**3GPP**

3rd Generation Partnership Project

**AAA**

Authentication, Authorization and Accounting

**ADC**

Application Detection and Control

**AF**

Application Function

**AMF**

Availability Management Framework

**APN-AMBR**

Access Point Name - Aggregated Maximum Bit Rate

**ARP**

Allocation Retention Priority

**AVP**

Attribute-Value Pair

**BBERF**

Bearer Binding and Event Reporting Function

**BBF**

Broadband Forum

**BRAS**

Broadband Remote Access Server

**BSS**

Business Support Systems

**CBA**

Component Based Architecture

**CCA**

Credit Control Answer

**CCR**

Credit Control Request

**CLI**

Command-Line Interface

**COTS**

Commercial of the Self

**CS**

Circuit Switch

**CTF**

Common Trace Format

**CUDB**

Centralized User Database

**DB**

Database

**DPI**

Deep Packet Inspection

**E-UTRAN**

Evolved Universal Mobile Telecommunications System Terrestrial Radio Access Network

**ECIM**

Ericsson Common Information Model

**EPC**

Evolved Packet Core

**EPS**

Evolved Packet System

**ePDG**

Evolved Packet Data Gateway

**EPG**

Evolved Packet Gateway

**ETSI**

European Telecommunications Standards Institute

**FMC**

Fixed-Mobile Convergence

**FQDN**

Fully-Qualified Domain Name

**GBR**

Guaranteed Bit Rate

**GPRS**

General Packet Radio Service

**GSM**

Global System for Mobile Communications

**HTTP**

Hypertext Transfer Protocol

**HW**

Hardware

**IETF**

Internet Engineering Task Force

**IMM**

Information Management Model

**IMS**

IP Multimedia Subsystem

**IP**

Internet Protocol

**IP-CAN**

IP Connectivity Access Network

**IPoE**

IP over Ethernet

**IPTV**

IP Television

**LAN**

Local Area Network

**LDAP**

Lightweight Directory Access Protocol

**LOG**

Logging

**LTE**

Long Term Evolution

**MBR**

Maximum Bit Rate

**MIB**

Management Information Base

**MS-BNG**

Multi Service-Broadband Network Gateway

**MSISDN**

Mobile Subscriber ISDN Number

**NAI**

Network Access Identifier

**NAT**

Network Address Translation

**NETCONF**

Network Configuration Protocol

**NetLoc**

Network Location

**NFV**

Network Functions Virtualization

**NFVI**

Network Functions Virtualization Infrastructure

**NIC**

Network Interface Card

**NMS**

Network Management System

**NTF**

Notifications Framework

**OAM**

Operation and Maintenance

**OCS**

Online Charging System

**OFCS**

Offline Charging System

**OSS**

Operations Support Systems

**OVF**

Open Virtualization Format

**P-CSCF**

Proxy Call Session Control Function





<b>PCAP</b> Packet Capture	<b>RAT</b> Radio Access Type
<b>PCC</b> Policy and Charging Control	<b>REST</b> Representational State Transfer
<b>PCEF</b> Policy and Charging Enforcement Function	<b>RG</b> Residential Gateway
<b>PCRF</b> Policy and Charging Rules Function	<b>SCTP</b> Stream Control Transmission Protocol
<b>PDN</b> Packet Data Networks	<b>SDF</b> Service Data Flow
<b>PDN-GW</b> Packet Data Networks Gateway	<b>SDN</b> Software Defined Network
<b>PDP</b> Policy Decision Point	<b>SDP</b> Session Description Protocol
<b>PEP</b> Policy Enforcement Point	<b>SIM</b> Subscriber Identity Module
<b>PLMN</b> Public Land Mobile Network	<b>SMF</b> Software Management Framework
<b>PM</b> Performance Management	<b>SMPP</b> Short Message Peer-to-Peer
<b>PNF</b> Physical Node Function	<b>SMS</b> Short Messaging System
<b>PPP</b> Point-to-Point Protocol	<b>SMSC</b> SMS Center
<b>PRA</b> Presence Reporting Area	<b>SNMP</b> Simple Network Management Protocol
<b>PS</b> Packet Switch	<b>SOAP</b> Simple Object Access Protocol
<b>PSTN</b> Public Switched Telephone Network	<b>SPID</b> Subscriber Profile ID
<b>QCI</b> QoS Class Identifier	<b>SPR</b> Subscription Profile Repository
<b>QoS</b> Quality of Service	<b>SRVCC</b> Single Radio Voice Call Continuity
<b>RAR</b> Reauthorization Request	<b>SW</b> Software

**TDF**

Traffic Detection Function

**TLS**

Transport Layer Security

**TTLS**

Tunneled Transport Layer Security

**UE**

User Equipment

**URL**

Uniform Resource Locator

**UTRAN**

Universal Mobile Telecommunications System  
Terrestrial Radio Access Network

**VAS**

Value-Added Services

**VNF**

Virtualized Network Function

**VoLTE**

Voice over Long Term Evolution

**SAPC**

Ericsson Service-Aware Policy Controller

**WLAN**

Wireless Local Area Network

**WMG**

Wi-Fi Mobility Gateway

**WSDL**

Web Services Description Language

**XML**

Extensible Markup Language



## Reference List

### Ericsson Documents

- [1] Technical Product Description: Virtual SAPC 1 Technical Product Description, 1/221 02-FGC 101 3390/1V Uen A
- [2] Ericsson Alarm MIB, Interwork Description, 1/155 19-APR 901 0443/1
- [3] BSP Technical Product Description, 221 02-FGC 101 2255 Uen D
- [4] NSP 6.1 HW Description, 1/1551-APR 901 0461/1 Uen M

### Standards

- [5] Policy and charging control architecture, 3GPP TS 23.203 v14.4.0
- [6] IMS Restoration Procedures, 3GPP TS 23.380 v14.1.0
- [7] Policy and Charging Control (PCC); Reference points, 3GPP TS 29.212 v14.4.0
- [8] Policy and charging control over Rx reference point, 3GPP TS 29.214 v14.4.0
- [9] Policy and charging control: Spending limit reporting over Sy reference point, 3GPP TS 29.219 v14.2.0
- [10] User Data Convergence (UDC); User data repository access protocol over the Ud interface; Stage 3, 3GPP TS 29.335 v14.0.0
- [11] Telecommunication management; Subscriber and equipment trace; Trace data definition and management, 3GPP TS 32.423 v14.0.0
- [12] Telecommunication management; Performance measurement; eXtensible Markup Language (XML) file format definition, 3GPP TS 32.435 v14.0.0
- [13] Broadband Policy Control Framework (BPCF), BBF TR-134 Corrigendum 1
- [14] Policy Convergence for Next Generation Fixed and 3GPP Wireless Networks, BBF TR-300 Issue 1
- [15] Network Functions Virtualisation; Architectural Framework, ETSI GS NFV 002 v1.1.1
- [16] Digital Exchange Performance Design Objectives, ITU-T Q.543
- [17] Diameter Credit-Control Application, RFC 4006
- [18] Network Configuration Protocol (NETCONF), RFC 6241



[19] Diameter Base Protocol, RFC 6733