

Statement of Compliance towards Broadband Forum Technical Report TR-134

Ericsson Service-Aware Policy Controller

STATEMENT OF COMPLIANCE

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.

Introduction

This document describes to what extent Ericsson Service-Aware Policy Controller (SAPC) implementation conforms with the Broadband Forum Technical Report (TR-134) standard Reference [1] with the exemptions or additions stated in this document.

Revision Information

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

General Considerations

This document is structured following the chapters of the Broadband Forum Technical Report (TR-134).

The following terms explain the columns in the fill-in tables in the document:

Qualifier	Defines whether the implementation of a certain requirement is required (MUST/MUST NOT), recommended (SHOULD/SHOULD NOT) or optional (MAY).
Compliance	Defines whether the implementation complies with the specified section in TR-134.
Comment	It may contain additional information.
No requirement (NR)	The TR statement contains general information for the understanding of other statements not applicable to SAPC (the statements may be applicable for other nodes).

One of the following statements (with the associated interpretation) is given to each of the requirements of the Technical Report:

Not compliant (NC)	The TR statement is not fulfilled.
Compliant (C)	All of the TR statements are fulfilled
Partially compliant (PC)	Not completely all of the TR statements are fulfilled, the exceptions are described.



Contents

1	Purpose and scope	1
2	References and Terminology	1
3	Technical Report Impact	1
4	Business Requirements for Policy	1
4.1	Session-Based Policies	1
4.2	Wholesale Sessions	3
4.3	Application Admission Control	3
4.4	Session Resource Request initiation sources	5
4.5	Bandwidth	6
4.6	QoS	6
4.7	Security	7
4.8	IPv6 Support	7
4.9	Network Threat Detection	7
4.10	Multicast	7
4.11	Routing	8
4.12	Auditing, Service monitoring and Accounting	8
4.13	Charging	9
4.14	Deep Packet Inspection	9
5	Use Cases	9
6	Functional Architecture elements	10
6.1	BPC Framework Functional Architecture	10
6.2	Policy Enforcement Point (PEP)	12
6.3	Policy Decision Point (PDP)	12
6.4	Admission Control Function	13
6.5	Repository Function	13
6.6	Security Proxy/Gateway function	13
6.7	Application Function (AF)	13
6.8	AAA Server Function	14
6.9	BPC Framework Policy Control Framework Interfaces	14
6.10	BPC Framework PCF Deployment Functional Architecture Mapping onto TR-101 Functional Architecture	14



6.11	Informative AAA implementation examples	14
6.12	Informative PEP/PDP implementation examples	14
7	Policy Information Flows	14
7.1	Information Flow Objectives	14
8	Annex I (Informative). Relationship to other Broadband Technical Reports	20
9	Annex II (Informative). Relationships with other Policy Control Standards	21
10	Annex III (Informative). Policy Information Objects Definitions	21
	Reference List	23



1 Purpose and scope

No requirements.

2 References and Terminology

No requirements.

3 Technical Report Impact

No requirements.

4 Business Requirements for Policy

No requirements.

Note: The Statement of Compliance towards the business requirements for policy is done considering the SAPC PDP functionality.

4.1 Session-Based Policies

Table 1 Session-Based Policies

Text	Qualifier	Compliance	Comment
R-1. The BPC Framework MUST support policies that are associated with the following session types: access, L2, subscriber, and application sessions.	MUST	C	L2 policies are not supported in SAPC.

Text	Qualifier	Compliance	Comment
R-2. The BPC Framework MUST support interaction with session establishment.	MUST	C	SAPC interacts with session establishment in Gx scenarios.
R-3. The BPC Framework MUST support Policy Change requests from Applications after session establishment.	MUST	C	Changes in policies defined per subscriber and service can be done using a REST interface.
R-4. The BPC Framework MUST support policies that apply to individual sessions.	MUST	C	Considering that one subscriber session has only one individual session.
R-5. The BPC Framework MUST support policy evaluation that is triggered by a change in state of a session.	MUST	C	
R-6. The BPC Framework MUST support policies that apply to aggregates of subscriber sessions sharing logical interfaces, and/or layer 2 interfaces, and/or a physical access e.g. DSL loop.	MUST	C	Subscribers sharing the same logical interfaces are behind the same RG. And they are managed as a single L3 IP session.
R-7. The BPC Framework MUST support policies that apply to logical interface/layer 2 interface based on individual subscriber session policies when multiple subscriber sessions share a logical interface, and/or layer 2 interfaces, and/or a physical access e.g. DSL loop.	MUST	C	Layer 2 policies can be enforced with just a single Gx response with a policy id. The PEP is the responsible for doing the actual control.



4.2 Wholesale Sessions

Table 2 Wholesale Sessions

Text	Qualifier	Compliance	Comment
R-8. The BPC Framework MUST support the application of policies to L2 access sessions.	MUST	C	See comment on R-7.
R-9. The BPC Framework MUST support the application of policies to subscriber sessions.	MUST	C	
R-10. The BPC Framework MUST support ASP/NSP application requests for policy changes and resources from the network, without any knowledge of network topology and network state.	MUST	NC	No ASP/NSP application requests are supported.
R-11. The BPC Framework MUST support ASP/NSP applications querying the status of policy changes and resource requests without any knowledge of network topology and network state.	MUST	NC	No ASP/NSP application requests are supported.
R-12. The BPC Framework MUST allow secure and controlled access by NSPs and ASPs to the Policy Control infrastructure	MUST	NC	No ASP/NSP application requests are supported.
R-13. The BPC Framework MUST support policies for traffic associated with a specific A10-NSP interface and the associated backhaul tunnel.	MUST	NC	No ASP/NSP application requests are supported.

4.3 Application Admission Control

Table 3 Application Admission Control

Text	Qualifier	Compliance	Comment
R-14. The BPC Framework MUST support policies that control traffic flows.	MUST	C	

Text	Qualifier	Compliance	Comment
R-15. The BPC Framework MUST support network capacity admission control.	MUST	NA	Admission control is not provided by SAPC. It is the PEP responsibility.
R-16. The BPC Framework MUST support pre-emption of existing reservations based on a priority scheme.	MUST	NA	Admission control is not provided by SAPC. It is the PEP responsibility.
R-17. The BPC Framework MUST support business authorization of application requests (time of day, group membership, etc.)	MUST	C	Changes in policies defined per subscriber and service can be done using a REST interface.
R-18. The BPC Framework MUST support activation of another policy as a condition of a first policy (e.g. in order to authorize a particular media flow, some charging policy must be activated). This is also known as nested policies.	MUST	NA	Admission control is not provided by SAPC. It is the PEP responsibility.
R-19. The BPC Framework MUST support combining the following information when making admission control decisions for a new session: <ul style="list-style-type: none"> • application requirements (e.g. bandwidth, QoS, etc.) • available bandwidth for the subscriber based on the subscribers subscription • current bandwidth usage • network topology • the available network capacity 	MUST	NA	Admission control is not provided by SAPC. It is the PEP responsibility.



Text	Qualifier	Compliance	Comment
R-20. The BPC Framework MUST support a reservation model based on a provisioned, static view of the topology and bandwidth.	MUST	NA	Admission control is not provided by SAPC. It is the PEP responsibility.
R-21. The BPC Framework MUST support a reservation model based on a dynamically learned view of the topology and bandwidth.	MUST	NA	Admission control is not provided by SAPC. It is the PEP responsibility.
R-22. The BPC Framework MUST support bandwidth reservations in networks which have alternate traffic delivery paths (multipath).	MUST	NA	Admission control is not provided by SAPC. It is the PEP responsibility.
R-23. The BPC Framework MUST support automatic re-establishment of bandwidth reservations impacted by network failure.	MUST	NA	Admission control is not provided by SAPC. It is the PEP responsibility.

4.4 Session Resource Request initiation sources

Table 4 Session Resource Request initiation sources

Text	Qualifier	Compliance	Comment
R-24. The BPC Framework MUST supports any application type requesting policy changes and/or resources from the network.	MUST	C	Changes in policies defined per subscriber and service can be done using a REST interface.
R-25. The BPC Framework MUST be able to consider the status of available network resources.	MUST	NA	Admission control information is not available SAPC.

Text	Qualifier	Compliance	Comment
R-26. The BPC Framework MUST support taking network events into account (e.g. events from Network elements).	MUST	C	
R-27. The BPC Framework MUST support time of day and duration based policies and policy changes	MUST	C	

4.5 Bandwidth

Table 5 Bandwidth

Text	Qualifier	Compliance	Comment
R-28. The BPC Framework MUST support policies that control bandwidth allocation in TR-059[2], TR-101[5] and WT-145[23] based access network resources.	MUST	PC	Varying bandwidth rates are provided for subscribers, per IP session and per service. RG is not supported as Policy Enforcement point.

4.6 QoS

Table 6 QoS

Text	Qualifier	Compliance	Comment
R-29. The BPC Framework MUST support policies that control QoS in TR-059[2], TR-101[5] and WT-145[23] based access networks.	MUST	PC	QoS Control is provided for subscribers, per IP-CAN session and per service. RG is not supported as Policy Enforcement point.



4.7 Security

No requirement.

4.8 IPv6 Support

Table 7 IPv6 Support

Text	Qualifier	Compliance	Comment
R-30. The BPC Framework MUST support the use of IPv6 for communication between the various policy related network elements.	MUST	NC	
R-31. The BPC Framework MUST support the use of the IPv6 header fields for the purposes of flow identification and policy enforcement.	MUST	C	
R-32. The BPC Framework MUST support the use of IPv6 address management and allocation in the policy related nodes	MUST	C	

4.9 Network Threat Detection

Table 8 Network Threat Detection

Text	Qualifier	Compliance	Comment
R-33. The BPC Framework MUST support policies that control response to any type of network intrusion event.	MUST	PC	Supported the redirection or filtering of subscriber traffic.

4.10 Multicast

Table 9 Multicast

Text	Qualifier	Compliance	Comment
R-34. The BPC Framework MUST allow control over multicast replication for individual multicast groups.	NR		

4.11 Routing

Table 10 Routing

Text	Qualifier	Compliance	Comment
R-35. The BPC Framework MUST support controlling routing policies for individual access sessions.	MUST	C	Routing policies are supported per subscriber session.

4.12 Auditing, Service monitoring and Accounting

Table 11 Auditing, Service monitoring and Accounting

Text	Qualifier	Compliance	Comment
R-36. The BPC Framework MUST support logging of all transactions for the purposes of troubleshooting and security.	MUST	PC	Only logged transactions related to errors, warnings, and atypical situations.
R-37. The BPC Framework MUST support the generation of Accounting information for the purposes of billing and non-repudiation	NR		
R-38. The BPC Framework MUST support the exchange of RADIUS and Diameter accounting messages with the AAA Server or network elements like the BNG.	MUST	NC	
R-39. The BPC Framework MUST support the use of AAA RADIUS and Diameter attributes in the accounting messages for policy decisions.	MUST	NC	



4.13 Charging

Table 12 Charging

Text	Qualifier	Compliance	Comment
R-40. The BPC Framework MUST support the use of the charging models defined in TR-058[1], TR-102[6] and TR-144[8].	MUST	C	
R-41. The BPC Framework MUST support the use of charging models for the use cases in Section 5.4	MUST	C	
R-42. The BPC Framework MUST support the identification of charging rules for the various charging models.	MUST	C	Supported by Gx interface.

4.14 Deep Packet Inspection

Table 13 Deep Packet Inspection

Text	Qualifier	Compliance	Comment
R-43. The BPC Framework MUST support interaction between DPI detection and enforcement functions.	NR		
R-44. The BPC Framework MUST support the use of L4-7 classifiers in defining traffic policy.	MUST	C	

5 Use Cases

No requirements.

6 Functional Architecture elements

6.1 BPC Framework Functional Architecture

Table 14 BPC Framework Functional Architecture

Text	Qualifier	Compliance	Comment
R-45. The BPC Framework MUST support architectures in which the PDP functionality can be centralized, or distributed in various physical and nodal locations.	MUST	C	
R-46. The BPC Framework MUST support a centralized PDP functionality which sends policy enforcement commands to multiple Policy Enforcement Points.	MUST	C	
R-47. The PDPs MUST be able to interact to support end-to-end control for the purposes scaling and or spanning different network administration boundaries.	MUST	NC	
R-48. The BPC Framework MUST support multiple PDPs, where each PDP is responsible for making policy decisions for a predefined network domain (geographical, administrative wholesale, or retail).	MUST	C	
R-49. The BPC Framework MUST support multiple PDPs, where each PDP is responsible for making policy decisions for different PEP types or PEP functions.	MUST	C	
R-50. The BPC Framework MUST support the acceptance or rejection of requested policy changes.	MUST	C	



Text	Qualifier	Compliance	Comment
R-51. The BPC Framework MUST support a single policy request being able to configure multiple individual sessions.	MUST	C	An RG in bridge mode, is handling a single IP session. This IP session manages several subscribers sessions. So SAPC, managing one single IP session, is managing several subscriber sessions
R-52. The BPC Framework MUST support a mechanism for communicating policy requests and decisions that is secure against spoofing, hijacking and DoS attacks.	MUST	C	Any user passwords are sent encrypted, to eliminate the possibility that someone snooping on an unsecured network could determine a user's password.
R-53. The PDP logical entity SHOULD be able to interact with an Application Server to allow dynamic real-time changes of policy for both upstream and downstream traffic, e.g. a QoS change.	SHOULD	C	Changes in policies defined per subscriber and service can be done using a REST interface.
R-54. The PDP MUST be able to communicate with the NMS/OSS, AAA Server, AF, Repository and other PDP(s) to facilitate making policy decisions.	MUST	PC	AAA is not supported.

6.2 Policy Enforcement Point (PEP)

Table 15 Policy Enforcement Point (PEP)

Text	Qualifier	Compliance	Comment
R-55. The BPC Framework MUST support policy enforcement for both downstream and upstream traffic.	MUST	C	
R-56. The PEP logical entity MUST be able to enforce policy for unicast and multicast traffic.	NR		
R-57. The PEP MUST be able to apply policy on Access Sessions, L2 Sessions, Subscriber Sessions and Traffic rule session.	NR		
R-58. The PEP MUST be able to receive policy information from the PDP over the R interface.	NR		
R-59. The PEP MUST be able to request policies from the PDP over the R interface.	NR		
R-60. The PEP MUST be able to be directed to receive/activate/modify/delete policies from the NMS/OSS over M/Q interface	NR		
R-61. The PEP MUST be able to be directed to receive/activate/modify/delete policies from AAA Server over the B interface.	NR		

6.3 Policy Decision Point (PDP)

Table 16 Policy Decision Point (PDP)

Text	Qualifier	Compliance	Comment
R-62. A PDP MUST be able to connect with another PDP(s) over the I interface. Examples of where this might be required include the case where multiple domains are involved, or when functionality is delegated from one PDP to another.	MUST	NC	



Text	Qualifier	Compliance	Comment
R-63. The PDP MUST be able to make policy decisions for Access Sessions, L2 Sessions, Subscriber Sessions and Traffic Rule session.	MUST	C	
R-64. The PDP MUST be able to provide policy decisions for multiple PEPs.	MUST	C	
R-65. The PDP SHOULD be able to retrieve subscriber information from a Repository or AAA Server function.	SHOULD	C	
R-66. The PDP SHOULD be able to install/activate/deactivate/modify/remove Policies in the PEP, and allow dynamic changes of policy for both upstream and downstream traffic.	SHOULD	C	

6.4 Admission Control Function

Table 17 Admission Control Function

Text	Qualifier	Compliance	Comment
R-67. The ACF MUST be able to make admission decisions based upon network resources and business policies.	MUST	NC	Admission control is not supported.

6.5 Repository Function

No requirement.

6.6 Security Proxy/Gateway function

No requirement.

6.7 Application Function (AF)

No requirement.

6.8 AAA Server Function

No requirement.

6.9 BPC Framework Policy Control Framework Interfaces

No requirement.

6.10 BPC Framework PCF Deployment Functional Architecture Mapping onto TR-101 Functional Architecture

No requirement.

6.11 Informative AAA implementation examples

No requirement.

6.12 Informative PEP/PDP implementation examples

No requirement.

7 Policy Information Flows

No requirements.

7.1 Information Flow Objectives

No requirement.

7.1.1 Policy Information Flow Structure

No requirements

7.1.2 Network Logical Functions

No requirements



7.1.3

Policy Information Model Elements and requirements

Table 18 Policy Information Model Elements and requirements

Text	Qualifier	Compliance	Comment
R-68. The PDP MUST be able to add policy rules in the PEP via the R interface.	MUST	C	
R-69. The PDP MUST be able to modify policy rules in the PEP via the R interface.	MUST	C	
R-70. The PDP MUST be able to remove policy rules in the PEP via the R interface.	MUST	C	
R-71. The PDP MUST be able to activate policy rules in the PEP via the R interface.	MUST	C	
R-72. The PDP MUST be able to deactivate policy rules in the PEP via the R interface.	MUST	C	
R-73. The PEP MUST be able to respond to policy rules received from the PDP via the R interface indicating the result of the request.	MUST	C	
R-74. The PEP MUST be able to request policy rules from the PDP via the R interface.	MUST	C	
R-75. The communication between the PDP and the PEP MUST be reliable.	MUST	C	
R-76. The PDP MUST be able to respond to a policy request from the PEP via the R reference point accepting or rejecting the request.	MUST	C	Only supported with Gx interface.
R-77. The protocol design for the R interface MUST support the exchange of Vendor-Specific Information.	MUST	C	

Text	Qualifier	Compliance	Comment
<p>R-78. The PDP SHOULD be able to submit the following message parameters to the PEP:</p> <ul style="list-style-type: none"> - Policy rule-set upon Subscriber session establishment - Policy rule update during Subscriber session, upon session event and on termination - Request for notification of specific events 	SHOULD	C	Policy rule update on termination is not supported.
<p>R-79. PDP decisions MUST be able to be based on:</p> <p>Information obtained from the AF via the E/G interfaces (e.g. the session, media and subscriber related information).</p> <p>Information obtained from the PEP via the R interface (e.g. bearer attributes, request type and subscriber related information).</p> <p>Information obtained from the AAA Server via the A interface</p> <p>Information obtained from another PDP via the I interface.</p> <p>Information obtained from the repository via the C interface (e.g. subscriber and service related data)</p>	MUST	PC	<p>Communication with another PDP is not supported.</p> <p>Information obtained from the AAA Server is not supported.</p>

7.1.4 Policy Information Model Messages between PDP and PEP over R Interface

No requirements.



7.1.4.1

Abstract Policy Information Elements – PDP -> PEP direction parameters submitted for policy

Table 19 PDP to PEP Direction Parameters

Text	Qualifier	Compliance	Comment
PDP ID	SHOULD	C	
Session ID	SHOULD	C	Supported Access session ID.
IP Address	SHOULD	C	
Policy Rule Request	SHOULD	C	
Policy lifetime	SHOULD	C	
Policy Rule Response	SHOULD	C	
QoS Parameter	SHOULD	C	
Policy Rule ID	SHOULD	C	
Policy Rule Group ID	SHOULD	C	
Policy Rule Precedence	SHOULD	C	
Traffic actions	SHOULD	C	
Application action	SHOULD	C	As example HTTP-Redirect .
Traffic flow filter (IP 5-tuple)	SHOULD	C	
Multicast ACL	SHOULD	NC	
Quota	SHOULD	C	
Charging Mode	SHOULD	C	
Rating-Group	SHOULD	C	
Charging-Correlation ID	SHOULD	C	
Policy Rule	SHOULD	C	
Policy Rule parameters	SHOULD	C	
Vendor-Id	SHOULD	NC	
Event Trigger	SHOULD	C	
Default-Access Profile	SHOULD	C	
Logical access ID	SHOULD	NC	
Physical Access ID	SHOULD	NC	
Globally Unique IP address	SHOULD	C	
Subscriber ID	SHOULD	NC	

Text	Qualifier	Compliance	Comment
HdrIpVersion	SHOULD	C	
HdrSrcAddress	SHOULD	C	
HdrSrcAddressEndOfRange	SHOULD	C	
HdrSrcMask	SHOULD	C	
HdrDestAddress	SHOULD	C	
HdrDestAddressEndOfRange	SHOULD	C	
HdrDestMask	SHOULD	C	
HdrProtocolID	SHOULD	C	
HdrSrcPortStart	SHOULD	C	
HdrSrcPortEnd	SHOULD	C	
HdrDestPortStart	SHOULD	C	
HdrDestPortEnd	SHOULD	C	
HdrDSCP	SHOULD	C	
HdrFlowLabel	SHOULD	C	
QoSInformation	SHOULD	C	
QoS Information Identifier	SHOULD	C	
8021 Source MAC address	SHOULD	NC	
8021 Destination MAC Address	SHOULD	NC	
8021 Protocol ID	SHOULD	NC	
8021 Priority Value	SHOULD	NC	
8021 VLAN ID	SHOULD	NC	

7.1.4.2 Abstract Policy Information Elements – PEP -> PDP direction parameters submitted during subscriber login

R-76. The PEP SHOULD be able to submit the following message parameters to the PDP during access session login and PEP initiated session modification.

Table 20 PEP to PDP direction parameters during subscriber login

Text	Qualifier	Compliance	Comment
Vendor-Id	SHOULD	C	Can be used to decide the policies for the subscriber.



Text	Qualifier	Compliance	Comment
Firmware revision	SHOULD	C	Can be used to decide the policies for the subscriber.
Policy Rule ID	SHOULD	C	
Subscriber ID	SHOULD	C	Can be used to decide the policies for the subscriber.
IP Address	SHOULD	C	Can be used to decide the policies for the subscriber.
Application / Traffic signature	SHOULD	C	
Traffic flow filter (IP 5-tuple)	SHOULD	C	
Application/ traffic signature /session ID	SHOULD	C	
Policy Rule Request	SHOULD	C	
Policy Rule Response	SHOULD	C	
Termination-Cause	SHOULD	C	
Policy lifetime	SHOULD	NC	
QoS Parameters	SHOULD	C	
Session modification trigger	SHOULD	C	
Default-Access Profile	SHOULD	NC	
Interface name	SHOULD	C	
MAC Address	SHOULD	C	If the MAC Address is the content of the Subscription-Id value in Gx interface.
Access Loop Characteristics	SHOULD	NC	
Access Session ID	SHOULD	C	
L2 Session ID	SHOULD	C	
Subscriber Session Id	SHOULD	C	
Service Session Id	SHOULD	C	
Application Session Id	SHOULD	C	

- 7.1.4.3 Abstract Policy Information Elements – PEP -> PDP direction parameters submitted for Access Port Configuration**
- No requirement.
- 7.1.4.4 Abstract Policy Information Elements – Access Node -> BRAS/BNG direction parameters submitted for Access Resource Reporting**
- No requirement.
- 7.1.4.5 Abstract Policy Information Elements – BRAS/BNG -> AAA direction parameters submitted for Access Resource Reporting**
- No requirement.
- 7.1.4.6 Abstract Policy Information Elements – AAA -> PDP direction parameters submitted for policy**
- No requirement.
- 7.1.4.7 Abstract Policy Information Elements – PDP -> AAA direction parameters submitted for policy**
- No requirement.
- 7.1.5 Vendor proprietary extensions**
- No requirement.

8 Annex I (Informative). Relationship to other Broadband Technical Reports

No requirements.



9 Annex II (Informative). Relationships with other Policy Control Standards

No requirements.

10 Annex III (Informative). Policy Information Objects Definitions

No requirements.





Reference List

Standard

- [1] TR-134 Broadband Policy Control Framework (BPCF), Issue: 1 Corrigendum
1 Issue date: January 2013