

# Sd Interface Description

Ericsson Service-Aware Policy Controller

Interwork Description

## **Copyright**

© Ericsson AB 2018. 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](#).



# Contents

<b>1</b>	<b>Sd Interface Overview</b>	<b>1</b>
1.1	Document Content Conventions	1
<b>2</b>	<b>Sd Interface Message Exchange</b>	<b>3</b>
<b>3</b>	<b>Diameter Base Protocol Messages</b>	<b>4</b>
3.1	Sd Capability Negotiation	4
3.2	Device Watchdog	5
3.3	Disconnect Peer	5
<b>4</b>	<b>Sd Interface Message Format</b>	<b>7</b>
4.1	Sd TDF Session Request	7
4.2	Sd TDF Session Answer	8
4.3	Sd Credit Control Request	8
4.4	Sd Credit Control Answer	9
4.5	Sd Re-Authorization Request	9
4.6	Sd Re-Authorization Answer	10
<b>5</b>	<b>Sd Interface AVPs</b>	<b>11</b>
<b>6</b>	<b>Sd Error Handling</b>	<b>12</b>
6.1	Sd Protocol Errors	12
6.2	Sd Application Errors	12
<b>7</b>	<b>Reference List</b>	<b>15</b>





# 1 Sd Interface Overview

This document describes the standard 3GPP Sd interface used between a Policy and Charging Rules Function (PCRF) and the Traffic Detection Function (TDF). The TDF is a functional entity that performs application detection and reports the detected application and its service data flow description, if deducible, to the PCRF.

The 3GPP Sd interface is built over the Diameter Base Protocol IETF RFC 6733. The Ericsson Service-Aware Policy Controller (SAPC) supports the 3GPP Sd interface from Release 11 onwards.

For detailed information about compliance to 3GPP standards, refer to the corresponding Statement of Compliance documents.

## 1.1 Document Content Conventions

This document contains the specific details supported by the SAPC implementation.

This document does not repeat information that can be found in 3GPP Technical Specifications or in the Diameter Base Protocol RFC.

For detailed information about Statement of Compliance (SoC) towards different 3GPP Release versions (for example Rel13, Rel14 and so on), see the corresponding SoCs documents.

Each message is described with the list of parameters (AVPs) exchanged between the Diameter peers.

- For **incoming** messages received in the SAPC, this document only indicates the AVPs that the SAPC reads to perform the corresponding business logic or evaluation inside policy conditions.

The SAPC can receive other AVPs (but does not use them) that can be found in 3GPP Technical Specifications, but are not stated in this document. This is possible because the SAPC uses a dictionary that specifies the format of messages and AVPs. The SAPC follows the standard Diameter Base Protocol behavior:

- If the SAPC receives an AVP with the M bit set to 1, and that AVP is not included in the dictionary, the SAPC rejects the message indicating `DIAMETER_AVP_UNSUPPORTED`.
- If the SAPC receives an AVP defined in the dictionary, but with different values in the flag bits, the SAPC rejects the message indicating `DIAMETER_INVALID_AVP_BITS`.



- If the SAPC receives an AVP with the M bit set to 0, and that AVP is not defined in the dictionary, the SAPC does not reject the message, but ignores the AVP value.
- For **outgoing** messages (and AVPs) sent by the SAPC, this document indicates only the AVPs that the SAPC fills.

**Note:** When the SAPC does not support a message or AVP for all 3GPP Release versions, it is explicitly indicated in this document.



## 2 Sd Interface Message Exchange

For an overview of the Sd Diameter message exchange between the Policy and Charging Enforcement Function (PCEF), SAPC, and TDF, see [Figure 1](#):

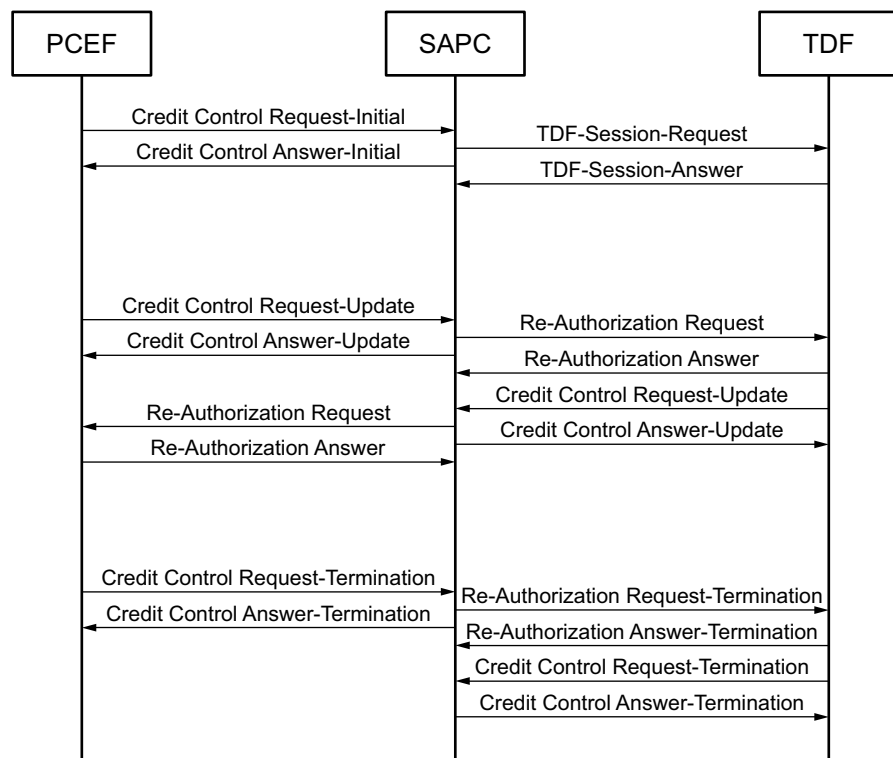


Figure 1 Sd Session Establishment, Modification, and Termination



## 3 Diameter Base Protocol Messages

### 3.1 Sd Capability Negotiation

[Table 1](#) lists the Attribute-Value Pairs (AVPs) that the SAPC sends in a Capabilities Exchange Request (CER) message.

Table 1 CER AVPs

AVP Name	AVP Code	Comment	Reference
[ Firmware-Revision ]	367	-	RFC 6733
1*{ Host-IP-Address }	257	-	RFC 6733
{ Origin-Host }	264	-	RFC 6733
{ Origin-Realm }	296	-	RFC 6733
{ Product-Name }	269	-	RFC 6733
*[ Supported-Vendor-Id ]	265	-	RFC 6733
{ Vendor-Id }	266	The SAPC sets it to value 193 (Ericsson).	RFC 6733
*[ Vendor-Specific- Application-Id ]	260	According to configuration, the SAPC sends the following AVP values:  —Vendor-Id= 10415 (3GPP)  —Auth-Application-Id= 16777303 (3GPP Sd)	RFC 6733

[Table 2](#) lists the AVPs that the SAPC supports in a Capabilities Exchange Answer (CEA) message.

Table 2 CEA AVPs

AVP Name	AVP Code	Comment	Reference
*[ Auth-Application-Id ]	258	-	RFC 6733
[ Error-Message ]	281	-	RFC 6733
[ Failed-AVP ]	279	-	RFC 6733
[ Firmware-Revision ]	267	-	RFC 6733
1*{ Host-IP-Address }	257	-	RFC 6733
{ Origin-Host }	264	-	RFC 6733
{ Origin-Realm }	296	-	RFC 6733
{ Product-Name }	269	-	RFC 6733
{ Result-Code }	268	-	RFC 6733
*[ Supported-Vendor-Id ]	265	-	RFC 6733
{ Vendor-Id }	266	-	RFC 6733
*[ Vendor-Specific- Application-Id ]	260	-	RFC 6733





**Note:** The SAPC does not handle the `Origin-State-Id` AVP in a CEA message.

## 3.2 Device Watchdog

[Table 3](#) lists the AVPs that the SAPC can receive or send in a Device Watchdog Request (DWR) message.

Table 3 DWR AVPs

AVP Name	AVP Code	Comment	Reference
{ <code>Origin-Host</code> }	264	-	RFC 6733
{ <code>Origin-Realm</code> }	296	-	RFC 6733
[ <code>Origin-State-Id</code> ]	278	-	RFC 6733

**Note:** The SAPC does not include an `Origin-State-Id` AVP when it sends an outgoing DWR message.

[Table 4](#) lists the AVPs that the SAPC can receive or send in a Device Watchdog Answer (DWA) message.

Table 4 DWA AVPs

AVP Name	AVP Code	Comment	Reference
[ <code>Error-Message</code> ]	281	-	RFC 6733
[ <code>Failed-AVP</code> ]	279	-	RFC 6733
{ <code>Origin-Host</code> }	264	-	RFC 6733
{ <code>Origin-Realm</code> }	296	-	RFC 6733
[ <code>Origin-State-Id</code> ]	278	-	RFC 6733

**Note:** The SAPC does not include an `Origin-State-Id` AVP when it sends an outgoing DWA message.

## 3.3 Disconnect Peer

[Table 5](#) lists the AVPs that the SAPC supports in a Disconnect Peer Request (DPR) message.

Table 5 DPR AVPs

AVP Name	AVP Code	Comment	Reference
{ <code>Origin-Host</code> }	264	-	RFC 6733
{ <code>Origin-Realm</code> }	296	-	RFC 6733
{ <code>Disconnect-Cause</code> }	273	-	RFC 6733



[Table 6](#) lists the AVPs that the SAPC supports in a Disconnect Peer Answer (DPA) message.

Table 6 DPA AVPs

AVP Name	AVP Code	Comment	Reference
[ Error-Message ]	281	-	RFC 6733
[ Failed-AVP ]	279	-	RFC 6733
{ Origin-Host }	264	-	RFC 6733
{ Origin-Realm }	296	-	RFC 6733
{ Result-Code }	268	-	RFC 6733



## 4 Sd Interface Message Format

### 4.1 Sd TDF Session Request

**Table 7** lists the AVPs that the SAPC sends in a TDF Session Request (TSR) message.

Table 7 TSR AVPs

AVP Name	AVP Code	Comment	Reference
< Session-Id >	263	-	RFC 6733
*[ ADC-Rule-Install ]	1092	This AVP is used to activate ADC rules as instructed by the SAPC. For detailed information, see <a href="#">Table 13</a> .	3GPP TS 29.212
[ Called-Station-Id ]	30	This AVP is received over the Gx interface.	RFC 4005
[ Destination-Host ]	293	-	RFC 6733
{ Destination-Realm }	283	-	RFC 6733
*[ Event-Trigger ]	1006	The SAPC supports the following values: —APPLICATION_START(39) —APPLICATION_STOP(40)	3GPP TS 29.212
[ Framed-IP-Address ] <sup>(1)</sup>	8	-	RFC 4005
[ Framed-Ipv6-Prefix ] <sup>(1)</sup>	97	-	RFC 4005
{ Origin-Host }	264	-	RFC 6733
{ Origin-Realm }	296	-	RFC 6733
[ Origin-State-Id ]	278	-	RFC 6733
*[ Subscription-Id ]	443	When a CCR-I message over Gx is received with one or more instances of the Subscription-Id AVP, the Subscription-Id AVP value includes:  —The traffic identity used in Gx to access the subscriber profile in Subscription-Id-Data AVP  —The same Subscription-Type AVP as the one considered for the Gx traffic	RFC 4006
[ User-Equipment-Info ]	458	The SAPC sends the User-Equipment-Info AVP as received in the CCR-I message over Gx.	RFC 4006
{ Vendor-Specific-Application-Id }	260	The SAPC sends the following AVP values: —Vendor-Id= 10415 (3GPP) —Auth-Application-Id= 16777303 (3GPP Sd)	RFC 6733

(1) Either the Framed-IP-Address or the Framed-Ipv6-Prefix AVP or both are sent depending on the AVPs received over Gx.



## 4.2 Sd TDF Session Answer

[Table 8](#) lists the AVPs that the SAPC supports in a TDF Session Answer (TSA) message.

Table 8 TSA AVPs

AVP Name	AVP Code	Comment	Reference
< Session-Id >	263	-	RFC 6733
[ Experimental-Result ]	297	-	RFC 6733
[ Failed-AVP ]	279	-	RFC 6733
{ Origin-Host }	264	-	RFC 6733
{ Origin-Realm }	296	-	RFC 6733
[ Origin-State-Id ]	278	-	RFC 6733
[ Result-Code ]	268	-	RFC 6733
{ Vendor-Specific-Application-Id }	260	The SAPC receives the following AVP values: —Vendor-Id= 10415 (3GPP) —Auth-Application-Id= 16777303 (3GPP Sd)	RFC 6733

## 4.3 Sd Credit Control Request

[Table 9](#) lists the AVPs that the SAPC supports in a Credit Control Request (CCR) message.

Table 9 CCR AVPs

AVP Name	AVP Code	Comment	Reference
< Session-Id >	263	-	RFC 6733
*[ Application-Detection-Information ] <sup>(1)</sup>	1098	The SAPC supports the following AVPs: —{TDF-Application-Identifier} —[TDF-Application-Instance-Identifier] —*[Flow-Information]	3GPP TS 29.212
{ Auth-Application-Id }	258	-	3GPP TS 29.212
{ CC-Request-Number }	415	-	RFC 4006
{ CC-Request-Type }	416	-	RFC 4006
[ Destination-Host ]	293	-	RFC 6733
{ Destination-Realm }	283	-	RFC 6733
*[ Event-Trigger ]	1006	The SAPC supports the following values: —APPLICATION_START(39) —APPLICATION_STOP(40)	3GPP TS 29.212



AVP Name	AVP Code	Comment	Reference
[ Framed-IP-Address ]	8	-	RFC 4005
[ Framed-Ipv6-Prefix ]	97	-	RFC 4005
{ Origin-Host }	264	-	RFC 6733
{ Origin-Realm }	296	-	RFC 6733
[ Origin-State-Id ]	278	-	RFC 6733

(1) If the CCR-U includes the Flow-Information AVPs, then it has to include the TDF-Application-Instance-Identifier AVP as well.

## 4.4 Sd Credit Control Answer

[Table 10](#) lists the AVPs that the SAPC sends in a Credit Control Answer (CCA) message.

Table 10 CCA AVPs

AVP Name	AVP Code	Comment	Reference
<Session-Id>	263	-	RFC 6733
*[ ADC-Rule-Install ]	1092	This AVP is used to activate ADC rules as instructed by the SAPC. For detailed information, see <a href="#">Table 13</a> .	3GPP TS 29.212
*[ ADC-Rule-Remove ]	1093	-	3GPP TS 29.212
{ Auth-Application-Id }	258	-	RFC 6733
{ CC-Request-Number }	415	-	RFC 4006
{ CC-Request-Type }	416	-	RFC 4006
[ Experimental-Result ]	297	-	RFC 6733
[ Failed-AVP ]	279	-	RFC 6733
{ Origin-Host }	264	-	RFC 6733
{ Origin-Realm }	296	-	RFC 6733
[ Origin-State-Id ]	278	-	RFC 6733
[ Result-Code ]	268	-	RFC 6733

## 4.5 Sd Re-Authorization Request

[Table 11](#) lists the AVPs that the SAPC sends in a Re-Authorization Request (RAR) message.

Table 11 RAR AVPs

AVP Name	AVP Code	Comment	Reference
<Session-Id>	263	-	RFC 6733
*[ ADC-Rule-Install ]	1092	This AVP is used to activate ADC rules as instructed by the SAPC.	3GPP TS 29.212



AVP Name	AVP Code	Comment	Reference
		For detailed information, see <a href="#">Table 13</a> .	
*[ ADC-Rule-Remove ]	1093	-	3GPP TS 29.212
{ Auth-Application-Id }	258	-	RFC 6733
{ Destination-Host }	293	-	RFC 6733
{ Destination-Realm }	283	-	RFC 6733
{ Origin-Host }	264	-	RFC 6733
{ Origin-Realm }	296	-	RFC 6733
[ Origin-State-Id ]	278	-	RFC 6733
{ Re-Auth-Request-Type }	285	-	RFC 6733
[ Session-Release-Cause ]	1045	The SAPC supports the following value: —IP_CAN_SESSION_TERMINATION(3)	3GPP TS 29.212

## 4.6 Sd Re-Authorization Answer

[Table 12](#) lists the AVPs that the SAPC supports in a Re-Authorization Answer (RAA) message.

Table 12 RAA AVPs

AVP Name	AVP Code	Comment	Reference
<Session-Id>	263	-	RFC 6733
[ Experimental-Result ]	297	-	RFC 6733
[ Failed-AVP ]	279	-	RFC 6733
{ Origin-Host }	264	-	RFC 6733
{ Origin-Realm }	296	-	RFC 6733
[ Origin-State-Id ]	278	-	RFC 6733
[ Result-Code ]	268	-	RFC 6733



## 5 Sd Interface AVPs

[Table 13](#) contains information about Sd specific AVPs.

Table 13 ADC-Rule-Install AVPs

AVP Name	AVP Code	Comment	Reference
ADC-Rule-Base-Name	1095	<p>This AVP indicates the name of a predefined group of ADC rules. This AVP is used to activate ADC rules as instructed by the SAPC. The following AVPs are supported:</p> <ul style="list-style-type: none"><li>—ADC-Rule-Name (AVP Code: 1096): this AVP is used as a reference for a predefined ADC rule in the TDF to be activated or deactivated</li><li>—ADC-Rule-Base-Name (AVP Code: 1095): this AVP is used as a reference for a group of predefined ADC rules in the TDF to be activated or deactivated</li></ul>	3GPP TS 29.212
ADC-Rule-Name	1096	This AVP defines a name for an ADC rule.	3GPP TS 29.212



## 6 Sd Error Handling

When the SAPC detects an error at protocol or application level, it returns a response including the Result-Code AVP with an error code specifying the error.

### 6.1 Sd Protocol Errors

The SAPC handles the following Diameter Base Protocol result codes:

Table 14 Sd Protocol Errors

Diameter Result Code	Value	Description
DIAMETER_SUCCESS	2001	A request is successfully completed.
DIAMETER_COMMAND_UNSUPPORTED	3001	A request contains a Command-Code that the SAPC does not recognize or support.
DIAMETER_TOO_BUSY	3004	An answer is received indicating that the TDF cannot handle the request due to overload.  A notification is sent when the SAPC is overloaded.
DIAMETER_APPLICATION_UNSUPPORTED	3007	A request is received for an unsupported application.
DIAMETER_INVALID_HDR_BITS	3008	A request is received with a Diameter header whose bits are set to an invalid combination or to a value that is inconsistent with the Command-Code definition.
DIAMETER_INVALID_AVP_BITS	3009	A request is received with an AVP whose flag bits are set to an unrecognized value or are inconsistent with the AVPs definition.

### 6.2 Sd Application Errors

The SAPC handles the following Sd interface application errors:





Table 15 Sd Application Errors

Result Code	Value	Description
DIAMETER_AVP_UNSUPPORTED	5001	<p>A request is received with an AVP that is not recognized or supported (not included in the SAPC Diameter dictionary) and was marked with the Mandatory bit.</p> <p>A Diameter message with this error must contain a Failed-AVP AVP containing the AVPs that caused the failure.</p>
DIAMETER_UNKNOWN_SESSION_ID	5002	Returned if the session does not exist for the user equipment IP address at session modification or termination.
DIAMETER_INVALID_AVP_VALUE	5004	<p>A request is received with an AVP with an invalid value in its data portion. A Diameter message with this error must contain a Failed-AVP AVP containing the AVPs that caused the failure.</p>
DIAMETER_MISSING_AVP	5005	<p>When a request is received including an AVP that is not required to process that request, that AVP is ignored and the request is processed as usual. On the contrary, when a request does not include an AVP that is required to process such request, the SAPC returns a response including the DIAMETER_MISSING_AVP Result-Code and the Failed-AVP AVP.</p>
DIAMETER_AVP_NOT_ALLOWED	5008	<p>A request is received with an AVP that must not be present.</p> <p>A Diameter message with this error must contain a Failed-AVP AVP with a copy of the offending AVP.</p>
DIAMETER_AVP_OCCURS_TOO_MANY_TIMES	5009	<p>A request is received with an AVP that appears more often than permitted in the message definition.</p> <p>A Diameter message with this error must contain a Failed-AVP AVP with a copy of the first instance of the offending AVP that exceeded the maximum number of occurrences.</p>
DIAMETER_NO_COMMON_APPLICATION	5010	A CER message is received and there are no common applications supported between the SAPC and the peer.



Result Code	Value	Description
DIAMETER_UNSUPPORTED_VERSION	5011	A request is received with an unsupported version number.
DIAMETER_UNABLE_TO_COMPLY	5012	This error is returned when the SAPC receives a request and detects an internal error which does not allow to continue processing a request.
DIAMETER_INVALID_BIT_IN_HEADER	5013	A request is received with an unrecognized bit in the Diameter header is set to one.
DIAMETER_INVALID_AVP_LENGTH	5014	<p>A request is received containing an AVP with an invalid length.</p> <p>A Diameter message with this error must contain a Failed-AVP AVP containing the offending AVP.</p>
DIAMETER_INVALID_MESSAGE_LENGTH	5015	A request is received with an invalid message length.
DIAMETER_INVALID_AVP_BIT_COMBO	5016	<p>A request is received with an AVP which is not allowed to have the received value in the AVP Flags field.</p> <p>A Diameter message with this error must contain a Failed-AVP AVP containing the offending AVP.</p>



# 7 Reference List

## Standard References

1. [Policy and Charging Control \(PCC\); Reference points](#), 3GPP TS 29.212

## Online References

1. [Diameter Base Protocol](#), IETF RFC 6733
2. [Diameter Credit-Control Application](#), IETF RFC 4006
3. [Diameter Network Access Server Application](#), IETF RFC 4005