

Smp 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

1	Smp Interface Overview	1
1.1	Document Content Conventions	1
2	Smp Message Exchange	2
3	Diameter Base Protocol Messages	3
3.1	Smp Capability Negotiation	3
3.2	Device Watchdog	4
3.3	Disconnect Peer	5
4	Smp Interface Message Format	6
4.1	Smp Credit-Control-Request (CCR)	6
4.2	Smp Credit-Control-Answer (CCA)	6
5	Smp Interface AVPs	8
5.1	MIP6-Agent-Info AVP	8
6	Smp Error Handling	9
6.1	Smp Protocol Errors	9
6.2	Smp Application Errors	9
7	Reference List	13





1 Smp Interface Overview

The Smp interface is an Ericsson proprietary interface built over *Diameter Base Protocol RFC*.

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 Diameter Base Protocol RFC.

For detailed information about Statement of Compliance 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 behaves in the following way (standard Diameter Base Protocol behavior):

- If the SAPC receives in a message an AVP with 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 in a message 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 in a message an AVP with 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 Smp Message Exchange

The Smp interface exchanges the following Diameter messages between the SGSN-MME and the SAPC:

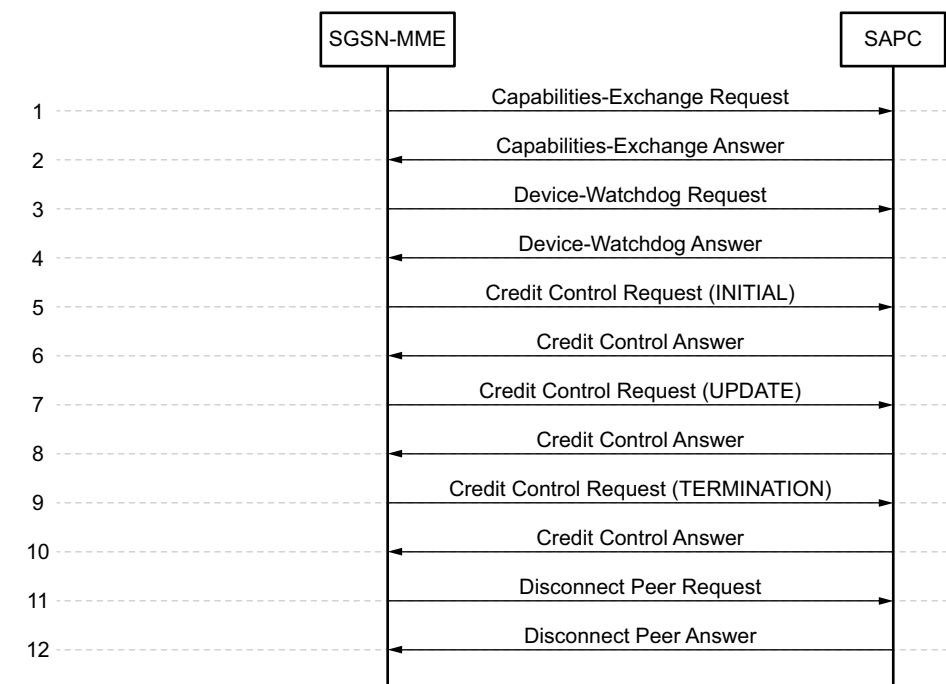


Figure 1 Smp Interface Message Flow



3 Diameter Base Protocol Messages

3.1 Smp Capability Negotiation

[Table 1](#) lists the AVPs that the SAPC supports in a Capabilities Exchange Request (CER) message.

Table 1 CER AVPs

AVP Name	AVP Code	Comment	Reference
* [Acct-Application-Id]	259	-	RFC 6733
* [Auth-Application-Id]	258	-	RFC 6733
[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	-	RFC 6733
*[Vendor-Specific-Application-Id]	260	-	RFC 6733

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

Table 2 CEA AVPs

AVP Name	AVP Code	Comment	Reference
* [Auth-Application-Id]	258	The SAPC sets it to value 16777327 (Smp).	RFC 6733
[Error-Message]	281	-	RFC 6733
[Failed-AVP]	279	-	RFC 6733
[Firmware-Revision]	367	-	RFC 6733



AVP Name	AVP Code	Comment	Reference
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	According to configuration, the SAPC sends the values assigned to other supported vendors different from the vendor device (Ericsson): —10415 (3GPP)	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= 193 (Ericsson) —Auth-Application-Id = 16777327 (Smp)	RFC 6733

Note: The SAPC does not send the Origin-State-Id AVP in the CEA message.

3.2 Device Watchdog

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

Table 3 DWR AVPs

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

Note: The SAPC does not include 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 DWA message.



Table 4 DWA 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
[Origin-State-Id]	278	-	RFC 6733

Note: The SAPC does not include 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 DPR message.

Table 5 DPR AVPs

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

[Table 6](#) lists the AVPs that the SAPC supports in a 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 Smp Interface Message Format

4.1 Smp Credit-Control-Request (CCR)

[Table 7](#) lists the AVPs that the SAPC supports in a CCR message.

Table 7 CCR AVPs

AVP Name	AVP Code	Comment	Reference
<Session-Id>	263	-	RFC 6733
[3GPP-User-Location-Info]	22	-	3GPP TS 29 061
{Auth-Application-Id}	258	-	3GPP TS 29.212
[Called-Station-ID] ⁽¹⁾	30	-	RFC 4005
{CC-Request-Number}	415	-	RFC 4006
{CC-Request-Type}	416	-	RFC 4006
{Destination-Realm}	283	-	RFC 6733
[Destination-Host]	293	-	RFC 6733
[Framed-IP-Address] ⁽²⁾	8	-	RFC 4005
[Framed-IPv6-Prefix] ⁽²⁾	97	-	RFC 4005
[IP-CAN-Type]	1027	The SAPC supports the following values: — 3GPP-GPRS (0) — 3GPP-EPS (5)	3GPP TS 29.212
{Origin-Host}	264	-	RFC 6733
{Origin-Realm}	296	-	RFC 6733
[Origin-State-Id]	278	-	RFC 6733
[RAT-Type]	1032	-	3GPP TS 29.212
*[Subscription-Id] ⁽¹⁾	443	The SGSN-MME always sends the IMSI as Subscription-Id, and also sends the MSISDN as Subscription-Id if available.	RFC 4006
[User-Equipment-Info]	458	-	RFC 4006

(1) Both Subscription-Id and Called-Station-ID AVPs are mandatory to be received for the SAPC in CCR INITIAL message. If not received, the SAPC returns DIAMETER_MISSING_AVP.

(2) The Framed-IP-Address or Framed-IPv6-Prefix AVPs are optional in a CCR Initial message.

4.2 Smp Credit-Control-Answer (CCA)

[Table 8](#) lists the AVPs that the SAPC sends in a CCA message.



Table 8 CCA AVPs

AVP Name	AVP Code	Comment	Reference
<Session-Id>	263	-	RFC 6733
{Auth-Application-Id}	258	-	3GPP TS 29.212
[Bearer-Control-Mode]	1023	The SAPC includes this AVP only in the CCA Initial message to indicate that only the Smp interface is supported, and supports the following value: —SX_ONLY (4)	3GPP TS 29.212
{CC-Request-Number}	415	-	RFC 4006
{CC-Request-Type}	416	-	RFC 4006
[Failed-AVP]	279	-	RFC 6733
*[MIP6-Agent-Info]	486	The SAPC includes this AVP only in the CCA Initial message. These AVPs contain the identities of the PDN-GWs. See MIP6-Agent-Info AVP on page 8.	RFC 5447
{Origin-Host}	264	-	RFC 6733
{Origin-Realm}	296	-	RFC 6733
[Origin-State-Id]	278	The SAPC increments its value in standalone mode. The SAPC does not increment its value in GeoRed mode, as the SAPC does a transparent switch-over (the Diameter peer always sees an operative node, which is in the active zone).	3GPP TS 29.212
[RAT-Frequency-Selection-Priority-ID]	1440	The SAPC includes this AVP in the CCA Initial message. This AVP contains the subscribed value of Subscriber Profile ID for RAT/Frequency Selection Priority (RFSP/SPID), which is also referred to as SPID. This AVP is of type Unsigned32 and coded in the Subscriber Profile ID for RAT/Frequency Priority IE. The range of values for this AVP is 1–256.	3GPP TS 29.272 3GPP TS 25.413 3GPP TS 36.413
{Result-Code}	268	-	RFC 6733



5 Smp Interface AVPs

The following subsections contain information for AVPs that cannot be explained in Message tables described in [Smp Interface Message Format](#) on page 6, owing to limited space.

5.1 MIP6-Agent-Info AVP

The MIP6-Agent-Info AVP is of type Grouped and contains the AVPs described in the following table:

Table 9 MIP6-Agent-Info AVPs

AVP Name	AVP Code	Comment	Reference
*2[MIP-Home-Agent-Address]	334	This AVP contains an IPv4 address, a 128-bit IPv6 address, or both for the PDN-GW.	RFC 5447
[MIP-Home-Agent-Host]	348	This is a grouped AVP that contains the FQDN for the PDN-GW in the Destination-Host AVP, and a dummy value for the Destination-Realm AVP.	RFC 5447



6 Smp Error Handling

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

6.1 Smp Protocol Errors

The SAPC handles the following Diameter Base Protocol error types:

Table 10 SAPC Diameter Base Protocol Errors

Diameter Result Code	Value	Description
DIAMETER_SUCCESS	2001	A request is successfully completed.
DIAMETER_COMMAND_UNSUPPORTED	3001	A request contains a <code>Command-Code</code> that the SAPC does not recognize or support.
DIAMETER_TOO_BUSY	3004	A request is received 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 <code>Command-Code</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.
DIAMETER_UNKNOWN_PEER	3010	A CER message is received from an unknown peer.

6.2 Smp Application Errors

The SAPC handles the following Smp interface Application errors:



Table 11 SAPC Application Errors

Diameter Result Code	Value	Description
DIAMETER_OUT_OF_SPACE	4002	A Diameter node received the request but was unable to commit it to stable storage due to a temporary lack of space.
ELECTION_LOST	4003	The peer has determined that it has lost the election process and has therefore disconnected the transport connection.
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 UE IP address at session modification/termination.
DIAMETER_INVALID_AVP_VALUE	5004	<p>A request is received with an AVP with an invalid value in its data portion.</p> <p>A Diameter message with this error must contain a Failed-AVP AVP containing the AVPs that caused the failure.</p>
DIAMETER_MISSING_AVP	5005	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 Result-Code DIAMETER_MISSING_AVP and the Failed-AVP AVP.
DIAMETER_CONTRADICTING_AVPS	5007	<p>A request is received with AVPs that are contradicted each other.</p> <p>A Diameter message with this error must contain a Failed-AVP AVP containing the AVPs that caused the failure.</p>
DIAMETER_AVP_NOT_ALLOWED	5008	A request is received with an AVP that must not be present.



Diameter Result Code	Value	Description
		A Diameter message with this error must contain a Failed-AVP AVP with a copy of the offending AVP.
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.
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>
DIAMETER_NO_COMMON_SECURITY	5017	<p>This error is returned when a CER message is received, and there are no common security mechanisms supported between the peers.</p> <p>A CEA MUST be returned with the Result-Code AVP set to DIAMETER_NO_COMMON_SECURITY.</p>



Table 12 The SAPC Application Errors (II)

Result Code	Value	Description
DIAMETER_CREDIT_CONTROL_NOT_APPLICABLE	4011	This error is returned when the SAPC determines that the IP-CAN session must continue without an Smp session.
DIAMETER_USER_UNKNOWN	5030	This error is returned when the subscriber specified in the Subscription-Id AVP is not known in the SAPC at session activation or modification.

No Smp specific Experimental-Result-Code is defined.



7 Reference List

Standards

1. Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN) - 3GPP TS 29.061
2. Policy and Charging Control (PCC) over Gx reference point - 3GPP TS 29.212
3. Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol - 3GPP TS 29.272
4. UTRAN Iu interface Radio Access Network Application Part (RANAP) signalling - 3GPP TS 25.413
5. Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1AP) - 3GPP TS 36.413

Online References

1. [Diameter Base Protocol](#)
2. [Diameter Credit-Control Application](#)
3. [Diameter Network Access Server Application](#)
4. [Diameter Mobile IPv6: Support for Network Access Server to Diameter Server Interaction](#)