

Statement of Compliance to RFC 6733 - Diameter Base Protocol

STATEMENT OF COMPLIANCE

Copyright

© Ericsson AB 2015, 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.



Contents

1	Introduction	1
1.1	Prerequisites	1
2	Statement of Compliance Definitions	3
3	Statement of Compliance	5





1 Introduction

This document provides information about the Diameter compliance to the RFC 6733 – Diameter Base Protocol.

1.1 Prerequisites

This section states the prerequisites for this document.

1.1.1 Specifications

The Diameter compliance to the RFC 6733 – Diameter Base Protocol standard is covered.





2 Statement of Compliance Definitions

One of the following statements is given to each of the sections in the standard specification:

- **Compliant** – The functionality that is provided has been implemented in accordance with relevant and mandatory requirements. Possible limitations in the functionality are summarized.
- **Partially Compliant** – Part of the functionality that is provided has either been implemented in a way that is not in accordance with relevant and mandatory requirements or there are functionalities that have not been implemented.
- **Not Compliant** – The functionality that is provided has been implemented in a way that is not in accordance with relevant and mandatory requirements.
- **Not Implemented** – The functionality specified is not provided.
- **Not Applicable** – The functionality specified is not relevant for the product.
- **Informative** – The section contains no normative requirements.





3 Statement of Compliance

This section lists the compliance for each section in RFC 6733 – Diameter Base Protocol.

Table 1 RFC 6733 – Diameter Base Protocol Compliance

Section in RFC 6733 – Diameter Base Protocol		Compliance
1	Introduction	Informative
2	Protocol Overview	Partially Compliant ⁽¹⁾
2.1	Transport	Partially Compliant ^{(2) (3) (4)}
2.1.1	SCTP Guidelines	Compliant
2.2	Securing Diameter Messages	Partially Compliant ^{(3) (5)}
2.3	Diameter Application Compliance	Compliant
2.4	Application Identifiers	Compliant
2.5	Connections against Sessions	Informative
2.6	Peer Table	Compliant ⁽⁶⁾
2.7	Realm-Based Routing Table	Compliant ^{(7) (6)}
2.8	Role of Diameter Agents	Compliant ⁽⁷⁾
2.8.1	Relay Agents	Partially Compliant ⁽⁷⁾
2.8.2	Proxy Agents	Partially Compliant ^{(7) (8)}
2.8.3	Redirect Agents	Partially Compliant ^{(7) (9) (6)}
2.8.4	Translation Agents	Partially Compliant ⁽⁷⁾
2.9	Diameter Path Authorization	Partially Compliant ⁽⁷⁾
3	Diameter Header	Partially Compliant ⁽¹⁰⁾
3.1	Command Codes	Compliant ⁽¹¹⁾
3.2	Command Code Format specification	Compliant ⁽¹²⁾
3.3	Diameter Command Naming Conventions	Informative
4	Diameter AVPs	Compliant
4.1	AVP Header	Compliant
4.1.1	Optional Header Elements	Compliant
4.2	Basic AVP Data Formats	Compliant
4.3	Derived AVP Data Formats	Compliant
4.3.1	Common Derived AVP Data Formats	Compliant
4.4	Grouped AVP Values	Compliant



Table 1 RFC 6733 – Diameter Base Protocol Compliance

Section in RFC 6733 – Diameter Base Protocol		Compliance
4.4.1	Example AVP with a Grouped Data Type	Informative
4.5	Diameter Base Protocol AVPs	Compliant ⁽⁸⁾ ⁽¹³⁾
5	Diameter Peers	Informative
5.1	Peer Connections	Compliant
5.2	Diameter Peer Discovery	Partially Compliant ⁽⁶⁾
5.3	Capabilities Exchange	Compliant
5.3.1	Capabilities-Exchange-Request	Compliant
5.3.2	Capabilities-Exchange-Answer	Compliant
5.3.3	Vendor-Id AVP	Compliant
5.3.4	Firmware-Revision AVP	Compliant
5.3.5	Host-IP-Address AVP	Compliant
5.3.6	Supported-Vendor-Id AVP	Compliant
5.3.7	Product-Name AVP	Compliant
5.4	Disconnecting Peer Connections	Partially Compliant ⁽¹⁴⁾
5.4.1	Disconnect-Peer-Request	Compliant
5.4.2	Disconnect-Peer-Answer	Compliant
5.4.3	Disconnect-Cause AVP	Partially Compliant ⁽¹⁴⁾
5.5	Transport Failure Detection	Compliant
5.5.1	Device-Watchdog-Request	Compliant
5.5.2	Device-Watchdog-Answer	Compliant
5.5.3	Transport Failure Algorithm	Compliant
5.5.4	Failover and Failback Procedures	Compliant
5.6	Peer State Machine	Partially Compliant ⁽¹⁵⁾
5.6.1	Incoming Connections	Compliant
5.6.2	Events	Compliant
5.6.3	Actions	Compliant
5.6.4	The Election Process	Compliant
6	Diameter Message Processing	Informative
6.1	Diameter Request Routing Overview	Partially Compliant ⁽⁷⁾
6.1.1	Originating a Request	Compliant
6.1.2	Sending a Request	Compliant
6.1.3	Receiving Requests	Compliant ⁽⁷⁾



Table 1 RFC 6733 – Diameter Base Protocol Compliance

Section in RFC 6733 – Diameter Base Protocol		Compliance
6.1.4	Processing Local Requests	Compliant
6.1.5	Request Forwarding	Compliant
6.1.6	Request Routing	Partially Compliant ^{(7) (16)}
6.1.7	Predictive Loop Avoidance	Partially Compliant ⁽⁷⁾
6.1.8	Redirecting Requests	Partially Compliant ^{(7) (17) (18)}
6.1.9	Relaying and Proxying Requests	Compliant ⁽⁷⁾
6.2	Diameter Answer Processing	Compliant ⁽¹⁶⁾
6.2.1	Processing Received Answers	Compliant
6.2.2	Relaying and Proxying Answers	Not Compliant ⁽⁷⁾
6.3	Origin-Host AVP	Compliant
6.4	Origin-Realm AVP	Compliant
6.5	Destination-Host AVP	Compliant
6.6	Destination-Realm AVP	Compliant
6.7	Routing AVPs	Compliant
6.7.1	Route-Record AVP	Compliant ⁽¹⁶⁾
6.7.2	Proxy-Info AVP	Compliant
6.7.3	Proxy-Host AVP	Compliant
6.7.4	Proxy-State AVP	Compliant
6.8	Auth-Application-Id AVP	Partially Compliant ⁽¹⁸⁾
6.9	Acct-Application-Id AVP	Partially Compliant ^{(1) (16)}
6.10	Inband-Security-Id AVP	Compliant
6.11	Vendor-Specific-Application-Id AVP	Partially Compliant ⁽¹⁶⁾
6.12	Redirect-Host AVP	Compliant ^{(6) (7)}
6.13	Redirect-Host-Usage AVP	Compliant ^{(6) (7) (19)}
6.14	Redirect-Max-Cache-Time AVP	Compliant ^{(6) (7) (20)}
7	Error Handling	Compliant
7.1	Result-Code AVP	Compliant ⁽¹⁶⁾
7.1.1	Informational	Not Compliant ^{(16) (20)}
7.1.2	Success	Compliant ⁽¹⁶⁾
7.1.3	Protocol Errors	Compliant ⁽⁷⁾
7.1.4	Transient Failures	Compliant ^{(16) (20)}
7.1.5	Permanent Failures	Compliant ⁽¹⁶⁾

Table 1 RFC 6733 – Diameter Base Protocol Compliance

Section in RFC 6733 – Diameter Base Protocol		Compliance
7.2	Error Bit	Compliant ⁽¹⁶⁾
7.3	Error-Message AVP	Compliant ⁽¹⁶⁾
7.4	Error-Reporting-Host AVP	Compliant ⁽¹⁶⁾
7.5	Failed-AVP AVP	Compliant ⁽¹⁶⁾
7.6	Experimental-Result AVP	Compliant ⁽¹⁶⁾
7.7	Experimental-Result-Code AVP	Compliant ⁽¹⁶⁾
8	Diameter User Sessions	Partially Compliant ^{(1) (16) (18)}
8.1	Authorization Session State Machine	Not Compliant ⁽¹⁸⁾
8.2	Accounting Session State Machine	Not Compliant ⁽¹⁾
8.3	Server-Initiated Re-Auth	Not Compliant ⁽¹⁸⁾
8.3.1	Re-Auth-Request	Compliant ^{(16) (18)}
8.3.2	Re-Auth-Answer	Partially Compliant ^{(16) (18) (19)}
8.4	Session Termination	Not Compliant ^{(1) (18) (21)}
8.4.1	Session-Termination-Request	Compliant ^{(1) (18) (21)}
8.4.2	Session-Termination-Answer	Compliant ^{(1) (18) (21)}
8.5	Aborting a Session	Compliant ^{(1) (18) (20) (21)}
8.5.1	Abort-Session-Request	Compliant ^{(1) (18) (20) (21)}
8.5.2	Abort-Session-Answer	Compliant ^{(1) (16) (18) (20) (21)}
8.6	Inferring Session Termination from Origin-State-Id	Compliant ⁽¹⁶⁾
8.7	Auth-Request-Type AVP	Compliant ⁽¹⁸⁾
8.8	Session-Id AVP	Partially Compliant ^{(16) (21)}
8.9	Authorization-Lifetime AVP	Partially Compliant ^{(16) (18)}
8.10	Auth-Grace-Period AVP	Compliant ⁽¹⁸⁾
8.11	Auth-Session-State AVP	Compliant ⁽¹⁸⁾
8.12	Re-Auth-Request-Type AVP	Compliant ^{(16) (18)}
8.13	Session-Timeout AVP	Compliant ^{(16) (21)}
8.14	User-Name AVP	Compliant
8.15	Termination-Cause AVP	Compliant
8.16	Origin-State-Id AVP	Compliant ^{(7) (16)}
8.17	Session-Binding AVP	Compliant ⁽²¹⁾
8.18	Session-Server-Failover AVP	Compliant ^{(16) (21)}



Table 1 RFC 6733 – Diameter Base Protocol Compliance

Section in RFC 6733 – Diameter Base Protocol		Compliance
8.19	Multi-Round-Time-Out AVP	Compliant ⁽¹⁸⁾
8.20	Class AVP	Compliant ^{(16) (18) (20)}
8.21	Event-Timestamp AVP	Compliant
9	Accounting	Not Compliant ⁽¹⁾
9.1	Server Directed Model	Not Compliant ⁽¹⁾
9.2	Protocol Messages	Not Compliant ⁽¹⁾
9.3	Accounting Application Extension and Document Requirements	Not Compliant ⁽¹⁾
9.4	Fault Resilience	Not Compliant
9.5	Accounting Records	Partially Compliant ^{(1) (16) (21)}
9.6	Correlation of Accounting Records	Not Compliant
9.7	Accounting Command-Codes	Partially Compliant ⁽¹⁾
9.7.1	Accounting-Request	Partially Compliant ^{(1) (16)}
9.7.2	Accounting-Answer	Partially Compliant ⁽¹⁶⁾
9.8	Accounting AVPs	Informative
9.8.1	Accounting-Record-Type AVP	Compliant ⁽¹⁾
9.8.2	Acct-Interim-Interval AVP	Partially Compliant ⁽¹⁾
9.8.3	Accounting-Record-Number AVP	Compliant ⁽¹⁾
9.8.4	Acct-Session-Id AVP	Compliant ^{(1) (7)}
9.8.5	Acct-Multi-Session-Id AVP	Partially Compliant ⁽¹⁾
9.8.6	Accounting-Sub-Session-Id AVP	Partially Compliant ⁽¹⁾
9.8.7	Accounting-Realtime-Required AVP	Compliant ⁽¹⁾
10	AVP Occurrence Table	Informative
10.1	Base Protocol Command AVP Table	Compliant
10.2	Accounting AVP Table	Compliant
11	IANA Considerations	Not Implemented
11.1	AVP Header	Not Implemented
11.1.1. 1	AVP Code	Not Implemented
11.1.2. 2	AVP Flags	Not Implemented
11.2	Diameter Header	Not Implemented
11.2.1	Command Codes	Not Implemented



Table 1 RFC 6733 – Diameter Base Protocol Compliance

Section in RFC 6733 – Diameter Base Protocol		Compliance
11.2.2	Command Flags	Not Implemented
11.3	AVP Values	Not Implemented
11.3.1	Experimental-Result-Code AVP	Not Implemented
11.3.2	Result-Code AVP Values	Not Implemented
11.3.3	Accounting-Record-Type AVP Values	Not Implemented
11.3.4	Termination-Cause AVP Values	Not Implemented
11.3.5	Redirect-Host-Usage AVP Values	Not Implemented
11.3.6	Session-Server-Failover AVP Values	Not Implemented
11.3.7	Session-Binding AVP Values	Not Implemented
11.3.8	Disconnect-Cause AVP Values	Not Implemented
11.3.9	Auth-Request-Type AVP Values	Not Implemented
11.3.10	Auth-Session-State AVP Values	Not Implemented
11.3.11	Re-Auth-Request-Type AVP Values	Not Implemented
11.3.12	Accounting-Realtime-Required AVP Values	Not Implemented
11.3.13	Inband-Security-Id AVP (code 299)	Not Implemented
11.4.	_diameters Service Name and Port Number Registration	Not Implemented
11.5	SCTP Payload Protocol Identifiers	Not Implemented
11.6	S-NAPTR Parameters	Not Implemented
12	Diameter Protocol Related Configurable Parameters	Compliant
13	Security Considerations	Not Compliant ^{(3) (5)}
13.1	TLS/TCP and DTLS/SCTP Usage	Not Compliant ⁽⁵⁾
13.2	Peer-to-Peer Considerations	Not Compliant ⁽⁵⁾
13.3	AVP Considerations	Not Compliant
14	References	Informative
Appendix A	Acknowledgments	Informative
Appendix B	S-NAPTR Example	Informative



Table 1 RFC 6733 – Diameter Base Protocol Compliance

Section in RFC 6733 – Diameter Base Protocol	Compliance
Appendix C Duplicate Detection	Not Compliant ⁽²²⁾
Appendix D Internationalized Domain Names	Compliant

(1) Accounting is handled by a user application.

(2) Internet Control Message Protocol (ICMP) messages are not handled by Diameter Base implementation.

(3) Transport Layer Security (TLS) or Datagram Transport Layer Security (DTLS) is not supported.

(4) An arbitrary port for receiving incoming connections cannot be specified.

(5) IPsec is not explicitly supported by Diameter Base implementation, but IPsec can be supported by the Component Base Architecture platform or an external security gateway.

(6) Domain Name System Server (DNS) peer discovery is not supported. Only manual configuration is available.

(7) Proxy agents, relay agents, redirect agents, and translation agents are supported as applications through the Application Programming Interface (API).

(8) End-to-end security is not supported.

(9) Incoming redirect messages are delivered to an application. The application is responsible for resending the message to the correct destination.

(10) The uniqueness of the end-to-end IDs is guaranteed for four minutes. If there is a Diameter traffic processor reload, disable or enable operations, or a reload by platform, the four-minute interval is not guaranteed and the end-to-end IDs generated after the mentioned operations can duplicate the ones generated before.

(11) The command codes in the Diameter Base Protocol RFC can be extended by an application.

(12) Different Augmented Backus-Naur Form (ABNF) definitions can be provided for the same command code by different applications.

(13) The Attribute-Value Pairs (AVPs) in the Diameter Base Protocol RFC can be extended by configuration.

(14) If a Disconnect-Peer-Request (DPR) message with reason DO_NOT_WANT_TO_TALK_TO_YOU is received, the connection can be reinitiated after disabling or enabling it.

(15) Capabilities-Exchange-Request (CER) or Capabilities-Exchange-Answer (CEA) are handled in R-Open/I-Open states. Capabilities-Update-Request (CUR) or Capabilities-Update-Answer (CUA) are not supported.

(16) The Diameter application is responsible for handling the AVPs and command codes it uses, including the command code and AVPs defined in the RFC (except for CER, CEA, Device-Watchdog-Request (DWR), Device-Watchdog-Answer (DWA), DPR, and Disconnect-Peer-Answer (DPA)).

(17) The Realm Routing Table (RRT) is not updated by incoming redirect messages.

(18) Authorization is handled by a user application.

(19) The redirect server is requested for each message.

(20) Authentication is handled by a user application.

(21) Sessions are handled by a user application.

(22) Duplication Detection is handled by a user application.