N-Squared Software High Performance Proxy Diameter Protocol Conformance Statement

Version 1.0

1 Document Information

1.1 Scope and Purpose

This document describes the implementation of the Diameter protocol using the N-Squared (N2) High Performance Proxy (HPP). It should be read in conjunction with the N2 HPP Technical Guide [R-1].

This document assumes a working knowledge of the relevant Diameter protocol documents and its network implementation.

1.2 Definitions, Acronyms, and Abbreviations

Term	Meaning
3GPP	Third-Generation Partnership Project
AVP	Attribute-Value Pair
BSS	Business Support Systems
CEA	Capabilities Exchange-Answer
CER	Capabilities-Exchange-Request
DPA	Disconnect-Peer-Answer
DPR	Disconnect-Peer-Request
DWA	Device Watchdog Answer
DWR	Device-Watchdog-Request
HPP	High Performance Proxy
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPSec	IP Security
N2	N-Squared
OCS	Online Charging Server
RFC	Request For Comments
SCTP	Stream Control Transmission Protocol
TCP	Transmission Control Protocol
TS	Technical Specification

1.3 References

The following documents are referenced within this document:

Reference	Document
[R-1]	N2 HPP Technical Guide
[R-2]	IETF RFC 6733 (Diameter Base Protocol)
[R-3]	IETF RFC 8506 (Diameter Credit Control Application)
[R-4]	3GPP TS 32.299 Diameter charging applications (Release 15)

1.4 Ownership and Usage

N-Squared Software (NZ) Limited
PO Box 5035
Terrace End
Palmerston North 4410
New Zealand

2 Contents

3 Introduction

3.1 N2 HPP Overview

The N-Squared High Performance Proxy is a software system for real-time relay and manipulation of messages between client and server endpoints.

The HPP provides high availability and linear horizontal scalability and is deployed on low-cost commodity x86-64 hardware with minimal third-party licensing charges. The result is a cost-effective deployment which can be easily upscaled in response to future business growth.

Both BSS systems and southbound network components – including other N2 components, such as the N2 OCS - may access the HPP to provide brokering of messages and functionality across a wide range of batch-processed and real-time protocols. This includes Diameter, where the HPP can function as a Diameter relay agent, message forwarder, or proxy.

3.2 Diameter Overview

The Diameter protocol is widely used for authorization and control of traffic. The base protocol is defined in RFC 6733 [R-2], with credit control extensions from RFC 8506 [R-3]. Credit control is further extended by the 3GPP charging applications [R-4].

One notable feature of the Diameter protocol is its ability to allow custom Attribute-Value Pairs (AVPs) to be used when both the client and server are configured to understand them.

3.3 General Restrictions

Specific compliance to the RFCs and TS documentation is described in section 5: RFC Compliance, but there are some high-level Diameter interactions and features that are not supported by the N2 HPP:

- In-band security over TLS/DTLS is not supported. If desired, an external IPSec gateway can provide transport layer security.
- Diameter peer election and request redirection are not supported. The HPP is intended to be used for Diameter relay, forwarding, or proxying in a single ecosystem.

4 Diameter Messaging

4.1 Message Encoding

All Diameter messaging sent by the HPP will follow the basic encoding of RFC 6733. Received Diameter messages must also follow this encoding.

4.1.1 Diameter Headers

All Diameter headers generated by the HPP are set in compliance with RFC 6733 section 3. For headers that are present in transferred messages, the HPP will alter values as required for routing and length changes, if any.

Field	Type / Length	Notes
Version	1 octet	Always set to 1.
Message Length	3 octets	Total message length, including header.
Command Flags	1 octet	Not altered for transferred messages. Set as per RFC 6733 for generated messages, i.e. *R P E T r r r r*.
Command Code	3 octets	Not altered.
Application-ID	4 octets	Not altered.
Hop-by-Hop Identifier	Unsigned32	Set as per RFC 6733.
End-to-End Identifier	Unsigned32	Not altered.

Table 1: Diameter headers

4.1.2 Diameter AVPs

All Diameter AVPs generated by the HPP are set in compliance with RFC 6733 section 3. For AVPs that are present in transferred messages, the HPP will not alter any values.

Field	Type / Length	Notes
AVP Code	4 octets	-
AVP Flags	1 octet	Not altered for transferred messages. Set as per RFC 6733 for generated messages, i.e. *V M P r r r r r.* Flag values will be set according to the individual AVP definition for generated messages.
AVP Length	3 octets	Total AVP length, including header.
Vendor-ID	4 octets	Always included. Set to 0 for AVPs from RFC 6733 or RFC 8506, or set according to the AVP definition for other AVPs.
Data	Variable	As specified by the AVP Code and AVP Length.

Table 2: Diameter AVPs

In addition to the stated compliance to standard AVPs given in *Table 6: HPP compliance to RFC 6733*, the HPP may be configured to receive and send arbitrary standard or vendor-specific AVPs. Refer to the HPP Technical Guide for further details.

4.1.3 AVP Data Types

The HPP supports most basic and derived data types specified in RFC 6733 sections 4.2 and 4.3. Specifically, the following AVP data types are supported:

- OctetString
- Integer32 / Integer64
- Unsigned32 / Unsigned64
- Grouped
- Address
- Time
- UTF8String
- DiameterIdentity
- DiameterURI
- Enumerated

The following AVP data types are not supported:

- Float32 / Float64
- IPFilterRule

4.2 Connection Management

The HPP may be configured to accept inbound connections from or to invoke outbound connections to other Diameter clients or servers, following the capability exchange transaction specified in RFC 6733 section 5.3. Connection management command codes supported by the HPP are:

- Capability-Exchange-Request (CER) and Capability-Exchange-Answer (CEA)
- Disconnect-Peer-Request (DPR) and Disconnect-Peer-Answer (DPA)
- Device-Watchdog-Request (DWR) and Device-Watchdog-Answer (DWA)

The message parameters for these command codes are shown in the following sections.

The HPP must be configured with a whitelist of information for clients or servers that initiate connections to the HPP.

Connections may be made to and from the HPP over either TCP or SCTP.

Refer to the HPP Technical Guide [R-1] for details of the configuration allowed for connection management.

4.2.1 Capability Exchange Messages

Depending on whether the HPP is configured to listen or initiate connections, both CER and CEA messages may be sent and/or received.

Field	AVP Code	Data Type	Presence		Inbound Notes	Outbound Notes
			CER	CEA		
Result-Code	268	Unsigned32	0	1	-	Set as per RFC 6733.
Origin-Host	264	DiameterIdentity	1	1	Must match whitelist.	Set from configuration.

Field	AVP Code	Data Type	Presence		Inbound Notes	Outbound Notes
			CER	CEA		
Origin-Realm	296	DiameterIdentity	1	1	-	Set from configuration.
Host-IP-Address	257	Address	1+	1+	Must match whitelist.	Set from configuration.
Vendor-Id	266	Unsigned32	1	1	-	Set from configuration.
Product-Name	269	UTF8String	1	1	-	Set from configuration.
Origin-State-Id	278	Unsigned32	0-1	0-1	-	Not used for session maintenance.
Error-Message	281	UTF8String	0	0-1	Ignored by default.	Only sent in error cases. Set as per RFC 6733.
Failed-AVP	279	Grouped	0	0-1	Ignored by default.	Only sent in error cases. Set as per RFC 6733.
Supported-Vendor-Id	265	Unsigned32	0+	0+	-	Set from configuration.
Auth-Application-Id	258	Unsigned32	0+	0+	Ignored by default.	Set from configuration.
Inband-Security-Id	299	Unsigned32	0+	0+	Ignored by default.	Not sent by default.
Acct-Application-Id	259	Unsigned32	0+	0+	Ignored by default.	Not sent by default.
Vendor-Specific-Application-Id	260	Grouped	0+	0+	Ignored by default.	Not sent by default.
Firmware-Revision	267	Unsigned32	0-1	0-1	Ignored by default.	Not sent by default.
(other AVPs)	*	*	*	*	Ignored by default.	Not sent by default.

Table 3: Capability exchange message parameters

4.2.2 Disconnect Peer Messages

When the HPP platform is taken out of service, a DPR message is sent to all connected clients and servers. These entities may attempt to reconnect as required.

In cases where a DPR is received from a client or server and the HPP is configured to initiate connections, the Disconnect-Cause AVP is not considered and reconnections will be made on the configured schedule.

Field	AVP Code	Data Type	Presence		Inbound Notes	Outbound Notes
			DPR	DPA		
Result-Code	268	Unsigned32	0	1	-	Set as per RFC 6733.

Field	AVP Code	Data Type	Presence		Inbound Notes	Outbound Notes
			DPR	DPA		
Origin-Host	264	DiameterIdentity	1	1	Must match CER/CEA.	As per CER/CEA.
Origin-Realm	296	DiameterIdentity	1	1	Must match CER/CEA.	As per CER/CEA.
Disconnect-Cause	273	Enumerated	1	0	Ignored by default. Reconnection will occur on the configured HPP schedule unless configured otherwise.	Set to 0 (REBOOTING).
Error-Message	281	UTF8String	0	0-1	Ignored by default.	Only sent in error cases. Set as per RFC 6733.
Failed-AVP	279	Grouped	0	0-1	Ignored by default.	Only sent in error cases. Set as per RFC 6733.
(other AVPs)	*	*	*	*	Ignored by default.	Not sent by default.

Table 4: Disconnect peer message parameters

4.2.3 Device Watchdog Messages

The HPP will send DWRs to connected clients and servers after no traffic is received from them for a configurable period.

Under normal circumstances, the HPP will always respond to a DWR from a connected entity positively to indicate that the system is functioning nominally.

Field	AVP Code	Data Type	Presence		Inbound Notes	Outbound Notes
			DWR	DWA		
Result-Code	268	Unsigned32	0	1	-	Set as per RFC 6733.
Origin-Host	264	DiameterIdentity	1	1	Must match CER/CEA.	As per CER/CEA.
Origin-Realm	296	DiameterIdentity	1	1	Must match CER/CEA.	As per CER/CEA.
Error-Message	281	UTF8String	0	0-1	Ignored by default.	Only sent in error cases. Set as per RFC 6733.
Failed-AVP	279	Grouped	0	0-1	Ignored by default.	Only sent in error cases. Set as per RFC 6733.

Field	AVP Code	Data Type	Presence		Inbound Notes	Outbound Notes
			DWR	DWA		
Origin-State-Id	278	Unsigned32	1	1	-	Not used for session maintenance.
(other AVPs)	*	*	*	*	Ignored by default.	Not sent by default.

Table 5: Device watchdog message parameters

4.3 Duplicate Messages

4.3.1 Received Messages

The HPP supports message retransmission by clients by using the retransmit command flag. For more information on this flag, refer to RFC 6733 section 3. Additionally, the HPP supports transport layer retransmission for Diameter messaging.

The HPP does not delay duplicate detection for out-of-order requests and will respond with the same answer message for each duplicate detected. The rolling detection window to preserve received messages and their answers is configurable; refer to the HPP Technical Guide.

For session-based credit control, the HPP does not impose constraints on the CC-Request-Number AVP field; messages will be processed in the order received.

Duplicate messages are detected by the combination of the Origin-Host AVP and the End-To-End-Identifier header value. The CC-Request-Number AVP field is not used for duplicate detection.

4.3.2 Sent Messages

The HPP does not set the retransmit command flag on answer messages, as per RFC 6733. However, the amount of transport layer retransmissions is configurable.

The retransmit flag may be set on request messages sent from the HPP where a link failure is detected. The number of retransmissions for request messages is configurable.

Note that the HPP does not persist Diameter sessions in non-volatile storage, so no duplication after reboot can occur for answer messages.

4.4 Diameter Messaging

As the HPP is intended to pass Diameter messages through itself, the Diameter application identifier and command code are not directly used outside of the messaging described in section *4.2:* Connection Management; all Diameter messages are supported for pass-through.

Similarly, all AVPs are supported for pass-through with the following caveats:

- The AVP type for all AVPs in the message must be noted as supported in section *4.1.3: AVP Data Types*.
- AVPs specified for inspection for routing purposes must either be marked as supported in *Table 6: HPP compliance to RFC 6733*, natively defined in RFC 8506 [3] or TS 32.299 [4], or have their AVP definition specified in the HPP configuration.

Refer to the HPP Technical Guide [R-1] for details of the configuration required for custom AVPs.

5 RFC Compliance

5.1 Compliance to RFC 6733 (Diameter Base Protocol)

Section	Section Heading	Compliance	Notes
1	Introduction	Not applicable.	-
1.1	Diameter Protocol	Not applicable.	-
1.1.1	Description of the Document Set	Not applicable.	-
1.1.2	Conventions Used in This Document	Not applicable.	-
1.1.3	Changes from RFC3588	Not applicable.	-
1.2	Terminology	Not applicable.	-
1.3	Approach to Extensibility	Not applicable.	-
1.3.1	Defining New AVP Values	Not applicable.	-
1.3.2	Creating New AVPs	Not applicable.	-
1.3.3	Creating New Commands	Not applicable.	-
1.3.4	Creating New Diameter Applications	Not applicable.	-
2	Protocol Overview	Fully compliant.	-
2.1	Transport	Fully compliant.	-
2.1.1	SCTP Guidelines	Fully compliant.	-
2.2	Securing Diameter Messages	Partially compliant.	IPSec may be applied via an external gateway. TLS/DTLS not supported.
2.3	Diameter Application Compliance	Fully compliant.	-
2.4	Application Identifiers	Fully compliant.	-
2.5	Connections vs. Sessions	Not applicable.	-
2.6	Peer Table	Fully compliant.	-
2.7	Routing Table	Fully compliant.	-
2.8	Role of Diameter Agents	Fully compliant.	-
2.8.1	Relay Agents	Fully compliant.	-
2.8.2	Proxy Agents	Fully compliant.	-
2.8.3	Redirect Agents	Not compliant.	Redirection not supported.
2.8.4	Translation Agents	Not compliant.	Translation not supported.
2.9	Diameter Path Authorization	Fully compliant.	-
3	Diameter Header	Fully compliant.	-
3.1	Command Codes	Fully compliant.	-
3.2	Command Code Format Specification	Not applicable.	-
3.3	Diameter Command Naming Conventions	Not applicable.	-

Section	Section Heading	Compliance	Notes
4	Diameter AVPs	Fully compliant.	-
4.1	AVP Header	Fully compliant.	-
4.1.1	Optional Header Elements	Fully compliant.	-
4.2	Basic AVP Data Formats	Partially compliant.	Float32 and Float64 not supported.
4.3	Derived AVP Data Formats	Not applicable.	-
4.3.1	Common Derived AVP Data Formats	Partially compliant.	IPFilterRule not supported.
4.4	Grouped AVP Values	Fully compliant.	-
4.4.1	Example AVP with a Grouped Data Type	Not applicable.	-
4.5	Diameter Base Protocol AVPs	Fully compliant.	-
5	Diameter Peers	Not applicable.	-
5.1	Peer Connections	Fully compliant.	-
5.2	Diameter Peer Discovery	Fully compliant.	-
5.3	Capabilities Exchange	Partially compliant.	TLS/DTLS not supported.
5.3.1	Capabilities-Exchange-Request	Fully compliant.	-
5.3.2	Capabilities-Exchange-Answer	Fully compliant.	-
5.3.3	Vendor-Id AVP	Fully compliant.	-
5.3.4	Firmware-Revision AVP	Fully compliant.	-
5.3.5	Host-IP-Address AVP	Fully compliant.	-
5.3.6	Supported-Vendor-Id AVP	Fully compliant.	-
5.3.7	Product-Name AVP	Fully compliant.	-
5.4	Disconnecting Peer Connections	Fully compliant.	-
5.4.1	Disconnect-Peer-Request	Fully compliant.	-
5.4.2	Disconnect-Peer-Answer	Fully compliant.	-
5.4.3	Disconnect-Cause AVP	Fully compliant.	-
5.5	Transport Failure Detection	Not applicable.	-
5.5.1	Device-Watchdog-Request	Fully compliant.	-
5.5.2	Device-Watchdog-Answer	Fully compliant.	-
5.5.3	Transport Failure Algorithm	Fully compliant.	-
5.5.4	Failover and Failback Procedures	Fully compliant.	-
5.6	Peer State Machine	Partially compliant.	Peer election not supported.
5.6.1	Incoming Connections	Fully compliant.	-
5.6.2	Events	Partially compliant.	Peer election not supported.
5.6.3	Actions	Partially compliant.	Peer election not supported.
5.6.4	The Election Process	Partially compliant.	Peer election not supported.

Section	Section Heading	Compliance	Notes
6	Diameter Message Processing	Not applicable.	-
6.1	Diameter Request Routing Overview	Fully compliant.	-
6.1.1	Originating a Request	Fully compliant.	-
6.1.2	Sending a Request	Fully compliant.	-
6.1.3	Receiving Requests	Not compliant.	Loop checking not supported.
6.1.4	Processing Local Requests	Fully compliant.	-
6.1.5	Request Forwarding	Fully compliant.	-
6.1.6	Request Routing	Not compliant.	Forwarding not supported.
6.1.7	Predictive Loop Avoidance	Not compliant.	Loop checking not supported.
6.1.8	Redirecting Requests	Not compliant.	Redirection not supported.
6.1.9	Relaying and Proxying Requests	Fully compliant.	-
6.2	Diameter Answer Processing	Fully compliant.	-
6.2.1	Processing Received Answers	Fully compliant.	-
6.2.2	Relaying and Proxying Answers	Not compliant.	Forwarding not supported.
6.3	Origin-Host AVP	Fully compliant.	-
6.4	Origin-Realm AVP	Fully compliant.	-
6.5	Destination-Host AVP	Fully compliant.	-
6.6	Destination-Realm AVP	Fully compliant.	-
6.7	Routing AVPs	Fully compliant.	-
6.7.1	Route-Record AVP	Fully compliant.	-
6.7.2	Proxy-Info AVP	Fully compliant.	-
6.7.3	Proxy-Host AVP	Fully compliant.	-
6.7.4	Proxy-State AVP	Fully compliant.	-
6.8	Auth-Application-Id AVP	Fully compliant.	-
6.9	Acct-Application-Id AVP	Fully compliant.	-
6.10	Inband-Security-Id AVP	Fully compliant.	-
6.11	Vendor-Specific-Application-Id AVP	Fully compliant.	-
6.12	Redirect-Host AVP	Not compliant.	Redirection not supported.
6.13	Redirect-Host-Usage AVP	Not compliant.	Redirection not supported.
6.14	Redirect-Max-Cache-Time AVP	Not compliant.	Redirection not supported.
7	Error Handling	Fully compliant.	-
7.1	Result-Code AVP	Fully compliant.	-
7.1.1	Informational	Fully compliant.	-
7.1.2	Success	Fully compliant.	-

Section	Section Heading	Compliance	Notes
7.1.3	Protocol Errors	Fully compliant.	-
7.1.4	Transient Failures	Fully compliant.	-
7.1.5	Permanent Failures	Fully compliant.	-
7.2	Error Bit	Fully compliant.	-
7.3	Error-Message AVP	Fully compliant.	-
7.4	Error-Reporting-Host AVP	Fully compliant.	-
7.5	Failed-AVP AVP	Fully compliant.	-
7.6	Experimental-Result AVP	Fully compliant.	-
7.7	Experimental-Result-Code AVP	Fully compliant.	-
8	Diameter User Sessions	Fully compliant.	-
8.1	Authorization Session State Machine	Not applicable.	Not applicable for pass-through.
8.2	Accounting Session State Machine	Not applicable.	Not applicable for pass-through.
8.3	Server-Initiated Re-Auth	Fully compliant.	-
8.3.1	Re-Auth-Request	Fully compliant.	-
8.3.2	Re-Auth-Answer	Fully compliant.	-
8.4	Session Termination	Fully compliant.	-
8.4.1	Session-Termination-Request	Fully compliant.	-
8.4.2	Session-Termination-Answer	Fully compliant.	-
8.5	Aborting a Session	Fully compliant.	-
8.5.1	Abort-Session-Request	Fully compliant.	-
8.5.2	Abort-Session-Answer	Fully compliant.	-
8.6	Inferring Session Termination from Origin-State-Id	Not compliant.	Session state is not inferred from Origin-State-Id.
8.7	Auth-Request-Type AVP	Fully compliant.	-
8.8	Session-Id AVP	Fully compliant.	-
8.9	Authorization-Lifetime AVP	Fully compliant.	-
8.10	Auth-Grace-Period AVP	Fully compliant.	-
8.11	Auth-Session-State AVP	Fully compliant.	-
8.12	Re-Auth-Request-Type AVP	Fully compliant.	-
8.13	Session-Timeout AVP	Fully compliant.	-
8.14	User-Name AVP	Fully compliant.	-
8.15	Termination-Cause AVP	Fully compliant.	-
8.16	Origin-State-Id AVP	Fully compliant.	-
8.17	Session-Binding AVP	Fully compliant.	-
8.18	Session-Server-Failover AVP	Fully compliant.	-
8.19	Multi-Round-Time-Out AVP	Fully compliant.	-

Section	Section Heading	Compliance	Notes
8.20	Class AVP	Fully compliant.	-
8.21	Event-Timestamp AVP	Fully compliant.	-
9	Accounting	Fully compliant.	-
9.1	Server Directed Model	Fully compliant.	-
9.2	Protocol Messages	Fully compliant.	-
9.3	Accounting Application Extension and Requirements	Fully compliant.	-
9.4	Fault Resilience	Fully compliant.	-
9.5	Accounting Records	Fully compliant.	-
9.6	Correlation of Accounting Records	Fully compliant.	-
9.7	Accounting Command Codes	Fully compliant.	-
9.7.1	Accounting-Request	Fully compliant.	-
9.7.2	Accounting-Answer	Fully compliant.	-
9.8	Accounting AVPs	Fully compliant.	-
9.8.1	Accounting-Record-Type AVP	Fully compliant.	-
9.8.2	Acct-Interim-Interval AVP	Fully compliant.	-
9.8.3	Accounting-Record-Number AVP	Fully compliant.	-
9.8.4	Acct-Session-Id AVP	Fully compliant.	-
9.8.5	Acct-Multi-Session-Id AVP	Fully compliant.	-
9.8.6	Accounting-Sub-Session-Id AVP	Fully compliant.	-
9.8.7	Accounting-Realtime-Required AVP	Fully compliant.	-
10	AVP Occurrence Tables	Fully compliant.	-
10.1	Base Protocol Command AVP Table	Partially compliant.	Refer to individual message definitions in previous sections.
10.2	Accounting AVP Table	Fully compliant.	-
11	IANA Considerations	Not applicable.	-
11.1	AVP Header	Fully compliant.	-
11.1.1	AVP Codes	Fully compliant.	-
11.1.2	AVP Flags	Fully compliant.	-
11.2	Diameter Header	Not applicable.	-
11.2.1	Command Codes	Fully compliant.	-
11.2.2	Command Flags	Fully compliant.	-
11.3	AVP Values	Fully compliant.	-
11.3.1	Experimental-Result-Code AVP	Fully compliant.	-
11.3.2	Result-Code AVP Values	Not applicable.	No IANA control required.

Section	Section Heading	Compliance	Notes
11.3.3	Accounting-Record-Type AVP Values	Not applicable.	No IANA control required.
11.3.4	Termination-Cause AVP Values	Not applicable.	No IANA control required.
11.3.5	Redirect-Host-Usage AVP Values	Not applicable.	No IANA control required.
11.3.6	Session-Server-Failover AVP Values	Not applicable.	No IANA control required.
11.3.7	Session-Binding AVP Values	Not applicable.	No IANA control required.
11.3.8	Disconnect-Cause AVP Values	Not applicable.	No IANA control required.
11.3.9	Auth-Request-Type AVP Values	Not applicable.	No IANA control required.
11.3.10	Auth-Session-State AVP Values	Not applicable.	No IANA control required.
11.3.11	Re-Auth-Request-Type AVP Values	Not applicable.	No IANA control required.
11.3.12	Accounting-Realtime-Required AVP Values	Not applicable.	No IANA control required.
11.3.13	Inband-Security-Id AVP (code299)	Not applicable.	No IANA control required.
11.4	_diameters Service Name and Port Number Registration	Not applicable.	No IANA control required.
11.5	SCTP Payload Protocol Identifiers	Not applicable.	No IANA control required.
11.6	S-NAPTR Parameters	Not applicable.	No IANA control required.
12	Diameter Protocol-Related Configurable Parameters	Fully compliant.	-
13	Security Considerations	Partially compliant.	IPSec may be applied via an external gateway. TLS/DTLS not supported.
13.1	TLS/TCP and DTLS/SCTP Usage	Not applicable.	TLS/DTLS not supported.
13.2	Peer-to-Peer Considerations	Not applicable.	TLS/DTLS not supported.
13.3	AVP Considerations	Partially compliant.	IPSec may be applied via an external gateway. TLS/DTLS not supported.
14	References	Not applicable.	-
14.1	Normative References	Not applicable.	-
14.2	Informative References	Not applicable.	-
Appendix A	Acknowledgements	Not applicable.	-
A.1	This Document	Not applicable.	-
A.2	RFC3588	Not applicable.	-
Appendix B	S-NAPTR Example	Not applicable.	-

Section	Section Heading	Compliance	Notes
Appendix C	Duplicate Detection	Not applicable.	-
Appendix D	Internationalized Domain Names	Not applicable.	-

Table 6: HPP compliance to RFC 6733

5.2 Compliance to RFC 8506 (Diameter Credit Control Application)

The HPP transparently supports Diameter credit control as set out in RFC 8506, section 2.

5.3 Compliance to 3GPP TS 32.299 (Release 15)

The HPP transparently supports Diameter credit control under TS 32.299.