N-Squared Software Online Charging Server Diameter Protocol Conformance Statement

Version 1.1

1 Document Information

1.1 Scope and Purpose

This document describes the implementation of the Diameter protocol for real-time charging using the N-Squared (N2) Online Charging Server (OCS). It should be read in conjunction with the N2 OCS 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
API	Application Programming Interface
ASA	Abort Session Answer
ASR	Abort-Session-Request
AVP	Attribute-Value Pair
BSS	Business Support Systems
CCA	Credit Control Answer
CCR	Credit-Control-Request
CEA	Capabilities Exchange-Answer
CER	Capabilities-Exchange-Request
DPA	Disconnect-Peer-Answer
DPR	Disconnect-Peer-Request
DWA	Device Watchdog Answer
DWR	Device-Watchdog-Request
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
MSCC	Multiple Services Credit-Control
N2	N-Squared
OCS	Online Charging Server
RAA	Re-Auth-Answer
RAR	Re-Auth-Request
REST	Representational State Transfer
RFC	Request For Comments
SCTP	Stream Control Transmission Protocol
Tcc	Credit-Control Timer
TCP	Transmission Control Protocol
TS	Technical Specification

1.3 References

The following documents are referenced within this document:

Reference	Document
[R-1]	N2 OCS Technical Guide
[R-2]	IETF RFC 6733 (Diameter Base Protocol)
[R-3]	IETF RFC 4006 (Diameter Credit Control Application)
[R-4]	3GPP TS 32.299 Diameter charging applications (Release 15)

1.4 Ownership and Usage

This document, including the information contained herein, is proprietary to N-Squared Software (NZ) Limited but released for informational purposes only.

This document shall not be used or reproduced for any other purpose without the written approval of N-Squared Software (NZ) Limited.

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

2 Contents

1 Document Information 2

1.1 Scope and Purpose 2

1.2 Definitions, Acronyms, and Abbreviations 2

1.3 References 3

1.4 Ownership and Usage 3

2 Contents 4

3 Introduction 6

3.1 N2 OCS Overview 6

3.2 Diameter Overview 6

3.3 General Restrictions 6

4 Diameter Messaging 7

4.1 Message Encoding 7

4.1.1 Diameter Headers 7

4.1.2 Diameter AVPs 7

4.1.3 AVP Data Types 8

4.2 Connection Management 8

4.2.1 Capability Exchange Messages 8

4.2.2 Disconnect Peer Messages 9

4.2.3 Device Watchdog Messages 10

4.3 Duplicate Messages 11

4.3.1 Received Messages 11

4.3.2 Sent Messages 11

4.4 Credit Control Messaging 11

4.4.1 Credit Control Messages 11

4.4.2 Abort Session Messages 15

4.4.3 Reauthorization Messages 16

5 Diameter Charging Scenarios 18

5.1 Single Session Charging 18

5.1.1 Successful Single Session Charging, OCS Termination 18

5.1.2 Successful Single Session Charging, Client Termination 19

5.1.3 Successful Single Session Charging, Reauthorization 20

5.1.4 Successful Single Session Charging, Validity Expiration 21

5.1.5 Unsuccessful Single Session Charging 21

5.2 Multiple Session Charging 22

5.2.1 Unsuccessful Multiple Session Charging 22
5.2.2 Successful Multiple Session Charging 23
5.3 Single Event Charging 24
5.3.1 Successful Single Event Charging 24
5.3.2 Successful Single Event Refund 24
5.3.3 Successful Multiple Session Charging, Validity Expiration 25
5.4 Other Charging Scenarios 25
5.4.1 Unsuccessful Session Charging, Tcc Timeout 25
6 RFC Compliance 27
6.1 Compliance to RFC 6733 (Diameter Base Protocol) 27
6.2 Compliance to RFC 4006 (Diameter Credit Control Application) 33
6.3 Compliance to 3GPP TS 32.299 (Release 15) 37

3 Introduction

3.1 N2 OCS Overview

The N-Squared Online Charging Server is a software system for real-time service rating, subscriber charging, and session control.

The OCS 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.

Northbound BSS systems access the OCS to provide a complete solution for invoicing, customer management, dunning, asset management, centralized product catalog, data mining, reporting interface, and other enterprise features.

Southbound network components are connected to the OCS via real-time billing protocols., including Diameter.

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 4006 [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 6: RFC Compliance, but there are some high-level Diameter interactions and features that are not supported by the N2 OCS:

- In-band security over TLS/DTLS is not supported. If desired, an external IPSec gateway can provide transport layer security.
- The OCS does not supply 3GPP quota management or Diameter MSCC credit pooling or tariff change. The standard validity time and quota grant mechanisms are used for credit control.
- Diameter peer election, request proxying, and request forwarding are not supported. The OCS is intended to be a terminal endpoint for credit control clients in a single ecosystem.

4 Diameter Messaging

4.1 Message Encoding

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

4.1.1 Diameter Headers

All Diameter headers sent by the OCS are set in compliance with RFC 6733 section 3.

Field	Type / Length	Notes
Version	1 octet	Always set to 1.
Message Length	3 octets	Total message length, including header.
Command Flags	1 octet	Set as per RFC 6733, i.e. *R P E T r r r r*.
Command Code	3 octets	Only the following command codes are supported: • Abort-Session-Request (ASR) and Abort-Session-Answer (ASA) • Capabilities-Exchange-Request (CER) and Capabilities-Exchange-Answer (CEA) • Device-Watchdog-Request (DWR) and Device-Watchdog-Answer (DWA) • Re-Auth-Request (RAR) and Re-Auth-Answer (RAA) • Credit-Control-Request (CCR) and Credit-Control-Answer (CCA) • Disconnect-Peer-Request (DPR) and Disconnect-Peer-Answer (DPA)
Application-ID	4 octets	Set to 4 for CCR and CCA and 0 otherwise.
Hop-by-Hop Identifier	Unsigned32, 4 octets	Set as per RFC 6733.
End-to-End Identifier	Unsigned32, 4 octets	Set as per RFC 6733.

Table 1: Diameter headers

4.1.2 Diameter AVPs

All Diameter AVPs sent by the OCS are set in compliance with RFC 6733 section 3.

Field	Type / Length	Notes
AVP Code	4 octets	-
AVP Flags	1 octet	Set as per RFC 6733, i.e. *V M P r r r r r.* Flag values will be set according to the individual AVP definition.
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 4006, 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 12: OCS compliance to RFC 6733, Table 13: OCS compliance to RFC 4006, and Table 14: OCS compliance to TS 32.299, the OCS may be configured to receive and send arbitrary standard or vendor-specific AVPs for use in rating. Refer to the OCS Technical Guide for further details.

4.1.3 AVP Data Types

The OCS 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 OCS may be configured to accept inbound connections from or to invoke outbound connections to charging clients, following the capability exchange transaction specified in RFC 6733 section 5.3. Connection management command codes supported by the OCS 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 OCS must be configured with a whitelist of charging client information for clients that initiate connections to the OCS.

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

Refer to the OCS Technical Guide for details of the configuration allowed for connection management.

4.2.1 Capability Exchange Messages

Depending on whether the OCS 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.
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+	Must be set to 4.	Set to 4.
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 OCS platform is taken out of service, a DPR message is sent to all connected charging clients. These clients may attempt to reconnect as required.

In cases where a DPR is received from a charging client and the OCS 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.
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 OCS 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 OCS will send DWRs to currently-connected charging clients after no traffic is received from them for a configurable period.

Under normal circumstances, the OCS will always respond to a DWR from a connected charging client 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 OCS 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 OCS supports transport layer retransmission for Diameter messaging.

The OCS 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 OCS Technical Guide.

For MSCC session-based credit control, the OCS 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 OCS 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 OCS. The number of retransmissions for request messages is configurable.

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

4.4 Credit Control Messaging

Credit control messaging is the primary function of the OCS's Diameter interface. Command codes supported by the OCS for credit control are:

- Credit-Control-Request (CCR) and Credit-Control-Answer (CCA)
- Re-Auth-Request (RAR) and Re-Auth-Answer (RAR)

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

Refer to the OCS Technical Guide for details of the configuration allowed for credit control.

4.4.1 Credit Control Messages

The OCS receives CCR messages from charging clients and returns CCA messages in response.

4.4.1.1 Credit-Control-Request Messages

The expected parameters for a CCR message as set out in RFC 4006 are shown below. Note that this is expected to be only the base of any charging control messaging for all but the simplest applications, and additional AVPs (either from the 3GPP standard or custom definitions) may be required to support rich charging definitions.

Field	AVP Code	Data Type	Presence				Inbound Notes
			I	U	T	E	
Session-Id	263	UTF8String	1	1	1	1	-
Origin-Host	264	DiameterIdentity	1	1	1	1	Must match sent CER/CEA value.
Origin-Realm	296	DiameterIdentity	1	1	1	1	Must match sent CER/CEA value.
Destination-Realm	283	DiameterIdentity	1	1	1	1	Must match OCS CER/CEA value.
Auth-Application-Id	258	Unsigned32	1	1	1	1	Must be set to 4.
Service-Context-Id	461	UTF8String	1	1	1	1	Must be set according to OCS rating configuration.
CC-Request-Type	461	Enumerated	1	1	1	1	Must be set according to RFC 4006.
CC-Request-Number	415	Unsigned32	1	1	1	0	Not used by OCS for duplicate detection.
Destination-Host	293	DiameterIdentity	1	1	1	1	Must match OCS CER/CEA value.
User-Name	1	UTF8String	-	-	-	-	Ignored by default.
CC-Sub-Session-Id	419	Unsigned64	0-1	0-1	0-1	0-1	Not used but returned in CCA if present.
Acct-Multi-Session-Id	50	UTF8String	0-1	0-1	0-1	0-1	Not used but returned in CCA if present.
Origin-State-Id	278	Unsigned32	-	-	-	-	Ignored by default.
Event-Timestamp	55	Time	1	1	1	1	Used as the time for charge occurrence.
Subscription-Id	443	Grouped	1	1	1	1	Maximum of one instance allowed. Refer to Table 12: OCS compliance to RFC 6733 for supported child AVPs.
Service-Identifier	439	Unsigned32	1*	1*	1*	1*	Required at root level if OCS is configured to not use MSCC. Ignored at root level if OCS is configured to use MSCC. Allowed values set as part of OCS rating configuration.
Termination-Cause	295	Enumerated	-	-	-	-	Ignored by default.

Field	AVP Code	Data Type	Presence				Inbound Notes
			I	U	T	E	
Requested-Service-Unit	437	Grouped	1*	1*	0	1*	Required at root level if OCS is configured to not use MSCC. Ignored at root level if OCS is configured to use MSCC. Refer to Table 13: OCS compliance to RFC 4006 for supported child AVPs. No child AVPs required for opening a parent session when OCS is configured to use MSCC or when centralized unit determination is used.
Requested-Action	436	Enumerated	0	0	0	1	-
Used-Service-Unit	446	Grouped	0	1*	1*	0	Required at root level if OCS is configured to not use MSCC. Ignored at root level if OCS is configured to use MSCC. Refer to Table 13: OCS compliance to RFC 4006 for supported child AVPs.
Multiple-Services-Indicator	455	Enumerated	1	1	1	1	-
Multiple-Services-Credit-Control	456	Grouped	0+	0+	0+	0+	Required if OCS is configured to use MSCC.
Service-Parameter-Info	440	Grouped	0+	0+	0+	0+	May be used as required for additional rating enrichment; refer to the OCS Technical Guide.
CC-Correlation-Id	411	OctetString	0-1	0-1	0-1	0-1	Ignored by default.
User-Equipment-Info	458	Grouped	0-1	0-1	0-1	0-1	Ignored by default.
Proxy-Info	284	Grouped	0+	0+	0+	0+	Not used but returned in CCA if present.
Route-Record	282	DiameterIdentity	0+	0+	0+	0+	Ignored by default.
(other AVPs)	*	*	*	*	*	*	Ignored unless configured for rating enrichment; refer to the OCS Technical Guide.

Table 6: Base Credit-Control-Request message parameters (sent to OCS)

4.4.1.2 Credit-Control-Answer Messages

The OCS returns CCA messages as shown below.

Field	AVP Code	Data Type	Presence				Outbound Notes
			I	U	T	E	
Session-Id	263	UTF8String	1	1	1	1	Set from CCR.
Result-Code	268	Unsigned32	1	1	1	1	Refer to Table 12: OCS compliance to RFC 6733 and Table 13: OCS compliance to RFC 4006 for supported values. Indicates status of master session only if OCS is configured to use MSCC; individual MSCC Result-Code values will be used for credit control if MSCC is used.
Origin-Host	264	DiameterIdentity	1	1	1	1	Set as per OCS CER/CEA.
Origin-Realm	296	DiameterIdentity	1	1	1	1	Set as per OCS CER/CEA.
Auth-Application-Id	258	Unsigned32	1	1	1	1	Set to 4.
CC-Request-Type	461	Enumerated	1	1	1	1	Set from CCR.
CC-Request-Number	415	Unsigned32	1	1	1	0	Set from CCR.
User-Name	1	UTF8String	0	0	0	0	Not sent by default.
CC-Session-Failover	418	Enumerated	0	0	0	0	Not sent by default.
CC-Sub-Session-Id	419	Unsigned64	0-1	0-1	0-1	0-1	Set from CCR if present.
Acct-Multi-Session-Id	50	UTF8String	0-1	0-1	0-1	0-1	Set from CCR if present.
Origin-State-Id	278	Unsigned32	1	1	1	1	Set as per OCS CER/CEA.
Event-Timestamp	55	Time	1	1	1	1	-
Granted-Service-Unit	431	Grouped	1*	1*	0	1*	Required at root level if OCS is configured to not use MSCC. Ignored at root level if OCS is configured to use MSCC. Refer to Table 13: OCS compliance to RFC 4006 for supported child AVPs.
Multiple-Services-Credit-Control	456	Grouped	0+	0+	0+	0+	Only sent if OCS is configured to use MSCC.
Cost-Information	423	Grouped	0	0	0	0	Not sent by default.
Final-Unit-Indication	430	Grouped	0-1	0-1	0	0	Refer to section Table 13: OCS compliance to RFC 4006 for supported values.
Check-Balance-Result	422	Enumerated	0	0	0	0	Not sent by default.

Field	AVP Code	Data Type	Presence				Outbound Notes
			I	U	T	E	
Credit-Control-Failure-Handling	427	Enumerated	1	1	0	0	Set to 0 (TERMINATE).
Direct-Debiting-Failure-Handling	427	Enumerated	0	0	0	1	Set to 0 (TERMINATE_OR_BUFFER).
Validity-Time	448	Unsigned32	1	1	0	0	Only sent if OCS is configured to not use MSCC.
Redirect-Host	292	DiameterURI	0	0	0	0	Not sent by default.
Redirect-Host-Usage	261	Enumerated	0	0	0	0	Not sent by default.
Redirect-Max-Cache-Time	262	Unsigned32	0	0	0	0	Not sent by default.
Proxy-Info	284	Grouped	0+	0+	0+	0+	Set from CCR if present.
Route-Record	282	DiameterIdentity	0	0	0	0	Not sent by default.
Failed-AVP	279	Grouped	0-1	0-1	0-1	0-1	Only included in error cases.
(other AVPs)	*	*	*	*	*	*	Not sent unless configured for charging control enrichment; refer to the OCS Technical Guide.

Table 7: Base Credit-Control-Answer message parameters (sent from OCS)

4.4.2 Abort Session Messages

4.4.2.1 Abort-Session-Request Messages

The OCS may need to stop an in-progress session on a Diameter charging client if the session supervision timer (Tcc, as defined in RFC 4006) expires. As the RFC does not allow for sub-sessions under MSCC to be aborted individually, all MSCC sub-sessions will be aborted as the parent session is closed.

Field	AVP Code	Data Type	Presence	Outbound Notes
Session-Id	263	UTF8String	1	Set from CCR.
Origin-Host	264	DiameterIdentity	1	Set as per OCS CER/CEA.
Origin-Realm	296	DiameterIdentity	1	Set as per OCS CER/CEA.
Destination-Host	293	DiameterIdentity	1	Set from CCR.
Destination-Realm	283	DiameterIdentity	1	Set from CCR.
Auth-Application-Id	258	Unsigned32	1	Set to 4.
(other AVPs)	*	*	*	Not sent by default.

Table 8: Abort-Session-Request message parameters (sent from OCS)

4.4.2.2 Abort-Session-Answer Messages

The charging client will indicate to the OCS whether the session has been aborted successfully. Note that the OCS does not take any further action for the session, other than logging the status returned.

Field	AVP Code	Data Type	Presence	Inbound Notes
Session-Id	263	UTF8String	1	Set from CCR.
Result-Code	268	Unsigned32	1	Logged as an error if not 2001 (DIAMETER_SUCCESS).
Origin-Host	264	DiameterIdentity	1	Must match sent CER/CEA value.
Origin-Realm	296	DiameterIdentity	1	Must match sent CER/CEA value.
User-Name	1	UTF8String	0-1	Ignored by default.
Error-Message	281	UTF8String	0-1	Ignored by default.
Error-Reporting-Host	294	DiameterIdentity	0-1	Ignored by default.
Failed-AVP	279	Grouped	0-1	Ignored by default.
Redirect-Host	292	DiameterURI	0+	Ignored by default.
Redirect-Host-Usage	261	Enumerated	0-1	Ignored by default.
Redirect-Max-Cache-Time	262	Unsigned32	0-1	Ignored by default.
Proxy-Info	284	Grouped	0+	Ignored by default.
(other AVPs)	*	*	*	Ignored by default.

Table 9: Abort-Session-Answer message parameters (sent to OCS)

4.4.3 Reauthorization Messages

4.4.3.1 Re-Auth-Request Messages

In some circumstances, for example if a user receives additional credit, the OCS may request charging clients with active sessions for the user to have reauthorization applied.

Field	AVP Code	Data Type	Presence	Outbound Notes
Session-Id	263	UTF8String	1	Set from CCR.
Origin-Host	264	DiameterIdentity	1	Set as per OCS CER/CEA.
Origin-Realm	296	DiameterIdentity	1	Set as per OCS CER/CEA.
Destination-Realm	283	DiameterIdentity	1	Set from CCR.
Destination-Host	293	DiameterIdentity	1	Set from CCR.
Auth-Application-Id	258	Unsigned32	1	Set to 4.
User-Name	1	UTF8String	0	Not sent by default.
Origin-State-Id	278	Unsigned32	1	Set as per OCS CER/CEA.
Proxy-Info	284	Grouped	0+	Set from CCR if present.
Route-Record	282	DiameterIdentity	0	Not sent by default.
(other AVPs)	*	*	*	Not sent by default.

Table 10: Re-Auth-Request message parameters (sent from OCS)

4.4.3.2 Re-Auth-Answer Messages

After sending an RAA in response to an RAR, the charging client is expected to immediately send a CCR-U for reauthorization if the session is still active.

Field	AVP Code	Data Type	Presence	Inbound Notes
Session-Id	263	UTF8String	1	Set from CCR.
Result-Code	268	Unsigned32	1	Logged as an error if not 2001 (DIAMETER_SUCCESS).
Origin-Host	264	DiameterIdentity	1	Must match sent CER/CEA value.
Origin-Realm	296	DiameterIdentity	1	Must match sent CER/CEA value.
User-Name	1	UTF8String	0-1	Ignored by default.
(other AVPs)	*	*	*	Ignored by default.

Table 11: Re-Auth-Answer message parameters (sent to OCS)

5 Diameter Charging Scenarios

Note that all scenarios in this section show charging interaction using the 3GPP model of decentralized unit determination with centralized rating, i.e. charging clients requesting specific units with rating granting those units. The OCS supports also supports the following alternate 3GPP charging models, but they are not shown here in the interests of brevity:

- Centralized unit determination and centralized rating, i.e. RSU received with no unit type and units determined by the OCS.
- Decentralized unit determination and decentralized rating, i.e. RSU received with CC-Money unit type and CC-Money granted by the OCS.

These alternate flows are referenced in-line underneath the associated diagram.

5.1 Single Session Charging

5.1.1 Successful Single Session Charging, OCS Termination

A user begins a voice call. The OCS grants the requested time but informs the client that no more time is available. Once the user consumes the granted time, the call is disconnected and the OCS commits the reservation of time.

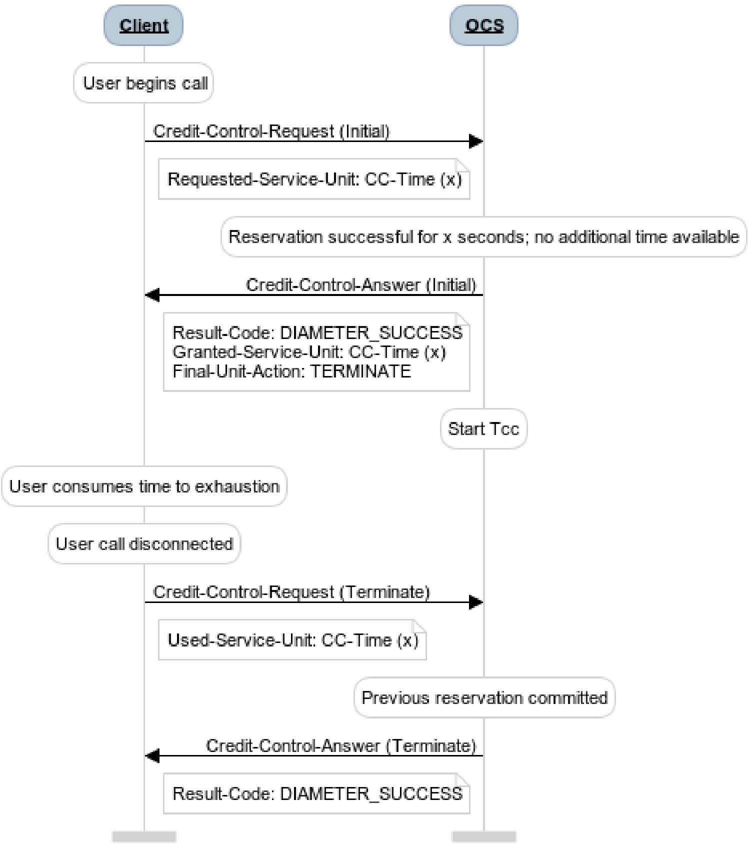
Client
OCS
User begins call
Credit-Control-Request (Initial)
Requested-Service-Unit: CC-Time (x)
Reservation successful for x seconds; no additional time available
Credit-Control-Answer (Initial)
Result-Code: DIAMETER_SUCCESS
Granted-Service-Unit: CC-Time (x)
Final-Unit-Action: TERMINATE
Start Tcc
User consumes time to exhaustion
User call disconnected
Credit-Control-Request (Terminate)
Used-Service-Unit: CC-Time (x)
Previous reservation committed
Credit-Control-Answer (Terminate)
Result-Code: DIAMETER_SUCCESS

Figure A: Successful single session charging, OCS termination

This scenario is based on Appendix A: Flow VII in RFC 4006.

5.1.2 Successful Single Session Charging, Client Termination

A user begins a single-session charging interaction through a data service. The initial reservation is successful, and the user continues using data. The charging client requests additional data from the OCS. The OCS commits the used quota from the initial reservation and grants additional quota to the user. The user consumes some of the additional quota and then ends the session. The OCS commits the used quota from the second reservation.

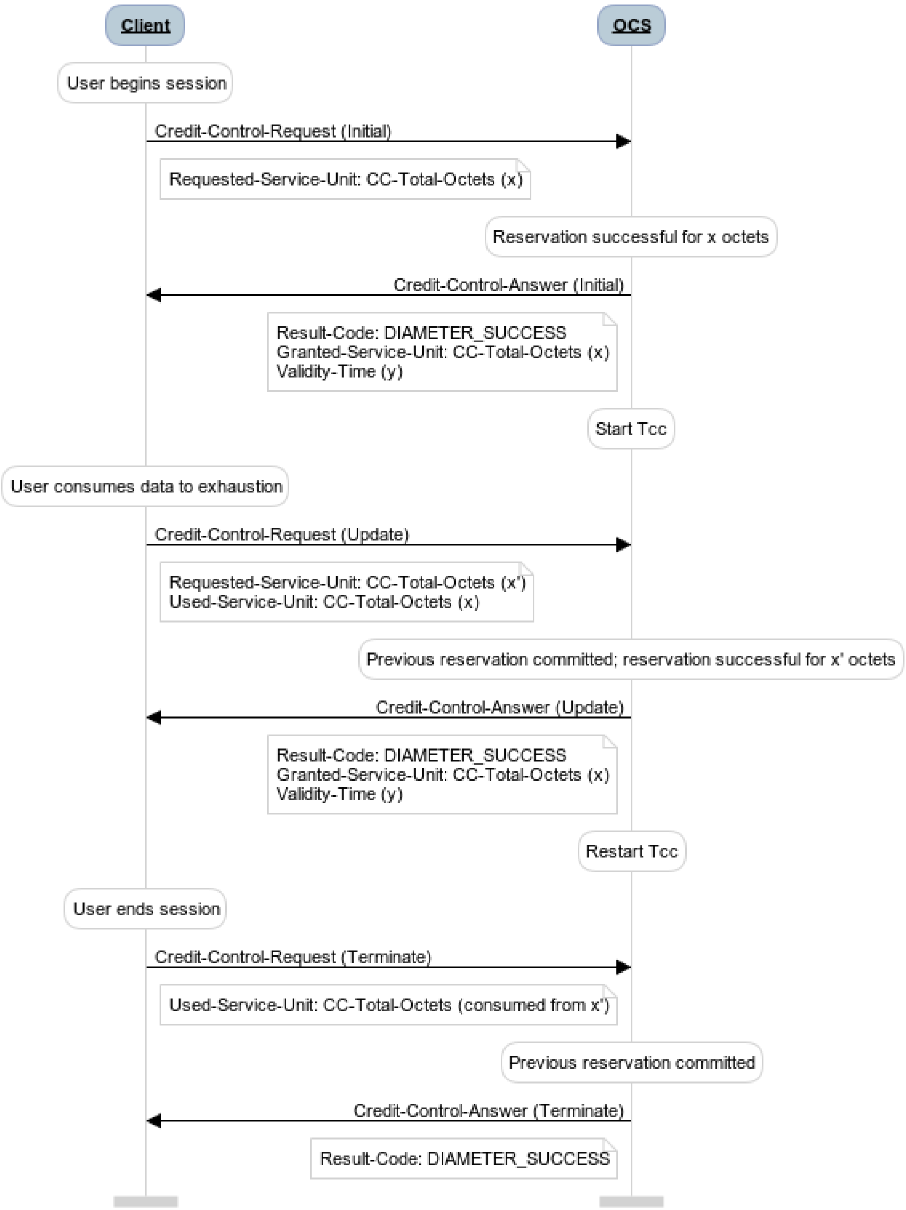
Client
OCS
User begins session
Credit-Control-Request (Initial)
Requested-Service-Unit: CC-Total-Octets (x)
Reservation successful for x octets
Credit-Control-Answer (Initial)
Result-Code: DIAMETER_SUCCESS
Granted-Service-Unit: CC-Total-Octets (x)
Validity-Time (y)
Start Tcc
User consumes data to exhaustion
Credit-Control-Request (Update)
Requested-Service-Unit: CC-Total-Octets (x')
Used-Service-Unit: CC-Total-Octets (x)
Previous reservation committed; reservation successful for x' octets
Credit-Control-Answer (Update)
Result-Code: DIAMETER_SUCCESS
Granted-Service-Unit: CC-Total-Octets (x)
Validity-Time (y)
Restart Tcc
User ends session
Credit-Control-Request (Terminate)
Used-Service-Unit: CC-Total-Octets (consumed from x')
Previous reservation committed
Credit-Control-Answer (Terminate)
Result-Code: DIAMETER_SUCCESS

Figure B: Successful single session charging, client termination

This scenario is based on Appendix A: Flow I in RFC 4006 and Figure 5.2.2.3.1.1 in 3GPP TS 32.299. With unit type substitution, it also reflects Figure 5.2.2.3.2.1 in 3GPP TS 32.299. With unit type substitution and no interim interrogation, it also reflects Figure 5.2.2.2.1.1, Figure 5.2.2.2.2.1, and Figure 5.2.2.2.3.1 in 3GPP TS 32.299.

5.1.3 Successful Single Session Charging, Reauthorization

A user begins a single-session charging interaction through a data service. The initial reservation is successful, but the OCS indicates that no more reservations will be possible. The user tops up their account via an external mechanism, and the OCS requests that the ongoing data session reauthenticate to use the new credit. The charging client requests additional data from the OCS. The OCS commits the used quota from the initial reservation and grants additional quota to the user. The session continues normally.

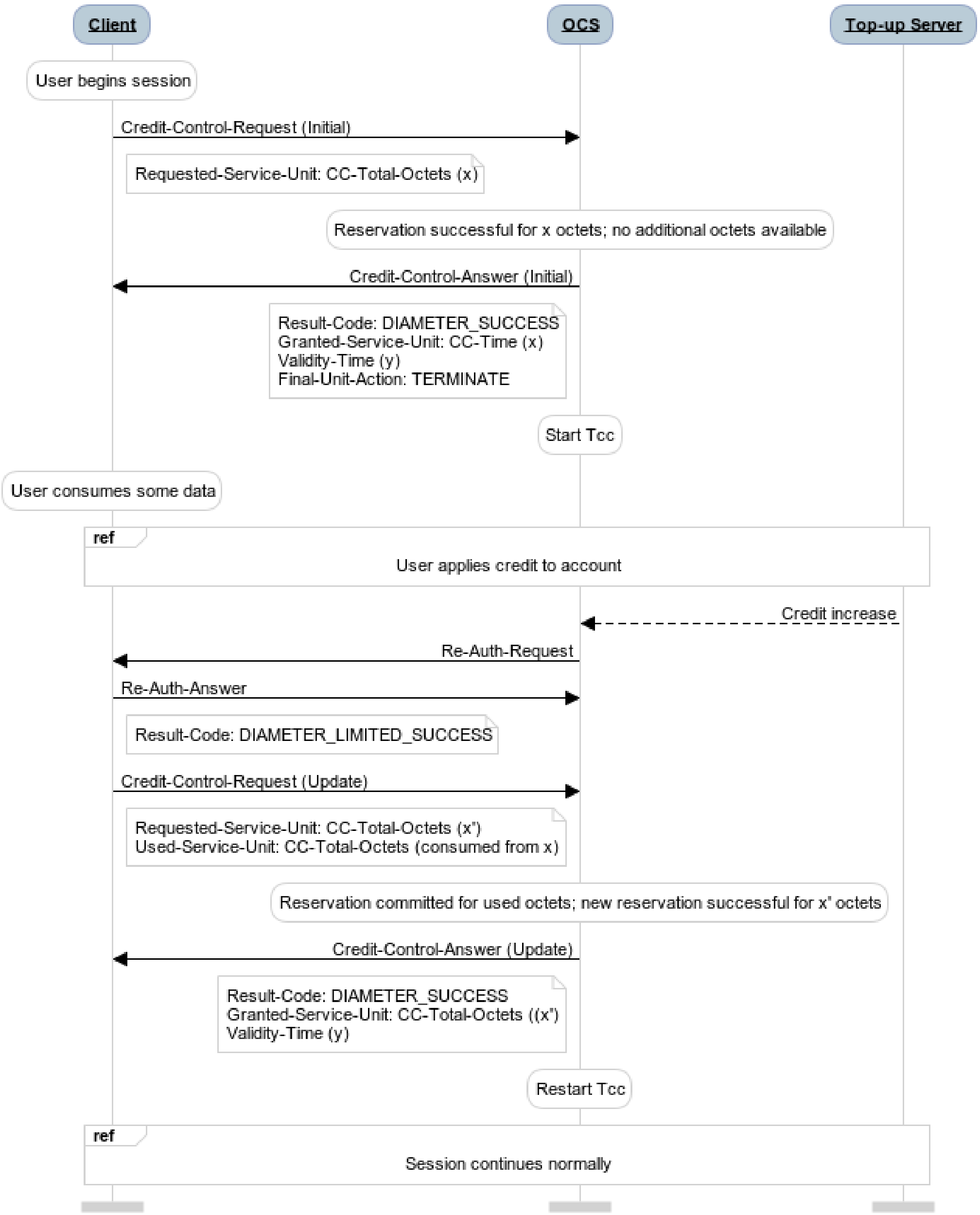
Client
OCS
Top-up Server
User begins session
Credit-Control-Request (Initial)
Requested-Service-Unit: CC-Total-Octets (x)
Reservation successful for x octets; no additional octets available
Credit-Control-Answer (Initial)
Result-Code: DIAMETER_SUCCESS
Granted-Service-Unit: CC-Time (x)
Validity-Time (y)
Final-Unit-Action: TERMINATE
Start Tcc
User consumes some data
ref
User applies credit to account
Credit increase
Re-Auth-Request
Re-Auth-Answer
Result-Code: DIAMETER_LIMITED_SUCCESS
Credit-Control-Request (Update)
Requested-Service-Unit: CC-Total-Octets (x')
Used-Service-Unit: CC-Total-Octets (consumed from x)
Reservation committed for used octets; new reservation successful for x' octets
Credit-Control-Answer (Update)
Result-Code: DIAMETER_SUCCESS
Granted-Service-Unit: CC-Total-Octets ((x')
Validity-Time (y)
Restart Tcc
ref
Session continues normally

Figure C: Successful single session charging, reauthorization

This scenario is based on Appendix A: Flow VIII in RFC 4006.

5.1.4 Successful Single Session Charging, Validity Expiration

A user begins a single-session charging interaction through a data service. The initial reservation is successful, and the user continues using data. The user does not use all the granted data quota before the validity period expires. The charging client relinquishes the granted quota and requests additional data from the OCS. The OCS commits the used quota from the initial reservation and grants additional quota to the user. The session continues normally.

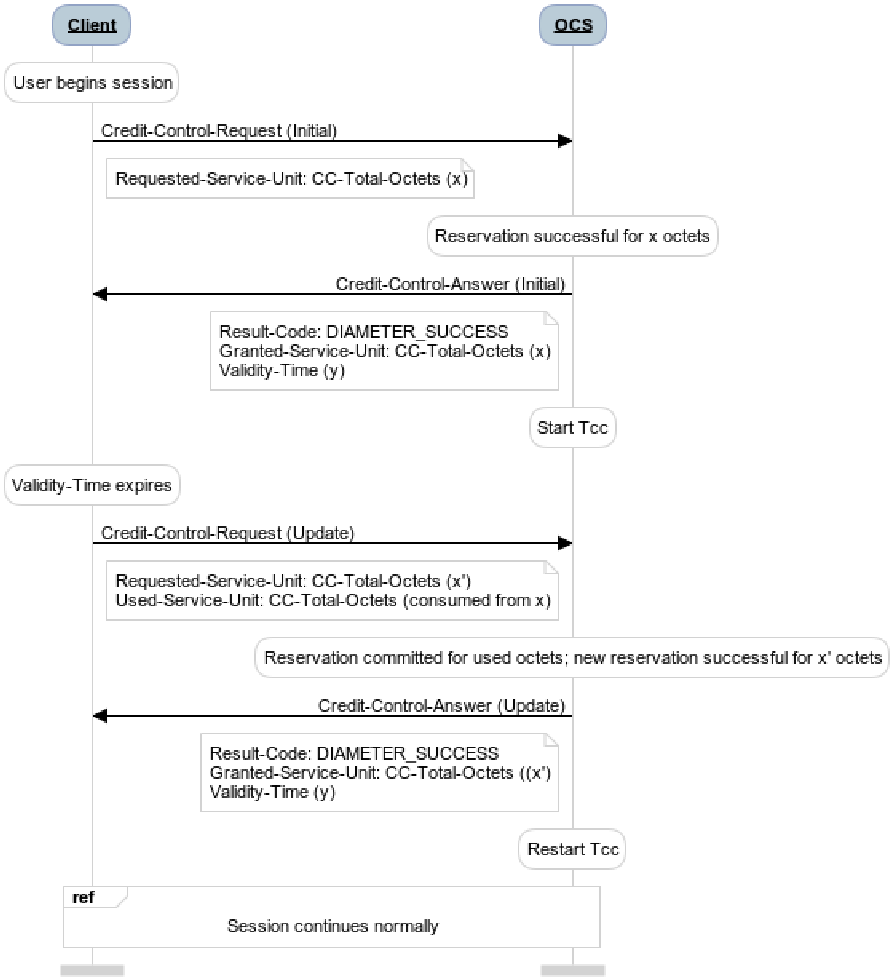
Client
OCS
User begins session
Credit-Control-Request (Initial)
Requested-Service-Unit: CC-Total-Octets (x)
Reservation successful for x octets
Credit-Control-Answer (Initial)
Result-Code: DIAMETER_SUCCESS
Granted-Service-Unit: CC-Total-Octets (x)
Validity-Time (y)
Start Tcc
Validity-Time expires
Credit-Control-Request (Update)
Requested-Service-Unit: CC-Total-Octets (x')
Used-Service-Unit: CC-Total-Octets (consumed from x)
Reservation committed for used octets; new reservation successful for x' octets
Credit-Control-Answer (Update)
Result-Code: DIAMETER_SUCCESS
Granted-Service-Unit: CC-Total-Octets ((x')
Validity-Time (y)
Restart Tcc
ref
Session continues normally

Figure D: Successful single session charging, validity expiration

5.1.5 Unsuccessful Single Session Charging

A user begins a voice call. No quota is granted by the OCS for the indicated reason returned to the charging client.

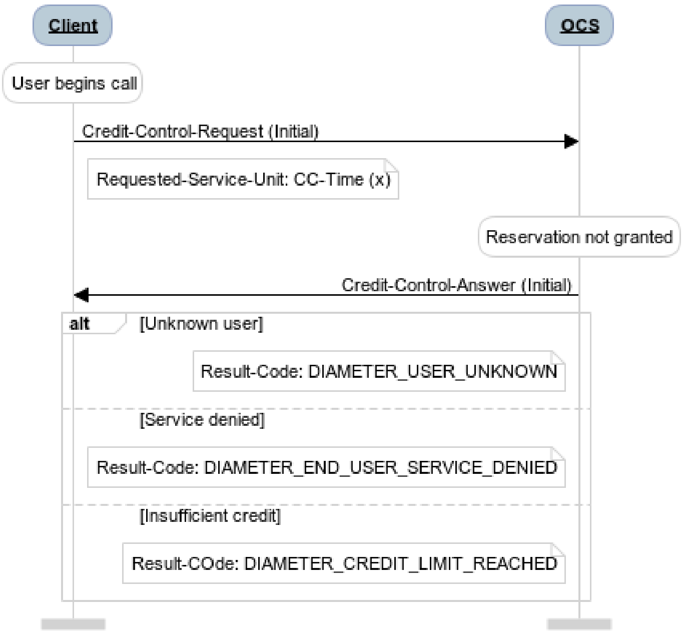
Client
OCS
User begins call
Credit-Control-Request (Initial)
Requested-Service-Unit: CC-Time (x)
Reservation not granted
Credit-Control-Answer (Initial)
alt
[Unknown user]
Result-Code: DIAMETER_USER_UNKNOWN
[Service denied]
Result-Code: DIAMETER_END_USER_SERVICE_DENIED
[Insufficient credit]
Result-COde: DIAMETER_CREDIT_LIMIT_REACHED

Figure E: Unsuccessful single session charging

5.2 Multiple Session Charging

5.2.1 Unsuccessful Multiple Session Charging

A user requests a new service during an existing MSCC session. The OCS does not grant the request. The parent session continues uninterrupted.

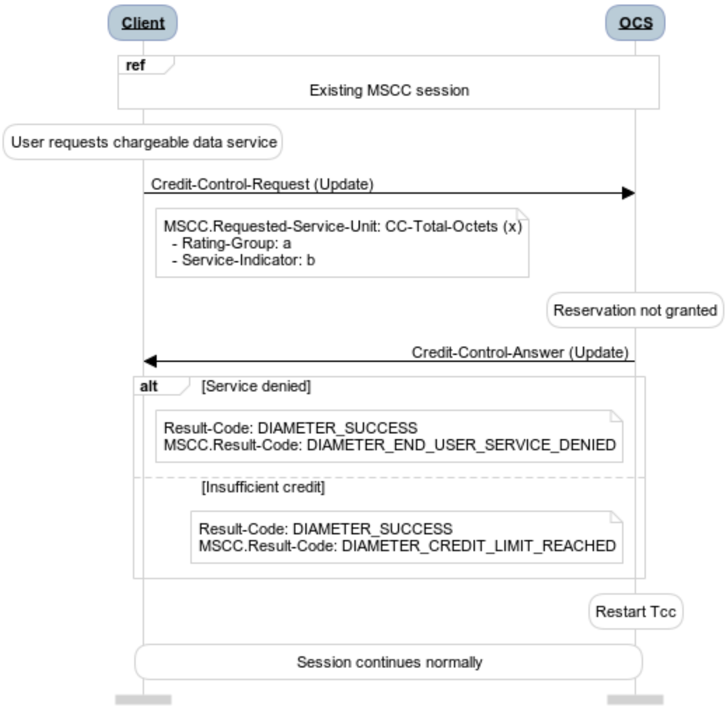
Client
OCS
ref
Existing MSCC session
User requests chargeable data service
Credit-Control-Request (Update)
MSCC.Requested-Service-Unit: CC-Total-Octets (x)
- Rating-Group: a
- Service-Indicator: b
Reservation not granted
Credit-Control-Answer (Update)
alt
[Service denied]
Result-Code: DIAMETER_SUCCESS
MSCC.Result-Code: DIAMETER_END_USER_SERVICE_DENIED
[Insufficient credit]
Result-Code: DIAMETER_SUCCESS
MSCC.Result-Code: DIAMETER_CREDIT_LIMIT_REACHED
Restart Tcc
Session continues normally

Figure F: Unsuccessful multiple session charging

5.2.2 Successful Multiple Session Charging

A user begins a charging control session when the OCS is configured for MSCC. Each service is charged separately within a single parent session. Note that multiple MSCC AVPs may be present in a single request, but this is not shown for the sake of brevity.

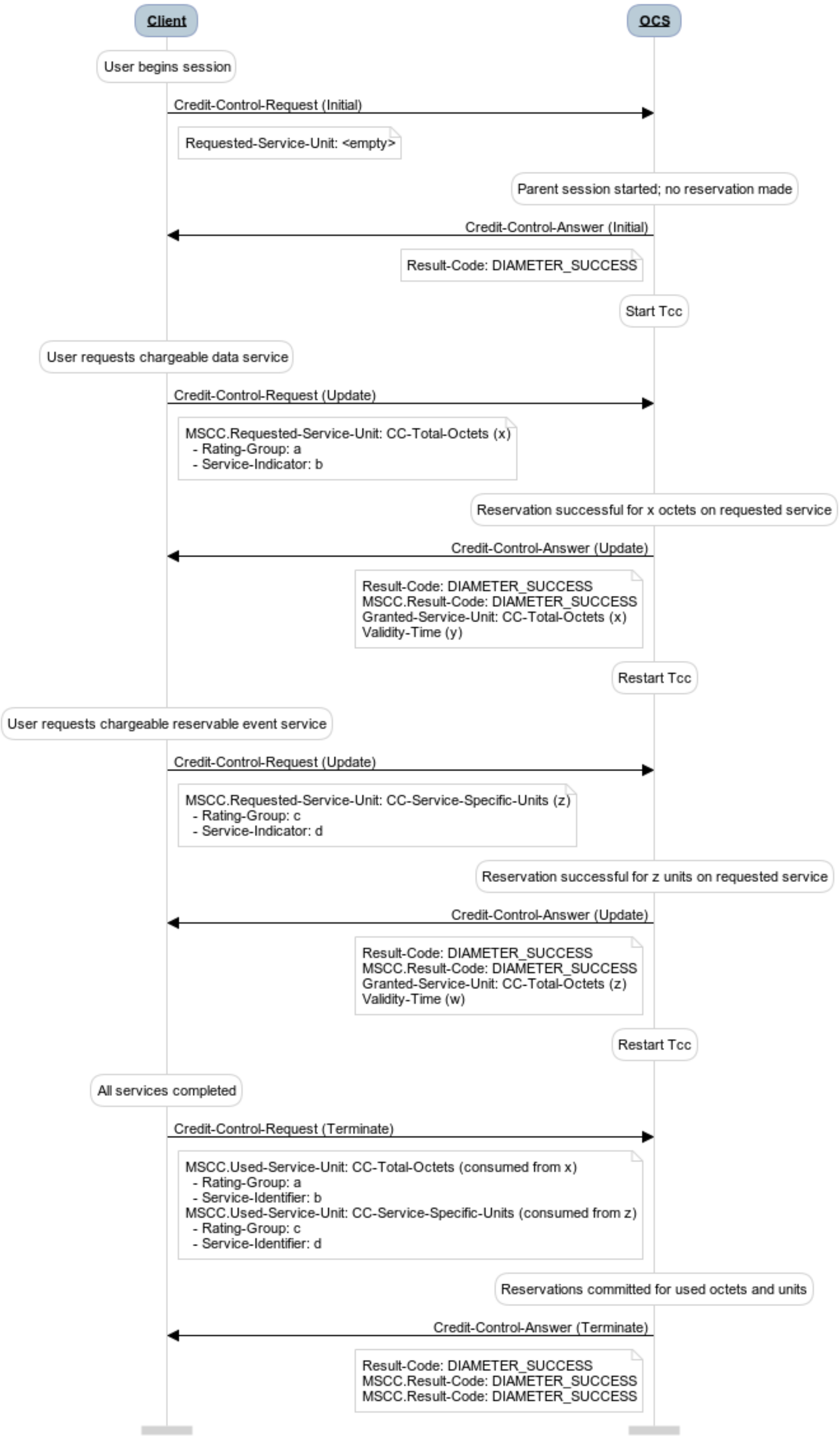
Client
OCS
User begins session
Credit-Control-Request (Initial)
Requested-Service-Unit: <empty>
Parent session started; no reservation made
Credit-Control-Answer (Initial)
Result-Code: DIAMETER_SUCCESS
Start Tcc
User requests chargeable data service
Credit-Control-Request (Update)
MSCC.Requested-Service-Unit: CC-Total-Octets (x)
- Rating-Group: a
- Service-Indicator: b
Reservation successful for x octets on requested service
Credit-Control-Answer (Update)
Result-Code: DIAMETER_SUCCESS
MSCC.Result-Code: DIAMETER_SUCCESS
Granted-Service-Unit: CC-Total-Octets (x)
Validity-Time (y)
Restart Tcc
User requests chargeable reservable event service
Credit-Control-Request (Update)
MSCC.Requested-Service-Unit: CC-Service-Specific-Units (z)
- Rating-Group: c
- Service-Indicator: d
Reservation successful for z units on requested service
Credit-Control-Answer (Update)
Result-Code: DIAMETER_SUCCESS
MSCC.Result-Code: DIAMETER_SUCCESS
Granted-Service-Unit: CC-Total-Octets (z)
Validity-Time (w)
Restart Tcc
All services completed
Credit-Control-Request (Terminate)
MSCC.Used-Service-Unit: CC-Total-Octets (consumed from x)
- Rating-Group: a
- Service-Identifier: b
MSCC.Used-Service-Unit: CC-Service-Specific-Units (consumed from z)
- Rating-Group: c
- Service-Identifier: d
Reservations committed for used octets and units
Credit-Control-Answer (Terminate)
Result-Code: DIAMETER_SUCCESS
MSCC.Result-Code: DIAMETER_SUCCESS
MSCC.Result-Code: DIAMETER_SUCCESS

Figure G: Successful multiple session charging

This scenario is based on Appendix A: Flow IX in RFC 4006.

5.3 Single Event Charging

5.3.1 Successful Single Event Charging

A user requests an event-based service. The OCS grants the requested number of units, and the user is granted service.

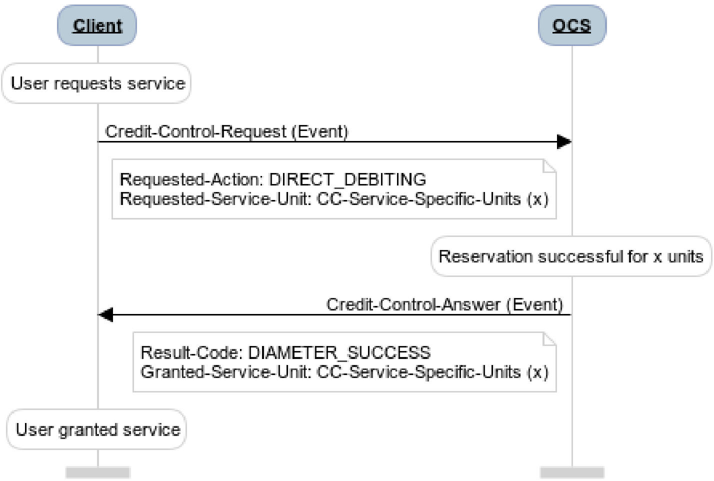
Client
OCS
User requests service
Credit-Control-Request (Event)
Requested-Action: DIRECT_DEBITING
Requested-Service-Unit: CC-Service-Specific-Units (x)
Reservation successful for x units
Credit-Control-Answer (Event)
Result-Code: DIAMETER_SUCCESS
Granted-Service-Unit: CC-Service-Specific-Units (x)
User granted service

Figure H: Successful single event charging

This scenario is based on Appendix A: Flow III in RFC 4006 and Figure 5.2.2.1.1.1 in 3GPP TS 32.299. WIth unit substitution, it also reflects both Figure 5.2.2.1.2.1 and Figure 5.2.2.1.3.1 in 3GPP TS 32.299.

5.3.2 Successful Single Event Refund

Delivery of a debited service to a user is unsuccessful. The OCS refunds the requested number of units to the user's account.

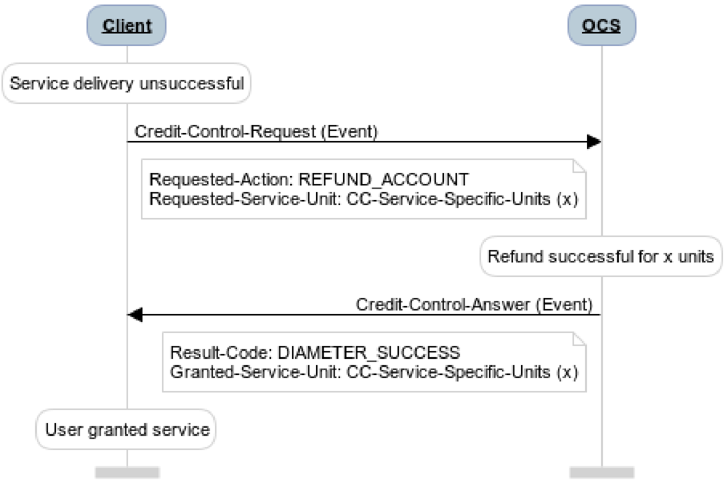
Client
OCS
Service delivery unsuccessful
Credit-Control-Request (Event)
Requested-Action: REFUND_ACCOUNT
Requested-Service-Unit: CC-Service-Specific-Units (x)
Refund successful for x units
Credit-Control-Answer (Event)
Result-Code: DIAMETER_SUCCESS
Granted-Service-Unit: CC-Service-Specific-Units (x)
User granted service

Figure I: Successful single event refund

This scenario is based on Appendix A: Flow VI in RFC 4006.

5.3.3 Successful Multiple Session Charging, Validity Expiration

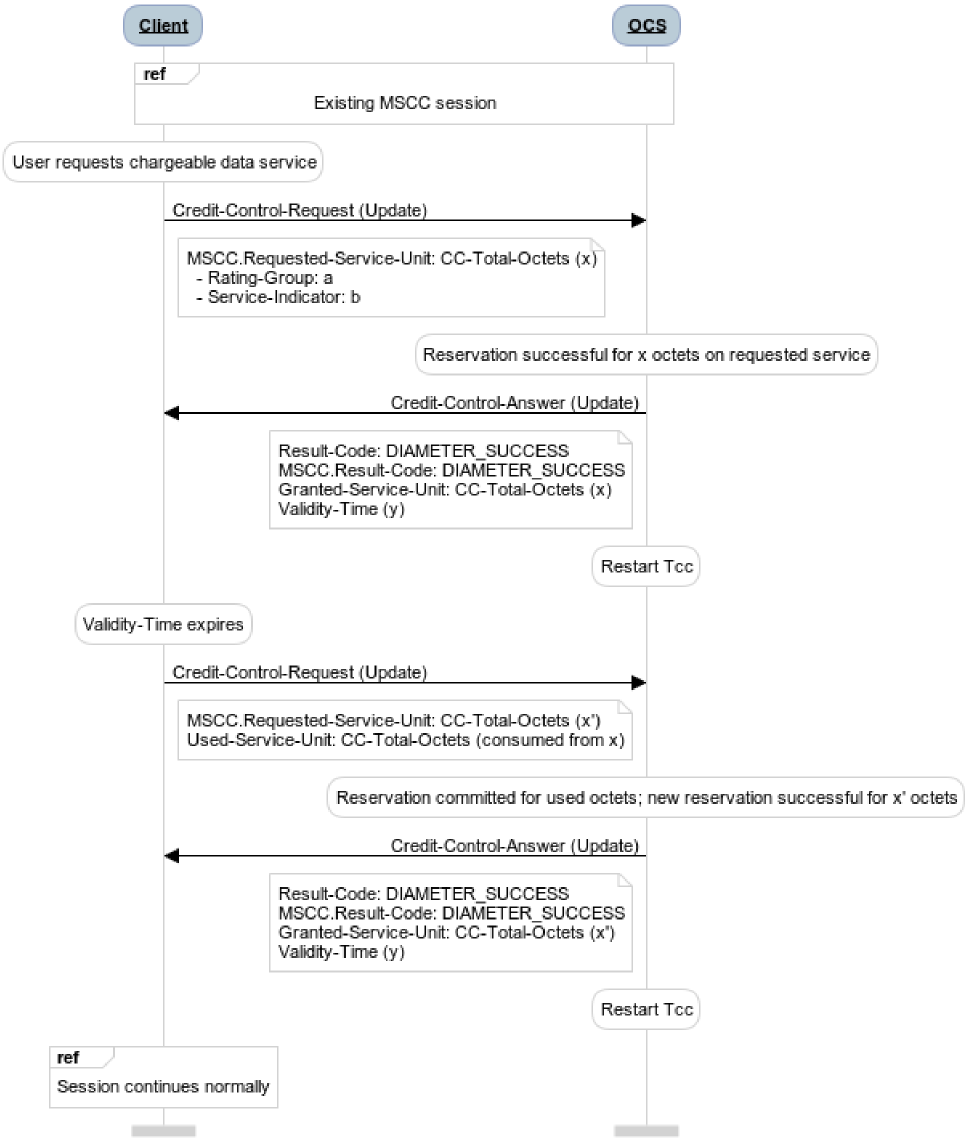
Client
OCS
ref
Existing MSCC session
User requests chargeable data service
Credit-Control-Request (Update)
MSCC.Requested-Service-Unit: CC-Total-Octets (x)
- Rating-Group: a
- Service-Indicator: b
Reservation successful for x octets on requested service
Credit-Control-Answer (Update)
Result-Code: DIAMETER_SUCCESS
MSCC.Result-Code: DIAMETER_SUCCESS
Granted-Service-Unit: CC-Total-Octets (x)
Validity-Time (y)
Restart Tcc
Validity-Time expires
Credit-Control-Request (Update)
MSCC.Requested-Service-Unit: CC-Total-Octets (x')
Used-Service-Unit: CC-Total-Octets (consumed from x)
Reservation committed for used octets; new reservation successful for x' octets
Credit-Control-Answer (Update)
Result-Code: DIAMETER_SUCCESS
MSCC.Result-Code: DIAMETER_SUCCESS
Granted-Service-Unit: CC-Total-Octets (x')
Validity-Time (y)
Restart Tcc
ref
Session continues normally

Figure J: Successful multiple session charging, validity expiration

5.4 Other Charging Scenarios

5.4.1 Unsuccessful Session Charging, Tcc Timeout

A user begins a chargeable data session. The charging client does not respond before the Tcc timer expires, and the session is forcibly disconnected by the OCS.

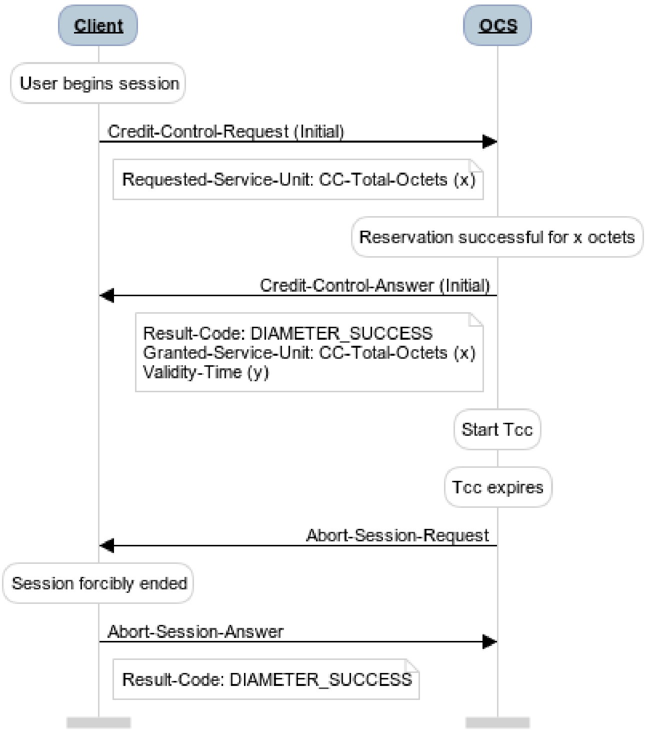
Client
OCS
User begins session
Credit-Control-Request (Initial)
Requested-Service-Unit: CC-Total-Octets (x)
Reservation successful for x octets
Credit-Control-Answer (Initial)
Result-Code: DIAMETER_SUCCESS
Granted-Service-Unit: CC-Total-Octets (x)
Validity-Time (y)
Start Tcc
Tcc expires
Abort-Session-Request
Session forcibly ended
Abort-Session-Answer
Result-Code: DIAMETER_SUCCESS

Figure K: Unsuccessful session charging, Tcc timeout

6 RFC Compliance

6.1 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	Not applicable.	-
2.7	Routing Table	Fully compliant.	-
2.8	Role of Diameter Agents	Not applicable.	-
2.8.1	Relay Agents	Not applicable.	-
2.8.2	Proxy Agents	Not applicable.	-
2.8.3	Redirect Agents	Not applicable.	-
2.8.4	Translation Agents	Not applicable.	-
2.9	Diameter Path Authorization	Fully compliant.	-
3	Diameter Header	Fully compliant.	-
3.1	Command Codes	Partially compliant.	ACR/ACA not supported.
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	Not compliant.	Forwarding not supported.
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.	Forwarding not supported.
6.1.9	Relaying and Proxying Requests	Not compliant.	Forwarding not supported.
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	Not applicable.	-
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.	Forwarding not supported.
6.13	Redirect-Host-Usage AVP	Not compliant.	Forwarding not supported.
6.14	Redirect-Max-Cache-Time AVP	Not compliant.	Forwarding 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	Not applicable.	Not used for credit control.
8.1	Authorization Session State Machine	Fully compliant.	-
8.2	Accounting Session State Machine	Not applicable.	Not used for credit control.
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	Not applicable.	Not used for credit control.
8.4.2	Session-Termination-Answer	Not applicable.	Not used for credit control.
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	Fully compliant.	Session state is not inferred from Origin-State-Id.
8.7	Auth-Request-Type AVP	Not applicable.	Not used for credit control.
8.8	Session-Id AVP	Fully compliant.	-
8.9	Authorization-Lifetime AVP	Not applicable.	Not used for credit control.
8.10	Auth-Grace-Period AVP	Not applicable.	Not used for credit control.
8.11	Auth-Session-State AVP	Not applicable.	Not used for credit control.
8.12	Re-Auth-Request-Type AVP	Not applicable.	Not used for credit control.
8.13	Session-Timeout AVP	Not applicable.	Not used for credit control.
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	Not applicable.	Not used for credit control.
8.18	Session-Server-Failover AVP	Not applicable.	Not used for credit control.
8.19	Multi-Round-Time-Out AVP	Not applicable.	Not used for credit control.

Section	Section Heading	Compliance	Notes
8.20	Class AVP	Not compliant.	-
8.21	Event-Timestamp AVP	Fully compliant.	-
9	Accounting	Not applicable.	Not used for credit control.
9.1	Server Directed Model	Not applicable.	Not used for credit control.
9.2	Protocol Messages	Not applicable.	Not used for credit control.
9.3	Accounting Application Extension and Requirements	Not applicable.	Not used for credit control.
9.4	Fault Resilience	Not applicable.	Not used for credit control.
9.5	Accounting Records	Not applicable.	Not used for credit control.
9.6	Correlation of Accounting Records	Not applicable.	Not used for credit control.
9.7	Accounting Command Codes	Not applicable.	Not used for credit control.
9.7.1	Accounting-Request	Not applicable.	Not used for credit control.
9.7.2	Accounting-Answer	Not applicable.	Not used for credit control.
9.8	Accounting AVPs	Not applicable.	Not used for credit control.
9.8.1	Accounting-Record-Type AVP	Not applicable.	Not used for credit control.
9.8.2	Acct-Interim-Interval AVP	Not applicable.	Not used for credit control.
9.8.3	Accounting-Record-Number AVP	Not applicable.	Not used for credit control.
9.8.4	Acct-Session-Id AVP	Not applicable.	Not used for credit control.
9.8.5	Acct-Multi-Session-Id AVP	Not applicable.	Not used for credit control.
9.8.6	Accounting-Sub-Session-Id AVP	Not applicable.	Not used for credit control.
9.8.7	Accounting-Realtime-Required AVP	Not applicable.	Not used for credit control.
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	Not applicable.	Not used for credit control.
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	Not applicable.	No vendor-specific command codes.
11.2.2	Command Flags	Fully compliant.	-
11.3	AVP Values	Fully compliant.	-
11.3.1	Experimental-Result-Code AVP	Not applicable.	No experimental result codes.

Section	Section Heading	Compliance	Notes
11.3.2	Result-Code AVP Values	Not applicable.	No IANA control required.
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.	-

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

Table 12: OCS compliance to RFC 6733

6.2 Compliance to RFC 4006 (Diameter Credit Control Application)

Section	Section Heading	Compliance	Notes
1	Introduction	Not applicable.	-
1.1	Requirements Language	Not applicable.	-
1.2	Terminology	Not applicable.	-
1.3	Advertising Application Support	Fully compliant.	-
2	Architecture Models	Fully compliant.	-
3	Credit-Control Messages	Fully compliant.	-
3.1	Credit-Control-Request (CCR) Command	Fully compliant.	-
3.2	Credit-Control-Answer (CCA) Command	Fully compliant.	-
4	Credit-Control Application Overview	Fully compliant.	-
4.1	Service-Specific Rating Input and Interoperability	Fully compliant.	-
4.1.1	Specifying Rating Input AVPs	Fully compliant.	-
4.1.2	Service-Specific Documentation	Fully compliant.	-
4.1.3	Handling of Unsupported/Incorrect Rating Input	Fully compliant.	-
4.1.4	RADIUS Vendor-Specific Rating Attributes	Fully compliant.	-
5	Session Based Credit-Control	Not applicable.	-
5.1	General Principles	Fully compliant.	-
5.1.1	Basic Tariff-Time Change Support	Not compliant.	Validity-Time is used instead of the tariff change mechanism.
5.1.2	Credit-Control for Multiple Services within a (sub-)Session	Partially compliant.	GSU pooling and tariff time change not supported.
5.2	First Interrogation	Fully compliant.	-
5.2.1	First Interrogation after Authorization and Authentication	Fully compliant.	-

Section	Section Heading	Compliance	Notes
5.2.2	Authorization Messages for First Interrogation	Fully compliant.	-
5.3	Intermediate Interrogation	Fully compliant.	-
5.4	Final Interrogation	Fully compliant.	-
5.5	Server-Initiated Credit Re-Authorization	Fully compliant.	-
5.6	Graceful Service Termination	Fully compliant.	-
5.6.1	Terminate Action	Fully compliant.	-
5.6.2	Redirect Action	Fully compliant.	-
5.6.3	Restrict Access Action	Not compliant.	-
5.6.4	Usage of the Server-Initiated Credit Re-Authorization	Fully compliant.	-
5.7	Failure Procedures	Fully compliant.	-
6	One Time Event	Fully compliant.	-
6.1	Service Price Enquiry	Not compliant.	-
6.2	Balance Check	Not compliant.	-
6.3	Direct Debiting	Fully compliant.	-
6.4	Refund	Fully compliant.	-
6.5	Failure Procedure	Fully compliant.	-
7	Credit-Control Application State Machine	Fully compliant.	-
8	Credit-Control AVPs	Not applicable.	-
8.1	CC-Correlation-Id AVP	Fully compliant.	-
8.2	CC-Request-Number AVP	Fully compliant.	-
8.3	CC-Request-Type AVP	Fully compliant.	-
8.4	CC-Session-Failover AVP	Fully compliant.	-
8.5	CC-Sub-Session-Id AVP	Fully compliant.	-
8.6	Check-Balance-Result AVP	Not compliant.	-
8.7	Cost-Information AVP	Not compliant.	-
8.8	Unit-Value AVP	Fully compliant.	-
8.9	Exponent AVP	Fully compliant.	-
8.10	Value-Digits AVP	Fully compliant.	-
8.11	Currency-Code AVP	Fully compliant.	-
8.12	Cost-Unit AVP	Fully compliant.	-
8.13	Credit-Control AVP	Fully compliant.	-
8.14	Credit-Control-Failure-Handling AVP	Fully compliant.	-
8.15	Direct-Debiting-Failure-Handling AVP	Fully compliant.	-

Section	Section Heading	Compliance	Notes
8.16	Multiple-Services-Credit-Control AVP	Partially compliant.	GSU pooling and tariff time change not supported. Only a single Service-Indicator is supported. Only a single Used-Service-Unit is supported.
8.17	Granted-Service-Unit AVP	Partially compliant.	Only a single unit type is supported.
8.18	Requested-Service-Unit AVP	Partially compliant.	Only a single unit type is supported.
8.19	Used-Service-Unit AVP	Partially compliant.	Only a single unit type is supported.
8.20	Tariff-Time-Change AVP	Not compliant.	-
8.21	CC-Time AVP	Fully compliant.	-
8.22	CC-Money AVP	Fully compliant.	-
8.23	CC-Total-Octets AVP	Fully compliant.	-
8.24	CC-Input-Octets AVP	Fully compliant.	-
8.25	CC-Output-Octets AVP	Fully compliant.	-
8.26	CC-Service-Specific-Units AVP	Fully compliant.	-
8.27	Tariff-Change-Usage AVP	Not compliant.	-
8.28	Service-Identifier AVP	Partially compliant.	Only a single Service-Indicator is supported.
8.29	Rating-Group AVP	Fully compliant.	-
8.30	G-S-U-Pool-Reference AVP	Not compliant.	-
8.31	G-S-U-Pool-Identifier AVP	Not compliant.	-
8.32	CC-Unit-Type AVP	Not compliant.	-
8.33	Validity-Time AVP	Fully compliant.	-
8.34	Final-Unit-Indication AVP	Fully compliant.	-
8.35	Final-Unit-Action AVP	Partially compliant.	Restricted access is not supported.
8.36	Restriction-Filter-Rule AVP	Not compliant.	-
8.37	Redirect-Server AVP	Fully compliant.	-
8.38	Redirect-Address-Type AVP	Fully compliant.	-
8.39	Redirect-Server-Address AVP	Fully compliant.	-
8.40	Multiple-Services-Indicator AVP	Fully compliant.	-
8.41	Requested-Action AVP	Partially compliant.	Values 2 (CHECK_BALANCE) and 3 (PRICE_ENQUIRY) not supported.
8.42	Service-Context-Id AVP	Fully compliant.	-
8.43	Service-Parameter-Info AVP	Fully compliant.	-
8.44	Service-Parameter-Type AVP	Fully compliant.	-
8.45	Service-Parameter-Value AVP	Fully compliant.	-
8.46	Subscription-Id AVP	Fully compliant.	-

Section	Section Heading	Compliance	Notes
8.47	Subscription-Id-Type AVP	Fully compliant.	-
8.48	Subscription-Id-Data AVP	Fully compliant.	-
8.49	User-Equipment-Info AVP	Fully compliant.	-
8.50	User-Equipment-Info-Type AVP	Fully compliant.	-
8.51	User-Equipment-Info-Value AVP	Fully compliant.	-
9	Result Code AVP Values	Fully compliant.	-
9.1	Transient Failures	Fully compliant.	-
9.2	Permanent Failures	Fully compliant.	-
10	AVP Occurrence Table	Fully compliant.	-
10.1	Credit-Control AVP Table	Fully compliant.	-
10.2	Re-Auth-Request/Answer AVP Table	Fully compliant.	-
11	RADIUS/Diameter Credit-Control Interworking Model	Fully compliant.	-
12	IANA Considerations	Not applicable.	-
12.1	Application Identifier	Fully compliant.	-
12.2	Command Codes	Fully compliant.	-
12.3	AVP Codes	Fully compliant.	-
12.4	Result-Code AVP Values	Fully compliant.	-
12.5	CC-Request-Type AVP	Fully compliant.	-
12.6	CC-Session-Failover AVP	Fully compliant.	-
12.7	CC-Unit-Type AVP	Fully compliant.	-
12.8	Check-Balance-Result AVP	Fully compliant.	-
12.9	Credit-Control AVP	Fully compliant.	-
12.10	Credit-Control-Failure-Handling AVP	Fully compliant.	-
12.11	Direct-Debiting-Failure-Handling AVP	Fully compliant.	-
12.12	Final-Unit-Action AVP	Fully compliant.	-
12.13	Multiple-Services-Indicator AVP	Fully compliant.	-
12.14	Redirect-Address-Type AVP	Fully compliant.	-
12.15	Requested-Action AVP	Fully compliant.	-
12.16	Subscription-Id-Type AVP	Fully compliant.	-
12.17	Tariff-Change-Usage AVP	Not compliant.	-
12.18	User-Equipment-Info-Type AVP	Fully compliant.	-
13	Credit-Control Application Related Parameters	Fully compliant.	-

Section	Section Heading	Compliance	Notes
14	Security Considerations	Partially compliant.	IPSec may be applied via an external gateway. TLS/DTLS not supported.
14.1	Direct Connection with Redirects	Not applicable.	-
15	References	Not applicable.	-
15.1	Normative References	Not applicable.	-
15.2	Informative References	Not applicable.	-
16	Acknowledgements	Not applicable.	-

Table 13: OCS compliance to RFC 4006

6.3 Compliance to 3GPP TS 32.299 (Release 15)

Note that compliance to individual AVP definitions is limited to their defined purpose within the 3GPP message flow structure; the OCS supports arbitrary AVP definitions for use in rating as set out in section 4.4: Credit Control Messaging.

Section	Section Heading	Compliance	Notes
-	Foreword	Not applicable.	-
1	Scope	Not applicable.	-
2	References	Not applicable.	-
3	Definitions, symbols and abbreviations	Not applicable.	-
3.1	Definitions	Not applicable.	-
3.2	Symbols	Not applicable.	-
3.3	Abbreviations	Not applicable.	-
4	Architecture considerations	Not applicable.	-
4.1	High level architecture	Not applicable.	-
4.1.0	General	Fully compliant.	OCS functions as OCF over Ro.
4.1.1	Charging related transfer requirements	Not applicable.	-
5	3GPP charging applications requirements	Not applicable.	-
5.1	Offline charging scenarios	Not applicable.	OCS functions as online charging.
5.1.1	Basic principles	Not applicable.	OCS functions as online charging.
5.1.1.0	Introduction	Not applicable.	OCS functions as online charging.
5.1.1.1	Event based charging	Not applicable.	OCS functions as online charging.
5.1.1.2	Session based charging	Not applicable.	OCS functions as online charging.
5.1.2	Basic operation	Not applicable.	OCS functions as online charging.
5.2	Online charging scenarios	Not applicable.	-
5.2.0	Introduction	Fully compliant.	OCS functions as OCF over Ro.
5.2.1	Basic principles	Fully compliant.	-
5.2.2	Charging scenarios	Not applicable.	-
5.2.2.0	Introduction	Fully compliant.	-

Section	Section Heading	Compliance	Notes
5.2.2.1	Immediate Event Charging (IEC)	Fully compliant.	Supported with CCR/CCA.
5.2.2.1.1	Decentralized Unit Determination and Centralized Rating	Fully compliant.	Supported with CCR/CCA.
5.2.2.1.2	Centralized Unit Determination and Centralized Rating	Fully compliant.	Supported with CCR/CCA.
5.2.2.1.3	Decentralized Unit Determination and Decentralized Rating	Fully compliant.	Supported with CCR/CCA.
5.2.2.1.4	Further options	Not applicable.	Service delivery is not an OCF function.
5.2.2.2	Event Charging with Unit Reservation (ECUR)	Fully compliant.	Supported with CCR/CCA.
5.2.2.2.1	Decentralized Unit Determination and Centralized Rating	Fully compliant.	Supported with CCR/CCA.
5.2.2.2.2	Centralized Unit Determination and Centralized Rating	Fully compliant.	Supported with CCR/CCA.
5.2.2.2.3	Decentralized Unit Determination and Decentralized Rating	Fully compliant.	Supported with CCR/CCA.
5.2.2.3	Session charging with Reservation	Fully compliant.	Supported with CCR/CCA.
5.2.2.3.1	Decentralized Unit Determination and Centralized Rating	Fully compliant.	Supported with CCR/CCA.
5.2.2.3.2	Centralized Unit Determination and Centralized Rating	Fully compliant.	Supported with CCR/CCA.
5.2.2.3.3	Decentralized Unit Determination and Decentralized Rating	Fully compliant.	Supported with CCR/CCA.
5.2.3	Basic operations	Partially compliant.	Supported with CCR/CCA. Forwarding not supported.
5.3	Other requirements	Not applicable.	-
5.3.1	Re-authorization	Fully compliant.	-
5.3.2	Threshold based re-authorization triggers	Not compliant.	-
5.3.3	Termination action	Fully compliant.	-
5.3.4	Account expiration	Not compliant.	-
6	3GPP charging applications – Protocol aspects	Not applicable.	-
6.1	Basic principles for Diameter offline charging	Not applicable.	-

Section	Section Heading	Compliance	Notes
6.1.0	Introduction	Not applicable.	OCS functions as online charging.
6.1.1	Event based charging	Not applicable.	OCS functions as online charging.
6.1.2	Session based charging	Not applicable.	OCS functions as online charging.
6.1.3	Offline charging error cases - Diameter procedures	Not applicable.	OCS functions as online charging.
6.1.3.1	CDF connection failure	Not applicable.	OCS functions as online charging.
6.1.3.2	No reply from CDF	Not applicable.	OCS functions as online charging.
6.1.3.3	Duplicate detection	Not applicable.	OCS functions as online charging.
6.1.3.4	CDF detected failure	Not applicable.	OCS functions as online charging.
6.2	Message contents for offline charging	Not applicable.	OCS functions as online charging.
6.2.1	Summary of offline charging message formats	Not applicable.	OCS functions as online charging.
6.2.1.1	General	Not applicable.	OCS functions as online charging.
6.2.1.2	Structure for the Accounting message formats	Not applicable.	OCS functions as online charging.
6.2.2	Accounting-Request message	Not applicable.	OCS functions as online charging.
6.2.3	Accounting-Answer (ACA) message	Not applicable.	OCS functions as online charging.
6.3	Basic principles for Diameter online charging	Not applicable.	-
6.3.1	Online Specific Credit-Control application requirements	Fully compliant.	-
6.3.2	Diameter description on the Ro reference point	Not applicable.	-
6.3.2.1	Basic principles	Fully compliant.	-
6.3.3	Immediate Event Charging (IEC)	Partially compliant.	CHECK_BALANCE and PRICE_ENQUIRY not supported.
6.3.4	Event Charging with Unit Reservation (ECUR)	Partially compliant.	Cost and balance information not supported.
6.3.5	Session Charging with Unit Reservation (SCUR)	Partially compliant.	Cost and balance information not supported.
6.3.6	Error cases and scenarios	Not applicable.	-
6.3.6.0	Introduction	Not applicable.	-
6.3.6.1	Duplicate detection	Fully compliant.	-
6.3.6.2	Reserve Units / Debit Units operation failure	Not applicable.	-
6.3.7	Support of tariff changes during an active user session	Not applicable.	-

Section	Section Heading	Compliance	Notes
6.3.7.1	Support of tariff changes using the tariff switch mechanism	Not compliant.	Validity-Time is used instead of the tariff change mechanism.
6.3.7.2	Support of tariff changes using Validity-Time AVP	Fully compliant.	-
6.3.8	Support of re-authorization	Fully compliant.	-
6.3.9	Support of failure handling	Not applicable.	-
6.3.10	Support of failover	Not applicable.	-
6.3.11	Credit pooling	Not compliant.	-
6.4	Message formats for online charging	Not applicable.	-
6.4.1	Summary of online charging message formats	Not applicable.	-
6.4.1.1	General	Fully compliant.	-
6.4.1.2	Structure for the Credit-Control message formats	Fully compliant.	-
6.4.2	Credit-Control-Request message	Partially compliant.	Advice of charge and forwarding not supported. Refer to individual AVP compliance.
6.4.3	Credit-Control-Answer message	Partially compliant.	Cost information, balance information, and forwarding not supported. Refer to individual AVP compliance.
6.4.4	Re-Auth-Request message	Partially compliant.	Credit pooling and forwarding not supported. Refer to individual AVP compliance.
6.4.5	Re-Auth-Answer message	Partially compliant.	Credit pooling and forwarding not supported. Refer to individual AVP compliance.
6.4.6	Capabilities-Exchange-Request message	-	Refer to Table 12: OCS compliance to RFC 6733.
6.4.7	Capabilities-Exchange-Answer message	-	Refer to Table 12: OCS compliance to RFC 6733.
6.4.8	Device-Watchdog-Request message	-	Refer to Table 12: OCS compliance to RFC 6733.
6.4.9	Device-Watchdog-Answer message	-	Refer to Table 12: OCS compliance to RFC 6733.
6.4.10	Disconnect-Peer-Request message	-	Refer to Table 12: OCS compliance to RFC 6733.
6.4.11	Disconnect-Peer-Answer message	-	Refer to Table 12: OCS compliance to RFC 6733.
6.4.12	Abort-Session-Request message	-	Refer to Table 12: OCS compliance to RFC 6733.
6.4.13	Abort-Session -Answer message	-	Refer to Table 12: OCS compliance to RFC 6733.

Section	Section Heading	Compliance	Notes
6.5	Other procedural description of the 3GPP charging applications	Not applicable.	-
6.5.1	Re-Authorization	Not applicable.	-
6.5.1.1	Idle timeout	Not compliant.	-
6.5.1.2	Change of charging conditions	Not compliant.	-
6.5.1.3	Reporting quota usage	Partially compliant.	Re-authorization triggers not supported.
6.5.1.4	Quota consumption	Not compliant.	-
6.5.2	Threshold based Re-Authorization triggers	Not compliant.	-
6.5.3	Termination action	Fully compliant.	-
6.5.4	Quota consumption time	Not compliant.	Validity-Time is used instead of the quota consumption time mechanism.
6.5.5	Service termination	Fully compliant.	-
6.5.6	Envelope reporting	Not applicable.	-
6.5.6.1	Envelope reporting in Online Charging	Not compliant.	-
6.5.6.2	Envelope reporting in Offline Charging	Not applicable.	OCS functions as online charging.
6.5.6.3	Envelope reporting - Quota consumption time	Not compliant.	-
6.5.6.4	Envelope reporting - Combinational quota	Not compliant.	-
6.5.7	Combinational quota	Not compliant.	-
6.5.8	Online control of offline charging information	Not compliant.	-
6.5.9	Support of multiple service	Fully compliant.	-
6.6	Bindings of the operation to protocol application	Not applicable.	-
6.6.0	General	Fully compliant.	-
6.6.1	Bindings of Charging Data Transfer to Accounting	Not applicable.	Not used for credit control.
6.6.2	Bindings of Debit / Reserve Units to Credit-Control	Fully compliant.	-
6.7	Securing Diameter messages	-	Refer to Table 12: OCS compliance to RFC 6733.
7	Summary of used Attribute Value Pairs	Not applicable.	-
7.1	Diameter AVPs	Not applicable.	-
7.1.0	General	Partially compliant.	Refer to individual AVP compliance.
7.1.1	Accounting-Input-Octets AVP	Not applicable.	Not used for credit control.

Section	Section Heading	Compliance	Notes
7.1.2	Void	Not applicable.	-
7.1.3	Accounting-Output-Octets AVP	Not applicable.	Not used for credit control.
7.1.4	Void	Not applicable.	-
7.1.5	Acct-Application-Id AVP	Not applicable.	Not used for credit control.
7.1.6	Auth-Application-Id AVP	Fully compliant.	-
7.1.7	Called-Station-Id AVP	Fully compliant.	-
7.1.8	Event-Timestamp AVP	Fully compliant.	-
7.1.9	Multiple-Services-Credit-Control AVP	Partially compliant.	GSU pooling, quota management, envelope reporting, triggering, and tariff time change not supported. Only a single Service-Indicator is supported. Only a single Used-Service-Unit is supported. Additional AVPs are supported.
7.1.10	Rating-Group AVP	Fully compliant.	-
7.1.11	Result-Code AVP	Fully compliant.	-
7.1.12	Service-Context-Id AVP	Fully compliant.	-
7.1.13	Service-Identifier AVP	Fully compliant.	-
7.1.14	Used-Service-Unit AVP	Partially compliant.	Only a single unit type is supported.
7.1.15	User-Name AVP	Fully compliant.	-
7.1.16	Vendor-Id AVP	Fully compliant.	-
7.1.17	User-Equipment-Info AVP	Fully compliant.	-
7.2	3GPP specific AVPs	Not applicable.	-
7.2.0	General	Partially compliant.	Refer to individual AVP compliance.
7.2.0A	Access-Network-Info-Change AVP	Fully compliant.	-
7.2.0aA	3GPP-PS-Data-Off-Status AVP	Fully compliant.	-
7.2.1	Access-Network-Information AVP	Fully compliant.	-
7.2.1A	Access-Transfer-Information AVP	Fully compliant.	-
7.2.1B	Access-Transfer-Type AVP	Fully compliant.	-
7.2.2	Account-Expiration AVP	Not compliant.	-
7.2.3	Accumulated-Cost AVP	Not compliant.	-
7.2.4	Adaptations AVP	Fully compliant.	-
7.2.5	Additional-Content-Information AVP	Fully compliant.	-
7.2.5A	Additional-Exception-Reports AVP	Fully compliant.	-
7.2.6	Additional-Type-Information AVP	Fully compliant.	-

Section	Section Heading	Compliance	Notes
7.2.7	Address-Data AVP	Fully compliant.	-
7.2.8	Address-Domain AVP	Fully compliant.	-
7.2.9	Address-Type AVP	Fully compliant.	-
7.2.10	Addressee-Type AVP	Fully compliant.	-
7.2.11	AF-Correlation-Information AVP	Fully compliant.	-
7.2.12	Alternate-Charged-Party-Address AVP	Fully compliant.	-
7.2.12aA	Announcement-Identifier AVP	Not compliant.	-
7.2.12aB	Announcement-Information AVP	Not compliant.	-
7.2.12aC	Announcement-Order AVP	Not compliant.	-
7.2.12aD	Announcing-PLMN-ID AVP	Not compliant.	-
7.2.12A	Announcing-UE-HPLMN-Identifier AVP	Not compliant.	-
7.2.12B	Announcing-UE-VPLMN-Identifier AVP	Not compliant.	-
7.2.13	AoC-Cost-Information AVP	Not compliant.	-
7.2.14	AoC-Format AVP	Not compliant.	-
7.2.15	AoC-Information AVP	Not compliant.	-
7.2.16	AoC-Request-Type AVP	Not compliant.	-
7.2.17	AoC-Service AVP	Not compliant.	-
7.2.18	AoC-Service-Obligatory-Type AVP	Not compliant.	-
7.2.19	AoC-Service-Type AVP	Not compliant.	-
7.2.20	AoC-Subscription-Information AVP	Not compliant.	-
7.2.20A	APN-Rate-Control AVP	Not compliant.	-
7.2.20B	APN-Rate-Control-Downlink AVP	Not compliant.	-
7.2.20C	APN-Rate-Control-Uplink AVP	Not compliant.	-
7.2.21	Applic-ID AVP	Fully compliant.	-
7.2.22	Application-Provided-Called-Party-Address AVP	Fully compliant.	-
7.2.23	Application-Server AVP	Fully compliant.	-
7.2.24	Application-Server-Information AVP	Fully compliant.	-
7.2.24A	Application-Specific-Data AVP	Fully compliant.	-
7.2.25	Associated-Party-Address AVP	Fully compliant.	-
7.2.26	Associated-URI AVP	Fully compliant.	-

Section	Section Heading	Compliance	Notes
7.2.27	Authorised-QoS AVP	Not compliant.	-
7.2.28	Aux-Applic-Info AVP	Fully compliant.	-
7.2.29	Base-Time-Interval AVP	Not compliant.	-
7.2.29A	Basic-Service-Code AVP	Fully compliant.	-
7.2.29B	Bearer-Capability AVP	Fully compliant.	-
7.2.30	Bearer-Service AVP	Fully compliant.	-
7.2.30A	BSSID AVP	Not compliant.	-
7.2.31	Called-Asserted-Identity AVP	Fully compliant.	-
7.2.31A	Called-Identity AVP	Fully compliant.	-
7.2.31B	Called-Identity-Change AVP	Fully compliant.	-
7.2.32	Called-Party-Address AVP	Fully compliant.	-
7.2.33	Calling-Party-Address AVP	Fully compliant.	-
7.2.34	Carrier-Select-Routing-Information AVP	Fully compliant.	-
7.2.35	Cause-Code AVP	Fully compliant.	-
7.2.35A	Cellular-Network-Information AVP	Fully compliant.	-
7.2.36	CG-Address AVP	Fully compliant.	-
7.2.37	Change-Condition AVP	Not compliant.	-
7.2.38	Change-Time AVP	Fully compliant.	-
7.2.38A	Charge-Reason-Code AVP	Fully compliant.	-
7.2.39	Charged-Party AVP	Fully compliant.	-
7.2.39A	Charging-Characteristics-Selection-Mode AVP	Not compliant.	-
7.2.39B	Charging-Per-IP-CAN-Session-Indicator AVP	Not applicable.	OCS functions as online charging.
7.2.40	Class-Identifier AVP	Fully compliant.	-
7.2.41	Client-Address AVP	Fully compliant.	-
7.2.41A	CN-Operator-Selection-Entity AVP	Fully compliant.	-
7.2.42	Content-Class AVP	Fully compliant.	-
7.2.43	Content-Disposition AVP	Not compliant.	-
7.2.44	Content-Length AVP	Fully compliant.	-
7.2.45	Content-Size AVP	Fully compliant.	-
7.2.46	Content-Type AVP	Fully compliant.	-
7.2.46aA	Coverage-Status AVP	Fully compliant.	-
7.2.46aaA	Coverage-Info AVP	Fully compliant.	-
7.2.46abA	CP-CIoT-EPS-Optimisation-Indicator AVP	Not compliant.	-
7.2.46acA	CPDT-Information AVP	Not compliant.	-
7.2.46A	CSG-Access-Mode AVP	Fully compliant.	-

Section	Section Heading	Compliance	Notes
7.2.46B	CSG-Membership-Indication AVP	Not compliant.	-
7.2.47	Current-Tariff AVP	Not compliant.	-
7.2.48	CUG-Information AVP	Not compliant.	-
7.2.49	Data-Coding-Scheme AVP	Fully compliant.	-
7.2.50	DCD-Information AVP	Fully compliant.	-
7.2.51	Deferred-Location-Event-Type AVP	Fully compliant.	-
7.2.52	Delivery-Report-Requested AVP	Fully compliant.	-
7.2.53	Destination-Interface AVP	Fully compliant.	-
7.2.54	Diagnostics AVP	Not compliant.	-
7.2.54A	Discoveree-UE-HPLMN-Identifier AVP	Not compliant.	-
7.2.54B	Discoveree-UE-VPLMN-Identifier AVP	Not compliant.	-
7.2.54C	Discoverer-UE-HPLMN-Identifier AVP	Not compliant.	-
7.2.54D	Discoverer-UE-VPLMN-Identifier AVP	Not compliant.	-
7.2.55	Domain-Name AVP	Fully compliant.	-
7.2.56	DRM-Content AVP	Fully compliant.	-
7.2.57	Dynamic-Address-Flag AVP	Fully compliant.	-
7.2.57A	Dynamic-Address-Flag-Extension AVP	Fully compliant.	-
7.2.58	Early-Media-Description AVP	Not compliant.	-
7.2.58A	Enhanced-Diagnostics AVP	Not compliant.	-
7.2.59	Envelope AVP	Not compliant.	-
7.2.60	Envelope-End-Time AVP	Not compliant.	-
7.2.61	Envelope-Reporting AVP	Not compliant.	-
7.2.62	Envelope-Start-Time AVP	Not compliant.	-
7.2.62A	EPDG-Address AVP	Fully compliant.	-
7.2.63	Event AVP	Fully compliant.	-
7.2.64	Event-Charging-TimeStamp AVP	Fully compliant.	-
7.2.65	Event-Type AVP	Fully compliant.	-
7.2.66	Expires AVP	Not compliant.	-
7.2.66A	FE-Identifier-List AVP	Not compliant.	-
7.2.67	File-Repair-Supported AVP	Not compliant.	-
7.2.67aA	Forwarding-Pending AVP	Fully compliant.	-
7.2.67A	From-Address AVP	Fully compliant.	-
7.2.68	GGSN-Address AVP	Fully compliant.	-

Section	Section Heading	Compliance	Notes
7.2.69	IM-Information AVP	Fully compliant.	-
7.2.70	Incremental-Cost AVP	Not compliant.	-
7.2.70A	Instance-Id AVP	Not compliant.	-
7.2.71	Interface-Id AVP	Not compliant.	-
7.2.72	Interface-Port AVP	Not compliant.	-
7.2.73	Interface-Text AVP	Not compliant.	-
7.2.74	Interface-Type AVP	Fully compliant.	-
7.2.74aA	Inter-UE-Transfer AVP	Not compliant.	-
7.2.74A	IMS-Application-Reference-Identifier AVP	Not compliant.	-
7.2.75	IMS-Charging-Identifier AVP	Fully compliant.	-
7.2.76	IMS-Communication-Service-Identifier AVP	Fully compliant.	-
7.2.76A	IMS-Emergency-Indicator AVP	Fully compliant.	-
7.2.77	IMS-Information AVP	Partially compliant.	Refer to individual AVP compliance.
7.2.77A	IMS-Visited-Network-Identifier AVP	Fully compliant.	-
7.2.78	IMSI-Unauthenticated-Flag AVP	Fully compliant.	-
7.2.79	Incoming-Trunk-Group-ID AVP	Not compliant.	-
7.2.79A	Initial-IMS-Charging-Identifier AVP	Fully compliant.	-
7.2.80	Inter-Operator-Identifier AVP	Fully compliant.	-
7.2.80A	IP-Realm-Default-Indication AVP	Not compliant.	-
7.2.80B	ISUP-Cause AVP	Fully compliant.	-
7.2.80C	ISUP-Cause-Diagnostics AVP	Fully compliant.	-
7.2.80D	ISUP-Cause-Location AVP	Fully compliant.	-
7.2.80E	ISUP-Cause-Value AVP	Fully compliant.	-
7.2.80F	ISUP-Location-Number AVP	Fully compliant.	-
7.2.80Fa	Language AVP	Not compliant.	-
7.2.80G	Layer-2-Group-ID AVP	Not compliant.	-
7.2.81	LCS-APN AVP	Not compliant.	-
7.2.82	LCS-Client-Dialed-By-MS AVP	Not compliant.	-
7.2.83	LCS-Client-External-ID AVP	Not compliant.	-
7.2.84	LCS-Client-ID AVP	Not compliant.	-
7.2.85	LCS-Client-Name AVP	Not compliant.	-
7.2.86	LCS-Client-Type AVP	Not compliant.	-

Section	Section Heading	Compliance	Notes
7.2.87	LCS-Data-Coding-Scheme AVP	Not compliant.	-
7.2.88	LCS-Format-Indicator AVP	Not compliant.	-
7.2.89	LCS-Information AVP	Partially compliant.	Refer to individual AVP compliance.
7.2.90	LCS-Name-String AVP	Fully compliant.	-
7.2.91	LCS-Requestor-ID AVP	Not compliant.	-
7.2.92	LCS-Requestor-ID-String AVP	Not compliant.	-
7.2.92A	Local-GW-Inserted-Indication AVP	Not compliant.	-
7.2.93	Local-Sequence-Number AVP	Not compliant.	-
7.2.94	Location-Estimate AVP	Not compliant.	-
7.2.95	Location-Estimate-Type AVP	Not compliant.	-
7.2.95A	Location-Info AVP	Not compliant.	-
7.2.96	Location-Type AVP	Not compliant.	-
7.2.97	Low-Balance-Indication AVP	Fully compliant.	-
7.2.97A	Low-Priority-Indicator AVP	Not compliant.	-
7.2.97B	MBMS-Charged-Party AVP	Not compliant.	-
7.2.98	MBMS-GW-Address AVP	Not compliant.	-
7.2.99	MBMS-Information AVP	Partially compliant.	Refer to individual AVP compliance.
7.2.100	MBMS-User-Service-Type AVP	Fully compliant.	-
7.2.101	Media-Initiator-Flag AVP	Not compliant.	-
7.2.102	Media-Initiator-Party AVP	Not compliant.	-
7.2.103	Message-Body AVP	Not compliant.	-
7.2.104	Message-Class AVP	Fully compliant.	-
7.2.105	Message-ID AVP	Not compliant.	-
7.2.106	Message-Size AVP	Fully compliant.	-
7.2.107	Message-Type AVP	Fully compliant.	-
7.2.108	MM-Content-Type AVP	Not compliant.	-
7.2.109	MMBox-Storage-Requested AVP	Not compliant.	-
7.2.110	MMS-Information AVP	Partially compliant.	Refer to individual AVP compliance.
7.2.111	MMTel-Information AVP	Not compliant.	-
7.2.111A	MMTel-SService-Type AVP	Not compliant.	-
7.2.111Aa	Monitored-PLMN-Identifier AVP	Not compliant.	-
7.2.111AaA	Monitoring-Event-Configuration-Activity AVP	Not compliant.	-
7.2.111AaB	Monitoring-Event-Functionality AVP	Not compliant.	-

Section	Section Heading	Compliance	Notes
7.2.111AaC	Monitoring-Event-Information AVP	Partially compliant.	Refer to individual AVP compliance.
7.2.111AaD	Monitoring-Event-Report-Data AVP	Not compliant.	-
7.2.111AaE	Monitoring-Event-Report-Number AVP	Not compliant.	-
7.2.111Ab	Monitoring-UE-HPLMN-Identifier AVP	Not compliant.	-
7.2.111Ac	Monitoring-UE-Identifier AVP	Not compliant.	-
7.2.111Ad	Monitoring-UE-VPLMN-Identifier AVP	Not compliant.	-
7.2.111B	MSC-Address AVP	Fully compliant.	-
7.2.111C	MTC-IWF-Address AVP	Not compliant.	-
7.2.111D	Neighbour-Node-Address AVP	Not compliant.	-
7.2.111E	Network-Call-Reference-Number AVP	Not compliant.	-
7.2.112	Next-Tariff AVP	Not compliant.	-
7.2.112aA	NIDD-Submission AVP	Not compliant.	-
7.2.112A	NNI-Information AVP	Partially compliant.	Refer to individual AVP compliance.
7.2.112B	NNI-Type AVP	Not compliant.	-
7.2.113	Node-Functionality AVP	Fully compliant.	-
7.2.114	Node-Id AVP	Fully compliant.	-
7.2.115	Number-Of-Diversions AVP	Fully compliant.	-
7.2.116	Number-Of-Messages-Sent AVP	Fully compliant.	-
7.2.117	Number-Of-Participants AVP	Fully compliant.	-
7.2.118	Number-Of-Received-Talk-Bursts AVP	Not compliant.	-
7.2.119	Number-Of-Talk-Bursts AVP	Not compliant.	-
7.2.120	Number-Portability-Routing-Information AVP	Not compliant.	-
7.2.121	Offline-Charging AVP	Not applicable.	OCS functions as online charging.
7.2.122	Online-Charging-Flag AVP	Not compliant.	-
7.2.123	Originating-IOI AVP	Not compliant.	-
7.2.124	Originator AVP	Fully compliant.	-
7.2.125	Originator-Address AVP	Fully compliant.	-
7.2.126	Originator-Interface AVP	Not compliant.	-
7.2.127	Originator-Received-Address AVP	Fully compliant.	-
7.2.128	Originator-SCCP-Address	Fully compliant.	-
7.2.128A	Outgoing-Session-Id AVP	Not compliant.	-

Section	Section Heading	Compliance	Notes
7.2.129	Outgoing-Trunk-Group-ID AVP	Not compliant.	-
7.2.130	Participants-Involved AVP	Not compliant.	-
7.2.131	Participant-Group AVP	Not compliant.	-
7.2.132	Participant-Access-Priority AVP	Not compliant.	-
7.2.133	Participant-Action-Type AVP	Not compliant.	-
7.2.134	Void	Not applicable.	-
7.2.135	Void	Not applicable.	-
7.2.135A	PC3-Control-Protocol-Cause AVP	Not compliant.	-
7.2.135B	PC3-EPC-Control-Protocol-Cause AVP	Not compliant.	-
7.2.136	PDN-Connection-Charging-ID AVP	Not compliant.	-
7.2.137	PDP-Address AVP	Not compliant.	-
7.2.137A	PDP-Address-Prefix-Length AVP	Not compliant.	-
7.2.138	PDP-Context-Type AVP	Not compliant.	-
7.2.138A	Play-Alternative AVP	Not compliant.	-
7.2.139	PoC-Change-Condition AVP	Not compliant.	-
7.2.140	PoC-Change-Time AVP	Not compliant.	-
7.2.141	PoC-Controlling-Address AVP	Not compliant.	-
7.2.142	PoC-Event-Type AVP	Not compliant.	-
7.2.143	PoC-Group-Name AVP	Not compliant.	-
7.2.144	PoC-Information AVP	Partially compliant.	Refer to individual AVP compliance.
7.2.145	PoC-Server-Role AVP	Not compliant.	-
7.2.146	PoC-Session-Id AVP	Not compliant.	-
7.2.147	PoC-Session-Initiation-Type AVP	Not compliant.	-
7.2.148	PoC-Session-Type AVP	Not compliant.	-
7.2.149	PoC-User-Role AVP	Not compliant.	-
7.2.150	PoC-User-Role-IDs AVP	Not compliant.	-
7.2.151	PoC-User-Role-Info-Units AVP	Not compliant.	-
7.2.152	Positioning-Data AVP	Not compliant.	-
7.2.153	Preferred-AoC-Currency AVP	Not compliant.	-
7.2.154	Priority AVP	Fully compliant.	-
7.2.154aA	Privacy-Indicator AVP	Not compliant.	-
7.2.154A	ProSe-3rd-Party-Application-ID AVP	Not compliant.	-

Section	Section Heading	Compliance	Notes
7.2.154Aa	ProSe-Direct-Communication-Reception-Data-Container AVP	Not compliant.	-
7.2.154B	ProSe-Direct-Communication-Transmission-Data-Container AVP	Not compliant.	-
7.2.154C	ProSe-Direct-Discovery-Model AVP	Not compliant.	-
7.2.154D	ProSe-Event-Type AVP	Not compliant.	-
7.2.154E	ProSe-Function-IP-Address AVP	Not compliant.	-
7.2.154F	ProSe-Function-PLMN-Identifier AVP	Not compliant.	-
7.2.154G	ProSe-Functionality AVP	Not compliant.	-
7.2.154H	ProSe-Group-IP-Multicast-Address AVP	Not compliant.	-
7.2.154I	ProSe-Information AVP	Partially compliant.	Refer to individual AVP compliance.
7.2.154J	ProSe-Range-Class AVP	Not compliant.	-
7.2.154K	ProSe-Reason-For-Cancellation AVP	Not compliant.	-
7.2.154L	ProSe-Request-Timestamp AVP	Not compliant.	-
7.2.154M	ProSe-Role-Of-UE AVP	Not compliant.	-
7.2.154N	ProSe-Source-IP-Address AVP	Not compliant.	-
7.2.154O	ProSe-UE-ID AVP	Not compliant.	-
7.2.154Oa	ProSe-UE-to-Network-Relay-UE-ID AVP	Not compliant.	-
7.2.154Ob	ProSe-Target-Layer-2-ID AVP	Not compliant.	-
7.2.154P	Proximity-Alert-Indication AVP	Not compliant.	-
7.2.154Q	Proximity-Alert-Timestamp AVP	Not compliant.	-
7.2.154R	Proximity-Cancellation-Timestamp AVP	Not compliant.	-
7.2.155	PS-Append-Free-Format-Data AVP	Not compliant.	-
7.2.156	PS-Free-Format-Data AVP	Not compliant.	-
7.2.157	PS-Furnish-Charging-Information AVP	Not compliant.	-
7.2.158	PS-Information AVP	Partially compliant.	Refer to individual AVP compliance.
7.2.159	Quota-Consumption-Time AVP	Not compliant.	Validity-Time is used instead of the quota consumption mechanism.

Section	Section Heading	Compliance	Notes
7.2.160	Quota-Holding-Time AVP	Not compliant.	Validity-Time is used instead of the quota consumption mechanism.
7.2.160aA	Quota-Indicator AVP	Not compliant.	-
7.2.160A	Radio-Frequency AVP	Not compliant.	-
7.2.160B	Radio-Parameter-Set-Info AVP	Not compliant.	-
7.2.160C	Radio-Parameter-Set-Values AVP	Not compliant.	-
7.2.160D	Radio-Resources-Indicator AVP	Not compliant.	-
7.2.160E	Rate-Control-Max-Message-Size AVP	Not compliant.	-
7.2.160F	Rate-Control-Max-Rate AVP	Not compliant.	-
7.2.160G	Rate-Control-Time-Unit AVP	Not compliant.	-
7.2.161	Rate-Element AVP	Not compliant.	-
7.2.162	Read-Reply-Report-Requested AVP	Not compliant.	-
7.2.163	Void	Not applicable.	-
7.2.164	Real-Time-Tariff-Information AVP	Not compliant.	-
7.2.164A	Reason-Header AVP	Fully compliant.	-
7.2.165	Received-Talk-Burst-Time AVP	Not compliant.	-
7.2.166	Received-Talk-Burst-Volume AVP	Not compliant.	-
7.2.167	Recipient-Address AVP	Fully compliant.	-
7.2.168	Recipient-Info AVP	Partially compliant.	Refer to individual AVP compliance.
7.2.169	Recipient-Received-Address AVP	Fully compliant.	-
7.2.170	Recipient-SCCP-Address	Fully compliant.	-
7.2.171	Refund-Information AVP	Fully compliant.	-
7.2.171A	Relationship-Mode AVP	Not compliant.	-
7.2.171Aa	Related-Change-Condition-Information AVP	Not compliant.	-
7.2.171Ab	Related-Trigger AVP	Not compliant.	-
7.2.171B	Related-IMS-Charging-Identifier AVP	Not compliant.	-
7.2.171C	Related-IMS-Charging-Identifier-Node AVP	Not compliant.	-
7.2.171D	Relay-IP-address AVP	Not compliant.	-
7.2.172	Remaining-Balance AVP	Not compliant.	-
7.2.173	Reply-Applic-ID AVP	Not compliant.	-
7.2.174	Reply-Path-Requested AVP	Not compliant.	-
7.2.175	Reporting-Reason AVP	Not compliant.	-

Section	Section Heading	Compliance	Notes
7.2.176	Requested-Party-Address AVP	Fully compliant.	-
7.2.176A	Requested-PLMN-Identifier AVP	Not compliant.	-
7.2.176B	Requestor-PLMN-Identifier AVP	Not compliant.	-
7.2.177	Role-Of-Node AVP	Fully compliant.	-
7.2.177aA	Role-Of-ProSe-Function AVP	Not compliant.	-
7.2.177A	Route-Header-Received AVP	Not compliant.	-
7.2.177B	Route-Header-Transmitted AVP	Not compliant.	-
7.2.178	Scale-Factor AVP	Not compliant.	-
7.2.178A	SCS-Address AVP	Fully compliant.	-
7.2.178B	SCS-AS-Address AVP	Fully compliant.	-
7.2.178C	SCS-Realm AVP	Fully compliant.	-
7.2.179	SDP-Answer-Timestamp AVP	Not compliant.	-
7.2.180	SDP-Media-Component AVP	Partially compliant.	Refer to individual AVP compliance.
7.2.181	SDP-Media-Description AVP	Not compliant.	-
7.2.182	SDP-Media-Name AVP	Not compliant.	-
7.2.183	SDP-Offer-Timestamp AVP	Not compliant.	-
7.2.184	SDP-Session-Description AVP	Not compliant.	-
7.2.185	SDP-TimeStamps AVP	Not compliant.	-
7.2.186	SDP-Type AVP	Not compliant.	-
7.2.186A	Session-Direction AVP	Fully compliant.	-
7.2.187	Served-Party-IP-Address AVP	Fully compliant.	-
7.2.188	Void	Not applicable.	-
7.2.189	Service-Data-Container AVP	Partially compliant.	Refer to individual AVP compliance.
7.2.190	Service-ID AVP	Not compliant.	-
7.2.191	Service-Generic-Information AVP	Not compliant.	-
7.2.192	Service-Information AVP	Partially compliant.	Refer to individual AVP compliance.
7.2.193	Service-Mode AVP	Not compliant.	-
7.2.194	Service-Specific-Data AVP	Fully compliant.	-
7.2.195	Service-Specific-Info AVP	Fully compliant.	-
7.2.196	Service-Specific-Type AVP	Fully compliant.	-
7.2.197	Void	Not applicable.	-
7.2.197a	Serving-Node-Identity	Fully compliant.	-
7.2.198	Serving-Node-Type AVP	Fully compliant.	-

Section	Section Heading	Compliance	Notes
7.2.198A	SGi-PtP-Tunnelling-Method AVP	Not compliant.	-
7.2.199	SGSN-Address AVP	Fully compliant.	-
7.2.199A	SGW-Address AVP	Fully compliant.	-
7.2.200	SGW-Change AVP	Not compliant.	-
7.2.201	SIP-Method AVP	Fully compliant.	-
7.2.202	SIP-Request-Timestamp AVP	Fully compliant.	-
7.2.203	SIP-Request-Timestamp-Fraction AVP	Not compliant.	-
7.2.204	SIP-Response-Timestamp AVP	Fully compliant.	-
7.2.205	SIP-Response-Timestamp-Fraction AVP	Not compliant.	-
7.2.205A	SM-Device-Trigger-Indicator AVP	Not compliant.	-
7.2.205B	SM-Device-Trigger-Information AVP	Partially compliant.	Refer to individual AVP compliance.
7.2.206	SM-Discharge-Time AVP	Not compliant.	-
7.2.207	SM-Message-Type AVP	Fully compliant.	-
7.2.208	SM-Protocol-Id AVP	Not compliant.	-
7.2.208A	SM-Sequence-Number AVP	Not compliant.	-
7.2.209	SM-Status AVP	Not compliant.	-
7.2.210	SM-User-Data-Header AVP	Not compliant.	-
7.2.211	SMS-Information AVP	Partially compliant.	Refer to individual AVP compliance.
7.2.212	SMS-Node AVP	Fully compliant.	-
7.2.212A	SMS-Result AVP	Fully compliant.	-
7.2.213	SM-Service-Type AVP	Not compliant.	-
7.2.214	SMSC-Address AVP	Fully compliant.	-
7.2.214A	Start-of-Charging AVP	Not compliant.	-
7.2.215	Start-Time AVP	Not compliant.	Event-Timestamp of a CCR-I or MSCC interaction is used for this purpose.
7.2.215A	Status-AS-Code AVP	Not compliant.	-
7.2.216	Stop-Time AVP	Not compliant.	Event-Timestamp of a CCR-T or MSCC interaction is used for this purpose.
7.2.217	Submission-Time AVP	Not compliant.	Event-Timestamp of a CCR-I, CCR-E, or MSCC interaction is used for this purpose.
7.2.218	Subscriber-Role AVP	Fully compliant.	-
7.2.219	Supplementary-Service AVP	Not compliant.	-
7.2.219A	TAD-Identifier AVP	Not compliant.	-
7.2.220	Talk-Burst-Exchange AVP	Not compliant.	-

Section	Section Heading	Compliance	Notes
7.2.221	Talk-Burst-Time AVP	Not compliant.	-
7.2.222	Talk-Burst-Volume AVP	Not compliant.	-
7.2.222A	Target-IP-Address AVP	Not compliant.	-
7.2.223	Tariff-Information AVP	Not compliant.	-
7.2.224	Tariff-XML AVP	Not compliant.	-
7.2.224A	Teleservice AVP	Fully compliant.	-
7.2.225	Terminating-IOI AVP	Not compliant.	-
7.2.225A	Time-First-Reception AVP	Not compliant.	Event-Timestamp of a CCR-I or MSCC interaction is used for this purpose.
7.2.225B	Time-First-Transmission AVP	Not compliant.	Event-Timestamp of a CCR-I or MSCC interaction is used for this purpose.
7.2.226	Time-First-Usage AVP	Not compliant.	Event-Timestamp of a CCR-I or MSCC interaction is used for this purpose.
7.2.226A	Time-Indicator AVP	Not compliant.	-
7.2.227	Time-Last-Usage AVP	Not compliant.	Event-Timestamp of a CCR-T or MSCC interaction is used for this purpose.
7.2.228	Time-Quota-Mechanism	Not compliant.	-
7.2.229	Time-Quota-Threshold AVP	Not compliant.	-
7.2.230	Time-Quota-Type AVP	Not compliant.	-
7.2.231	Time-Stamps AVP	Partially compliant.	Refer to individual AVP compliance.
7.2.232	Time-Usage AVP	Not compliant.	-
7.2.233	Traffic-Data-Volumes AVP	Partially compliant.	Refer to individual AVP compliance.
7.2.233A	Transcoder-Inserted-Indication AVP	Not compliant.	-
7.2.233B	Transit-IOI-List AVP	Not compliant.	-
7.2.233C	Transmitter-Info AVP	Not compliant.	-
7.2.234	Token-Text AVP	Not compliant.	-
7.2.235	Trigger AVP	Not compliant.	-
7.2.236	Trigger-Type AVP	Not compliant.	-
7.2.237	Trunk-Group-ID AVP	Not compliant.	-
7.2.237A	Void	Not applicable.	-
7.2.237B	Void	Not applicable.	-
7.2.237Ba	TWAG-Address AVP	Fully compliant.	-
7.2.237C	TWAN-User-Location-Info AVP	Not compliant.	-
7.2.238	Type-Number AVP	Not compliant.	-
7.2.238A	UNI-PDU-CP-Only-Flag AVP	Not compliant.	-
7.2.239	Unit-Cost AVP	Not compliant.	-
7.2.240	Unit-Quota-Threshold AVP	Not compliant.	-

Section	Section Heading	Compliance	Notes
7.2.240a	Unused-Quota-Timer AVP	Not compliant.	-
7.2.240A	User-CSG-Information AVP	Not compliant.	-
7.2.240B	Usage-Information-Report-Sequence-Number AVP	Not compliant.	-
7.2.241	User-Participating-Type AVP	Not compliant.	-
7.2.242	User-Session-Id AVP	Not compliant.	-
7.2.242aaA	UWAN-User-Location-Info AVP	Not compliant.	-
7.2.242aA	Variable-Part AVP	Not compliant.	-
7.2.242aB	Variable-Part-Order AVP	Not compliant.	-
7.2.242aC	Variable-Part-Type AVP	Not compliant.	-
7.2.242aD	Variable-Part-Value AVP	Not compliant.	-
7.2.242A	VCS-Information AVP	Partially compliant.	Refer to individual AVP compliance.
7.2.242B	VLR-Number AVP	Fully compliant.	-
7.2.243	Volume-Quota-Threshold AVP	Not compliant.	-
7.2.244	Void	Not applicable.	-
7.2.245	Void	Not applicable.	-
7.2.246	Void	Not applicable.	-
7.2.247	Void	Not applicable.	-
7.2.248	Void	Not applicable.	-
7.2.249	Void	Not applicable.	-
7.2.250	Void	Not applicable.	-
7.3	3GPP2 specific AVPs	Not compliant.	-
7.4	ETSI specific AVPs	Not compliant.	-
7.5	oneM2M specific AVPs	Not compliant.	-
Annex A	Bibliography	Not applicable.	-
Annex B	Change history	Not applicable.	-

Table 14: OCS compliance to TS 32.299