Oracle® Communications Network Charging and Control

Diameter Control Agent Protocol Implementation Conformance Statement

Release 6.0.1

April 2017

ORACLE®

Copyright

Contents

About This Document

Scope

The purpose of this document is to describe the Oracle implementation of the Diameter protocol for the purposes of real-time charging, from a Diameter Credit-Control Server perspective.

Audience

This guide is intended for use by software engineers and testers that need a description of the SLC Credit-Control messages used by the DCA.

It is in addition to the functional details provided by the *Diameter Control Agent Technical Guide*. It is assumed that readers are familiar with Prepaid Charging and the Diameter RFCs.

Related Documents

The following documents are related to this document:

- Internet Engineering Task Force (IETF) specifications:
  - RFC 3588 - Diameter Base Protocol
  - RFC 4006 - Diameter Credit Control Application
- *Diameter Control Agent Technical Guide*
- Diameter and Diameter Control Agent SRS
- 3GPP TS 32.299 V11.3.0 (2012-03) - 3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; Telecommunication management; Charging management; Diameter charging applications (Release 11)

Document Conventions

Typographical Conventions

The following terms and typographical conventions are used in the Oracle Communications Network Charging and Control (NCC) documentation.

Formatting Convention	Type of Information
Special Bold	Items you must select, such as names of tabs. Names of database tables and fields.
Italics	Name of a document, chapter, topic or other publication. Emphasis within text.
Button	The name of a button to click or a key to press. **Example:** To close the window, either click **Close**, or press **Esc**.
Key+Key	Key combinations for which the user must press and hold down one key and then press another. Example: **Ctrl+P** or **Alt+F4**.
`Monospace`	Examples of code or standard output.
`Monospace Bold`	Text that you must enter.
variable	Used to indicate variables or text that should be replaced with an actual value.
menu option > menu option >	Used to indicate the cascading menu option to be selected. Example: **Operator Functions > Report Functions**
hypertext link	Used to indicate a hypertext link.

Specialized terms and acronyms are defined in the glossary at the end of this guide.

Chapter 1

Compliance Statement

Overview

Introduction

This chapter introduces the Diameter Control Agent (DCA) compliance limitations.

In this chapter

This chapter contains the following topics.

DCA Overview

Introduction

The Diameter Control Agent (DCA) is an interface used by Prepaid Charging to allow processing of Diameter based billing requests utilizing existing Oracle SLC and Charging infrastructure.

The Diameter base protocol is defined by RFC 3588, and extended to include real-time credit-control messages by RFC 4006.

In addition, the Diameter protocol defined by RFC 4006 is further extended by GPP TS 32.299 V11.3.0 Diameter charging applications.

DCA Coverage

The DCA (and thus this document) only covers the use of Prepaid Charging as a Diameter Credit Control server. For information about Prepaid Charging acting as a Diameter Credit Control Client, see the Diameter Charging Driver (DCD) documentation.

DCA Server

The DCA server runs on the SLC SLEE, taking inbound requests from Diameter Credit-Control clients and passing them to Prepaid Charging for further processing. This may involve passing the request on to an existing billing engine using a different protocol such as FOX, OSA or Diameter.

The DCA server maintains the connections to the Diameter Credit-Control client (or, if configured, intermediate Diameter peer, such as a proxy).

General restrictions

Specific adherence to the RFCs is described in a later section, but there are some general properties of Diameter that are not handled by the DCA.

These are:

- TLS (RFC 2246) is not supported.
- Authentication and Authorization messages are not supported

- Tariff Time Change is not supported
- Dynamic peer discovery is not performed.
- SNMP client alarm generation (SMS alarm mechanism is used instead)
- There is no expectation to provide Network Access Services (NAS) server functionality as part of the Oracle Diameter implementation. Note that this does not prohibit existing Diameter based NAS servers acting as Diameter Credit Control clients, for the purposes of billing a service.

Chapter 2

Diameter Message Encoding

Overview

Introduction

This chapter details the Diameter Control Agent (DCA) compliances.

In this chapter

This chapter contains the following topics.

Diameter Message Encoding

Introduction

The DCA client will send (and expect to receive) Diameter messages that have a basic encoding in compliance with RFC 3588.

Diameter Headers

The header of Diameter messages sent by DCA are fully compliant with RFC 3588.

The individual parameters are:

Field	Type/Length	Comment
Version	1 byte	Always set to 1.
Message Length	3 bytes	Length includes header fields.
Command Flags	1 byte	Format: *RPETrrrr* All set as per RFC 3588.
Command Code	3 bytes	Will be one of: • 257 (CER/A) • 280 (DWR/A) • 282 (DPR/A) • 272 (CCR/A)
Application ID	4 bytes	Set to 4 for CCRs, 0 for all other message types.
Hop-by-hop identifier	Unsigned32; 4 bytes	Set as per RFC 3588.
End-to-end identifier	Unsigned32; 4 bytes	Set as per RFC 3588.

Attribute-Value Pairs (AVPs)

The header on an AVP consists of the following fields:

Field	Type/Length	Comment
AVP Code	4 bytes	
AVP Flags	1 byte	Format: *VMPrrrrr*: *V* is vendor bit. Will be set only if a vendor-ID is used. *M* is mandatory bit: If the AVP Code is from RFC 3588 or 4006, the bit is set. Otherwise (for example, a vendor specific AVP code), the bit is not set. *P* is an encryption indicator. Set to 0.
AVP Length	3 bytes	AVP length in bytes, including these header fields.
Vendor-ID	4 bytes	Will be 0 for RFC 3588 and 4006 AVPs, or 111 for Oracle specific AVPs.
Data		As specified by the AVP code and length.

AVP Data Types

The DCA can send and receive all the basic and derived data types mentioned in RFC 3588, except Float32 and Float64. Where the data types are used, they are encoded in complete compliance with RFC 3588 and RFC 2279.

INAP extensions

The following may be mapped to or from INAP extensions:

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

Note: The OctetString type can have number values as an array of either ASCII characters or integers.

Extension formats

Supported INAP extension formats are:

- inapnumber
- asn1integer
- octets
- encoded (as ACS Profile Block)

INAP fields

As an alternative to extension formats, DCA also support mapping of AVPs to (Inbound) or from (Outbound) INAP Fields. Supported INAP Fields are:

INAP Field	Direction
AdditionalCallingPartyID	Inbound only
CalledPartyBCDNumber	Inbound only
CalledParty	Inbound only
CallingParty	Inbound, Outbound
Cause	Outbound only
DestinationRoutingAddress	Outbound only
IMSI	Inbound only
LocationInformation	Inbound only
LocationNumber	Outbound only
MaxCallDuration	Outbound only
MscAddress	Inbound only
OriginalCalledParty	Inbound, Outbound
RedirectingPartyID	Inbound, Outbound

Note:
Inbound direction (Diameter AVP to INAP Field)
Outbound direction (INAP Field to Diameter AVP)

Chapter 3

Connection Management

Overview

Introduction

This chapter covers the connection management compliances.

In this chapter

This chapter contains the following topics.

Introduction

Introduction

The DCA server will accept inbound connections initiated by Diameter Credit-Control clients as per RFC 3588. However, the DCA will only allow connections from peers that are in its configured list. CERs from unknown peers will have a CEA message sent before the client closes the connection. DCA will not initiate connections to unconnected peers. Connections can be over either TCP or SCTP.

To manage the connections, the following messages from RFC 3588 are used:

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

Capabilities Exchange Messages

Capabilities Exchange Messages

The DCA will receive CER messages and respond with CEA messages, as per formats specified in RFC 3588. The content of the individual fields is as follows:

Field	AVP Code	Data Type	Comment
Origin-Host	264	DiameterIdentity	Set from configuration. Default is hostname.

Field	AVP Code	Data Type	Comment
Origin-Realm	296	DiameterIdentity	Set from configuration. Default is hostname.
Host-IP-Address	257	Address	Set from configuration. Default is INADDR_ANY.
Vendor-ID	266	Unsigned32	Set from configuration (Oracle vendor ID is 111).
Product-Name	269	UTF8String	Set from configuration.
Origin-State-Id	278	Unsigned32	Used to detect a re-booting peer and wipe sessions for the host if it has rebooted.
Supported-Vendor-Id	265	Unsigned32	Set from configuration.
Auth-Application-Id	258	Unsigned32	Must be as specified in configuration. Default is 4 (Credit-Control). Inbound CER messages will be rejected.
Inband-Security-Id	299	Unsigned32	Set to 0 (NO_INBAND_SECURITY).
Acct-Application-Id	259	Unsigned32	Not included.
Vendor-Specific-Application-Id	260	Grouped	Not included.
Firmware-Revision	267	Unsigned32	Not included.
Result-Code	268	Unsigned32	Set as per RFC 3588.
Error-Message	281	UTF8String	Human-readable string, as per RFC 3588.
Failed-AVP	279	Grouped	Set as per RFC3588.

Disconnect Peer Messages

Disconnect Peer Messages

A literal interpretation of RFC 3588 could assume that after either side sends a DPR message, the receiving peer should never again attempt to reconnect the connection. On shutdown, DCA will send a DPR message. The client might take this literal interpretation and never try to reconnect. In this case, the client may need to be reinitialized or restarted.

The possible fields are as follows:

Field	AVP Code	Data Type	Comment
Origin-Host	264	DiameterIdentity	Set from configuration. Default is hostname.
Origin-Realm	296	DiameterIdentity	Set from configuration. Default is hostname.
Disconnect-Cause	273	Enumerated	The only cause sent by the DCA is 2, DO_NOT_WANT_TO_TALK_TO_YOU.
Result-Code	268	Unsigned32	Set as per RFC 3588.
Error-Message	281	UTF8String	Human-readable string, as per RFC 3588.
Failed-AVP	279	Grouped	Set as per RFC3588.

Device Watchdog Messages

Device Watchdog Messages

Provision is to be made for determining if there has been a transport failure by supporting the Device Watchdog Request (DWR) and Device Watchdog Answer (DWA) messages. This necessitates the ability to receive DWR messages and send an appropriate DWA message as a response. The purpose of this is that if a client detects a connection failure to the server, the client should make a periodic attempt to reconnect.

The length of the silent interval that must precede a DWR message is configurable. The possible fields are as follows:

Field	AVP Code	Data Type	Comment
Origin-Host	264	DiameterIdentity	Set from configuration. Default is hostname
Origin-Realm	296	DiameterIdentity	Set from configuration. Default is hostname.
Origin-State-Id	278	Unsigned32	Used to detect a re-booting peer and wipe sessions for the host if it has rebooted.
Result-Code	268	Unsigned32	Set as per RFC 3588.
Error-Message	281	UTF8String	Human-readable string, as per RFC 3588.
Failed-AVP	279	Grouped	Set as per RFC3588.

Message Retransmission and Duplicate Detection

RFC 3588 and Event Based Credit-Control Duplicate Detection

In Diameter clients (and agents) may retransmit messages, where an unexpected failure has occurred. This may occur when a client has sent a request, but has not received a reply, within a specified period. This retransmission behavior can potentially lead to duplicates being sent. In such cases clients which send messages, which may be duplicates, may indicate the possibility that a subsequent message is a duplicate by setting the T command flag / bit (refer to Chapter 3 Diameter Header of RFC 3588).

Note: The T-flag not being set is not necessarily a definitive indicator that no duplicate is present.

End to end identifier

The DCA uses the End-to-End Identifier for detecting duplicate messages (in conjunction with the Origin-Host AVP). The DCA also ensures that answers must have the same identifier as in the original request. In addition duplicate requests result in essentially the same response, but should not affect state (that is, in Credit-Control duplicate billing must not occur).

Non-volatile storage

Non-volatile storage of End-to-End identifier or recently sent responses is not supported, due to the significant processing overhead this can introduce.

Duplicate message

The case where a duplicate arrives at a different SLC is also not supported. For real-life deployments each SLC should be treated as a separate realm in order to avoid double processing of duplicates. This means that the realm name and hostname may effectively be the same for each DCA SLC.

Note: Duplicate detection is not applied to Device Watchdog messages.

General duplicate detection

The following generalized approach is utilized for the detection of duplicates.

When the server receives a message which is a candidate for duplicate detection:

1. The code searches a map of recently received messages for a matching End-to-End Identifier.
2. If a duplicate message was encountered:
   Resend the original response (which should have been remembered).
3. If NO duplicates were detected in either backwards time frame or the original message was late:
   Process the message like normal (that is, assume the message was never dealt with in the first place).

Session-Based Credit-Control Duplicate Detection

For session-based CCR messages (that is, those with Requested-Action AVP of INITIAL_REQUEST, TERMINATION_REQUEST, or UPDATE_REQUEST), duplicate detection is based on the mechanism described in RFC 4006. That is, duplicate detection for session-based messages is performed using the Session-Id AVP and CC-Request-Number AVP, in conjunction with the Credit-Control servers own internal state, for non Multiple-Services-Credit-Control cases.

CC-Request-Number detects out-of-sequence messages, and is expected to be sequential (as suggested by RFC 4006).

However, this does not hold for Multiple-Services-Credit-Control, because that CC-Request-Number will not necessarily be sequential. Clients are not required to wait for a CCA before sending a new Credit-Control-Request (CCR) message. This might happen if a client sends a new CCR for a different service (than those currently pending response), when that service requires further authorization to use more units.

For Multiple-Services-Credit-Control, a lookup is performed based on the inbound CC-Request-Number. If one is found, it can be assumed to be a duplicate and the same answer returned.

Chapter 4

Credit Control Requests

Overview

Introduction

This chapter describes the mappings between INAP parameters and Diameter AVPs.

In this chapter

This chapter contains the following topics.

Credit Control Request and Response AVPs

AVP List descriptions

This table describes the function of each AVP.

AVP Name	Action
Session-Id	Used to identify the relevant session.
Origin-Host	Used to identify sender.
Origin-Realm	Used to identify sender.
Destination-Realm	Used to identify the realm of the target Credit Control Server (normally expected to be the machine DCA is running on)
Auth-Application-Id	Disregarded if not 4 (Diameter Credit-Control)
Service-Context-Id	Used as part of the key to look up the service.
CC-Request-Type	Used as part of the key to look up the service. Also used to determine the next state.
CC-Request-Number	Used in duplicate detection.
Destination-Host	Used to identify the host of the target Credit Control Server (normally expected to be the machine DCA is running on).
User-Name	Ignored unless mapped to an IDP extension by the AVP mappings in **eserv.config**.
CC-Sub-Session-Id	Ignored. We do not support multiple session IDs but some clients may set this anyway. If so this will be ignored.
Acct-Multi-Session-Id	Ignored. We do not support multiple session IDs but some clients may set this

AVP Name	Action
	anyway. If so this will be ignored.
Origin-State-Id	Used to detect a client re-booting and wipe sessions for the host if it has rebooted.
Event-Timestamp	For EVENT_REQUEST messages, this gets copied into IDP extension type 504.
Subscription-Id	Gets copied to IDP extension type 505. If this is an E 164 number, it also gets copied to CallingPartyNumber, after applying the configured normalization rules.
Service-Identifier	Used as part of the key to look up the service.
Termination-Cause	May be traced if tracing is enabled. Otherwise, ignored.
Requested-Service-Unit	The type of the service unit (derived from which sub-AVP is contained within this one) is placed in IDP extension type 502. The value of the sub-AVP is placed in IDP extension type 501. DCA supports the use of multiple unit-types within a single Requested-Service-Unit AVP for both Basic Credit Control and Multiple Services Credit Control (MSCC) upon service initiation. A single Requested-Service-Unit AVP (containing more than 1 unit type) will result in DCA triggering multiple slee_acs calls (1 for each unit type).
Requested-Action	Used as part of the key to look up the service. Also used to determine the next state.
Used-Service-Unit	The cumulative total of all the Used-Service-Unit AVPs is multiplied by 10 (to create deci-seconds) and used to identify the total used units for the call.
Multiple-Services-Indicator	DCA fully supports Multiple-Services-Credit Control. The DCA mechanism for supporting multiple service credit-control allows multiple charging sessions with ACS to be associated with one DIAMETER session.So if the received Multiple-Services-Indicator is set to MULTIPLE_SERVICES_SUPPORTED, DCA will accept the incoming message and subsequent Multiple-Services-Credit-Control AVPs if received in CCR/CCA update and CCR/CCA final request messages. All incoming diameter messages and associated MSCC AVPs will be processed and dispatched as separate calls/sessions to ACS. An association will be maintained between these multiple ACS calls/sessions and the single diameter session with responses from ACS aggregated before a single CCA response containing an MSCC AVP is returned. The segregation of the single MSCC session into separate ACS calls is internally managed by DCA and is transparent to the Diameter Client.
Multiple-Services-Credit-Control	Requires that Multiple-Services-Indicator AVP has been received, with value set to MULTIPLE_SERVICES_SUPPORTED. DCA supports the use of multiple unit-types within a single Requested-Service-Unit AVP for both multiple services credit-control (MSCC) and basic credit control. As described above, the mechanism for multiple service credit-control allows multiple ACS charging sessions to be dispatched and associated with one DIAMETER session. If more than one unit type is received within the MSCC AVP, a similar mechanism of segregation and dispatch to ACS will be used (that is, one ACS session/call for each unit type)
Service-Parameter-Info	Ignored unless mapped to an IDP extension by the AVP mappings in **eserv.config**.
CC-Correlation-Id	Ignored unless mapped to an IDP extension by the AVP mappings in

AVP Name	Action
	eserv.config.
User-Equipment-Info	Ignored unless mapped to an IDP extension by the AVP mappings in **eserv.config**.
Proxy-Info	Returned unmodified in CCA.
Route-Record	Ignored at present, unless mapped to an IDP extension by the AVP mappings in **eserv.config**.

AVP Data source

This table describes how each AVP content is set.

Some of these AVPs are for both Credit Control Requests and Credit Control Responses. Some are for one only.

AVP Name	Set From
Session-Id	The Session-Id AVP of the first message in this transaction.
Result-Code	Set to DIAMETER_SUCCESS unless otherwise stated. **Note:** If quiescing and this is an INITIAL_REQUEST or an EVENT_REQUEST then return CCA(Result-Code=DIAMETER_TOO_BUSY).
Origin-Host	Set according to configuration. Normally defaults to host name.
Origin-Realm	Set according to configuration. Normally defaults to host name.
Auth-Application-Id	Always set to 4 (Diameter Credit-Control)
CC-Request-Type	The value of CC-Request-Type from the corresponding request.
CC-Request-Number	The value of CC-Request-Number from the corresponding request.
User-Name	Set if configured.
CC-Session-Failover	Set if configured (which should be treated as FAILOVER-NOT-SUPPORTED according to RFC 4006).
CC-Sub-Session-Id	Set to the value from the corresponding request message.
Acct-Multi-Session-Id	Set to the value from the corresponding request message, of present.
Origin-State-Id	Set to current system time, at time of last DCA restart.
Event-Timestamp	Set to the value of the Event-Timestamp AVP from the corresponding request.
Granted-Service-Unit	For session based services, this is ApplyCharging.maxDuration (divided by 10 if the unit type is Time). For Requested-Action type DIRECT_DEBIT, in the success case, this is the same as the Requested-Service-Unit AVP in the corresponding request. Otherwise, not present.
Multiple-Services-Credit-Control	For each incoming MSCC AVP containing a Requested-Service-Unit, DCA will dispatch an individual ACS call. DCA starts the calls by sending an InitialDP (IDP) to ACS and expects a subsequent ApplyCharging (AC) response. DCA aggregates the AC responses and maps the appropriate data into the MSCC AVP in the CCA message that DCA then returns to the Diameter client. DCA will populate the MSCC AVPs in CCA messages with the following sub-AVPs where applicable: • Granted-Service-Units (See Granted-Service-Unit above that is,

AVP Name	Set From
	from ApplyCharging.maxDuration) • Rating-Group or Service-Identifier (Set by DCA in accordance with what was sent by the Diameter Client in the initial request) • Result-Code (See Result-Code above. For an MSCC request, the individual result codes are also combined to produce an overall result code). Any partial failure will result in an overall failure. • Time-Quota-Threshold (if applicable) • Volume-Quota-Threshold (if applicable) • Validity-Time (if applicable) • Final-Unit-Indication (if applicable)
Cost-Information	For Request-Action type PRICE_ENQUIRY, success case, this comes from the value of extension 603 in the INAP Connect. Otherwise, not set.
Final-Unit-Indication	Final-Unit-Action is set to REDIRECT or TERMINATE depending on the INAP operations received (from ACS/Prepaid Charging). Redirect-Server is set to the number matched in the redirectNumbers config list or TEL:<Connect destinationRoutingAddress>@<Configured SIP host>.
Check-Balance-Result	This is derived from the type of INAP operation received: Continue ENOUGH_CREDIT ReleaseCall (Reason = 31) NO_CREDIT
Credit-Control-Failure-Handling	Set to TERMINATE
Direct-Debiting-Failure-Handling	Set if configured. (According to RFC 4006, it will default to TERMINATE_OR_BUFFER).
Validity-Time	Set to the configured validity-time for the service in the graceful termination scenarios only.
Redirect-Host	Set if configured.
Redirect-Host-Usage	Set if configured.
Redirect-Max-Cache-Time	Set if configured.
Proxy-Info	Returned as per CCR.
Route-Record	Set if configured.
Failed-AVP	Set in some cases when Result-Code != success, that is: If the incoming message contains unsupported AVPs then return CCA(Result-Code=DIAMETER_AVP_UNSUPPORTED, Failed-AVPs)
Custom AVPs	Determined by DCA mapping configuration: • For Outbound Diameter messages, data sources may be INAP Fields, INAP Extensions or literal values. • For Inbound Diameter messages, the incoming Custom AVPs may be mapped to target INAP Fields or INAP Extensions.

In additional to the functionality described in the table above:

- For AVPs marked "Set if configured", refer to *Considerations* (on page 77).
- Outbound AVPs such as Result-Code may have the default data source or value changed by DCA mapping configuration as per "Custom AVPs" above.
- Any inbound AVPs may be mapped to additional target data field(s) by DCA mapping configuration as per "Custom AVPs" above.

Also note that:

- INAP Fields are determined by the INAP Standards (for example, Calling Party Number, Destination Routing Address)
- INAP Extensions when encoded into an ACS Profile Block may be used to carry Grouped AVPs and other more complex structures.
- Literal values are simple data types (for example, a literal string or integer constant)

For a full listing of AVPs and compliance to the standards document, please see the section titled "Compliance to 3GPP TS 32.299" *Section 7* (on page 45).

INAP Extension Mappings

Introduction

As INAP is not designed to contain Diameter AVPs, these will be carried, where necessary, in INAP fields and extensions in the INAP operations.

For a specific Diameter interface, there will be differences in which AVPs will be relevant for rating or which vendor specific AVPs will be used. So, for each service, the configuration allows:

- In the inbound direction, a mapping of AVPs to INAP fields or INAP extensions
- In the outbound direction, a mapping of INAP fields or INAP extensions to AVPs

The extensions that arrive through inbound mapping are available to ACS in the control plan in the incoming extensions block. These are available for manipulation such as in control plan nodes and branching decisions such as to implement tariff override if applicable.

The ACS control plan may also choose to set outgoing extensions that are sent in INAP operations and subsequently mapped into AVPs in the outbound Diameter responses.

The AVP to pass is identified according to AVP code. Multiple AVPs may be identified and passed to:

- Target profile tags, available within the inbound extensions block
- INAP Fields, available within ACS Context fields

Likewise the INAP Fields or Profile Blocks to pass is identified by name or tag code respectively.

Multiple fields may be identified and passed to target AVPs.

In addition it is possible to selectively apply the same or different mapping schemes for specific Diameter request and response messages.

INAP Extensions are possible in the following INAP Operations:

- Initial DP
- Apply Charging Report
- Continue With Argument
- Release Call (See *Note*)
- Connect
- ApplyCharging

Note: The Release Call does not use INAP Extensions, but instead encodes the extension data within the Cause Diagnostics field of the Cause parameter. This mechanism is transparent to the end-user from a functional viewpoint.

Extensions in the IDP

501 = Requested-Service-Units

502 = Requested service unit type

1 = CC-Time
2 = CC-Money
3 = CC-Total-Octets
4 = CC-Input-Octets
5 = CC-Output-Octets
6 = CC-Service-Specific-Units

503 = Requested-action

DIRECT_DEBITING	0
REFUND_ACCOUNT	1
CHECK_BALANCE	2
PRICE_ENQUIRY	3

504 = Event-Timestamp (passed as seconds since the Unix Epoch)

505 = Subscription-Id (E.164 based number representing subscriber)

506 = CC-Money.Currency-Code (if Requested-Service-Unit is type CC-Money)

507 = CC-Money.Unit-Value.Exponent (if Requested-Service-Unit is type CC-Money)

701 = Multiple Encoded AVPs, mapped to Inbound Extension profile block (as per configuration)

Extensions in the Connect operation

601 = Granted service units

602 = Granted service unit type

1 = CC-Time
2 = CC-Money
3 = CC-Total-Octets
4 = CC-Input-Octets
5 = CC-Output-Octets
6 = CC-Service-Specific-Units

603 = Cost information (in system currency)

701 = Multiple Encoded AVPs, mapped from the Outbound Extension profile block (as per configuration)

Extensions in the ApplyChargingReport

701 = Multiple Encoded AVPs, mapped from the Inbound Extension profile block (as per configuration)

Extensions in the ApplyCharging operation

701 = Multiple Encoded AVPs, mapped from the Outbound Extension profile block (as per configuration)

Extensions in the Continue WithArgument operation

701 = Multiple Encoded AVPs, mapped from the Outbound Extension profile block (as per configuration)

Cause Diagnostics in ReleaseCall operation

The "extensions" are carried in the Cause Diagnostics sub-field within the Cause parameter in the ReleaseCall.

Cause Diagnostics = Multiple Encoded AVPs, mapped from the Outbound Extension profile block (as per configuration).

INAP Field Mappings

Introduction

Instead of mapping AVPs to or from INAP Extensions, DCA also allows AVPs to be mapped to or from INAP fields.

The supported INAP Fields are:

INAP Field	Direction (INAP Operation)
AdditionalCallingPartyID	Inbound only (IDP)
CalledPartyBCDNumber	Inbound only (IDP)
CalledParty	Inbound only (IDP)
CallingParty	Inbound (IDP), Outbound (Connect)
Cause	Outbound only (ReleaseCall)
DestinationRoutingAddress	Outbound only (Connect)
IMSI	Inbound only (IDP)
LocationInformation	Inbound only (IDP)
LocationNumber	Outbound only (Connect)
MaxCallDuration	Outbound only (ApplyCharging)
MscAddress	Inbound only (IDP)
OriginalCalledParty	Inbound, Outbound (IDP)
RedirectingPartyID	Inbound, Outbound (IDP, Connect)

Notes:

Unlike INAP Extensions which, depending on configuration, can be typically applied in one or both directions, some INAP Fields can only be applied in a single direction (see table above).

"Direction" is relative to DCA for Diameter messages (that is, "Inbound" refers to an incoming Diameter message)

Example Control Plans

Introduction

Seven example control plans are shipped with the DCA packages. These are sufficient to run simple Diameter services.

There are two control plans for session based services:

- No redirect to top-up-server functionality
- Redirect to top-up-server functionality

There are four control plans for event based services:

- DIRECT_DEBITING
- REFUND_ACCOUNT
- CHECK_BALANCE
- PRICE_ENQUIRY
- SCREENING

No redirect to top-up server functionality

The Session No Redirect control plan is a session based plan with no redirect to a top-up server.

This consists of a Start node connected to a UATB node. The exits of the UATB node are connected to an End node (Success cases) and to the Disconnect nodes with various release causes. The release causes in the Disconnect nodes are such as to cause diameterControlAgent to use the appropriate Result-Code.

Redirect to top-up server functionality

This will be the same as the no redirect to top-up server functionality control plan with the following differences.

- The NSF (Disconnected) branch of the UATB node will be connected to an unconditional termination node which will contain a number mapped to the address of the top-up-server.
- The following must be set in the `CCS` and `acsCharging` sections of the **eserv.config** file if this is to be used:

```
CCS = {
    oracleUserAndPassword="xxxx/xxxx"
    CCSMacroNodes = {
        UseDisconnectLeg = true
    }
    …
}

acsCharging = {
    switchConfiguration = [
        {
            switchType = "internal"
            addDisconnectOrRelease = true
        }
    ]
}
```

DIRECT_DEBITING

This control plan starts with two profile branching nodes to determine if this is a time-based direct debit (through INAP extension 502) with an Event-Timestamp AVP (INAP extension 504).

- If it is, a DUCR node is used with the `Debit` option selected to debit the account.
- If it is not, a Named Event node is used with the `Direct Event` option selected to debit the account. The Named Event node reads its number of events from INAP extension 501 (Requested-Service-Units).

Failure branches are connected to Disconnect nodes with appropriate cause values to produce the correct Diameter Result-Code values.

REFUND_ACCOUNT

This control plan determines if this is a time or volume based account refund (through extension 502) with an Event-Timestamp AVP (extension 504).

- If it is, a DUCR node is used to credit the account.
- If it is not, a Named Event node with the `Direct Event` option selected is used to credit the account. The cost of the selected event is negative. The Named Event node reads its number of events from extension 501 (Requested-Service-Units).

Failure branches are connected to disconnect nodes with appropriate cause values to produce the correct Diameter Result-Code values.

CHECK_BALANCE

The Check Balance control plan determines if the user is able to reserve a specified number of units. It returns either a success or failure only; it does not return the number of units in the balance.

This control plan consists of a start node followed by two Named Event nodes and a terminate unchanged node, with Disconnect nodes as appropriate. The first Named Event node reserves an event type (the `Reserve Event` option selected), appropriate for this service. If the first Named Event node:

- Fails to reserve the event, it goes to a Disconnect node with the reason set to the configured no funds cause.
- Successfully reserves the event, the second Named Event node cancels the reservation (the `Revoke Event` option selected). Then, a Terminate Unchanged node sends an INAP Continue, which signals to diameterControlAgent that the balance check succeeded.

PRICE_ENQUIRY

This control plan has a Named Event node connected to:

- Disconnect nodes (for failures)
- An unconditional terminate node (for successes)

The Named Event node has the `Cost of event` option selected and is configured to store the cost of the event under a tag in the ACS temporary storage area. Then, the DCA service loader plug-in picks up this tag and puts it in INAP extension 603 in the Connect. The diameterControlAgent copies this into the Cost-information AVP.

SCREENING

The Screening control plan denies service for voice but allows service for data, based on the bearer type received from DCA.

This consists of a Start node connected to a Transmission Type Branch node. The Transmission Type Branch node exits for voice (Exits 1 and 4) are connected to a Disconnect node with a release cause of `50`. The exits for non-voice are connected to a Terminate Uncharged node.

Abort Session Request (ASR)

Abort Session Request

DCA can be configured to send an Abort-Session-Request (ASR) to the diameter client when the Session Supervision Timer (Tcc timer) expires while waiting for the diameter client to send a request to DCA. If a timeout occurs while waiting for a server process (for example, ACS, VWS) an ASR will not be sent. In this scenario, we are processing a CCR, so we manage the error condition in the CCA response.

DCA supports Multiple Services Credit Control, which means that the diameter client can request charging for many services in a single session, which results in DCA managing many charging sessions with ACS per single session with the client.

The ASR message (defined in RFC 3588) does not support the notion of services in MSCC (defined in RFC 4006), so when the Tcc timer expires for any service for a given GGSN session, all ACS charging sessions associated with the GGSN session must be terminated.

Note: Diameter provides the client with the capacity to decline aborting a session, by returning DIAMETER_UNABLE_TO_COMPLY, however DCA does not attempt to keep a session open in this case: it acts the same in all cases, simply logging the response.

The possible fields are as follows:

Field	AVP Code	Data Type	Comment
Session-Id	263	UTF8String	The Session-Id AVP of the first message in this transaction.
Origin-Host	264	DiameterIdentity	Set according to configuration. Normally defaults to host name.
Origin-Realm	296	DiameterIdentity	Set according to configuration. Normally defaults to host name.
Destination-Host	293	DiameterIdentity	The Origin-Host of the first message in this transaction.
Destination-Realm	283	DiameterIdentity	The Origin-Realm of the first message in this transaction.
Auth-Application-Id	258	Unsigned32	Set to the Auth-Application-Id received earlier in the session (in a CCR) from the Diameter credit-control client.

Scenarios

Introduction

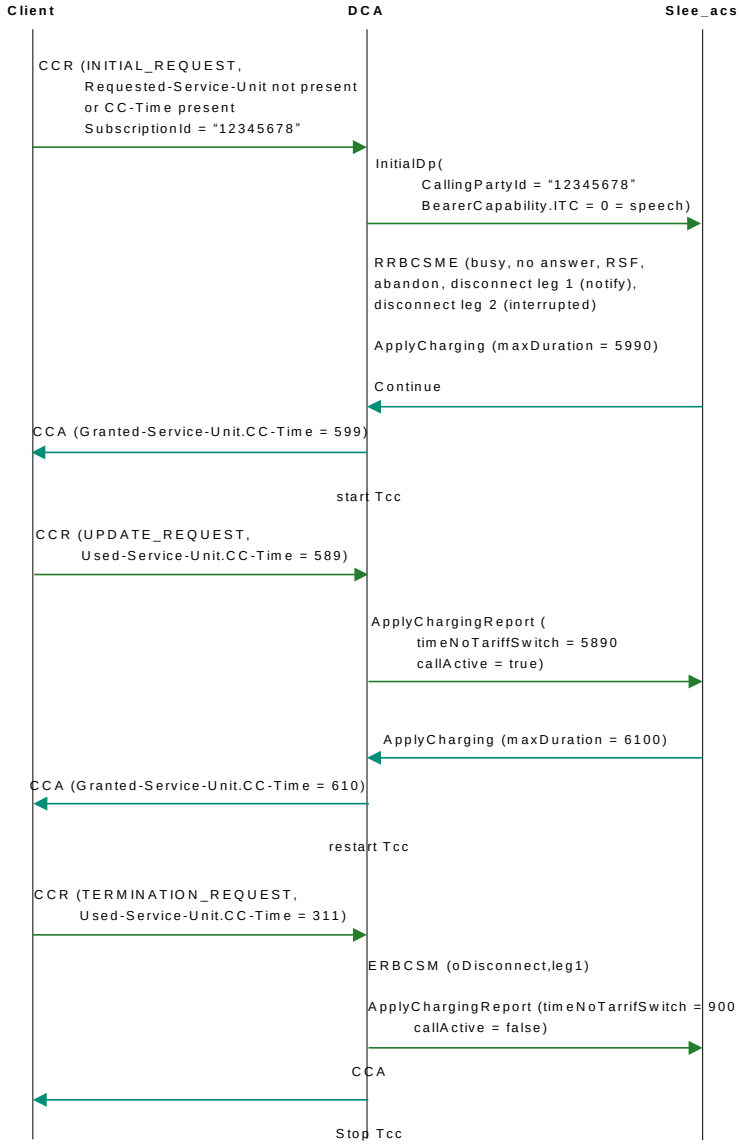
This topic explains how the flow through the software achieves Diameter server services and also gives more details on the mapping between INAP operations/parameters and Diameter messages/AVPs.

The following scenarios are based on (and named after) the relevant appendixes in *RFC 4006*.

For each scenario, a message sequence chart is given.

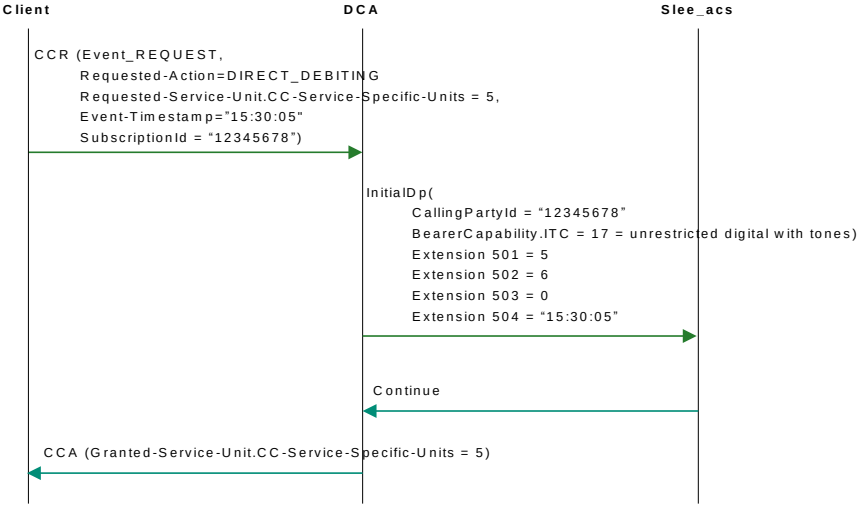
Successful session-based charging, client terminates session

Here is an example successful session-based charging, client terminates session.



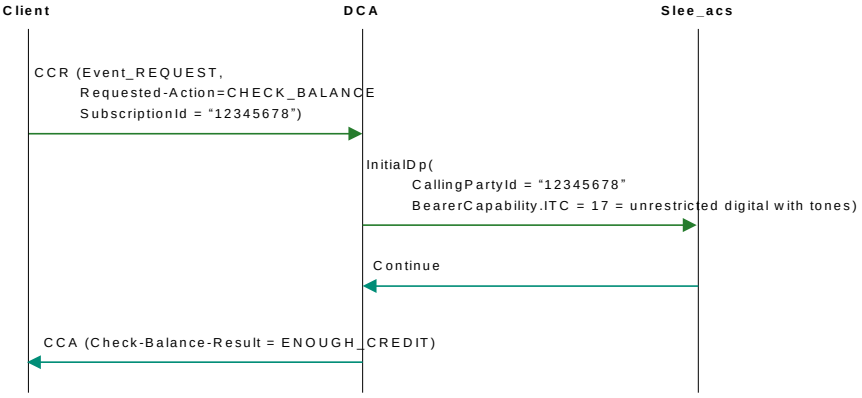
Multimedia messaging direct debit scenario

Here is an example multimedia messaging direct debit scenario.



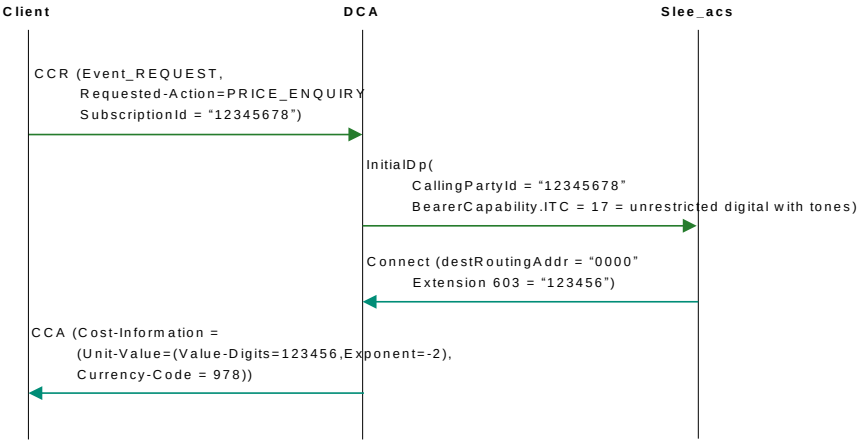
Check balance, with a result of enough credit

Here is an example check balance, with a result of enough credit.



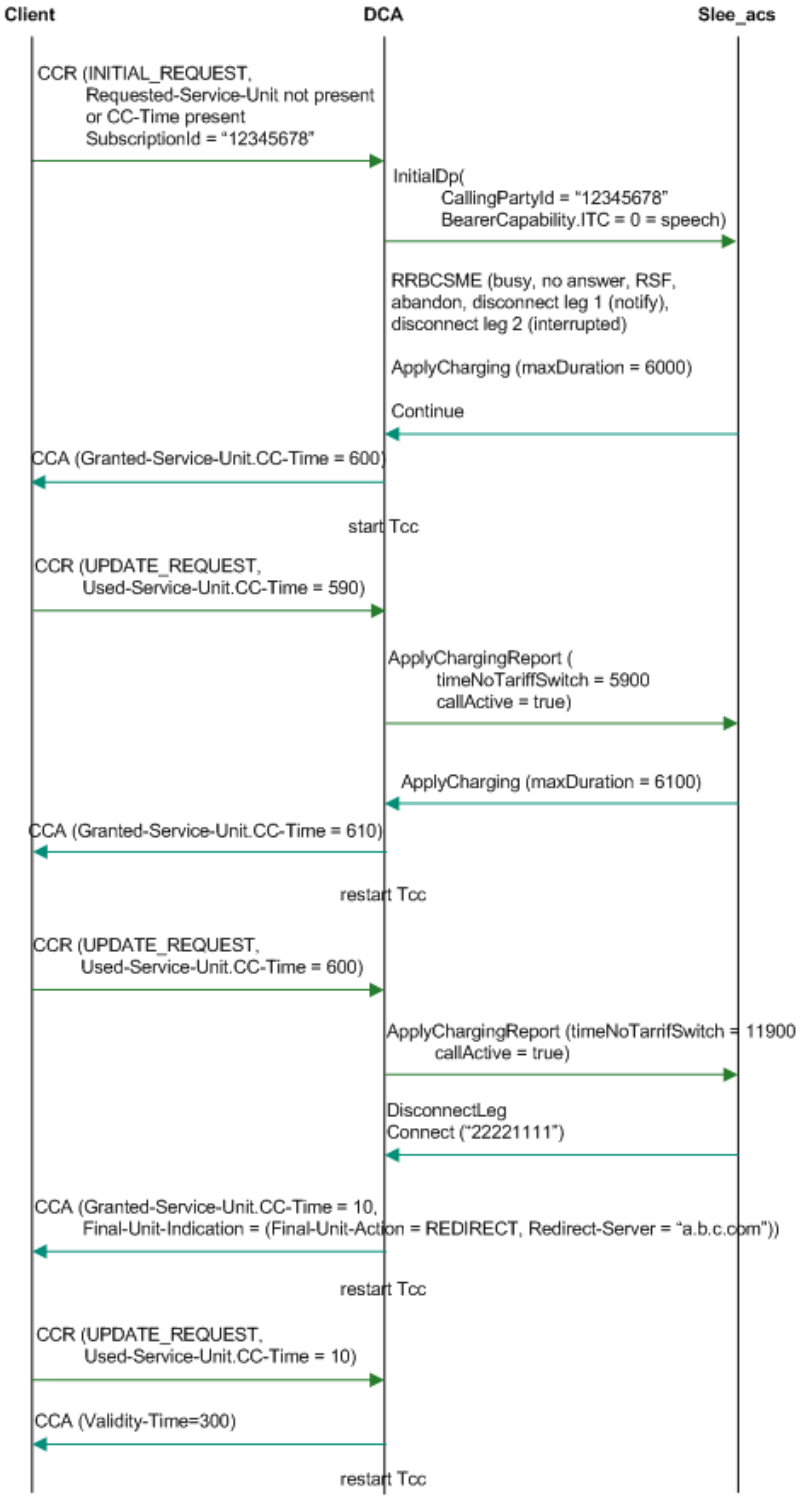
Price enquiry

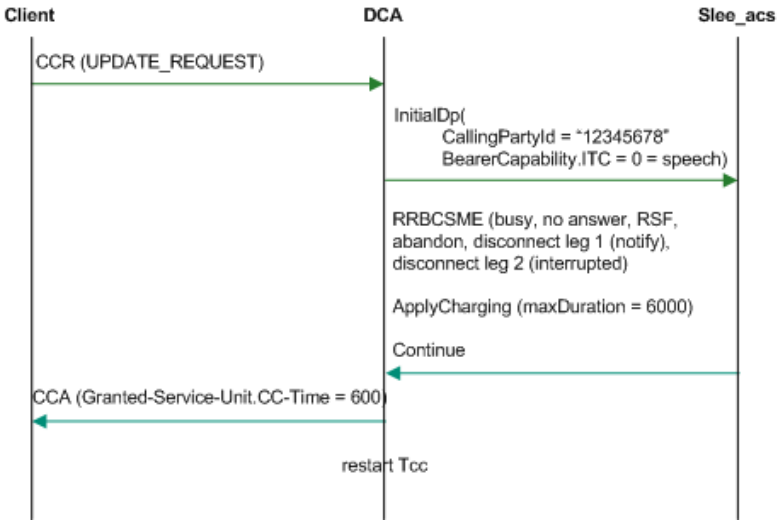
Here is an example price enquiry.



Funds expiry, redirect, top-up and reconnect

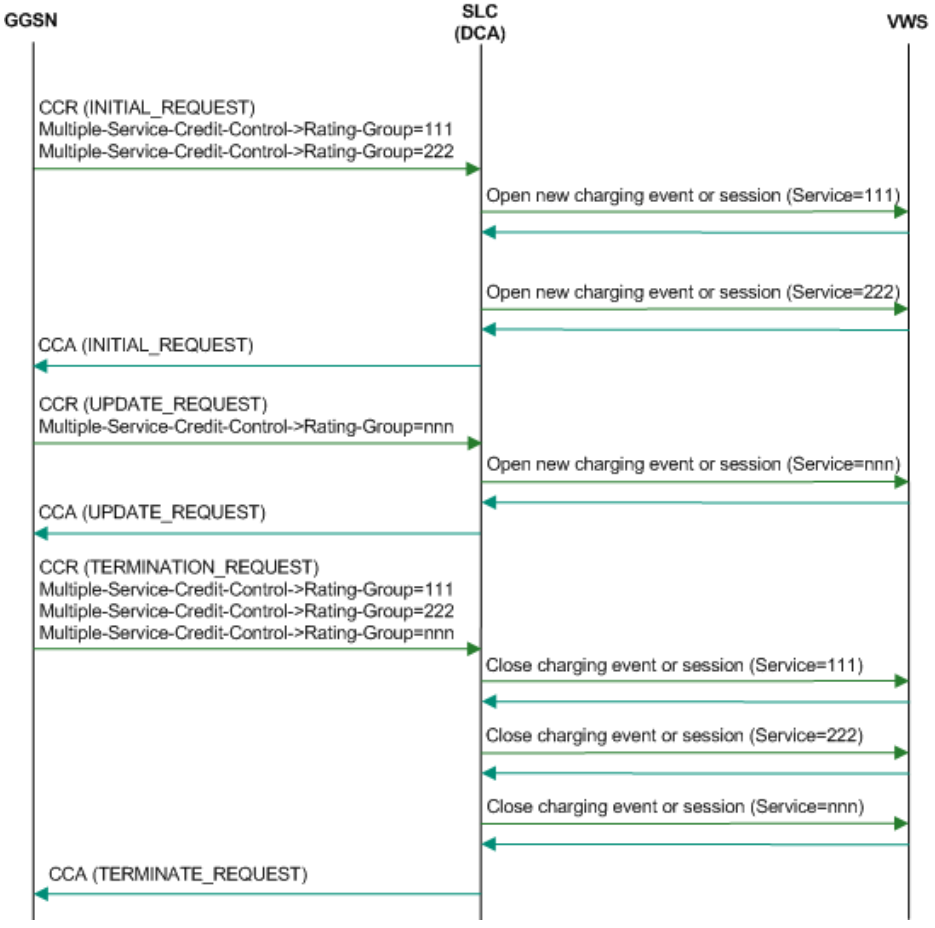
Here is an example funds expiry, redirect, top-up and reconnect.





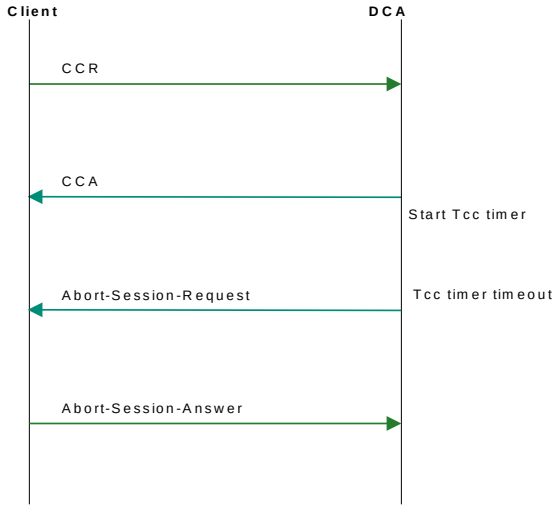
Multiple services credit control scenario

Here is an example multiple services credit control scenario.



Abort Session Request Scenario

Here is an example of an abort session request scenario.



Chapter 5

Compliance Tables

Overview

Introduction

This chapter identifies the level of compliance of DCA to Internet Engineering Task Force (IETF) specifications RFC 3588 and RFC 4006, and 3GPP TS 32.299 V10.4.

In this chapter

This chapter contains the following topics.

Compliance to RFC 3588

Introduction

This topic details the compliance of DCA with RFC 3588.

For more information about the compliance levels and notes referred to in the compliance tables, see *Compliance Levels and Considerations* (on page 76).

Introduction - Section 1

This table lists the compliances for section 1.

Section	Section Heading	Compliance Level	Comment
1	Introduction	N/A	

Protocol Overview - Section 2

This table lists the compliances for section 2.

Section	Section Heading	Compliance Level	Comment
2	Protocol Overview	N/A	
2.1	Transport	Fully compliant TCP + SCTP supported	TCP is selected by default
2.2	Security	Partially compliant IPSec through g/w function	
2.3	Application Compliance	Fully compliant	
2.4	Application Identification	Fully compliant	

Section	Section Heading	Compliance Level	Comment
2.5	Connection Management	Partially compliant	Credit-Control clients (or next hop peers) must establish connection to DCA. DCA does not establish outbound connections. Inbound connections are established and added to pool for use by Diameter sessions. Number of connections per realm is configurable.
2.6	Peers	N/A	A static list of permissible peers is configurable.
2.7	Realm Based Routing	Fully compliant	Responses will be returned to the same realm through the Peer from which the request was received.
2.8	Role of agents	N/A	
2.9	End-to-end security	Partial compliance	Only 'Never use end-to-end security' is supported
2.10	Path Authentication	N/A	

Headers - Section 3

This table lists the compliances for section 3.

Section	Section Heading	Compliance Level	Comment
3	Headers	N/A	
3.1	Command Codes	Partially compliant	CER, CEA, DWR, DWA, DPR, DPA, ASR, ASA supported.
3.2	ABNF Specification	Fully compliant	
3.3	Naming Conventions	Fully compliant	

Diameter AVPs - Section 4

This table lists the compliances for section 4.

Section	Section Heading	Compliance Level	Comment
4	Diameter AVPs	N/A	
4.1	AVP Header	Fully compliant	
4.2	Basic AVP Data Formats	Fully compliant for all basic types except float32 and float64. Partially compliant for float32 and float64. Float32 and Float64 treated as OctetString.	
4.3	Derived AVP Data Formats	Fully compliant	No specific AVPs are defined by default.
4.4	Grouped AVP Values	Fully compliant	
4.5	Diameter Base Protocol AVPs	Fully compliant	Support for all AVPs needed for compliance to section 3.1

Diameter AVPs - Section 4

This table lists the compliances for section 5.

Section	Section Heading	Compliance Level	Comment
5	Diameter Peers	N/A	
5.1	Peer Connections	Fully compliant	
5.2	Peer discovery	Non compliant	
5.3	Capability Exchange	Fully compliant	
5.4	Disconnecting Peer Connections	Fully compliant	
5.5	Transport Failure	Fully compliant	
5.6	Peer State Machine	Partially compliant	

Diameter Message Processing - Section 6

This table lists the compliances for section 6.

Section	Section Heading	Compliance Level	Comment
6	Diameter Message Processing		
6.1	Request Routing	Fully compliant	Please note that proxy and forward are not supported
6.2	Diameter Answer Processing	Fully compliant	
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	
6.8	Auth-Application-Id AVP	Fully compliant	Will be 4 for Credit-Control
6.9	Acct-Application-Id AVP	Fully compliant	Not used for Credit-Control
6.10	Inband-Security ID AVP	Fully compliant	
6.11	Vendor Specific Application-Id AVP	Fully compliant	No variable specific AVPs are defined today. See Section 9 for additional details.
6.12	Redirect-Host AVP	Non compliant	No explicit routing supported.
6.13	Redirect-Host-Usage AVP	Non compliant	
6.14	Redirect-Max-Cache-Time AVP	Non compliant	
6.15	E2E-Sequence AVP	Fully compliant	This AVP may be turned off to support peers which do not support this AVP

Error Handling - Section 7

This table lists the compliances for section 7.

Section	Section Heading	Compliance Level	Comment
7	Error Handling		
7.1	Result-Code AVP	Fully compliant	
7.2	Error Bit	Fully compliant	
7.3	Error-Message ACP	Fully compliant	
7.4	Error-Reporting-Host AVP	Fully compliant	
7.5	Failed-AVP AVP	Fully compliant	
7.6	Experimental Result ACP	Fully compliant	
7.7	Experimental Result Code AVP	Fully compliant	

Diameter User Sessions - Section 8

This table lists the compliances for section 8.

Section	Section Heading	Compliance Level	Comment
8	Diameter User Sessions		
8.1	Authorization Session State Machine	Non Complaint	
8.2	Accounting Session State Machine	Partially compliant	Implements only the server side of the state machine
8.3	Server-Initiated Re-Auth	Non compliant	
8.4	Session Termination	Not applicable	Not used by DCA for server-side Credit-Control
8.5	Abort Session	Fully compliant	
8.6	Inferring Session Termination from Origin-State-Id	Non compliant	
8.7	Auth-Request-Type AVP	Non compliant	
8.8	Session-Id AVP	Fully compliant	
8.9	Authorization-Lifetime AVP	Non compliant	
8.10	Auth-Grace-Period AVP	Non compliant	
8.11	Auth-Session-State AVP	Non compliant	
8.12	Re-Auth-Request AVP	Non compliant	
8.13	Session Timeout AVP	Fully compliant	
8.14	User Name AVP	Fully compliant	
8.15	Termination Cause	Fully compliant	

Section	Section Heading	Compliance Level	Comment
8.16	Origin State ID AVP	Fully compliant	`
8.17	Session Binding AVP	Non compliant	
8.18	Session-Server-Failover AVP	Non compliant	
8.19	Multi-Round-Time-Out AVP	Non compliant	
8.20	Class AVP	Non compliant	
8.21	Event Timestamp AVP	Fully compliant	

Accounting - Section 9

This table lists the compliances for section 9.

Section	Section Heading	Compliance Level	Comment
9	Accounting		
9.1	Server Directed Model	N/A - Offline.	See Note NC-1. Not applicable to DCA for offline charging. For online charging.
9.2	Protocol Messages	N/A - Offline.	See Note NC-1. Not applicable to DCA for offline charging. For online charging. No IP compression is supported at this time. Support for negotiation is however provided.
9.3	Application document requirements	N/A - Offline.	See Note NC-1. Not applicable to DCA for offline charging. For online charging. See Credit Control Application defined in RFC 4006.
9.4	Fault Resilience	N/A - Offline.	See Note NC-1. Not applicable to DCA for offline charging. For online charging. Please note that only the server side is implemented.
9.5	Accounting Records	N/A - Offline	See Note NC-1. Not applicable for Credit-Control or online charging.
9.6	Correlation of Accounting Records	N/A - Offline.	See Note NC-1. Not applicable for Credit-Control or online charging.
9.7	Accounting Command-Codes	N/A - Offline.	See Note NC-1. Not applicable for Credit-Control or online charging.
9.8	Accounting AVPs	N/A - Offline.	See Note NC-1. Not applicable for Credit-Control or online charging.

AVP Occurrence Table - Section 10

This table lists the compliances for section 10.

Section	Section Heading	Compliance Level	Comment
10	AVP Occurrence Table	Partial compliant	As detailed elsewhere in this document and as needed for CER, CEA, DWR, DWA, DPR, DPA.

IANA Considerations - Section 11

This table lists the compliances for section 11.

Section	Section Heading	Compliance Level	Comment
11	IANA Considerations		
11.1	AVP Header	Fully compliant	
11.2	AVP Codes	Fully compliant	
11.3	Application Identifiers	Fully compliant	
11.4	AVP Values	Fully compliant	As detailed elsewhere in this document and as needed for CER, CEA, DWR, DWA, DPR, DPA. Please note that unused AVPs are ignored by the client implementation.
11.5	Diameter TCP/SCTP Port Numbers	Fully compliant	
11.6	NAPR Service Fields	Fully compliant	This information is updated when the client package is installed

Diameter Protocol Related Configurable Parameters - Section 12

This table lists the compliances for section 12.

Section	Section Heading	Compliance Level	Comment
12	Diameter Protocol Related Configurable Parameters	Partial compliant	Statically configured peers are supported.

Security Considerations - Section 13

This table lists the compliances for section 13.

Section	Section Heading	Compliance Level	Comment
13	Security Considerations	Partially compliant	Note: Use of network provided IPSec may be used in deployments. TLS is not supported. End-to-End security is not supported.

Compliance to RFC 4006

Introduction

This topic details the compliance of DCA with RFC 4006.

For more information about the compliance levels and notes referred to in the compliance tables, see *Compliance Levels and Considerations* (on page 76).

Introduction - Section 1

This table lists the compliances for sections 4.2 and 4.3 of the "Programmer's Guide - Service Charging Based on Diameter Charging Control Node 5.

Section	Section Heading	Compliance Level	Comment
4.2.1	Messages	Fully compliant	
4.2.2	Diameter Base Protocol AVPs	Partially compliant	Refer to Draft 8 compliance above.
4.2.3	Defined Application Specific AVPs	Fully compliant	Values may be set according to configuration.
4.2.4	Description of Application Specific AVPs	Fully compliant	Values may be set according to configuration.
4.3.1	Service Charging Types	Fully compliant	
4.3.2	Service Charging Methods	Fully compliant	
4.3.3	List of Service Operations with Scenarios	Fully compliant	

Architecture Model - Section 2

This table lists the compliances for section 2.

Section	Section Heading	Compliance Level	Comment
2	Architecture Model	Partial compliant	Authentication and Authorization messages are not used.

Credit-Control Messages - Section 3

This table lists the compliances for section 3.

Section	Section Heading	Compliance Level	Comment
3	Credit-Control Messages	Fully compliant	

Credit-Control Application Overview - Section 4

This table lists the compliances for section 4.

Section	Section Heading	Compliance Level	Comment
4	Credit-Control Application Overview		
4.1	Service-Specific Rating Input and Interoperability	Fully compliant	Details of specific AVP implementation is given later in this document.

Session Based Credit-Control - Section 5

This table lists the compliances for section 5.

Section	Section Heading	Compliance Level	Comment
5	Session Based Credit-Control		
5.1.1	Basic Tariff-Time Change Support	Non compliant	
5.1.2	Credit Control for Multiple Services within a Sub Session	Partially compliant	Tariff-Change-Usage and G-S-U-Pool-Reference are not supported. See also notes on Service-Identifier AVP.
5.2	First Interrogation	Fully compliant	
5.3	Intermediate Interrogation	Fully compliant	
5.4	Final Interrogation	Fully compliant	
5.5	Server-Initiated Credit Re-Authorization	Non compliant	
5.6	Graceful Service Termination	Partially compliant	Graceful service termination with "Redirect Action" is supported.
5.7	Failure Procedures	Fully compliant	Managed through BFT in control plans.

One Time Event - Section 6

This table lists the compliances for section 6.

Section	Section Heading	Compliance Level	Comment
6	One Time Event		
6.1	Service Price Enquiry	Fully compliant	
6.2	Balance Check	Fully compliant	
6.3	Direct Debit	Fully compliant	
6.4	Refund	Fully compliant	
6.5	Failure Procedure	Fully compliant	

Credit-Control State Machine - Section 7

This table lists the compliances for section 7.

Section	Section Heading	Compliance Level	Comment
7	Credit-Control State Machine	Fully compliant	Server side only is implemented.

Credit-Control AVPs - Section 8

This table lists the compliances for section 8.

Note In the table below, where an AVP is labeled as "Non compliant", DCA has the ability to utilize the DCA AvpMapping Configuration and ACS to possibly enable partial or limited compliance. The DCA AvpMapping Configuration combined with the features provided by ACS and the ACS Control Plan together make up a powerful toolset for service design and permit further customization beyond the default capabilities provided by DCA.

Section	Section Heading	Compliance Level	Comment
8	Credit-Control AVPs		
8.1	CC-Correlation-ID AVP	Fully compliant	Ignored unless mapped to an IDP extension by the AVP mappings in **eserv.config**.
8.2	CC-Request-Number AVP	Fully compliant	Implemented as per suggestion in RFC 4006
8.3	CC-Request-Type AVP	Fully compliant	
8.4	CC-Session-Failover AVP	Fully compliant	Not set, which according to RFC is equivalent to AVP set to FAILOVER-NOT-SUPPORTED
8.5	CC-Sub-Session-Id AVP	Non compliant	
8.6	Check-Balance-Result AVP	Fully compliant	
8.7	Cost-Information AVP	Fully compliant	For Request-Action type PRICE_ENQUIRY, success case, this comes from the value of extension 603 in the INAP Connect. Otherwise, not set.
8.8	Unit Value	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-Debit-Failure-Handling	Fully compliant	
8.16	Multiple-Services-	Partially compliant	Tariff-Change-Usage and G-S-U-Pool-

Section	Section Heading	Compliance Level	Comment
	Credit-Control AVP		Reference are not supported.
8.17	Granted-Service-Unit AVP	Fully compliant	Multiple unit types are fully supported, for Basic Credit Control as well as Multiple Services Credit Control. In the case of Multiple Services Credit Control, one or more unit types are permitted per Multiple-Services-Credit-Control AVP.
8.18	Requested-Service-Unit AVP	Fully compliant	Multiple unit types are fully supported, for Basic Credit Control as well as Multiple Services Credit Control. In the case of Multiple Services Credit Control, one or more unit types are permitted per Multiple-Services-Credit-Control AVP.
8.19	Used-Service-Unit AVP	Fully compliant	Multiple unit types are fully supported, for Basic Credit Control as well as Multiple Services Credit Control. In the case of Multiple Services Credit Control, one or more unit types are permitted per Multiple-Services-Credit-Control AVP.
8.20	Tariff-Time-Change AVP	Non 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 ACP	Fully compliant	
8.25	CC-Output-Octets ACP	Fully compliant	
8.26	CC-Service-Specific-Units AVP	Fully compliant	
8.27	Tariff-Change-Usage AVP	Non compliant	
8.28	Service-Identifier AVP	Fully compliant	For multiple services, DCA allows for one or more service-identifier per Multiple-Services-Credit-Control (MSCC) AVP. Where both Service-Identifier and Rating-Group have been specified within the same MSCC AVP, the Service-Identifier will take precedence. If multiple Service-Identifier AVPs are provided per Multiple-Services-Credit-Control AVP, then DCA may be configured to either: • Only charge for the first Service-Identifier encountered. This is based on the following statement in RFC 4006: "Note that each instance of this AVP carries units related to one or more services or related to a single rating group." • Or create a separate charging sub-

Section	Section Heading	Compliance Level	Comment
			session, for each session identifier supplied. In this case each charging sub-session will be reported back in a separate Multiple-Services-Credit-Control AVP.
8.29	Rating-Group AVP	Fully compliant	For multiple services, DCA allows for multiple MSCC AVPs with each MSCC containing a different RatingGroup. If more than one Multiple-Services-Credit-Control AVP are received (each containing a distinct Rating Group), then DCA will create a separate charging sub-session, for each Rating Group supplied. In this case each charging sub-session will be reported back in a separate Multiple-Services-Credit-Control AVP.
8.30	G-S-U Pool Reference AVP	Non compliant	
8.31	G-S-U Pool Identifier AVP	Non compliant	
8.32	CC-Unit-Type AVP	Fully compliant	
8.33	Validity-Time AVP	Fully compliant	
8.34	Final-Unit-Indication AVP	Fully compliant	
8.35	Final-Unit-Action AVP	Fully compliant	
8.36	Restriction-Filter-Rule AVP	Non compliant	These rules are defined using the Oracle Control Plan Editor.
8.37	Redirect-Server AVP	Fully compliant	Please note that SIP E.164 addresses must be used for voice and SMS sessions
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	Fully compliant	
8.42	Service-Context-Id AVP	Fully compliant	
8.43	Service-Parameter-Info AVP	Fully compliant	May be mapped in configuration to indicate supplementary rating information.
8.44	Service-Parameter-Type AVP	Fully compliant	May be mapped in configuration to indicate supplementary rating information.
8.45	Service-Parameter-Value AVP	Fully compliant	May be mapped in configuration to indicate supplementary rating information.
8.46	Subscription-Id AVP	Fully compliant	
8.47	Subscription-Id-Type AVP	Fully compliant	E164 and SIP URI are used today.

Section	Section Heading	Compliance Level	Comment
8.48	Subscription-Id-Data AVP	Fully compliant	
8.49	User-Equipment-Info AVP	Compliant by Configuration	See Note C-1.
8.50	User-Equipment-Info-Type AVP	Non compliant	Ignored unless mapped to an IDP extension by the AVP mappings in **eserv.config**.
8.51	User-Equipment-Info-Data AVP	Non compliant	

Result Code AVP Values - Section 9

This table lists the compliances for section 9.

Section	Section Heading	Compliance Level	Comment
9	Result Code AVP Values		
9.1	Transient Failures	Fully compliant	
9.2	Permanent Failures	Fully compliant	

AVP Occurrence Table - Section 10

This table lists the compliances for section 10.

Section	Section Heading	Compliance Level	Comment
10	AVP Occurrence Table		
10.1	Credit-Control AVP Table	Fully compliant	
10.2	Re-Auth-Request/Answer Table AVP	Non compliant	

RADIUS/Diameter Credit-Control Interworking Model - Section 11

This table lists the compliances for section 11.

Section	Section Heading	Compliance Level	Comment
11	RADIUS/Diameter Credit-Control Interworking Model	Fully compliant	

IANA Considerations - Section 12

This table lists the compliances for section 12.

Section	Section Heading	Compliance Level	Comment
12	IANA Considerations	Fully compliant	

Credit-Control Application Related Parameters - Section 13

This table lists the compliances for section 13.

Section	Section Heading	Compliance Level	Comment
13	Credit-Control Application Related Parameters	Fully compliant	Tcc session supervision timer is supported timers are supported.

Security Considerations - Section 14

This table lists the compliances for section 14.

Section	Section Heading	Compliance Level	Comment
14	Security Considerations	Partially compliant	Use of network provided IPSec may be used in deployments.
14.1	Direct Connection with Redirect	Non compliant	Statically configured peers are supported.

Compliance to 3GPP TS 32.299 V10.4

Introduction

This topic details the compliance of DCA with 3GPP TS 32.299 V10.4.

For more information about the compliance levels and notes referred to in the compliance tables, see *Compliance Levels and Considerations* (on page 76).

3GPP TS 32.299 V11.3.0 compliance

Compliance is specified for 3GPP TS 32.299 V10.4 specification with the following highlighted:

- **[V11.3]** - Where this mark appears, the specific section only applies to V11.3 of the specification.

Section 5

DCA is an on-line charging application. All references and text relating to off-line charging are not applicable and are marked as "N/A - Offline" in the tables below.

This table lists the compliances for Section 5.

Section	Section Heading	Compliance Level	Comment
5	3GPP charging applications requirements	Fully compliant for On-line Charging only	
5.1	Offline Charging Scenarios	N/A - Offline	Offline charging not applicable to DCA Note NC-1
5.2	Online Charging scenarios		
5.2.1	Basic principles		
5.2.2	Charging Scenarios		
5.2.2.1	Immediate Event Charging		
5.2.2.1.1	Decentralized Unit Determination and Centralized Rating	Fully compliant	Debit Units Request will be implemented in Credit-Control-Request (CCR) and Debit Units Response in Credit-Control-Answer (CCA).
5.2.2.1.2	Centralized Unit Determination and Centralized Rating	Fully compliant	As above
5.2.2.1.3	Decentralized Unit Determination and Decentralized Rating	Fully compliant	As above
5.2.2.1.4	Further Options	N/A	Service delivery options are not determined by DCA.
5.2.2.2	Event charging with Reservation		
5.2.2.2.1	Decentralized Unit Determination and Centralized Rating	Fully compliant	Debit Units Request will be implemented in Credit-Control-Request (CCR) and Debit Units Response in Credit-Control-Answer (CCA).
5.2.2.2.2	Centralized Unit Determination and Centralized Rating	Fully compliant	
5.2.2.2.3	Decentralized Unit Determination and Decentralized Rating	Fully compliant	
5.2.2.3	Session charging with Reservation		
5.2.2.3.1	Decentralized Unit Determination and Centralized Rating	Fully compliant	Debit Units Request will be implemented in Credit-Control-Request (CCR) and Debit Units Response in Credit-Control-Answer (CCA).
5.2.2.3.2	Centralized Unit Determination and Centralized Rating	Fully compliant	
5.2.2.3.3	Decentralized Unit Determination and Decentralized Rating	Fully compliant	

Section	Section Heading	Compliance Level	Comment
5.2.3	Basic Operations	Compliant using CCR/CCR messages. See Section *Credit Control Request and Response AVPs* (on page 11) for details.	DCA messages for the Debit / Reserve Unit Request operation is Credit-Control-Request (CCR) and for the Debit / Reserve Unit Response operation is Credit-Control-Answer (CCA) as specified in RFC 4006.
5.3	Other requirements		
5.3.1	Re-authorization	Compliant by Configuration	Compliant by Configuration with limitations. Mid-Session tariff changes may not be possible. See Note C-3 and Note C-1 for limitations.
5.3.2	Threshold based re-authorization triggers	Non compliant	
5.3.3	Termination action	Compliant	
5.3.4	Account Expiration	Compliant by Configuration	Compliant by Configuration with limitations. May require use of other NCC products and additional set up and signaling or traffic handling requirements. Also see Note C-3 and Note C-1 for other limitations

Section 6

This table lists the compliances for Section 6.

Section	Section Heading	Compliance Level	Comment
6	3GPP Charging Applications – Protocol Aspects	-	
6.1	Basic Principles for Diameter Offline Charging	N/A - Offline	Offline charging not applicable for DCA Note NC-1
6.1.1	Event based charging	N/A - Offline	Not Applicable, For Offline Charging
6.1.2	Session based charging	N/A - Offline	Not Applicable, For Offline Charging
6.1.3	Offline charging error cases - Diameter procedures	N/A - Offline	Not Applicable, For Offline Charging
6.1.3.1	CDF connection failure	N/A - Offline	Not Applicable, For Offline Charging
6.1.3.2	No reply from CDF	N/A - Offline	Not Applicable, For Offline Charging
6.1.3.3	Duplicate detection	N/A - Offline	Not Applicable, For Offline Charging
6.1.3.4	CDF detected failure		
6.2	Message Contents for Offline Charging	-	
6.2.1	Summary of Offline Charging Message Formats	N/A - Offline	Not Applicable, For Offline Charging

Section	Section Heading	Compliance Level	Comment
6.2.1.1	General	N/A - Offline	Not Applicable, For Offline Charging
6.2.1.2	Structure for the Accounting Message Formats	N/A - Offline	Not Applicable, For Offline Charging
6.2.2	Accounting-Request Message	N/A - Offline	Not Applicable, For Offline Charging
6.2.3	Accounting-Answer Message	N/A - Offline	Not Applicable, For Offline Charging
6.3	Basic Principles for Diameter Online charging	-	
6.3.1	Online Specific Credit Control Application Requirements	Fully compliant	
6.3.2	Diameter Description on the Ro reference point	-	
6.3.2.1	Basic Principles	N/A	
6.3.3	Immediate Event Charging (IEC)	Fully compliant	DCA supports Event Request with DirectDebit requested action. DCA also supports the Refund Account, Check Balance, Price Enquiry requested actions (RFC 4006).
6.3.4	Event Charging with Unit Reservation (ECUR)	Fully compliant	DCA supports Initial Request followed by Terminate Request CCR/CCA messages.
6.3.5	Session Charging with Unit Reservation (SCUR)	Fully compliant	DCA supports Initial Request followed by one or more Update Requests CCR/CCA and a Terminate Request CCR/CCA.
6.3.6	Error Cases and Scenarios	Fully compliant	DCA always sends TERMINATE Credit-Control-Failure-Handling AVP to the network element.
6.3.6.1	Duplicate Detection	Fully compliant	
6.3.6.2	Reserve Units and Debit Units Operation Failure	Fully compliant. For compliance to RFC 3588 and RFC 4006, see sections above titled: • *Compliance to RFC 3588* (on page 27) • *Compliance to RFC 4006* (on page 33)	
6.3.7	Support of Tariff Changes during an Active User Session		
6.3.7.1	Support of Tariff Changes using the Tariff Switch Mechanism	Non compliant	

Section	Section Heading	Compliance Level	Comment
6.3.7.2	Support of Tariff Changes using Validity Time AVP	Partially compliant	When the validity-time is up (as indicated by the AVP), the client must come back to ask for more. At this point the rating engine (VWS) can choose to grant more quota which is charged at a different new rate.
6.3.8	Support of Re-authorisation	Non compliant	
6.3.9	Support of Failure Handling	Partially compliant	CTF aspects are not applicable. DCA is fully compliant for the OCF aspects for the TERMINATE Credit Control Failure Handling AVP; DCA always send the TERMINATE Credit Control Failure Handling AVP in the CCA. Other Credit Control Failure Handling AVP values are not used.
6.3.10	Support of Failover	Non compliant	DCA does not support mid-session failover within a realm, as described in RFC 4006, including the use of the CC-Session-Failover AVP. Failover of newly commenced Credit Control sessions to different SLCs is permitted.
6.3.11	Credit Pooling	Non compliant	
6.4	Message formats for Online Charging	-	
6.4.1	Summary of Online Charging Message Formats	-	
6.4.1.1	General	N/A	
6.4.1.2	Structure for the Credit Control Message Formats	N/A	
6.4.2	Credit-Control-Request Message	Fully compliant	DCA fully complies to the CCR message format structure. However, not all optional AVPs may be supported. See section titled *Credit Control Request and Response AVPs* (on page 11).
6.4.3	Credit-Control-Answer Message	Fully compliant	DCA fully complies to the CCA message format structure. However, not all optional AVPs may be supported. See section titled *Credit Control Request and Response AVPs* (on page 11).
6.4.4	Re-Auth-Request Message	Non compliant	
6.4.5	Re-Auth-Answer Message	Non compliant	
6.4.6	Capabilities-Exchange-Request Message	Fully compliant	DCA fully complies with the CER message format structure. See section titled *Capabilities Exchange Messages* (on page 7) for further details.

Section	Section Heading	Compliance Level	Comment
6.4.7	Capabilities-Exchange-Answer Message	Fully compliant	DCA fully complies with the CEA message format structure. See section titled *Capabilities Exchange Messages* (on page 7) for further details.
6.4.8	Device-Watchdog-Request Message	Fully compliant	DCA fully complies with the message format structure. See section titled *Device Watchdog Messages* (on page 9) for further details.
6.4.9	Device-Watchdog-Answer Message	Fully compliant	DCA fully complies with the message format structure. See section titled *Device Watchdog Messages* (on page 9) for further details.
6.4.10	Disconnect-Peer-Request Message	Fully compliant	DCA fully complies with the message format structure. See section titled *Disconnect Peer Messages* (on page 8) for further details.
6.4.11	Disconnect-Peer-Answer Message	Fully compliant	DCA fully complies with the message format structure. See section titled *Disconnect Peer Messages* (on page 8) for further details.
6.4.12	Abort-Session-Request Message	Fully compliant	DCA fully complies with the message format structure. See section titled *Abort Session Request (ASR)* (on page 19) for further details.
6.4.13	Abort-Session -Answer Message	Fully compliant	DCA fully complies with the message format structure. See section titled *Abort Session Request (ASR)* (on page 19) for further details.
6.5	Other procedural description of the 3GPP charging applications	-	
6.5.1	Re-authorization	-	
6.5.1.1	Idle timeout	Compliant by Configuration	Fully compliant without additional configuration, that is, if this AVP is not present, a locally configurable default value in the client shall be used. If DCA is configured with a Quota-Holding-Time value of zero, this indicates that this mechanism shall not be used. For non-zero configured times, compliant with Limitations. See Note C-3. If configured for a specific service, Quota-Holding-Time AVP can be statically set or mapped from ACS through a field set by the Control Plan. The timer is run on the client and DCA still relies on Requested/Granted/Used-Service-Units AVPs.
6.5.1.2	Change of charging conditions	Non compliant	
6.5.1.3	Reporting quota usage	Non compliant	

Section	Section Heading	Compliance Level	Comment
6.5.2	Threshold based re-authorization triggers	Fully compliant	DCA has Quota Threshold configurations which are used in MSCC.
6.5.3	Termination action	Fully compliant	DCA support "REDIRECT" Final-Units-Action AVP and redirect to a Redirect Server.
6.5.4	Quota consumption time	Non compliant	The 3GPP specification states "The server may optionally indicate...". This is optional functionality which is not implemented.
6.5.5	Service Termination	Fully compliant	The CCA Result Code is configurable. Also see section titled *Abort Session Request (ASR)* (on page 19).
6.5.6	Envelope reporting	Non compliant	
6.5.7	Combinational quota	Non compliant	
6.5.8	Online control of offline charging information	Non compliant	
6.6	Bindings of the operation to protocol application		
6.6.1	Bindings of Charging Data Transfer to Accounting	N/A - Offline	
6.6.2	Bindings of Debit / Reserve Units to Credit-Control	Fully compliant	DCA uses the DCCA shown in the table. See "*Credit Control Requests* (on page 11)" for details.

Section 7

This table lists the compliances for section 7.

Section	Section Heading	Compliance Level	Comment
7	Summary of used Attribute Value		
7.1	Diameter AVPs	See *7.1 - Use Of IETF Diameter AVPs* (on page 45)	
7.2	3GPP specific AVPs	See *7.2 - 3GPP specific AVPs* (on page 51)	
7.3	3GPP2 Accesses specific AVPs	Compliant by Configuration	Note C-3, Note NC-4

7.1 - Use Of IETF Diameter AVPs

This table lists the compliances for section 7.1

AVP Name	AVP Code	ACR	ACA	CCR	CCA	Value Type	Compliance Level	Comment	Reference
Accounting-Input-Octets	363	OC	-	-	-	Unsigned64	N/A - Offline	Note NC-1	7.1.1
Accounting-Input-	365	OC	-	-	-	Unsigned6	N/A - Offline	Note NC-1	7.1.2

AVP Name	AVP Code	ACR	ACA	CCR	CCA	Value Type	Compliance Level	Comment	Reference
Packets						4			
Accounting-Output-Octets	364	OC	-	-	-	Unsigned64	N/A - Offline	Note NC-1	7.1.3
Accounting-Output-Packets	366	OC	-	-	-	Unsigned64	N/A - Offline	Note NC-1	7.1.4
Accounting-Realtime-Required	483	-	-	-	-	Enumerated	N/A - Offline	Note NC-1	
Accounting-Record-Number	485	M	M	-	-	Unsigned32	N/A - Offline	Note NC-1	
Accounting-Record-Type	480	M	M	-	-	Enumerated	N/A - Offline	Note NC-1	
Accounting-Sub-Session-Id	287	-	-	-	-	Unsigned64	N/A - Offline	Note NC-1	
Acct-Application-Id	259	OC	OC	-	-	Unsigned32	Compliant by Configuration	Fully compliant when used in Capabilities Negotiation. Compliant by Configuration when used as statically mapped AVP or mapped from ACS field through Control Plan.	7.1.5
Acct-Interim-Interval	85	OC	OC	-	-	Unsigned32	N/A - Offline	Note NC-1	
Acct-Multi-Session-Id	50	-	-	-	-	Unsigned32	Partially compliant	Not sent but will be returned in CCA if received in CCR.	
Acct-Session-Id	44	-	-	-	-	OctetString	Non compliant		
Auth-Application-Id	258	-	-	M	M	Unsigned32	Fully compliant		7.1.6
AVP	*	-	-	-	-	Grouped	-		
Called-Station-Id	30	OC	-	OC	-	UTF8String	Compliant by Configuration	Note C-1	7.1.7
CC-Correlation-Id	411	-	-	OC	-	OctetString	Compliant by Configuration	Note C-1, Note NC-4	
CC-Input-Octets	412	-	-	OC	OC	Unsigned64	Fully compliant	Basic Credit Control and MSCC	
CC-Money	413	-	-	-	-	Grouped	Fully compliant	Basic Credit Control and MSCC	
CC-Output-Octets	414	-	-	OC	OC	Unsigned64	Fully compliant	Basic Credit Control and MSCC	
CC-Request-Number	415	-	-	M	M	Unsigned32	Fully compliant		
CC-Request-Type	416	-	-	M	M	Enumerate	Fully		

AVP Name	AVP Code	ACR	ACA	CCR	CCA	Value Type	Compliance Level	Comment	Reference
						d	compliant		
CC-Service-Specific-Units	417	-	-	OC	OC	Unsigned64	Fully compliant	Basic Credit Control and MSCC	
CC-Session-Failover	418	-	-	-	OC	Enumerated	Non compliant		
CC-Sub-Session-Id	419	-	-	-	-	Unsigned64	Fully compliant	Will be returned in CCA if received in CCR.	
CC-Time	420	-	-	OC	OC	Unsigned32	Fully compliant	Basic Credit Control and MSCC	
CC-Total-Octets	421	-	-	OC	OC	Unsigned64	Fully compliant	Basic Credit Control and MSCC	
CC-Unit-Type	454	-	-	-	M	Enumerated	Compliant by configuration	Note C-1	
Check-Balance-Result	422	-	-	-	-	Enumerated	Fully compliant	For Check Balance	
Cost-Information	423	-	-	-	OC	Grouped	Fully compliant	For Price Enquiry	
Cost-Unit	424	-	-	-	OC	UTF8String	Fully compliant	For Price Enquiry	
Credit-Control	426	-	-	-	-	Enumerated	-		
Credit-Control-Failure-Handling	427	-	-	-	OC	Enumerated	Fully compliant	Always set to TERMINATE	
Currency-Code	425	-	-	-	M	Unsigned32	Fully compliant	Basic Credit Control and MSCC	
Destination-Host	293	-	-	OC	-	DiamIdent	Fully compliant		
Destination-Realm	283	M	-	M	-	DiamIdent	Fully compliant		
Direct-Debiting-Failure-Handling	428	-	-	-	OC	Enumerated	Compliant by Configuration	Note C-3	
Error-Message	281	-	-	-	-	UTF8String	Compliant by Configuration	Note C-3	
Error-Reporting-Host	294	-	OC	-	-	DiamIdent	N/A - Offline	Note NC-1	
Event-Timestamp	55	OC	OC	OC	-	Time	Fully compliant		7.1.8
Exponent	429	-	-	-	OC	Integer32	Fully compliant		
Failed-AVP	279	-	-	-	OC	Grouped	Fully compliant		
Filter-Id	11	-	-	-	OC	UTF8String	Non compliant		
Final-Unit-Action	449	-	-	-	OC	Enumerated	Fully compliant	Set to TERMINATE or REDIRECT	

AVP Name	AVP Code	ACR	ACA	CCR	CCA	Value Type	Compliance Level	Comment	Reference
Final-Unit-Indication	430	-	-	-	OC	Grouped	Fully compliant	Set for Final Unit Action REDIRECT	
Granted-Service-Unit	431	-	-	-	OC	Grouped	Fully compliant	Basic Credit Control and MSCC	
G-S-U-Pool-Identifier	453	-	-	-	OC	Unsigned32	Non compliant	Note NC-5	
G-S-U-Pool-Reference	457	-	-	-	OC	Grouped	Non compliant	Note NC-5	
Location-Type	IANA	OC	-	OC	-	refer [403]	Compliant by Configuration	Note C-1	
Location-Information	IANA	OC	-	OC	-	refer [403]	Compliant by Configuration	Note C-1	
Multiple-Services-Credit-Control	456	-	-	OC	OC	Grouped	Partially compliant	Fully compliant with the supported sub-AVPs shown below: Granted-Service-Unit Requested-Service-Unit Used-Service-Unit Service-Identifier Rating-Group Validity-Time Result-Code Time-Quota-Threshold Volume-Quota-Threshold Final-Unit-Indication Non compliant or Partially compliant by configuration if the following AVPs can be statically set or mapped from ACS fields through the Control Plan: Tariff-Change-Usage Unit-Quota-Threshold Quota-Holding-Time Quota-	7.1.9

AVP Name	AVP Code	ACR	ACA	CCR	CCA	Value Type	Compliance Level	Comment	Reference
								Consumption-Time Reporting-Reason Trigger PS-Furnish-Charging-Information Refund-Information AF-Correlation-Information Envelope Envelope-Reporting Time-Quota-Mechanism Service-Specific-Info QoS-Information AVP	
Multiple-Services-Indicator	455	-	-	OM	-	Enumerated	Fully compliant		
Operator-Name	IANA	OC	-	OC	-	refer [403]	Compliant by Configuration	Note C-1	
Origin-Host	264	M	M	M	M	DiamIdent	Fully compliant		
Origin-Realm	296	M	M	M	M	DiamIdent	Fully compliant		
Origin-State-Id	278	OC	OC	OC	-	Unsigned32	Fully compliant		
Proxy-Info	284	OC	OC	OC	OC	Grouped	Compliant by Configuration	Note C-1, Note C-3	
Proxy-Host	280	M	M	M	M	DiamIdent	Compliant by Configuration	Note C-1, Note C-3	
Proxy-State	33	M	M	M	M	OctetString	Compliant by Configuration	Note C-1, Note C-3	
Rating-Group	432	OC	-	OC	OC	Unsigned32	Fully compliant		7.1.10
Redirect-Address-Type	433	-	-	M	M	Enumerated	Fully compliant		
Redirect-Host	292	-	-	-	OC	DiamURI	Non compliant	Note NC-5	
Redirect-Host-Usage	261	-	-	-	OC	Enumerated	Non compliant	Note NC-5	
Redirect-Max-Cache-Time	262	-	-	-	OC	Unsigned32	Non compliant	Note NC-5	
Redirect-Server	434	-	-	-	OC	Grouped	Fully compliant		
Redirect-Server-	435	-	-	-	M	UTF8String	Fully		

AVP Name	AVP Code	ACR	ACA	CCR	CCA	Value Type	Compliance Level	Comment	Reference
Address							compliant		
Requested-Action	436	-	-	OC	-	Enumerated	Fully compliant		
Requested-Service-Unit	437	-	-	OC	-	Grouped	Fully compliant	Basic Credit Control and MSCC	
Restriction-Filter-Rule	438	-	-	-	OC	IPFilterRule	Non compliant		
Result-Code	268	-	M	-	M	Unsigned32	Fully compliant	Basic Credit Control and MSCC Additional mapping flexibility available through DCA AvpMapping Configuration	7.1.11
Route-Record	282	OC	-	OC	OC	DiamIdent	Compliant by Configuration	Note C-1, Note C-3 ACS Control Plan Modify Node	
Service-Context-Id	461	OM	-	M	-	UTF8String	Fully compliant		7.1.12
Service-Identifier	439	OC	-	OC	OC	Unsigned32	Fully compliant	Basic Credit Control and MSCC	7.1.13
Service-Parameter-Info	440	-	-	-	-	Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-1 See sub-AVPs: Service-Parameter-Type Service-Parameter-Value	
Service-Parameter-Type	441	-	-	-	-	Unsigned32	Compliant by Configuration	Note C-1	
Service-Parameter-Value	442	-	-	-	-	OctetString	Compliant by Configuration	Note C-1	
Session-Id	263	M	M	M	M	UTF8String	Fully compliant		
Subscription-Id	443	OC	-	OM	-	Grouped	Fully compliant		
Subscription-Id-Data	444	M	-	M	-	UTF8String	Fully compliant		
Subscription-Id-Type	450	M	-	M	-	Enumerated	Fully compliant		
Tariff-Change-Usage	452	-	-	OC	-	Enumerated	Non compliant		
Tariff-Time-Change	451	-		-	OC	Time	Non compliant	Note NC-5	
Termination-Cause	295	OC	-	-	-	Enumerated	N/A - Offline	Note NC-1	

AVP Name	AVP Code	ACR	ACA	CCR	CCA	Value Type	Compliance Level	Comment	Reference
Unit-Value	445	-		-	M	Grouped	Fully compliant		
Used-Service-Unit	446	-		OC	-	Grouped	Fully compliant	Basic Credit Control and MSCC	7.1.14
User-Equipment-Info	458	OC		OC	-	Grouped	Compliant by configuration	Note C-1	
User-Equipment-Info-Type	459	OM		M	-	Enumerated	Compliant by Configuration	Note C-1	
User-Equipment-Info-Value	460	OM		M	-	OctetString	Compliant by Configuration	Note C-1	
User-Name	1	OC	OC	OC	-	UTF8String	Compliant by Configuration	Note C-1	7.1.15
Value-Digits	447	-	-	-	M	Integer64	Fully compliant		
Validity-Time	448	-	-	-	OC	Unsigned32	Fully compliant		
Vendor-Id	266	-	-	-	-	Unsigned32	Fully compliant		7.1.16
Vendor-Specific-Application-Id	260	-	-	-	-	Grouped	Compliant by Configuration	Inbuilt support if configured. See sub-AVPs: Vendor-Id Auth-Application-Id Acct-Application-Id	

7.2 - 3GPP specific AVPs

DCA is an on-line charging application; off-line charging is not applicable.

The table below specifies the compliance level for on-line charging only.

For example:

- Where an AVP is marked as both off-line and on-line, the compliance level stated is for on-line charging only.
- Where an AVP is marked as only for off-line use, the AVP is marked as Non-compliant.

This table lists the compliances for section 7.2.

AVP Name	AVP Code	ACR	ACA	CCR	CCA	Value Type	Compliance Level	Comment	Reference
3GPP-Charging-Characteristics	13	X	-	X	-	refer [207]	Compliant by configuration	Note NC-5	3GPP TS 29.061 (PLMN↔PDN)
3GPP-Charging-Id	2	X	-	X	-	refer [207]	Compliant by configuration	Note C-1, Note NC-4	3GPP TS 29.061 (PLMN↔PDN)
3GPP-GGSN-MCC-MNC	9	X	-	X	-	refer [207]	Compliant by configuration	Note G-2, Note C-2	3GPP TS 29.061 (PLMN↔PDN)
3GPP-IMSI	1	-	-	X	-	refer [207]	Compliant by configuration	Note G-2, Note C-2	3GPP TS 29.061 (PLMN↔PDN) 3GPP TS 32.271

AVP Name	AVP Code	ACR	ACA	CCR	CCA	Value Type	Compliance Level	Comment	Reference
									(LCS)
3GPP-IMSI-MCC-MNC	8	X	-	X	-	refer [207]	Compliant by configuration	Note G-2, Note C-2	3GPP TS 29.061 (PLMN↔PDN)
3GPP-MS-TimeZone	23	X	-	X	-	refer [207]	Compliant by configuration	Note C-1, Note G-2	3GPP TS 29.061 (PLMN↔PDN)
3GPP-NSAPI	10	X	-	X	-	refer [207]	Compliant by configuration	Note C-1, Note G-2	3GPP TS 29.061 (PLMN↔PDN)
3GPP-PDP-Type	3	X	-	X	-	refer [207]	Compliant by configuration	Note C-1, Note G-2	3GPP TS 29.061 (PLMN↔PDN)
3GPP-RAT-Type	21	X	-	X	-	refer [207]	Compliant by configuration	Note C-1, Note G-2	3GPP TS 29.061 (PLMN↔PDN) 3GPP TS 32.251 (PS) - Sec 6.3.2.1 3GPP TS 32.270 (MMS)
3GPP-Selection-Mode	12	X	-	X	-	refer [207]	Compliant by configuration	Note C-1, Note G-2	3GPP TS 29.061 (PLMN↔PDN)
3GPP-Session-Stop-Indicator	11	-	-	X	-	refer [207]	Compliant by configuration	Note C-1	3GPP TS 29.061 (PLMN↔PDN)
3GPP-SGSN-MCC-MNC	18	X	-	X	-	refer [207]	Compliant by configuration	Note G-2,-Note C-2	3GPP TS 29.061 (PLMN↔PDN)
3GPP-User-Location-Info	22	X	-	X	-	refer [207]	Compliant by configuration	Note G-2, Note C-1	3GPP TS 29.061 (PLMN↔PDN) 3GPP TS 32.251 (PS) - Sec 6.3.2.1 3GPP TS 32.270 (MMS)
Access-Network-Charging-Identifier-Value	503	X	-	X	-	refer [214]	N/A - Non-Ro	Note NC-2	3GPP TS 29.214 (Policy Rx)
Access-Network-Information	1263	X	-	X	-	OctetString	Compliant by configuration	Note C-1	7.2.1 3GPP TS 32.260 (IMS)
Account-Expiration	2309	-	-	-	X	Time	Compliant by configuration	Note C-1	7.2.2 3GPP TS 32.260 (IMS)
Accumulated-Cost	2052	-	-	-	X	Grouped	Compliant by configuration and dependent on sub-AVPs and external system	Note NC-3	7.2.3
Adaptations	1217	-	-	X	-	Enumerated	Compliant by configuration	Note C-1	7.2.4 3GPP TS 32.270 (MMS)
Additional-Content-Information	1207	-	-	X	-	Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-1 See sub-AVPs: Type-Number Additional-Type-Information	7.2.5

AVP Name	AVP Code	ACR	ACA	CCR	CCA	Value Type	Compliance Level	Comment	Reference
								Content-Size	
Additional-Type-Information	1205	-	-	X	-	UTF8String	Compliant by configuration	Note C-1	7.2.6
Address-Data	897	-	-	X	-	UTF8String	Compliant by configuration	Note C-2	7.2.7
Address-Domain	898	-	-	X	-	Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-1 See sub-AVPs: Domain-Name 3GPP-IMSI-MCC-MNC	7.2.8
Addressee-Type	1208	-	-	X	-	Enumerated	Compliant by configuration	Note C-1	7.2.10
Address-Type	899	-	-	X	-	Enumerated	Compliant by configuration	Note C-1	7.2.9
AF-Charging-Identifier	505	-	-	X	-	refer [214]	N/A - Non-Ro	Note NC-2	3GPP TS 29.214 (Policy Rx)
AF-Correlation-Information	1276	X	-	X	-	Grouped	N/A - Non-Ro	Note NC-2 Rx/Gx Interface See sub-AVPs: AF-Charging-Identifier Flows	7.2.11 3GPP TS 29.214 (Policy-Rx) and TS 29.212 (Policy-Gx)
Allocation-Retention-Priority	1034	X	-	X	-	refer [215]	N/A - Non-Ro	Note NC-2	3GPP TS 29.212 (Policy-Gx)
Alternate-Charged-Party-Address	1280	X	-	-	-	UTF8string	N/A - Offline	Note NC-1	7.2.12 3GPP TS 32.260 (IMS)
AoC-Cost-Information	2053	-	-	X	X	Grouped	Compliant by configuration and dependent on external system	Note NC-3	7.2.13 3GPP TS 32.280 (AoC)
AoC-Format	2310	-	-	X	-	Enumerated	Compliant by configuration and dependent on external system	Note NC-3	7.2.14 3GPP TS 32.280 (AoC)
AoC-Information	2054	-	-	-	X	Grouped	Compliant by configuration and dependent on sub-AVPs and external system	Note NC-3	7.2.15 3GPP TS 32.280 (AoC)
AoC-Request-Type	2055	-	-	X	-	Enumerated	Compliant by configuration and dependent on external system	Note NC-3	7.2.16 3GPP TS 32.280 (AoC)

AVP Name	AVP Code	ACR	ACA	CCR	CCA	Value Type	Compliance Level	Comment	Reference
AoC-Service	2311	-	-	X	-	Grouped	Compliant by configuration and dependent on sub-AVPs and external system	Note NC-3	7.2.17 3GPP TS 32.280 (AoC)
AoC-Service-Obligatory-Type	2312	-	-	X	-	Enumerated	Compliant by configuration and dependent on external system	Note NC-3	7.2.18 3GPP TS 32.280 (AoC)
AoC-Service-Type	2313	-	-	X	-	Enumerated	Compliant by configuration and dependent on external system	Note NC-3	7.2.19 3GPP TS 32.280 (AoC)
AoC-Subscription-Information	2314	-	-	X	-	Grouped	Compliant by configuration and dependent on external system	Note NC-3	7.2.20 3GPP TS 32.280 (AoC)
Application-Provided-Called-Party-Address	837	X	-	X	-	UTF8String	Compliant by configuration	Note C-1	7.2.22
Application-Server	836	X	-	X	-	UTF8String	Compliant by configuration	Note C-1	7.2.23
Application-Server-ID	2101	X	-	X	-	refer[223]	Compliant by configuration	Note C-1, Note NC-4	
Application-Service-Provider-Identity	532	X	-	-	-	refer[214]	N/A - Offline	Note NC-1 Note NC-2	3GPP TS 29.214 (Policy Rx)
Application-Server-Information	850	X	-	X	-	Grouped	Compliant by configuration and Dependent on sub-AVPs	Note C-1 See sub-AVPs: Application-Server Application-Provided-Called-Party-Address	7.2.24 3GPP TS 32.260 (IMS)
Application-Service-Type	2102	X	-	X	-	refer[223]	Compliant by configuration	Note C-1	
Application-Session-ID	2103	X	-	X	-	refer[223]	Compliant by configuration	Note C-1, Note NC-4	
Applic-ID	1218	-	-	X	-	UTF8String	Compliant by configuration	Note C-1, Note NC-4	7.2.21 3GPP TS 32.270 (MMS)
Associated-Party-Address	2035	X	-	X	-	UTF8String	Compliant by configuration	Note C-2	7.2.25
Associated-URI	856	X	-	X	-	UTF8String	Compliant by configuration	Note C-2	7.2.26 3GPP TS 29.061 3GPP TS 32.260 (IMS)
Authorised-QoS	849	X	-	-	-	UTF8Str	N/A - Offline	Note NC-1	7.2.27

AVP Name	AVP Code	ACR	ACA	CCR	CCA	Value Type	Compliance Level	Comment	Reference
						ing			
Aux-Applic-Info	1219	-	-	X	-	UTF8String	Compliant by configuration	Note C-1, Note NC-4	7.2.28 3GPP TS 32.270 (MMS)
Base-Time-Interval	1265	-	-	-	X	Unsigned32	Compliant by configuration	Note C-3	7.2.29
Bearer-Service	854	X	-	-	-	OctetString	N/A - Offline	Note NC-1	7.2.30 3GPP TS 32.260 (IMS)
Called-Asserted-Identity	1250	X	-	X	-	UTF8String	Compliant by configuration	Note C-2	7.2.31
Called-Party-Address	832	X	-	X	-	UTF8String	Compliant by configuration	Note C-2	7.2.32 3GPP TS 32.260 (IMS) 3GPP TS 32.272: (PoC)
Calling-Party-Address	831	X	-	X	-	UTF8String	Compliant by configuration	Note C-2	7.2.33 3GPP TS 32.260 (IMS)
Carrier-Select-Routing-Information	2023	X	-	X	-	UTF8String	Compliant by configuration	Note C-1	7.2.34 3GPP TS 32.260 (IMS) / SIP
Cause-Code	861	X	-	X	-	Integer32	Compliant by configuration	Note C-1	7.2.35 3GPP TS 32.260 (IMS) 3GPP TS 32.272: (PoC)
CG-Address	846	X	-	X	-	Address	Compliant by configuration	Note C-2	7.2.36 3GPP TS 32.251 (PS) - Sec 6.3.2.1
Change-Condition	2037	X	-	-	-	Integer32	N/A - Offline	Note NC-1	7.2.37 3GPP TS 32.251 (PS) - Sec 6.3.2.1
Change-Time	2038	X	-	-	-	Time	N/A - Offline	Note NC-1	7.2.38
Charged-Party	857	X	-	-	-	UTF8String	N/A - Offline	Note NC-1	7.2.39
Charging-Characteristics-Selection-Mode	2066	X	-	X	-	Enumerated	Compliant by configuration	Note C-1	7.2.39A
Charging-Rule-Base-Name	1004	X	-	X	-	refer [215]	N/A - Non-Ro	Note NC-2 (S9 or Gx/Sd Interface)	3GPP TS 32.251 (PS) - Sec 6.3.2.1 3GPP TS 29.212 (Policy-Gx)
Class-Identifier	1214	-	-	X	-	Enumerated	Compliant by configuration	Note C-1	7.2.40
Client-Address	2018	-	-	X	-	Address	Compliant by configuration	Note C-2	7.2.41
CN-IP-Multicast-	921	X	-	-	-	refer	N/A - Offline	Note NC-1	

AVP Name	AVP Code	ACR	ACA	CCR	CCA	Value Type	Compliance Level	Comment	Reference
Distribution						[207]			
Content-Class	1220	-	-	X	-	Enumerated	Compliant by configuration	Note C-1	7.2.42 3GPP TS 32.270 (MMS)
Content-Disposition	828	X	-	X	-	UTF8String	Compliant by configuration	Note C-1	7.2.43 RFC 3261 3GPP TS 32.272: (PoC)
Content-ID	2116	X	-	X	-	refer[223]	Compliant by configuration	Note C-1, Note NC-4	
Content-Provider-ID	2117	X	-	X	-	refer[223]	Compliant by configuration	Note C-1, Note NC-4	
Content-Length	827	X	-	X	-	Unsigned32	Compliant by configuration	Note C-1	7.2.44 RFC 3261
Content-Size	1206	-	-	X	-	Unsigned32	Compliant by configuration	Note C-1	7.2.45 RFC 3261
CSG-Access-Mode	2317	X	-	X	-	Enumerated	Compliant by configuration	Note C-1	7.2.46A
CSG-Id	1437	X	-	X	-	refer[219]	Compliant by configuration	Note C-1	
CSG-Membership-Indication	2318	X	-	X	-	Enumerated	Compliant by configuration	Note C-1	7.2.46B
Content-Type	826	X	-	X	-	UTF8String	Compliant by configuration	Note C-1	7.2.46 RFC 3261 3GPP TS 32.272: (PoC)
Current-Tariff	2056	-	-	X	X	Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-1, Note C-3, Note NC-5, Note NC-7 See: Currency-Code Scale-Factor Rate-Element	7.2.47
CUG-Information	2304	X	-	X	-	OctetString	Compliant by configuration	Note C-1	7.2.48
Data-Coding-Scheme	2001	-	-	X	-	Integer32	Compliant by configuration	Note C-1	7.2.49
DCD-Information	2115	X	-	X	-	refer[223]	Compliant by configuration and dependent on sub-AVPs	Note C-1 See sub-AVPs: Content-ID Content-provider-ID	7.2.50 OMA-DDS-Charging
Deferred-Location-Event-Type	1230	-	-	X	-	UTF8String	Compliant by configuration	Note C-1	7.2.51 3GPP TS 32.271 (LCS)
Delivery-Report-Requested	1216	-	-	X	-	Enumerated	Compliant by configuration	Note C-1	7.2.52 3GPP TS 32.270 (MMS)
Delivery-Status	2104	X	-	X	-	refer[223]	Compliant by configuration	Note C-1	OMA-DDS-Charging

AVP Name	AVP Code	ACR	ACA	CCR	CCA	Value Type	Compliance Level	Comment	Reference
Destination-Interface	2002	-	-	X	-	Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-1 See sub-AVPs: Interface-Id Interface-Text Interface-Port Interface-Type	7.2.53
Diagnostics	2039	X	-	X	-	Integer32	Compliant by configuration	Note C-1	7.2.54 3GPP TS 32.251 (PS) - Sec 6.3.2.1
Domain-Name	1200	-	-	X	-	UTF8String	Compliant by configuration	Note C-1	7.2.55
DRM-Content	1221	-	-	X	-	Enumerated	Compliant by configuration	Note C-1	7.2.56 3GPP TS 32.270 (MMS)
Dynamic-Address-Flag	2051	X	-	X	-	Enumerated	Compliant by configuration	Note C-1	7.2.57 3GPP TS 32.251 (PS) - Sec 6.3.2.1
Dynamic-Address-Flag-Extension	2068	X	-	X	-	Enumerated	Compliant by configuration	Note C-1	3GPP TS 32.251 (PS) - Sec 6.3.2.1
Early-Media-Description	1272	X	-	-	-	Grouped	N/A - Offline	Note NC-1	7.2.58 3GPP TS 32.260 (IMS)
Envelope	1266	-	-	X	-	Grouped	Compliant by configuration	Note C-4	7.2.59
Envelope-End-Time	1267	-	-	X	-	Time	Compliant by configuration	Note C-4	7.2.60
Envelope-Reporting	1268	-	-	-	X	Enumerated	Compliant by configuration	Note C-4	7.2.61
Envelope-Start-Time	1269	-	-	X	-	Time	Compliant by configuration	Note C-4	7.2.62
Event	825	X	-	X	-	UTF8String	Compliant by configuration	Note C-1	7.2.63 3GPP TS 32.260 (IMS)
Event-Charging-TimeStamp	1258	-	-	X	-	Time	Compliant by configuration	Note C-1	7.2.64
Event-Type	823	X	-	X	-	Grouped	Compliant by configuration	Note C-1 (SIP)	7.2.65 3GPP TS 32.260 (IMS)
Expires	888	X	-	X	-	Unsigned32	Compliant by configuration	Note C-1 (SIP)	7.2.66 3GPP TS 32.260 (IMS)
File-Repair-Supported	1224	X	-	X	-	Enumerated	Compliant by configuration	Note C-1	7.2.67 3GPP TS 32.273 (MBMS)
Flows	510	-	-	X	-	refer [214]	N/A - Non-Ro	Note NC-2	3GPP TS 29.214 (Policy Rx)
GGSN-Address	847	X	-	X	-	Address	Compliant by	Note C-2	7.2.68

AVP Name	AVP Code	ACR	ACA	CCR	CCA	Value Type	Compliance Level	Comment	Reference
							configuration		3GPP TS 32.273 (MBMS) 3GPP TS 32.272: (PoC)
Guaranteed-Bitrate-UL	1026	X	-	X	-	refer[215]	N/A - Non-Ro	Note NC-2	3GPP TS 29.212 (Policy-Gx)
IM-Information	2110	X	-	X	-	refer[223]	Compliant by configuration and dependent on sub-AVPs	Note C-1 See sub-AVPs: Total-Number-Of-Messages-Sent Total-Number-Of-Messages-Exploded Number-Of-Messages-Successfully-Sent Number-Of-Messages-Successfully-Exploded	7.2.69 OMA-DDS-Charging
IMS-Application-Reference-Identifier	2601	X	-	-	-	UTF8String	N/A - Offline	Note NC-1	7.2.74A 3GPP TS 32.260 (IMS)
IMS-Charging-Identifier	841	X	-	X	-	UTF8String	Compliant by configuration	Note C-1	7.2.75 3GPP TS 32.260 (IMS)
IMS-Communication-Service-Identifier	1281	X	-	X	-	UTF8String	Compliant by configuration	Note C-1	7.2.76 3GPP TS 32.260 (IMS)
IMS-Information	876	X	-	X	-	Grouped	Compliant by configuration	Note C-1	7.2.77 3GPP TS 32.260 (IMS) 3GPP TS 32.272: (PoC)
IMSI-Unauthenticated-Flag	2308	X	-	X	-	Enumerated	Compliant by configuration	Note C-1	7.2.78 3GPP TS 32.251 (PS) - Sec 6.3.2.1
Incoming-Trunk-Group-Id	852	X	-	-	-	UTF8String	N/A - Offline	Note NC-1	7.2.79
Incremental-Cost	2062	-	-	X	X	Grouped	Compliant by configuration and dependent on external system	Note NC-3	7.2.70 3GPP TS 32.280 (AoC)
Initial-IMS-Charging-Identifier	2321	X	-	X	-	UTF8String	Compliant by configuration	Note C-1, Note NC-4	7.2.79A 3GPP TS 32.260: IMS
Interface-Id	2003	-	-	X	-	UTF8String	Compliant by configuration	Note C-1, Note NC-4	7.2.71

AVP Name	AVP Code	ACR	ACA	CCR	CCA	Value Type	Compliance Level	Comment	Reference
Interface-Port	2004	-	-	X	-	UTF8String	Compliant by configuration	Note C-1, Note NC-4	7.2.72
Interface-Text	2005	-	-	X	-	UTF8String	Compliant by configuration	Note C-1, Note NC-4	7.2.73
Interface-Type	2006	-	-	X	-	Enumerated	Compliant by configuration	Note C-1, Note NC-4	7.2.74
Inter-Operator-Identifier	838	X	-	X	-	Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-1 See: Originating-IOI Terminating-IOI	7.2.80 3GPP TS 32.260 (IMS) IETF RFC 3455 (SIP)
IP-Realm-Default-Indication	2603	X	-	-	-	Enumerated	N/A - Offline	Note NC-1	7.2.80A
LCS-Client-Dialed-By-MS	1233	-	-	X	-	UTF8String	Compliant by configuration	Note C-1	7.2.82 3GPP TS 32.271 (LCS)
LCS-Client-External-ID	1234	-	-	X	-	UTF8String	Compliant by configuration	Note C-1, Note NC-4	7.2.83 3GPP TS 32.271 (LCS)
LCS-Client-Id	1232	-	-	X	-	Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-1, Note NC-4 See sub-AVPs: LCS-Client-Type LCS-Client-External-ID LCS-Client-Dialed-By-MS LCS-Client-Name LCS-APN LCS-Requestor-ID	7.2.84 3GPP TS 32.271 (LCS)
LCS-APN	1231	-	-	X	-	UTF8String	Compliant by configuration	Note C-1	7.2.81 3GPP TS 32.271 (LCS)
LCS-Client-Name	1235	-	-	X	-	Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-1 See sub-AVPs: LCS-Data-Coding-Scheme LCS-Name-String LCS-Format-Indicator	7.2.85 3GPP TS 32.271 (LCS)
LCS-Client-Type	1241	-	-	X	-	Enumerated	Compliant by configuration	Note C-1	7.2.86 3GPP TS 32.271 (LCS)
LCS-Data-Coding-Scheme	1236	-	-	X	-	UTF8String	Compliant by configuration	Note C-1	7.2.87 3GPP TS 32.271 (LCS)
LCS-Format-Indicator	1237	-	-	X	-	Enumer	Compliant by	Note C-1	7.2.88

AVP Name	AVP Code	ACR	ACA	CCR	CCA	Value Type	Compliance Level	Comment	Reference
						ated	configuration		3GPP TS 32.271 (LCS)
LCS-Information	878	-	-	X	-	Grouped	Compliant by configuration	Note 1 See sub-AVPs: LCS-Client-ID Location-Type Location-Estimate Positioning-Data 3GPP-IMSI MSISDN	7.2.89 3GPP TS 32.271 (LCS)
LCS-Name-String	1238	-	-	X	-	UTF8String	Compliant by configuration	Note C-1	7.2.90 3GPP TS 32.271 (LCS)
LCS-Requestor-Id	1239	-	-	X	-	Grouped	Compliant by configuration	Note C-1, Note NC-4 See sub-AVPs: LCS-Data-Coding-Scheme LCS-Requestor-ID-String (MSISDN or Logical Name)	7.2.91 3GPP TS 32.271 (LCS)
LCS-Requestor-Id-String	1240	-	-	X	-	UTF8String	Compliant by configuration	Note C-1	7.2.92 3GPP TS 32.271 (LCS)
Local-GW-Inserted-Indication	2604	X	-	-	-	Enumerated	N/A - Offline	Note NC-1	7.2.92A (SDP)
Local-Sequence-Number	2063	X	-	-	-	Unsigned32	N/A - Offline	Note NC-1	7.2.93
Location-Estimate	1242	-	-	X	-	OctetString	Compliant by configuration	Note C-1 and using Raw Data (Note G-2)	7.2.94 3GPP TS 32.271 (LCS)
Location-Estimate-Type	1243	-	-	X	-	Enumerated	Compliant by configuration	Note C-1	7.2.95 3GPP TS 32.271 (LCS)
Location-Type	1244	-	-	X	-	Grouped	Compliant by configuration	Note C-1 See sub-AVPs: Location-Estimate-Type Deferred-Location-Event-Type	7.2.96 3GPP TS 32.271 (LCS)
Low-Balance-Indication	2020	-	-	-	X	Enumerated	Compliant by configuration	Note C-3	7.2.97
Low-Priority-Indicator	2602	X	-	-	-	Enumerated	N/A - Offline	Note NC-1	7.2.97A 3GPP TS 32.251 (PS) - Sec 6.3.2.1
Mandatory-Capability	604	X	-	-	-	refer [204]	N/A - Offline	Note NC-1	

AVP Name	AVP Code	ACR	ACA	CCR	CCA	Value Type	Compliance Level	Comment	Reference
Max-Requested-Bandwidth-DL	515	X	-	X	-	refer [214]	N/A - Non-Ro	Note NC-2	3GPP TS 29.214 (Policy Rx)
Max-Requested-Bandwidth-UL	516	X	-	X	-	refer [214]	N/A - Non-Ro	Note NC-2	3GPP TS 29.214 (Policy Rx)
MBMS-2G-3G-Indicator	907	X	-	X	-	refer [207]	Compliant by configuration	Note C-1	3GPP TS 29.061 (PLMN«PDN) 3GPP TS 32.273 (MBMS)
MBMS GW-Address	2307	X	-	-	-	Address	N/A - Offline	Note NC-1	7.2.98
MBMS-Information	880	X	-	X	-	Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-1 See sub-AVPs: TMGI MBMS-Service-Type MBMS-User-Service-Type File-Repair-Supported Required-MBMS-Bearer-Capabilities MBMS-2G-3G-Indicator RAI MBMS-Service-Area MBMS-Session-Identity CN-IP-Multicast-Distribution MBMS GW-Address	7.2.99 3GPP TS 32.273 (MBMS)
MBMS-Service-Area	903	X	-	X	-	refer [207] OctetString	Compliant by configuration	Note C-1, Note NC-6	3GPP TS 29.061 (PLMN«PDN) 3GPP TS 32.273 (MBMS)
MBMS-Service-Type	906	X	-	X	-	refer [207] Enumerated	Compliant by configuration	Note C-1	3GPP TS 29.061 (PLMN«PDN) 3GPP TS 32.273 (MBMS)
MBMS-Session-Identity	908	X	-	X	-	refer [207] OctetString	Compliant by configuration	Note C-1, Note NC-6	3GPP TS 29.061 (PLMN«PDN) 3GPP TS 32.273 (MBMS)
MBMS-User-Service-Type	1225	X	-	X	-	Enumerated	Compliant by configuration	Note C-1	7.2.100 3GPP TS 32.273 (MBMS)
Media-Initiator-Flag	882	X	-	X	-	Enumerated	Compliant by configuration	Note C-1	7.2.101 3GPP TS 32.272: (PoC) 3GPP TS

AVP Name	AVP Code	ACR	ACA	CCR	CCA	Value Type	Compliance Level	Comment	Reference
									32.260: (IMS)
Media-Initiator-Party	1288	X	-	X	-	UTF8String	Compliant by configuration	Note C-1	7.2.102 3GPP TS 32.272: (PoC)
Message-Body	889	X	-	X	-	Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-1 See sub-AVPs: Content-Type Content-Length Content-Disposition Originator	7.2.103 3GPP TS 32.260 (IMS)
Message-Class	1213	-	-	X	-	Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-1 See sub-AVPs: Class-Identifier Token-Text	7.2.104 3GPP TS 32.270 (MMS)
Message-ID	1210	-	-	X	-	UTF8String	Compliant by configuration	Note C-1, Note NC-4	7.2.105
Message-Size	1212	-	-	X	-	Unsigned32	Compliant by configuration	Note C-1	7.2.106 3GPP TS 32.270 (MMS)
Message-Type	1211	-	-	X	-	Enumerated	Compliant by configuration	Note C-1	7.2.107 3GPP TS 32.270 (MMS)
MMBox-Storage-Requested	1248	-	-	X	-	Enumerated	Compliant by configuration	Note C-1	7.2.109 3GPP TS 32.270 (MMS)
MM-Content-Type	1203	-	-	X	-	Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-1 See sub-AVPs: Type-Number Additional-Type-Information Content-Size Additional-Content-Information	7.2.108 3GPP TS 32.270 (MMS)
MMS-Information	877	-	-	X	-	Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-1 See sub-AVPs: Originator-Address Recipient-Address Submission-Time MM-Content-Type Priority Message-ID Message-Type Message-Size Message-Class Delivery-Report-	7.2.110 3GPP TS 32.270 (MMS)

AVP Name	AVP Code	ACR	ACA	CCR	CCA	Value Type	Compliance Level	Comment	Reference
								Requested Read-Reply-Report-Requested MMBox-Storage-Requested Applic-ID Reply-Applic-ID Aux-Applic-Info Content-Class DRM-Content Adaptations VASP-Id VAS-Id	
MMTel-Information	2030	X	-	X	-	Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-1 See sub-AVPs: Supplementary-Service	7.2.111
MSISDN	701	-	-	X	-	refer [221]	Complaint by configuration	Note C-2	3GPP TS 29.329 (Sh I/F) 3GPP TS 32.271 (LCS)
Next-Tariff	2057			X	X	Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-1, Note NC-5, Note NC-7 See: Currency-Code Scale-Factor Rate-Element	7.2.112
Node-Functionality	862	X	-.	X	-	Enumerated	Complaint by configuration	Note C-1	7.2.113
Node-Id	2064	X	-	X	-	UTF8String	Complaint by configuration	Note C-1	7.2.114 3GPP TS 32.251 (PS) - Sec 6.3.2.1
Number-Of-Diversions	2034	X	-	X	-	Unsigned32	Complaint by configuration	Note C-1	7.2.115
Number-Of-Messages-Sent	2019	X	-	X	-	Unsigned32	Complaint by configuration	Note C-1	7.2.116
Number-Of-Messages-Successfully-Exploded	2111	X	-	X	-	refer[223]	Compliant by configuration	Note C-1	OMA-DDS-Charging
Number-Of-Messages-Successfully-Sent	2112	X	-	X	-	refer[223]	Compliant by configuration	Note C-1	OMA-DDS-Charging
Number-Of-Participants	885	X	-	X	-	Unsigned32	Compliant by configuration	Note C-1	7.2.117 3GPP TS 32.272: (PoC)
Number-Of-Received-Talk-Bursts	1282	X	-	-	-	Unsigned32	N/A - Offline	Note NC-1	7.2.118
Number-Of-Talk-Bursts	1283	X	-	-	-	Unsigned32	N/A - Offline	Note NC-1	7.2.119

AVP Name	AVP Code	ACR	ACA	CCR	CCA	Value Type	Compliance Level	Comment	Reference
Number-Portability-Routing-Information	2024	X	-	X	-	UTF8String	Compliant by configuration	Note C-1	7.2.120 3GPP TS 32.260 (IMS)
Offline-Charging	1278	-	-	-	X	Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-1, Note NC-1 See sub-AVPs: Quota-Consumption-Time Time-Quota-Mechanism Envelope-Reporting Multiple-Services-Credit-Control	7.2.121
Online-Charging-Flag	2303	X	-	-	-	Enumerated	N/A - Offline	Note NC-1	7.2.122 3GPP TS 32.260 (IMS)
Optional-Capability	605	X	-	-	-	refer [204]	N/A - Offline	Off-line Charging	
Originating-IOI	839	X	-	X	-	UTF8String	Compliant by configuration	Note C-1, Note NC-4 (SIP)	7.2.123 IETF RFC 3455 (SIP) 3GPP TS 32.260 (IMS)
Originator-SCCP-Address	2008	-	-	X	-	Address	Compliant by configuration	Note C-2	7.2.128
Originator	864	X	-	X	-	Enumerated	Compliant by configuration	Note C-1	7.2.124
Originator-Address	886	-	-	X	-	Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-1 See sub-AVPs: Address-Type Address-Data Address-Domain	7.2.125 3GPP TS 32.270 (MMS)
Originator-Received-Address	2027	-	-	X	-	Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-1 See sub-AVPs: Address-Type Address-Data Address-Domain	7.2.127
Originator-Interface	2009	-	-	X	-	Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-1 See sub-AVPs: Interface-Id Interface-Text Interface-Port Interface-Type	7.2.126
Outgoing-Session-Id	2320	X	-	X	-	UTF8String	Compliant by configuration	Note C-1, Note NC-4	7.2.128A 3GPP TS 32.260 (IMS)
Outgoing-Trunk-Group-Id	853	X	-	-	-	UTF8Str	N/A - Offline	Off-line Charging	7.2.129

AVP Name	AVP Code	ACR	ACA	CCR	CCA	Value Type	Compliance Level	Comment	Reference
						ing			
Participant-Access-Priority	1259	X	-	X	-	Enumerated	Compliant by configuration	Note C-1	7.2.132 3GPP TS 32.272: (PoC)
Participant-Action-Type	2049	X	-	X	-	Enumerated	Compliant by configuration	Note C-1	7.2.133
Participant-Group	1260	X	-	X	-	Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-1 See sub-AVPs: Called-Party-Address Participant-Access-Priority User-Participating-Type	7.2.131 3GPP TS 32.272: (PoC)
Participants-Involved	887	X	-	X	-	UTF8String	Compliant by configuration	Note C-2	7.2.130 3GPP TS 32.272: (PoC)
PDG-Address	895	X	-	X	-	Address	Compliant by configuration	Note C-1	7.2.134
PDG-Charging-Id	896	X	-	X	-	Unsigned32	Compliant by configuration	Note C-1, Note NC-4	7.2.135
PDN-Connection-Charging-ID	2050	X	-	X	-	Unsigned32	Compliant by configuration	Note C-1, Note NC-4	7.2.136 3GPP TS 32.251 (PS) - Sec 6.3.2.1
PDP-Address	1227	X	-	X	-	Address	Compliant by configuration	Note C-1	7.2.137 3GPP TS 32.270 (MMS)
PDP-Context-Type	1247	X	-	X	-	Enumerated	Compliant by configuration	Note C-1, Note NC-4 Note NC-2 for Gn/Gp	7.2.138 3GPP TS 32.251 (PS) - Sec 6.3.2.1
PDP-Address-Prefix-Length	2606	X	-	X	-	Unsigned32	Compliant by configuration	Note C-1, Note NC-2	
PoC-Change-Condition	1261	X	-	-	-	Enumerated	N/A - Offline	Note NC-1	7.2.139
PoC-Change-Time	1262	X	-	-	-	Time	N/A - Offline	Note NC-1	7.2.140
PoC-Controlling-Address	858	X	-	X	-	UTF8String	Compliant by configuration	Note C-1	7.2.141 3GPP TS 32.272: (PoC)
PoC-Event-Type	2025	X	-	X	-	Enumerated	Compliant by configuration	Note C-1	7.2.142 3GPP TS 32.272: (PoC)
PoC-Group-Name	859	X	-	X	-	UTF8String	Compliant by configuration	Note C-1	7.2.143 3GPP TS 32.272: (PoC)
PoC-Information	879	X	-	X	-	Grouped	Compliant by configuration and dependent on	Note C-1 See sub-AVPs: PoC-Server-Role	7.2.144 3GPP TS 32.272: (PoC)

AVP Name	AVP Code	ACR	ACA	CCR	CCA	Value Type	Compliance Level	Comment	Reference
							sub-AVPs	PoC-Session-Type PoC-User-Role PoC-Session-Initiation-type PoC-Event-Type Number-Of-Participants Participants-Involved Participant-Group Talk-Burst-Exchange PoC-Controlling-Address PoC-Group-Name PoC-Session-Id Charged-Party	
PoC-Server-Role	883	X	-	X	-	Enumerated	Compliant by configuration	Note C-1	7.2.145 3GPP TS 32.272: (PoC)
PoC-Session-Id	1229	X	-	X	-	UTF8String	Compliant by configuration	Note C-1, Note NC-4	7.2.146 3GPP TS 32.272: (PoC)
PoC-Session-Initiation-type	1277	X	-	X	-	Enumerated	Compliant by configuration	Note C-1	7.2.147 3GPP TS 32.272: (PoC)
PoC-Session-Type	884	X	-	X	-	Enumerated	Compliant by configuration	Note C-1	7.2.148 3GPP TS 32.272: (PoC)
PoC-User-Role	1252	X	-	X	-	Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-1 See sub-AVPs: PoC-User-Role-Ids PoC-User-Role-info-Units	7.2.149 3GPP TS 32.272: (PoC)
PoC-User-Role-IDs	1253	X	-	X	-	UTF8String	Compliant by configuration	Note C-1	7.2.150 3GPP TS 32.272: (PoC)
PoC-User-Role-info-Units	1254	X	-	X	-	Enumerated	Compliant by configuration	Note C-1 Possible values: 1. Moderator 2. Dispatcher 3. Session-Owner 4. Session-Participant	7.2.151 3GPP TS 32.272: (PoC)
Positioning-Data	1245	-	-	X	-	UTF8String	Compliant by configuration	Note C-1	7.2.152 3GPP TS 32.271

AVP Name	AVP Code	ACR	ACA	CCR	CCA	Value Type	Compliance Level	Comment	Reference
									(LCS) 3GPP TS 25.305 3GPP TS 43.059
Preferred-AoC-Currency	2315	-	-	X	-	Unsigned32	Compliant by configuration and Dependent on External System	Note NC-3	7.2.153 3GPP TS 32.280 (AoC) RFC 4006
Priority	1209	-	-	X	-	Enumerated	Compliant by configuration	Note C-1	7.2.154
Priority-Level	1046	X	-	X	-	refer [215]	N/A - Non-Ro	Note NC-2	3GPP TS 29.212 (Policy-Gx)
PS-Append-Free-Format-Data	867	X	-	-	X	Enumerated	Compliant by configuration	Note C-3	7.2.155
PS-Free-Format-Data	866	X	-	-	X	OctetString	Compliant by configuration	Note C-3	7.2.156
PS-Furnish-Charging-Information	865	X	-	-	X	Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-3	7.2.157 3GPP TS 32.251 (PS) - Sec 5.3.2.3, 6.3.2.1
PS-Information	874	X	-	X	X	Grouped	Compliant by configuration and dependent on sub-AVPs	Note 1, Note 5 (TS 32.251) See sub-AVPs: User Location Info (PoC) GGSN Address (PoC)	7.2.158 3GPP TS 32.251 (PS) - Sec 6.3.2.1 3GPP TS 32.270 (MMS) 3GPP TS 32.272: (PoC) 3GPP TS 32.273 (MBMS)
QoS-Information	1016	X	-	X	-	refer [215]	N/A - Non-Ro	Note NC-2	3GPP TS 29.212 (Policy-Gx)
QoS-Class-Identifier	1028	X	-	X	-	refer [215]	N/A - Non-Ro	Note NC-2	3GPP TS 29.212 (Policy-Gx)
Quota-Consumption-Time	881	-	-	-	X	Unsigned32	Compliant by configuration if configured. If not configured, compliant (as AVP is optional and not required)	Note C-3	7.2.159
Quota-Holding-Time	871	-	-	-	X	Unsigned32	Compliant by configuration	A Quota-Holding-Time value of zero indicates that this mechanism shall not be used. If the Quota-Holding-Time AVP is not	7.2.160

AVP Name	AVP Code	ACR	ACA	CCR	CCA	Value Type	Compliance Level	Comment	Reference
								present, then a locally configurable default value in the client shall be used Note C-3	
RAI	909	X	-	X	-	refer [207] UTF8String	Compliant by configuration	Note C-1, Note NC-6	3GPP TS 29.061 (PLMN«PDN)
Rate-Element	2058	-	-	X	X	Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-1, Note NC-3 See sub-AVPs: CC-Unit-Type Reason-Code Unit-Value Unit-Cost Unit-Quota-Threshold	
RAT-Type	1032	X	-	X	-	refer [215]	N/A - Non-Ro	Note NC-2	3GPP TS 29.212 (Policy-Gx)
Read-Reply-Report-Requested	1222	-	-	X	-	Enumerated	Compliant by configuration	Note C-1	7.2.162 3GPP TS 32.270 (MMS)
Reason-Code	2316	-	-	X	X	Enumerated	Compliant by configuration	Note C-1, Note C-3	7.2.163
Real-Time-Tariff-Information	2305	X	-	-	-	Grouped	N/A - Offline	Note NC-1	7.2.164 3GPP TS 32.260 (IMS)
Received-Talk-Burst-Time	1284	X	-	-	-	Unsigned32	N/A - Offline	Note NC-1	7.2.165
Received-Talk-Burst-Volume	1285	X	-	-	-	Unsigned32	N/A - Offline	Note NC-1	7.2.166
Recipient-Address	1201	-	-	X	-	Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-1 See sub-AVPs: Address-Type Address-Data Address-Domain Addressee-Type	7.2.167 3GPP TS 32.270 (MMS)
Recipient-Info	2026	-	-	X	-	Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-1 See sub-AVPs: Destination-Interface Recipient-Address Recipient-Received-Address Recipient-SCCP-Address	7.2.168

AVP Name	AVP Code	ACR	ACA	CCR	CCA	Value Type	Compliance Level	Comment	Reference
								SM-Protocol-ID	
Recipient-Received-Address	2028	-	-	X	-	Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-1 See sub-AVPs: Address-Type Address-Data Address-Domain	7.2.169
Recipient-SCCP-Address	2010	-	-	X	-	Address	Compliant by configuration	Note C-2	7.2.170
Refund-Information	2022	-	-	X	X	OctetString	Compliant by configuration	Note C-1, Note C-3, Note G-2.	7.2.171
Remaining-Balance	2021	-	-	-	X	Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-1 See sub-AVPs: Unit-Value Currency-Code	7.2.172
Reply-Applic-ID	1223	-	-	X	-	UTF8String	Compliant by configuration	Note C-1	7.2.173 3GPP TS 32.270 (MMS)
Reply-Path-Requested	2011	-	-	X	-	Enumerated	Compliant by configuration	Note C-1	7.2.174
Reporting-Reason	872	-	-	X	-	Enumerated	Compliant by configuration	Note C-1	7.2.175
Requested-Party-Address	1251	X	-	X	-	UTF8String	Compliant by configuration	Note C-2	7.2.176 3GPP TS 32.260 (IMS)
Required-MBMS-Bearer-Capabilities	901	X	-	X	-	refer [207] UTF8String	Compliant by configuration	Note C-1	3GPP TS 29.061 (PLMN«PDN)
Role-Of-Node	829	X	-	X	-	Enumerated	Compliant by configuration	Note C-1	7.2.177 3GPP TS 32.260 (IMS)
Scale-Factor	2059	-	-	X	X	Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-1, Note C-3 See sub-AVPs: Value-Digits Exponent	7.2.178
SDP-Answer-Timestamp	1275	X	-	-	-	Time	N/A - Offline	Note NC-2	7.2.179
SDP-Media-Component	843	X	-	X	-	Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-1 See sub-AVPs: SDP-Media-Name SDP-Media-Description Local-GW-Inserted-Indication IP-Realm-Default-Indication Transcoder-	7.2.180 3GPP TS 32.260 (IMS) 3GPP TS 32.272: (PoC)

AVP Name	AVP Code	ACR	ACA	CCR	CCA	Value Type	Compliance Level	Comment	Reference
								Inserted-Indication Media-Initiator-Flag Media-Initiator-Party Authorised-QoS 3GPP-Charging-Id Access-Network-Charging-Identifier-Value SDP-Type	
SDP-Media-Description	845	X	-	X	-	UTF8String	Compliant by configuration	Note C-1	7.2.181
SDP-Media-Name	844	X	-	X	-	UTF8String	Compliant by configuration	Note C-1	7.2.182
SDP-Offer-Timestamp	1274	X	-	-	-	Time	N/A - Offline	Note NC-1	7.2.183
SDP-Session-Description	842	X	-	X	-	UTF8String	Compliant by configuration	Note C-1	7.2.184 3GPP TS 32.260 (IMS) 3GPP TS 32.272: (PoC)
SDP-TimeStamps	1273	X	-	-	-	Grouped	N/A - Offline	Note NC-1	7.2.185 3GPP TS 32.260 (IMS)
SDP-Type	2036	X	-	X	-	Enumerated	Compliant by configuration	Note C-1	7.2.186
Served-Party-IP-Address	848	X	-	-	-	Address	N/A - Offline	Note NC-1	7.2.187 3GPP TS 32.260 (IMS) 3GPP TS 32.272: (PoC)
Server-Capabilities	603	X	-	-	-	refer [204]	N/A - Offline	Note NC-1	3GPP TS 32.260 (IMS)
Server-Name	602	X	-	-	-	refer [204]	N/A - Offline	Note NC-1	
Service-Data-Container	2040	X	-	-	-	Grouped	N/A - Offline	Note NC-1	7.2.189 3GPP TS 32.251 (PS) - Sec 6.3.2.1
Service-Generic-Information	1256	X	-	X	-	Refer[223] Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-1 See sub-AVPs: Application-Server-ID Application-Service-Type Application-Session-ID Delivery-Status	7.2.191
Service-Id	855	X	-	X	-	UTF8String	Compliant by configuration	Note C-1, Note NC-7	7.2.190 3GPP TS 32.260

AVP Name	AVP Code	ACR	ACA	CCR	CCA	Value Type	Compliance Level	Comment	Reference
									(IMS) 3GPP TS 32.271 (LCS)
Service-Information	873	X	-	X	X	Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-1, Note L-Note C-3, Note NC-7 See sub-AVPs: Subscription-Id AoC-Information PS-Information WLAN-Information IMS-Information MMS-Information LCS-Information PoC-Information BMS-Information SMS-Information MMTel-Information Service-Generic-Information IM-Information DCD-Information	7.2.192 3GPP TS 32.270 (MMS) 3GPP TS 32.272: (PoC) 3GPP TS 32.273 (MBMS)
Service-Mode	2032	X	-	X	-	Unsigned32	Compliant by configuration	Note C-1	7.2.193
Service-Specific-Data	863	X	-	-	-	UTF8String	N/A - Offline	Off-line Charging	7.2.194 3GPP TS 32.272: (PoC)
Service-Specific-Info	1249	X	-	-	-	Grouped	N/A - Offline	Off-line Charging	7.2.195 3GPP TS 32.260 (IMS)
Service-Specific-Type	1257	X	-	-	-	Unsigned32	N/A - Offline	Off-line Charging	7.2.196
Serving-Node-Type	2047	X	-	X	-	Enumerated	Compliant by configuration	Note C-1	7.2.198 3GPP TS 32.251 (PS) - Sec 6.3.2.1
Service-Type	2031	X	-	X	-	Unsigned32	Compliant by configuration	Note C-1	7.2.197
Session-Priority	650	X	-	X	-	Refer [204]	N/A - Non-Ro	Note NC-2	
SGSN-Address	1228	X	-	X	-	Address	Compliant by configuration	Note C-1	7.2.199
SGW-Address	2067	X	-	-	-	Address	N/A - Offline	Note NC-1	7.2.199A 3GPP TS 32.251 (PS) - Sec 6.3.2.1
SGW-Change	2065	X	-	-	-	Enumerated	N/A - Offline	Note NC-1	7.2.200 3GPP TS 32.251

AVP Name	AVP Code	ACR	ACA	CCR	CCA	Value Type	Compliance Level	Comment	Reference
									(PS) - Sec 6.3.2.1
SIP-Method	824	X	-	X	-	UTF8String	Compliant by configuration	Note C-1	7.2.201 (IMS/SIP)
SIP-Request-Timestamp-Fraction	2301	X	-	X	-	Unsigned32	Compliant by configuration	Note C-1	7.2.203
SIP-Request-Timestamp	834	X	-	X	-	Time	Compliant by configuration	Note C-1	7.2.202
SIP-Response-Timestamp-Fraction	2302	X	-	X	-	Unsigned32	Compliant by configuration	Note C-1	7.2.205
SIP-Response-Timestamp	835	X	-	X	-	Time	Compliant by configuration	Note C-1	7.2.204
SM-Discharge-Time	2012	-	-	X	-	Time	Compliant by configuration	Note C-1	7.2.206
SM-Message-Type	2007	-	-	X	-	Enumerated	Compliant by configuration	Note C-1	7.2.207
SM-Protocol-ID	2013	-	-	X	-	OctetString	Compliant by configuration	Note C-1	7.2.208
SMSC-Address	2017	-	-	X	-	Address	Compliant by configuration	Note C-1	7.2.214
SMS-Information	2000	-	-	X	-	Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-1 See sub-AVPs: SMS-Node Client-Address Originator-SCCP-Address SMSC-Address Data-Coding-Scheme SM-Discharge-Time SM-Message-Type Originator-Interface SM-Protocol-ID Reply-Path-Requested SM-Status SM-User-Data-Header Number-Of-Messages-Sent Recipient-Info Originator-Received-Address SM-Service-Type	7.2.211
SMS-Node	2016	-	-	X	-	Enumerated	Compliant by configuration	Note C-1	7.2.212
SM-Service-Type	2029	-	-	X	-	Enumerated	Compliant by configuration	Note C-1	7.2.213

AVP Name	AVP Code	ACR	ACA	CCR	CCA	Value Type	Compliance Level	Comment	Reference
SM-Status	2014	-	-	X	-	OctetString	Compliant by configuration	Note C-1, Note G-2	7.2.209
SM-User-Data-Header	2015	-	-	X	-	OctetString	Compliant by configuration	Note C-1, Note G-2	7.2.210
Sponsor-Identify	531	X	-	-	-	refer[214]	N/A - Offline	Note NC-1	
Start-Time	2041	X	-	-	-	Time	N/A - Offline	Note NC-1	7.2.215 3GPP TS 32.251 (PS) - Sec 6.3.2.1
Status	2702	X	-	-	-	Enumerated	N/A - Offline	Note NC-1	7.2.215A **[V11.3]**
Stop-Time	2042	X	-	-	-	Time	N/A - Offline	Note NC-1	7.2.216 3GPP TS 32.251 (PS) - Sec 6.3.2.1
Submission-Time	1202	-	-	X	-	Time	Compliant by configuration	Note C-1	7.2.217 3GPP TS 32.270 (MMS)
Subscriber-Role	2033	X	-	X	-	Enumerated	Compliant by configuration	Note C-1	7.2.218
Supplementary-Service	2048	X	-	X	-	Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-1 See sub-AVPs: Service-Type Service-Mode Number-Of-Diversions Associated-Party-Address Service-ID Change-Time Number-Of-Participants Participant-Action-Type CUG-Information AoC-Information	7.2.219
Talk-Burst-Exchange	1255	X	-	-	-	Grouped	N/A - Offline	Note NC-1	7.2.220
Talk-Burst-Time	1286	X	-	-	-	Unsigned32	N/A - Offline	Note NC-1	7.2.221
Talk-Burst-Volume	1287	X	-	-	-	Unsigned32	N/A - Offline	Note NC-1	7.2.222
Tariff-Information	2060	X	-	X	X	Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-1, Note NC-5, Note NC-7 See sub-AVPs: Current-Tariff Tariff-Time-Change	7.2.223

AVP Name	AVP Code	ACR	ACA	CCR	CCA	Value Type	Compliance Level	Comment	Reference
								Next-Tariff	
Tariff-XML	2306	X	-	-	-	UTF8String	N/A - Offline	Note NC-1	7.2.224
Terminal-Information	1401	X	-	X	-	refer [219]	N/A - Offline	Note C-1, Note NC-1 Offline charging (Online charging uses User-Equipment Info) Note NC-1	3GPP TS 29.272 (MME&SGSN) 3GPP TS 32.251 (PS) - Sec 6.3.2.1
Terminating-IOI	840	X	-	X	-	UTF8String	Compliant by configuration	Note C-1	7.2.225 IETF RFC 3455 (SIP) 3GPP TS 32.260 (IMS)
Time-First-Usage	2043	X	-	-	-	Time	N/A - Offline	Note NC-1	7.2.226
Time-Last-Usage	2044	X	-	-	-	Time	N/A - Offline	Note NC-1	7.2.227
Time-Quota-Mechanism	1270	-	-	-	X	Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-3 See sub-AVPs: Time-Quota-Type Base-Time-Interval	7.2.228
Time-Quota-Threshold	868	-	-	-	X	Unsigned32	Fully compliant		7.2.229
Time-Quota-Type	1271	-	-	-	X	Enumerated	Compliant by configuration	Note C-3	7.2.230
Time-Stamps	833	X	-	X	-	Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-1 See sub-AVPs: SIP-Request-Timestamp SIP-Response-Timestamp SIP-Request-Timestamp-Fraction SIP-Response-Timestamp-Fraction	7.2.231 3GPP TS 32.260 (IMS)
Time-Usage	2045	X	-	-	-	Unsigned32	N/A - Offline	Note NC-1	7.2.232
TMGI	900	X	-	X	-	refer [207] OctetString	Compliant by configuration	Note C-1, Note G-2, Note NC-4	
Token-Text	1215	-	-	X	-	UTF8String	Compliant by configuration	Note C-1	7.2.234
Total-Number-Of-Messages-Exploded	2113	X	-	X	-	refer[223]	Compliant by configuration	Note C-1	OMA-DDS-Charging
Total-Number-Of-Messages-Sent	2114	X	-	X	-	refer[223]	Compliant by configuration	Note C-1	OMA-DDS-Charging

AVP Name	AVP Code	ACR	ACA	CCR	CCA	Value Type	Compliance Level	Comment	Reference
Traffic-Data-Volumes	2046	X	-	-	-	Grouped	N/A - Offline	Note NC-1	7.2.233 3GPP TS 32.251 (PS) - Sec 6.3.2.1
Transcoder-Inserted-Indication	2605	X	-	-	-	Enumerated	N/A - Offline	Note NC-1	7.2.233A
Transit-IOI-List	2701	X	-	-	-	UTF8String	N/A - Offline	Note NC-1	7.2.233B **[V11.3]** 3GPP TS 32.260 (IMS)
Trigger	1264	-	-	X	X	Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-1, Note L-Note C-3 See sub-AVP: Trigger-Type	7.2.235 3GPP TS 32.272: (PoC)
Trigger-Type	870	-	-	X	X	Enumerated	Compliant by configuration	Note C-1	7.2.236
Trunk-Group-Id	851	X	-	-	-	Grouped	N/A - Offline	Note NC-1	7.2.237 3GPP TS 32.260 (IMS)
Type-Number	1204	-	-	X	-	Enumerated	Compliant by configuration	Note C-1	7.2.238
Unit-Cost	2061	-	-	X	X	Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-1, Note C-3 See sub-AVPs: Value-Digits Exponent	7.2.239
Unit-Quota-Threshold	1226	-	-	-	X	Unsigned32	Compliant by configuration	Note C-3, Note C-5	7.2.240
User-CSG-Information	2319	X	-	X	X	Grouped	Compliant by configuration and dependent on sub-AVPs	Note L-1, Note C-3, Note NC-4 See sub-AVPs: CSG-Id CSG-Access-Mode CSG-Membership-Indication	7.2.240A 3GPP TS 32.251 (PS) - Sec 6.3.2.1
User-Data	606	X	-	-	-	refer [204]	N/A - Offline	Note NC-1	
User-Participating-Type	1279	X	-	X	-	Enumerated	Compliant by configuration	Note C-1	7.2.241 3GPP TS 32.272: (PoC)
User–Session-Id	830	X	-	X	-	UTF8String	Compliant by configuration	Note C-1, Note NC-4	7.2.242 3GPP TS 32.260 (IMS)
VAS-Id	1102	-	-	X	-	refer [213]	N/A - Non-Ro	Note C-1, Note NC-4	3GPP TS 29.140 (MM10) 3GPP TS 32.270 (MMS)
VASP-Id	1101	-	-	X	-	refer	N/A - Non-Ro	Note C-1, Note	3GPP TS 29.140

AVP Name	AVP Code	ACR	ACA	CCR	CCA	Value Type	Compliance Level	Comment	Reference
						[213]		NC-4	(MM10) 3GPP TS 32.270 (MMS)
Volume-Quota-Threshold	869	-	-	-	X	Unsigned32	Fully compliant		7.2.243
WAG-Address	890	X	-	X	-	Address	Compliant by configuration	Note C-1	7.2.244
WAG-PLMN-Id	891	X	-	X	-	OctetString	Compliant by configuration	Note C-1, Note NC-6	7.2.245
WLAN-Information	875	X	-	X	-	Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-1 See sub-AVPs: WLAN-Session-Id PDG-Address PDG-Charging-Id WAG-Address WAG-PLMN-Id WLAN-Radio-Container WLAN-UE-Local-IPAddress	7.2.246
WLAN-Radio-Container	892	X	-	X	-	Grouped	Compliant by configuration and dependent on sub-AVPs	Note C-1 See sub-AVPs: Operator-Name Location-Type Location-Information WLAN-Technology	7.2.247
WLAN-Session-Id	1246	X	-	X	-	UTF8String	Compliant by configuration	Note C-1	7.2.248
WLAN-Technology	893	X	-	X	-	Unsigned32	Compliant by configuration	Note C-1	7.2.249
WLAN-UE-Local-IPAddress	894	X	-	X	-	Address	Compliant by configuration	Note C-1	7.2.250

Compliance Levels and Considerations

Definition of compliance levels

Compliance Level	Meaning
Fully compliant	DCA understands and supports the AVP. Will provide the functionality intended. Where relevant, scope of compliance indicated by accompanying note.
Non compliant	DCA does not support the AVP. However limited AVP support can still be obtained using the DCA configuration and the feature set provided by ACS. See indicated "NC" Notes and "G" Notes.
Compliant by configuration	DCA does not use the AVP. However partial or full AVP support can still be obtained using DCA configuration and the feature set provided by ACS. See indicated Note(s).

Compliance Level	Meaning
N/A - Offline	DCA is an online charging application. The AVP is marked for use with ACR/ACA offline charging and is not applicable to DCA. See Note NC-1.
N/A - Non-Ro	DCA is an online charging application (Ro Interface). See Note NC-2.

Considerations

Where a specific AVP is marked as "Compliant by configuration", the compliance level is limited by the notes below:

Note C-1

The specific AVP can be mapped through DCA AvpMapping configuration and used in the ACS control plan such as in branch decisions and inclusion in ACS generated EDRs and in various fields and records (for example, to complete the information collected for rating of the session).

Note that currently some limitations exists in the capabilities of ACS and CCS. If NCC CCS Prepaid Charging is used, the specific AVP (if relevant) may be used to select a Tariff Plan only at the start of a charging session (for example, at CCR Initial Requests for session based reservations) or for a re-engaged session* by using the ACS Tariff Plan Override control plan node. For some scenarios (for example, in a UATB Node for a non re-engaged session), the tariff plan cannot be subsequently changed mid-session. See NCC *Charging Control Services User's Guide* and *Charging Control Services Technical Guide* for details.

Where applicable, "Note C-2" may also apply.

The above limitations are based on the current service logic used for rating (that is, when using the UATB node). The interface provides the flexibility to allow future customized service logic nodes (through SDK or future developments), and future product capabilities, to utilize (and set) values mid-session.

Non-complaint, if the requirements cannot be meet by any of the approaches described above:

- See Note NC-4 where applicable.
- See NC-6 for OctetString and UTF8String AVPs that contain sub-fields or are formatted using data structures not supported by DCA.

* A re-engaged session is one where DCA treats the inbound Diameter CCR Update Request as an Initial Request and creates a new charging session through ACS. An example is when a new requested unit type is received in an Update Request for an existing service. See *Diameter Control Agent Technical Guide* for full details.

DCA may be used in different network configurations:

(i) with NCC Prepaid Charging/VWS and the standard UATB Node in the ACS control plans.

(ii) with a convergent billing engine (Oracle BRM or third party using NCC DCD)

(iii) with (i) or (ii) but with Custom development (using SDK).

Limitations described here apply to (i) only.

These limitations may be non-existent in (ii) and (iii).

Note C-2

Where the specific AVP is an address, "Note C-1" above applies except that, in addition to mapping to acsProfile fields, the specific AVP may be mapped to a predefine set of INAP address fields (for example, the called or calling party number) and sent to ACS and used in the ACS control plan such as in branch decisions and inclusion in ACS generated EDRs or in various fields and records. If the AVP is mapped as an acsProfile field (for example, through Raw Data mapping), the Profile may be copied to the relevant ACS address field (for example, Session Data's calling party number or equivalent). The scope is limited by the featureset and capabilities of ACS and CCS.

If NCC CCS Prepaid Charging is used, the address† (if applicable) may be used in the rating of the call when address-based CLI-DN tariffs are applied. For some scenarios (for example‡, in a UATB Node for a non re-engaged session), if the specific AVP is mapped to a location-specific address, the location information cannot be updated mid-session to change or update the tariff used for rating of the current session. The Tariff Plan (once selected at the start of the UATB session) cannot be subsequently changed mid-session.

Also, session based NCC CCS Prepaid Charging when used with the NCC VWS has the following limitations:

- Use of 2 addresses for CLI-DN tariffs. However, if additional addresses are to be used to determine the rating (and if inclusion of the additional information in ACS generated EDRs is not sufficient), other CCS feature have to be employed such as Tariff Plan Override.
- Use of address fields that are digits only (that is, UTF8String AVP Format) or that which where the digits can be extracted from (for example, TEL URI such as "tel:+12015550123"). The CLI-DN tariffs only deal with pure digit-based addresses. Non-digit addresses cannot be handled and have to be mapped externally before these can be used in the CLI-DN tariffs.

The above VWS-specific limitations are not applicable if BRM is used instead of NCC CCS Prepaid Charging. See Note C-3. Consult BRM documentation and the NCC <BCD_Tg_fn> for details.

Non-complaint, if the requirements cannot be met by any of the approaches described above; See "Note NC-4".

† Only specific numbers (for example, Calling Party or Called Party numbers) can be used for CLI-DN Rating. See *Charging Control Services Technical Guide* for details.

‡ Tariff plan override node permits configuration according to changes in location mid-call/mid-session.

However this depends on the sending of ATI messages which DCA does not currently support.

Note C-3

For outbound AVPs, fully compliant AVP values are set in the service logic.

For outbound AVPs that are compliant by configuration, user-configurable mappable values may be mapped from:

- An ACS field (for example, an acsProfile Session Data fields).
- A literal (fixed value or constant) or a literal that is dependent on the value of another AVP field or acsProfile field

In any case, the AVP mapping must be applied for a specific service.

If the outbound AVP forms a request to the Diameter client, the following restrictions apply:

- The outbound AVP is fixed to a specific outbound diameter message type as defined by the configuration. This may restrict the message sequence or scenarios required to be supported.
- The request to the diameter client in the form of outbound AVPs in the Diameter response message may result in subsequent AVPs that are "Compliant by configuration" to be sent to DCA. See Note C-1 for details, however if these inbound AVPs required.

Non-complaint, if the requirements cannot be meet by any of the approaches described above; See "Note NC-5".

Note C-4

DCA does not contain inbuilt support for envelop reporting. Partial or limited compliance may be possible by configuration and restricting the use of the AVP:

- To a specific service
- With a single set value or a limited range of values
- To specific messages or under a limited set of scenarios (message flows) only

Non-Compliance Issues

NC-1

DCA is an online charging application. AVPs associated only with offline charging are marked as "N/A". However, if the specific AVP is received, "Note C-1" can still be applied for this AVP.

NC-2

AVPs associated with non-Ro interfaces are marked as "N/A". However, if the specific AVP is received, "Note C-1" can still be applied for this AVP.

NC-3

When used with the NCC VWS, DCA does not provide inbuilt support for the AoC Service. If no configuration is applied:

- DCA is able to receive AoC (Advice of Charge) AVPs in the inbound Diameter request messages (all unconfigured AVPs are simply ignored),
- DCA will not send AoC AVPs in the outbound Diameter messages.
- DCA does supports Diameter Event based Price Enquiry which allows for reporting the price of the call/session separately from the call/session itself (for example, before the call).

With the appropriate configuration:

- For session based charging, sending of AoC information AVPs at the end of the call is not readily supported without configuration issues.
- For event based charging, when the Named Event node is used in the ACS control plan, DCA may be able to map the session charge into outbound AoC information AVPs but under a restricted set of conditions (See *Diameter Control Agent Technical Guide* and *Charging Control Services Technical Guide* for details).
- Sending of real-time (AoC) information (for example, to provide accumulated cost for ongoing usage every 5 seconds) is not supported. DCA is non-compliant for real-time AoC service when used with the NCC VWS.
- Any Diameter responses sent will be limited by DCA's AvpMapping configuration, the ACS UATB control plan node (for Session-based charging) and "Note C-1" (above).
- When used with BRM or the NCC DCD application, support for the AoC Service is dependent on the external billing or rating system. See G-2 and G-3 for details and specific limitations.

Generic capabilities and limitations for sending outbound information are summarized in Note C-3 and NC-5.

NC-4

Not compliant if the specific AVP is a context or identifier or field that requires correlation with another session for tariff determination of the current session and/or the specific AVP involves other service-specific correlation or if the charging session flow involves non-standard session-control or real-time requirement that cannot be handled by the capabilities and featureset of DCA and/or the ACS control plan.

Note that Northbound convergent billing/rating engines may offer the ability to correlate this information. The ability to do this is dependent on the capabilities of the target convergent platform. See Note G-3.

NC-5

Non compliant if the outbound AVP is a concept that ACS does not understand (that is, AVP value cannot be mapped from any available ACS field) and the AVP cannot be dealt with using the DCA AvpMapping configuration (for example, by assigning a fixed constant per applicable service to be returned in the Diameter response message).

Note however that new fields can be defined as a user-defined ACS Profile and used in the ACS control plan and subsequently mapped to an outbound AVP. This may or may not provide the level of functionality or compliance required.

NC-6

For some highly complex data structure, the DCA Raw Data AvpMapping feature may not be sufficient to provide adequate compliance (see Note G-2 for additional details).

For example, if a complex AVP contains multiple subfields and:

- only subfield-1 is required and subfield-1 is always present and always located at the start of the AVP and has a known fixed length, then this subfield can be extracted and hence DCA complies for the specific AVP.
- only subfield-8 is required, but subfield-8 does not have a known (well-defined) offset within the AVP value and it is not the first or last subfield in the AVP and it's length is variable, then it is likely that DCA would not comply for the specific AVP.

NC-7

DCA does not support non-Ro interface messages, Price Request/Response, Tariff Request/Response, Service Usage Request/Response; DCA also does not support AVPs associated with these messages. Non-compliant if AVP is received in these messages.

However Note C-1 still applies for support messages such as Credit Control Request/Response.

DCA also supports Event-based Price Enquiry when sent over the Ro interface.

General

For *all* compliance levels (including some non-compliant AVPs), the following notes apply.

Note that all "G" notes below apply to all AVPs shown in 7.1 and 7.2.

Note G-1

The AVP can be received by DCA without causing adverse conditions. If no Inbound AvpMapping is configured, DCA will simply ignore the AVP. If an Inbound AvpMapping is configured, see Note C-1.

The AVP will not be sent by DCA in outbound diameter message if no Outbound AvpMapping is configured. If an Outbound AvpMapping is configured, see Note C-3.

Note G-2

DCA Raw Data Mapping can be used to extract information (sub-fields) from AVPs that contain complex data structures. If DCA Raw Data mapping is used, the specific AVP value (or a sub-field) can be mapped from an OctetString to ACS. This feature allows unsupported AVP formats to be mapped but is limited to the capabilities of the Raw Data feature described in the *Diameter Control Agent Technical Guide*. See NC-6 for additional details.

Note G-3

The specific AVP can be passed through to the NCC DCD Application to a third Party Convergent Billing Engine (using Diameter Credit-Control). Compliance would depend on the capabilities of the external Credit-Control server (The capabilities of the external Credit-Control server is out-of-scope). Also, if during mid-session (CCR Update) requests, the units (used-service-units AVP) is determined to be not sufficiently exhausted (based on specific CCS threshold parameters; see *Charging Control Services Technical Guide* for details), the SLC (CCS/ACS) may not request additional units from the external Credit-Control server. This feature may restrict timely pass-through of specific AVPs and may impact services that require proper real-time transfer of AVPs through the SLC.

Note G-4

For convergent deployments where BRM is used for rating (as opposed to VWS) compliance would depend on the capabilities of BRM (the BRM specifics are out-of-scope; consult BRM documentation for details). Also, if during mid-session (CCR Update) requests, the units (used-service-units AVP) is determined to be not sufficiently exhausted (based on specific CCS threshold parameters; see *Charging Control Services Technical Guide* for details), the SLC (CCS/ACS) may not request additional units from the BRM server. This feature may restrict timely pass-through of specific AVPs and may impact services that require proper real-time transfer of AVPs through the SLC.

Note G-5

If configured to use an external billing system, compliance would depend on the capabilities of external system and with the limitations described in Notes G-2 and G-3 above.

Glossary of Terms

AAA

Authentication, Authorization, and Accounting. Specified in Diameter RFC 3588.

AC

Application Context. A parameter in a TCAP message which indicates what protocol is conveyed. May indicate, for example, MAP, CAMEL, or INAP. Also usually specifies the particular version of the conveyed protocol, for example, which CAMEL Phase.

ACS

Advanced Control Services configuration platform.

ANI

Automatic Number Identification - Term used in the USA by long-distance carriers for CLI.

API

Application Programming Interface

ASA

Session message: Abort Session Answer

ASR

Session message: Abort Session Request

ATI

Any Time Interrogation - this process is used on a GSM network to interrogate the HLR for location and or subscriber information.

AVP

Attribute Value Pair, used in Diameter to represent properties of a particular request or answer.

BFT

Billing Failure Treatment - the process that is applied if the system has lost all connections to a billing engine. It allows for limited continuation of call processing functions, if configured.

CAMEL

Customized Applications for Mobile network Enhanced Logic

This is a 3GPP (Third Generation Partnership Project) initiative to extend traditional IN services found in fixed networks into mobile networks. The architecture is similar to that of traditional IN, in that the control functions and switching functions are remote. Unlike the fixed IN environment, in mobile networks the subscriber may roam into another PLMN (Public Land Mobile Network), consequently the controlling function must interact with a switching function in a foreign network. CAMEL specifies the agreed information flows that may be passed between these networks.

CC

Country Code. Prefix identifying the country for a numeric international address.

CCA

Credit-Control-Answer, used in Diameter by the credit-control server to acknowledge a Credit-Control-Request (CCR) from the credit-control client.

CCR

Credit-Control-Request, used in Diameter by the credit-control client to request credit authorization from the credit-control server.

CCS

1) Charging Control Services component.

2) Common Channel Signalling. A signalling system used in telephone networks that separates signalling information from user data.

CEA

Peer message: Capabilities Exchange Answer

CER

Peer message: Capabilities Exchange Request

CLI

Calling Line Identification - the telephone number of the caller. Also referred to as ANI.

Connection

Transport level link between two peers, providing for multiple sessions.

Convergent

Also “convergent billing”. Describes the scenario where post-paid and pre-paid calls are handed by the same service platform and the same billing system. Under strict converged billing, post-paid subscribers are essentially treated as “limited credit pre-paid”.

CORBA

Common Object Request Broker Architecture. It is a framework that provides interoperability between objects built in different programming languages, running on different physical machines perhaps on different networks. It specifies an Interface Definition Language, and API that allows client / server interaction with the ORB.

cron

Unix utility for scheduling tasks.

Diameter

A feature rich AAA protocol. Utilises SCTP and TCP transports.

DP

Detection Point

DPA

Peer message: Disconnect Peer Answer

DPR

Peer message: Disconnect Peer Request

DTMF

Dual Tone Multi-Frequency - system used by touch tone telephones where one high and one low frequency, or tone, is assigned to each touch tone button on the phone.

DWA

Peer message: Device Watchdog Answer

DWR

Peer message: Device Watchdog Request

FDA

First Delivery Attempt - the delivery of a short message directly to the SME rather than relaying it through the MC.

FOX

Fast OSA eXtensions. A TCP/IP billing protocol intended for use with external vendors. Based on OSA, it fills in functional gaps missing in OSA, and defines “combined” OSA operations to increase platform throughput. Uses a non-CORBA transport layer in order to provide enhanced fail-over and connection redundancy.

GPRS

General Packet Radio Service - employed to connect mobile cellular users to PDN (Public Data Network- for example the Internet).

GSM

Global System for Mobile communication.

It is a second generation cellular telecommunication system. Unlike first generation systems, GSM is digital and thus introduced greater enhancements such as security, capacity, quality and the ability to support integrated services.

HLR

The Home Location Register is a database within the HPLMN (Home Public Land Mobile Network). It provides routing information for MT calls and SMS. It is also responsible for the maintenance of user subscription information. This is distributed to the relevant VLR, or SGSN (Serving GPRS Support Node) through the attach process and mobility management procedures such as Location Area and Routing Area updates.

HPLMN

Home PLMN

HTML

HyperText Markup Language, a small application of SGML used on the World Wide Web.

It defines a very simple class of report-style documents, with section headings, paragraphs, lists, tables, and illustrations, with a few informational and presentational items, and some hypertext and multimedia.

IDP

INAP message: Initial DP (Initial Detection Point)

IMS

IP Multimedia Subsystem (3GPP) enables the use of multimedia services based on and built upon Internet applications, services and protocols. These protocols include SIP, which is used to manage the IP multimedia sessions.

IMSI

International Mobile Subscriber Identifier. A unique identifier allocated to each mobile subscriber in a GSM and UMTS network. It consists of a MCC (Mobile Country Code), a MNC (Mobile Network Code) and a MSIN (Mobile Station Identification Number).

The IMSI is returned by the HLR query (SRI-SM) when doing FDA. This tells the MSC exactly who the subscriber is that the message is to be sent to.

IN

Intelligent Network

INAP

Intelligent Network Application Part - a protocol offering real time communication between IN elements.

Initial DP

Initial Detection Point - INAP Operation. This is the operation that is sent when the switch reaches a trigger detection point.

IP

1) Internet Protocol

2) Intelligent Peripheral - This is a node in an Intelligent Network containing a Specialized Resource Function (SRF).

IPSec

IP Security. Security protocol implemented at the IP layer.

ISDN

Integrated Services Digital Network - set of protocols for connecting ISDN stations.

ISUP

ISDN User Part - part of the SS7 protocol layer and used in the setting up, management, and release of trunks that carry voice and data between calling and called parties.

ITU

International Telecommunication Union

MAP

Mobile Application Part - a protocol which enables real time communication between nodes in a mobile cellular network. A typical usage of the protocol would be for the transfer of location information from the VLR to the HLR.

MC

Message Centre. Also known as SMSC.

MCC

Mobile Country Code. In the location information context, this is padded to three digits with leading zeros. Refer to ITU E.212 ("Land Mobile Numbering Plan") documentation for a list of codes.

Messaging Manager

The Messaging Manager service and the Short Message Service components of Oracle Communications Network Charging and Control product. Component acronym is MM (formerly MMX).

MM

Messaging Manager. Formerly MMX, see also *XMS* (on page 91) and *Messaging Manager* (on page 87).

MNC

Mobile Network Code. The part of an international address following the mobile country code (MCC), or at the start of a national format address. This specifies the mobile network code, that is, the operator owning the address. In the location information context, this is padded to two digits with a leading zero. Refer to ITU E.212 ("Land Mobile Numbering Plan") documentation for a list of codes.

MS

Mobile Station

MSC

Mobile Switching Centre. Also known as a switch.

MSIN

Mobile Station Identification Number.

MSISDN

Mobile Station ISDN number. Uniquely defines the mobile station as an ISDN terminal. It consists of three parts; the country code (CC), the national destination code (NDC) and the subscriber number (SN).

MT

Mobile Terminated

MTP

Message Transfer Part (part of the SS7 protocol stack).

NAS

Network Access Services. Control point for authorising (and restricting) access to a network. Normally located on the network fringe.

ORB

Object Request Broker. Within an Object based communication system, an ORB keeps track of the actual addresses of all defined objects and thus is used to route traffic to the correct destination. The CORBA defines the ORB in a series of standards enabling different platforms to share common information.

OSA

Open Service Access provides a standard interface through which developers can design services that may interact with functions within the network.

Peer

Remote machine, which for our purposes is capable of acting as a Diameter agent.

PI

Provisioning Interface - used for bulk database updates/configuration instead of GUI based configuration.

PLMN

Public Land Mobile Network

RADIUS

Remote Authentication Dial-In User Service - a system of distributed security that secures remote access to networks and network services against unauthorised access.

SCCP

Signalling Connection Control Part (part of the SS7 protocol stack).

SCTP

Stream Control Transmission Protocol. A transport-layer protocol analogous to the TCP or User Datagram Protocol (UDP). SCTP provides some similar services as TCP (reliable, in-sequence transport of messages with congestion control) but adds high availability.

Session

Diameter exchange relating to a particular user or subscriber access to a provided service (for example, a telephone call).

SGML

Standard Generalized Markup Language. The international standard for defining descriptions of the structure of different types of electronic document.

SGSN

Serving GPRS Support Node

SIP

Session Initiation Protocol - a signaling protocol for Internet conferencing, telephony, event notification and instant messaging. (IETF)

SLC

Service Logic Controller (formerly UAS).

SLEE

Service Logic Execution Environment

SME

Short Message Entity - This is an entity which may send or receive short messages. It may be located in a fixed network, a mobile, or an SMSC.

SMS

Depending on context, can be:

- Service Management System hardware platform
- Short Message Service
- Service Management System platform
- NCC Service Management System application

SMSC

Short Message Service Centre stores and forwards a short message to the indicated destination subscriber number.

SN

Service Number

SNMP

Simple Network Management Protocol. Usually responsible for notifying faults on a network.

SRF

Specialized Resource Function – This is a node on an IN which can connect to both the SSP and the SLC and delivers additional special resources into the call, mostly related to voice data, for example play voice announcements or collect DTMF tones from the user. Can be present on an SSP or an Intelligent Peripheral (IP).

SRI

Send Routing Information - This process is used on a GSM network to interrogate the HLR for subscriber routing information.

SS7

A Common Channel Signalling system is used in many modern telecoms networks that provides a suite of protocols which enables circuit and non-circuit related information to be routed about and between networks. The main protocols include MTP, SCCP and ISUP.

SSL

Secure Sockets Layer protocol

SSP

Service Switching Point

TCAP

Transaction Capabilities Application Part – layer in protocol stack, message protocol.

TCP

Transmission Control Protocol. This is a reliable octet streaming protocol used by the majority of applications on the Internet. It provides a connection-oriented, full-duplex, point to point service between hosts.

TLS

Transport Layer Security. Cryptographic protocol used to provide secure communications. Evolved from SSL.

URI

Uniform Resource Identifier.

VLR

Visitor Location Register - contains all subscriber data required for call handling and mobility management for mobile subscribers currently located in the area controlled by the VLR.

VWS

Oracle Voucher and Wallet Server (formerly UBE).

XML

eXtensible Markup Language. It is designed to improve the functionality of the Web by providing more flexible and adaptable information identification.

It is called extensible because it is not a fixed format like HTML. XML is a `metalanguage' — a language for describing other languages—which lets you design your own customized markup languages for limitless different types of documents. XML can do this because it's written in SGML.

XMS

Three letter code used to designate some components and path locations used by the Oracle Communications Network Charging and Control *Messaging Manager* (on page 87) service and the Short Message Service. The published code is *MM* (on page 87) (formerly MMX).

Index

T

U

V

X