amdocs

DCCA Interface for Content Service (Aepona)

Document Information

Software Version:	
Publication Date:	
Catalog Number:	**1886434**
Security Level:	**Level 3 - Highly Sensitive**
Creation Date:	**11 April 2013**
Account/FOP:	
Author:	**Torchinsky Elena**
Editor:	**Ori Riechman**
Last Edit Date:	**13.8.2013**
File Name:	
Template:	**Universal1Side.dot**

Internal Document Approvals

Document Owner Approval		Business Analyst Approval	
Name	**Date**	**Name**	**Date**
	mm-dd-yyyy		mm-dd-yyyy

Document Internal Release Notes

Author/Editor			Change Comments		DC Ver.
Name	**Application**	**Date mm-dd-yyyy**	**Section #**	**Change**	

Contents

1. INTRODUCTION

1.1. Purpose and Scope

This document contains the description of the Diameter Credit Control Application (DCCA) for integration of the AEPONA and Amdocs OCS.

The chosen protocol for the real-time interface between the AEPONAand Amdocs OCS is the Diameter Credit Control Application (DCCA). It is a standard Diameter-base application, as used in the telecommunication market for the implementation of real-time credit control and as a service cost interface between a network element and a billing system.

The definition of the interface is based on 3GPP 32.299, RFC 4006 and RFC 3588.

1.2. Related Documentation

DC#	Document Title
	RFC 3588, Diameter Base Protocol, September 2003
	RFC 4006, Diameter Credit-Control Application, August 2005
	3GPP TS 32.299 - Charging management; Diameter charging applications

1.3. Terminology

The document includes the following key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL". The key words are to be interpreted as follows:

MUST This word, or the terms "REQUIRED" or "SHALL", indicate an absolute requirement.

MUST NOT This phrase, or the phrase "SHALL NOT", indicates an absolute prohibition.

SHOULD This word, or the adjective "RECOMMENDED", indicates that there may be valid reasons in certain circumstances to ignore a particular item, but the full implications MUST be understood and carefully considered before choosing a different course. When an item is ignored the bidder is asked to detail the underlying reasons.

SHOULD NOT This phrase, or the phrase "NOT RECOMMENDED" indicates that there may be valid reasons in certain circumstances when the particular behavior is acceptable or even useful, but the full implications SHOULD be understood and the case carefully considered before implementing any behavior described with this label. In such a case the bidder is asked to detail the underlying reasons for implementing this behavior.

MAY This word, or the adjective "OPTIONAL", means that an item is truly optional.

The declarations are compliant with DCCA RFC-s.

1.4. Terms and Definitions

Following is a list of terms used in this document that the reader should be familiar with:

Term	Definition
AMC	Amdocs Management & Control
API	Application Programming Interface
AVP	Attribute-Value Pairs
DCCA	Diameter Credit-Control Application
FR	Formatting and Routing
MD	Mediation Device
MOC	Mobile Originated Call
MTC	Mobile Terminated Call
O/M	Optional/Mandatory
OCS	Online Charging
RB	Rating and Balance management
TCP	Transmission Control Protocol

1.5. Assumptions

1. The transport protocol is TCP/IP.
2. No support is provided for Diameter Relay, Proxy, Redirect, or Translation Agents.

   For real time reasons, the connection is a direct permanent socket-based connection between the Diameter Client and Diameter Server (Amdocs OCS FR).
3. If the Diameter client does not receive a response from the Diameter server within the configurable (in milliseconds) timeout period the Diameter client should reject or allow the session according to the predefined policy.

   There are multiple connections between the Diameter Client and Diameter Server for failover and load balancing purposes.
    If one Diameter connection fails, the Diameter Client is able to switch over to another Diameter connection between the Diameter Client and Diameter Server. The Diameter Client is able to recover the failed connect when available in the background.
   The load balancing across multiple active connections to Diameter Serveris supported by Diameter Client.
4. The length of a Session-Id AVP will be less than 128 bytes
5. As currently there is no DRA solution in place, The redundancy and failover will be performed by the client Diameter , meaning Aepona
6. Based on agreement between U.C. Cellular and Aepona, Aepona will handle the following:
   - Support Amount-based charging Diameter transactions for one time and recurring app purchases.
   - Aepona will not support volume based Gy interface.

2. PROTOCOL DESCRIPTION

DCCA uses the TCP for the transport layer. The Diameter Client application (AEPONA) is the initiator that establishes a connection. Amdocs OCS (FR) is the Diameter Server component that responds to the client's requests.

2.1. Connection Management

The Online Charging (OCS) server supports multiple connections to multiple client applications.

The interaction-on-socket connection:

Establishes connection at TCP/IP level and DCCA level

Sends/receives application messages

Sends/receives keep-alive Device Watchdog Requests/answer messages (when there is no application traffic)

Disconnects

2.2. Connection Establishment

A permanent bi-directional TCP/IP connection is established between Diameter Client and Diameter Server (OCS). Diameter Client is the initiator that establishes the connection.

OCS supports multiple connections to the same standard Diameter port #3868, and handles multiple concurrent sessions on each connection.

After establishing the connection at the TCP/IP level, Diameter Client sends a Capabilities Exchange Request (CER) and waits for the Capabilities Exchange Answer (CEA). The CER/CEA exchange must be successfully completed before application messages can be exchanged.

It is required that the first DCCA message of connection established between Diameter Client and Diameter Server be a CER message. Otherwise, Diameter Server sends a reject response (with Message Sequence Error) and closes the network connection.

The CEA returns the status of the established connection.

2.3. Connection Failure Detection

Device Watchdog Request/Answer (DWR/DWA) messages provide the mechanism thatenables Diameter Client to keep the connection open when it is not in use.

A DWR will be sent by the client in the following cases:

- **No CCR sent within "Idle-Connection" timeout** from the last response – just to keep the connection alive.

A DWR message resets the connection timeout period in OCS, thus preventing the server from disconnecting an idle connection.

Regardless of DWR/DWA messages, if Diameter Client detects a TCP/IP connection error when sending a message, it will try to re-establish the connection.

2.4. Disconnection

Diameter Client may wish to close the connection to Diameter Server. However, the request may be initiated from Diameter Server, too (for example, before an upgrade procedure starts).

An initiator of a connection termination uses the Disconnect Peer Request (DPR). The receiver of the request responds with a Disconnect Peer Answer (DPA).

When there is a disconnection (for any reason), Diameter Client will periodically try to reestablish the connection. The frequency of the reconnection attempts is configurable.

2.5. Message Structure

Once a socket connection is established, communication is conducted via binary messages on the TCP/IP socket. The communication is based on request and response messages, which include a fixed message header and a variable message body according to RFC 3588.

All message attributes must be in network-byte order.

A message starts with a Diameter header and AVP as defined by RFC 3588 according to type of message.

2.6. Message Timeouts

There are managed message-related timeouts in both Diameter Client and Diameter Server.

In OCS, there is a managed Maximal-Request-Processing timeout. If the Maximal-Request-Processing timeout exceeds, OCS assumes that the answer is not relevant any more for Diameter Client - the message is discarded and an error is logged.

The timeouts of Diameter Client and Diameter Server have to be synchronized – Message-Response (client) timeout should be longer than the Maximal Request Processing (OCS) timeout plus the network delay.

2.7. Session Management

This section describes the management of a session established between Diameter Client and Diameter Server.

2.7.1. Source Identifier

The *Origin-Host* (AVP code 264) is mandatory in all Diameter messages. The Origin-Host uniquely identifies the Diameter Client from which the request message originates. The ID of the Diameter Client is used by Amdocs Online Charging to identify the session. The Origin-Host is echoed on all types of message responses.

2.7.2. Session-ID AVP and CC-Request-Number AVP

The Session ID identifies a session-based interaction between the Diameter Client and Amdocs Online Charging. The Session ID is unique and should not be duplicated or reused until the entire range of session IDs (2^{64}IDs) has been used. The uniqueness of every Session ID should be guaranteed by the Diameter Client even in the event of a failure.

The 64-bit Session ID contains the decimal high and low 32-bit parts of the Session-ID RFC 3588 AVP sequence:

<DiameterIdentity>;<high 32 bits>;<low 32 bits>[;<optional value>]

The uniqueness of the Session ID serves the following purposes:

- Correlation of session-based reservations and charge requests
- Detection and handling of duplicate requests

The response message must specify the same Session ID that was received in the original request.

The Amdocs Online Charging implementation does not include handling the optional part of the Session ID. However, Amdocs Online Charging is responsible for returning this part to the DCCA client in the Session ID response attribute.

2.7.3. OCS Handling of Duplicate Requests

Message attributes (Event-Timestamp, Subscription-Id-Data,) are logged into a processed-transactions table for every reservation or charge message that is checked for a duplicate. The table is cycled,its size is configurable. It is mainly used for online retransmission only.

In case of a duplicated message will arrive to the system, OCS will send a success response to AMP.

2.8. Communication Problems

OCS supports a degraded mode of operations – useful in cases when a real time connection between Diameter Client and Diameter Server is lost.

After communication between Diameter Client and Diameter Server is re-established, Diameter Client re-news sending events online to Diameter Server.

In case of a connection problem, Diameter Client behaves according to apre-defined policy.

2.8.1. TCP/IP Level Error

Diameter Client:

- The status of the TCP/IP connection and DCCA session is set to *Disconnected*.
- The Diameter Client attempts to re-establish a DCCA connection.

2.8.2. No CCA Received in Specified Timeout

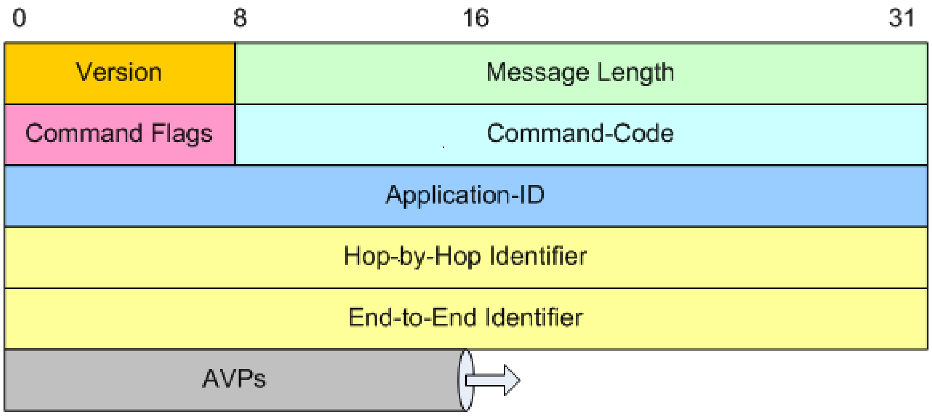
The Diameter Client:

- Resends the CCR (if supported).
- Sends DWR requests (number of send attempts).
- If a DWA is received, sets the connection to *Open*.
- If a DWA is not received, resets the TCP/IP connection (performs TCP/IP disconnect) and then restarts the TCP/IP connection and DCCA session.

3. MESSAGE DESCRIPTIONS

This chapter describes the charging messages supported by the protocol.

3.1. Diameter Header



Every DCCA message starts with a Diameter header. The header is 20 octets long and includes the following fields:

- Version – Diameter version (1 octet long) – 1
- Message length – (3 octets)
- Command flags – (1 octet) indicators occupying eight bytes:
  - Request/answer
  - Proximal – NOT IN USE in this interface
  - Error – Message contains protocol error
  - Retransmit – Indicates POTENTIAL re-transmission
  - Reserved – NOT IN USE
- Command code – (3 octets)
- Application ID – (4 octets)
  - “0” for CER/DWR/DPR CEA/DWA/DPA
  - “4” for CCR/CCA message
- Hop-by-hop identifier – The response must contain the same value that was received in the request.
- End-to-End Identifier – (4 octets) unsigned 32-bit integer
  - NOT IN USE by the server (OCS) for unique message ID
  - This field is copied by the server into the Answer message

3.2. Transaction Table

The following messages defined in the Diameter base must be supported.

Command Name	Abbreviation	Source Application	Destination Application
Credit Control Request	CCR	Diameter Client	Diameter Server
Credit Control Answer	CCA	Diameter Server	Diameter Client
Capabilities Exchange Request	CER	Diameter Client	Diameter Server
Capabilities Exchange Answer	CEA	Diameter Server	Diameter Client
Device Watchdog Request	DWR	Diameter Client	Diameter Server
Device Watchdog Answer	DWA	Diameter Server	Diameter Client
Disconnect Peer Request	DPR	Diameter Client/Server	Diameter Client/Server
Disconnect Peer Answer	DPA	Diameter Client/Server	Diameter Client/Server

3.3. Capabilities Exchange Request (CER)

A CER is sent by Diameter Client after the TCP connection is established.

Message format:

Diameter header

Host-IP-Address Used to inform a Diameter peer of the sender’s IP address.

Origin-Host Unique identifier of client instance (mandatory).

Vendor-ID Zero value, required as CER mandatory attribute.

Origin-Realm This AVP contains the Realm of the originator of any Diameter message.

Product-Name The Product-Name AVP should remain constant across firmware revisions for the same product.

Auth-Application-ID Advertises support of the Authentication and Authorization portion of an application.

```
<CER> ::= < Diameter Header: 257, REQ >
     { Host-IP-Address }
     { Origin-Host }
     { Origin-Realm }
     { Product-Name }
     { Vendor-ID }
      [ Auth-Application-ID ]
```

The *Inband-Security-ID* and *Firmware-Revision* are optional attributes. They are not in use for current implementation of the DCCA.

The *Auth-Application-ID* must be set to the value 4, indicating the Diameter credit-control application.

3.4. Capabilities Exchange Answer (CEA)

The CEA is Diameter Server’s response to the CER.

Diameter Server (OCS) returns CEA with proper result code.

Message format:

Diameter header

Host-IP-Address Used to inform a Diameter peer of the sender’s IP address.

Origin-Host Unique identifier of server instance (mandatory). The Origin-Host is echoed on all types of message responses.

Vendor-ID Value 11580 , required as CEA mandatory attribute.

Origin-Realm Sent back by Diameter Server, required to be different from the value send by Diameter Client.

Product-Name Sent back by Diameter Server, required to be different from the value sent by Diameter Client.

The Product-Name value responded to Diameter Client is ‘*Amdocs DCCA*’.

Result-Code

```
<CEA> ::= < Diameter Header: 257, RES >
     { Host-IP-Address }
     { Origin-Host }
     { Origin-Realm }
     { Product-Name }
     [ Auth-Application-ID ]
     { Vendor-ID }
     { Result-Code }
```

3.5. Device Watchdog Request (DWR)

DWR is the keep-alive message sent by Diameter Client.

Message format:

Diameter header

Origin-Host Unique identifier of the client instance (mandatory).

Origin-Realm This AVP contains the Realm of the originator of any Diameter message.

Origin-State-Id A monotonically increasing value that is advanced whenever a Diameter entity restarts with loss of previous state, for example upon reboot.

```
<DWR>::= < Diameter Header: 280, REQ >
     { Origin-Host }
     { Origin-Realm }
     { Origin-State-Id }
```

3.6. Device Watchdog Answer (DWA)

DWA is Diameter Server's response to the DWR.

Message format:

Diameter header

Origin-Host Unique identifier of the server instance (mandatory)
Origin-Host is echoed on all types of message responses

Origin-Realm Sent back by Diameter Server, required to be different from the value sent by the Diameter Client

Result-Code

```
<DWA>::= < Diameter Header: 280, RES >
     { Origin-Host }
     { Origin-Realm }
     { Result-Code }
```

3.7. Disconnect Peer Request (DPR)

This is the peer request to disconnect the transport connection.

Message format:

Diameter header

Origin-Host Unique identifier of the client instance (mandatory)

Disconnect-Cause Reason for disconnect

Origin-Realm This AVP contains the Realm of the originator of any Diameter message

```
<DPR>::= < Diameter Header: 282, REQ >
     { Origin-Host }
     { Origin-Realm }
     { Disconnect-Cause }
```

3.8. Disconnect Peer Answer (DPA)

This is the peer response to the DPR.

Message format:

Diameter header

Origin-Host Unique identifier of server instance (mandatory). Origin-Host is echoed on all types of message responses.

Origin-Realm Sent back by Diameter Server, required to be different from the value sent by the Diameter Client.

Result-Code

```
<DPA>::= < Diameter Header: 282, RES >
     { Origin-Host }
     { Origin-Realm }
     { Result-Code }
```

3.9. Credit Control Messages

Credit control request/answer messages are used for all credit control events.

The following application events are in scope for this document:

CCR Direct Debit

CCR Authorization

CCR Terminate

CCR Refund

3.9.1. General

3.9.1.1. Message Reject Policy

Unknown Message

If an unknown message type and/or unknown *CC-Request-Type* are sent from Diameter Client to Diameter Server, Diameter Server will not continue to process the message.

Instead, Diameter Server will send a message reject response back with a result code value of DIAMETER_UNABLE_TO_COMPLY.

Unknown Attribute

If an unknown attribute or incorrect optional attribute is sent to Diameter Server from Diameter Client,Diameter Server will reject the request with the error code 'Diameter-Rating-Failed'.

3.9.2. Content Service

3.9.2.1. CCR Authorization

The CCR Authorization message results in OCS processing an authorize unit transaction.

- The CCR request is implemented with

CC-Request-Type = 1 (INITIAL_REQUEST)

a) Request Parameters

```
<CCR> ::= < Diameter Header: 272, REQ >
     < Session-ID>
     { Origin-Host }
     { Origin-Realm }
     { Destination-Realm }
     { Auth-Application-Id }
     [ Content-Description ]
     { CC-Request-Type }
     { CC-Request-Number }
     [ Destination-Host ]
     [ Requested-Action ]
     { Event-Timestamp }
     *{ Subscription-ID }
          { Subscription-ID-Type }
          { Subscription-ID-Data }
     { Service-Identifier }
     *{ Requested-Service-Unit }
          *{ CC-Money }
               *{ Unit-Value }
                    { Value-Digits }
                    { Exponent }
                [ Currency-Code]
     { Purchase-Category-Code }
     { Application-Type }
```

b) Response Parameters

```
<CCA> ::= < Diameter Header: 272,RES>
     < Session-ID>
     { Origin-Host }
     { Origin-Realm }
     { Auth-Application-ID }
     { CC-Request-Number }
     { CC-Request-Type }
     { Result-Code }
```

3.9.2.2. CCR Terminate

The CCR Terminate message results in OCS processing a charge unit transaction.

The CCR request is implemented with *CC-Request-Type=3 (TERMINATION*_REQUEST). We will distinguish whether client sent a Cancel (Cancel-event) or a Commit (Terminate event) using the Used-Service-Unit AVP. - The Used-Service-Unit AVP value of the Cancel (Cancel-event) request will be $0 and for Commit (Terminate-event), the value is greater than $0.
Request Parameters

```
<CCR> ::= < Diameter Header: 272, REQ >
     < Session-Id>
     { Origin-Host }
     { Origin-Realm }
     { Destination-Realm }
     { Auth-Application-Id }
     [ Content-Description ]
     { CC-Request-Type }
     { CC-Request-Number }
     [ Destination-Host ]
     [ Requested-Action ]
     { Event-Timestamp }
     *{ Subscription-ID }
          { Subscription-ID-Type }
          { Subscription-ID-Data }
     [ Termination-Cause ]
     { Service-Identifier }
     *{ Used-Service-Unit }
          *{ CC-Money }
               *{ Unit-Value }
                    { Value-Digits }
                    { Exponent }
               [ Currency-Code]

     {Partner-Id}
     { Purchase-Category-Code }
     { Application-Type }
```

c) Response Parameters

```
<CCA> ::= < Diameter Header: 272,RES>
     < Session-ID>
     { Origin-Host }
     { Origin-Realm }
     { Auth-Application-ID }
     { CC-Request-Number }
     { CC-Request-Type }
     { Result-Code }
```

3.9.2.3. CCR Refund

The CCR Refund message results in OCS processing a refund unit transaction.

The CCR request is implemented with the *Requested-Action=REFUND_ACCOUNT and CC-Request-Type=4 (EVENT_REQUEST)*.

d) Request Parameters

```
<CCR> ::= < Diameter Header: 272, REQ >
     < Session-Id>
     { Origin-Host }
     { Origin-Realm }
     { Destination-Realm }
     { Auth-Application-Id }
     [ Content-Description ]
     { CC-Request-Type }
     { CC-Request-Number }
     [ Destination-Host ]
     { Requested-Action }
     { Event-Timestamp }
     *{ Subscription-ID }
          { Subscription-ID-Type }
          { Subscription-ID-Data }
     { Service-Identifier }
     *{ Requested-Service-Unit }
          *{ CC-Money }
               *{ Unit-Value }
                    { Value-Digits }
                    { Exponent }
          [ Currency-Code]

     {Partner-Id}
     { Purchase-Category-Code }
     { Application-Type }
     { Adjustment-Reason-Code }
```

e) Response Parameters

```
<CCA> ::= < Diameter Header: 272,RES>
     < Session-ID>
     { Origin-Host }
     { Origin-Realm }
     { Auth-Application-ID }
     { CC-Request-Number }
     { CC-Request-Type }
     { Result-Code }
```

3.9.2.4. CCR Direct Debit

The CCR Direct Debit message results in OCS processing a charge unit transaction.

The CCR request is implemented with the *Requested-Action=DIRECT_DEBITING and CC-Request-Type=4 (EVENT_REQUEST)*.

f) Request Parameters

```
<CCR> ::= < Diameter Header: 272, REQ >
     < Session-Id>
     { Origin-Host }
     { Origin-Realm }
     { Destination-Realm }
     { Auth-Application-Id }
     [ Content-Description ]
     { CC-Request-Type }
     { CC-Request-Number }
     [ Destination-Host ]
     { Requested-Action }
     { Event-Timestamp }
     *{ Subscription-ID }
          { Subscription-ID-Type }
          { Subscription-ID-Data }
     { Service-Identifier }
     *{ Used-Service-Unit }
          *{ CC-Money }
               *{ Unit-Value }
                    { Value-Digits }
                    { Exponent }
          [ Currency-Code]

     {Partner-Id}
     { Purchase-Category-Code }
     { Application-Type }
```

g) Response Parameters

```
<CCA> ::= < Diameter Header: 272,RES>
     < Session-ID>
     { Origin-Host }
     { Origin-Realm }
     { Auth-Application-ID }
     { CC-Request-Number }
     { CC-Request-Type }
     { Result-Code }
```

4. Charging Parameters– Implementing Valid Values

4.1. Result-Code

The following is a list of the values for the Result-Code attribute. The description of each Result-Code value includes code, value, source of declaration and a description.

In the column ‘Trx-Message’, marked in red is the parameter which will be included in the message. Trx-Message is not an AVP, but only a description the client can send to its users based on RESULT-CODE returned on CCA.

Name	Value	Source	Description	Trx-Message - Trx message can display a message to the user by the client
DIAMETER_SUCCESS	2001	RFC-3588	Success	For Authorization: **Balance is greater than (or equal to) <amount requested for balance check >** For Debit: **01 Your application download was successful. To retrieve your account balance, dial #BAL**
DIAMETER_UNABLE_TO_COMPLY	5012	RFC-3588	System/Application Error	**03 Transaction could not be completed. Try again or contact customer service by dialing 611.**
DIAMETER_TOO_BUSY	3004	RFC-3588	System Overload Error	**03 Transaction could not be completed. Try again or contact customer service by dialing 611.**

Name	Value	Source	Description	Trx-Message - Trx message can display a message to the user by the client
DIAMETER_CREDIT_LIMIT_REACHED	4012	RFC-4006	Insufficient Balance	**07 Download failed due to insufficient funds. Available balance: <balance>**
DIAMETER_USER_UNKNOWN	5030	RFC-4006	Unknown Subscriber	**04 Account not found. Please call 611 for customer assistance.**
DIAMETER_RATING_FAILED	5031	RFC-4006	PE Processing failed	**03 Transaction could not be completed. Try again or contact customer service by dialing 611.**

5. AVP Descriptions

AVP Summary

The following table contains descriptions of all AVP protocol attributes.

The current table is a Data Dictionary original for both client and server systems.

- M – This AVP will always be present in the message.
- C – This AVP shall be present in the message only when certain conditions are met. These conditions are specified in the description column.
- O– This AVP is optional.

AVP Name	AVP Code	Vendor ID	Used in								Value Type	AVP Flags			Description / Comments
			CER	CEA	DWR	DWA	DPR	DPA	CCR	CCA		V	M	P	
Session-Id	263	-							M	M	UTF8String	0	1	0	All messages pertaining to a specific session MUST include only one Session-Id AVP and the same value MUST be used throughout the life of a session. The format is as follows: **<DiameterIdentity>;<high 32 bits>;<low 32 bits>[;<optional value>]**, where high 32-bit and low 32-bit parts represent the 64-bit session identifier. The optional part is out of server support.
Origin-Host	264	-	M	M	M	M	M	M	M	M	Diameter Identity	0	1	0	The host name of the DCCA where the request originated, as seen by Amdocs Online Charging. A different value can be configured for every diameter server. The origin host name is constructed by prefixing the configured host name with the name of the node.

AVP Name	AVP Code	Vendor ID	Used in								Value Type	AVP Flags			Description / Comments
			CER	CEA	DWR	DWA	DPR	DPA	CCR	CCA		V	M	P	
Destination-Host	293								O		Diameter Identity	0	1	0	This AVP MUST be present in all unsolicited agent-initiated messages. It MAY be present in Request messages, and MUST NOT be present in Answer messages.
Origin-Realm	296	-	M	M	M	M	M	M	M	M	Diameter Identity	0	1	0	Realm of the originator of any Diameter message. A different value can be configured for every diameter server. In the response the value will be “amdocs.com”. In the request the value will be “uscellular.com”.
Destination-Realm	283								M		Diameter Identity	0	1	0	Realm to which the message is to be routed
Auth-Application-ID	258	-	M	M					M	M	Unsigned 32	0	1	0	Advertises support of the Authentication and Authorization portion of an application. Must be set to the value 4, indicating the Diameter credit-control application.
Result-Code	268	-		M		M		M		M	Unsigned 32	0	1	0	Indicates the result of the credit authorization.

AVP Name	AVP Code	Vendor ID	Used in								Value Type	AVP Flags			Description / Comments
			CER	CEA	DWR	DWA	DPR	DPA	CCR	CCA		V	M	P	
Disconnect-Cause	273	-					M				Enumerated	0	1	0	A Diameter node MUST include this AVP in the Disconnect-Peer-Request message to inform the peer of the reason for its intention to shut down the transport connection. The following values are supported: REBOOTING (0) – A scheduled reboot is imminent. BUSY (1) – The peer's internal resources are constrained, and it has determined that the transport connection needs to be closed. DO_NOT_WANT_TO_TALK_TO_YOU (2) – The peer has determined that it does not see a need for the transport connection to exist, because it does not expect any messages to be exchanged in the near future
CC-Money	413								M		Grouped	0	1	0	

AVP Name	AVP Code	Vendor ID	Used in								Value Type	AVP Flags			Description / Comments
			CER	CEA	DWR	DWA	DPR	DPA	CCR	CCA		V	M	P	
CC-Request-Number	415	-							M	M	Unsigned 32	0	1	0	This AVP identifies this request within one session. The value will be 0 for one-time events, but it will increase to '1' for Diameter Terminate that follows an Initial request.
CC-Request-Type	416	-							M	M	Enumerated	0	1	0	Specifies the request type: 1 (INITIAL_REQUEST) –two pass event 3 (TERMINATION_REQUEST) - two pass event 4 (EVENT_REQUEST) – for Refund event or charge (one pass event)
Currency-Code	425	-							O		Unsigned 32	0	1	0	if not populated assume USD - code = 840

AVP Name	AVP Code	Vendor ID	Used in								Value Type	AVP Flags			Description / Comments
			CER	CEA	DWR	DWA	DPR	DPA	CCR	CCA		V	M	P	
Unit-Value	445	-							M		Grouped	0	1	0	Specifies the units (money in the case of this interface) as decimal value. The Unit-Value is a value with an exponent; i.e., Unit-Value = Value-Digits AVP * 10^Exponent. This representation avoids unwanted rounding off. For example, the value of 2,3 is represented as Value-Digits = 23 and Exponent = -1. The absence of the exponent part MUST be interpreted as an exponent equal to zero.
Value-Digits	447	-							M		Integer64	0	1	0	Contains the significant digits of the number. If decimal values are needed to present the units, the scaling MUST be indicated with the related Exponent AVP. For example, for the monetary amount $ 0.05 the value of Value-Digits AVP MUST be set to 5, and the scaling MUST be indicated with the Exponent AVP set to -2.

AVP Name	AVP Code	Vendor ID	Used in								Value Type	AVP Flags			Description / Comments
			CER	CEA	DWR	DWA	DPR	DPA	CCR	CCA		V	M	P	
Exponent	429								O		Integer32	0	1	0	Contains the exponent value to be applied for the Value-Digit AVP within the Unit-Value AVP.
Event-Timestamp	55	-							M		Time	0	1	0	Timestamp generated by CSP when CCR is sent. UTC in seconds, since January 1, 1900 00:00
Origin-State-Id	278	-			M						Unsigned32	0	1	0	This field contains the state associated to the CTF. A monotonically increasing value that is advanced whenever a Diameter entity restarts with loss of previous state, for example upon reboot.
Subscription-Id	443	-							M		Grouped	0	1	0	Used to identify the end user’s subscription. The Subscription-Id AVP includes a Subscription-Id-Data AVP that holds the identifier which should be only 10 digits, and a Subscription-Id-Type AVP that defines the identifier type, which as described below should be 0 for MDN type.
Subscription-Id-Data	444	-							M		UTF8String	0	1	0	Used to identify the end user.

AVP Name	AVP Code	Vendor ID	Used in								Value Type	AVP Flags			Description / Comments
			CER	CEA	DWR	DWA	DPR	DPA	CCR	CCA		V	M	P	
Subscription-Id-Type	450	-							M		Enumerated	0	1	0	Used to determine which type of identifier is carried by the Subscription-Id AVP. The value for this field will be 0.(MDN)
Requested-Service-Unit	437	-							C		Grouped	0	1	0	Contains the amount of requested units This empty Grouped AVP is present if more quotas are needed for the associated MSCC instance. This AVP is omitted in the following cases: • The DCCA session is about to be terminated. • The GGSN terminates the MSCC instance. • The Amdocs Online Charging terminates the MSCC instance. The final unit indication is received, and final units are exhausted We need the hierarchy of Requested-Service-Unit --> CC-Money -->Unit-Value --> Value-Digits AVP for the monetary payment. This AVP will be used in Init and Refund events.

AVP Name	AVP Code	Vendor ID	Used in								Value Type	AVP Flags			Description / Comments
			CER	CEA	DWR	DWA	DPR	DPA	CCR	CCA		V	M	P	
Used-Service-Unit	446								C		Grouped	0	1	0	It contains the amount of used units measured from the point when the service became active or, if interim interrogations are used during the session, from the point when the previous measurement ended. We need the hierarchy of Used-Service-Unit --> CC-Money -->Unit-Value --> Value-Digits AVP for the monetary payment. This AVP will be used in Terminate and Direct-Debit events.
Requested-Action	436	-							M		Enumerated	0	1	0	Contains the requested action being sent by Credit-Control-Request command where the CC-Request-Type is set to EVENT_REQUEST. The value will be: 0 (DIRECT_DEBITING) 1 (REFUND_ACCOUNT) This AVP is optional for Init and Terminate events.

AVP Name	AVP Code	Vendor ID	Used in								Value Type	AVP Flags			Description / Comments
			CER	CEA	DWR	DWA	DPR	DPA	CCR	CCA		V	M	P	
Service-Identifier	439	-							M		Unsigned 32	0	1	0	Contains a numeric identifier for a service. Only one service identifier may be present. The value is 9
Termination-Cause	295								O		Enumerated	0	1	0	Sent in CCR. Indicates the reason for session termination. Termination-Cause AVP is mandatory in both Cancel (Cancel-event) and Commit (Terminate event). - The value of Termination-Cause AVP in both cases is "DIAMETER_LOGOUT (1)".
Content-Description	1102	11580							O		UTF8String (max size 64)	1	1	0	This attribute will hold the purchase description field.

AVP Name	AVP Code	Vendor ID	Used in								Value Type	AVP Flags			Description / Comments
			CER	CEA	DWR	DWA	DPR	DPA	CCR	CCA		V	M	P	
Vendor-ID	266	-	M	M							Unsigned32	0	1	0	Contains the IANA “SMI Network Management Private Enterprise Codes” ASSIGNNO] value assigned to the vendor of the Diameter application. In combination with the Supported-Vendor-Id AVP (Section 5.3.6), this MAY be used in order to know which vendor specific attributes may be sent to the peer. A Vendor-Id value of zero in the CER or CEA messages is reserved and indicates that this field is ignored.
Product-Name	269	-	M	M							UTF8String	0	1	0	Vendor-assigned name for the product

AVP Name	AVP Code	Vendor ID	Used in								Value Type	AVP Flags			Description / Comments
			CER	CEA	DWR	DWA	DPR	DPA	CCR	CCA		V	M	P	
Partner-ID	1103	11580							M		UTF8String (max size 32)	1	1	0	This attribute will hold the unique transaction id and this attribute will be stored in the ape1_rated_event table under L9_PARTNER_ID field. This attribute will enable to tie between a charge and refund events. In case this AVP is missing from the request, event will be rejected.
Purchase-Category-Code	1104	11580							M		UTF8String (max size 128)	1	1	0	This field together with Application_Type AVP will hold “Charge_Code_Description”.
Application-Type	1105	11580							M		UTF8String (max size 64)	1	1	0	This field together with Purchase_Category_Code AVP will hold “Charge_Code_Description”.
Adjustment-Reason-Code	1106	11580							C		UTF8String (max size 64)	1	1	0	This field is mandatory for CCR Refund events.

Document Release Information

Software Version	Editor	Edited Date	Comments	Sent to site	Approved By	Doc Ver.
	Ori Riechman	July 3, 2013				
	Ori Riechman	July 16, 2013	Adding 3 AVP’s: Purchase-Category-Code, Application-Type and Adjustment-Reason-Code			
	Sigal Chen	July 23, 2013	Updated with last comments on IDD.			
	Ori Riechman	August 13, 2013	Updated with one more assumption based on agreement between U.S. Cellular and Aepona.			

Soft-ware Version	Editor	Edited Date	Comments	Sent to site	Approved By	Doc Ver.
	Sigal Chen	August 18, 2013	Add assumption regarding DRA. Remove the assumption regarding Support GY interface for third parties			