Oracle® Communications Convergent Charging Controller

Diameter Control Driver Compliance Protocol Implementation Conformance Statement

Release 6.0

May 2016

ORACLE®

Copyright

Contents

About This Document

Scope

The purpose of this document is to describe the Convergent Charging Controller implementation of the DIAMETER protocol for the purposes of real-time charging.

Audience

This guide is intended for use by software engineers and testers that need a description of the SCP<->BE messages used by the DCD that is more detailed than that provided by the SRS and technical guide.

It is assumed that readers are familiar with CCS and the DIAMETER RFCs.

Related Documents

The following documents are related to this document:

- 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 V6.3.0 (2005-06) - 3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; Telecommunication management; Charging management; Diameter charging applications (Release 6)

Document Conventions

Typographical Conventions

The following terms and typographical conventions are used in the Oracle Communications Convergent Charging Controller 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 Driver (DCD) compliance limitations.

In this chapter

This chapter contains the following topics.

DCD Overview

Introduction

The Diameter Charging Driver (DCD) is an interface used by CCS to allow communication of billing requests from an SLC to a billing platform using the DIAMETER protocol. The DIAMETER base protocol is defined by RFC 3588, and extended to include real-time credit-control messages by RFC 4006.

The DCD (and thus this document) only covers the use of CCS as a DIAMETER client. For information about CCS acting as a DIAMETER server, see the Diameter Control Agent (DCA) documentation.

The DCD client runs on the SLC SLEE, taking requests from the billing actions of slee_acs and forwards them to the billing engine. It maintains the connections to the billing engines (or, if configured, DIAMETER proxies).

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 DCD.

They 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.
- Sub-sessions are not supported.

Chapter 2

Diameter Message Encoding

Overview

Introduction

This chapter details the Diameter Charging Driver (DCD) message encoding.

In this chapter

This chapter contains the following topics.

Diameter Message Encoding

Introduction

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

Diameter Headers

The header of Diameter messages sent by DCD 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	as per RFC 3588
End-to-end identifier	Unsigned32; 4 bytes	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 AVPCode 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 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 16247 for eServ specific AVPs.
Data		As specified by the AVP code and length.

AVP Data Types

The DCD can send and receive the all basic and derived data types mentioned in RFC 3588, with the exception of Float32 and Float64 which are not used by CCS.

Where the data types are used, they are encoded in complete compliance with RFC 3588 and RFC 2279.

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

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 DCD client will both initiate and receive connections in accordance with RFC 3588 or Diameter Base Protocol Draft 8. However, the DCD 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. The client will perform elections as specified in RFC 3588. 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 DCD will send both CER and CEA messages, as instructed by RFC 3588. Alternatively Diameter Base Protocol Draft 8 compliant CER and CEA messages may be exchanged if so configured.

The content of the individual fields is as follows:

Field	AVP Code	Data Type	Comment
Origin-Host	264	DiameterIdentity	Set from configuration.
Origin-Realm	296	DiameterIdentity	Set from configuration.
Host-IP-Address	257	Address (RFC 3588) OR IPAddress (Draft 8)	Set from configuration.
Vendor-ID	266	Unsigned32	Set from configuration (eServ vendor ID is 16247)
Product-Name	269	UTF8String	Set from configuration
Origin-State-Id	278	Unsigned32	Can be set from configuration. Due to the multiple process nature of slee_acs, this should not be set, and this AVP will then not be included.
Supported-Vendor-Id	265	Unsigned32	Not included.
Auth-Application-Id	258	Unsigned32	Set from configuration.
Inband-Security-Id	299	Unsigned32	Set to 0 (NO_INBAND_SECURITY). Not included if Draft 8 compliance is enabled.
Acct-Application-Id	259	Unsigned32	Set from configuration. If not set, then not included.
Vendor-Specific-Application-Id	260	Grouped	Set from configuration. If not set, then not included.
Firmware-Revision	267	Unsigned32	Not included.
Result-Code	268	Unsigned32	Set as per RFC 3588 or Diameter Base Protocol Draft 8 if configured as such.
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

The DCD will send and respond to DWR message as instructed by RFC 3588.

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.
Origin-Realm	296	DiameterIdentity	Set from configuration.
Origin-State-Id	278	Unsigned32	Can be set from configuration. Due to the multiple process nature of slee_acs, this should not be set,

Field	AVP Code	Data Type	Comment
			and this AVP will then not be included.
Result-Code	268	Unsigned32	Set as per RFC 3588 or Diameter Base Protocol Draft 8 if configured as such.
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 receiving a DPR message, the client should never again attempt to reconnect the connection.

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 DCD 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.

Failover

Copy of Failover

The DCD supports several failover models, depending on the logical distribution of subscriber accounts across billing engines. CCS allows a subscriber account (CCS "Wallet") to be in multiple realms (although only one realm is recommended). The DCD will also allow several peer connections within a single realm.

The selection of which realm when one account is in multiple realms can be via a proportional distribution, or a round-robin selection model. The selection of which peer for a realm can be via a proportional distribution, or a round-robin selection model.

If a request fails to get a response, retransmitting to another peer within the realm will be tried a configurable number of times. If this is exhausted, and the request is an INITIAL or EVENT request, then resubmitting to another realm will be tried, if one is available. Failover across a realm is only permitted once for each request.

A change in a received Origin-State-Id will never initiate failover of sessions.

Session failover behavior is only performed if permitted by the most recent CC-Session-Failover AVP received in the session. The initial behavior (until overridden by the CC-Session-Failover AVP) is configurable.

In addition to the behavior above, it is possible to group together peers into sets where only one of the peer will be used at any time. The currently active peer of a group will be the only connection opened, and will remain active until the connection fails. At that point the next peer will become active, and remain active until it fails.

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.

Introduction

Introduction

The DCD can send both session and event based credit control requests. The type used is determined by the CCS request made of the DCD , and the CCS configuration.

To enable the maximum interoperability with billing engines, the structure of the CCRs that the client sends (and the CCAs that it expects to receive) is highly configurable. This configuration is per CCS action type requested, so not all CCRs need have the same structure.

Non-configurable AVPs

AVP List descriptions

The first set of AVPs in any CCR or CCA are not determined by the structure config, but rather the current CCS state and the action requested.

These AVPs are:

AVP Name	AVP Code	Data Type	Comment
Session-Id	263	UTF8String	Format: *DiameterIdentity*;*Unix time_t*;*SLEE_CallID* where the time is the time of the first request.
Origin-Host	264	DiameterIdentity	Set from configuration
Origin-Realm	296	DiameterIdentity	Set from configuration
Destination-Realm	283	DiameterIdentity	From CCS configuration
Auth-Application-Id	258	Unsigned32	Set from configuration
Service-Context-Id	461	UTF8String	Set from configuration
CC-Request-Type	416	Enumerated	All 4 values are used.

AVP Name	AVP Code	Data Type	Comment
CC-Request-Number	415	Unsigned32	Starts at 0, and consecutively incremented by each message of the session.
Destination-Host	293	DiameterIdentity	Set from configuration
User-Name	1	UTF8String	Not included in CCRs
CC-Sub-Session-Id	419	Unsigned64	Not included in CCRs
Acct-Multi-Session-Id	50	UTF8String	Not included in CCRs
Origin-State-Id	278	Unsigned32	Can be set from configuration. Due to the multiple process nature of slee_acs, this should not be set, and this AVP will then not be included.
Event-Timestamp	55	Time	The time of the request construction.

Structure Configurable AVPs

Structure configurable AVPs

The AVPs following the Event-Timestamp are massively configurable. The configuration defines a tree structure of which AVPs to include, which CCS variables they represent, and how they are formatted. There is separate configuration for each CCS action involved. The CCS actions for which CCRs can be configured are:

- ConfirmNamedEventReservation
- ConfirmTimeReservation
- DirectNamedEvent
- DirectTimeCharge
- ExtendTimeReservation
- GetNamedEventRates
- InitialTimeReservation
- NamedEventReservation
- RevokeNamedEventReservation
- RevokeTimeReservation
- WalletInfo
- CreateEDR
- WalletRecharge

ccsConcepts

To match an AVP to a variable in CCS, the DCD has "ccsConcepts". These can be a specific parameter of the CCS action, a general CCS variable, some of the call's context, or even an ACS profile value.

The DCD provides functionality to scale values by a factor, and also allows a mapping of one set of integers to another while reading/writing to CCS concepts. The specific formatting of the value field is quite configurable, see the *Diameter Charging Driver Technical Guide* for formatting details.

Note: All concepts are available to be set from Responses. The availability only refers to requests.

The complete list of CCS concepts that are available to CCRs/CCAs is:

Concept Label	Availability	Comment
acsCallID	always	The call ID from the SLEE
acsProductType	always	The ACS product type ID
acsServiceProvider	always	The ACS service provider ID
acsSubscriber	always	The CCS subscriber ID
acsSubscriberReference	always	The CCS subscriber number (ie their MSISDN)
acsWallet	always	The CCS wallet ID (BE_WALLET.ID)
acsWalletReference	always	The CCS wallet Reference (the Billing System's reference to the wallet)
acsWalletType	always	The CCS wallet type. (CCS_WALLET_TYPE.ID)
acsChargingDomain	always	The destined billing domain (logical collection of wallets) for this request.
acsTariffCode	After an initial reservation.	Tariff Code string returned in the Initial Reservation Response (if present).
acsUnnormalisedCalledNumber	always	The called party number digits from the IDP, without any attempt at normalization.
acsProfile	always	An ACS profile buffer from the Call plan. If the buffer is not set, then the AVP is not included.
discountMaxCharge	After a setDiscount	Present after a setDiscount node or a response that has the discountMaxCharge present.
discountPeriod	After a setDiscount	Present after a setDiscount node or a response that has the discountPeriod present.
tariffPlan	After a setTariffPlan	Integer representing the tariff Plan.
tariffCugName	After a setTariffPlan	The Closed User Group Name.
cascade	After a setCascade Override.	Also can be set by previous responses. The integer ID of the cascade to apply.
chargeInfoBalanceType	After a chargeInfo response	The CCS ID of the balance Type for the current balance of the Charge structure.
chargeInfoBalanceUnitType	After a chargeInfo response	The CCS ID of the balance Unit for the current balance of the Charge structure. This is not necessary for a ChargeInfo in a response, it can be derived from the balance type.
chargeInfoBalanceSystemValue	After a chargeInfo response	The balance Unit for the current item of the Charge structure. This is in units of the system currency.
chargeInfoBalanceUserValue	After a chargeInfo response	The balance Unit for the current item of the Charge structure. This is in units of the user's currency. Note that the system currency value is mandatory, while this entry is optional.
walletInfoBalanceUnitType	After a walletInfo response	The CCS ID of the balance Unit for the current balance item of the Wallet structure. This is not necessary for a balance in a response, it can be derived from the balance type.

Concept Label	Availability	Comment
walletInfoBalanceType	After a walletInfo response	The CCS ID of the balance Type for the current balance of the Wallet structure.
walletInfoBalanceSystemValue	After a walletInfo response	The balance Unit for the current item of the balance structure. This is in units of the system currency.
walletInfoBalanceUserValue	After a walletInfo response	The balance Unit for the current item of the balance structure. This is in units of the user's currency. Note that the system currency value is mandatory, while this entry is optional.
walletInfoBalanceExpiry	After a walletInfo response	The expiry date (in time_t) of the current balance. The DCD handles conversion from time_t to DIAMETER times.
walletInfoBalanceMaxCredit	After a walletInfo response	The maximum amount of credit allowed for this subscriber.
walletInfoBalanceLimitType	After a walletInfo response	The balances limit type: An integer representing one of: limitedPostpaid, postpaid, prepaid, singleUsePrepaid
walletInfoBalanceExponent	After a walletInfo response	An exponent to apply to the balance system value.
walletInfoExpiry	After a walletInfo response	The expiry date (in time_t) of the wallet. The DCD handles conversion from time_t to DIAMETER times.
walletInfoState	After a walletInfo response	A single character representing the wallet's state. One of: 'A' = Active, 'D' = Dormant, 'F' = Frozen, 'P' = Pre-Use, 'S' = Suspended, 'T' = Terminated. Note that conversion to different representations is possible.
walletInfoLastAccess	After a walletInfo response	time_t of the wallet's last access. The DCD handles conversion from time_t to DIAMETER times.
walletInfoActivationDate	After a walletInfo response	time_t of the wallet's activation date. The DCD handles conversion from time_t to DIAMETER times.
walletInfoMaxConcurrent	After a walletInfo response	The maximum number of concurrent users allowed for this wallet.
walletInfoSystemCurrency	After a walletInfo response	The system currency.
walletInfoUserCurrency	After a walletInfo response	The CCS_ACCT.CURRENCY value for this wallet.
cli	After a DirectTimeCharge or InitialTimeReservation	
destinationNumber	After a	

Concept Label	Availability	Comment
	DirectTimeCharge or InitialTimeReservation	
callerTimeZone	After a DirectTimeCharge or InitialTimeReservation	
expectedReservationTotal	InitialTimeReservation and ExtendTimeReservation	
expectedReservationDelta	InitialTimeReservation and ExtendTimeReservation	
callDurationTotal	Any Time Charging Action	
callDurationDelta	Any Time Charging Action	
lowCreditBuffer	After set from a response	Usually part of an initialTimeReservationResponse. Number of seconds from the end of the last good reservation period until a low credit beep should be played
freeCallDisposition	After set from a response	Usually part of an initialTimeReservationResponse.
singleReservation	After set from a response	Usually part of an initialTimeReservationResponse.
initialLowBalanceIndicator	After set from a response	Usually part of an initialTimeReservationResponse. If present and non zero the indicated pre call warning announcement should be played to the subscriber.
initialLowBalanceAnnouncement	After set from a response	Usually part of an initialTimeReservationResponse. The Announcement ID of the announcement to play.
maxCallLength	After set from a response	Usually part of an initialTimeReservationResponse.
retrieveLCRNumbers	After set from a response	Usually part of an initialTimeReservationResponse.
validityPeriod	After set from a response	
reservedLengthTotal	After set from a response	Usually part of an xxxTimeReservationResponse.
reservedLengthDelta	After set from a response	Usually part of an xxxTimeReservationResponse.
timeReservationStatus	After set from a response	Usually part of an xxxTimeReservationResponse.

Concept Label	Availability	Comment
maxSeconds	After set from a response	Session Time left. Usually part of an xxxTimeReservationResponse.
callAnsweredTime	ConfirmTimeReservation	
confirmTimeReservationStatus	After set from a response	Usually part of an confirmTimeReservationResponse.
revokeTimeReservationStatus	After set from a response	Usually part of an revokeTimeReservationResponse.
eventClass	NamedEvent Actions	A string representing the CCS event Class.
eventName	NamedEvent Actions	A string of the CCS event name.
eventType	NamedEvent Actions	An integer representing the type of CCS named event.
minUnitsRequested	NamedEvent Actions	
maxUnitsRequested	NamedEvent Actions	
discountPercentage	After a setDiscount or DirectNamed Event or NamedEvent Reservation	Present after a setDiscount node or a response that has the discountPeriod present.
extraInformation		Usually call information for adding to Billing EDRs. Contents varies for each action.
ignoreBalanceLimit	DirectNamed Event, DirectTimeCharge, NamedEvent Reservation	
numUnitsGranted	After set from a response	
numUnitsUsed	ConfirmNamedEventReservation	
ratingPrecision	InitialTimeReservation	Integer representing one of seconds, tenths-of-a-second or hundredths-of-a-second
callDate	DirectTimeCharge	
balanceUnitFilter	WalletInfo	Request the billing engine to only return balances of this unit.
balanceTypeFilter	WalletInfo	Request the billing engine to only return balances of this type.
setFreeform	always	The next AVP of concept "freeform" will instead use/update the concept indexed by the value of this AVP.
freeform	always	Uses/updates the concept previously defined by setFreeform.

Concept Label	Availability	Comment
voucherInfoVoucher	After a VoucherRedeem response	The ID of the voucher that was redeemed (for example in the Voucher Management system). Not to be confused with voucher number as known to customer – that will normally be available as a profile variable set or captured in the control plan.
voucherInfoWalletExpiryExtension	After a VoucherRedeem response	How much of an extension to apply to the wallet (expressed in units of time given by VoucherInfoWalletExpiryExtensionType).
voucherInfoWalletExpiryExtensionType	After a VoucherRedeem response	Specifies the unit of time referred to by the value in voucherInfoWalletExpiryExtension. Hours (0) or Months (1).
voucherInfoWalletExpiryExtensionPolicy	After a VoucherRedeem response	An enumeration that shows how the wallet expiry is to be updated by a voucher redemption: best = 0 extend extendFromToday override dontChange
voucherInfoBalanceType	After a VoucherRedeem response	This is the ID of the CCS balance type of the current VoucherValue 'slot' in the VoucherInfo structure, obtained from the last voucher redemption.
voucherInfoValue	After a VoucherRedeem response	This is the monetary value from the current VoucherValue 'slot' in the VoucherInfo structure, obtained from the last voucher redemption.
voucherInfoBalanceExpiryExtension	After a VoucherRedeem response	How much of an extension to apply to the wallet balance referred to by the current VoucherValue 'slot' in the VoucherInfo structure (expressed in units of time given by VoucherInfoBalanceExpiryExtensionType).
voucherInfoBalanceExpiryExtensionType	After a VoucherRedeem response	Specifies the unit of time referred to by the voucherInfoBalanceExpiryExtension value in the current VoucherValue 'slot' of the VoucherInfo structure. Hours (0) or Months (1).
voucherInfoWalletExpiryExtensionPolicy	After a VoucherRedeem response	An enumeration that shows how the current voucher value balance expiry is to be updated by a voucher redemption: • best = 0 • extend • extendFromToday • override • dontChange
voucherInfoNewBucket	After a VoucherRedeem response	States whether the money amount from the current VoucherValue 'slot' of the VoucherInfo structure should be stored in a new bucket ir added to an existing one.
voucherInfoMissingBalancePolicy	After a VoucherRedeem response	States how to handle the lack of any existing balance of this type in the wallet: • allow = 0,

Concept Label	Availability	Comment
		• fail, • ignoreBalance
voucherInfoReplaceBalance	After a VoucherRedeem response	Specifies whether or not the current voucher value replaces any existing balance of that type in the wallet.
scpAction	Set after a response	For handling CCAs only. May be set based on an enumerated AVP to indicate combinations of: • supervise (1) • release (2) • sendMessage (3) • playAnnouncement (4) • superviseWithoutControlling (5) Where such an enumerated AVP exists, it may appear more than once with different values. This will result in DCD context values (booleans) being set according to each of the above names. These boolean values may be copied back into profile locations using the ContextCopy section in **eserv.config**, for the purposes of branching within control plans. See *Diameter Charging Driver Technical Guide* for further details.

Balance structure limitations

There is a small limitation to the flexibility of AVP structures to define balances. Multiple balances are allowed for charge, wallet and voucher information, but all properties of the balance must be grouped together.

Basically, CCS must parse all information about a particular balance before parsing a different balance. So two grouped AVPs of balance value and balance type is fine, but a grouped AVP of all balance values and another grouped AVP of all balance types cannot be parsed by CCS.

This approach was established for the BalanceInfo transaction, and has been followed for the management of VoucherInfo structures, which define the proceeds from a voucher redemption. The information comprises a set of wallet information, and a recurring set of VoucherValue structures that each identify how to update a single wallet balance type. Accordingly CCS must parse all information about a particular voucher value before parsing fields from a different one.

Configuring different types of DirectNamedEvent

This CCS action allows for highly configurable types of billing even to be triggered by the SLC. It is obviously desirable to be able to configure different AVPs for different types of DirectNamedEvent. The feature node that is used to emit a DirectNamedEvent is told what type of event it should trigger, categorized by event class (a kind of subject matter grouping) and event name. Both aspects are fully configurable in the CCS screens.

To make the DNE action more useful, its DCD implementation looks first for a request AVP named DirectNamedEventRequest-*xxx*, where *xxx* is the configured name of the CCS named event.

- If one is found, it is used to generate the outgoing AVP.
- If none is found, the code then falls back to the more general "DirectNamedEventRequest".

A similar logic applies to the processing of responses: that is, DCD looks first for DirectNamedEventResponse-*xxx*, then DirectNamedEventResponse.

Result Code Mapping

Introduction

The mapping of DIAMETER result codes to CCS node responses is not configurable, and depends on the CCS Action involved.

Initial time reservation

This table lists the mapped responses for initial time reservation.

DIAMETER Result Code	InitialTimeReservationResponse
DIAMETER_SUCCESS	success
DIAMETER_LIMITED_SUCCESS	success
DIAMETER_UNABLE_TO_DELIVER	declineCommunicationError
DIAMETER_CREDIT_LIMIT_REACHED	declineInsufficientFunds
DIAMETER_USER_UNKNOWN	declineUnknownWallet
DIAMETER_END_USER_SERVICE_DENIED	declineCallRestricted
DIAMETER_CREDIT_CONTROL_NOT_APPLICABLE	freecall
DIAMETER_RATING_FAILED	declineSystemError
all others	declineSystemError

Extend time reservation

This table lists the mapped responses for extend time reservation.

DIAMETER Result Code	InitialTimeReservationResponse
DIAMETER_SUCCESS	success
DIAMETER_LIMITED_SUCCESS	success
DIAMETER_UNABLE_TO_DELIVER	declineCommunicationError
DIAMETER_CREDIT_LIMIT_REACHED	declineInsufficientFunds
DIAMETER_USER_UNKNOWN	declineUnknownWallet
DIAMETER_END_USER_SERVICE_DENIED	declineSystemError
DIAMETER_CREDIT_CONTROL_NOT_APPLICABLE	freecall
DIAMETER_RATING_FAILED	declineSystemError
all others	declineSystemError

Confirm time reservation

This table lists the mapped responses for confirm time reservation.

DIAMETER Result Code	InitialTimeReservationResponse
DIAMETER_SUCCESS	success
DIAMETER_LIMITED_SUCCESS	success
DIAMETER_UNABLE_TO_DELIVER	declineCommunicationError
DIAMETER_CREDIT_LIMIT_REACHED	declineInsufficientFunds
DIAMETER_END_USER_SERVICE_DENIED	declineWalletDisabled
all others	declineSystemError

Revoke time reservation

This table lists the mapped responses for revoke time reservation.

DIAMETER Result Code	InitialTimeReservationResponse
DIAMETER_SUCCESS	success
DIAMETER_LIMITED_SUCCESS	success
DIAMETER_UNABLE_TO_DELIVER	declineCommunicationError
all others	declineSystemError

Named event reservation

This table lists the mapped responses for named event reservation.

DIAMETER Result Code	InitialTimeReservationResponse
DIAMETER_SUCCESS	success
DIAMETER_CREDIT_CONTROL_NOT_APPLICABLE	declineSystemError
DIAMETER_CREDIT_LIMIT_REACHED	declineInsufficientFunds
DIAMETER_END_USER_SERVICE_DENIED	declineNotAllowed
all others	declineSystemError

Confirm named event reservation

This table lists the mapped responses for confirm named event reservation.

DIAMETER Result Code	InitialTimeReservationResponse
DIAMETER_SUCCESS	success
all others	declineSystemError

Revoke named event reservation

This table lists the mapped responses for revoke named event reservation.

DIAMETER Result Code	InitialTimeReservationResponse
DIAMETER_SUCCESS	success
all others	failed

Direct named event

This table lists the mapped responses for direct named event.

DIAMETER Result Code	InitialTimeReservationResponse
DIAMETER_SUCCESS	success
DIAMETER_CREDIT_LIMIT_REACHED	declineInsufficientFunds
DIAMETER_END_USER_SERVICE_DENIED	declineNotAllowed
all others	declineSystemError

Direct time charge

This table lists the mapped responses for direct time charge.

DIAMETER Result Code	InitialTimeReservationResponse
DIAMETER_SUCCESS	success
all others	declineSystemError

Get named event rates

This table lists the mapped responses for get named event rates.

DIAMETER Result Code	InitialTimeReservationResponse
DIAMETER_SUCCESS	success
DIAMETER_CREDIT_CONTROL_NOT_APPLICABLE	success
DIAMETER_RATING_FAILED	rateNotAvailable
DIAMETER_END_USER_SERVICE_DENIED	declineNotAllowed
all others	declineSystemError

Wallet Info

This table lists the mapped responses for wallet info.

DIAMETER Result Code	InitialTimeReservationResponse
DIAMETER_SUCCESS	success
all others	failed

Create EDR

This table lists the mapped responses for create edr.

DIAMETER Result Code	InitialTimeReservationResponse
DIAMETER_SUCCESS	success
all others	failed

Wallet recharge

This table lists the mapped responses for wallet recharge.

DIAMETER Result Code	InitialTimeReservationResponse
DIAMETER_SUCCESS	success
all others	failed

Chapter 5

Compliance Tables

Overview

Introduction

This chapter identifies the level of compliance to RFC 3588 and RFC 4006.

In this chapter

This chapter contains the following topics.

Compliance to RFC 3588

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	
2.5	Connection Management	Fully compliant	Connection is established and added to pool for use by Diameter sessions. Number of connections per Charging realm is configurable.
2.6	Peers	N/A	A list of static peers are configured using the SMS platform.
2.7	Realm Based Routing	Not Supported	No.

Section	Section Heading	Compliance Level	Comment
2.8	Role of agents	N/A	Convergent Charging Controller offer a Diameter client only.
2.9	End-to-end security	Partial compliance	Only 'Never use end-to-end security' is supported
2.10	Path Authentication	N/A	The list of valid paths are configured using the SMS management node.

Headers - Section 3

This table lists the compliances for section 3.

Section	Section Heading	Compliance Level	Comment
3	Headers	Fully compliant	
3.1	Command Codes	Partially compliant	CER, CEA, DWR, DWA, DPR, DPA supported. Each message may be enabled independently to allow support for various applications/peers.
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	
4.3	Derived AVP Data Formats	Fully compliant	No Convergent Charging Controller 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 Peers - Section 5

This table lists the compliances for section 6.

Section	Section Heading	Compliance Level	Comment
5	Diameter Peers	N/A	
5.1	Peer Connections	Fully compliant	Multiple peers per realm are supported – where 2 peers are defined primary/secondary is assumed. For multiple peers load sharing is based on round-robin approach.
5.2	Peer discovery	Non compliant	The list of valid paths are configured using the SMS management node

Section	Section Heading	Compliance Level	Comment
5.3	Capability Exchange	Fully compliant	
5.4	Disconnecting Peer Connections	Fully compliant	Supported non-persistently per client interface.
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 5.

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	
6.9	Acct-Application-Id AVP	Fully compliant	
6.10	Inband-Security ID AVP	Fully compliant	
6.11	Vendor Specific Application-Id AVP	Fully compliant	No Convergent Charging Controller specific AVPs are defined today.
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	

Section	Section Heading	Compliance Level	Comment
7.5	Failed-AVP AVP	Fully compliant	This information may be included in the ACSapplication EDR for further debugging.
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 compliant	
8.2	Accounting Session State Machine	Partially compliant	Implements only the client side of the state machine.
8.3	Server-Initiated Re-Auth	Non compliant	
8.4	Session Termination	Fully compliant	When Convergent Charging Controller receive this message from an application all session in progress will released and this information will be included in EDRs produced.
8.5	Abort Session	Fully compliant	When Convergent Charging Controller receive this message from an application all session in progress will released and this information will be included in EDRs produced.
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	
8.16	Origin State ID AVP	Fully compliant	
8.17	Session Binding AVP	Non compliant	
8.18	Session-Server-	Non compliant	

Section	Section Heading	Compliance Level	Comment
	Failover AVP		
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	Fully compliant	
9.2	Protocol Messages	Partially compliant	No IP compression is supported at this time. Support for negotiation is however provided.
9.3	Application document requirements	Fully compliant	See Credit Control Application defined in RFC 4006
9.4	Fault Resilience	Fully compliant	Please note that only the client side is implemented.
9.5	Accounting Records	Fully compliant	
9.6	Correlation of Accounting Records	Fully compliant	
9.7	Accounting Command-Codes	Fully compliant	
9.8	Accounting AVPs	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	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	

Section	Section Heading	Compliance Level	Comment
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 Convergent Charging Controller 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	Only statically configured peers are supported by Convergent Charging Controller.

Security Considerations - Section 13

This table lists the compliances for section 13.

Section	Section Heading	Compliance Level	Comment
13	Security Considerations	Fully compliant	

Compliance to Diameter Base Protocol Draft 8

Introduction

This section highlights compliance for the Diameter Base Protocol Draft 8 (refered to below as Draft 8), where there is variance for RFC 3588. Compliance is as per that for RFC 3588, unless stated otherwise.

Note: The use of Draft 8 is facilitated for compatibility with Ericsson SCAP. Stated levels of compliance only apply to the use of Draft 8, with SCAP.

Protocol Overview - Section 2

This table lists the compliances for section 2.

Section	RFC3588	Section Heading	Compliance Level	Comment
2.4	2.4	Application Identification	Not compliant	Not used for SCAP
N/A	2.9	End-to-end security	N/A	Not supported for Draft 8.

Headers - Section 3

This table lists the compliances for section 3.

Section	RFC3588	Section Heading	Compliance Level	Comment
3.0	3.0	Headers	Fully compliant	Note **T** (retransmit) flag is not supported in Draft 8.
3.2	3.2	ABNF Specification	Partial compliance. Errors assumed in Draft 8.	In Section 3.2 of Draft 8, the Command Code ABNF specification appears to conflict with section 3.0, with respect to the position of Vendor-Id. This is assumed to be an error in Draft 8. Similarly the definition for "qual" in section 3.2 appears to be ambiguous in Draft 8, but is clearer in RFC 3588.

Diameter AVPs - Section 4

This table lists the compliances for section 4.

Section	RFC3588	Section Heading	Compliance Level	Comment
4.4	4.3	Derived AVP Data Formats	Fully compliant	IPAddress in Draft 8 is replaced by Address in RFC 3588. Address represents the address type, which contains an Address Family. This is as opposed to Draft 8 which determines the type of address based on the AVP length. The Draft 8 definition for Diameter-Identity conflicts with RFC 3588, which has both Diameter-Identity (sometimes referred to as DiameterIdentity) and DiameterURI. Effectively the Draft 8 Diameter-Identity appears to match DiameterURI in RFC 3588. This is specified as a UTF8 String.
4.6	4.5	Diameter Base Protocol AVPs	Partially compliant	Acct-Application-Id and Auth-Application-Id Draft 8, are specified Integer32 rather than Unsigned32. This is assumed to be a mistake as this conflicts with other sections within Draft 8 (that is, Section 6).

Section	RFC3588	Section Heading	Compliance Level	Comment
				Destination-Realm and Origin-Realm, are specified as type UTF8String in Draft 8. However in RFC 3588 they are specified as type DiameterIdentity. Host-IP-Address is missing from the list of Diameter Base Protocol AVPs for Draft 8. This is assumed to be an error as they are present in RFC 3588. The AVP header flags for the Product-Name AVP differ. For Error-Message (281) OctetString is used for Draft 8, instead of UTF8String. For Error-Reporting-Host (294), UTF8String is used instead vs. DiameterIdentity

Diameter Peers - Section 5

This table lists the compliances for section 6.

Section	RFC3588	Section Heading	Compliance Level	Comment
5.1	5.1	Peer Connections	Partially compliant.	It is assumed that the "not invoke" versus "invoked" difference in section 5.1 is a correction to an existing mistake.
5.3.1	5.3.1	Capabilities Exchange - Request	Fully compliant	Inband-Security-Id (AVP code 299), is not supported by Draft 8. Similarly DIAMETER_NO_COMMON_SECURITY, is not supported in Draft 8 as a Result-Code.
5.3.2	5.3.2	Capabilities Exchange - Answer	Partially compliant	In Draft 8 Vendor-Specific-Application-Id, is shown as NOT grouped in CEA (but it is in CER). This lack of grouping in CEA is assumed to be a mistake.
5.3.5	5.3.5	Host-IP-Address AVP	Fully compliant	Host-IP-Address (257), is specified as an IPAddress type in Draft 8, but an Address in RFC 3588.

Section	RFC3588	Section Heading	Compliance Level	Comment
5.4.3	5.4.3	Disconnect-Cause AVP	Partially compliant	Disconnect-Cause AVP, only features the value ELECTION_LOST in Draft 8. In RFC 3588, this is handled via the Result-Code AVP instead. As per SCAP Programmer's Guide, "CCN acts as a Diameter SCAP Server and does not initiate connections". Hence this is not implemented.
5.6	5.6	Peer State Machine	Partially compliant	There is no I-snd-DWR in section 5.6 of Draft 3588. This is not deemed to be an issue as R-snd-DWR from the peer will ensure connection is kept alive.

Diameter Message Processing - Section 6

This table lists the compliances for section 5.

Section	RFC3588	Section Heading	Compliance Level	Comment
6.6	6.6	Destination-Realm AVP	Fully compliant	Destination-Realm and Origin-Realm, are specified as type UTF8String in Draft 8. However in RFC 3588 they are specified as type DiameterIdentity.

Error Handling - Section 7

This table lists the compliances for section 7.

Section	RFC3588	Section Heading	Compliance Level	Comment
7.1.3	7.1.3	Protocol Errors	Partially compliant	For Draft 8 Result-Codes 5011 through to 5017, subtract 1 to get the equivalent in RFC 3588, that is, DIAMETER_NO_COMMON_APPLICATION is 5011 for Draft 8 and 5010 for RFC 3588. In RFC 3588, a Result-Code of 5017 is DIAMETER_NO_COMMON_SECURITY. DIAMETER_UNSUPPORTED_TRANSFORM is not present

Section	RFC3588	Section Heading	Compliance Level	Comment
				in RFC 3588, and is unused by DCD However given that a CMS-Data AVP is not expected, this is not implemented.

Diameter User Sessions - Section 8

This table lists the compliances for section 8.

Section	RFC3588	Section Heading	Compliance Level	Comment
8.8	8.8	Session-Id AVP	Fully compliant	**Note:** According to section 8.8 Draft 8, Session-Id must start with DiameterIdentity. This is not enforced, but may be specified appropriately via configuration.

Accounting - Section 9

This table lists the compliances for section 9.

Section	RFC3588	Section Heading	Compliance Level	Comment
9.7 and 9.8	9.7 and 9.8	Accounting-Request	Partially compliant	The SCAP version of the ACR message is assumed to take precedence to Draft 8. **Note:** The Draft 8 Accounting-Interim-Interval (AVP Code 482), is replaced by Acct-Interim-Interval (85) in RFC 3588. If required this can be configured, according to a profile or a static value. However this optional is generally not used. A number of (optional) AVPs are changed between Draft 8, RFC 3588 and SCAP Programmer's Guide. Due to the configurable nature of DCD this should not cause too many issues. That is: Accounting-Radius-Session-Id Draft 8 is not in RFC 3588 but is in SCAP Programmer's Guide. This is replaced by Acct-Session-Id in RFC 3588.

AVP Occurrence Table - Section 10

This table lists the compliances for section 10.

Section	RFC3588	Section Heading	Compliance Level	Comment
10.2	10.2	Accounting AVP Table	Partially compliant	In addition to above comments regarding Accounting messages, the following should be noted: Termination-Cause is shown in Section 10.2 RFC 3588, but is not specified in Draft 8 or SCAP Programmer's Guide, so it is assumed that this should not be sent.

IANA Considerations - Section 11

This table lists the compliances for section 11.

Section	RFC3588	Section Heading	Compliance Level	Comment
11.2.2	11.2.2	Command Flags	Partially compliant	Byte ordering is incorrect compared to other parts of the document and RFC 3588. It is assumed that the bits specified and byte order should be as per RFC 3588.

Compliance to RFC 4006

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	Non compliant	
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	Fully compliant	Please note that if this information is not present from the Billing Server no post credit expiration behavior may be defined.
5.7	Failure Procedures	Fully compliant	Please note that if this information is not present from the Billing Server normal Billing Failure Treatment may be

Section	Section Heading	Compliance Level	Comment
			applied inside the Convergent Charging Controller system.

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	The number of retries may be configured.

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	Client side only is implemented

Credit-Control AVPs - Section 8

This table lists the compliances for section 8.

Section	Section Heading	Compliance Level	Comment
8	Credit-Control AVPs		
8.1	CC-Correlation-ID AVP	Fully compliant	This field contains the unique identifier extracted from the session control protocol (that is, Call Reference from CAP). It is expected that this field be included in the BE EDR created
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	This parameter may be configured to allow/reject support for session failover
8.5	CC-Sub-Session-Id AVP	Non compliant	
8.6	Check-Balance-Result AVP	Fully compliant	
8.7	Cost-Information AVP	Fully compliant	Please note that current balance information may be requested via this

Section	Section Heading	Compliance Level	Comment
			AVP group where Balance Check is requested with the Service-Identifier value set to 'Information'
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	This value may be stored for SMS notification
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-Credit-Control AVP	Non compliant	Each session relates to only one network session
8.17	Granted-Service-Unit AVP	Fully compliant	
8.18	Requested-Service-Unit AVP	Fully compliant	Convergent Charging Controller implement Time, Money, Total Octets and CC-Service-Specific-Units only today
8.19	Used-Service-Unit ACP	Fully compliant	
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	Non compliant	
8.25	CC-Output-Octets ACP	Non 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	This AVP may contain the special value 'Information' if a balance query is to be performed – otherwise this value is configured to be the CCS Capability as configured on the SLC for this particular interaction. Examples include 'MO Voice', 'MT Voice', 'MO SMS', and the rest.
8.29	Rating-Group AVP	Fully compliant	
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	

Section	Section Heading	Compliance Level	Comment
8.33	Validity-Time AVP	Fully compliant	
8.34	Final-Unit-Indication AVP	Partially compliant	Only Final-Unit-Action of TERMINATE is supported.
8.35	Final-Unit-Action AVP	Partially compliant	Only Final-Unit-Action of TERMINATE is supported.
8.36	Restriction-Filter-Rule AVP	Non compliant	These rules are defined using the ACS Control Plan Editor.
8.37	Redirect-Server AVP	Non compliant	
8.38	Redirect-Address-Type AVP	Fully compliant	
8.39	Redirect-Server-Address AVP	Fully compliant	
8.40	Multiple-Services-Indicator AVP	Fully compliant	Please note that multiple services are not requested by the client
8.41	Requested-Action AVP	Fully compliant	
8.42	Service-Context-Id AVP	Fully compliant	
8.43	Service-Parameter-Info AVP	Fully compliant	This parameter is used to indicate supplementary rating information toward the BE. Please note that today only a single value is sent in this group. It is expected that the BE will use this value when determining the rate for the interaction.
8.44	Service-Parameter-Type AVP	Fully compliant	
8.45	Service-Parameter-Value AVP	Fully compliant	
8.46	Subscription-Id AVP	Fully compliant	
8.47	Subscription-Id-Type AVP	Fully compliant	E164 and SIP URI are used today
8.48	Subscription-Id-Data AVP	Fully compliant	
8.49	User-Equipment-Info AVP	Non compliant	
8.50	User-Equipment-Info-Type AVP	Non compliant	
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	

Section	Section Heading	Compliance Level	Comment
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	Fully 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	Non 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	Tx and Tcc timers are supported

Security Considerations - Section 14

This table lists the compliances for section 14.

Section	Section Heading	Compliance Level	Comment
14	Security Considerations	Fully compliant	
14.1	Direct Connection with	Non compliant	Statically configured peers are

Section	Section Heading	Compliance Level	Comment
	Redirect		supported by Convergent Charging Controller.

Compliance to Ericsson SCAP

Overview

This section highlights compliance for to sections 4.2 and 4.3 of the "Programmer's Guide - Service Charging Based on Diameter Charging Control Node 5".

Note: For SCAP the use of Diameter Base Protocol Draft 8 is required.

Compliance - Section 4

This table lists the compliances for section 1.

Section	Section Heading	Compliance Level	Comment
1	Introduction	N/A	

Glossary of Terms

AAA

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

ACS

Advanced Control Services configuration platform.

AVP

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

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.

CAP

CAMEL Application Part

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 (or Prepaid Charging) 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

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”.

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

IDP

INAP message: Initial DP (Initial Detection Point)

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.

MO

Mobile Originated

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

Peer

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

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.

SCP

Service Control Point. Also known as SLC.

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).

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

SMS

Depending on context, can be:

- Service Management System hardware platform
- Short Message Service
- Service Management System platform
- Convergent Charging Controller Service Management System application

SN

Service Number

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).

SSL

Secure Sockets Layer protocol

SSP

Service Switching Point

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.

Index

N

O

P

R

S

T

U

W