

CSCF Ro Interface

Call Session Control Function

INTERWORK DESCRIPTION

Copyright

© Ericsson AB 2013–2017. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



Contents

1	Introduction	1
2	Interface Overview	3
2.1	Interface Role	3
2.2	Services	3
2.3	Encapsulation and Addressing	4
3	Procedures	7
3.1	Error Handling	8
3.2	Usage Examples	8
4	Information Model	11
5	Formal Syntax	13
5.1	Message Contents for Online Charging	13
5.2	Attribute-Value Pairs	17
6	Security Considerations	53
6.1	IPsec Tunnel	53
7	Related Standards	55





1 Introduction

This document specifies the Diameter protocol used by Serving Call Session Control Function (S-CSCF) for online charging between the S-CSCF and a Charging System of the IMS. The 3GPP® defines this as the Ro interface between the Charging Trigger Function (CTF) and the Online Charging System (OCS).

This document explains the Charging requests sent by the S-CSCF to an OCS using the Diameter protocol as bearer for Charging messages. It also explains the Charging responses received by the S-CSCF from the OCS. Charging information is described in the document in terms of Attribute-Value Pairs (AVPs) as defined in the following specifications, with Ericsson-specific additions:

- [RFC 3588 Diameter Base Protocol](#)
- [RFC 4006 Diameter Credit-Control Application](#)
- [3GPP TS 32.299 v6.8.0 Diameter Charging Applications](#)





2 Interface Overview

The Ro interface is defined by 3GPP and is the reference point between a CTF and an OCS.

The CSCF acts a CTF, collecting the information pertaining to chargeable events, assembling this information into matching Charging events, and sending these Charging events to the OCS, see Figure 1.

The OCS receives Charging events from the CSCF and uses the information contained for authorization, credit reservation, and Charging actions. The outcome of these actions is indicated in the responses returned to the CSCF.

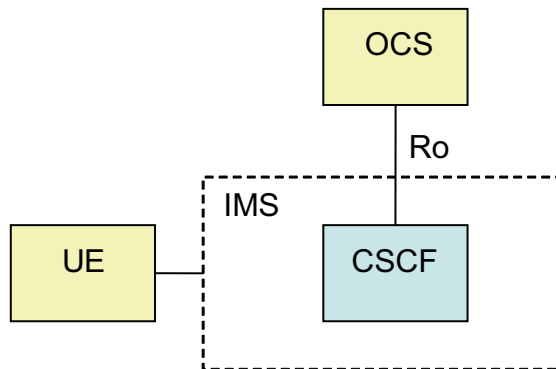


Figure 1 Interface Entities

For more details of the CTF, the OCS, and the Ro reference point, refer to the [3GPP TS 32.240 v7.2.0 Charging management; Charging architecture and principles](#) specification.

2.1 Interface Role

This document describes the services offered by the OCS that are used by the CSCF.

The CSCF sends Diameter Credit Control Request (CCR) messages to the OCS.

The OCS responds to the CSCF using Diameter Credit Control Answer (CCA) messages.

2.2 Services

The services used by the CSCF are shown in Table 1.

Table 1 Used Services

Used Service	Description
Session Charging with Unit Reservation	CCR Initial, Update, and Termination messages are used for credit control purposes relating to a communication session attempt.
Immediate Event Charging for Unsuccessful Attempt to Establish a SIP Session	A CCR Event message is used to convey credit control information to the OCS relating to an unsuccessful attempt to establish a communication session.
Immediate Event Charging for Session Unrelated Event	A CCR Event message is used to convey credit control information to the OCS relating to the session unrelated events.

2.3 Encapsulation and Addressing

This interface uses Diameter accounting messages transported over the Transmission Control Protocol (TCP). The message contents are based on the content defined by 3GPP supplemented, where applicable, with Ericsson-defined information conveyed in vendor-specific AVPs.

Common Charging parameters must be preconfigured for the connections between the CSCF and all relevant OCSs.

For more details on configuration on native CSCF, refer to *CSCF Charging Parameter Description*.

For more details on configuration on virtual CSCF, refer to *Managed Object Model (MOM)*.

Connections between the CSCF and OCSs are only established based on the preconfigured data.

The OCS realm address that is to be used for reporting accounting information for a particular SIP session is identified from the Charging function address information provisioned against the user in the HSS. If no Charging function address information has been configured for the user, a locally configured default OCS realm address is used instead.

The OCS realm address that is to be used for credit control is identified from the Charging function address information provisioned against the user in the HSS. If no Charging function address information has been provisioned for the user, a locally configured default OCS realm address is used instead.

Address information can contain transport mechanism and port number information as well as the OCS realm address; however the transport mechanism and port number information is not used. The CSCF always sends



messages using TCP to the preconfigured port number associated with the connection to the OCS identified by the realm address.





3 Procedures

For online charging, the basic functionality as defined by the IETF Diameter Credit Control application is used. The basic structure follows a mechanism where the CTF, S-CSCF, requests resource allocation and reports credit control information to the OCS.

3GPP TS 32.299 defines the following three cases for online charging:

- Immediate Event Charging (IEC)
- Event Charging with Unit Reservation (ECUR)
- Session Charging with Unit Reservation (SCUR)

The S-CSCF supports ECUR and SCUR as described in Section 3.2 Usage Examples on page 8. The decision whether to apply ECUR or SCUR is based on SIP Message.

SCUR is used for credit control of sessions. SCUR also includes the process of requesting, reserving, releasing, and returning unused units for sessions, and the deduction of the corresponding monetary units. During a SIP session, there can be repeated execution of unit reservation and debit operations as specified in [3GPP TS 32.299 v6.8.0 Diameter Charging Applications](#). The type of unit used for sessions is continuous time.

3GPP defines a basic mode for event handling with quota reservation (ECUR) where the serving node, in this case S-CSCF request quota for the SIP event received. Event Charging with Unit Reservation (ECUR) includes the process of requesting, reserving, releasing, and returning unused units for events. The deduction of the corresponding monetary units then occurs upon conclusion of the ECUR transaction. In this case, the Credit Control Request is used to control the credit control session. The type of unit used for events is service-specific.

The authorization indication is included in the *Service-Specific-Units* AVP with values 0–1 generated by the OCS system showing the non-authorization/authorization decision.

The Charging information is transferred from a client to a Charging Server using the Diameter Credit Control Request (CCR) and Credit Control Answer (CCA) messages.

A Charging session is initiated when the Diameter client issues a CCR with *CC-Request-Type* set to **INITIAL_REQUEST**. The Charging Server defines when the Diameter client sends the next CCR by including *Validity-Time* in the CCA. The Diameter client then sends a CCR, *CC-Request-Type* set to **UPDATE_REQUEST**, if the validity time elapses. The CCA response includes a new *Validity-Time* value that is used. If the client does not receive the

Validity-Time, no time-based UPDATE request is send by the client. A CCR, UPDATE_REQUEST, is also sent when the granted units are consumed.

When SCUR applies, a CCR, UPDATE_REQUEST, can also be triggered by SIP re-INVITE and SIP UPDATE requests that contain SDP data.

The Charging session is ended when the Diameter client sends a CCR with the CC-Request-Type set to **TERMINATION_REQUEST**.

For SCUR, the deduction of the time quota for the session can start at different moments according to an operator configuration option. The possible values are as follows:

- After reception of the INVITE
- After reception of 180 provisional response
- After 200 (OK) to the initial INVITE

A couple of sequences that illustrate SCUR and ECUR can be found in Section 3.2 Usage Examples on page 8.

3.1 Error Handling

The Diameter stack automatically resends the CCR a configurable number of times in case of internal time-out waiting for a CCA.

The S-CSCF uses the Tx timer to supervise the sending of CCR. In the case of Tx time-out, the S-CSCF acts according to the Credit Control Failure Handling (CCFH). CCFH can be locally configured to at a fault situation either **TERMINATE** the Credit Control and SIP sessions, or to treat the service as granted and let it **CONTINUE** free of charge. The reception of a Credit Control-Failure-Handling AVP in a CCA overrides the local configuration for the remainder of the Credit Control session.

When S-CSCF receives an incorrect CCA message, the S-CSCF terminates the credit control session with **Termination-Cause** set to **DIAMETER_BAD_ANSWER**.

3.2 Usage Examples

The charging online principles SCUR and ECUR to reserve and debit units used in S-CSCF are shown in Figure 2 and Figure 3.

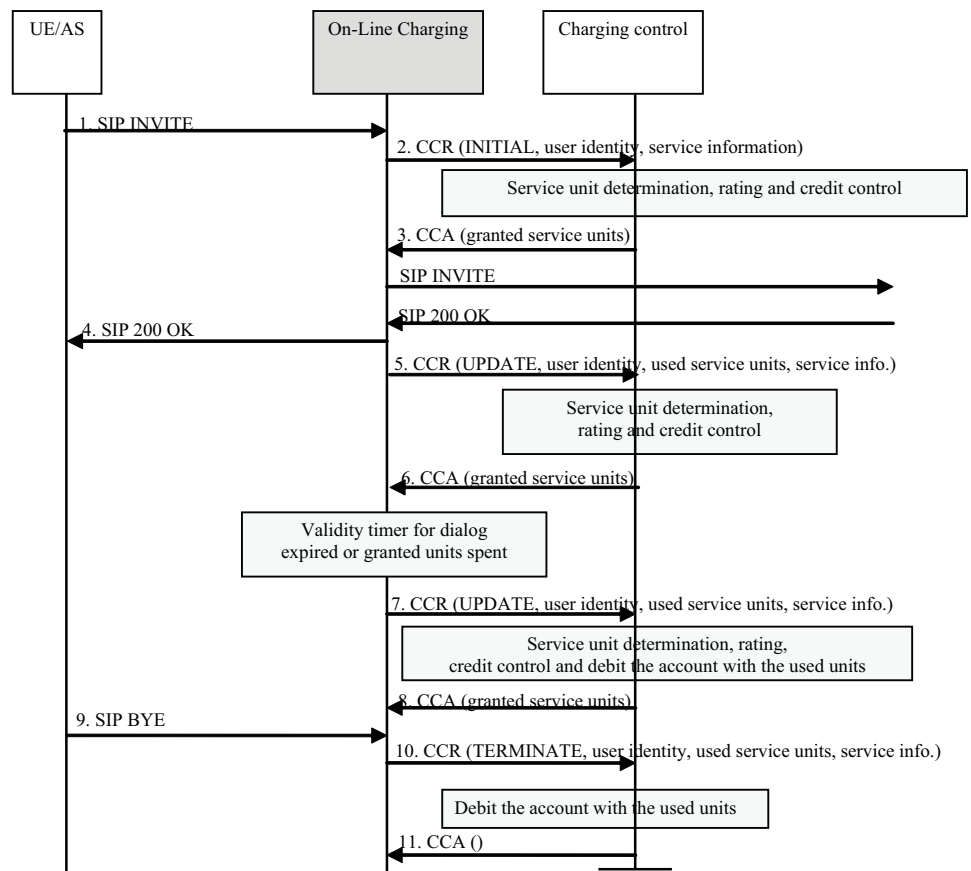


Figure 2 Session Charging with Unit Reservation

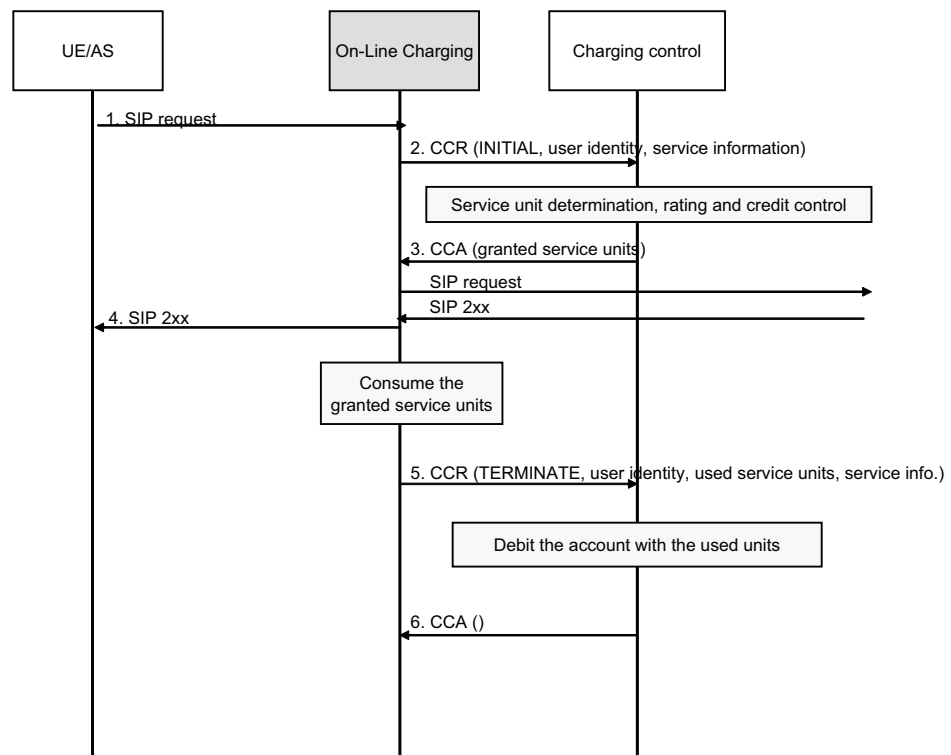


Figure 3 Event Charging with Unit Reservation



4 Information Model

The command codes used to identify messages sent on the Ro interface are specified in the [RFC 4006 Diameter Credit-Control Application](#) specification.

The two Diameter Charging messages used in the CSCF for online charging have the command codes defined in Table 2.

Table 2 Commands Used on the Ro Interface

Command-Name	Code	Code Direction
Credit-Control-Request	272	CSCF to OCS
Credit-Control-Answer	272	OCS to CSCF



5 Formal Syntax

This section refers to specification where the formal syntax notation is defined.

5.1 Message Contents for Online Charging

The Diameter credit control messages Credit Control Request (CCR) and Credit Control Answer (CCA) are used for online charging.

The purpose and content of these messages are described in Section 5.1.1 Credit-Control-Request on page 13 and Section 5.1.2 Credit-Control-Answer Content on page 16.

The AVPs used in the messages are described in Section 5.2 Attribute-Value Pairs on page 17.

The following symbols are used in this document:

- **< AVP >** indicates a mandatory AVP with a fixed position in the message.
- **{ AVP }** indicates a mandatory AVP in the message.
- **[AVP]** indicates an optional AVP in the message.
- *** AVP** indicates that multiple occurrences of an AVP are possible.

The symbols are according to the [3GPP TS 32.299 v6.8.0 Diameter Charging Applications](#) specification.

5.1.1 Credit-Control-Request

The format of the Credit-Control-Request (CCR) content is listed in Table 3. Refer to the following specifications:

- [RFC 3588 Diameter Base Protocol](#)
- [RFC 4006 Diameter Credit-Control Application](#)
- [3GPP TS 32.299 v6.8.0 Diameter Charging Applications](#)

Table 3 Credit-Control-Request Content

AVP	AVP Code	Value Type
< Session-Id >	263	UTF8String
{ Origin-Host }	264	DiameterIdentity

Table 3 Credit-Control-Request Content

AVP	AVP Code	Value Type
{ Origin-Realm }	296	DiameterIdentity
{ Destination-Realm }	283	DiameterIdentity
{ Auth-Application-Id }	258	Unsigned32
{ Service-Context-Id }	461	UTF8String
{ CC-Request-Type }	416	Enumerated
{ CC-Request-Number }	415	Unsigned32
[Destination-Host]	293	DiameterIdentity
[User-Name]	1	UTF8String
[Event-Timestamp]	55	Time
[Subscription-id]	443	Grouped
→ { Subscription-Id-Type }	450	Enumerated
→ { Subscription-Id-Data }	444	UTF8String
[Termination-Cause]	295	Enumerated
[Multiple-Services-Indicator]	455	Enumerated
[Multiple-Services-Credit-Control] See Table 4	456	Grouped
[Service-Information]	873	Grouped
→ [PS-Information]	874	Grouped
→→ [3GPP-SGSN-MCC-MNC]	18	UTF8String
→ [IMS-Information] See Table 5	876	Grouped
[Ericsson-Service-Information]	285	Grouped
→ * [IMS-Service-Identification]	284	UTF8String
→ [Called-Party-Original-Address]	286	UTF8String
→ [Dial-Around-Indicator]	1160	UTF8String
→ [Authentication-Method]	1261	Enumerated
→ [SIP-Request-Timestamp-Fraction]	2301	Unsigned32
→ [SIP-Response-Timestamp-Fraction]	2302	Unsigned32
→ [Disconnect-Direction]	1305	Enumerated
→ * [Transaction-Info]	1264	Grouped
→→ { Transaction-Type }	1265	Enumerated
→→ { Transaction-Data-Name }	1266	UTF8String
→→ 1 * { Transaction-Data-Value }	1267	UTF8String



Table 3 Credit-Control-Request Content

AVP	AVP Code	Value Type
[SIP-Reason]	335	Grouped
→ [SIP-Reason-Cause]	336	Unsigned32
→ [SIP-Reason-Text]	337	UTF8String
[GPRS-Roaming-Status]	333	Enumerated
[Event-NTP-Timestamp]	340	OctetString
[SIP-Ringing-Timestamp]	338	Time
[Quota-Deduction-Start]	339	Enumerated

Multiple-Service-Credit-Control (MSCC), see Table 4, is in CCR, also refer to the [RFC 4006 Diameter Credit-Control Application](#) specification.

Table 4 Multiple-Service-Credit-Control

AVP	Code	Type
[Requested-Service-Unit]	437	Grouped
[Used-Service-Unit]	446	Grouped
→ [Reporting-Reason]	872	Enumerated
→ [CC-Time]	420	Unsigned32
→ [CC-Service-Specific-Units]	417	Unsigned64
[Service-Identifier]	439	Unsigned32

IMS-information, see Table 5, also refer to the [3GPP TS 32.299 v6.8.0 Diameter Charging Applications](#) specification.

Table 5 IMS-Information

AVP	Code	Type
[Event-Type]	823	Grouped
→ [SIP-Method]	824	UTF8String
→ [Event]	825	UTF8String
* [Called-Asserted-Identity]	1250	UTF8String
[Role-of-node]	829	Enumerated
{ Node-Functionality }	862	Enumerated
[User-Session-ID]	830	UTF8String
* [Calling-Party-Address]	831	UTF8String
[Called-Party-Address]	832	UTF8String

Table 5 IMS-Information

AVP	Code	Type
[Time-Stamps]	833	Grouped
→ [SIP-Request-Timestamp]	834	Time
→ [SIP-Response-Timestamp]	835	Time
[Inter-Operator-Identifier]	838	Grouped
→ [Originating IOI]	839	UTF8String
→ [Terminating IOI]	840	UTF8String
[IMS-Charging-Identifier]	841	UTF8String
* [SDP-Session-Description]]	842	UTF8String
* [SDP-Media-Component]	843	Grouped
→ [SDP-Media-Name]	844	UTF8String
→ * [SDP-Media-Description]	845	UTF8String
* [Message-Body]	889	Grouped
→ [Content-Type]	826	UTF8String
→ [Content-Length]	827	Unsigned32
→ [Content-Disposition]	828	UTF8String
→ [Originator]	864	Enumerated
{ Cause-Code }	861	Integer32
[Access-Network-Information]	1263	OctetString
[Carrier-Select-Routing-Information]	2023	UTF8String
[Number-Portability-Routing-Information]	2024	UTF8String

5.1.2 Credit-Control-Answer Content

The AVPs that are supported in a `Credit-Control-Answer` are listed in Table 6. Refer to the following specifications:

- [RFC 3588 Diameter Base Protocol](#)
- [RFC 4006 Diameter Credit-Control Application](#)
- [3GPP TS 32.299 v6.8.0 Diameter Charging Applications](#)

Table 6 Credit-Control-Answer Content

AVP	Code	Type
< Session-Id >	263	UTF8String

Table 6 Credit-Control-Answer Content

AVP	Code	Type
{ Result-Code }	268	Unsigned32
{ Origin-Host }	264	DiameterIdentity
{ Origin-Realm }	296	DiameterIdentity
{ Auth-Application-Id }	258	Unsigned32
{ CC-Request-Type }	416	Enumerated
{ CC-Request-Number }	415	Unsigned32
* { Multiple-Services-Credit-Control }	456	Grouped
→ [Granted-Service-Unit]	431	Grouped
→→ [CC-Time]	420	Unsigned32
→→ [CC-Service-Specific-Units]	417	Unsigned64
→ [Service-Identifier]	439	Unsigned32
→ [Validity-Time]	448	Unsigned32
→ [Result-Code]	268	Unsigned32
→ [Final-Unit-Indication]	430	Grouped
→→ { Final-Unit-Action }	449	Enumerated
→ [Trigger-Type]	870	Enumerated
[Credit-Control-Failure-Handling]	427	Enumerated
* [Failed-AVP]	279	Grouped

5.2 Attribute-Value Pairs

A Diameter AVP header has the format shown in Figure 4.

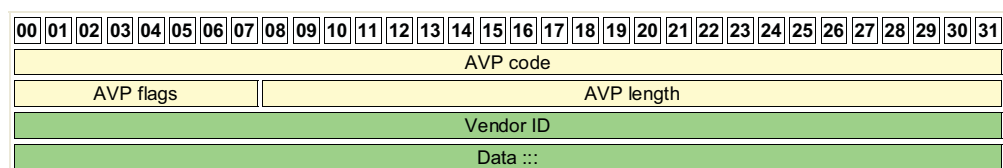


Figure 4 Diameter AVP Header

In the following sections, the AVPs are split up into the following groups:

- Diameter Base Protocol AVPs
- Diameter Credit Control Application AVPs
- 3GPP Diameter Protocol-Specific AVPs

- Ericsson Vendor-Specific AVPs

5.2.1 Diameter Base Protocol AVPs

5.2.1.1 Auth-Application-Id

The `Auth-Application-Id` AVP, see Table 7, is used to advertise support of the Diameter Credit Control Application. The value of the `Auth-Application-Id` is set by the S-CSCF.

Table 7 *Auth-Application-Id*

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	258	12	Unsigned32

Example

```
Value = 4
```

5.2.1.2 Destination-Host

The `Destination-Host` AVP, see Table 8, is provided from the `Origin-Host` AVP in the CCA for (`INITIAL_REQUEST`) message, and points out the Charging Server address to be used for this Charging session and therefore included in the following CCR messages.

Table 8 *Destination-Host AVP*

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	293	> 8	DiameterIdentity

Example

```
neighbour1.ericsson.se
```

5.2.1.3 Destination-Realm

The `Destination-Realm` AVP, see Table 9, contains the realm the message is to be routed to. The `Destination-Realm` must be present in a CCR message.

Table 9 *Destination-Realm AVP*

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	283	> 8	DiameterIdentity



The value is extracted from the ECF-address (`DiameterURI`) in the user profile downloaded from HSS. If no `Destination-Realm` in the user profile is available, a local configured ECF-address is used. The value does not change during the Charging session.

Example

```
ericsson.se
```

5.2.1.4 Event-Timestamp

The `Event-Timestamp` AVP is shown in Table 10.

Table 10 *Event-Timestamp AVP*

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	55	12	Time

The `Event-Timestamp` is set by the S-CSCF and used to record the time that the reported chargeable event occurred in CTF, expressed in seconds since January 1 1900 00:00 UTC.

Sent to indicate the time the quota is requested.

5.2.1.5 Failed-AVP

The `Failed-AVP` AVP, see Table 11, provides debugging information in cases where a request is rejected or not fully processed because of erroneous information in a specific AVP. The value of the `Result-Code` AVP provides information on the reason for the `Failed-AVP` AVP.

Table 11 *Failed-AVP*

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	279	>16	Grouped

Grammar:

```
< Failed-AVP > ::= < AVP Header: 279 >
1 * { AVP }
```

5.2.1.6 Origin-Host

The `Origin-Host` AVP, see Table 12, identifies the S-CSCF that originated the Diameter message, and must be present in all Diameter Charging messages. It is also the `Diameter-Identity` of the OCF when sent in CCA.

Table 12 Origin-Host AVP

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	264	> 8	DiameterIdentity

The `Origin-Host` is a configurable value in S-CSCF.

Example

```
scscf.ericsson.se
```

5.2.1.7

Origin-Realm

The `Origin-Realm` AVP, see Table 13, contains the realm address of S-CSCF and must be present in all Diameter Charging messages. It is also the OCF realm when sent in CCA. The data `Origin-Realm` is configurable by the S-CSCF.

Table 13 Origin-Realm AVP

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	296	> 8	DiameterIdentity

Example

```
ericsson.se
```

5.2.1.8

Result-Code

The `Result-Code` AVP, see Table 14, indicates whether a particular request was completed successfully or whether an error occurred.

Table 14 Result-Code AVP

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	268	12	Unsigned32

A mandatory `Result-Code` is present in the top level of Diameter CCA AVPs and an optional `Result-Code` in the Grouped Multiple-Service-Credit-Control (MSCC) as shown in Table 14. The CSCF ignores the `Result-Code` if received in the grouped MSCC.

If the `Result-Code` on the command level indicates a value other than SUCCESS, then the `Result-Code` on command level takes precedence over any included in the Multiple-Services-Credit-Control AVP. The classes of Diameter errors for `Result-Code` are described in Table 15.



Table 15 Diameter Error Classes Derived from Mandatory Result-Code and S-CSCF Actions

Result Class	Description	CSCF Action
1XXX	Informational	Terminate Credit Control and SIP sessions.
2XXX	DIAMETER_SUCCESS	Process the ACA
3XXX	DIAMETER_ERROR	For Result-Code = <ul style="list-style-type: none"> • DIAMETER_UNABLE_TO_DELIVER (3002) • DIAMETER_TOO_BUSY (3004) • DIAMETER_LOOP_DETECTED (3005) According to Section 3.1 Error Handling on page 8. Else, terminate Credit Control and SIP session.
4XXX	TRANSIENT_FAILURE	If Result-Code = 4011, then allow service and terminate Credit Control session. If Result-Code = 4010 or 4012, then terminate Credit Control and SIP sessions. Else, seeSection 3.1 Error Handling on page 8.
5XXX	PERMANENT_FAILURE	If Result-Code = 5030, then terminate Credit Control and SIP sessions. Else, seeSection 3.1 Error Handling on page 8.
OTHER	Non-recognized class	Terminate Credit Control and SIP sessions.

5.2.1.9 Session-Id

The Session-Id AVP, see Table 16, is used to identify a specific Credit Control session. All messages pertaining to the same session must include a unique Session-Id AVP. The value of Session-Id does not change during the Charging session. The Session-Id is created by the S-CSCF initiating the Credit Control session.

Table 16 Session-Id AVP

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	263	> 35	UTF8String

Grammar:

< DiameterIdentity >;< high bits >;< low bits >;< optional value >

Where:

- `< DiameterIdentity >` = S-CSCF domain name
- `< high bits >` = Hexadecimal number of seconds since the 1970-01-01 (8 characters)
- `< low bits >` = Number of micro seconds (6 characters)
- `< optional value >` = Hash sum of the SIP Call-ID (8 characters)

Example

```
cscf.abcdef.com;89071234;087654;12348765
```

5.2.1.10

Termination-Cause

The `Termination-Cause` AVP, see Table 17, is used to indicate the reason why a session was terminated on the access device.

Table 17 *Termination-Cause AVP*

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	295	12	Enumerated

Defined values:

- Not used 1–2
- `DIAMETER_BAD_ANSWER` 3
- Not used 4–8

`Termination-Cause` is used when terminating a Credit Control session because a malformed CCA message or unexpected AVP values have been received.

5.2.1.11

User-Name

The `User-Name` AVP, see Table 18, contains the Private User Identity that is assigned by the home network.

Table 18 *User-Name AVP*

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	1	> 8	UTF8String

If the private identity of the user is not known in the S-CSCF node, this attribute is not sent. The `User-Name` data is configurable and is fetched from the user profile. The value does not change during the Charging session.



Example

```
userA@domain_name.com
```

5.2.2 Diameter Credit Control Application AVPs

5.2.2.1 CC-Request-Number

The CC-Request-Number AVP, see Table 19, is set by the S-CSCF.

Table 19 CC-Request-Number AVP

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	415	12	Unsigned32

As Session-Id AVPs are globally unique. The combination of Session-Id and CC-Request-Number AVPs is also globally unique and can be used in matching Credit Control messages with confirmations. The value of CC-Request-Number is set to 0 for Credit Control Request of type INITIAL_REQUEST and EVENT_REQUEST. The value is set to 1 for the first UPDATE_REQUEST, to 2 for the second, and so on, until the value for TERMINATION_REQUEST is one more than for the last UPDATE_REQUEST.

5.2.2.2 CC-Request-Type

The CC-Request-Type AVP, see Table 20, contains the reason for sending the Credit Control Request message. The CC-Request-Type is set by the S-CSCF.

Table 20 CC-Request-Type AVP

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	416	12	Enumerated

Defined values:

- INITIAL_REQUEST 1
- UPDATE_REQUEST 2
- TERMINATION_REQUEST 3
- Not used 4

5.2.2.3 CC-Service-Specific-Units

The `CC-Service-Specific-Units` AVP, see Table 21, specifies the number of service-specific units given in a selected service. Examples of specific units are number of events or points.

Table 21 *CC-Service-Specific-Units AVP*

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	417	16	Unsigned64

The service-specific units always refer to the service identified in the `Service-Identifier` AVP. Service-specific units are the only supported unit type in ECUR. Granted units must be greater than zero.

5.2.2.4 CC-Time

The `CC-Time` AVP, see Table 22, indicates the length of the requested or used time in seconds. Granted time must be greater than zero. Used time can be zero. Time is the only supported unit type in SCUR.

Table 22 *CC-Time AVP*

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	420	12	Unsigned32

5.2.2.5 Credit-Control-Failure-Handling

The `Credit-Control-Failure-Handling` AVP, see Table 23, defines what the S-CSCF does in fault situations during the rest of the Credit Control session.

Table 23 *Credit-Control-Failure-Handling AVP*

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	427	12	Enumerated

The information in this AVP overrides the local configuration for the remainder of the session. See also Section 3.1 Error Handling on page 8 for more information.

Defined values:

- `TERMINATE` 0

The S-CSCF will, in the case of transport or temporary failures, see the service as failed and the SIP dialog or transaction is terminated.

- `CONTINUE` 1

The S-CSCF will, in the case of failures, see the service as granted and continue without an established Credit Control session.

- Not used 2

Treated as if `TERMINATE` is received.

5.2.2.6 Final-Unit-Action

The `Final-Unit-Action` AVP, see Table 24, indicates to the CSCF the action to be taken when the account of the user cannot cover the service cost.

Table 24 *Final-Unit-Action AVP*

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	449	12	Enumerated

Defined values:

- `TERMINATE` 0
- `REDIRECT` 1 (not supported)
- `RESTRICT_ACCESS` 2 (not supported)

5.2.2.7 Final-Unit-Indication

The `Final-Unit-Indication` AVP, see Table 25, indicates that the `Granted-Service-Unit` AVP in the `Credit-Control-Answer`, contains the final units for the service. After these units have expired, the Diameter Credit Control client is responsible for executing the action indicated in the `Final-Unit-Action` AVP.

Table 25 *Final-Unit-Indication AVP*

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	430	20	Grouped

Grammar:

```
< Final-Unit-Indication > ::= < AVP Header: 430 >
{ Final-Unit-Action }
```

5.2.2.8 Granted-Service-Unit

Grouped `Granted-Service-Unit` AVP, see Table 26, contains the number of units that the S-CSCF can provide to the end user until the service must be released or a new CCR must be sent.

Table 26 *Granted-Service-Unit AVP*

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	431	20	Grouped

Grammar:

```
< Granted-Service-Unit > ::= < AVP Header: 431 >
[ CC-Time ]
[ CC-Service-Specific-Units ]
```

5.2.2.9

Multiple-Services-Credit-Control

Multiple-Services-Credit-Control AVP, see Table 27, contains the AVPs related to the independent Credit Control of multiple services feature. Only one instance of this AVP can be handled at a time.

Table 27 *Multiple-Services-Credit-Control AVP*

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	456	> 16	Grouped

Multiple-Services-Credit-Control occurs in CCRs and has the following grammar:

```
<Multiple-Services-Credit-Control > ::= < AVP Header: 456>
    [Requested-Service-Unit]
    [Used-Service-Unit]
        [Reporting-Reason]
        [CC-Time]
        [CC-Service-Specific-Units]
    [Service-Identifier]
```

Multiple-Services-Credit-Control occurs in CCA and has the following grammar:

```
< Multiple-Services-Credit-Control > ::= < AVP Header: 456 >
    [Granted-Service-Unit]
        [CC-Time]
        [CC-Service-Specific-Units]
    [Validity-Time]
    [Result-Code]
    [Final-Unit-Indication]
        { Final-Unit-Action }
    [Trigger-Type]
```



5.2.2.10 Multiple-Services-Indicator

The `Multiple-Services-Indicator` AVP, see Table 28, indicates that S-CSCF is capable of handling multiple services independently within a (sub)session.

Table 28 *Multiple-Services-Indicator AVP*

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	455	12	Enumerated

Although the `Multiple-Services-Credit-Control` AVP is used, the S-CSCF at this stage does not fully support this mechanism, only one service can be handled at a time.

Defined values:

- Not used 0
- `MULTIPLE_SERVICES_SUPPORTED` 1

Client supports independent Credit Control of multiple services.

5.2.2.11 Requested-Service-Unit

The `Requested-Service-Unit` AVP, see Table 29, is when sent, always sent empty. The Credit Control server takes all Charging and rating decisions.

Table 29 *Requested-Service-Unit AVP*

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	437	8	Grouped

Grammar:

```
< Requested-Service-Unit > ::= < AVP Header: 437 >
                                [CC-Time]
                                [CC-Service-Specific-Units]
```

5.2.2.12 Service-Context-Id

The `Service-Context-Id` AVP, see Table 30, contains a unique identifier of the Diameter Credit Control service-specific document that applies to the request.

Table 30 *Service-Context-Id AVP*

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	461	> 8	UTF8String

The value is configurable in the S-CSCF. The grammar of the `Service-Context-Id` is according to the [RFC 4006 Diameter Credit-Control Application](#) specification.

Default value: 6.32260@3gpp.org

5.2.2.13 Service-Identifier

The `Service-Identifier` AVP, see Table 31, contains the identifier of a service. The specific service the request relates to is uniquely identified by the combination of `Service-Context-Id` and `Service-Identifier` AVPs.

Table 31 *Service-Identifier AVP*

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	439	12	Unsigned32

The AVP is demanded by the [RFC 4006 Diameter Credit-Control Application](#) specification.

There is no need to use this AVP to distinguish different services, as only one service is handled in each request.

Example

```
Value = 1
```

5.2.2.14 Subscription-Id

The `Subscription-Id` AVP, see Table 32, is used to identify the subscription of the served end user.

Table 32 *Subscription-Id AVP*

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	433	> 28	Grouped

The `Subscription-Id` AVP includes a `Subscription-Id-Data` AVP that holds the identifier and a `Subscription-Id-Type` AVP that defines the identifier type. Only one instance can exist at a time.

Grammar:

```
< Subscription-Id > ::= < AVP Header: 443 >
    { Subscription-Id-Type }
    { Subscription-Id-Data }
```




5.2.2.15 Subscription-Id-Data

The Subscription-Id-Data AVP, see Table 33, is used to identify the end user. The identifier is fetched from the user profile.

Table 33 Subscription-Id-Data AVP

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	444	> 8	UTF8String

5.2.2.16 Subscription-Id-Type

The Subscription-Id-Type AVP, see Table 34, is used to determine which type of identifier is carried by the Subscription-Id-Data AVP.

Table 34 Subscription-Id-Type AVP

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	450	12	Enumerated

Defined values:

- END_USER_E164 0
- Not used 1–4

5.2.2.17 Used-Service-Unit

The Used-Service-Unit AVP, see Table 35, contains the number 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.

Table 35 Used-Service-Unit AVP

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	446	> 16	Grouped

Grammar:

```
< Used-Service-Unit > ::= < AVP Header: 446 >
    [ Reporting-Reason ]
    [ CC-Time ]
    [ CC-Service-Specific-Units ]
```

5.2.2.18 Validity-Time

The `Validity-Time` AVP, see Table 36, is sent from the Credit Control server to the Credit Control client and contains the validity time of the Granted Service Units.

Table 36 *Used-Service-Unit AVP*

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	448	12	Unsigned32

The measurement of the `Validity-Time` is started upon receipt of the `Credit-Control-Answer` message containing this AVP. If the Granted Service Units have not been consumed within the validity time specified in this AVP, a `Credit-Control-Request` message is sent to the server, with `CC-Request-Type` set to **UPDATE_REQUEST**. The `Validity-Time` AVP contains a non-zero value and is given in seconds.

5.2.3 3GPP Diameter Accounting AVPs

5.2.3.1 3GPP-SGSN-MCC-MNC

The `3GPP-SGSN-MCC-MNC` AVP, see Table 37, holds the Mobile Country Code and the Mobile Network Code used by an operator. The value is downloaded from the HSS in the user-profile.

Table 37 *3GPP-SGSN-MCC-MNC AVP*

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	18	> 12	UTF8String	10415

The MCC consists of three digits and the MNC consists of two or three digits depend on the value of MCC.

Example

23415

Where:

- 2=MCC digit 1
- 3=MCC digit 2
- 4=MCC digit 3
- 1=MNC digit 1
- 5=MNC digit 2



The value does not change during the Charging session.

5.2.3.2 Access-Network-Information

The Access-Network-Information AVP, see Table 38, contains the content of the SIP P-Header P-Access-Network-Information.

Table 38 Access-Network-Information AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	1263	> 12	OctetString	10415

The location can change during a SIP session.

Example

```
3GPP-GERAN; network-provided; cgi-3gpp=23415;
X-gprs-roaming-status=visited
```

5.2.3.3 Called-Asserted-Identity

This AVP, see Table 39, holds the SIP URI or tel URI or both addresses of the asserted called party. The address is obtained from the P-Asserted-Identity SIP header field of the 2xx responses corresponding to a SIP request either initiating a dialog or a standalone transaction. This field can appear several times in the request when the P-Asserted-Identity contains both a SIP URI and a tel URI.

Table 39 Called-Asserted-Identity AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	1250	> 12	UTF8String	10415

The S-CSCF puts at most one SIP URI and at most one tel URI in the Called-Asserted-Identity. A maximum of two Called-Asserted-Identity AVP instances are supported.

The value of Called-Asserted-Identity AVP does not change during the Charging session. Each AVP instance only contains the SIP or tel URI parameters taken from the P-Asserted-Identity, without including any extra URI parameters.

Example

```
- As SIP URI:
sip: +46813200000@ericsson.com
- As tel URI:
tel: +468132000000
```

5.2.3.4 Called-Party-Address

The Called-Party-Address AVP, see Table 40, identifies the terminating user of the session. It is a SIP URI or a tel URI obtained from the SIP message including all other URI parameters separated by “;”.

Table 40 Called-Party-Address AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	832	> 12	UTF8String	10415

On the originating side, the Called-Party-Address is obtained from the Request-URI of the outgoing SIP message.

On the terminating side, the Called-Party-Address is obtained from the Request-URI of the incoming SIP message.

The value of Called-Party-Address does not change during the Charging session.

Example

```
- As SIP URI:
sip: +468132000000@ericsson.com
- As tel URI:
tel: +468132000000
```

5.2.3.5 Calling-Party-Address

The Calling-Party-Address AVP, see Table 41, identifies the originating user of the session.

Table 41 Calling-Party-Address AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	831	> 12	UTF8String	10415

It is a SIP URI, tel URI, or both, if available, including possible parameters obtained from the P-Served-User header, applicable only for AS UAC, of a SIP message. If it is missing in the P-Served-User, or not an AS UAC case, then it is obtained from the P-Asserted-Identity header of a SIP message. If it is missing in the P-Asserted-Identity header, then it is obtained from the From header.

It is configurable whether to use the SIP URI or the tel URI, or both. If the wanted type of address is not available, the existing type is used. A maximum of two Calling Party Address AVP instances are supported, containing a SIP URI and a tel URI.

The value of `Calling-Party-Address` does not change during the Charging session.

5.2.3.6 Carrier-Select-Routing-Information

This AVP, see Table 42, holds information the Carrier Select routing information received by an originating S-CSCF. If the parameter is available in the `Request-URI` in the initial SIP request, before service invocation, it is included in the CCR (Initial) request. Otherwise the AVP is included in the CCR (UPDATE) and CCR (TERMINATE) request. The value of the Charging AVP is not updated during the Charging session.

Table 42 Carrier-Select-Routing-Information AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	2023	> 12	UTF8String	10415

The Carrier Select routing information is outputted in global format if the CIC Routing feature is enabled.

In a terminating S-CSCF, this AVP holds information on the Carrier Select routing information received in an initial SIP request within the `Request-URI` header. If present, the AVP is included in all CCR requests (INITIAL, UPDATE, TERMINATE) and the value of the Charging AVP is not updated during the Charging session.

5.2.3.7 Cause-Code

The Cause-Code AVP, see Table 43, is the cause code value from the S-CSCF node. It is used in CCR (TERMINATE) messages.

Table 43 Cause-Code AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	861	16	Integer32	10415

Within the cause codes, values less than or equal to 0 are reserved for successful causes while values greater than or equal to 1 are used for failure causes. In case of errors where the session has been terminated as a result of a specific known SIP error code, then the SIP error code is also used as the cause code.

Successful Cause-Code values:

- “Normal end of session” 0

This cause is used in CCR (TERMINATE) message to indicate that an ongoing SIP session has been normally released either by the user or by the network (SIP BYE message initiated by the user or initiated by the

network has been received by the IMS node after the reception of the SIP ACK message).

- “Successful transaction” -1

This cause is used to indicate a successful SIP transaction, for example MESSAGE, NOTIFY, and SUBSCRIBE.

- “End of SUBSCRIBE dialog” -2

This cause is used to indicate the closure of a SIP SUBSCRIBE dialog. The subscription terminates when a SIP NOTIFY with a Subscription-State header containing the value terminated is received.

- “2xx Final Response” -2xx

This cause is used to indicate the closure of a SIP transaction after receiving/initiating a 2xx Final response, except 200.

- “3xx Redirection” -3xx

This cause is used when the SIP transaction is terminated because of an IMS node receiving/initiating a 3xx response.

Failure Cause-Code values:

- “Unspecified error” 1

This cause is used when the SIP transaction is terminated because of an unknown error.

- “4xx Request failure” 4xx

This cause is used when the SIP transaction is terminated because of an IMS node receiving/initiating a 4xx error response.

- “5xx Server failure” 5xx

This cause is used when the SIP transaction is terminated after receiving/initiating a 5xx error response.

- “6xx Global failure” 6xx

This cause is used when the SIP transaction is terminated after receiving/initiating a 6xx error response.

- “Unsuccessful session setup” 2

This cause is used in the CCR (Terminate) when the SIP session has not been successfully established.

- “Internal error” 3

This cause is used when the SIP transaction is terminated because of an internal error, for example error in processing a request/response.

5.2.3.8 Content-Disposition

The `Content-Disposition` AVP, see Table 44, indicates how the SIP message body or a message body part is to be interpreted, for example, session, render, as described in the [RFC 3261 Session Initiation Protocol](#) specification.

Table 44 *Content-Disposition AVP*

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	828	> 12	UTF8String	10415

The value of this AVP is fetched from the `Content-Disposition` Header.

5.2.3.9 Content-Length

The `Content-Length` AVP, see Table 45, holds the size of the SIP message body.

Table 45 *Content-Length AVP*

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	827	16	Unsigned32	10415

The value of this AVP is fetched from the `Content-Length` header. The `Content-Length` AVP occurs in Diameter Charging message if the `Content-Length` is greater than 0.

5.2.3.10 Content-Type

The `Content-Type` AVP, see Table 46, holds the media type, for example, `application/sdp`, `text/html`, of the message body.

Table 46 *Content-Type AVP*

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	826	> 12	UTF8String	10415

The value of this AVP is fetched from the `Content-Type` header or, in case of MIME/multipart, from the message body and the included Content Type information.

5.2.3.11 Event

The `Event` AVP, see Table 47, holds the content of the `Event` header.

Table 47 Event AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	825	> 12	UTF8String	10415

5.2.3.12

Event-Type

The Event-Type AVP, see Table 48, contains information about the type of chargeable telecommunication service/event for which the CCR message is generated. Event-Type is triggered by SIP requests and occurs only in CCRs.

Table 48 Event-Type AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	823	> 24	Grouped	10415

Grammar:

```
< Event-Type > ::= <AVP Header: 823 >
    [ SIP-Method ]
    [ Event ]
```

5.2.3.13

IMS-Charging-Identifier

The IMS-Charging-Identifier AVP is shown in Table 49.

Table 49 IMS-Charging-Identifier AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	841	> 12	UTF8String	10415

This is the IMS Charging Identifier (ICID) as generated by an IMS node for a SIP session in the P-Charging-Vector. For all messages outside an established SIP session, a new ICID is generated. This ICID is used in all SIP request messages during all session until the session is terminated. The value of this AVP is fetched from the P-Charging-Vector header or locally generated depending on the traffic case.

At each SIP session unrelated method, for example REGISTER, NOTIFY, MESSAGE, a new ICID is generated at the first IMS node that processes the method.

At each SIP session establishment a new, session-specific, ICID is generated at the first “session state aware” IMS network element that processes the session-initiating SIP INVITE message. This ICID is used in all SIP request messages during the session until the session is terminated.

The ICID value is globally unique across all 3GPP IMS networks for at least a month as defined by 3GPP.

Example

00000028003c06c830735

5.2.3.14 IMS-Information

The purpose of the `IMS-Information` AVP, see Table 50, is to allow the transmission of additional IMS service-specific information elements.

Table 50 *IMS-Information AVP*

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	876	> 28	Grouped	10415

Grammar:

```
< IMS-Information > ::= < AVP Header: 876 >
  [ Event-Type ]
  [ Role-Of-Node ]
  { Node-Functionality }
  [ User-Session-ID ]
  * [ Calling-Party-Address ]
  [ Called-Party-Address ]
  [ Time-Stamps ]
  [ Inter-Operator-Identifier ]
  [ IMS-Charging-Identifier ]
  * [ SDP-Session-Description ]
  * [ SDP-Media-Component ]
  * [ Message-Body ]
  [ Cause-Code ]
  [ Access-Network-Information ]
  [ Carrier-Select-Routing-Information ]
  [ Number-Portability-Routing-Information ]
```

5.2.3.15 Inter-Operator-Identifier

The `Inter-Operator-Identifier` AVP is shown in Table 51.

Table 51 *Inter-Operator-Identifier AVP*

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	838	> 16	Grouped	10415

A globally unique identifier to share between operator networks, service providers, and content providers to correlate billing information generated within the IP Multimedia Subsystem.

Grammar:

```
< Inter-Operator-Identifier > ::= < AVP Header: 838 >
    [ Originating-IOI ]
    [ Terminating-IOI ]
```

5.2.3.16 Message-Body

The Message-Body AVP, see Table 52, holds information about the message bodies including user-to-user data. Message-Body is only in CCRs triggered by SIP requests.

Table 52 Message-Body AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	889	> 24	Grouped	10415

Grammar:

```
< Message-Body > ::= < AVP Header: 889 >
    [ Content-Type ]
    [ Content-Length ]
    [ Content-Disposition ]
    [ Originator ]
```

5.2.3.17 Node-Functionality

The Node-Functionality AVP, see Table 53, includes the functionality identifier of the node.

Table 53 Node-Functionality AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	862	16	Enumerated	10415

The functionality identifier can be one of the following:

- S-CSCF 0
- Reserved 1–6

5.2.3.18 Number-Portability-Routing-Information

The Number-Portability-Routing-Information AVP, see Table 54, holds information on Number Portability routing information received by an originating S-CSCF. This information is sent over SIP in the Request-URI header. This AVP is not available in the CCR (Initial) request but is available in the CCR (Update) and CCR (Terminate) requests. The value of the Charging AVP is not updated during the Charging session.



Table 54 Number-Portability-Routing-Information AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	2024	> 12	UTF8String	10415

In a terminating S-CSCF, this AVP holds information on the Number Portability routing information received in an incoming SIP Request, within the Request-URI header. If present, the AVP is included in all CCR requests (Initial, Update, Terminate) and the value of the Charging AVP is not updated during the Charging session.

The Number Portability routing information is outputted in global format if the Generic Number Portability feature is enabled.

5.2.3.19 Originating-IOI

The *Originating-IOI* AVP, see Table 55, holds the Inter-Operator Identifier (IOI) for the originating network as generated by the S-CSCF in the home network of the originating end user.

Table 55 Originating-IOI AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	839	> 12	UTF8String	10415

The value of this parameter is fetched from the P-Charging-Vector header and is sent in CCR (Initial) if available.

Example

```
home1.se
```

5.2.3.20 Originator

The *Originator* AVP, see Table 56, indicates the originating party of the message body.

Table 56 Originator AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	864	16	Enumerated	10415

Defined values:

- Calling Party 0
- Called Party 1

5.2.3.21 PS-Information

The *PS-Information* AVP, see Table 57, is used to carry additional 3GPP PS-specific information.

Table 57 *PS-Information AVP*

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	874	> 24	Grouped	10415

Grammar:

```
< PS-Information > ::= < AVP Header: 874 >
                        [ 3GPP-SGSN-MCC-MNC ]
```

5.2.3.22 Reporting-Reason

The *Reporting-Reason* AVP, see Table 58, specifies the reason for usage reporting for one type of quota.

Table 58 *Reporting-Reason AVP*

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	872	16	Enumerated	10415

Defined values:

- Not used 0–1
- FINAL 2
Indicates a normal PDP context termination.
- UOTA_EXHAUSTED 3
Indicates that a particular quota type in *Used-Service-Units* AVP has been exhausted.
- VALIDITY_TIME 4
Indicates that the reason for *Reporting-Reason* is that the credit authorization lifetime provided in the *Validity-Time* AVP has expired.
- Not used 5
- RATING_CONDITION_CHANGE 6
Indicates that a change has happened in some of the rating conditions that were previously armed through the *Trigger-Type* AVP. The specific condition that has changed is indicated in an associated *Trigger-Type* AVP.

- Not used 7–8

Note: The Reporting-Reason AVP is set to **VALIDITY_TIME** when the validity timer expires.

5.2.3.23

Role-of-Node

The Role-of-Node AVP, see Table 59, specifies the role of the S-CSCF.

Table 59 Role-of-Node AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	829	16	Enumerated	10415

The identifier can be one of the following:

- ORIGINATING_ROLE 0
- TERMINATING_ROLE 1
- Not used 2–3

The value of Role-of-Node does not change with the direction of the current SIP dialogue.

5.2.3.24

SDP-Media-Component

The SDP-Media-Component AVP, see Table 60, contains information about media used for an IMS session. The SDP-Media-Component is only in CCRs triggered by SIP requests containing SDP data.

Table 60 SDP-Media-Component AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	843	> 24	Grouped	10415

Grammar:

```
< SDP-Media-Component > ::= < AVP Header: 843 >
    [ SDP-Media-Name ]
    * [ SDP-Media-Description ]
```

5.2.3.25

SDP-Media-Description

The SDP-Media-Description AVP, see Table 61, holds the content of an attribute-line (i=, c=, b=, k=, a=, and so on) related to a media component, as described in the [RFC 3261 Session Initiation Protocol](#) specification.

Table 61 SDP-Media-Description AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	845	> 12	UTF8String	10415

The attributes are specifying the media described in the `SDP-Media-Name` AVP.

5.2.3.26

SDP-Media-Name

The `SDP-Media-Name` AVP, see Table 62, holds the content of an “m=” line in the SDP data.

Table 62 SDP-Media-Name AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	844	> 12	UTF8String	10415

Example

```
m=audio 5002 RTP/AVP 109
```

5.2.3.27

SDP-Session-Description

The `SDP-Session-Description` AVP, see Table 63, holds the content of an attribute-line (i=, c=, b=, k=, a=, and so on) related to a session, as described in the [RFC 2327 SDP Session Description Protocol](#) specification.

Table 63 SDP-Session-Description AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	842	> 12	UTF8String	10415

`SDP-Session-Description` is only in CCRs triggered by SIP requests containing SDP data.

Example

```
a=rtpmap:109 AMR/8000/1
```

5.2.3.28

Service-Information

The purpose of the `Service-Information` AVP, see Table 64, is to allow the transmission of additional 3GPP service-specific information elements.



Table 64 Service-Information AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	873	> 24	Grouped	10415

Grammar:

```
< Service-Information > ::= < AVP Header: 873 >
                        [ PS-Information ]
                        [ IMS-Information ]
```

5.2.3.29

SIP-Method

The SIP-Method AVP, see Table 65, holds the name of the SIP Method (INVITE, UPDATE, and so on) causing a Credit Control Request to be sent to OCS.

Table 65 SIP-Method AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	824	> 12	UTF8String	10415

5.2.3.30

SIP-Request-Timestamp

The SIP-Request-Timestamp AVP, see Table 66, holds the time when the triggering SIP INVITE is received in UTC format; expressed in seconds since January 1 1900 00:00 UTC. The same time stamp value is sent throughout the Credit Control session.

Table 66 SIP-Request-Timestamp AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	834	16	Time	10415

5.2.3.31

SIP-Response-Timestamp

The SIP-Response-Timestamp AVP, see Table 67, holds the time when 200 (OK) for the triggering SIP INVITE is received in UTC format; expressed in seconds since January 1 1900 00:00 UTC. The same time stamp value is sent throughout the Credit Control session.

Table 67 SIP-Response-Timestamp AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	835	16	Time	10415

5.2.3.32 Terminating-IOI

The *Terminating-IOI* AVP, see Table 68, holds the Inter-Operator Identifier (IOI) for the terminating network as generated by the S-CSCF in the home network of the terminating end user. The value of this AVP is fetched from the *P-Charging-Vector* header by the originating S-CSCF.

Table 68 *Terminating-IOI AVP*

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	840	> 12	UTF8String	10415

The terminating S-CSCF includes this AVP in CCR (*Initial*). The originating S-CSCF is not able to include it until CCR (*Update*) or CCR (*Terminate*). In all cases, it is only sent once during a Credit Control session.

Example

```
home1.se
```

5.2.3.33 Time-Stamps

The *Time-Stamps* AVP, see Table 69, holds the time of the SIP request (for example, *Invite*, *Update*) and the time of the response to that SIP Request.

Table 69 *Time-Stamps AVP*

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	833	>= 28	Grouped	10415

Grammar:

```
< Time-Stamps > ::= < AVP Header: 833 >
    [ SIP-Request-Timestamp ]
    [ SIP-Response-Timestamp ]
```

5.2.3.34 Trigger-Type

The *Trigger-Type* AVP, see Table 70, is used to indicate a single reauthorization event type. Only events included CCA in *Trigger-Type* AVP are to reauthorize the associated quota. The *Trigger-Type* AVP included in CCR indicates the specific event which caused the reauthorization request of the *Reporting-Reason* with value *RATING_CONDITION_CHANGE* associated.



Table 70 Time-Stamped AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	870	12	Enumerated	10415

Defined values:

- CHANGE-IN-MEDIA-COMPOSITION 40

This value is used to indicate that a change in the media composition, as identified within SDP, for an existing SIP session causes the credit control client to ask for a reauthorization of the associated quota.

- Any value other than 40 is ignored if received.

5.2.3.35

User-Session-ID

The `User-Session-Id` AVP, see Table 71, holds the session identifier, the SIP Call ID.

Table 71 User-Session-ID AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	830	> 12	UTF8String	10415

The value of this AVP is fetched from the `Call-ID` header and does not change during the Charging session.

Example

```
0014f2e9-7d990017-63999cc2-05b5507d@86.224.4.130
```

5.2.4

Ericsson Vendor-Specific AVPs

5.2.4.1

Called-Party-Original-Address

The `Called-Party-Original-Address` AVP, see Table 72, identifies the destination as received by the S-CSCF from the end user or an Application Server. The AVP is present only when the address in the received `Request-URI` is modified before it is sent out.

Table 72 Called-Party-Original-Address AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	286	> 12	UTF8String	193

The value of `Called-Party-Original-Address` does not change during the Charging session.

Since the `Called-Party-Original-Address` AVP is only valid on the originating side, it is not sent in a terminating Charging session.

5.2.4.2 Dial-Around-Indicator

The `Dial-Around-Indicator` AVP, see Table 73, identifies how the carrier specified in the `Carrier-Select-Routing-Information` AVP was selected. The value of the `DAI` parameter is included in this AVP.

Table 73 *Dial-Around-Indicator AVP*

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	1160	> 12	UTF8String	193

The possible values of the AVP are identified in the [Internet Draft: DAI Parameter for the "tel" URI](#) specification.

If the CSCF receives a `DAI` parameter from the application server, it inserts the value into the AVP without modify it. If the CSCF receives a `CIC` parameter from an ENUM server, it adds a `DIA` parameter with the value of operator.

5.2.4.3 Ericsson-Service-Information

The `Ericsson-Service-Information` AVP, see Table 74, contains vendor-specific AVPs used in Ericsson IMS solutions.

Table 74 *Ericsson-Service-Information AVP*

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	285	> 24	Grouped	193

Grammar:

```
< Ericsson-Service-Information > ::= < AVP Header: 285, Vendor Id: 193 >
* [ IMS-Service-Identification ]
[ Called-Party-Original-Address ]
[ Dial-Around-Indicator ]
[ Authentication-Method ]
[ SIP-Request-Timestamp-Fraction ]
[ SIP-Response-Timestamp-Fraction ]
[ Disconnect-Direction ]
* [ Transaction-Info ]
```

5.2.4.4 Authentication-Method

The Authentication-Method AVP, see Table 75, identifies the Authentication Method of the originating subscriber.

Table 75 Authentication-Method AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	1261	16	Enumerated	193

This AVP is only contained in the CCR triggered by the Requests in the originating half call. The possible values for Authentication type are as follows:

- NoAuthentication 0
- AkaAuthentication 1
- NassBundledAuthentication 2
- DigestAuthentication 3
- GibaAuthentication 4

Note: The Authentication type NoAuthentication represents two cases: authentication disabled in the CSCF node and authentication enabled but performed in a trusted gateway. DigestAuthentication includes Digest authentication on first REGISTER without SIP Authorization header and Optimized Digest authentications.

5.2.4.5 SIP-Request-Timestamp-Fraction

The SIP-Request-Timestamp-Fraction AVP, see Table 76, holds the milliseconds fraction in relation to SIP-Request-Timestamp. Together with SIP-Request-Timestamp, these two AVPs represent the number of seconds and milliseconds since January 1 1900 00:00 UTC.

Table 76 SIP-Request-Timestamp-Fraction AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	2301	16	Unsigned32	10415

Example

CE8117BE

5.2.4.6 SIP-Response-Timestamp-Fraction

The SIP-Response-Timestamp-Fraction AVP, see Table 77, holds the milliseconds fraction in relation to SIP-Response-Timestamp. Together

with `SIP-Response-Timestamp`, these two AVPs represent the number of seconds and milliseconds since January 1 1900 00:00 UTC.

Table 77 SIP-Response-Timestamp-Fraction AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	2302	16	Unsigned32	10415

Example

CE8117BC

5.2.4.7

Transaction-Info

The `Transaction-Info` is a grouped AVP, see Table 78, including the following AVPs:

- `Transaction-Type` AVP which contains the type of transaction in interest
- `Transaction-Data-Name` AVP which contains the Name of the transaction data
- `Transaction-Data-Value` AVP which contains the value of the transaction data named in `Transaction-Data-Name` AVP

Table 78 Transaction-Info AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	1264	>52	Grouped	193

Grammar:

```
< Transaction-Info > ::=
  < AVP Header: 1264, Vendor Id: 193 >
    { Transaction-Type }
    { Transaction-Data-Name }
    1 * { Transaction-Data-Value }
```

5.2.4.8

Transaction-Type

The `Transaction-Type`, see Table 79, is the type of transaction the related information is captured from. It is an `Enumerated` AVP.

Table 79 Transaction-Type AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	1265	16	Enumerated	193

Defined values:

- SIP Request 0
- SIP Response 1

5.2.4.9 Transaction-Data-Name

The `Transaction-Data-Name` AVP, see Table 80, identifies the name of the selected data, typically a header, or an element in a message.

Table 80 Transaction-Data-Name AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	1266	>12	UTF8String	193

Example

Contact

5.2.4.10 Transaction-Data-Value

The `Transaction-Data-Value` AVP, see Table 81, contains the value of the selected data based on `Transaction-Data-Name`.

Table 81 Transaction-Data-Value AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	1267	>12	UTF8String	193

Example

sip:bob@192.0.100.2

5.2.4.11 Event-NTP-Timestamp

The `Event-NTP-Timestamp` AVP is shown in Table 82.

Table 82 Event-NTP-Timestamp AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	340	20	OctetString	193

This is a timestamp recorded when the event that caused the ACR message to be sent was received in the S-CSCF. The value represents the number of seconds and milliseconds since January 1 1900 00:00 UTC. The integer part is

in the first four octets and the fraction part is in the last four octets. The format of the AVP is according to the NTP format as specified by [RFC 2030](#).

Example

```
095c90c780000000
```

5.2.4.12 GPRS-Roaming-Status

The `GPRS-Roaming-Status`, see Table 83, is used to indicate if the user is attached to the home network or not.

Table 83 *GPRS-Roaming-Status AVP*

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	333	16	Enumerated	193

Values downloaded from the HSS:

- HOME 0
- VISITED 1

5.2.4.13 IMS-Service-Identification

The `IMS-Service-Identification` AVP, see Table 84, identifies the Communication Service or IMS Port related to a session.

Table 84 *IMS-Service-Identification AVP*

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	284	> 12	UTF8String	193

One AVP is generated for each feature tag starting with “+g.” or “+u.” received in the `Accept-Contact` header of the SIP message. Feature tags are not always available, it depends on the actual service or terminal used, and therefore controls the presence of this AVP.

Example

```
+g.ims.mmtel
```

5.2.4.14 Quota-Deduction-Start

`Quota-Deduction-Start` indicates the SIP event that triggered the CSCF to start deduction of the granted quota, see Table 85.



Table 85 Quota-Deduction-Start AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	339	16	Enumerated	193

Defined values:

- SIP-INVITE 0
- SIP-180-Ringing 1
- SIP-200OK 2

5.2.4.15

SIP-Reason

The SIP-Reason AVP, see Table 86, contains parameters from the SIP Reason header occurs in SIP BYE and SIP CANCEL requests.

Table 86 SIP-Reason AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	335	> 40	Grouped	193

SIP Reason Header Field is defined in the [RFC 4006 Diameter Credit-Control Application](#) specification.

Grammar:

```
< SIP-Reason > := < AVP Header: xxx, Vendor Id: 193 >
                  [ SIP-Reason-Cause ]
                  [ SIP-Reason-Text ]
```

5.2.4.16

SIP-Reason-Cause

The SIP-Reason-Cause AVP, see Table 87, contains the value of the cause parameter in the Reason header.

Table 87 SIP-Reason-Cause AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	336	16	Unsigned32	193

5.2.4.17

SIP-Reason-Text

The SIP-Reason-Text, see Table 88, contains the value of the reason-text parameter in the SIP Reason header.

Table 88 SIP-Reason-Text AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	337	> 12	UTF8String	193

5.2.4.18

SIP-Ringing-Timestamp

The `SIP-Ringing-Timestamp` AVP, see Table 89, contains the time on reception of SIP 180 (Ringing). The given time is expressed in seconds since January 1 1900 00:00 UTC.

Table 89 SIP-Ringing-Timestamp AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	338	16	Time	193

5.2.4.19

Disconnect-Direction

The `Disconnect-Direction` AVP, see Table 90, reports which side, calling or called, initiated the termination of the session, or whether it was the reporting node itself that initiated the termination.

Table 90 Disconnect-Direction AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	1305	16	Enumerated	193

Defined values:

- Originating side 0
- Terminating side 1
- Network 2



6 Security Considerations

6.1 IPsec Tunnel

The communication between the S-CSCF and the Charging system can be further secured using IPsec (Zb interface) on the IP transport layer, refer to the [3GPP TS 33.210 3G security; Network Domain Security \(NDS\); IP network layer security](#) specification.

IP Security (IPsec) tunnels can be defined between the two nodes. Internet Key Exchange version 1 (IKEv1) performs mutual authentication between the two nodes and establishes an IKE Security Association that includes shared secret information used to establish IPsec Security Associations (SAs). Different forms of authentication and encryptions can be selected when defining the IPsec tunnels. For the native CSCF, refer to *Security Management User Guide*, and for the virtual CSCF, refer to *eVIP Management Guide*.





7 Related Standards

This section states the related standards and explains any deviations from them.

The online charging implementation is fully compliant with the mandatory parts of the following specifications:

- [RFC 3588 Diameter Base Protocol](#)
- [RFC 4006 Diameter Credit-Control Application](#)
- [3GPP TS 32.299 v6.8.0 Diameter Charging Applications](#)
- [3GPP TS 32.260 v6.7.0 IP Multimedia Subsystem \(IMS\) Charging](#)

All other parts that are relevant for the Online Charging Function in the S-CSCF are supported with the following comments:

- RFC 3588:
 - TLS is not supported.
 - Diameter commands RAR code 258, STR code 275, and ASR code 274 are not supported.
- RFC 4006:
 - Multiple Services: The AVPs for multiple services are used but the S-CSCF can at this stage only handle one service at a time.
 - Service identification: The `Service-Identifier` AVP has a static value, included only as it is required by the RFC. The actual service identification is performed by the charging system using the vendor-specific `IMS-Service-Identification` AVP and data from the AVPs with SDP information.
- 3GPP TS 32.260 and 3GPP TS 32.299:
 - The two specifications are not aligned with each other. The structure and handling of CCR/CCA is taken from 3GPP TS 32.260 and the definition of the relevant AVPs is taken from 3GPP TS 32.299.

Of the AVPs listed in Table 6.4.2 in 3GPP TS 32.299 and not marked as “Not used”, the following AVPs are not supported:

- AVP
- CC-Input-Octets
- CC-Output-Octets

- CC-Total-Octets
- Origin-State-Id
- Proxy-Host
- Proxy-Info
- Proxy-State
- Rating-Group
- Requested-Action
- Route-Record
- User-Equipment-Info
- User-Equipment-Info-Type
- User-Equipment-Info-Value

Immediate Event Charging (IEC) is not supported.

Reauthorization mechanism is not supported.

The failover mechanism triggered by the CC-Session-Failover AVP is not supported. See Section 3.1 Error Handling on page 8 for information about the existing failover mechanism.

The AVPs Carrier-Select-Routing-Information and Number-Portability-Routing-Information are extracted from table 7.2 in the [3GPP TS 32.299 v8.2.0 Diameter Charging Applications](#) specification.

The AVP grammar used in this document is compliant to the [RFC 3588 Diameter Base Protocol](#) specification.