

ETSI TS 132 299 V7.4.0 (2006-12)

Technical Specification

**Universal Mobile Telecommunications System (UMTS);
Telecommunication management;
Charging management;
Diameter charging applications
(3GPP TS 32.299 version 7.4.0 Release 7)**



Reference

RTS/TSGS-0532299v740

Keywords

UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:

<http://www.etsi.org>

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at

<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, please send your comment to one of the following services:

http://portal.etsi.org/chaicor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2006.
All rights reserved.

DECTTM, **PLUGTESTS**TM and **UMTS**TM are Trade Marks of ETSI registered for the benefit of its Members.
TIPHONTM and the **TIPHON logo** are Trade Marks currently being registered by ETSI for the benefit of its Members.
3GPPTM is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<http://webapp.etsi.org/IPR/home.asp>).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under <http://webapp.etsi.org/key/queryform.asp>.

Contents

Intellectual Property Rights	2
Foreword.....	2
Foreword.....	8
1 Scope	9
2 References	9
3 Definitions, symbols and abbreviations	11
3.1 Definitions	11
3.2 Symbols.....	11
3.3 Abbreviations	11
4 Architecture Considerations	12
4.1 High level architecture	12
4.1.1 Charging related transfer requirements.....	13
5 3GPP charging applications requirements.....	14
5.1 Offline Charging Scenarios	14
5.1.1 Basic Principles	14
5.1.1.1 Event based charging	14
5.1.1.2 Session based charging	15
5.1.2 Basic Operation	16
5.2 Online Charging scenarios	18
5.2.1 Basic principles.....	18
5.2.2 Charging Scenarios	18
5.2.2.1 Immediate Event Charging	19
5.2.2.1.1 Decentralized Unit Determination and Centralized Rating	19
5.2.2.1.2 Centralized Unit Determination and Centralized Rating	20
5.2.2.1.3 Decentralized Unit Determination and Decentralized Rating.....	21
5.2.2.1.4 Further Options.....	22
5.2.2.2 Event charging with Reservation	23
5.2.2.2.1 Decentralized Unit Determination and Centralized Rating	23
5.2.2.2.2 Centralized Unit Determination and Centralized Rating	25
5.2.2.2.3 Decentralized Unit Determination and Decentralized Rating.....	27
5.2.2.3 Session charging with Reservation	29
5.2.2.3.1 Decentralized Unit Determination and Centralized Rating	29
5.2.2.3.2 Centralized Unit Determination and Centralized Rating	31
5.2.2.3.3 Decentralized Unit Determination and Decentralized Rating.....	33
5.2.3 Basic Operations.....	34
5.3 Other requirements	36
5.3.1 Re-authorization	36
5.3.2 Threshold based re-authorization triggers.....	36
5.3.3 Termination action.....	36
6 3GPP Charging Applications – Protocol Aspects	37
6.1 Basic Principles for Diameter Offline Charging	37
6.1.1 Event based charging	38
6.1.2 Session based charging	39
6.1.3 Offline charging error cases - Diameter procedures	40
6.1.3.1 CDF Connection Failure	40
6.1.3.2 No Reply from CDF.....	40
6.1.3.3 Duplicate Detection.....	40
6.1.3.4 CDF Detected Failure	40
6.2 Message Contents for Offline Charging	41
6.2.1 Summary of Offline Charging Message Formats	41
6.2.1.1 General	41
6.2.1.2 Structure for the Accounting Message Formats	41

6.2.2	Accounting-Request Message.....	41
6.2.3	Accounting-Answer Message	43
6.3	Basic Principles for Diameter Online charging	45
6.3.1	Online Specific Credit Control Application Requirements.....	45
6.3.2	Diameter Description on the Ro reference point.....	45
6.3.2.1	Basic Principles.....	45
6.3.3	Immediate Event Charging (IEC).....	46
6.3.4	Event Charging with Unit Reservation (ECUR).....	47
6.3.5	Session Charging with Unit Reservation (SCUR)	49
6.3.6	Error Cases and Scenarios	50
6.3.6.1	Duplicate Detection.....	50
6.3.6.2	Reserve Units and Debit Units Operation Failure	50
6.3.7	Support of Tariff Changes during an Active User Session	51
6.3.7.1	Support of Tariff Changes using the Tariff Switch Mechanism.....	51
6.3.7.2	Support of Tariff Changes using Validity Time AVP	51
6.3.8	Support of Re-authorization	51
6.3.9	Support of Failure Handling	51
6.3.10	Support of Failover	51
6.3.11	Credit Pooling.....	52
6.4	Message formats for Online Charging.....	52
6.4.1	Summary of Online Charging Message Formats	52
6.4.1.1	General	52
6.4.1.2	Structure for the Credit Control Message Formats.....	53
6.4.2	Credit-Control-Request Message	53
6.4.3	Credit-Control-Answer Message	56
6.4.4	Re-Auth-Request Message	59
6.4.5	Re-Auth-Answer Message	60
6.4.6	Capabilities-Exchange-Request Message	60
6.4.7	Capabilities-Exchange-Answer Message.....	60
6.4.8	Device-Watchdog-Request Message	60
6.4.9	Device-Watchdog-Answer Message.....	60
6.4.10	Disconnect-Peer-Request Message.....	60
6.4.11	Disconnect-Peer-Answer Message	60
6.4.12	Abort-Session-Request Message	60
6.4.13	Abort-Session -Answer Message.....	61
6.5	Other procedural description of the 3GPP charging applications.....	61
6.5.1	Re-authorization	61
6.5.1.1	Idle timeout	61
6.5.1.2	Change of charging conditions.....	61
6.5.1.3	Reporting quota usage.....	61
6.5.2	Threshold based re-authorization triggers.....	61
6.5.3	Termination action	62
6.5.4	Quota consumption time	62
6.5.5	Service Termination.....	62
6.6	Bindings of the operation to protocol application	62
6.6.1	Bindings of Charging Data Transfer to Accounting	63
6.6.2	Bindings of Debit / Reserve Units to Credit-Control.....	63
7	Summary of used Attribute Value Pairs.....	64
7.1	Diameter AVPs	64
7.1.1	Acct-Application-Id AVP	65
7.1.2	Auth-Application-Id AVP.....	65
7.1.3	Event-Timestamp AVP.....	66
7.1.4	Multiple-Services-Credit-Control	66
7.1.5	Rating-Group AVP	66
7.1.6	Result-Code AVP	66
7.1.7	Service-Context-Id AVP.....	67
7.1.8	Service-Identifier AVP	67
7.1.8A	Used-Service-Unit AVP	68
7.1.9	User-Name AVP.....	68
7.1.10	Vendor-Id AVP.....	68
7.2	3GPP specific AVPs.....	68

7.2.1	Adaptations AVP	71
7.2.1A	Access-Network-Information AVP	72
7.2.2	Additional-Content-Information AVP	72
7.2.3	Additional-Type-Information AVP	72
7.2.4	Address-Data AVP	72
7.2.5	Address-Domain AVP	72
7.2.6	Address-Type AVP	72
7.2.7	Addressee-Type AVP	73
7.2.8	Applic-ID AVP	73
7.2.9	Additional-Content-Information AVP	73
7.2.10	Application-provided-Called-Party-Address AVP	73
7.2.11	Application-Server AVP	73
7.2.12	Application-Server-Information AVP	73
7.2.13	Associated-URI AVP	74
7.2.14	Authorised-QoS AVP	74
7.2.15	Aux-Applic-Info AVP	74
7.2.16	Bearer-Service AVP	74
7.2.17	Called-Asserted-Identity AVP	74
7.2.18	Called-Party-Address AVP	74
7.2.19	Calling-Party-Address AVP	74
7.2.20	Cause-Code AVP	74
7.2.21	CG-Address AVP	76
7.2.22	Charged-Party AVP	76
7.2.23	Charging-Rule-Base-Name AVP	76
7.2.24	Class-Identifier AVP	76
7.2.25	Content-Class AVP	76
7.2.26	Content-Disposition AVP	77
7.2.27	Content-Length AVP	77
7.2.28	Content-Size AVP	77
7.2.29	Content-Type AVP	77
7.2.30	Deferred-Location-Event-Type AVP	77
7.2.31	Delivery-Report-Requested AVP	77
7.2.32	Domain-Name AVP	77
7.2.33	DRM-Content AVP	77
7.2.34	Event AVP	77
7.2.34A	Event-Charging-TimeStamp AVP	78
7.2.35	Event-Type AVP	78
7.2.36	Expires AVP	78
7.2.37	File-Repair-Supported AVP	78
7.2.38	GGSN-Address AVP	78
7.2.39	IMS-Charging-Identifier (ICID) AVP	78
7.2.40	IMS-Information AVP	78
7.2.41	Incoming-Trunk-Group-ID AVP	79
7.2.42	Inter-Operator-Identifier AVP	79
7.2.43	LCS-APN AVP	79
7.2.44	LCS-Client-Dialed-By-MS AVP	79
7.2.45	LCS-Client-External-ID AVP	79
7.2.46	LCS-Client-ID AVP	79
7.2.47	LCS-Client-Name AVP	80
7.2.48	LCS-Client-Type AVP	80
7.2.49	LCS-Data-Coding-Scheme AVP	80
7.2.50	LCS-Format-Indicator AVP	80
7.2.51	LCS-Information AVP	80
7.2.52	LCS-Name-String AVP	81
7.2.53	LCS-Requestor-ID AVP	81
7.2.54	LCS-Requestor-ID-String AVP	81
7.2.55	Location-Estimate AVP	81
7.2.56	Location-Estimate-Type AVP	81
7.2.57	Location-Type AVP	81
7.2.58	MBMS-Information AVP	81
7.2.59	MBMS-User-Service-Type AVP	82
7.2.60	Media-Initiator-Flag AVP	82

7.2.61	Message-Body AVP	82
7.2.62	Message-Class AVP	82
7.2.63	Message-ID AVP	83
7.2.64	Message-Size AVP	83
7.2.65	Message-Type AVP	83
7.2.66	MM-Content-Type AVP	83
7.2.67	MMBox-Storage-Requested AVP	84
7.2.68	MMS-Information AVP	84
7.2.69	Node-Functionality AVP	84
7.2.70	Number-Of-Participants AVP	84
7.2.71	Originating-IOI AVP	85
7.2.72	Originator AVP	85
7.2.73	Originator-Address AVP	85
7.2.74	Outgoing-Trunk-Group-ID AVP	85
7.2.75	Participants-Involved AVP	85
7.2.75A	Participants-Group AVP	86
7.2.75B	Participant-Access-Priority AVP	86
7.2.76	PDG-Address AVP	86
7.2.77	PDG-Charging-Id AVP	86
7.2.78	PDP-Address AVP	86
7.2.79	PDP-Context-Type AVP	86
7.2.80	PoC-Change-Condition AVP	87
7.2.81	PoC-Change-Time AVP	87
7.2.82	PoC-Controlling-Address AVP	87
7.2.83	PoC-Group-Name	87
7.2.84	PoC-Information AVP	87
7.2.85	PoC-Server-Role AVP	87
7.2.86	PoC-Session-Id AVP	88
7.2.87	PoC-Session-Type AVP	88
7.2.87A	PoC-User-Role AVP	88
7.2.87B	PoC-User-Role-IDs AVP	88
7.2.87C	PoC-User-Role-info-Units AVP	88
7.2.88	Positioning-Data AVP	88
7.2.89	Priority AVP	88
7.2.90	PS-Append-Free-Format-Data AVP	89
7.2.91	PS-Free-Format-Data AVP	89
7.2.92	PS-Furnish-Charging-Information AVP	89
7.2.93	PS-Information AVP	89
7.2.94	Quota-Consumption-Time AVP	90
7.2.95	Quota-Holding-Time AVP	90
7.2.96	Read-Reply-Report-Requested AVP	90
7.2.97	Recipient-Address AVP	90
7.2.98	Reply-Applic-ID AVP	90
7.2.99	Reporting-Reason AVP	91
7.2.100	Requested-Party-Address AVP	92
7.2.101	Role-of-node AVP	92
7.2.102	SDP-Media-Component AVP	92
7.2.103	SDP-Media-Description AVP	92
7.2.104	SDP-Media-Name AVP	93
7.2.105	SDP-Session-Description AVP	93
7.2.106	Served-Party-IP-Address AVP	93
7.2.107	Service-ID AVP	93
7.2.107A	Service-Generic-Information AVP	93
7.2.108	Service-Information AVP	93
7.2.109	Service-Specific-Data AVP	93
7.2.109A	Service-Specific-Info AVP	94
7.2.109B	Service-Specific-Type AVP	94
7.2.110	SGSN-Address AVP	94
7.2.111	SIP-Method AVP	94
7.2.112	SIP-Request-Timestamp AVP	94
7.2.113	SIP-Response-Timestamp AVP	94
7.2.114	Submission-Time AVP	94

7.2.115	Talk-Burst-Exchange AVP	94
7.2.116	Terminating-IOI AVP	95
7.2.117	Time-Quota-Threshold AVP	95
7.2.118	Time-Stamps AVP	95
7.2.119	Token-Text AVP	95
7.2.120	Trigger-Type AVP	95
7.2.121	Trunk-Group-ID AVP	98
7.2.122	Type-Number AVP	98
7.2.123	Unit-Quota-Threshold AVP	98
7.2.124	User-Session-ID AVP	98
7.2.125	Volume-Quota-Threshold AVP	98
7.2.126	WAG-Address AVP	98
7.2.127	WAG-PLMN-Id AVP	98
7.2.128	WLAN-Information AVP	99
7.2.129	WLAN-Radio-Container AVP	99
7.2.130	WLAN-Session-Id AVP	99
7.2.131	WLAN-Technology AVP	99
7.2.132	WLAN-UE-Local-IPAddress AVP	99
Annex A (informative):	Bibliography	100
Annex B (informative):	Change history	101
History		103

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
 - 1 presented to TSG for information;
 - 2 presented to TSG for approval;
 - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document is part of a series of documents that specify charging functionality and charging management in GSM/UMTS networks. The GSM/UMTS core network-charging architecture and principles are specified in 3GPP TS 32.240 [1], which provides an umbrella for other charging management documents that specify.

- The content of the CDRs' per domain and subsystem (offline charging);
- The content of real-time charging messages per domain / subsystem (online charging);
- The functionality of online and offline charging for those domains and subsystems;
- The interfaces that are used in the charging framework to transfer the charging information (i.e. CDRs or charging events).

The complete document structure for these TSs is defined in 3GPP TS 32.240 [1].

The present document specifies in detail the Diameter based offline and online charging applications for 3GPP networks. It includes all charging parameters, scenarios and message flows..

All terms, definitions and, abbreviations used in the present document, that are common across 3GPP TSs, are defined in 3GPP TR 21.905 [50]. Those that are common across charging management in GSM/UMTS domains, services or subsystems are provided in the umbrella document 3GPP TS 32.240 [1] and are copied into clause 3 of the present document for ease of reading. Finally, those items that are specific to the present document are defined exclusively in the present document.

Furthermore, requirements that govern the charging work are specified in 3GPP TS 22.115 [102].

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

- [1] 3GPP TS 32.240: "Telecommunication management; Charging management; Charging Architecture and Principles".
- [2]-[49] Void.
- [50] 3GPP TR 21.905: 'Vocabulary for 3GPP Specifications'
- [51]-[199] Void.
- [200] 3GPP TS 23.207: "End to end quality of service concept and architecture".
- [201] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".
- [202] 3GPP TS 24.229: "IP Multimedia Call Control Protocol based on SIP and SDP; Stage 3."
- [203] 3GPP TS 29.207: "Policy control over Go interface".
- [204] 3GPP TS 29.229: "Cx and Dx Interfaces based on the Diameter protocol; Protocol Details".
- [205] 3GPP TS 29.210: "Charging rule provisioning over Gx interface".

- [206] 3GPP TS 29.230: "3GPP specific codes and identifiers".
- [207] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)".
- [208] 3GPP TS 23.140: " Multimedia Messaging Service (MMS); Functional description; Stage 2".
- [209] OMA "Multimedia Messaging Service; Encapsulation Protocol"
- [210] OMNA WSP Content Type Codes database.
<http://www.openmobilealliance.org/tech/omna/omna-wsp-content-type.htm>
- [211] OMA-CP-POC: "OMA PoC Control Plane"
- [212] 3GPP 29.234: "3GPP system to Wireless Local Area Network (WLAN) interworking; Stage 3".
- [213] 3GPP TS 29.140: "MM10 interface based on Diameter protocol; Stage 3".
- [214] 3GPP TS 29.214: "Policy and Charging Control over Rx reference point; Stage 3".
- [215]-[400] Void.
- [401] IETF RFC 3588: "Diameter Base Protocol".
- [402] IETF RFC 4006: "Diameter Credit Control Application"
- [403] IETF Draft, "Carrying Location Objects in RADIUS", draft-ietf-geopriv-radius-lo-04.txt, work in progress
- [404] IETF RFC 3455 , "Private Extensions to the Session Initiation Protocol (SIP) for the 3rd Generation Partnership Projects (3GPP)".
- [405] IETF RFC 3261: "SIP: Session Initiation Protocol".
- [406] IETF Internet-Draft, "SDP: Session Description Protocol".
<http://www.ietf.org/internet-drafts/draft-ietf-mmusic-sdp-new-24.txt>
- [407] IETF RFC 4005: "Diameter Network Access Server Application"

NOTE: The above reference will need to be updated to reference the assigned RFC number, once the draft achieves RFC status within the IETF.

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

offline charging: charging mechanism where charging information **does not** affect, in real-time, the service rendered

online charging: charging mechanism where charging information can affect, in real-time, the service rendered and therefore a direct interaction of the charging mechanism with session/service control is required

Editor's note: Include middle tier TS...

3.2 Symbols

For the purposes of the present document, the following symbols apply:

Rf	Offline Charging Reference Point between a 3G network element and the CDF.
Ro	Online Charging Reference Point between a 3G network element and the OCS.

3.3 Abbreviations

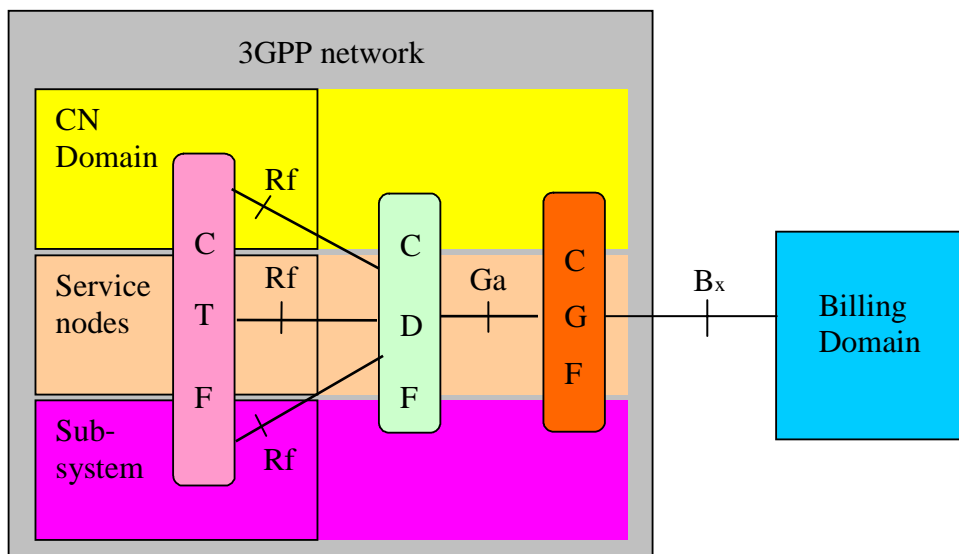
For the purposes of the present document, the following abbreviations apply:

ACA	ACcounting Answer
ACR	ACcounting Request
AS	Application Server
ASA	Abort Session Answer
ASR	Abort Session Request
AVP	Attribute Value Pair
CCA	Credit Control Answer
CCR	Credit Control Request
CDF	Charging Data Function
CDR	Charging Data Record
CI	Cost-Information
DBPA	Diameter Base Protocol Accounting
DPA	Disconnect Peer Answer
DPR	Disconnect Peer Request
ECUR	Event Charging with Unit Reservation
FUI	Final-Unit-Indication
GSU	Granted-Service-Unit
IEC	Immediate Event Charging
IMS	IP Multimedia Subsystem
OCS	Online Charging System
SDP	Session Description Protocol

4 Architecture Considerations

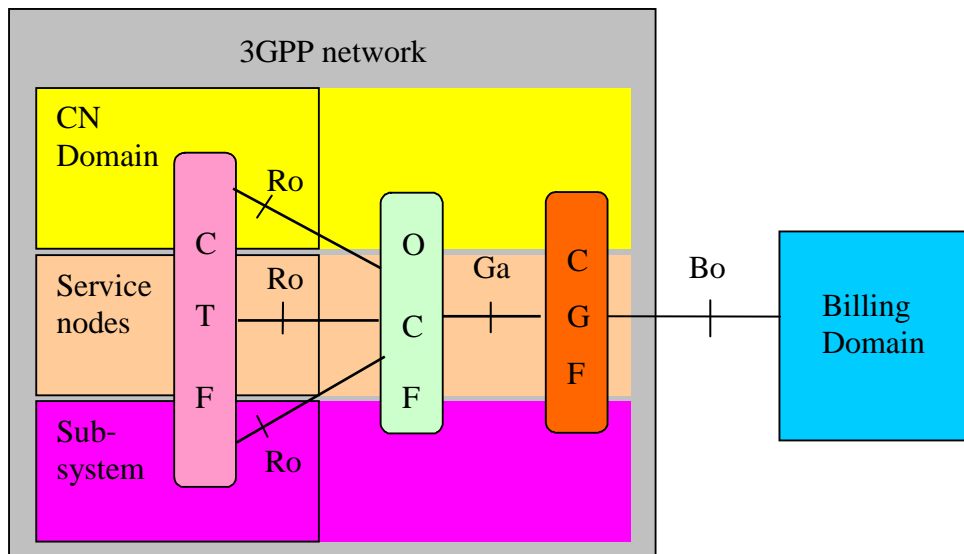
4.1 High level architecture

The Rf and the Ro are reference points from the Charging Trigger Function (CTF) to the Charging Data Function (CDF) and the Online Charging Function (OCF) respectively, and are intended for the transport of charging events. Rf is used for offline charging whereas Ro is used for online charging. The following figures depict the position of the Rf and Ro reference points within the overall 3GPP online and offline charging architecture.



- CTF:** Charging Trigger Function
- CDF:** Charging Data Function
- CGF:** Charging Gateway Function
- BD:** Billing Domain. This may also be a billing mediation device / post-processing system.

Figure 4.1.1: Logical ubiquitous offline charging architecture



- CTF:** Charging Trigger Function
- OCF:** Online Charging Function
- CGF:** Charging Gateway Function
- BD:** Billing Domain. This may also be a billing mediation device / post-processing system.

Figure 4.1.2: Logical ubiquitous online charging architecture

Different mappings of the ubiquitous offline charging functions, CTF, CDF and CGF, onto physical implementations are possible. Further details of the configuration refer to 3GPP TS 32.240 [1]. Details of the implementation options per domain / subsystem / service (usually a subset of the overall possible variants described above) are specified in the respective middle tier TS.

4.1.1 Charging related transfer requirements

Each CTF would have CDF and OCF address list to which it can send its charging events and/or charging requests. The list will be organized in address priority order. If the primary charging function is not available (e.g., out of service) then the CTF shall send the charging information to the secondary charging function and so on.

Within the scope of this release, each network element that generates charging information will send the information only to the charging entities of the same PLMN, and not to charging entities in other PLMNs.

Each CDF in the PLMN may know of other CDFs' network addresses (e.g., for redundancy reasons, to be able to recommend another CDF address with the Redirection Request message). This is achieved by OAM&P configuration facilities that will enable each CDF to have a configurable list of peer CDF addresses.

5 3GPP charging applications requirements

5.1 Offline Charging Scenarios

5.1.1 Basic Principles

Offline charging for both events and sessions between CTF and the CDF is performed using the Rf reference point as defined in TS 32.240[1].

Two basic scenarios are used:

- Event based Charging;
- Session based Charging.

5.1.1.1 Event based charging

In the following scenario, CTF asks the CDF to store event related charging data.

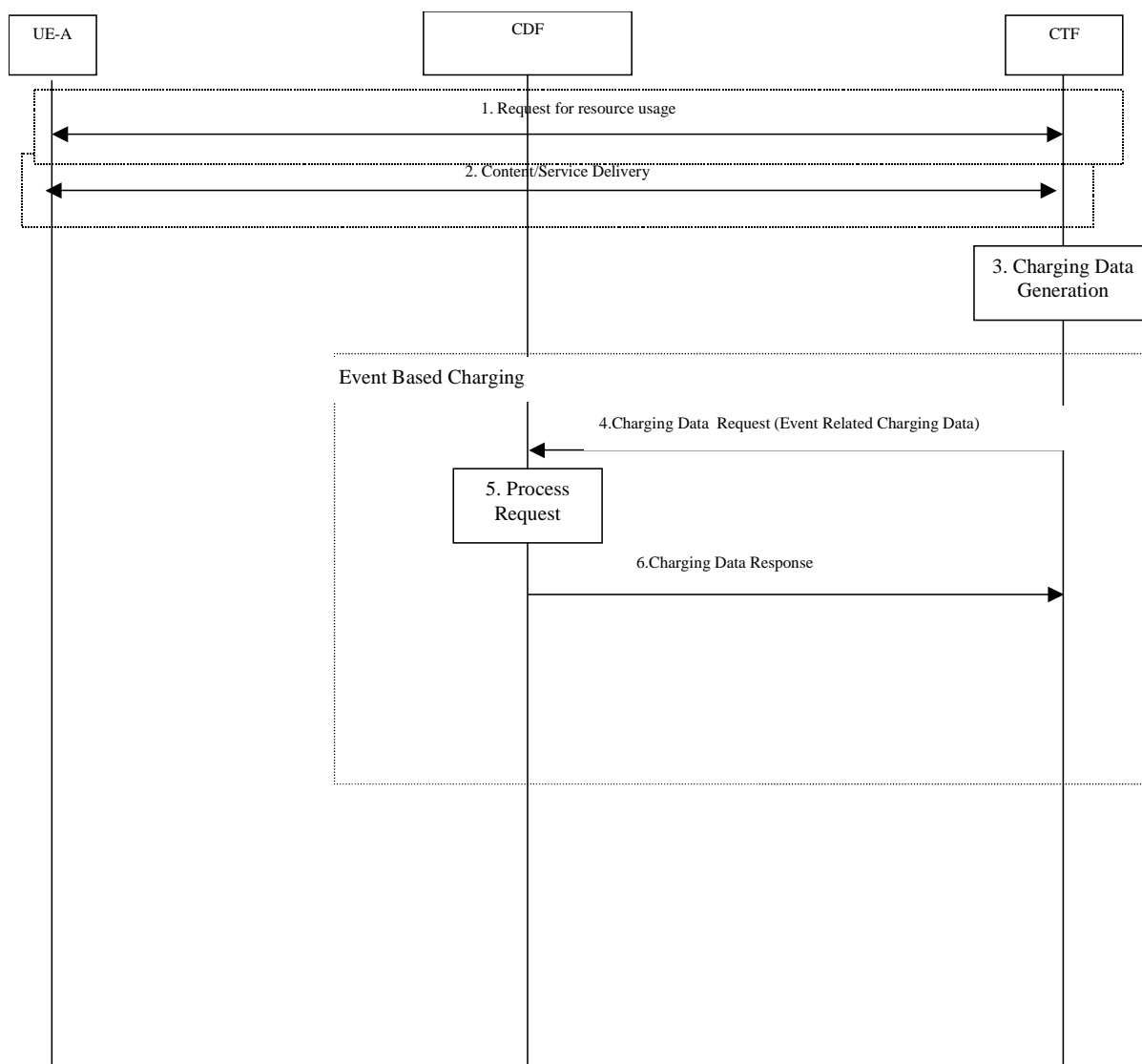


Figure 5.1.1.1: Event Based Charging

1. **Request for resource usage:** UE-A requests the desired resource from the network element.
2. **Content/Service Delivery:** the network element delivers the content/service.
3. **Charging Data Generation:** the CTF generates charging data related to service delivery
4. **Record Charging Data Request:** the CTF requests the CDF to store event related charging data for CDR generation purposes.
5. **Process Request:** CDF stores received information. Whether the CDR is generated or not depends on CDR generation configuration.
6. **Record Charging Data Response:** the CDF informs the CTF that charging data was stored.

5.1.1.2 Session based charging

In the following scenario, CTF asks the CDF to store session related charging data.

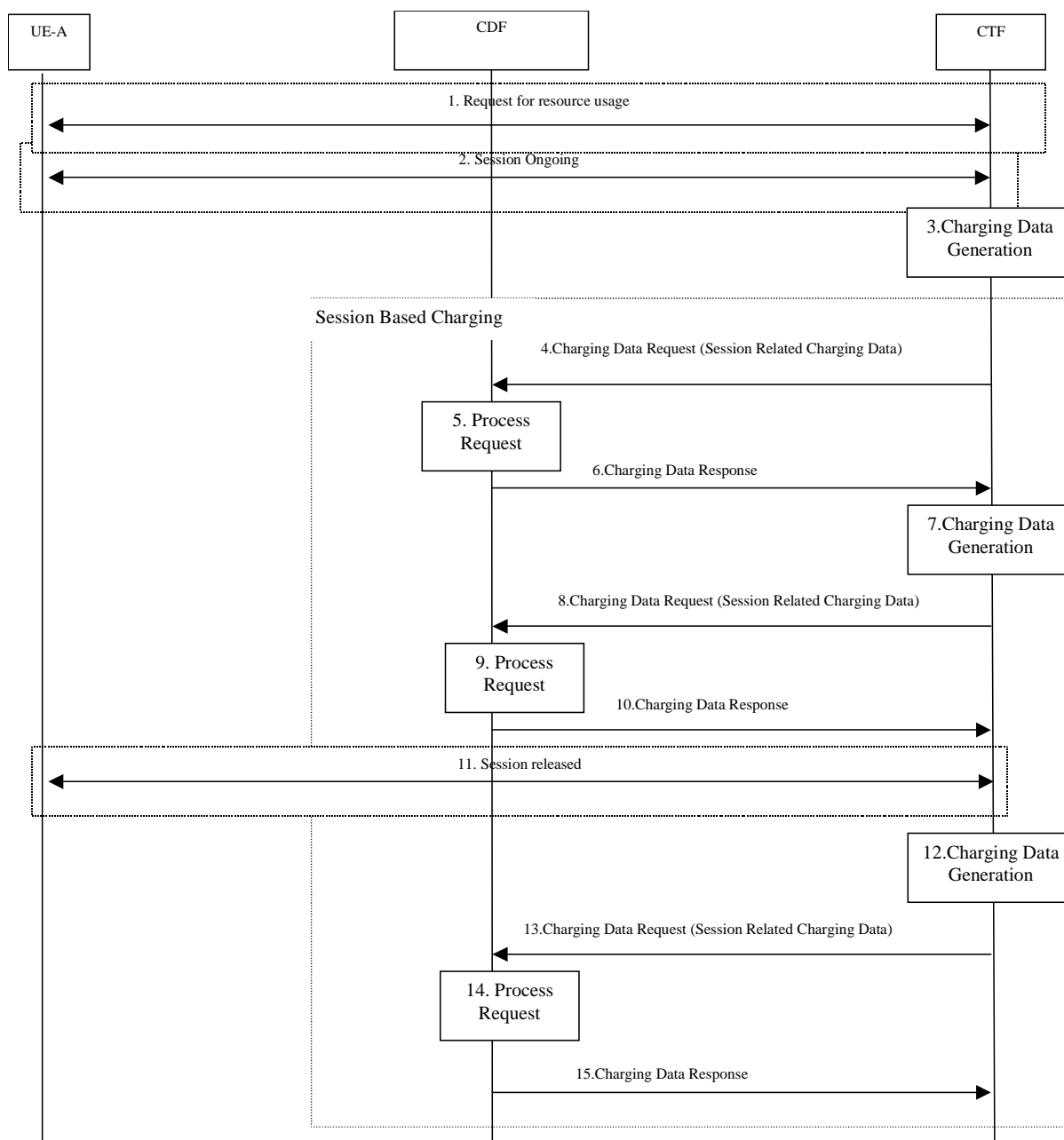


Figure 5.1.1.2: Session based charging

1. **Request for resource usage:** UE-A requests the desired session from the network element.
2. **Session ongoing:** the network element establish the session

3. **Charging Data Generation:** the CTF generates charging data related to session.
4. **Record Charging Data Request:** the CTF requests the CDF to store session related charging data for CDR generation purposes.
5. **Process Request:** CDF stores received information. Whether the CDR is generated or not depends on CDR generation configuration.
6. **Record Charging Data Response:** the CDF informs the CTF that charging data was stored
7. **Charging Data Generation:** the CTF generates charging data related to session due of e.g. intermediate timer expiry
8. **Record Charging Data Request:** the CTF requests the CDF to store session related charging data for CDR generation purposes.
9. **Process Request:** CDF stores received information. Whether the CDR is generated or not depends on CDR generation configuration.
10. **Record Charging Data Response:** the CDF informs the CTF that charging data was stored
11. **Session release:** the session is released
12. **Charging Data Generation:** the CTF generates charging data related to session due of session termination.
13. **Record Charging Data Request:** the CTF requests the CDF to store session related charging data for CDR generation purposes.
14. **Process Request:** CDF stores received information. Whether the CDR is generated or not depends on CDR generation configuration.
15. **Record Charging Data Response:** the CDF informs the CTF that charging data was stored.

5.1.2 Basic Operation

Event and session based Charging are performed by the use of the "*Charging Data Transfer*" operation:

- "*Charging Data Request*"; sent from CTF → CDF
After detecting a chargeable event, the CTF sends a Charging Data Request to the CDF.
- "*Charging Data Response*"; sent from CDF → CTF
The CDF replies with a Charging Data Response, which informs the CTF that charging data was received.

Table 5.1.2.1 and table 5.1.2.2 describe the content of these operations.

Table 5.1.2.1: Charging Data Request Content

Charging Data Request	Category	Description
Session Identifier	M	This field identifies the operation session.
Originator Host	M	This field contains the identification of the source point of the operation and the realm of the operation originator.
Originator Domain	M	This field contains the realm of the operation originator.
Destination Domain	M	This field contains the realm of the operation destination.
Operation Type	M	This field defines the transfer type: event for event based charging and start, interim, stop for session based charging.
Operation Number	M	This field contains the sequence number of the transferred messages.
Operation Identifier	O _M	The field corresponds to the unique operation identification.
User Name	O _C	The field contains the identification of the service user.
Operation Interval	O _C	
Origination State	O _C	
Origination Timestamp	O _C	This field contains the time when the operation is requested.
Proxy Information	O _C	This field contains the parameter of the proxy.
Route Information	O _C	This field contains the parameter of the route.
Operation Token	O _M	This field identifies the domain, subsystem or service and release.
Service information	O _M	This parameter holds the individual service specific parameters as defined in the corresponding "middle tier" TS.

Table 5.1.2.2: Charging Data Response Content

Charging Data Response	Category	Description
Session Identifier	M	This field identifies the operation session.
Operation Result	M	This field identifies the result of the operation.
Originator Host	M	This field contains the identification of the source point of the operation and the realm of the operation originator.
Originator Domain	M	This field contains the realm of the operation originator.
Operation Type	M	This field defines the transfer type: event for event based charging and start, interim, stop for session based charging.
Operation Number	M	This field contains the sequence number of the transferred messages.
Operation Identifier	O _M	The field corresponds to the unique operation identification.
Operation Interval	O _C	
Error Reporting Host	O _C	If proxies exist between the accounting client and the accounting server this field contains the identity of the proxy that sent a response other than 2001 (Success).
Origination State	O _C	
Origination Timestamp	O _C	This field contains the time when the operation is requested.
Proxy Information	O _C	This field contains the parameter of the proxy.

5.2 Online Charging scenarios

Online charging for both events and sessions between CTF and the OCF is performed using the Ro reference point. The Ro reference point supports integrity protection and authentication for the case that the CTF is outside the operator domain.

5.2.1 Basic principles

There are two sub-functions for online charging that affect online charging principles and require a more detailed description: rating and unit determination. Both rating and unit determination can be implemented centralized, i.e. on the OCF, or decentralized, that is, on the CTF.

Unit determination refers to the calculation of the number of non-monetary units (service units, data volume, time and events) that shall be assigned prior to starting service delivery.

- With Centralized Unit Determination, the OCF determines the number of non-monetary units that a certain service user can consume based on a service identifier received from the CTF.
- With the Decentralized Unit Determination approach, the CTF determines itself how many units are required to start service delivery, and requests these units from the OCF.

After checking the service user's account balance, the OCF returns the number of granted units to the CTF. The CTF is then responsible for the supervision of service delivery. Particularly, the CTF shall limit service delivery to the corresponding number of granted units.

Rating refers to the calculation of a price out of the non-monetary units calculated by the unit determination function.

- With the Centralized Rating approach, the CTF and the OCF exchange information about non-monetary units. The OCF translates these units into monetary units.
- With the Decentralized Rating approach, the corresponding rating control is performed within the CTF. Consequently, CTF and OCF exchange information about monetary units.

Three cases for online charging can be distinguished: immediate event charging (IEC), event charging with unit reservation (ECUR) and session charging with unit reservation (SCUR). These cases are further described in 3GPP TS 32.240 [1].

Editor's note: The text above in green could be moved to the top, however, then there needs to be relation with the succeeding text.

5.2.2 Charging Scenarios

In order to perform event charging via Ro, the scenarios between the involved entities UE-A, OCF and CTF need to be defined. The charging flows shown in this subclause include scenarios with immediate event charging and event charging with reservation. In particular, the following cases are shown:

- 1) Immediate Event Charging
 - a) Decentralized Unit Determination and Centralized Rating
 - b) Centralized Unit Determination and Centralized Rating
 - c) Decentralized Unit Determination and Decentralized Rating
- 2) Event charging with Reservation
 - a) Decentralized Unit Determination and Centralized Rating
 - b) Centralized Unit Determination and Centralized Rating
 - c) Decentralized Unit Determination and Decentralized Rating
- 3) Session charging with Reservation
 - a) Decentralized Unit Determination and Centralized Rating

- b) Centralized Unit Determination and Centralized Rating
- c) Decentralized Unit Determination and Decentralized Rating

The combination of Centralized Unit Determination with Decentralized Rating is not possible.

5.2.2.1 Immediate Event Charging

5.2.2.1.1 Decentralized Unit Determination and Centralized Rating

In the following scenario, CTF asks the OCF to assign a defined number of units.

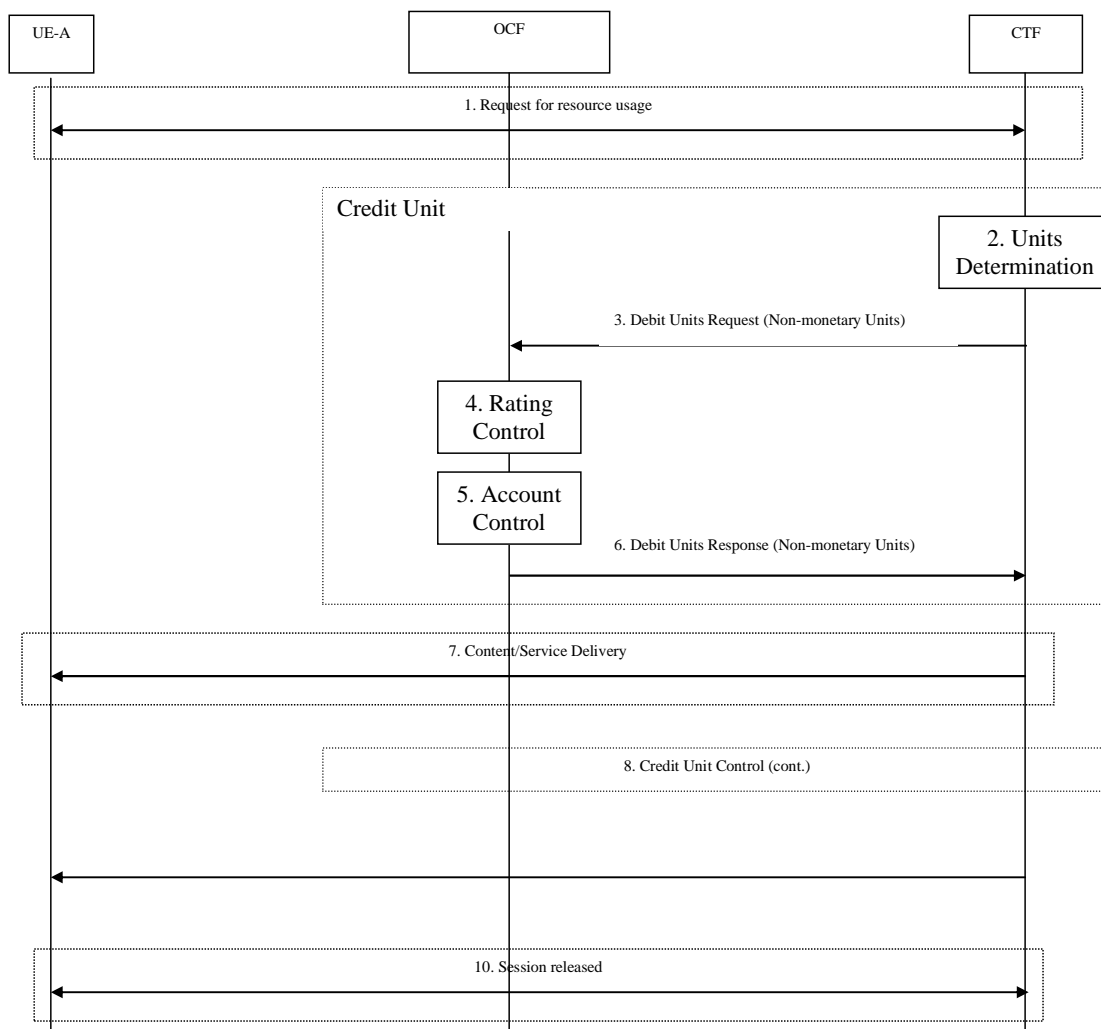


Figure 5.2.2.1.1: Immediate Event Charging with Centralized Rating and Decentralized Unit Determination

1. **Request for resource usage:** UE-A requests the desired resource from the network element.
2. **Units Determination:** depending on the requested service the CTF determines the number of units accordingly.
3. **Debit Units Request:** the CTF requests the OCF to assign the defined number of units.
4. **Rating Control:** assisted by the rating entity the OCF calculates the number of monetary units that represents the price for the number of units determined in item 2.
5. **Account Control:** provided that the user's credit balance is sufficient, the OCF triggers the deduction of the calculated amount from the subscriber's account.
6. **Debit Units Response:** the OCF informs the CTF of the number of granted units.

- 7. **Content/Service Delivery:** the CTF delivers the content/service at once, in fractions or in individually chargeable items, corresponding to the number of granted units.
- 8. **Credit Unit Control (cont.):** this function block is optional and a replication of items 2 to 6.
- 9. **Content/Service Delivery (cont.):** the continuation of content delivery occurs in correspondence with the occurrence of item 8.
- 10. **Session released:** Session is released.

5.2.2.1.2 Centralized Unit Determination and Centralized Rating

In the following scenario, CTF asks the OCF to assign units based on the service identifier specified by the CTF.

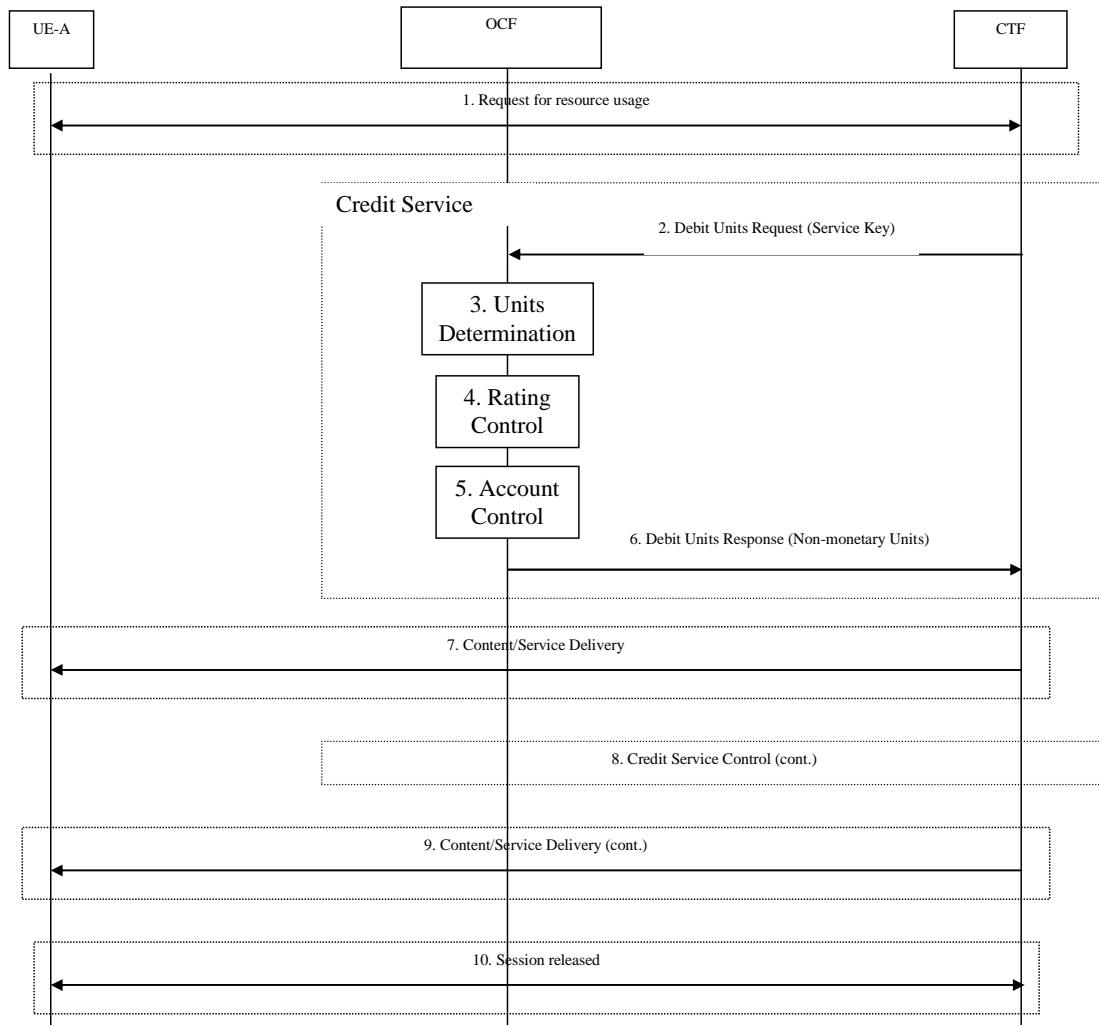


Figure 5.2.2.1.2: Immediate Event Charging with Centralized Rating and Centralized Unit Determination

- 1. **Request for resource usage:** The UE-A requests the desired resource or content from the network element.
- 2. **Debit Units Request:** depending on the service requested by the UE-A, the CTF selects the service identifier and forwards the Debit Units Request to the OCF.
- 3. **Units Determination:** the OCF determines the number of non-monetary units needed for the content/service delivery, based on the received service key.
- 4. **Rating Control:** assisted by the rating entity the OCF calculates the number of monetary units that represent the price for the number of units determined in item 3.
- 5. **Account Control:** provided that the user's credit balance is sufficient, the OCF triggers the deduction of the calculated amount from the subscriber's account.

- 6. **Debit Units Response:** the OCF informs the CTF of the number of granted units. This includes the case where the number of units granted indicates the permission to render the service that was identified by the received service key.
- 7. **Content/Service Delivery:** the CTF delivers the content/service at once, in fractions or in individually chargeable items, corresponding to the number of granted units.
- 8. **Credit Service Control (cont.):** this function block is optional and a replication of items 2 to 6.
- 9. **Content/Service Delivery (cont.):** the continuation of content delivery occurs in correspondence with the occurrence of item 8.
- 10. **Session released:** the session is released.

5.2.2.1.3 Decentralized Unit Determination and Decentralized Rating

In the following scenario, the CTF asks the OCF to assure the deduction of an amount of the specified number of monetary units from the subscriber's account.

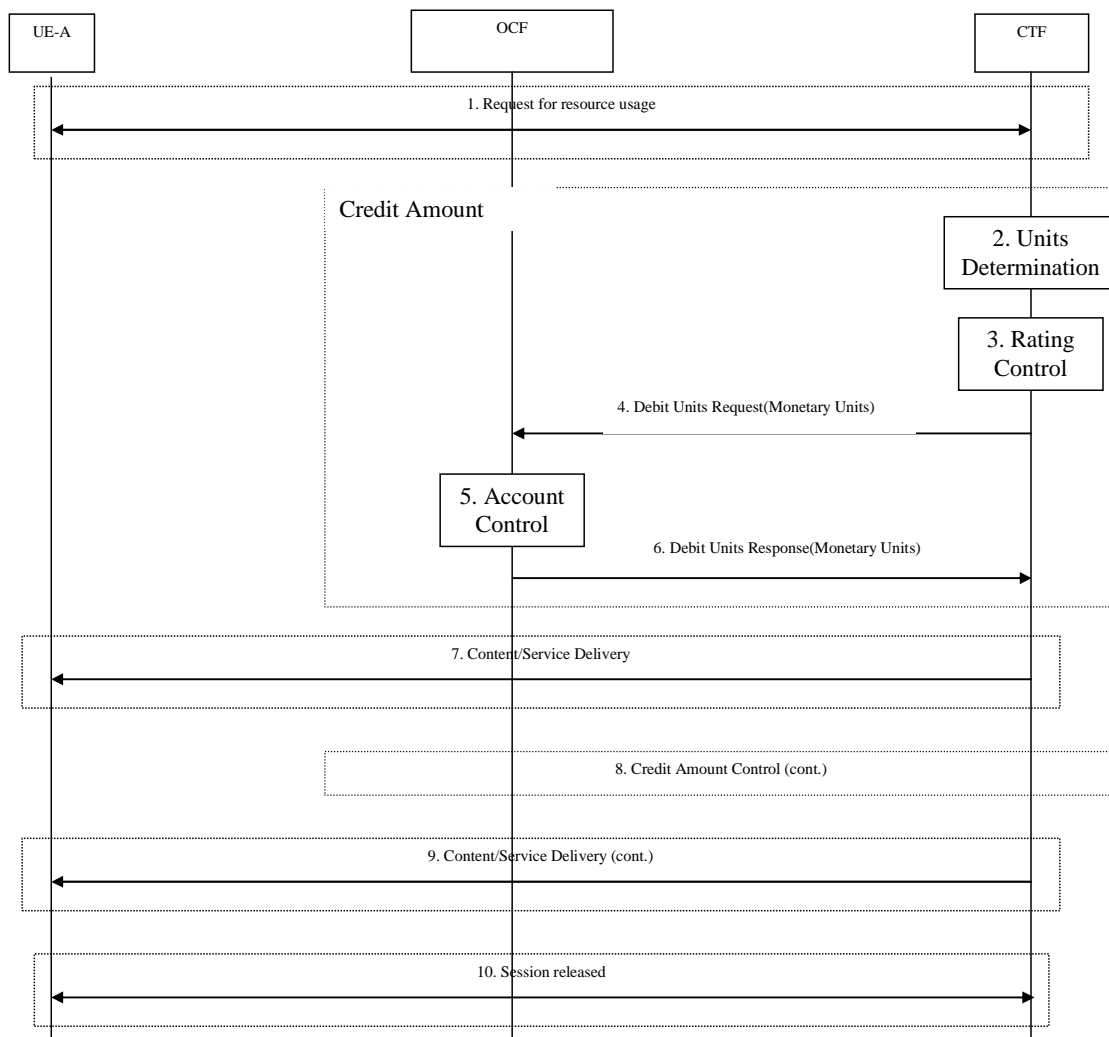


Figure 5.2.2.1.3: Immediate Event Charging with Decentralized Rating and Decentralized Unit Determination

- 1. **Request for resource usage:** The UE-A requests the desired content from the network element.
- 2. **Units Determination:** depending on the service requested by the UE-A, the CTF determines the number of units accordingly.
- 3. **Rating Control:** the CTF calculates the number of monetary units that represent the price for the number of units determined in item 2.
- 4. **Debit Units Request:** the CTF requests the OCF to assure the deduction of an amount corresponding to the calculated number of monetary units from the subscriber's account.

5. **Account Control:** provided that the user's credit balance is sufficient, the OCF triggers the deduction of the calculated amount from the subscriber's account.
6. **Debit Units Response:** the OCF indicates to the CTF the number of deducted monetary units.
7. **Content/Service Delivery:** the CTF delivers the content/service at once, in fractions or in individually chargeable items, corresponding to the number of units as specified in items 2 and 3.
8. **Credit Amount Control (cont.):** this function block is optional and a replication of items 2 to 6.
9. **Content/Service Delivery (cont.):** the continuation of content delivery occurs in correspondence with the occurrence of item 8.
10. **Session released:** the session is released.

5.2.2.1.4 Further Options

In addition to the flows that are specified in the previous subclauses, the Debit Unit operation may alternatively be carried out concurrently with service delivery, or after completion of service delivery.

5.2.2.2 Event charging with Reservation

5.2.2.2.1 Decentralized Unit Determination and Centralized Rating

In the following scenario, the CTF requests the reservation of units prior to service delivery. An account debit operation is carried out following the conclusion of service delivery.

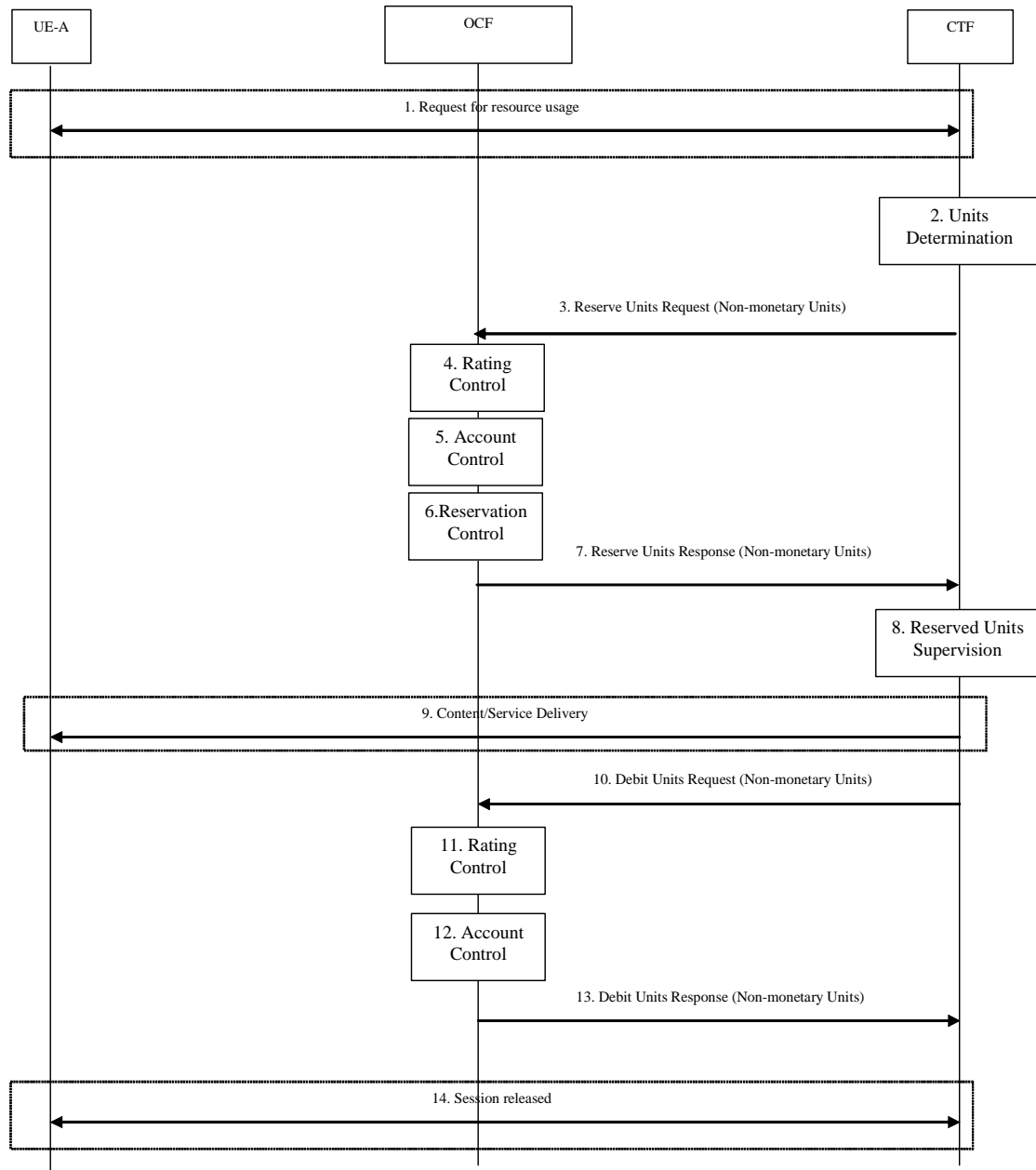


Figure 5.2.2.2.1: Event Charging with Reservation / Decentralized Unit Determination and Centralized Rating

1. **Request for resource usage:** The UE-A requests the desired content/service from the NE.
2. **Units Determination:** depending on the requested service the CTF determines the number of units accordingly.
3. **Reserve Units Request:** the CTF requests the OCF to reserve the number of units determined in item 2.
4. **Rating Control:** assisted by the rating entity the OCF calculates the number of monetary units that represents the price for the number of units determined in item 2.
5. **Account Control:** the OCF checks whether the user's account balance is sufficient for the requested reservation.
6. **Reservation Control:** if the user's account balance is sufficient then the corresponding reservation is made.

7. **Reserve Units Response:** the OCF informs the CTF of the reserved number of units. Items 3 to 7 may be repeated several times.
8. **Reserved Units Supervision:** simultaneously with the service delivery, the CTF monitors the consumption of the reserved units.
9. **Content/Service Delivery:** the CTF delivers the content/service at once, in fractions or in individually chargeable items, corresponding to the reserved number of units.
10. **Debit Units Request:** the CTF requests the OCF to assure the deduction of an amount corresponding to the consumed number of units from the subscriber's account. In the case that no further units are required for this service, an appropriate indication triggering the release of the remaining reservation is given.
11. **Rating Control:** assisted by the rating entity the OCF calculates the number of monetary units to deduct from the subscriber's account.
12. **Account Control:** the OCF triggers the deduction of the calculated amount from the subscriber's account.
13. **Debit Units Response:** the OCF informs the CTF of the actually deducted units. Items 10 to 13 may be repeated several times.
14. **Session Release:** the session is released.

5.2.2.2.2 Centralized Unit Determination and Centralized Rating

In the following scenario, the CTF requests the OCF to reserve units based on the service identifier specified by the CTF. An account debit operation is carried out following the conclusion of service delivery.

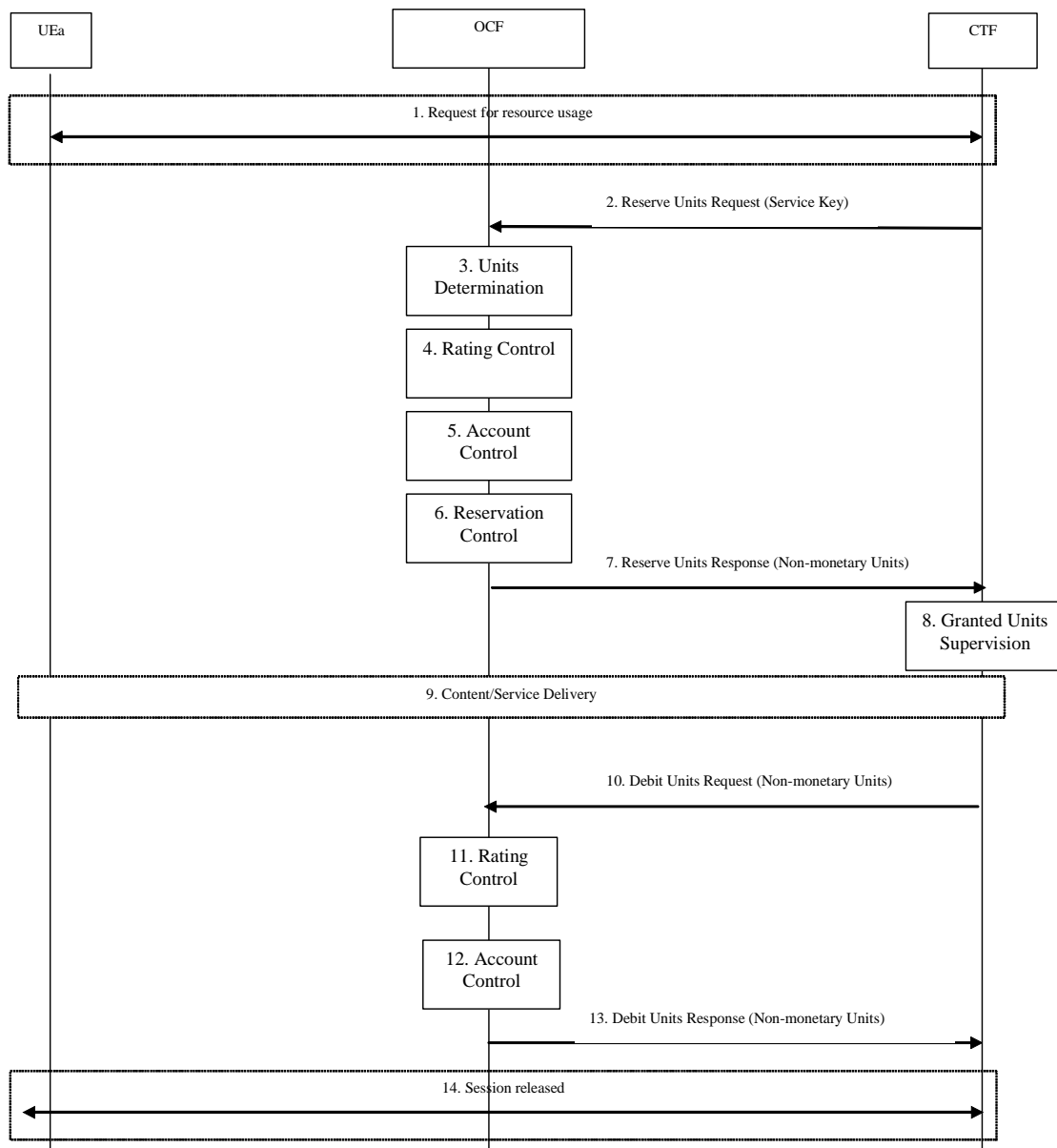


Figure 5.2.2.2.2: Event Charging with Reservation / Centralized Unit Determination and Centralized Rating

1. **Request for resource usage:** The UE-A requests the desired content from the CTF.
2. **Reserve Units Request:** depending on the service requested by the UE-A, the CTF selects the service identifier and forwards the Reserve Units Request to the OCF.
3. **Units Determination:** the OCF determines the number of non-monetary units needed for the content/service delivery, based on the received service key.
4. **Rating Control:** assisted by the rating entity the OCF calculates the number of monetary units that represent the price for the number of units determined in item 3.
5. **Account Control:** the OCF checks whether the user's account balance is sufficient for the requested reservation.
6. **Reservation Control:** if the user's account balance is sufficient, then the corresponding reservation is made.
7. **Reserve Units Response:** the OCF informs the CTF of the reserved number of units. This includes the case where the number of units reserved indicates the permission to render the service that was identified by the received service key. Items 2 to 7 may be repeated several times.

8. **Granted Units Supervision:** simultaneously with the service delivery, the CTF monitors the consumption of the reserved units.
9. **Content/Service Delivery:** the CTF delivers the content/service at once, in fractions or in individually chargeable items, corresponding to the reserved number of units.
10. **Debit Units Request:** the CTF provides according to previous Reserve Units Response either the request to deduct of an amount corresponding to the consumed number of units from the subscriber's account, or solely the indication of whether the service was successfully delivered or not. In the case that no further units are required for this service, an appropriate indication triggering the release of the remaining reservation is given.
11. **Rating Control:** assisted by the rating entity the OCF calculates the number of monetary units to deduct from the subscriber's account.
12. **Account Control:** the OCF triggers the deduction of the calculated amount from the subscriber's account.
13. **Debit Units Response:** the OCF informs the CTF of the actually deducted units. Items 10 to 13 may be repeated several times.
14. **Session Released:** the session is released.

Editor's note: the content of step 9 till 11 should be corrected.

5.2.2.2.3 Decentralized Unit Determination and Decentralized Rating

In the following scenario, the CTF request the OCF to assure the reservation of an amount of the specified number of monetary units from the subscriber's account. An account debit operation that triggers the deduction the amount from the subscriber's account is carried out following the conclusion of service delivery.

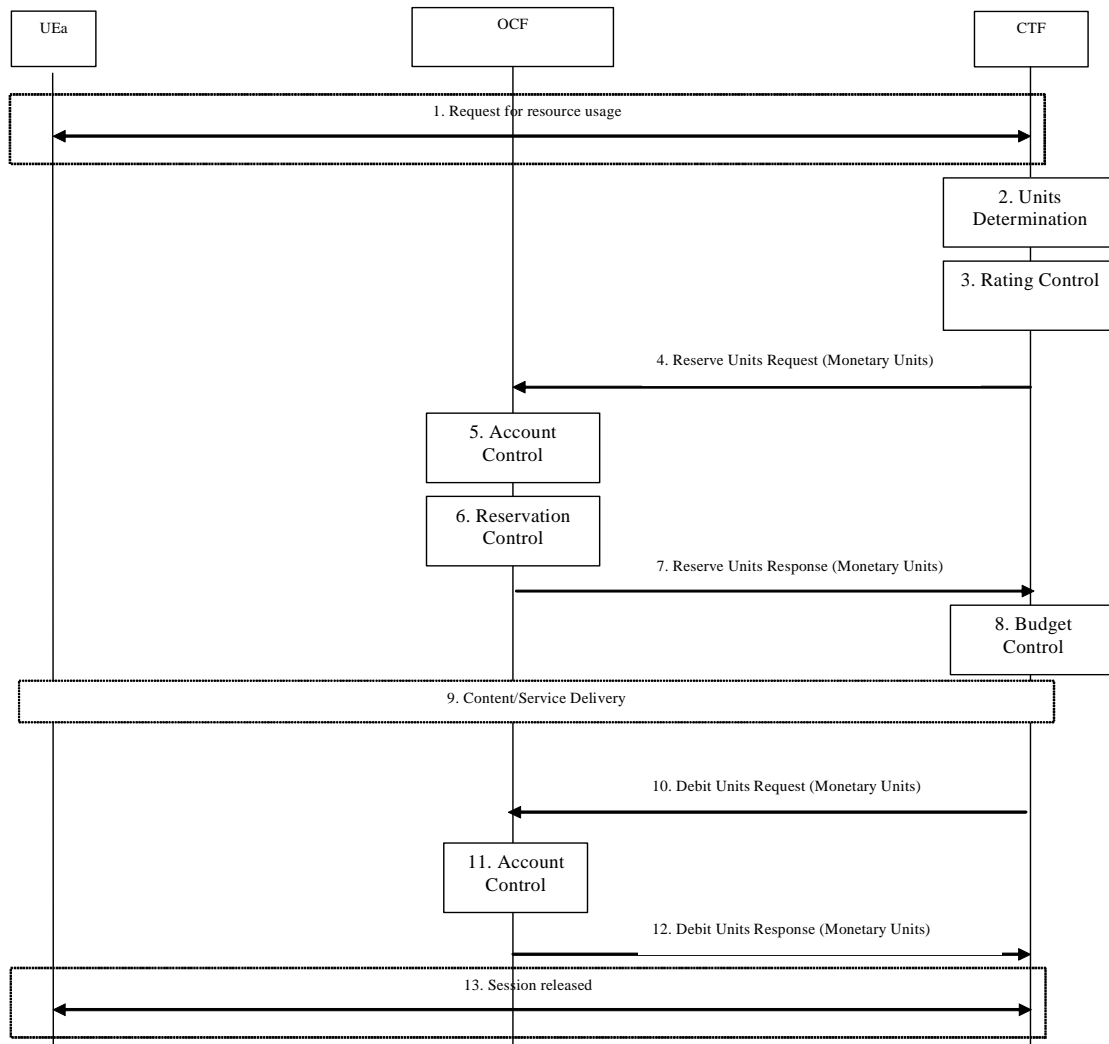


Figure 5.2.2.2.3: Event Charging with Reservation / Centralized Unit Determination and Centralized Rating

1. **Request for resource usage:** The UE-A requests the desired content from the CTF.
2. **Units Determination:** depending on the service requested by the UE-A, the CTF determines the number of units accordingly.
3. **Rating Control:** the CTF calculates the number of monetary units that represent the price for the number of units determined in item 2.
4. **Reserve Units Request:** the CTF requests the OCF to assure the reservation of an amount corresponding to the calculated number of monetary units from the subscriber's account.
5. **Account Control:** the OCF checks whether the user's account balance is sufficient for the requested reservation.
6. **Reservation Control:** if the user's credit balance is sufficient, then the corresponding reservation is made.
7. **Reserve Units Response:** the OCF informs the CTF of the reserved number of monetary units. Items 4 to 7 may be repeated several times.
8. **Budget Control:** simultaneously with the service delivery, the CTF monitors the consumption of the granted amount.

9. **Content/Service Delivery:** the CTF delivers the content/service at once, in fractions or in individually chargeable items, corresponding to the number of units.
10. **Debit Units Request:** the CTF requests the OCF to assure the deduction of an amount corresponding to the consumed number of monetary units from the subscriber's account.
11. **Account Control:** the OCF triggers the deduction of the consumed amount from the subscriber's account.
12. **Debit Units Response:** the OCF indicates to the CTF the number of deducted monetary units. Items 10 to 12 may be repeated several times.
13. **Session Released:** the session is released.

Editor's note: Move the above intent to the session charging clause as it is not applicable to event charging. E.g. as an addition to the description in step 9.

5.2.2.3 Session charging with Reservation

5.2.2.3.1 Decentralized Unit Determination and Centralized Rating

In the following scenario, the CTF requests the reservation of units prior to session supervision. An account debit operation is carried out following the conclusion of session termination.

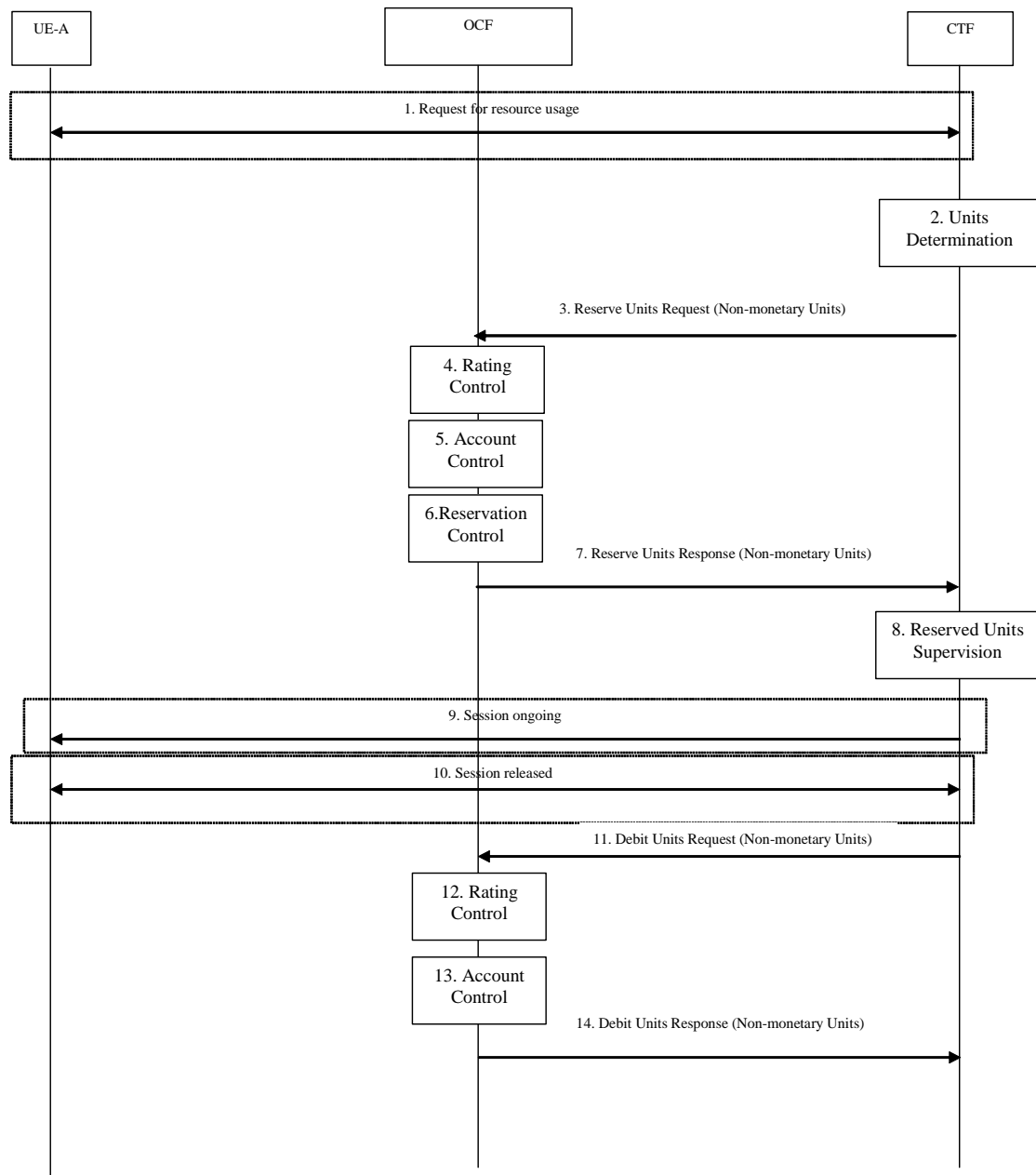


Figure 5.2.2.3.1: Session Charging with Reservation / Decentralized Unit Determination and Centralized Rating

1. **Request for resource usage:** The UE-A requests session establishment from the CTF.
2. **Units Determination:** depending on the requested type of the session the CTF determines the number of units accordingly.
3. **Reserve Units Request:** the CTF requests the OCF to reserve the number of units determined in item 2
4. **Rating Control:** assisted by the rating entity the OCF calculates the number of monetary units that represents the price for the number of units determined in item 2.
5. **Account Control:** the OCF checks whether the user's account balance is sufficient for the requested reservation.
6. **Reservation Control:** if the user's account balance is sufficient then the corresponding reservation is made.

7. **Reserve Units Response:** the OCF informs the CTF of the reserved number of units.
8. **Reserved Units Supervision:** simultaneously with the ongoing session, the CTF monitors the consumption of the reserved units.
9. **Session ongoing:** the CTF maintains the session, corresponding to the reserved number of units.
10. **Session Release:** the session is released
11. **Debit Units Request:** the CTF requests the OCF to assure the deduction of an amount corresponding to the consumed number of units from the subscriber's account. In the case that no further units are required for this service, an appropriate indication triggering the release of the remaining reservation is given.
12. **Rating Control:** assisted by the rating entity the OCF calculates the number of monetary units to deduct from the subscriber's account.
13. **Account Control:** the OCF triggers the deduction of the calculated amount from the subscriber's account.
14. **Debit Units Response:** the OCF informs the CTF of the actually deducted units.

5.2.2.3.2 Centralized Unit Determination and Centralized Rating

In the following scenario, the CTF requests the OCF to reserve units based on the session identifiers specified by the CTF. An account debit operation is carried out following the conclusion of session.

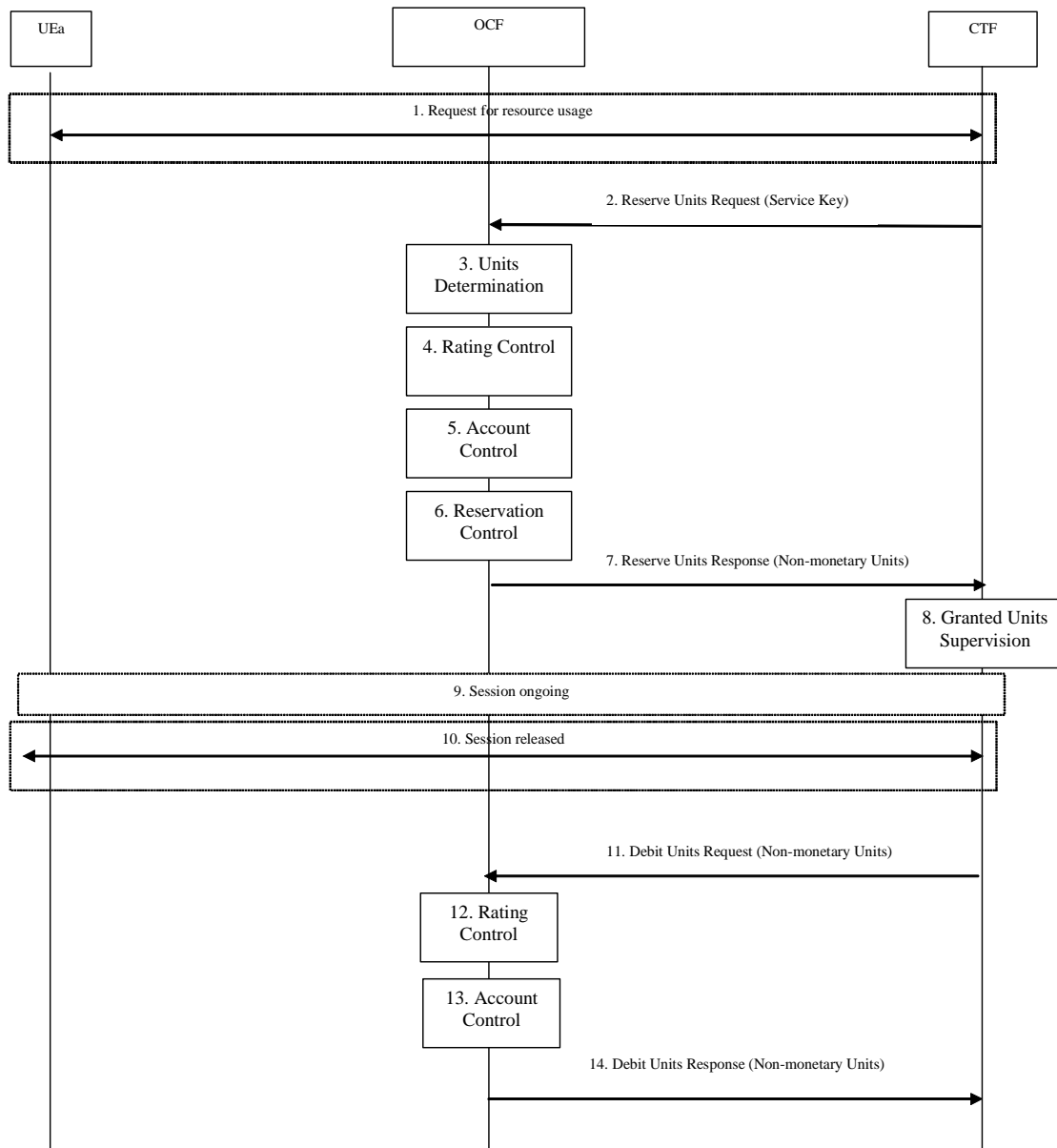


Figure 5.2.2.3.2: Session Charging with Reservation / Centralized Unit Determination and Centralized Rating

1. **Request for resource usage:** The UE-A requests the session establishment from the CTF.
2. **Reserve Units Request:** depending on the requested type of the session by the UE-A, the CTF selects the service identifier and forwards the Reserve Units Request to the OCF.
3. **Units Determination:** the OCF determines the number of non-monetary units needed for the content/service delivery, based on the received service key.
4. **Rating Control:** assisted by the rating entity the OCF calculates the number of monetary units that represent the price for the number of units determined in item 3.
5. **Account Control:** the OCF checks whether the user's account balance is sufficient for the requested reservation.
6. **Reservation Control:** if the user's account balance is sufficient, then the corresponding reservation is made.

7. **Reserve Units Response:** the OCF informs the CTF of the reserved number of units. This includes the case where the number of units reserved indicates the permission to render the service that was identified by the received service key.
8. **Granted Units Supervision:** simultaneously with the ongoing session, the CTF monitors the consumption of the reserved units.
9. **Session ongoing:** the CTF provides according to previous Reserve Units Response either the request to deduct of an amount corresponding to the consumed number of units from the subscriber's account, or solely the indication of whether the session was successfully established or not. In the case that no further units are required for this service, an appropriate indication triggering the release of the remaining reservation is given.
10. **Session Released:** the session is released.
11. **Debit Units Request:** the CTF requests the OCF to assure the deduction of an amount corresponding to the consumed number of units from the subscriber's account
12. **Rating Control:** assisted by the rating entity the OCF calculates the number of monetary units to deduct from the subscriber's account.
13. **Account Control:** the OCF triggers the deduction of the calculated amount from the subscriber's account.
14. **Debit Units Response:** the OCF informs the CTF of the actually deducted units.

5.2.2.3.3 Decentralized Unit Determination and Decentralized Rating

In the following scenario, the CTF request the OCF to assure the reservation of an amount of the specified number of monetary units from the subscriber's account. An account debit operation that triggers the deduction the amount from the subscriber's account is carried out following the conclusion of session establishment.

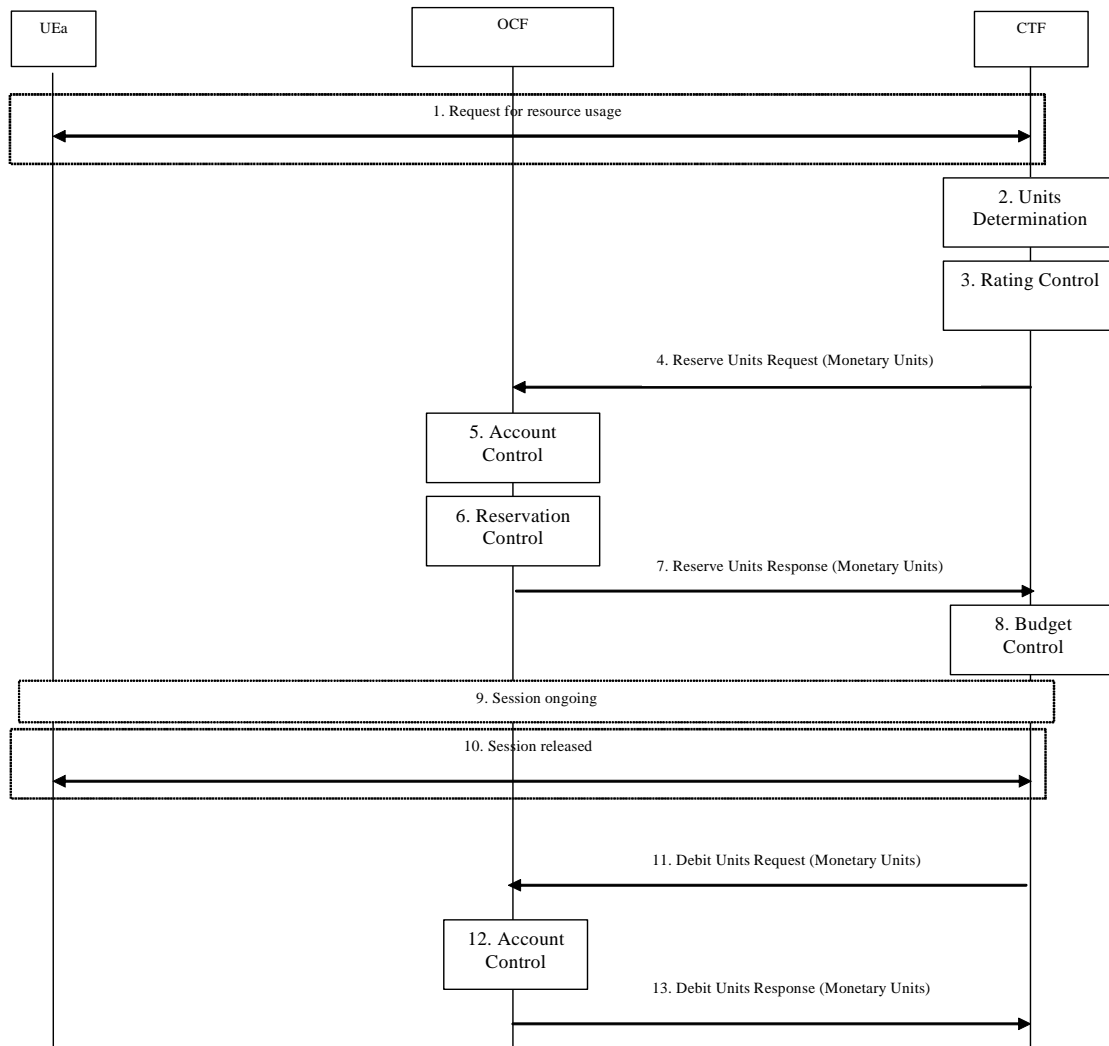


Figure 5.2.2.3.3: Session Charging with Reservation / Decentralized Unit Determination and Decentralized Rating

1. **Request for resource usage:** The UE-A requests the session establishment from the CTF.
2. **Units Determination:** depending on the requested type of the session by the UE-A, the CTF determines the number of units accordingly.
3. **Rating Control:** the CTF calculates the number of monetary units that represent the price for the number of units determined in item 2.
4. **Reserve Units Request:** the CTF requests the OCF to assure the reservation of an amount corresponding to the calculated number of monetary units from the subscriber's account.
5. **Account Control:** the OCF checks whether the user's account balance is sufficient for the requested reservation.
6. **Reservation Control:** if the user's credit balance is sufficient, then the corresponding reservation is made.
7. **Reserve Units Response:** the OCF informs the CTF of the reserved number of monetary units.
8. **Budget Control:** simultaneously with the ongoing session, the CTF monitors the consumption of the granted amount.
9. **Session ongoing:** the CTF maintains the session corresponding to the number of units.
10. **Session Released:** the session is released.

11. **Debit Units Request:** the CTF requests the OCF to assure the deduction of an amount corresponding to the consumed number of monetary units from the subscriber's account.
12. **Account Control:** the OCF triggers the deduction of the consumed amount from the subscriber's account.
13. **Debit Units Response:** the OCF indicates to the CTF the number of deducted monetary units.

Editor's note: If needed, it would be moved to another clause on revision.

5.2.3 Basic Operations

Immediate event charging is performed by the use of the "*Debit Units*" operation:

- "*Debit Units Request*"; sent from CTF → OCF
After receiving a service request from the subscriber, the CTF sends a *Debit Units Request* to the OCF. The CTF may either specify a service identifier (centralised unit determination) or the number of units requested (decentralised unit determination).
- "*Debit Units Response*"; sent from OCF → CTF
The OCF replies with a *Debit Units Response*, which informs the CTF of the number of units granted as a result of the *Debit Units Request*. This includes the case where the number of units granted indicates the permission to render the requested service.

In addition, the "*Reserve Units*" operation is used with both event charging with unit reservation, and session charging with unit reservation:

- "*Reserve Units Request*"; sent from CTF → OCF
Request to reserve a number of units for the service to be provided by an CTF. In case of centralised unit determination, the CTF specifies a service identifier in the *Reserve Unit Request*, and the OCF determines the number of units requested. In case of decentralised unit determination, the number of units requested is specified by the CTF.
- "*Reserve Units Response*"; sent from OCF → CTF
Response from the OCF which informs the CTF of the number of units that were reserved as a result of the "*Reserve Units Request*".

The consumed units are deducted from the subscriber's account after service delivery. Thus, the reserved and consumed units are not necessarily the same. Using this operation, it is also possible for the CTF to modify the current reservation, including the return of previously reserved units.

Table 5.2.3.1 and table 5.2.3.2 describe the content of these operations.

Table 5.2.3.1: Debit and Reserve Units Request Content

Debit and Reserve Units Request	Category	Description
Session Identifier	M	This field identifies the operation session.
Originator Host	M	This field contains the identification of the source point of the operation.
Originator Domain	M	This field contains the realm of the operation originator.
Destination Domain	M	This field contains the realm of the operation destination.
Operation Identifier	M	This field is a unique operation identifier.
Operation Token	M	This field contains the service identifier.
Operation Type	M	This field defines the transfer type: event for event based charging and start, interim, stop for session based charging.
Operation Number	M	This field contains the sequence number of the transferred messages.
Destination Host	O _C	This field contains the identification of the destination point of the operation.
User Name	O _C	This field contains the identification of the user.
Origination State	O _C	Tbd.
Origination Timestamp	O _C	This field contains the time when the operation is requested.
Subscriber Identifier	O _M	This field contains the identification of the mobile subscriber (i.e. MSISDN) that uses the requested service.
Termination Cause	O _C	This field contains the termination reason of the service.
Requested Action	O _C	This field contains the requested action.
Multiple Operation	O _M	This field indicate the occurrence of multiple operations.
Multiple Unit Operation	O _M	This field contains the parameter for the quota management.
Subscriber Equipment Number	O _C	This field contains the identification of the mobile device (i.e. IMEI) that uses the subscriber.
Proxy Information	O _C	This field contains the parameter of the proxy.
Route Information	O _C	This field contains the parameter of the route.
Service Information	O _M	This parameter holds the individual service specific parameters as defined in the corresponding "middle tier" TS.

Table 5.2.3.2: Debit and Reserve Units Response Content

Debit and Reserve Units Response	Category	Description
Session Identifier	M	This field identifies the operation session.
Operation Result	M	This field identifies the result of the operation.
Originator Host	M	This field contains the identification of the source point of the operation.
Originator Domain	M	This field contains the realm of the operation originator.
Operation Identifier	M	This field is a unique operation identifier.
Operation Type	M	This field defines the transfer type: event for event based charging and start, interim, stop for session based charging.
Operation Number	M	This field contains the sequence number of the transferred messages.
Operation Failover	O _C	This field contains an indication to the CTF whether or not a failover handling is to be used when necessary.
Multiple Unit Operation	O _M	This field contains the parameter for the quota management.
Operation Failure Action	O _C	For credit control sessions the content of this field enables the credit-control client to decide what to do if sending credit-control messages to the credit-control server has been temporarily prevented.
Operation Event Failure Action	O _C	For one time event direct debiting the content of this field enables the credit-control client to decide what to do if sending credit-control messages to the credit-control server has been temporarily prevented.
Redirection Host	O _C	Tbd.
Redirection Host Usage	O _C	Tbd.
Redirection Cache Time	O _C	Tbd.
Proxy Information	O _C	This field contains the parameter of the proxy.
Route Information	O _C	This field contains the parameter of the route.
Failed parameter	O _C	This field contains missing and/or unsupported parameter that caused the failure.
Service Information	O _C	This parameter holds the individual service specific parameters as defined in the corresponding "middle tier" TS.

5.3 Other requirements

5.3.1 Re-authorization

The server may specify an idle timeout associated with a granted quota. Alternatively, the client may have a configurable default value. The expiry of that timer shall trigger a re-authorization request.

Mid-session service events (re-authorization triggers) may affect the rating of the current service usage. The server may instruct the credit control client to re-authorize the quota upon a number of different session related triggers that can affect the rating conditions.

When a re-authorization is triggered, the client shall report quota usage. The reason for the quota being reported shall be notified to the server.

5.3.2 Threshold based re-authorization triggers

The server may optionally include an indication to the client of the remaining quota threshold that shall trigger a quota re-authorization.

5.3.3 Termination action

The server may specify to the client the behaviour on consumption of the final granted units; this is known as termination action.

6 3GPP Charging Applications – Protocol Aspects

6.1 Basic Principles for Diameter Offline Charging

In order to support the offline charging principles described in the present document, the Diameter client and server must implement at least the following Diameter options listed in RFC 3588 [401], i.e. the basic functionality of Diameter accounting, as defined by the Diameter Base Protocol (RFC 3588 [401]) is re-used..

The charging architecture implementing Diameter adheres to the structure where all communications for offline charging purposes between the CTF (Diameter client) and the CDF (Diameter server) are carried out on the Diameter Rf reference point, where the CTF reports charging information to the Charging Data Function (CDF). The CDF uses this information to construct and format CDRs. The above-mentioned reference points are defined in 3GPP TS 32.240 [1].

A configurable timer is supported in the CDF to supervise the reception of the ACR [Interim] and/or ACR [Stop]. An instance of the "Timer" is started at the beginning of the accounting session, reset on the receipt of an ACR [Interim] and stopped at the reception of the ACR [Stop]. Upon expiration of the timer, the CDF stops the accounting session with the appropriate error indication.

For offline charging, the CTF implements the accounting state machine described in RFC 3588 [401]. The server (CDF) implements the accounting state machine "SERVER, STATELESS ACCOUNTING" as specified in RFC 3588 [401], i.e. there is no order in which the server expects to receive the accounting information.

The offline charging functionality is based on the network elements reporting accounting information upon reception of various messages which trigger charging generation, as most of the accounting relevant information is contained in these messages. This reporting is achieved by sending Diameter *Accounting Requests* (ACR) [Start, Interim, Stop and Event] from the network elements to the CDF.

Following the Diameter base protocol specification, the following "types" of accounting data may be sent with regard to offline charging:

- START session accounting data.
- INTERIM session accounting data.
- STOP session accounting data.
- EVENT accounting data.

Two cases are currently distinguished for offline charging purposes:

- Event based charging; and
- Session based charging.

ACR types START, INTERIM and STOP are used for accounting data related to successful sessions. In contrast, EVENT accounting data is unrelated to sessions, and is used e.g. for a simple registration or interrogation and successful service event triggered by a network element. In addition, EVENT accounting data is also used for unsuccessful session establishment attempts.

The flows and scenarios for the above two described cases are further detailed below.

6.1.1 Event based charging

In the case of event based charging, the network reports the usage or the service rendered where the service offering is rendered in a single operation. It is reported using the ACR EVENT.

The following figure shows the transactions that are required on the Diameter offline interface in order to perform event based charging. The operation may alternatively be carried out prior to, concurrently with or after service/content delivery.

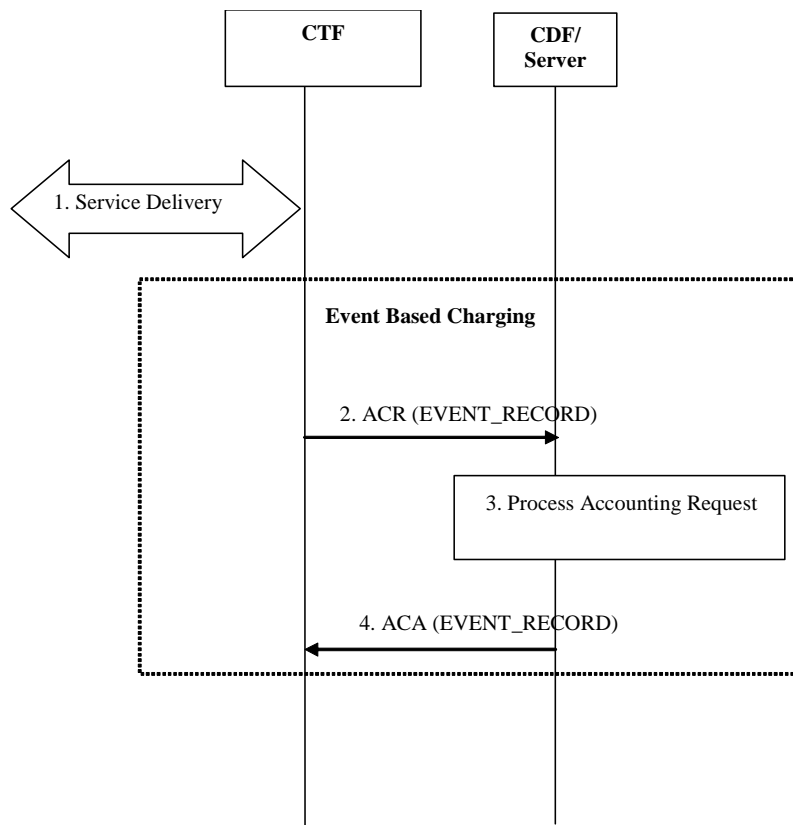


Figure 6.1.1: Event Based offline charging

- Step 1: The network element receives indication that service has been used/delivered.
- Step 2: The network element (acting as client) sends *Accounting-Request* (ACR) with *Accounting-Record-Type* AVP set to EVENT_RECORD to indicate service specific information to the CDF (acting as server).
- Step 3: The CDF receives the relevant service charging parameters and processes accounting request.
- Step 4: The CDF returns *Accounting-Answer* message with *Accounting-Record-Type* AVP set to EVENT_RECORD to the network element in order to inform that charging information was received.

6.1.2 Session based charging

Session based charging is the process of reporting usage reports for a session and uses the START, INTERIM & STOP accounting data. During a session, a network element may transmit multiple ACR Interims' depending on the proceeding of the session.

The following figure shows the transactions that are required on the Diameter offline interface in order to perform session based charging.

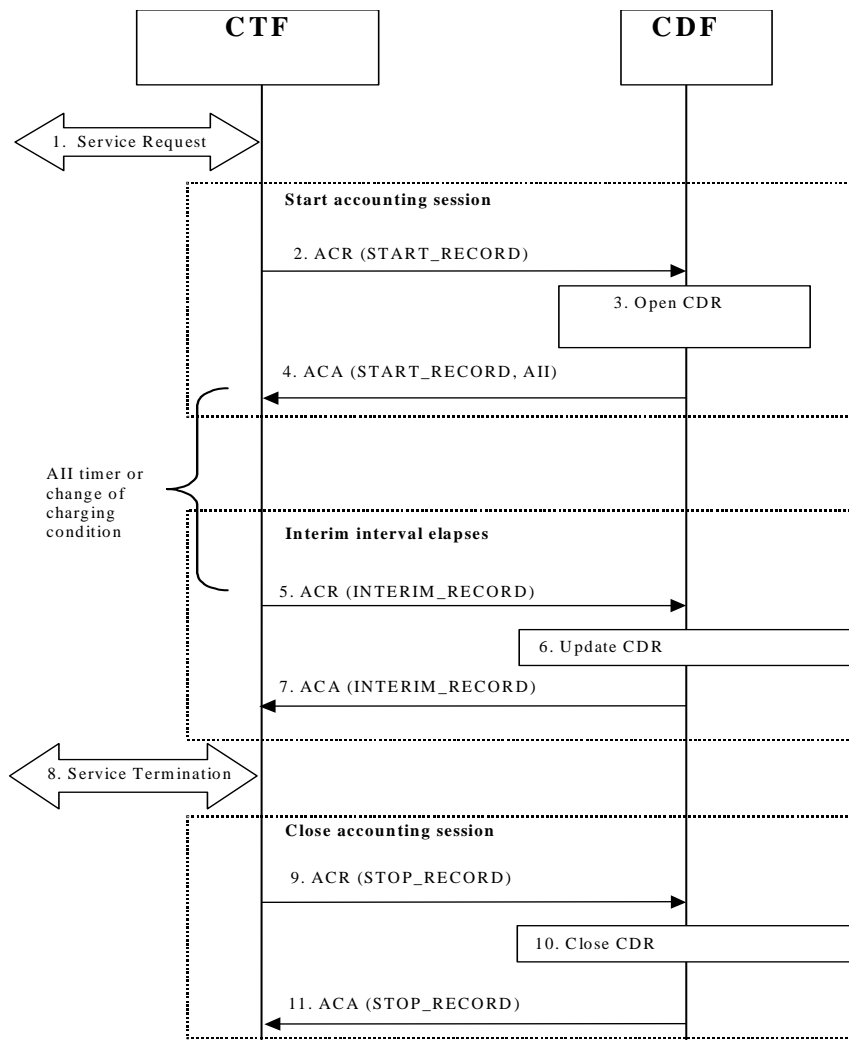


Figure 6.1.2: Session based offline charging

- Step 1: The network element receives a service request. The service request may be initiated either by the user or the other network element.
- Step 2: In order to start accounting session, the network element sends a *Accounting-Request* (ACR) with *Accounting-Record-Type* AVP set to START_RECORD to the CDF.
- Step 3: The CDF opens a CDR for current session.
- Step 4: The CDF returns *Accounting-Answer* (ACA) message with *Accounting-Record-Type* set to START_RECORD to the network element and possibly *Acct-Interim-Interval* AVP (AII) set to non-zero value indicating the desired intermediate charging interval.
- Step 5: When either AII elapses or charging conditions changes are recognized at Network Element (NE), the NE sends an *Accounting-Request* (ACR) with *Accounting-Record-Type* AVP set to INTERIM_RECORD to the CDF.
- Step 6: The CDF updates the CDR in question.
- Step 7: The CDF returns *Accounting-Answer* (ACA) message with *Accounting-Record-Type* set to INTERIM_RECORD to the network element.
- Step 8: The service is terminated.

- Step 9: The network element sends a *Accounting-Request (ACR)* with *Accounting-Record-Type* AVP set to *STOP_RECORD* to the CDF.
- Step 10: The CDF updates the CDR accordingly and closes the CDR.
- Step 11: The CDF returns *Accounting-Answer (ACA)* message with *Accounting-Record-Type* set to *STOP_RECORD* to the network element.

6.1.3 Offline charging error cases - Diameter procedures

6.1.3.1 CDF Connection Failure

When the connection towards the primary CDF is broken, the process of sending accounting information should continue towards a secondary CDF (if such a CDF is configured). For further CDF connection failure functionality, see subclause "*Transport Failure Detection*" in the RFC 3588 [401].

If no CDF is reachable the network element may buffer the generated accounting data in non-volatile memory. Once the CDF connection is working again, all accounting messages stored in the buffer is sent to the CDF, in the order they were stored in the buffer.

6.1.3.2 No Reply from CDF

In case a network element does not receive an ACA in response to an ACR, it may retransmit the ACR message. The waiting time until a retransmission is sent, and the maximum number of repetitions are both configurable by the operator. When the maximum number of retransmissions is reached and still no ACA reply has been received, the network element executes the CDF connection failure procedure as specified above.

If retransmitted ACRs' are sent, they are marked with the T-flag as described in RFC 3588 [401], in order to allow duplicate detection in the CDF, as specified in the next subclause.

6.1.3.3 Duplicate Detection

A Diameter client marks possible duplicate request messages (e.g. retransmission due to the link fail over process) with the T-flag as described in RFC 3588 [401].

If the CDF receives a message that is marked as retransmitted and this message was already received, then it discards the duplicate message. However, if the original of the re-transmitted message was not yet received, it is the information in the marked message that is taken into account when generating the CDR. The CDRs are marked if information from duplicated message(s) is used.

6.1.3.4 CDF Detected Failure

The CDF closes a CDR when it detects that expected Diameter ACRs for a particular session have not been received for a period of time. The exact behaviour of the CDF is operator configurable.

6.2 Message Contents for Offline Charging

6.2.1 Summary of Offline Charging Message Formats

6.2.1.1 General

The corresponding Diameter accounting application messages for the Charging Data Transfer operation is Accounting Request (ACR) and Accounting Answer (ACA) as specified in the Diameter Base Protocol Accounting (DBPA) application [401].

The following table describes the use of these messages for offline charging.

Table 6.2.1.1: Offline Charging Messages Reference Table

Command-Name	Source	Destination	Abbreviation
Accounting-Request	CTF	CDF	ACR
Accounting-Answer	CDF	CTF	ACA

6.2.1.2 Structure for the Accounting Message Formats

The following is the basic structure shared by all offline charging messages. This is based directly on the format of the messages defined in the Diameter Base Protocol Application specification [401].

Those Diameter Accounting AVPs that are used for 3GPP Offline Charging are marked in the table 6.2.2 and table 6.2.3 with a category as specified in TS 32.240 [1].

An AVP in grey strikethrough in the message format (in grey in the tables) is not used by 3GPP.

The following symbols are used in the message format definition:

- <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 is possible.

6.2.2 Accounting-Request Message

The ACR messages, indicated by the Command-Code field set to 271 is sent by the CTF to the CDF in order to sent charging information for the request bearer / subsystem /service.

The ACR message format is defined according to the Diameter Base Protocol [401] as follows:

```
<ACR> ::= < Diameter Header: 271, REQ, PXY >

< Session-Id >
{ Origin-Host }
{ Origin-Realm }
{ Destination-Realm }
{ Accounting-Record-Type }
{ Accounting-Record-Number }
[ Acct-Application-Id ]
{ Vendor-Specific-Application-Id }
[ User-Name ]
{ Accounting-Sub-Session-Id }
{ Acct-Session-Id }
{ Acct-Multi-Session-Id }
[ Acct-Interim-Interval ]
{ Accounting-Realtime-Required }
[ Origin-State-Id ]
[ Event-Timestamp ]
* [ Proxy-Info ]
```

- * [Route-Record]
- [Service-Context-Id]
- [Service-Information]
- * [AVP]

NOTE: Similar information as in subscription_id should be added as 3GPP parameter, IMEI.

Table 6.2.2 illustrates the basic structure of a 3GPP Diameter *Accounting-Request* message as used for 3GPP offline charging.

Table 6.2.2: 3GPP Accounting-Request Message Contents

AVP	Category	Description
Session-Id	M	This field identifies the operation session.
Origin-Host	M	This field contains the identification of the source point of the operation and the realm of the operation originator.
Origin-Realm	M	This field contains the realm of the operation originator.
Destination-Realm	M	This field contains the realm of the operator domain. The realm will be addressed with the domain address of the corresponding public URI.
Accounting-Record-Type	M	This field defines the transfer type: event for event based charging and start, interim, stop for session based charging.
Accounting-Record-Number	M	This field contains the sequence number of the transferred messages.
Acct-Application-Id	O _M	The field corresponds to the application ID of the Diameter Accounting Application and is defined with the value 3.
Vendor-Specific-Application-Id	-	Not used in 3GPP.
Vendor-Id	-	Not used in 3GPP.
Auth-Application-Id	-	Not used in 3GPP.
Acct-Application-Id	-	Not used in 3GPP.
User-Name	O _C	Contains the user name determined by the domain: bearer, sub-system or service as described in middle tier TS.
Accounting-Sub-Session-Id	-	Not used in 3GPP.
Accounting-Session-Id	-	Not used in 3GPP.
Acct-Multi-Session-Id	-	Not used in 3GPP.
Acct-Interim-Interval	O _C	
Accounting-Realtime-Required	-	Not used in 3GPP.
Origin-State-Id	O _C	This field contains the state associated to the CTF.
Event-Timestamp	O _C	This field corresponds to the exact time the accounting is requested.
Proxy-Info	O _C	This field contains information of the host.
Proxy-Host	M	This field contains the identity of the host that added the Proxy-Info field.
Proxy-State	M	This field contains state local information.
Route-Record	O _C	This field contains an identifier inserted by a relaying or proxying node to identify the node it received the message from.
Service-Context-Id	O _M	This field indicates the service and the corresponding 'middle tier' TS.
Service-Information	O _M	This parameter holds the individual service specific parameters as defined in the corresponding "middle tier" TS.
AVP	O _C	

NOTE: A detailed description of the AVPs is provided in clause 7.

6.2.3 Accounting-Answer Message

The Accounting Answer (ACA) messages, indicated by the Command-Code field set to 271 is sent by the CDF to the CTF in order to reply to the ACR.

The ACA message format is defined according to the Diameter Base Protocol [401] as follows:

```
<ACA> ::= < Diameter Header: 271, PXY >

    < Session-Id >
    { Result-Code }
    { Origin-Host }
    { Origin-Realm }
    { Accounting-Record-Type }
    { Accounting-Record-Number }
    [ Acct-Application-Id ]
    [Vendor-Specific-Application-Id]
    [ User-Name ]
    [Accounting-Sub-Session-Id]
    [Acct-Session-Id]
    [Acct-Multi-Session-Id]
    [Error-Reporting-Host]
    [ Acct-Interim-Interval ]
    [Accounting-Realtime-Required]
    [ Origin-State-Id ]
    [ Event-Timestamp ]
    * [ Proxy-Info ]
    * [ AVP ]
```

Table 6.2.3 illustrates the basic structure of a 3GPP Diameter *Accounting-Answer* message as used for offline charging. This message is always used by the CDF as specified below, regardless of the CTF it is received from and the ACR record type that is being replied to.

Table 6.2.3: 3GPP Accounting-Answer (ACA) Message Content

AVP	Category	Description
Session-Id	M	This field identifies the operation session.
Result-Code	M	This field contains the result of the specific query.
Origin-Host	M	This field contains the identification of the source point of the operation and the realm of the operation originator.
Origin-Realm	M	This field contains the realm of the operation originator.
Accounting-Record-Type	M	This field defines the transfer type: event for event based charging and start, interim, stop for session based charging.
Accounting-Record-Number	M	This field contains the sequence number of the transferred messages.
Acct-Application-Id	O _M	The field corresponds to the application ID of the Diameter Accounting Application and is defined with the value 3.
Vendor-Specific-Application-Id	-	Not used in 3GPP
Vendor-Id	-	Not used in 3GPP
Auth-Application-Id	-	Not used in 3GPP
Acct-Application-Id	-	Not used in 3GPP
User-Name	O _C	Contains the user name determined by the domain: bearer, sub-system or service as described in middle tier TS.
Accounting-Sub-Session-Id	-	Not used in 3GPP
Accounting-RADIUS-Session-Id	-	Not used in 3GPP
Acct-Multi-Session-Id	-	Not used in 3GPP
Error-Reporting-Host	O _C	This field contains the identity of the Diameter host that sent the Result-Code AVP to a value other than 2001 (Success) if the host setting the Result-Code is different from the one encoded in the Origin-Host AVP.
Acct-Interim-Interval	O _C	
Accounting-Realtime-Required	-	Not used in 3GPP
Origin-State-Id	O _C	
Event-Timestamp	O _C	This field contains the time when the operation is requested.
Proxy-Info	O _C	This field contains information of the host.
Proxy-Host	M	This field contains the identity of the host that added the Proxy-Info field.
Proxy-State	M	This field contains state local information.

AVP	Category	Description
AVP	O _C	Not used in 3GPP

6.3 Basic Principles for Diameter Online charging

Editor's note: This clause has been added to update the document to the Rel-6 IETF dependency on the Diameter Credit Control Application and currently does not exist in the 3GPP Rel-5 3GPP TS 32.225.

Page: 44

Here we have:

- Basic principles
- List of mandatory Diameter Credit Control Application AVPs used for online charging,
- No 3GPP AVPs unless they MUST be used every and each domain
- Basic client - server signalling flow showing how CCR/CCA is used
- Signalling flows for and + other common methods
- (Maybe) Content of CCR/CCA in INITIAL/UPDATE/TERMINATE/EVENT cases

6.3.1 Online Specific Credit Control Application Requirements

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 online client (CTF) requests resource allocation and reports credit control information to the Online Charging System (OCS).

The usage and values of *Validity-Time* AVP and the timer "Tcc" are under the sole control of the credit control server (OCS) and determined by operator configuration of the OCS.

Editor's note: There may be a requirement to add a minimum value for the *Validity-Time* AVP. It may need to be moved the subsection where the *Validity-Time* AVP is handled.

The online client implements the state machine described in IETF RFC 4006 [402] for "CLIENT, EVENT BASED" and/or "CLIENT, SESSION BASED". I.e. when the client applies IEC it uses the "CLIENT, EVENT BASED" state machine, and when the client applies ECUR it uses the "CLIENT, SESSION BASED" state machine for the first, intermediate and final interrogations.

The OCS implements the state machine described in IETF RFC 4006 [402] for the "SERVER, SESSION AND EVENT BASED" in order to support Immediate Event Charging and Event Charging with Unit Reservation.

6.3.2 Diameter Description on the Ro reference point

Editor's note: Message flows and scenarios should be moved into clause 5.

6.3.2.1 Basic Principles

For online charging the Diameter Credit Control Application (DCCA) defined in IETF RFC 4006 [402] is used with additional AVPs defined in the present document.

Three cases for control of user credit for online charging are distinguished:

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

In the case of Immediate Event Charging (IEC), the credit control process for events is controlled by the corresponding *CC-Requested-Type* EVENT_REQUEST that is sent with *Credit-Control-Request* (CCR) for a given credit control event.

In the case of Event Charging with Unit Reservation (ECUR) the *CC-Request-Type* INITIAL / TERMINATION_REQUEST are used for charging for a given credit control event, however, where a reservation is made prior to service delivery and committed on execution of a successful delivery.

Session Charging with Unit Reservation is used for credit control of sessions and uses the *CC-Request-Type* INITIAL / UPDATE and TERMINATION_REQUEST.

The network element may apply IEC, where CCR Event messages are generated, or ECUR, using CCR Initial, Termination and Update. The decision whether to apply IEC or ECUR is based on the service and/or operator's policy.

6.3.3 Immediate Event Charging (IEC)

Figure 6.3.3 shows the transactions that are required on the Ro reference point in order to perform event based Direct Debiting operation. The Direct Debiting operation may alternatively be carried out prior to service/content delivery. The Network Element must ensure that the requested service execution is successful, when this scenario is used.

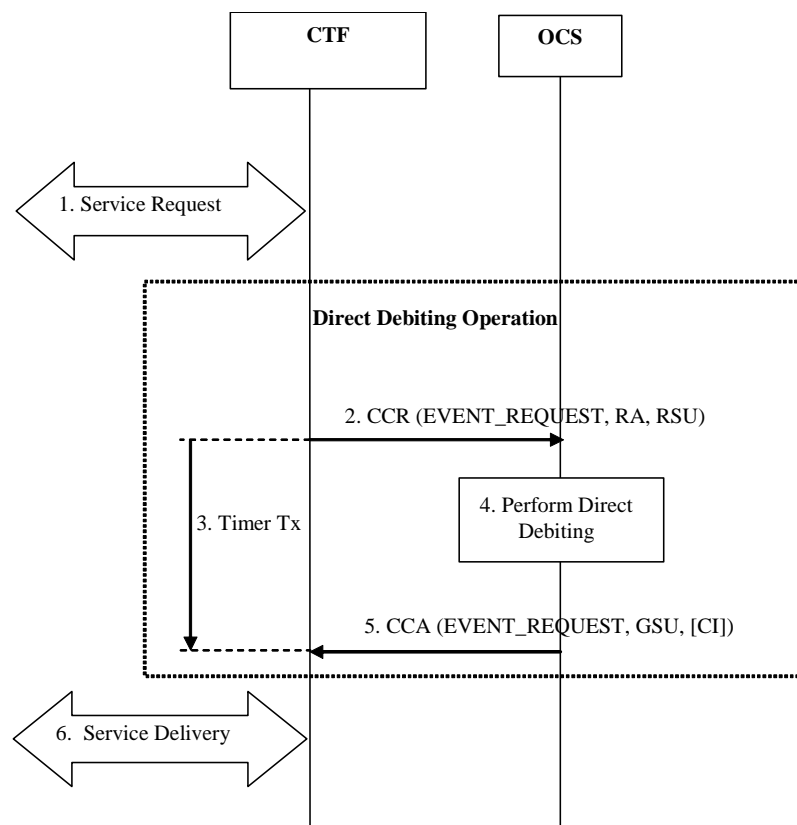


Figure 6.3.3: IEC Direct Debiting Operation

- Step 1. The network element receives a service request.
- Step 2. The Direct Debiting Operation is performed as described in IETF RFC 4006 [402]. The network element performs direct debiting prior to service execution. Network element (acting as DCCA client) sends *Credit-Control-Request* (CCR) with *CC-Request-Type* AVP set to EVENT_REQUEST to indicate service specific information to the OCS (acting as DCCA server). The *Requested-Action* AVP (RA) is set to DIRECT_DEBITING. If known, the network element may include *Requested-Service-Unit* AVP (RSU) (monetary or non-monetary units) in the request message.
- Step 3. Having transmitted the *Credit-Control-Request* message the network element starts the communication supervision timer 'Tx' (IETF RFC 4006 [402]). Upon receipt of the *Credit-Control- Answer* (CCA) message the network element shall stop timer Tx.
- Step 4. The OCS determines the relevant service charging parameters .

- Step 5. The OCS returns *Credit-Control-Answer* message with *CC-Request-Type* AVP set to *EVENT_REQUEST* to the network element in order to authorize the service execution (*Granted-Service-Unit* AVP (GSU) and possibly *Cost-Information* AVP (CI) indicating the cost of the service are included in the *Credit-Control-Answer* message). The *Credit-Control-Answer* message has to be checked by the network element accordingly and the requested service is controlled concurrently with service delivery.
- Step 6. Service is being delivered.

NOTE: It is possible to perform also *REFUND_ACCOUNT*, *CHECK_BALANCE* and *PRICE_ENQUIRY* using above described mechanism IETF RFC 4006 [402].

6.3.4 Event Charging with Unit Reservation (ECUR)

Figure 6.3.4 shows the transactions that are required on the Ro reference point in order to perform the ECUR. ECUR is used when event charging needs separate reserve and commit actions.

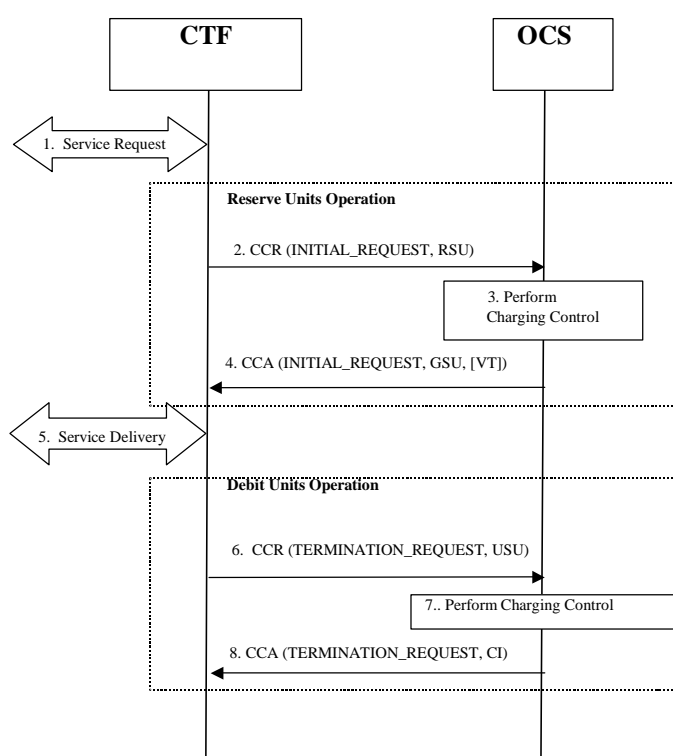


Figure 6.3.4: ECUR for session based credit control

- Step 1. The network element receives a service request. The service request may be initiated either by the user or the other network element.
- Step 2. In order to perform Reserve Units operation for a number of units (monetary or non-monetary units), the network element sends a *Credit-Control-Request* (CCR) with *CC-Request-Type* AVP set to *INITIAL_REQUEST* to the OCS. If known, the network element may include *Requested-Service-Unit* (RSU) AVP (monetary or non monetary units) in the request message.

- Step 3. If the service cost information is not received by the OCS, the OCS determines the price of the desired service according to the service specific information received by issuing a rating request to the Rating Function. If the cost of the service is included in the request, the OCS directly reserves the specified monetary amount. If the credit balance is sufficient, the OCS reserves the corresponding amount from the users account.
- Step 4. Once the reservation has been made, the OCS returns *Credit-Control-Answer* (CCA) message with *CC-Request-Type* set to INITIAL_REQUEST to the network element in order to authorize the service execution (*Granted-Service-Unit* and possibly *Cost-Information* indicating the cost of the service are included in the *Credit-Control-Answer* message). The OSC may return the *Validity-Time* (VT) AVP with value field set to a non-zero value.
- Step 5. Content/service delivery starts and the reserved units are concurrently controlled.
- Step 6. When content/service delivery is completed, the network element sends CCR with *CC-Request-Type* AVP set to TERMINATION_REQUEST to terminate the active credit control session and report the used units.
- Step 7. The OCS deducts the amount used from the account. Unused reserved units are released, if applicable.
- Step 8. The OCS acknowledges the reception of the CCR message by sending CCA message with *CC-Request-Type* AVP indicating TERMINATION_REQUEST (possibly *Cost-Information* AVP indicating the cumulative cost of the service is included in the *Credit-Control-Answer* message).

NOTE: This scenario is supervised by corresponding timers (e.g. validity time timer) that are not shown in the figure 6.3.4.

6.3.5 Session Charging with Unit Reservation (SCUR)

Figure 6.3.5 shows the transactions that are required on the Ro reference point in order to perform the SCUR.

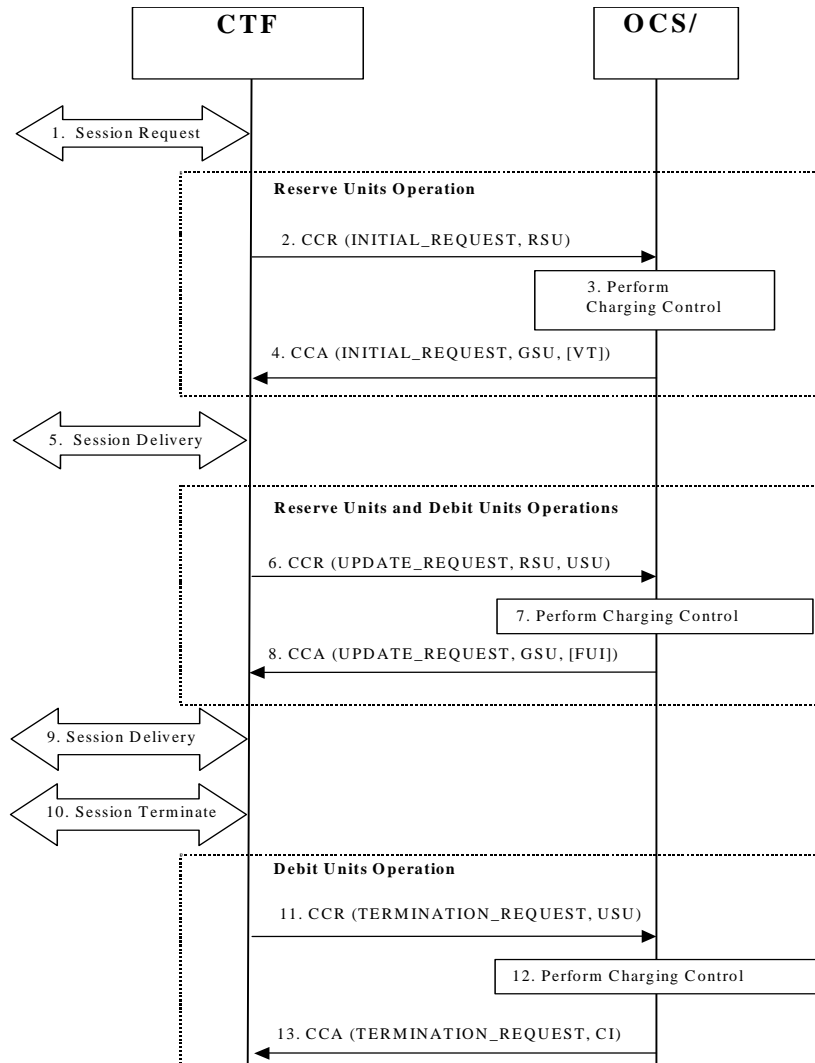


Figure 6.3.5: SCUR for session based credit control

- Step 1. The network element receives a session initiation. The session initiation may be done either by the user or the other network element.
- Step 2. In order to perform Reserve Units operation for a number of units (monetary or non-monetary units), the network element sends a *Credit-Control-Request* (CCR) with *CC-Request-Type* AVP set to INITIAL_REQUEST to the OCS. If known, the network element may include *Requested-Service-Unit* (RSU) AVP (monetary or non monetary units) in the request message.
- Step 3. If the service cost information is not received by the OCS, the OCS determines the price of the desired service according to the service specific information received by issuing a rating request to the Rating Function. If the cost of the service is included in the request, the OCS directly reserves the specified monetary amount. If the credit balance is sufficient, the OCS reserves the corresponding amount from the users account.
- Step 4. Once the reservation has been made, the OCS returns *Credit-Control-Answer* (CCA) message with *CC-Request-Type* set to INITIAL_REQUEST to the network element in order to authorize the service execution (*Granted-Service-Unit* and possibly *Cost-Information* indicating the cost of the service are included in the *Credit-Control-Answer* message). The OSC may return the *Validity-Time* (VT) AVP with value field set to a non-zero value.
- Step 5. Content/service delivery starts and the reserved units are concurrently controlled.

- Step 6. During session delivery, in order to perform Debit Units and subsequent Reserve Units operations, the network element sends a CCR with *CC-Request-Type* AVP set to UPDATE_REQUEST, to report the units used and request additional units, respectively. The CCR message with *CC-Request-Type* AVP set to UPDATE_REQUEST must be sent by the network element between the INITIAL_REQUEST and TERMINATION_REQUEST either on request of the credit control application within the validity time or if the validity time is elapsed. If known, the network element may include *Requested-Service-Unit* AVP (monetary or non monetary units) in the request message. The *Used-Service-Unit* (USU) AVP is complemented in the CCR message to deduct units from both the user's account and the reserved units, respectively.
- Step 7. The OCS deducts the amount used from the account. If the service cost information is not received by the OCS, the OCS determines the price of the desired service according to the service specific information received by issuing a rating request to the Rating Function. If the cost of the service is included in the request, the OCS directly reserves the specified monetary amount. If the credit balance is sufficient, the OCS reserves the corresponding amount from the users account.
- Step 8. Once the deduction and reservation have been made, the OCS returns *Credit-Control-Answer* message with *CC-Request-Type* set to UPDATE_REQUEST to the network element, in order to allow the content/service delivery to continue (new *Granted-Service-Unit* (GSU) AVP and possibly *Cost-Information* (CI) AVP indicating the cumulative cost of the service are included in the *Credit-Control-Answer* message). The OCS may include in the CCA message the *Final-Unit-Indication* (FUI) AVP to indicate the final granted units.
- Step 9. Session delivery continues and the reserved units are concurrently controlled.
- Step 10. The session is terminated at the network element.
- Step 11. The network element sends CCR with *CC-Request-Type* AVP set to TERMINATION_REQUEST to terminate the active credit control session and report the used units.
- Step 12. The OCS deducts the amount used from the account. Unused reserved units are released, if applicable.
- Step 13. The OCS acknowledges the reception of the CCR message by sending CCA message with *CC-Request-Type* AVP indicating TERMINATION_REQUEST (possibly *Cost-Information* AVP indicating the cumulative cost of the service is included in the *Credit-Control-Answer* message).

NOTE: This scenario is supervised by corresponding timers (e.g. validity time timer) that are not shown in figure 6.3.5.

6.3.6 Error Cases and Scenarios

This subclause describes various error cases and how these should be handled.

The failure handling behaviour is locally configurable in the network element. If the *Direct-Debiting-Failure-Handling* or *Credit-Control-Failure-Handling* AVP is not used, the locally configured values are used instead.

6.3.6.1 Duplicate Detection

The detection of duplicate request is needed and must be enabled. To speed up and simplify as much as possible the duplicate detection, the all-against-all record checking should be avoided and just those records marked as potential duplicates need to be checked against other received requests (in real-time) by the receiver entity.

The network element marks the request messages that are retransmitted after a link fail over as possible duplicates with the T-flag as described in [401]. For optimized performance, uniqueness checking against other received requests is only necessary for those records marked with the T-flag received within a reasonable time window. This focused check is based on the inspection of the *Session-Id* and *CC-Request-Number* AVP pairs.

Note that for EBCC the duplicate detection is performed in the Correlation Function that is part of the OCS. The OCS that receives the possible duplicate request should mark as possible duplicate the corresponding request that is sent over the 'Rc' reference point. However, this assumption above is for further study and needs to be clarified.

For credit control duplicate detection, please refer to the Diameter Credit Control.

6.3.6.2 Reserve Units and Debit Units Operation Failure

In the case of an OCS connection failure, and/or receiving error responses from the OCS, please refer to RFC 3588 [401] and RFC 4006 [402] for failure handling descriptions.

6.3.7 Support of Tariff Changes during an Active User Session

6.3.7.1 Support of Tariff Changes using the Tariff Switch Mechanism

After a tariff switch has been reached, all the active user sessions shall report their session usage by the end of the validity period of the current request and receive new quota for resource usage for the new tariff period.

In order to avoid the need for mass simultaneous quota refresh, the traffic usage can be split into resource usage before a tariff switch and resources used after a tariff switch.

The Tariff-Time-Change AVP is used to determine the tariff switch time as described by IETF RFC 4006 [402]. In addition to the scenarios described in IETF RFC 4006 [402], the Tariff-Time-Change AVP may also be used in the context of continuously time-based charging.

The Tariff-Change-Usage AVP is used within the Used-Service-Units AVP to distinguish reported usage before and after the tariff time change.

The Tariff-Change-Usage AVP is used within the Multiple-Services-Credit-Control AVP to allow separate quota to be reported before and after the tariff switch. If this AVP is not present, the granted quota may be consumed both before and after the tariff switch, but usage can not be reported separately.

6.3.7.2 Support of Tariff Changes using Validity Time AVP

Changes to the tariffs pertaining to the service during active user sessions may also be handled using the Validity Time AVP as described by IETF RFC 4006 [402].

Editor's note: Additional details need to be added.

6.3.8 Support of Re-authorisation

Mid Diameter CC session re-authorisations of multiple active resource quotas within a DCC session can be achieved using a single Diameter *Credit Control Request/Answer* message sequence.

The OCS may also re-authorise multiple active resource quotas within a DCC session by using a single Diameter *Re-Auth-Request/Answer* message sequence.

New quota allocations received by the Network Element override any remaining held quota resources after accounting for any resource usage while the re-authorisation was in progress.

6.3.9 Support of Failure Handling

The Credit-Control-Failure-Handling AVP as defined in IETF RFC 4006 [402] determines what to do if the sending of Diameter credit-control messages to the OCS has been temporarily prevented. The usage of Credit-Control-Failure-Handling AVP gives flexibility to have different failure handling for credit-control session.

This AVP may be received from the OCS or may be locally configured. The value received from the OCS in the Diameter Credit-Control-Answer message always override any already existing value.

As defined in IETF RFC 4006 [402], the Tx timer is introduced to limit the waiting time in the CTF for an answer to the credit control request sent to the OCS. When the Tx timer elapses the CTF takes an action to the end user according to the value of the Credit-Control-Failure-Handling AVP.

It is possible that several concurrent Credit Control Request messages are triggered for the same online charging session. In this case, each Credit Control Request message shall reset the Tx timer as defined in IETF RFC 4006 [402].

6.3.10 Support of Failover

As defined in IETF RFC 4006 [402] if a failure occurs during an ongoing credit-control session, the CTF may move the credit control message stream to an alternative OCS if the primary OCS indicated `FAILOVER_SUPPORTED` in the `CC-Session-Failover` AVP. In case `CC-Session-Failover` AVP is set to `FAILOVER_NOT_SUPPORTED` the credit control message stream is not moved to a backup OCS.

For new credit control sessions, failover to an alternative OCS should be performed if possible. For instance, if an implementation of the CTF can determine primary OCS unavailability it can establish the new credit control sessions with a possibly available secondary OCS.

Since the OCS has to maintain session states, moving the credit-control message stream to a backup OCS requires a complex charging context transfer solution. This charging context transfer mechanism by OCS is out of the scope of the 3GPP standardization work.

6.3.11 Credit Pooling

Credit pooling shall be supported as described in TS 32.240 [1].

Note: Credit pooling is not applicable to IEC since there is no quota management between CTF and OCF.

6.4 Message formats for Online Charging

6.4.1 Summary of Online Charging Message Formats

6.4.1.1 General

The corresponding Diameter credit control application messages for the Debit / Reserve Unit Request operation is Credit-Control-Request (CCR) and for the Debit / Reserve Unit Response operation is Credit-Control-Answer (CCA) as specified in IETF RFC 4006 [402].

The Diameter Credit-Control Application (DCCA) specifies an approach based on a series of "interrogations":

- Initial interrogation.
- Zero, one or more interim interrogations.
- Final interrogation.

In addition to a series of interrogations, also a one time event (interrogation) can be used e.g. in the case when service execution is always successful.

All of these interrogations use *Credit-Control-Request* and *Credit-Control-Answer* messages. The *Credit-Control-Request* for the "interim interrogation" and "final interrogation" reports the actual number of "units" that were used, from what was previously reserved. This determines the actual amount debited from the subscriber's account.

Table 6.4.1.1 describes the use of these Diameter messages for online charging.

Table 6.4.1.1: Online Charging Messages Reference Table

Command-Name	Source	Destination	Abbreviation
Credit-Control-Request	CTF	OCS	CCR
Credit-Control-Answer	OCS	CTF	CCA
Re-Auth-Request	OCS	CTF	RAR
Re-Auth-Answer	CTF	OCS	RAA
Capabilities-Exchange-Request	CTF	OCS	CER
Capabilities Exchange Answer	OCS	CTF	CEA
Device-Watchdog-Request	CTF/OCS	OCS/CTF	DWR
Device-Watchdog-Answer	OCS/CTF	CTF/OCS	DWA
Disconnect-Peer-Request	OCS/CTF	CTF/OCS	DPR
Disconnect-Peer-Answer	CTF/OCS	OCS/CTF	DPA
Abort-Session-Request	OCS	CTF	ASR
Abort-Session-Answer	CTF	OCS	ASA

CER/CEA and DWR/DWA are mandatory Diameter capabilities for capabilities exchange and transport failure detection.

6.4.1.2 Structure for the Credit Control Message Formats

The following is the basic structure shared by all online charging messages. This is based directly on the format of the messages defined in IETF RFC 4006 [402].

Those Diameter Accounting AVPs that are used for 3GPP online charging are marked in the table of contents 6.4.2 and 6.4.3 with a category as specified in TS 32.240 [1].

In the definition of the Diameter Commands, the AVPs that are specified in the referenced specifications but not used by the 3GPP charging specifications are marked with strikethrough, e.g. ~~{Acct-Multi-Session-Id}~~.

The following symbols are used in the message format definitions:

- <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 is possible.

6.4.2 Credit-Control-Request Message

The CCR messages, indicated by the Command-Code field set to 272 is sent by the CTF to the OCF in order to request credits for the request bearer / subsystem /service.

The CCR message format is defined according to IETF RFC 4006 [402] as follows:

```
<CCR> ::= < Diameter Header: 272, REQ, PXY >

    < Session-Id >
    { Origin-Host }
    { Origin-Realm }
    { Destination-Realm }
    { Auth-Application-Id }
    { Service-Context-Id }
    { CC-Request-Type }
    { CC-Request-Number }
    [ Destination-Host ]
    [ User-Name ]
{ CC-Sub-Session-Id }
{ Acct-Multi-Session-Id }
    [ Origin-State-Id ]
    [ Event-Timestamp ]
    *[ Subscription-Id ]
{ Service-Identifier }
    [ Termination-Cause ]
{ Requested-Service-Unit }
    [ Requested-Action ]
*{ Used-Service-Unit }
    [ Multiple-Services-Indicator ]
    *[ Multiple-Services-Credit-Control ]
*{ Service-Parameter-Info }
{ CC-Correlation-Id }
    [ User-Equipment-Info ]
    *[ Proxy-Info ]
    *[ Route-Record ]
    [ Service-Information ]
    *[ AVP ]
```

Table 6.4.2 illustrates the basic structure of a 3GPP Diameter Credit Control *Credit-Control-Request* message as used for Online Charging.

Table 6.4.2: 3GPP Credit-Control-Request Message Content

AVP	Category	Description
Session-Id	M	This field identifies the operation session.
Origin-Host	M	This field contains the identification of the source point of the operation and the realm of the operation originator.
Origin-Realm	M	This field contains the realm of the operation originator.
Destination-Realm	M	This field contains the realm of the operator domain. The realm will be addressed with the domain address of the corresponding public URI.
Auth-Application-Id	M	The field corresponds to the application ID of the Diameter Credit Control Application and is defined with the value 4.
Service-Context-Id	M	This field indicates the supported protocol version.
CC-Request-Type	M	This field defines the transfer type: event for event based charging and initial, update, terminate for session based charging.
CC-Request-Number	M	This field contains the sequence number of the transferred messages.
Destination-Host	O _C	This field contains the destination peer address of the OCS identity.
User-Name	O _C	Contains the user name determined by the domain: bearer, sub-system or service as described in middle tier TS.
CC-Sub-Session-Id	-	Not used in 3GPP.
Acct-Multi-Session-Id	-	Not used in 3GPP.
Origin-State-Id	O _C	This field contains the state associated to the CTF.
Event-Timestamp	O _C	This field corresponds to the exact time the quota is requested.
Subscription-Id	O _M	This field contains the identification of the user that is going to access the service in order to be identified by the OCS.
Subscription-Id-Type	O _M	This field determines the type of the identifier, e.g. t value 0 is used for the international E.164 format according to ITU-T E.164 numbering plan.
Subscription-Id-Data	O _M	This field contains the user data content e.g. the MSISDN.
Service-Identifier	-	Not used in 3GPP.
Termination-Cause	O _C	This field contains the reason the credit control session was terminated.
Requested-Service-Unit	-	Not used in 3GPP, see Multiple-Services-Credit-Control.
CC-Time	-	Not used in 3GPP.
CC-Money	-	Not used in 3GPP.
Unit-Value	-	Not used in 3GPP.
Value-Digits	-	Not used in 3GPP.
Exponent	-	Not used in 3GPP.
Currency-Code	-	Not used in 3GPP.
CC-Total-Octets	-	Not used in 3GPP.
CC-Input-Octets	-	Not used in 3GPP.
CC-Output-Octets	-	Not used in 3GPP.
CC-Service-Specific-Units	-	Not used in 3GPP.
AVP	-	Not used in 3GPP.
Requested-Action	O _C	The field defines the type of action if the CC-Request-Type indicates EVENT.
Used-Service-Unit	-	Not used in 3GPP, see Multiple-Services-Credit-Control.
Tariff-Change-Usage	-	Not used in 3GPP.
CC-Time	-	Not used in 3GPP.
CC-Money	-	Not used in 3GPP.
Unit-Value	-	Not used in 3GPP.
Value-Digits	-	Not used in 3GPP.
Exponent	-	Not used in 3GPP.
Currency-Code	-	Not used in 3GPP.
CC-Total-Octets	-	Not used in 3GPP.
CC-Input-Octets	-	Not used in 3GPP.
CC-Output-Octets	-	Not used in 3GPP.
CC-Service-Specific-Units	-	Not used in 3GPP.
AVP	-	Not used in 3GPP.
Multiple-Services-Indicator	O _M	This field indicates whether the CTF is capable of handling multiple services independently.
Multiple-Services-Credit Control	O _M	This field contains all parameters for the CTF quota management and defines the quotas to allow traffic to flow.

Granted-Service-Unit	-	Not used in CCR.
Tariff-Change-Usage	-	Not used in CCR.
CC-Time	-	Not used in CCR.
CC-Money	-	Not used in CCR.
Unit-Value	-	Not used in CCR.
Value-Digits	-	Not used in CCR.
Exponent	-	Not used in CCR.
Currency-Code	-	Not used in CCR.
CC-Total-Octets	-	Not used in CCR.
CC-Input-Octets	-	Not used in CCR.
CC-Output-Octets	-	Not used in CCR.
CC-Service-Specific-Units	-	Not used in CCR.
AVP	-	Not used in 3GPP.
Requested-Service-Unit	O _c	This field contains the amount of requested service units for a particular category.
CC-Time	O _c	This field contains the amount of requested time.
CC-Money	-	Not used in 3GPP.
Unit-Value	-	Not used in 3GPP.
Value-Digits	-	Not used in 3GPP.
Exponent	-	Not used in 3GPP.
Currency-Code	-	Not used in 3GPP.
CC-Total-Octets	O _c	This field contains the requested amount of octets to be sent and received.
CC-Input-Octets	O _c	This field contains the requested amount of octets to be received.
CC-Output-Octets	O _c	This field contains the requested amount of octets to be sent.
CC-Service-Specific-Units	O _c	This field contains the requested amount of service specific units, e.g. number of events.
AVP	-	Not used in 3GPP.
Used-Service-Unit	O _c	This field contains the amount of used non-monetary service units measured for a particular category to a particular quota type.
Reporting-Reason	O _c	Used as defined in clause 7.2.
Tariff-Change-Usage	O _c	This field identifies the reporting period for the used service unit, i.e. before, after or during tariff change.
CC-Time	O _c	This field contains the amount of used time.
CC-Money	-	Not used in 3GPP.
Unit-Value	-	Not used in 3GPP.
Value-Digits	-	Not used in 3GPP.
Exponent	-	Not used in 3GPP.
Currency-Code	-	Not used in 3GPP.
CC-Total-Octets	O _c	This field contains the amount of sent and received octets.
CC-Input-Octets	O _c	This field contains the amount of received octets.
CC-Output-Octets	O _c	This field contains the amount of sent octets.
CC-Service-Specific-Units	O _c	This field contains the amount of service specific units, e.g. number of events.
Event-Charging-TimeStamp	O _c	Used as defined in clause 7.2.
AVP	-	Not used in 3GPP.
Tariff-Change-Usage	-	Not used in 3GPP.
Service-Identifier	O _c	This field contains identity of the used service. This ID with the Service-Context-ID together forms an unique identification of the service.
Rating-Group	O _c	This field contains the identifier of a rating group.
G-S-U-Pool-Reference	-	Not used in CCR.
G-S-U-Pool-Identifier	-	Not used in CCR.
CC-Unit-Type	-	Not used in CCR.
Unit-Value	-	Not used in CCR.
Value-Digits	-	Not used in CCR.
Exponent	-	Not used in CCR.
Validity-Time	-	Not used in CCR.
Result-Code	-	Not used in CCR.
Final-Unit-Indication	-	Not used in CCR.
Final-Unit-Action	-	Not used in CCR.
Restriction-Filter-Rule	-	Not used in CCR.
Filter-Id	-	Not used in CCR.
Redirect-Server	-	Not used in CCR.
Redirect-Address-Type	-	Not used in CCR.
Redirect-Server-Address	-	Not used in CCR.

Time-Quota-Threshold	-	Not used in CCR.
Volume-Quota-Threshold	-	Not used in CCR.
Quota-Holding-Time	-	Not used in CCR.
Quota-Consumption-Time	-	Not used in CCR.
Reporting-Reason	O _C	Used as defined in clause 7.2.
Trigger-Type	O _C	Used as defined in clause 7.2.
AVP	-	Not used in 3GPP.
Service-Parameter-Info	-	Not used in 3GPP.
Service-Parameter-Type	-	Not used in 3GPP.
Service-Parameter-Value	-	Not used in 3GPP.
CC-Correlation-Id	-	Not used in 3GPP.
User-Equipment-Info	O _C	This field contains the identification of the identity and terminal capability the subscriber is using for the connection to mobile network if available.
User-Equipment-Info-Type	M	This field determines the type of the identifier. The used value is 0 for the international mobile equipment identifier and software version according to 3GPP TS 23.003.
User-Equipment-Info-Value	M	This field contains the user IMEISV.
Proxy-Info	O _C	This field contains information of the host.
Proxy-Host	M	This field contains the identity of the host that added the Proxy-Info field.
Proxy-State	M	This field contains state local information.
Route-Record	O _C	This field contains an identifier inserted by a relaying or proxying node to identify the node it received the message from.
Service-Information	O _M	This parameter holds the individual service specific parameters as defined in the corresponding "middle tier" TS.
AVP	O _C	

6.4.3 Credit-Control-Answer Message

The Credit-Control-Answer (CCA) messages, indicated by the Command-Code field set to 272 is sent by the OCF to the CTF in order to reply to the CCR.

The CCA message format is defined according to IETF RFC 4006 [402] as follows:

```
<CCA> ::= < Diameter Header: 272, PXY >

    < Session-Id >
    { Result-Code }
    { Origin-Host }
    { Origin-Realm }
    { Auth-Application-Id }
    { CC-Request-Type }
    { CC-Request-Number }
    [User-Name]
    [ CC-Session-Failover ]
    [CC-Sub-Session-Id]
    [Acct-Multi-Session-Id]
    [Origin-State-Id]
    [Event-Timestamp]
    [Granted-Service-Unit]
    *[ Multiple-Services-Credit-Control ]
    [ Cost-Information ]
    [Final-Unit-Indication]
    [Check-Balance-Result]
    [ Credit-Control-Failure-Handling ]
    [Direct-Debiting-Failure-Handling]
    [Validity-Time]
    *[ Redirect-Host ]
    [ Redirect-Host-Usage ]
    [ Redirect-Max-Cache-Time ]
    *[ Proxy-Info ]
    *[ Route-Record ]
    *[ Failed-AVP ]
    [ Service-Information ]
    *[ AVP ]
```

Table 6.4.3 illustrates the basic structure of a 3GPP Diameter Credit-Control *Credit-Control-Answer* message as used for online charging. This message is always used by the OCF as specified below, independent of the receiving CTF and the CCR record type that is being replied to.

Table 6.4.3: 3GPP Credit-Control-Answer Message Content

AVP	Category	Description
Session-Id	M	This field identifies the operation session.
Result-Code	M	This field contains the result of the specific query.
Origin-Host	M	This field contains the identification of the source point of the operation and the realm of the operation originator.
Origin-Realm	M	This field contains the realm of the operation originator.
Auth-Application-Id	M	The field corresponds to the application ID of the Diameter Credit Control Application and is defined with the value 4.
CC-Request-Type	M	This field defines the transfer type: initial, update, terminate for session based charging and event for event based charging.
CC-Request-Number	M	This field contains the sequence number of the transferred messages.
User-Name	-	Not used in 3GPP.
CC-Session Failover	O _C	This field contains an indication to the CTF whether or not a failover handling is to be used when necessary.
CC-Sub-session-Id	-	Not used in 3GPP.
Acct-Multi-Session-Id	-	Not used in 3GPP.
Origin-State-Id	-	Not used in 3GPP.
Event-Timestamp	-	Not used in 3GPP.
Granted-Service-Unit	-	Not used in 3GPP, see Multiple-Services-Credit-Control.
Tariff-Time-Change	-	Not used in 3GPP.
CC-Time	-	Not used in 3GPP.
CC-Money	-	Not used in 3GPP.
Unit-Value	-	Not used in 3GPP.
Value-Digits	-	Not used in 3GPP.
Exponent	-	Not used in 3GPP.
Currency-Code	-	Not used in 3GPP.
CC-Total-Octets	-	Not used in 3GPP.
CC-Input-Octets	-	Not used in 3GPP.
CC-Output-Octets	-	Not used in 3GPP.
CC-Service-Specific-Units	-	Not used in 3GPP.
AVP	-	Not used in 3GPP.
Multiple-Services-Credit-Control	O _M	This field contains all parameters for the CTF quota management and defines the quotas to allow traffic to flow.
Granted-Service-Unit	O _C	This field contains the amount of granted service units for a particular category.
Tariff-Time-Change	O _C	This field identifies the reporting period for the granted service units, i.e. before, after or during tariff change.
CC-Time	O _C	This field contains the amount of granted time.
CC-Money	-	Not used in 3GPP.
Unit-Value	-	Not used in 3GPP.
Value-Digits	-	Not used in 3GPP.
Exponent	-	Not used in 3GPP.
Currency-Code	-	Not used in 3GPP.
CC-Total-Octets	O _C	This field contains the amount for sent and received octets.
CC-Input-Octets	O _C	This field contains the amount for received octets.
CC-Output-Octets	O _C	This field contains the amount for sent octets.
CC-Service-Specific-Units	O _C	This field contains the amount for service specific units, e.g. number of events.
AVP	-	Not used in CCA.
Requested-Service-Unit	-	Not used in CCA.
Tariff-Time-Change	-	Not used in CCA.
CC-Time	-	Not used in CCA.
CC-Money	-	Not used in CCA.
Unit-Value	-	Not used in CCA.
Value-Digits	-	Not used in CCA.
Exponent	-	Not used in CCA.
Currency-Code	-	Not used in CCA.
CC-Total-Octets	-	Not used in CCA.

CC-Input-Octets	-	Not used in CCA.
CC-Output-Octets	-	Not used in CCA.
CC-Service-Specific-Units	-	Not used in CCA.
Used-Service-Unit	-	Not used in CCA.
Tariff-Time-Change	-	Not used in CCA.
CC-Time	-	Not used in CCA.
CC-Money	-	Not used in CCA.
Unit-Value	-	Not used in CCA.
Value-Digits	-	Not used in CCA.
Exponent	-	Not used in CCA.
Currency-Code	-	Not used in CCA.
CC-Total-Octets	-	Not used in CCA.
CC-Input-Octets	-	Not used in CCA.
CC-Output-Octets	-	Not used in CCA.
CC-Service-Specific-Units	-	Not used in CCA.
Tariff-Change-Usage	-	Not used in 3GPP.
Service-Identifier	O _C	This field contains identity of the used service. This ID with the Service-Context-ID together forms an unique identification of the service.
Rating-Group	O _C	This field contains the identifier of a rating group.
G-S-U-Pool-Reference	O _C	Only used in ECUR and SCUR.
G-S-U-Pool-Identifier	M	
CC-Unit-Type	M	
Unit-Value	M	
Value-Digits	M	
Exponent	O _C	
Validity-Time	O _C	This field defines the time in order to limit the validity of the granted quota for a given category instance.
Result-Code	O _C	This field contains the result of the query.
Final-Unit-Indication	O _C	This field indicates that the Granted-Service-Unit containing the final units for the service.
Final-Unit-Action	O _C	
Restriction-Filter-Rule	O _C	
Filter-Id	O _C	
Redirect-Server	O _C	
Redirect-Address-Type	M	
Redirect-Server-Address	M	
Time-Quota-Threshold	O _C	Used as defined in clause 7.2.
Volume-Quota-Threshold	O _C	Used as defined in clause 7.2.
Unit-Quota-Threshold	O _C	Used as defined in clause 7.2.
Quota-Holding-Time	O _C	Used as defined in clause 7.2.
Quota-Consumption-Time	O _C	Used as defined in clause 7.2.
Reporting-Reason	-	Not used in CCA.
Trigger-Type	O _C	Used as defined in clause 7.2.
PS-Furnish-Charging-Information	O _C	Used as defined in clause 7.2.
AVP	-	Not used in 3GPP.
Cost-Information	O _C	Used as defined in DCCA [402].
Unit-Value	M	Used as defined in DCCA [402].
Value-Digits	M	Used as defined in DCCA [402].
Exponent	O _C	Used as defined in DCCA [402].
Currency-Code	M	Used as defined in DCCA [402].
Cost-Unit	O _C	Used as defined in DCCA [402].
Final-Unit-Indication	-	Not used in 3GPP, see Multiple-Services-Credit-Control.
Final-Unit-Action	-	Not used in 3GPP.
Restriction-Filter-Rule	-	Not used in 3GPP.
Filter-Id	-	Not used in 3GPP.
Redirect-Server	-	Not used in 3GPP.
Redirect-Address-Type	-	Not used in 3GPP.
Redirect-Server-Address	-	Not used in 3GPP.
Check-Balance-Result	-	Not used in 3GPP.
Credit-Control-Failure-Handling	O _C	Used as defined in DCCA [402].
Direct-Debiting-Failure-Handling	O _C	Used as defined in DCCA [402].
Validity-Time	-	Not used in 3GPP.
Redirect-Host	O _C	
Redirect-Host-Usage	O _C	

Redirect-Max-Cache-Time	O _C	
Proxy-Info	O _C	This field contains information of the host.
Proxy-Host	M	This field contains the identity of the host that added the Proxy-Info field.
Proxy-State	M	This field contains state local information.
Route-Record	O _C	This field contains an identifier inserted by a relaying or proxying node to identify the node it received the message from.
Failed-AVP	O _C	
Service-Information	O _C	This parameter holds the individual service specific parameters as defined in the corresponding "middle tier" TS.
AVP	O _C	

6.4.4 Re-Auth-Request Message

Table 6.4.4 illustrates the basic structure of a Diameter Credit Control *Re-Auth-Request* message as used for online charging.

Table 6.4.4: Re-Auth-Request (RAR) Message Contents for Online Charging

AVP	Category	Description
Session-Id	M	This field identifies the operation session.
Origin-Host	M	This field contains the identification of the source point of the operation and the realm of the operation originator.
Origin-Realm	M	This field contains the realm of the operation originator.
Destination-Realm	M	This field contains the realm of the operator domain. The realm will be addressed with the domain address of the corresponding public URI.
Destination-Host	M	This field contains the destination peer address of the OCS identity.
Auth-Application-Id	M	The field corresponds to the application ID of the Diameter Credit Control Application and is defined with the value 4.
Re-Auth-Request-Type	M	This field is used to inform the CTF of the action expected upon expiration of the Authorization-Lifetime
User-Name	O _C	This field contains the username.
Origin-State-Id	O _C	This field contains the state associated to the CTF.
Proxy-Info	O _C	This field contains information of the host.
Proxy-Host	M	This field contains the identity of the host that added the Proxy-Info field.
Proxy-State	M	This field contains state local information.
Route-Record	O _C	This field contains an identifier inserted by a relaying or proxying node to identify the node it received the message from.
CC-Sub-Session-Id	-	Not used in 3GPP.
G-S-U-Pool-Reference	O _C	
Service-Identifier	O _C	
Rating-Group	O _C	
AVP	O _C	

6.4.5 Re-Auth-Answer Message

Table 6.4.5 illustrates the basic structure of a Diameter Credit Control *Re-Auth-Answer* message as used for online charging.

Table 6.4.5: Re-Auth-Answer (RAA) Message Contents for Online Charging

Diameter Credit Control Application AVPs	
AVP	Used in 3GPP
<Diameter Header: 258, PXY>	Yes
<Session-Id>	Yes
{Result-Code}	Yes
{Origin-Host}	Yes
{Origin-Realm}	Yes
[User-Name]	Yes
[Origin-State-Id]	Yes
[Error-Message]	Yes
[Error-Reporting-Host]	Yes
*[Failed-AVP]	Yes
*[Redirect-Host]	Yes
[Redirect-Host-Usage]	Yes
[Redirect-Host-Cache-Time]	Yes
* [Proxy-Info]	No
{ Proxy-Host }	No
{ Proxy-State }	No
*[AVP]	Yes

Editor's note: The rationale for "NO" above should be provided. If the message is identical to the definition in DCC the table may be replaced by a reference to DCC.

6.4.6 Capabilities-Exchange-Request Message

The Capabilities-Exchange-Request message structure is described in [401].

6.4.7 Capabilities-Exchange-Answer Message

The Capabilities-Exchange-Answer message structure is described in [401].

6.4.8 Device-Watchdog-Request Message

The Device-Watchdog-Request message structure is described in [401].

6.4.9 Device-Watchdog-Answer Message

The Device-Watchdog-Answer message structure is described in [401].

6.4.10 Disconnect-Peer-Request Message

The Disconnect-Peer-Request message structure is described in [401].

6.4.11 Disconnect-Peer-Answer Message

The Disconnect-Peer-Answer message structure is described in [401].

6.4.12 Abort-Session-Request Message

The Abort-Session-Request message structure is described in [401].

6.4.13 Abort-Session -Answer Message

The Abort-Session-Answer message structure is described in [401].

6.5 Other procedural description of the 3GPP charging applications

6.5.1 Re-authorization

6.5.1.1 Idle timeout

The server may specify an idle timeout associated with a granted quota using the Quota-Holding-Time AVP. If no traffic associated with the quota is observed for this time, the client shall understand that the traffic has stopped and the quota is returned to the server. The client shall start the quota holding timer when quota consumption ceases. This is always when traffic ceases, i.e. the timer is re-started at the end of each packet. It applies equally to the granted time quota and to the granted volume quota. The timer is stopped on sending a CCR and re-initialised on receiving a CCA with the previous used value or a new value of Quota-Holding-Time if received.

Alternatively, if this AVP is not present, a locally configurable default value in the client shall be used. A Quota-Holding-Time value of zero indicates that this mechanism shall not be used.

6.5.1.2 Change of charging conditions

There are a number of mid-session service events (re-authorization triggers), which could affect the rating of the current service usage, e.g. end user QoS changes or location updates. When allocating resources, the server may instruct the credit control client to re-authorize the quota upon a number of different session related triggers that can affect the rating conditions. The server instructs the Network Element to monitor for such events by using the Trigger-Type AVP in the CCA command.

When one of the activated triggers happen a credit re-authorization shall be sent to the server including information related to the service event even if all the granted service units have not been used. The quota is also being reported.

The client shall not re-authorise the quota when events which are not included in the Trigger AVP occur.

Multiple triggers monitoring may be associated to a single quota allocation by including multiple Trigger-Type AVPs.

6.5.1.3 Reporting quota usage

The credit control client shall report the quota usage under a number of circumstances. When this happens, the reason for the quota being reported is notified to the server through the use of the Reporting-Reason AVP in the CCR. The reason for reporting credit usage can occur directly in the Multiple-Services-Credit-Control AVP, or in the Used-Service-Units AVP, depending on whether it applies for all quota types or a particular quota type respectively. It shall not be used at command level. It shall always and shall only be sent when usage is being reported.

When the reason is RATING_CONDITION_CHANGE, the Trigger-Type AVP shall also be included to indicate the specific armed trigger event which caused the reporting and re-authorization request.

6.5.2 Threshold based re-authorization triggers

The server may optionally include as part of the Multiple-Services-Credit-Control AVP, when it is providing a quota, an indication to the client of the remaining quota threshold that shall trigger a quota re-authorization. The Time-Quota-Threshold AVP indicates the threshold in seconds when the granted quota is time, and the Volume-Quota-Threshold AVP indicates the threshold in octets when the granted quota is volume. The Unit-Quota-Threshold AVP indicates the threshold in service specific units, that are defined in the service specific documents, when the granted quota is service specific.

If the threshold triggers were included along with the quota granted, the Credit Control client, then, shall seek re-authorization from the server for the quota when the quota contents fall below the supplied threshold. The client shall allow service to continue whilst the re-authorization is progress, until the original quota had been consumed.

6.5.3 Termination action

The termination action is sent over the Ro reference point. Two different approaches are specified:

- The Final-Unit-Indication AVP with Final-Unit-Action TERMINATE does not include any other information. When the user has consumed the final granted units, the network element shall terminate the service. This is the default handling applicable whenever the client receives an unsupported Final-Unit-Action value. A final Credit-Control-Request message to the server shall be sent if the Final-Unit-Indication AVP indicating action TERMINATE was present at command level or Multiple-Services-Credit-Control AVP level. If the Final-Unit-Indication AVP is at command level, the CC-Request-Type AVP in the request is set to the value TERMINATION_REQUEST. If the Final-Unit-Indication AVP is at Multiple-Services-Credit-Control level, the network element shall set the CC-Request-Type AVP to the value UPDATE_REQUEST and report the Used-Service-Unit AVP for the service that has terminated, as defined in IETF RFC 4006 [402].
- Another termination action consists in re-directing packets corresponding to a terminated service (consumption of the final granted units) to an application server. This allows the client to redirect user originated requests to a top-up server so that network access can be re-instated. This functionality is achieved with the server returning a "REDIRECT" and redirect-to URL in the Final-Units-Action AVP of the Multiple-Services-Credit-Control AVP or at command level. Upon receiving this result code, the Network Element shall apply the redirection. The URL should be categorized so that the End-User's ability to reach it is guaranteed.

6.5.4 Quota consumption time

The server may optionally indicate to the client that the quota consumption must be stopped after a period equal to the Quota Consumption Time in which no packets are received or at session termination, whichever is sooner. This is indicated by including the Quota-Consumption-Time AVP in the CCA. The idle period equal to the Quota Consumption Time is included in the reported usage. The quota is consumed normally during gaps in traffic of duration less than or equal to the Quota-Consumption-Time. Quota consumption resumes on receipt of a further packet belonging to the service data flow.

If packets are allowed to flow during a Credit Control Request (Update)/Credit Control Answer exchange, and the Quota-Consumption-Time AVP value in the provided quota is the same as in the previously provided quota, then the Quota-Consumption-Time runs normally through this procedure. For example, if 5 seconds of a 10 second QCT timer have passed when a CCR(U) is triggered, and the CCA(U) returns 2 seconds later, then the QCT timer will expire 3 seconds after the receipt of the CCA and the remaining unaccounted 5 seconds of usage will be recorded against the new quota even though no packets were transmitted with the new quota.

In the case of a new quota with the Quota-Consumption-Time AVP, or when packets are blocked during the CCR(U)/CCA procedure then the Quota-Consumption-Time stops running (if it was running) and quota consumption begins again when the next service data flow packet matching the Charging Rule is received.

If a Quota-Consumption-Time AVP value of zero is provided, or if no Quota-Consumption-Time AVP is present in the CCA, the quota is consumed continuously from the point at which it is granted.

6.5.5 Service Termination

The OCF may determine that a service requires termination. The OCF may perform this termination synchronously if it has a CCR pending processing by returning CCA with Result-Code AVP with value DIAMETER-AUTHORIZATION-REJECTED. If the OCF does not have a pending request (asynchronous), the OCF may trigger an ASR to terminate the Diameter session related to the service. On reception of an ASR, the CTF shall close the associated Credit-Control session by sending a CCR [TERMINATE]. The behaviour of the CTF, in relation to the user session, on reception of an ASR is detailed in the middle-tier TS. As an alternative to the ASR, the OCF may trigger a RAR to which the CTF behaves as described in RFC 4006 [402] and the OCF shall return a CCA with Result-Code AVP with value DIAMETER-AUTHORIZATION-REJECTED for the resulting CCR.

6.6 Bindings of the operation to protocol application

This clause aims to describe the mapping between the protocol independent messages and parameter with the Diameter messages and AVP utilized on the 3GPP Offline and Online Charging.

6.6.1 Bindings of Charging Data Transfer to Accounting

Table 6.6.1 describes the bindings of the *Charging Data Transfer* operation parameter to the DBPA AVP for 3GPP Offline Charging.

Table 6.6.1: Bindings to Accounting

Charging Data Transfer parameter	Diameter Accounting AVP
Operation Number	Accounting-Record-Number
Operation Type	Accounting-Record-Type
Operation Identifier	Acct-Application-Id
Operation Interval	Acct-Interim-Interval
Destination Domain	Destination-Realm
Origination Timestamp	Event-Timestamp
Originator Host	Origin-Host
Originator Domain	Origin-Realm
Origination State	Origin-State-Id
Proxy Information	Proxy-Info
Operation Result	Result-Code
Route Information	Route-Record
Service Information	Service-Information
Session Identifier	Session-Id
Operation Token	Service-Context-Id
User Name	User-Name

6.6.2 Bindings of Debit / Reserve Units to Credit-Control

Table 6.6.2 describes the bindings of the *Debit / Reserve Units* operation parameter to the DCCA AVP for 3GPP Online Charging.

Table 6.6.2: Bindings to Credit-Control

Debit / Reserve Units parameter	DCCA AVP
Destination Domain	Destination-Realm
Destination Host	Destination-Host
Failed parameter	Failed-AVP
Multiple Operation	Multiple-Services-Indicator
Multiple Unit Operation	Multiple-Services-Credit Control
Operation Failover	CC-Session-Failover
Operation Failure Action	Credit-Control-Failure-Handling
Operation Identifier	Auth-Application-Id
Operation Number	CC-Request-Number
Operation Result	Result-Code
Operation Token	Service-Context-Id
Operation Type	CC-Request-Type
Origination State	Origin-State-Id
Origination Timestamp	Event-Timestamp
Originator Domain	Origin-Realm
Originator Host	Origin-Host
Proxy Information	Proxy-Info
Redirection Cache Time	Redirect-Max-Cache-Time
Redirection Host	Redirect-Host
Redirection Host Usage	Redirect-Host-Usage
Requested Action	Requested-Action
Route Information	Route-Record
Service Information	Service-Information
Session Identifier	Session-Id
Subscriber Equipment Number	User-Equipment-Info
Subscriber Identifier	Subscription-Id
Termination Cause	Termination-Cause
User Name	User-Name

7 Summary of used Attribute Value Pairs

7.1 Diameter AVPs

The use of the Attribute Value Pairs (AVPs) that are defined in the Diameter Protocol is specified in clause 6.2 for offline charging and in clause 6.4 for online charging. The information is summarized in the table 7.1 with the accounting AVPs and in table 7.2 with credit control AVPs listed in alphabetical order. Detailed specification of these AVPs is available in this specification.

Those Diameter AVPs that are used are marked "Yes" in the following tables. Those Diameter AVPs that are not used are marked "-" in the following tables. This implies that their content can (M) or (Oc) be used by the CDF for offline and for the OCF for online charging purposes.

Table 7.1: Use Of IETF Diameter AVPs

AVP Name	AVP Code	Used in				Value Type	AVP Flag rules				
		ACR	ACA	CCR	CCA		Must	May	Should not	Must not	May Encr.
Accounting-Realtime-Required	483	-	-	-	-	Enumerated	-	-	-	-	-
Accounting-Record-Number	485	M	M	-	-	Unsigned32	M	P	-	V	Y
Accounting-Record-Type	480	M	M	-	-	Enumerated	M	P	-	V	Y
Accounting-Sub-Session-Id	287	-	-	-	-	Unsigned64	-	-	-	-	-
Acct-Application-Id	259	O _C	O _C	-	-	Unsigned32	M	P	-	V	N
Acct-Interim-Interval	85	O _C	O _C	-	-	Unsigned32	M	P	-	V	Y
Acct-Multi-Session-Id	50	-	-	-	-	Unsigned32	-	-	-	-	-
Acct-Session-Id	44	-	-	-	-	OctetString	-	-	-	-	-
Auth-Application-Id	258	-	-	M	M	Unsigned32	M	P	-	V	N
AVP	*	-	-	-	-	Grouped	-	-	-	-	-
Called-Station-Id	30	O _C	-	O _C	-	OctetString	M	P	-	V	N
CC-Correlation-Id	411	-	-	-	-	OctetString	-	-	-	-	-
CC-Input-Octets	412	-	-	O _C	O _C	Unsigned64	-	P,M	-	V	Y
CC-Money	413	-	-	-	-	Grouped	-	-	-	-	-
CC-Output-Octets	414	-	-	O _C	O _C	Unsigned64	M	P	-	V	Y
CC-Request-Number	415	-	-	M	M	Unsigned32	M	P	-	V	Y
CC-Request-Type	416	-	-	M	M	Enumerated	M	P	-	V	Y
CC-Service-Specific-Units	417	-	-	O _C	O _C	Unsigned64	M	P	-	V	Y
CC-Session-Failover	418	-	-	-	-	Enumerated	-	-	-	-	-
CC-Sub-Session-Id	419	-	-	-	-	Unsigned64	-	-	-	-	-
CC-Time	420	-	-	O _C	O _C	Unsigned32	M	P	-	V	Y
CC-Total-Octets	421	-	-	O _C	O _C	Unsigned64	M	P	-	V	Y
CC-Unit-Type	454	-	-	-	-	Enumerated	-	-	-	-	-
Check-Balance-Result	422	-	-	-	-	Enumerated	-	-	-	-	-
Cost-Information	423	-	-	-	O _C	Grouped	M	P	-	V	Y
Cost-Unit	424	-	-	-	O _C	UTF8String	M	P	-	V	Y
Credit-Control	426	-	-	-	-	Enumerated	-	-	-	-	-
Credit-Control-Failure-Handling	427	-	-	-	O _C	Enumerated	M	P	-	V	Y
Currency-Code	425	-	-	-	M	Unsigned32	M	P	-	V	Y
Destination-Host	293	-	-	O _C	-	DiamIdent	M	P	-	V	N
Destination-Realm	283	M	-	M	-	DiamIdent	M	P	-	V	N
Direct-Debiting-Failure-Handling	428	-	-	-	O _C	Enumerated	M	P	-	V	Y
Error-Message	281	-	-	-	-	UTF8String	-	-	-	-	-
Error-Reporting-Host	294	-	O _C	-	-	DiamIdent	-	P	-	V,M	N
Event-Timestamp	55	O _C	O _C	O _C	-	Time	M	P	-	V	N
Exponent	429	-	-	-	O _C	Integer32	M	P	-	V	Y
Failed-AVP	279	-	-	-	O _C	Grouped	M	P	-	V	N
Filter-Id	11	-	-	-	O _C	UTF8String	M	P	-	V	Y
Final-Unit-Action	449	-	-	-	O _C	Enumerated	M	P	-	V	Y
Final-Unit-Indication	430	-	-	-	O _C	Grouped	M	P	-	V	Y
Granted-Service-Unit	431	-	-	-	O _C	Grouped	M	P	-	V	Y
G-S-U-Pool-Identifier	453	-	-	-	O _C	Unsigned32	M	P	-	V	Y
G-S-U-Pool-Reference	457	-	-	-	O _C	Grouped	M	P	-	V	Y

AVP Name	AVP Code	Used in				Value Type	AVP Flag rules				
		ACR	ACA	CCR	CCA		Must	May	Should not	Must not	May Encr.
Location-Type	IANA	O _C	-	O _C	-	refer [403]					
Location-Information	IANA	O _C	-	O _C	-	refer [403]					
Multiple-Services-Credit-Control	456	-	-	O _M	O _M	Grouped	M	P	-	V	Y
Multiple-Services-Indicator	455	-	-	O _M	-	Enumerated	M	P	-	V	Y
Operator-Name	IANA	O _C	-	O _C	-	refer [403]					
Origin-Host	264	M	M	M	M	DiamIdent	M	P	-	V	N
Origin-Realm	296	M	M	M	M	DiamIdent	M	P	-	V	N
Origin-State-Id	278	O _C	O _C	-	-	Unsigned32	M	P	-	V	N
Proxy-Info	284	O _C	O _C	O _C	O _C	Grouped	M	-	-	P,V	N
Proxy-Host	280	M	M	M	M	DiamIdent	M	-	-	P,V	N
Proxy-State	33	M	M	M	M	OctetString	M	-	-	P,V	N
Rating-Group	432	-	-	O _C	O _C	Unsigned32	M	P	-	V	Y
Redirect-Address-Type	433	-	-	M	M	Enumerated	M	P	-	V	Y
Redirect-Host	292	-	-	-	O _C	DiamURI	M	P	-	V	N
Redirect-Host-Usage	261	-	-	-	O _C	Enumerated	M	P	-	V	N
Redirect-Max-Cache-Time	262	-	-	-	O _C	Unsigned32	M	P	-	V	N
Redirect-Server	434	-	-	-	O _C	Grouped	M	P	-	V	Y
Redirect-Server-Address	435	-	-	-	M	UTF8String	M	P	-	V	Y
Requested-Action	436	-	-	O _C	-	Enumerated	M	P	-	V	Y
Requested-Service-Unit	437	-	-	O _C	-	Grouped	M	P	-	V	Y
Restriction-Filter-Rule	438	-	-	-	O _C	IPFilterRule	M	P	-	V	Y
Result-Code	268	-	M	-	M	Unsigned32	M	P	-	V	N
Route-Record	282	O _C	-	O _C	O _C	DiamIdent	M	-	-	P,V	N
Service-Context-Id	461	O _M	-	M	-	UTF8String	M	P	-	V	Y
Service-Identifier	439	-	-	O _C	O _C	Unsigned32	M	P	-	V	Y
Service-Parameter-Info	440	-	-	-	-	Grouped	-	-	-	-	-
Service-Parameter-Type	441	-	-	-	-	Unsigned32	-	-	-	-	-
Service-Parameter-Value	442	-	-	-	-	OctetString	-	-	-	-	-
Session-Id	263	M	M	M	M	UTF8String	M	P	-	V	Y
Subscription-Id	443	O _M	-	O _M	-	Grouped	M	P	-	V	Y
Subscription-Id-Data	444	M	-	M	-	UTF8String	M	P	-	V	Y
Subscription-Id-Type	450	M	-	M	-	Enumerated	M	P	-	V	Y
Tariff-Change-Usage	452	-	-	O _C	-	Enumerated	M	P	-	V	Y
Tariff-Time-Change	451	-	-	-	O _C	Time	M	P	-	V	Y
Unit-Value	445	-	-	-	M	Grouped	M	P	-	V	Y
Used-Service-Unit	446	-	-	O _C	-	Grouped	M	P	-	V	Y
User-Equipment-Info	458	-	-	O _C	-	Grouped	-	P,M	-	V	Y
User-Equipment-Info-Type	459	-	-	M	-	Enumerated	-	P,M	-	V	Y
User-Equipment-Info-Value	460	-	-	M	-	OctetString	-	P,M	-	V	Y
User-Name	1	O _C	O _C	O _C	-	UTF8String	M	P	-	V	Y
Value-Digits	447	-	-	-	M	Integer64	M	P	-	V	Y
Validity-Time	448	-	-	-	O _C	Unsigned32	M	P	-	V	Y
Vendor-Id	266	-	-	-	-	Unsigned32	-	-	-	-	-
Vendor-Specific-Application-Id	260	-	-	-	-	Grouped	-	-	-	-	-

NOTE: *Result-Code* AVP is defined in Diameter Base Protocol [401]. However, new values are used in offline and online charging applications. These additional values are defined below.

7.1.1 Acct-Application-Id AVP

The *Acct-Application-Id* AVP (AVP code 259) shall contain the value of 3 as defined in [401] according 3GPP TS 29.230 [206].

7.1.2 Auth-Application-Id AVP

The *Auth-Application-Id* AVP (AVP code 258) shall contain the value of 4 as defined in IETF RFC 4006 [402] according 3GPP TS 29.230 [206].

7.1.3 Event-Timestamp AVP

The *Event-Timestamp* AVP (AVP code 55) shall contain the time when the chargeable event is received in the CTF.

7.1.4 Multiple-Services-Credit-Control

The *Multiple-Services-Credit-Control* AVP (AVP code 456) is of type grouped as specified in IETF RFC 4006 [402]. It contains additional 3GPP specific charging parameters.

It has the following ABNF grammar:

```

<Multiple-Services-Credit-Control> ::=
    < AVP Header: 456 >
        [ Granted-Service-Unit ]
        [ Requested-Service-Unit ]
        * [ Used-Service-Unit ]
        [Tariff-Change-Usage]
        * [ Service-Identifier ]
        [ Rating-Group ]
        * [ G-S-U-Pool-Reference ]
        [ Validity-Time ]
        [ Result-Code ]
        [ Final-Unit-Indication ]
        [ Time-Quota-Threshold ]
        [ Volume-Quota-Threshold ]
        [ Unit-Quota-Threshold ]
        [ Quota-Holding-Time ]
        [ Quota-Consumption-Time ]
        * [ Reporting-Reason ]
        * [ Trigger-Type ]
        [ PS-Furnish-Charging-Information ]
        * [AVP]

```

7.1.5 Rating-Group AVP

The *Rating-Group* AVP (AVP code 432), is defined in IETF RFC 4006 [402]. It contains the charging key (defined in 3GPP TS 23.125 [70]). Each quota allocated to a Diameter CC session has a unique Rating Group value as specified in IETF RFC 4006 [402].

7.1.6 Result-Code AVP

This subclause defines new *Result-Code* AVP (AVP code 268) values that must be supported by all Diameter implementations that conform to the present document. The Result-Code AVP operates as described in RFC 3588 [401] and IETF RFC 4006 [402].

The following result code descriptions are examples of the possible uses for the code:

Transient Failures (4xxx):

DIAMETER_END_USER_SERVICE_DENIED 4010

The OCF denies the service request due to service restrictions (e.g. terminate rating group) or limitations related to the end-user, for example the end-user's account could not cover the requested service.

DIAMETER_CREDIT_CONTROL_NOT_APPLICABLE 4011

The OCF determines that the service can be granted to the end user but no further credit control needed for the service (e.g. service is free of charge or the PDP context is treated for offline charging).

DIAMETER_CREDIT_LIMIT_REACHED 4012

The OCF denies the service request since the end-user's account could not cover the requested service. If the CCR contained used-service-units they are deducted, if possible.

Permanent Failures (5xxx):

DIAMETER_AUTHORIZATION_REJECTED 5003

The OCF denies the service request in order to terminate the service for which credit is requested. For example this error code is used to inform PDP Context has to be terminated in the CCR message or to inform blacklist the rating group in the Multiple-Service-Credit-Control AVP.

DIAMETER_USER_UNKNOWN 5030

The specified end user could not be found in the OCF.

DIAMETER_RATING_FAILED 5031

This error code is used to inform the CTF that the OCF cannot rate the service request due to insufficient rating input, incorrect AVP combination or due to an AVP or an AVP value that is not recognized or supported in the rating. For Flow Based Charging this error code is used if the Rating group is not recognized. The Failed-AVP AVP MUST be included and contain a copy of the entire AVP(s) that could not be processed successfully or an example of the missing AVP complete with the Vendor-Id if applicable. The value field of the missing AVP should be of correct minimum length and contain zeroes.

7.1.7 Service-Context-Id AVP

The *Service-Context-Id* AVP is defined in IETF RFC 4006 [402]. It is of type UTF8String and contains a unique identifier of the Diameter Credit Control service specific document that applies to the request. This is an identifier allocated by the service provider/operator, by the service element manufacturer or by a standardization body and MUST uniquely identify a given Diameter Credit Control service specific document. For offline charging, this identifies the service specific document ('middle tier' TS) on which associated CDRs should be based. The format of the Service-Context-Id is:

"extensions".MNC.MCC."Release"."service-context" "@" "domain"

The 3GPP specific values for "service-context" "@" "domain" are:

- For PS charging: 32251@3gpp.org
- For WLAN charging: 32252@3gpp.org
- For IMS charging: 32260@3gpp.org
- For MMS service charging: 32270@3gpp.org
- For LCS service charging: 32271@3gpp.org
- For PoC service charging: 32272@3gpp.org
- For MBMS service charging: 32273@3gpp.org

The "Release" indicates the 3GPP Release the service specific document is based upon e.g. 6 for Release 6.

As a minimum, Release "service-context" "@" "domain" shall be used. If the minimum is used all operator configurable parameters (Oc and Om) are optional.

The MNC.MCC identifies the operator implementing the service specific document, which is used to determine the specific requirements for the operator configurable parameters.

The "extensions" is operator specific information to any extensions in a service specific document.

7.1.8 Service-Identifier AVP

The *Service-Identifier* AVP (AVP code 439), is defined in IETF RFC 4006 [402]. For further details, please refer the middle-tier specification.

7.1.8A Used-Service-Unit AVP

The *Used-Service-Unit* AVP (AVP code 446) is of type grouped as specified in IETF RFC 4006 [402]. It contains additional 3GPP specific charging parameters.

It has the following ABNF grammar:

```
<Used-Service-Unit> ::= < AVP Header: 446 >
                        [ Reporting-Reason ]
                        [ Tariff-Change-Usage ]
                        [ CC-Time ]
                        [CC-Money]
                        [ CC-Total-Octets ]
                        [ CC-Input-Octets ]
                        [ CC-Output-Octets ]
                        [ CC-Service-Specific-Units ]
                        *[ Event-Charging-TimeStamp ]
                        *[ AVP ]
```

7.1.9 User-Name AVP

The *User-Name* AVP (AVP code 1) contains the user name in the format of a NAI according to RFC 3588 [401].

7.1.10 Vendor-Id AVP

The *Vendor-Id* AVP (AVP code 266), as part of the *Vendor-Specific-Application-Id* grouped AVP, shall contain the value of 10415, which is the IANA registered value for '3GPP' in 3GPP TS 29.230 [206].

7.2 3GPP specific AVPs

For the purpose of offline charging additional AVPs are used in ACR / ACA and for online charging additional AVPs are used in CCR / CCA. All 3GPP specific AVPs mentioned are relevant for both offline and online charging unless specifically excluded. The information is summarized in the following table along with the AVP flag rules.

The 3GPP Charging Application uses the value 10415 (3GPP) as *Vendor-Id*.

Detailed descriptions of AVPs that are used specifically for 3GPP charging are provided in the subclauses below the table. However, for AVPs that are just borrowed from other applications only the reference (e.g. TS 29.229 [204]), is provided in the following table and the detailed description is not repeated.

Where 3GPP Radius VSAs are re-used, they shall be translated to Diameter AVPs as described in IETF RFC 4005 [407] with the exception that the 'M' flag shall be set and the 'P' flag may be set.

Table 7.2: 3GPP specific AVPs

AVP Name	AVP Code	Used in				Value Type	AVP Flag rules				
		ACR	ACA	CCR	CCA		Must	May	Should not	Must not	May Encr.
3GPP-CAMEL-Charging-Info	24	-	-	X	-	refer [207]					
3GPP-Charging-Characteristics	13	-	-	X	-	refer [207]					
3GPP-Charging-Id	2	-	-	X	-	refer [207]					
3GPP-GGSN-MCC-MNC	9	-	-	X	-	refer [207]					
3GPP-GPRS-Negotiated-QoS-Profile	5	-	-	X	-	refer [207]					
3GPP-IMSI-MCC-MNC	8	-	-	X	-	refer [207]					
3GPP-MS-TimeZone	23	-	-	X	-	refer [207]					
3GPP-NSAPI	10	-	-	X	-	refer [207]					
3GPP-PDP-Type	3	-	-	X	-	refer [207]					
3GPP-RAT-Type	21	-	-	X	-	refer [207]					
3GPP-Selection-Mode	12	-	-	X	-	refer [207]					
3GPP-Session-Stop-Indicator	11	-	-	X	-	refer [207]					
3GPP-SGSN-MCC-MNC	18	-	-	X	-	refer [207]					
3GPP-User-Location-Info	22	-	-	X	-	refer [207]					
Access-Network-Charging-Identifier-Value	503	X	-	X	-	refer [214]					
Access-Network-Information	1263	X	-	X	-	OctetString	V,M	P			N
Adaptations	1217	-	-	X	-	Enumerated	V,M	P			N
Additional-Content-Information	1207	-	-	X	-	Grouped	V,M	P			N
Additional-Type-Information	1205	-	-	X	-	UTF8String	V,M	P			N
Address-Data	897	-	-	X	-	UTF8String	V,M	P			N
Address-Domain	898	-	-	X	-	Grouped	V,M	P			N
Address-Type	899	-	-	X	-	Enumerated	V,M	P			N
Addressee-Type	1208	-	-	X	-	Enumerated	V,M	P			N
Applic-ID	1218	-	-	X	-	UTF8String	V,M	P			N
Application-provided-called-party-address	837	X	-	X	-	UTF8String	V,M	P			N
Application-Server	836	X	-	X	-	UTF8String	V,M	P			N
Application-Server-Information	850	X	-	X	-	Grouped	V,M	P			N
Associated-URI	856	X	-	X	-	UTF8String	V,M	P			N
Authorized-QoS	849	X	-	-	-	UTF8String	V,M	P			N
Aux-Applic-Info	1219	-	-	X	-	UTF8String	V,M	P			N
Bearer-Service	854	X	-	-	-	OctetString	V,M	P			N
Called-Party-Address	832	X	-	X	-	UTF8String	V,M	P			N
Calling-Party-Address	831	X	-	X	-	UTF8String	V,M	P			N
Called-Asserted-Identity	1250	X	-	X	-	UTF8String	V,M	P			N
Cause-Code	861	X	-	X	-	Integer32	V,M	P			N
CG-Address	846	X	-	X	-	Address	V,M	P			Y
Charged-Party	857	X	-	-	-	UTF8String	V,M	P			N
Charging-Rule-Base-Name	1004	-	-	X	-	refer [205]					
Class-Identifier	1214	-	-	X	-	Enumerated	V,M	P			N
Content-Class	1220	-	-	X	-	Enumerated	V,M	P			N
Content-Disposition	828	X	-	X	-	UTF8String	V,M	P			N
Content-Length	827	X	-	X	-	Unsigned32	V,M	P			N
Content-Size	1206	-	-	X	-	Unsigned32	V,M	P			N
Content-Type	826	X	-	X	-	UTF8String	V,M	P			N
Deferred-Location-Event-Type	1230	-	-	X	-	UTF8String	V,M	P			N
Delivery-Report-Requested	1216	-	-	X	-	Enumerated	V,M	P			N
Domain-Name	1200	-	-	X	-	UTF8String	V,M	P			N
DRM-Content	1221	-	-	X	-	Enumerated	V,M	P			N
Event	825	X	-	X	-	UTF8String	V,M	P			N
Event-Type	823	X	-	X	-	Grouped	V,M	P			N
Event-Charging-TimeStamp	1258	-	-	X	-	Time	V,M	P			N
Expires	888	X	-	X	-	Unsigned32	V,M	P			N
File-Repair-Supported	1224	X	-	X	-	Enumerated	V,M	P			Y
GGSN-Address	847	X	-	X	-	Address	V,M	P			N
IMS-Charging-Identifier	841	X	-	X	-	UTF8String	V,M	P			N
IMS-Information	876	X	-	X	-	Grouped	V,M	P			N
Incoming-Trunk-Group-Id	852	X	-	-	-	UTF8String	V,M	P			N
Inter-Operator-Identifier	838	X	-	-	-	Grouped	V,M	P			N
LCS-Client-Dialed-By-MS	1233	-	-	X	-	UTF8String	V,M	P			N
LCS-Client-External-ID	1234	-	-	X	-	UTF8String	V,M	P			N

AVP Name	AVP Code	Used in				Value Type	AVP Flag rules				
		ACR	ACA	CCR	CCA		Must	May	Should not	Must not	May Encr.
LCS-Client-Id	1232	-	-	X	-	Grouped	V,M	P			N
LCS-Client-Name	1231	-	-	X	-	UTF8String	V,M	P			N
LCS-Client-Name	1235	-	-	X	-	Grouped	V,M	P			N
LCS-Client-Type	1241	-	-	X	-	Enumerated	V,M	P			N
LCS-Data-Coding-Scheme	1236	-	-	X	-	UTF8String	V,M	P			N
LCS-Format-Indicator	1237	-	-	X	-	Enumerated	V,M	P			N
LCS-Information	878	-	-	X	-	Grouped	V,M	P			N
LCS-Name-String	1238	-	-	X	-	UTF8String	V,M	P			N
LCS-Requestor-Id	1239	-	-	X	-	Grouped	V,M	P			N
LCS-Requestor-Id-String	1240	-	-	X	-	UTF8String	V,M	P			N
Location-Estimate	1242	-	-	X	-	UTF8String	V,M	P			N
Location-Estimate-Type	1243	-	-	X	-	Enumerated	V,M	P			N
Location-Type	1244	-	-	X	-	Grouped	V,M	P			N
Mandatory-Capability	604	X	-	-	-	refer [204]					
Media-Initiator-Flag	882	X	-	X	-	Enumerated	V,M	P			N
Message-Body	889	X	-	X	-	Grouped	V,M	P			N
MBMS-Information	880	X	-	X	-	Grouped	V,M	P			N
MBMS-Service-Area	903	X	-	X	-	refer [207]					
MBMS-Session-Identity	908	X	-	X	-	refer [207]					
MBMS-Service-Type	906	X	-	X	-	refer [207]					
MBMS-User-Service-Type	1225	X	-	X	-	Enumerated	V,M	P			Y
MBMS-2G-3G-Indicator	907	X	-	X	-	refer [207]					
Message-Class	1213	-	-	X	-	Grouped	V,M	P			N
Message-ID	1210	-	-	X	-	UTF8String	V,M	P			N
Message-Type	1211	-	-	X	-	Enumerated	V,M	P			N
Message-Size	1212	-	-	X	-	Unsigned32	V,M	P			N
MMBox-Storage-Requested	1248	-	-	X	-	Enumerated	V,M	P			N
MM-Content-Type	1203	-	-	X	-	Grouped	V,M	P			N
MMS-Information	877	-	-	X	-	Grouped	V,M	P			N
Node-Functionality	862	X	-	X	-	Enumerated	V,M	P			N
Number-Of-Participants	885	X	-	X	-	Unsigned32	V,M	P			N
Optional-Capability	605	X	-	-	-	refer [204]					
Originating-IOI	839	X	-	X	-	UTF8String	V,M	P			N
Originator	864	X	-	X	-	Enumerated	V,M	P			N
Originator-Address	886	-	-	X	-	Grouped	V,M	P			N
Outgoing-Trunk-Group-Id	853	X	-	-	-	UTF8String	V,M	P			N
Participants-Involved	887	X	-	X	-	UTF8String	V,M	P			N
Participant-Access-Priority	1259	X	-	X	-	Enumerated	V,M	P			N
Participant-Group	1260	X	-	X	-	Grouped	V,M	P			N
PDG-Address	895	X	-	X	-	Address	V,M	P			N
PDG-Charging-Id	896	X	-	X	-	Unsigned32	V,M	P			N
PDP-Address	1227	-	-	X	-	Address	V,M	P			Y
PDP-Context-Type	1247	-	-	X	-	Enumerated	V,M	P			N
PoC-Change-Condition	1261	X	-	-	-	Enumerated	V,M	P			N
PoC-Change-Time	1262	X	-	-	-	Time	V,M	P			N
PoC-Controlling-Address	858	X	-	X	-	UTF8String	V,M	P			N
PoC-Group-Name	859	X	-	X	-	UTF8String	V,M	P			N
PoC-Information	879	X	-	X	-	Grouped	V,M	P			N
PoC-Server-Role	883	X	-	X	-	Enumerated	V,M	P			N
PoC-Session-Id	1229	X	-	X	-	UTF8String	V,M	P			N
PoC-Session-Type	884	X	-	X	-	Enumerated	V,M	P			N
PoC-User-Role	1252	X	-	X	-	Grouped	V,M	P			N
PoC-User-Role-IDs	1253	X	-	X	-	UTF8String	V,M	P			N
PoC-User-Role-info-Units	1254	X	-	X	-	Enumerated	V,M	P			N
Positioning-Data	1245	-	-	X	-	UTF8String	V,M	P			N
Priority	1209	-	-	X	-	Enumerated	V,M	P			N
PS-Append-Free-Format-Data	867	X	-	-	X	Enumerated	V,M	P			N
PS-Free-Format-Data	866	X	-	-	X	OctetString	V,M	P			N
PS-Furnish-Charging-Information	865	X	-	-	X	Grouped	V,M	P			N
PS-Information	874	X	-	X	X	Grouped	V,M	P			N
Quota-Consumption-Time	881	-	-	-	X	Unsigned32	V,M	P			N
Quota-Holding-Time	871	-	-	-	X	Unsigned32	V,M	P			N

AVP Name	AVP Code	Used in				Value Type	AVP Flag rules				
		ACR	ACA	CCR	CCA		Must	May	Should not	Must not	May Encr.
RAI	909	X	-	X	-	refer [207]					
Read-Reply-Report-Requested	1222	-	-	X	-	Enumerated	V,M	P			N
Recipient-Address	1201	-	-	X	-	Grouped	V,M	P			N
Reply-Applic-ID	1223	-	-	X	-	UTF8String	V,M	P			N
Reporting-Reason	872	-	-	X	-	Enumerated	V,M	P			N
Requested-Party-Address	1251	X	-	X	-	UTF8String	V,M	P			N
Required-MBMS-Bearer-Capabilities	901	X	-	X	-	refer [207]					
Role-of-Node	829	X	-	X	-	Enumerated	V,M	P			N
SDP-Media-Component	843	X	-	X	-	Grouped	V,M	P			N
SDP-Media-Description	845	X	-	X	-	UTF8String	V,M	P			N
SDP-Media-Name	844	X	-	X	-	UTF8String	V,M	P			N
SDP-Session-Description	842	X	-	X	-	UTF8String	V,M	P			N
Served-Party-IP-Address	848	X	-	-	-	Address	V,M	P			N
Server-Capabilities	603	X	-	-	-	refer [204]					
Server-Name	602	X	-	-	-	refer [204]					
Service-Generic-Information	1256	X	-	X	-	Grouped	V,M	P			N
Service-Id	855	X	-	X	-	UTF8String	V,M	P			N
Service-Information	873	X	-	X	X	Grouped	V,M	P			N
Service-Specific-Data	863	X	-	-	-	UTF8String	V,M	P			N
Service-Specific-Type	1257	X	-	-	-	Unsigned32	V,M	P			N
Service-Specific-Info	1249	X	-	-	-	Grouped	V,M	P			N
SGSN-Address	1228	X	-	X	-	Address	V,M	P			N
SIP-Method	824	X	-	X	-	UTF8String	V,M	P			N
SIP-Request-Timestamp	834	X	-	X	-	Time	V,M	P			N
SIP-Response-Timestamp	835	X	-	X	-	Time	V,M	P			N
Submission-Time	1202	-	-	X	-	Time	V,M	P			N
Talk-Burst-Exchange	1255	X	-	-	-	Grouped	V,M	P			N
Terminating-IOI	840	X	-	X	-	UTF8String	V,M	P			N
Time-Quota-Threshold	868	-	-	-	X	Unsigned32	V,M	P			N
Time-Stamps	833	X	-	X	-	Grouped	V,M	P			N
TMGI	900	X	-	X	-	refer [207]					
Token-Text	1215	-	-	X	-	UTF8String	V,M	P			N
Trigger-Type	870	-	-	X	X	Enumerated	V,M	P			N
Trunk-Group-Id	851	X	-	-	-	Grouped	V,M	P			N
Type-Number	1204	-	-	X	-	Enumerated	V,M	P			N
Unit-Quota-Threshold	1226	-	-	-	X	Unsigned32	V,M	P			N
User-Data	606	X	-	-	-	refer [204]	V,M	P			N
User-Session-Id	830	X	-	X	-	UTF8String	V,M	P			N
VAS-Id	1102	-	-	X	-	refer [213]					
VASP-Id	1101	-	-	X	-	refer [213]					
Volume-Quota-Threshold	869	-	-	-	X	Unsigned32	V,M	P			N
WAG-Address	890	X	-	X	-	Address	V,M	P			N
WAG-PLMN-Id	891	X	-	X	-	OctetString	V,M	P			N
WLAN-Information	875	X	-	X	-	Grouped	V,M	P			N
WLAN-Radio-Container	892	X	-	X	-	Grouped	V,M	P			N
WLAN-Session-Id	1246	X	-	X	-	UTF8String	V,M	P			N
WLAN-Technology	893	X	-	X	-	Unsigned32	V,M	P			N
WLAN-UE-Local-IPAddress	894	X	-	X	-	Address	V,M	P			N

7.2.1 Adaptations AVP

The *Adaptations* AVP (AVP code 1217) is of type Enumerated and indicates whether the originator allows adaptation of the content (default Yes).

The values indicating whether adaptations are allowed are:

0 Yes

1 No

7.2.1A Access-Network-Information AVP

The *Access-Network-Information* AVP (AVP code 1263) is of type OctetString and indicates the SIP P-header "P-Access-Network-Information".

7.2.2 Additional-Content-Information AVP

The *Additional-Content-Information* AVP (AVPcode 1207) is of type Grouped and identifies any subsequent content types. It is used to identify each content (including re-occurrences) within an MM when the Type-Number AVP or Additional-Type-Information AVP from the Content-Type AVP indicate a multi-part content.

It has the following ABNF grammar:

```
Additional-Content-Information:: = < AVP Header: 1207 >
                                   [ Type-Number ]
                                   [ Additional-Type-Information ]
                                   [ Content-Size ]
```

7.2.3 Additional-Type-Information AVP

The *Additional-Type-Information* AVP (AVP code 1205) is of type UTF8String and identifies any additional information beyond well-known media types or non-well-known media types.

7.2.4 Address-Data AVP

The *Address-Data* AVP (AVP code 897) is of type UTF8String and indicates the address information and formatted according type of address indicated in the Address-Type AVP and according to MMS encapsulation [209].

7.2.5 Address-Domain AVP

The *Address-Domain* AVP (AVP code 898) is of type Grouped and indicates the domain/network to which the associated address resides. If this AVP is present, at least one of the AVPs described within the grouping must be included.

It has the following ABNF:

```
Address-Domain :: = < AVP Header: 898 >
                   [ Domain-Name ]
                   [ 3GPP-IMSI-MCC-MNC ]
```

7.2.6 Address-Type AVP

The *Address-Type* AVP (AVP code 899) is of type Enumerated and indicates the type of address carried within the Address-Information AVP.

It has the following values:

- 0 e-mail address
- 1 MSISDN
- 2 IPv4 Address
- 3 IPv6 Address
- 4 Numeric Shortcode
- 5 Alphanumeric Shortcode

6 Other

7.2.7 Addressee-Type AVP

The Addressee-Type AVP (AVP code 1208) is of type Enumerated and identifies the how the recipient is addressed in the header of an MM.

The following values are defined:

- 0 TO ;
- 1 CC ;
- 2 BCC.

7.2.8 Applic-ID AVP

The *Applic-ID* AVP (AVP code 1218) is of type UTF8String and holds the identification of the destination application that the underlying MMS abstract message was addressed to.

7.2.9 Additional-Content-Information AVP

The *Additional-Content-Information* AVP (AVPcode 1207) is of type Grouped and identifies any subsequent content types. It is used to identify each content (including re-occurrences) within an MM when the Type-Number AVP or Additional-Type-Information AVP from the Content-Type AVP indicate a multi-part content.

It has the following ABNF grammar:

```
Additional-Content-Information::= < AVP Header: 1207 >  
                                [ Type-Number ]  
                                [ Additional-Type-Information ]  
                                [ Content-Size ]
```

7.2.10 Application-provided-Called-Party-Address AVP

The *Application-Provided-Called-Party-Address* AVP (AVP code 837) is of type UTF8String and holds the called party number (SIP URI, E.164), if it is determined by an application server.

7.2.11 Application-Server AVP

The *Application-Server* AVP (AVP code 836) is of type UTF8String and holds the SIP URL(s) of the AS(s) addressed during the session.

7.2.12 Application-Server-Information AVP

The *Application-Server-Information* AVP (AVP code 850) is of type Grouped and contains information about application servers visited through ISC interface.

It has the following ABNF grammar:

```
<Application-Server-Information>::= <AVP Header: 850 >  
                                [ Application-Server ]  
                                * [ Application-Provided-Called-Party-Address ]
```

7.2.13 Associated-URI AVP

The Associated-URI AVP (AVP code 856) is of type UTF8String and holds a non-barred public user identity (SIP URI or TEL URI) associated to the the public user identity under registration. This identity is obtained from the P-Associated-URI header of a 200 OK SIP response to a REGISTER request. This AVP may appear several times when the P-Associated-URI header contains more than one public user identity.

7.2.14 Authorised-QoS AVP

The *Authorised-QoS* AVP (AVP code 849) is of type UTF8String and holds the Authorised QoS as defined in TS 23.207 [200] / TS 29.207 [203] and applied via the Go reference point.

7.2.15 Aux-Applic-Info AVP

The *Aux-Applic-Info* AVP (AVP code 1219) is of type UTF8String and holds additional application/implementation specific control information.

7.2.16 Bearer-Service AVP

The *Bearer-Service* AVP (AVP code 854) is of type OctetString and holds the used bearer service for the PSTN leg.

7.2.17 Called-Asserted-Identity AVP

The *Called-Asserted-Identity* AVP (AVP code 1250) is of type UTF8String and holds the address (Public User ID: SIP URI, E.164, etc.) of the finally 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 may appear several times in the request when the P-Asserted-Identity contains both a SIP URI and a TEL URI.

This field shall be present when the P-Asserted-Identity SIP header field is available in the SIP 2xx response.

7.2.18 Called-Party-Address AVP

The *Called-Party-Address* AVP (AVP code 832) is of type UTF8String. In IMS charging (except for SIP Register and SIP Subscription transactions), it holds the address (SIP URI or TEL URI) of the party (Public User ID or Public Service ID) to whom the SIP transaction is posted. The Called Party Address shall be populated with the SIP URI or TEL URI contained in the Request-URI of the outgoing request.

For a registration procedure, this field holds the party (Public User ID) to be registered. In this case, the Called Party Address field is obtained from the 'To' SIP header of the SIP Request. For a subscription procedure this field holds the address of the resource for which the originator wants to receive notifications of change of states. In this case, the Called Party Address field is obtained from the outgoing Request-URI of the SIP Request.

7.2.19 Calling-Party-Address AVP

The *Calling-Party-Address* AVP (AVP code 831) is of type UTF8String and holds the address (SIP URI or TEL URI) which identifies the party (Public User Identity or Public Service Identity) initiating a SIP transaction. . It is obtained from the P-Asserted-Identity header of any non-REGISTER SIP Request, either initiating a dialog or a standalone transaction. This AVP may appear several times when the P-Asserted-Identity header contains both a SIP URI and a TEL URI.

7.2.20 Cause-Code AVP

The *Cause-Code* AVP (AVP code 861) is of type Integer32 and includes the cause code value from IMS node. It is used in Accounting-request[stop] and/or Accounting-request[event] messages. It is also used in the Credit-Control-request [Terminate] and/or Credit-Control-request [Event] messages.

Within the cause codes, values ≤ 0 are reserved for successful causes while values ≥ 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

The cause "Normal end of session" is used in Accounting-request[stop] 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

The cause "Successful transaction" is used in Accounting-request[event] message to indicate a successful SIP transaction (e.g. REGISTER, MESSAGE, NOTIFY, SUBSCRIBE). It may also be used by an Application Server to indicate successful service event execution.

"End of SUBSCRIBE dialog" -2

The cause "End of SUBSCRIBE dialog" is used to indicate the closure of a SIP SUBSCRIBE dialog. For instance a successful SIP SUBSCRIBE transaction terminating the dialog has been detected by the IMS node (i.e. SUBSCRIBE with expire time set to 0).

"2xx Final Response" -2xx

The cause-code "2xx Final Response" (except 200) is used when the SIP transaction is terminated due to an IMS node receiving/initiating a 2xx Final response [405].

"3xx Redirection" -3xx

The cause "3xx Redirection" is used when the SIP transaction is terminated due to an IMS node receiving/initiating a 3xx response [405].

"End of REGISTER dialog" -3

The cause "End of REGISTER dialog" is used to indicate the closure of a SIP REGISTER dialog. For instance a successful SIP REGISTER transaction terminating the dialog has been detected by the IMS node (i.e. REGISTER with expire time set to 0).

Failure cause code values.

"Unspecified error" 1

The cause "Unspecified error" is used when the SIP transaction is terminated due to an unknown error.

"4xx Request failure" 4xx

The cause "4xx Request failure" is used when the SIP transaction is terminated due to an IMS node receiving/initiating a 4xx error response [405].

"5xx Server failure" 5xx

The cause "5xx Server failure" is used when the SIP transaction is terminated due to an IMS node receiving/initiating a 5xx error response [405].

"6xx Global failure" 6xx

The cause "6xx Global failure" is used when the SIP transaction is terminated due to an IMS node receiving/initiating a 6xx error response [405].

"Unsuccessful session setup" 2

The cause "Unsuccessful session setup" is used in the Accounting-request[stop] when the SIP session has not been successfully established (i.e. Timer H expires and SIP ACK is not received or SIP BYE is received after reception of the 200OK final response and SIP ACK is not received) [202] [405].

"Internal error" 3

The cause "Internal error" is used when the SIP transaction is terminated due to an IMS node internal error (e.g. error in processing a request/response).

7.2.21 CG-Address AVP

The *CG-Address* AVP (AVP code 846) is of type Address and holds the IP-address of the charging gateway.

7.2.22 Charged-Party AVP

The Charged-Party AVP (AVP code 857) is of type UTF8String and holds the address (Public User ID: SIP URI, TEL URI, etc.) of the party to be charged.

7.2.23 Charging-Rule-Base-Name AVP

The *Charging-Rule-Base-Name* AVP (AVP code 1004) is of type OctetString, and it indicates the group name of charging rules residing in the TPF. The default Charging-Rule-Base-Name corresponds with the pre-defined group of charging rules as specified in 3GPP TS 29.210 [205].

7.2.24 Class-Identifier AVP

The *Class-Identifier* AVP (AVP code 1214) is of type Enumerated and

The values are:

- 0 Personal
- 1 Advertisement
- 2 Informational
- 3 Auto

7.2.25 Content-Class AVP

The *Content-Class* AVP (AVP code 1220) is of type Enumerated and classifies the content of the MM to the highest content class to which the MM belongs, as defined in MMS Encapsulation [209].

The classes can be one of the following:

- 0 text
- 1 image-basic
- 2 image-rich
- 3 video-basic
- 4 video-rich
- 5 megapixel
- 6 content-basic
- 7 content-rich

7.2.26 Content-Disposition AVP

The *Content-Disposition* AVP (AVP code 828) is of type UTF8String and indicates how the message body or a message body part is to be interpreted (e.g. session, render), as described in [405].

7.2.27 Content-Length AVP

The *Content-Length* AVP (AVP code 827) is of type Unsigned32 and holds the size of the message-body, as described in [405].

7.2.28 Content-Size AVP

The *Content-Size* AVP (AVP code 1206) is of type Unsigned32 and indicates the size in bytes of the specified content type.

7.2.29 Content-Type AVP

The *Content-Type* AVP (AVP code 826) is of type UTF8String and holds the media type (e.g. application/sdp, text/html) of the message-body, as described in [405].

7.2.30 Deferred-Location-Event-Type AVP

The *Deferred-Location-Event-Type* AVP (AVP code 1230) is of type UTF8String and holds information related to a deferred location request.

7.2.31 Delivery-Report-Requested AVP

The *Delivery-Report-Requested* AVP (AVP code 1216) is of type Enumerated and indicates whether a delivery report has been requested by the originator MMS User Agent or not.

The values for whether a report was requested are:

- 0 No
- 1 Yes

7.2.32 Domain-Name AVP

The *Domain-Name* AVP (AVP code 1200) is of type UTF8String and represents a fully qualified domain name (FQDN).

7.2.33 DRM-Content AVP

The *DRM-Content* AVP (AVP code 1221) is of type Enumerated and indicates if the MM contains DRM-protected content.

The values are:

- 0 No
- 1 Yes

7.2.34 Event AVP

The *Event* AVP (AVP code 825) is of type UTF8String and holds the content of the "Event" header.

7.2.34A Event-Charging-TimeStamp AVP

The *Event-Charging-TimeStamps* AVP (AVP code 1258) is of type Time, and it holds the timestamp of the event reported in the CC-Service-Specific-Units AVP when event based charging applies.

7.2.35 Event-Type AVP

The *Event-Type* AVP (AVP code 823) is of type Grouped and contains information about the type of chargeable telecommunication service/event for which the accounting-request and/or credit control request message(s) is generated.

It has the following ABNF grammar:

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

7.2.36 Expires AVP

The *Expires* AVP (AVP code 888) is of type Unsigned32 and holds the content of the "Expires" header.

Editor's note: to be clarified.

7.2.37 File-Repair-Supported AVP

The File-Repair-Supported AVP (AVP code 1224) is of type Enumerated and indicates whether the MBMS user service supports point-to-point file repair. The following values are supported:

SUPPORTED (1)

The MBMS user service does support point-to-point file repair.

NOT_SUPPORTED (2)

The MBMS user service does not support point-to-point file repair.

7.2.38 GGSN-Address AVP

The *GGSN-Address* AVP (AVP code 847) is of type Address and holds the IP-address of the GGSN that generated the GPRS Charging ID, as described in [1].

7.2.39 IMS-Charging-Identifier (ICID) AVP

The *IMS-Charging-Identifier* AVP (AVP code 841) is of type UTF8String and holds the IMS Charging Identifier (ICID) as generated by a IMS node for a SIP session and described in subclause 5.2.4.10.

7.2.40 IMS-Information AVP

The *IMS-Information* AVP (AVP code 876) is of type Grouped. Its purpose is to allow the transmission of additional IMS service specific information elements.

It has the following ABNF grammar:

```
IMS-Information :: = <AVP Header: 876>
                   [ Event-Type ]
                   [ Role-Of-Node ]
                   { Node-Functionality }
```

```

    [ User-Session-ID ]
  * [ Calling-Party-Address ]
    [ Called-Party-Address ]
  * [ Called-Asserted-Identity ]
    [ Requested-Party-Address ]
  * [ Associated-URI ]
    [ Time-Stamps ]
  * [ Application-Server-Information ]
  * [ Inter-Operator-Identifier ]
    [ IMS-Charging-Identifier ]
  * [ SDP-Session-Description ]
  * [ SDP-Media-Component ]
    [ Served-Party-IP-Address ]
    [ Server-Capabilities ]
    [ Trunk-Group-ID ]
    [ Bearer-Service ]
    [ Service-Id ]
  * [ Service-Specific-Info ]
  * [ Message-Body ]
    [ Cause-Code ]
    [ Access-Network-Information ]

```

7.2.41 Incoming-Trunk-Group-ID AVP

The *Incoming-Trunk-Group-ID* AVP (AVP code 852) is of type UTF8String and identifies the incoming PSTN leg.

7.2.42 Inter-Operator-Identifier AVP

The *Inter-Operator-Identifier* AVP (AVP code 838) is of type Grouped and holds the identification of the network neighbours (originating and terminating) as exchanged via SIP signalling and described in [404].

It has the following ABNF grammar:

```

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

```

7.2.43 LCS-APN AVP

The *LCS-Client-Name* AVP (AVP code 1231) is of type UTF8String and contains the APN of the LCS Client.

7.2.44 LCS-Client-Dialed-By-MS AVP

The *LCS-Client-Dialed-By-MS* AVP (AVP code 1233) is of type UTF8String and holds the number of the LCS Client dialled by the UE.

7.2.45 LCS-Client-External-ID AVP

The *LCS-Client-External-ID* AVP (AVP code 1234) is of type UTF8String and holds the identification of the external LCS Client.

7.2.46 LCS-Client-ID AVP

The *LCS-Client-Id* AVP (AVP code 1232) is of type Grouped and holds information related to the identity of an LCS client.

It has the following ABNF grammar:


```

<LCS-Client-ID>:: = < AVP Header: 1232 >
                    [ LCS-Client-Type ]
                    [ LCS-Client-External-ID ]
                    [ LCS-Client-Dialed-By-MS ]
                    [ LCS-Client-Name ]
                    [ LCS-APN ]
                    [ LCS-Requestor-ID ]

```

7.2.47 LCS-Client-Name AVP

The *LCS-Client-Name* AVP (AVP code 1235) is of type Grouped and contains the information related to the name of the LCS Client.

It has the following ABNF grammar:

```

<LCS-Client-Name>:: = < AVP Header: 1235>
                    [ LCS-Data-Coding-Scheme ]
                    [ LCS-Name-String ]
                    [ LCS-Format-Indicator ]

```

7.2.48 LCS-Client-Type AVP

The *LCS-Client-Type* AVP (AVP code 1241) is of type Enumerated and contains an estimate of the location of an MS in universal coordinates and the accuracy of the estimate.

It can be one of the following values:

EMERGENCY_SERVICES	0
VALUE_ADDED_SERVICES	1
PLMN_OPERATOR_SERVICES	2
LAWFUL_INTERCEPT_SERVICES	3

7.2.49 LCS-Data-Coding-Scheme AVP

The *LCS-Data-Coding-Scheme* AVP (AVP code 1236) is of type UTF8String and contains the information of the alphabet and the language used.

7.2.50 LCS-Format-Indicator AVP

The *LCS-Format-Indicator* AVP (AVP code 1237) is of type Enumerated and contains the format of the LCS Client name.

It can be one of the following values:

LOGICAL_NAME	0
EMAIL_ADDRESS	1
MSISDN	2
URL	3
SIP_URL	

7.2.51 LCS-Information AVP

The *LCS-Information* AVP (AVP code 878) is of type Grouped. Its purpose is to allow the transmission of additional LCS service specific information elements.

It has the following ABNF grammar:

```

LCS-Information :: = < AVP Header: 878>
                    [ LCS-Client-ID ]

```

[Location-Type]
 [Location-Estimate]
 [Positioning-Data]
 [IMSI]
 [MSISDN]

7.2.52 LCS-Name-String AVP

The *LCS-Name-String* AVP (AVP code 1238) is of type UTF8String and contains the LCS Client name.

7.2.53 LCS-Requestor-ID AVP

The *LCS-Requestor-Id* AVP (AVP code 1239) is of type Grouped and contains information related to the identification of the Requestor.

It has the following ABNF grammar:

```
<LCS-Requestor-ID>::= < AVP Header: 1239 >
                        [ LCS-Data-Coding-Scheme ]
                        [ LCS-Requestor-ID-String ]
```

7.2.54 LCS-Requestor-ID-String AVP

The *LCS-Requestor-Id-String* AVP (AVP code 1240) is of type UTF8String and contains the identification of the Requestor and can be e.g. MSISDN or logical name.

7.2.55 Location-Estimate AVP

The *Location-Estimate* AVP (AVP code 1242) is of type UTF8String and contains an estimate of the location of an MS in universal coordinates and the accuracy of the estimate.

7.2.56 Location-Estimate-Type AVP

The *Location-Estimate-Type* AVP (AVP code 1243) is of type Enumerated and contains one of the following values:

CURRENT_LOCATION	0
CURRENT_LAST_KNOWN_LOCATION	1
INITIAL_LOCATION	2
ACTIVATE_DEFERRED_LOCATION	3
CANCEL_DEFERRED_LOCATION	4

7.2.57 Location-Type AVP

The *Location-Type* AVP (AVP code 1244) is of type Grouped and indicates the type of location estimate required by the LCS client.

It has the following ABNF grammar:

```
Location-Type::= < AVP Header: 1244 >
                 [ Location-Estimate-Type ]
                 [ Deferred-Location-Event-Type ]
```

7.2.58 MBMS-Information AVP

The *MBMS-Information* AVP (AVP code 880) is of type Grouped. Its purpose is to allow the transmission of additional MBMS service specific information elements.

It has the following ABNF grammar:

```

MBMS-Information ::= < AVP Header: 880 >
                    [ TMGI ]
                    [ MBMS-Service-Type ]
                    [ MBMS-User-Service-Type ]
                    [ File-Repair-Supported ]
                    [ Required-MBMS-Bearer-Capabilities ]
                    [ MBMS-2G-3G-Indicator ]
                    [ RAI ]
                    * [ MBMS-Service-Area ]
                    [ MBMS-Session-Identity ]

```

7.2.59 MBMS-User-Service-Type AVP

The *MBMS-User-Service-Type* AVP (AVP code 1225) is of type Enumerated and indicates type of service the MBMS user service that is being delivered. The following values are supported:

DOWNLOAD (1)

The MBMS user service of type: download.

STREAMING (2)

The MBMS user service is of type: streaming.

7.2.60 Media-Initiator-Flag AVP

The *Media-Initiator-Flag* AVP (AVP code 882) is of type Enumerated and indicates which party has requested the session modification. The default value is "0" indicating the called party initiated the modification.

- [0] called party
- [1] calling party
- [2] unknown

7.2.61 Message-Body AVP

The *Message-Body* AVP (AVP Code 889) is of type Grouped AVP and holds information about the message bodies including user-to-user data.

It has the following ABNF grammar:

```

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

```

The message bodies shall not include the bodies' of Content-Type = "application-sdp" as these are captured in other AVPs.

7.2.62 Message-Class AVP

The *Message-Class* AVP (AVP code 1213) is of type Grouped.

It has the following ABNF grammar:

```

Message-Class ::= < AVP Header: 1213 >
                 [ Class-Identifier ]
                 [ Token-Text ]

```

7.2.63 Message-ID AVP

The *Message-ID* AVP (AVP code 1210) is of type UTF8String and holds the MM identification provided by the originating MMS Relay/Server.

7.2.64 Message-Size AVP

The *Message-Size* AVP (AVP code 1212) is of type Unsigned32 and holds the total size in bytes of the MM calculated according to TS 23.140 [208] .

7.2.65 Message-Type AVP

The *Message-Type* AVP (AVP code 1211) is of type Enumerated and holds the type of the message according to the MMS transactions e.g. submission, delivery.

The following values are defined and are as specified in MMS Encapsulation [209]:

- 1 m-send-req
- 2 m-send-conf
- 3 m-notification-ind
- 4 m-notifyresp-ind
- 5 m-retrieve-conf
- 6 m-acknowledge-ind
- 7 m-delivery-ind
- 8 m-read-rec-ind
- 9 m-read-orig-ind
- 10 m-forward-req
- 11 m-forward-conf
- 12 m-mbox-store-conf
- 13 m-mbox-view-conf
- 14 m-mbox-upload-conf
- 15 m-mbox-delete-conf

7.2.66 MM-Content-Type AVP

The *MM-Content-Type* AVP (AVP code 1203) is of type Grouped and indicates the overall content type of the MM content and includes information about all the contents of an MM.

It has the following ABNF grammar:

```
MM-Content-Type ::= < AVP Header: 1203 >
                    [ Type-Number ]
                    [ Additional-Type-Information ]
                    [ Content-Size ]
                    * [ Additional-Content-Information ]
```

7.2.67 MMBox-Storage-Requested AVP

The *MMBox-Storage-Requested* AVP (AVP code 1248) is of type Enumerated and indicates whether an MMBoxstorage has been requested by the originator MMS User Agent or not. The values for whether an MMBox Storage was requested are:

- 0 No
- 1 Yes

7.2.68 MMS-Information AVP

The *MMS-Information* AVP (AVP code 877) is of type Grouped. Its purpose is to allow the transmission of additional MMS service specific information elements.

It has the following ABNF grammar:

```
MMS-Information ::= < AVP Header: 877>
    [ Originator-Address ]
    * [ Recipient-Address ]
    [ Submission-Time ]
    [ MM-Content-Type ]
    [ Priority ]
    [ Message-ID ]
    [ Message-Type ]
    [ Message-Size ]
    [ Message-Class ]
    [ Delivery-Report-Requested ]
    [ Read-Reply-Report-Requested ]
    [ MMBox-Storage-Information ]
    [ Applic-ID ]
    [ Reply-Applic-ID ]
    [ Aux-Applic-Info ]
    [ Content-Class ]
    [ DRM-Content ]
    [ Adaptations ]
    [ VASP-Id ]
    [ VAS-Id ]
```

7.2.69 Node-Functionality AVP

The *Node-Functionality* AVP (AVP code 862) is of type Enumerated and includes the *functionality* identifier of the *node*.

The functionality identifier can be one of the following:

- S-CSCF 0
- P-CSCF 1
- I-CSCF 2
- MRFC 3
- MGCF 4
- BGCF 5
- AS 6

7.2.70 Number-Of-Participants AVP

The *Number-Of-Participants* AVP (AVP code 885) is of type Unsigned32 and holds the number of invited parties of the PoC session when included in the initial charging request message. When included in interim / update charging messages, it indicates the number of parties who are currently attached in the session at the time the interim / update messages are sent.

NOTE: The information to populate this field may be obtained from the TBCP-Talk-Burst-Grant message.

7.2.71 Originating-IOI AVP

The *Originating-IOI* AVP (AVP code 839) is of type UTF8String (alphanumeric string) and holds the Inter Operator Identifier (IOI) for the originating network as generated by the IMS network element which takes responsibility for populating this parameter [404] in a SIP request [202].

The Originating IOI contains the following values:

- Type 1 IOI: IOI of the visited network where the P-CSCF is located.
- Type 2 IOI:
 - IOI of the home network of the originating end user where the S-CSCF is located in case a session is initiated from the IMS. In case of redirection by the S-CSCF, *Originating-IOI* AVP indicates the terminating party's network operator from which the session is redirected.
 - IOI of the originating network where the MGCF is located in case a session is initiated from the PSTN toward the IMS.
- Type 3 IOI:
 - IOI of the home network (originating side or terminating side) where the S-CSCF is located when forwarding a SIP request [202] to an AS (proxy, terminating UA or redirect server or B2BUA).
 - IOI of the service provider network where the AS is located when an AS (originating UA or B2BUA) initiates a SIP request [202].

For further details on the Type 1, Type 2 and Type 3 IOIs, please refer to 3GPP TS 32.240 [1].

7.2.72 Originator AVP

The *Originator* AVP (AVP code 864) is of type Enumerated and indicates the originating party of the message body. The following values are defined:

Calling Party 0

Called Party 1

7.2.73 Originator-Address AVP

The *Originator-Address* AVP (AVP code 886) is of type Grouped. Its purpose is to identify the originator of a MM.

It has the following ABNF grammar:

```
Originator-Address ::= < AVP Header: 886 >
                        [ Address-Type ]
                        [ Address-Data ]
                        [ Address-Domain ]
```

7.2.74 Outgoing-Trunk-Group-ID AVP

The *Outgoing-Trunk-Group-ID* AVP (AVP code 853) is of type UTF8String and identifies the outgoing PSTN leg.

7.2.75 Participants-Involved AVP

The *Participants-Involved* AVP (AVP code 887) is of type UTF8String and holds the list of address (Public User ID: SIP URI, TEL URI, MSISDN) of the parties who are involved into the PoC session.

7.2.75A Participants-Group AVP

The *Participants-Group* AVP (AVP code 1260) is of type Grouped and holds detailed information, e.g. the addresses (Public User ID: SIP URI, TEL URI, MSISDN), the access priority parameters, etc, of the parties who are involved into the PoC session.

It has the following ABNF grammar:

```
< Participants-Group > : : = < AVP Header: 1260 >  
  
                        [Called-Party-Address ]  
                        [Participant-Access-Priority]
```

7.2.75B Participant-Access-Priority AVP

Participant-Access-Priority AVP (AVP code 1259) is of type Enumerated. It is a subfield of Participants-Group AVP to indicate the priority level for users when initiating a new PoC session or participating in a PoC session.

The AVP may take the values as follows:

- 1 Pre-emptive priority: The highest level priority. A request with pre-emptive priority SHALL cause the current other requests to be revoked immediately, unless they are also with pre-emptive priority.
- 2 High priority: Lower than Pre-emptive priority.
- 3 Normal priority: Normal level. Lower than High priority.
- 4 Low priority: Lowest level priority.

7.2.76 PDG-Address AVP

The *PDG-Address* AVP (AVP code 895) is of type Address and contains the PDG IP address.

7.2.77 PDG-Charging-Id AVP

The *PDG-Charging-Id* AVP (AVP code 896) is of type Unsigned32 and contains the charging identifier generated by the PDG for the tunnel. Charging identifier is generated at tunnel establishment and transferred to 3GPP AAA Server.

Different PDGs allocate the charging identifier independently of each other and may allocate the same numbers. PDG-Charging-Id together with PDG-Address constitutes a unique identifier for the tunnel.

Coding of this AVP is same as 3GPP-Charging-Id coding described in 3GPP TS 29.061 [207].

7.2.78 PDP-Address AVP

The *PDP-Address* AVP (AVP code 1227) is of type Address and holds the IP-address associated with the PDP session.

7.2.79 PDP-Context-Type AVP

The *PDP-Context-Type* AVP (AVP code 1247) is of type Enumerated and indicates the type of a PDP context.

The values for requested are:

- 0 PRIMARY
- 1 SECONDARY

This AVP shall only be present in the CCR Initial.

7.2.80 PoC-Change-Condition AVP

The *PoC-Change-Condition* AVP (AVP code 1261) is of type Enumerated and contains the reason for closing a container and the addition of a new container. The AVP may take the following values:

serviceChange	(0)
volumeLimit	(1)
timeLimit	(2)
numberOfTalkBurstLimit	(3)
numberOfActiveParticipants	(4)
tariffTime	(5)

7.2.81 PoC-Change-Time AVP

The *PoC-Change-Time* AVP (AVP code 1262) is of type Time and is a time stamp that defines the moment when a container is closed or the CDR is closed.

7.2.82 PoC-Controlling-Address AVP

The *PoC-Controlling-Address* AVP (AVP code 858) is of type UTF8String and identifies the PoC server performing the controlling function for the associated PoC session.

7.2.83 PoC-Group-Name

The *PoC-Group-Name* AVP (AVP code 859) is of type UTF8String and identifies a group. Included if the session is a pre-arranged group session or a chat group session.

7.2.84 PoC-Information AVP

The *PoC-Information* AVP (AVP code 879) is of type Grouped. Its purpose is to allow the transmission of additional PoC service specific information elements.

It has the following ABNF grammar:

```
PoC-Information ::= =
    < AVP Header: 879>
    [ PoC-Server-Role ]
    [ PoC-Session-Type ]
    [ PoC-User-Role ]
    [ Number-Of-Participants ]
    * [ Participants-Involved ]
    * [ Talk-Burst-Exchange ]
    [ PoC-Controlling-Address ]
    [ PoC-Group-Name ]
    [ PoC-Session-Id ]
    [ Charged-Party ]
```

7.2.85 PoC-Server-Role AVP

The *PoC-Server-Role* AVP (AVP code 883) is of type Enumerated and specifies the role of the PoC server.

The identifier can be one of the following:

0	Participating PoC Server
1	Controlling PoC Server

7.2.86 PoC-Session-Id AVP

The *PoC-Session-Id* AVP (AVP code 1229) is of type UTF8String. It uniquely identifies an end-to-end PoC session and may be used for correlation between charging information generated by participating and controlling PoC functions. This information is obtained from the "Contact" header of the SIP message received from the controlling PoC function.

Note: The PoC-Session-Id may not be available in the initial charging interactions for the PoC session.

7.2.87 PoC-Session-Type AVP

The *PoC-Session-Type* AVP (AVP code 884) is of type Enumerated and specifies the type of the PoC session.

The identifier can be one of the following, refer Appendix C.5.1 in OMA PoC Control Plane specification [211]:

- 0 1 to 1 PoC session
- 1 chat PoC group session
- 2 pre-arranged PoC group session
- 3 ad-hoc PoC group session

7.2.87A PoC-User-Role AVP

The *PoC-User-Role* AVP (AVP code: 1252) is of type Grouped. It specifies the role(s) related information of the PoC User that participating in the PoC Session.

It has the following grammar:

```
PoC-User-Role ::  
    <AVP header: TBD>  
    [PoC-User-Role-IDs]  
    [PoC-User-Role-info-Units]
```

7.2.87B PoC-User-Role-IDs AVP

The *PoC-User-Role-IDs* AVP (AVP code 1253) is of type UTF8String and identifies the PoC user role.

7.2.87C PoC-User-Role-info-Units AVP

The *Poc-User-Role-info-Units* (AVP code: 1254) is of type Enumerated and specify the role type details of PoC users.

The identifier can be one of the following:

- 1. Moderator
- 2. Dispatcher

7.2.88 Positioning-Data AVP

The *Positioning-Data* AVP (AVP code 1245) is of type UTF8String and indicates the usage of each positioning method that was attempted to determine the location estimate either successfully or unsuccessfully.

7.2.89 Priority AVP

The *Priority* AVP (AVP code 1209) is of type Enumerated and the priority (importance) of the message if specified by the originator MMS User Agent.

The values are:

- 0 Low
- 1 Normal

2 High

7.2.90 PS-Append-Free-Format-Data AVP

The PS-Append-Free-Format-Data AVP (AVP code 867) is of type enumerated and indicates if the information sent in the PS-Free-Format-Data AVP must be appended to the PS-free-format-data stored for the online-session.

The following values are defined:

- 0 "Append": If this AVP is present and indicates "Append", the GGSN shall append the received PS free format data to the PS free format data stored for the online charging session.
- 1 "Overwrite": If this AVP is absent or in value "Overwrite", the GGSN shall overwrite all PS free format data already stored for the online charging session.

The GGSN shall ignore this AVP if no PS free format data is stored for the online charging session.

7.2.91 PS-Free-Format-Data AVP

The PS-Free-Format-Data AVP (AVP code 866) is of type OctetString and holds online charging session specific data.

7.2.92 PS-Furnish-Charging-Information AVP

The PS-Furnish-Charging-Information AVP (AVP code 865) is of type Grouped. Its purpose is to add online charging session specific information, received via the Ro reference point, onto the Rf reference point in order to facilitate its inclusion in CDRs. This information element may be received in a CCA message via the Ro reference point. In situations where online and offline charging are active in parallel, the information element is transparently copied into an ACR to be sent on the Rf reference point.

It has the following ABNF grammar:

```
PS-Furnish-Charging-Information ::= < AVP Header: 865>
                                   { 3GPP-Charging-Id }
                                   { PS-Free-Format-Data }
                                   [ PS-Append-Free-Format-Data ]
```

7.2.93 PS-Information AVP

The *PS-Information* AVP (AVP code 874) is of type Grouped. Its purpose is to allow the transmission of additional PS service specific information elements.

It has the following ABNF grammar:

```
PS-Information ::= < AVP Header: 874>
                 [ 3GPP-Charging-Id ]
                 [ 3GPP-PDP-Type ]
                 [ PDP-Address ]
                 [ 3GPP-GPRS-Negotiated-QoS-Profile ]
                 [ SGSN-Address ]
                 [ GGSN-Address ]
                 [ CG-Address ]
                 [ 3GPP-IMSI-MCC-MNC ]
                 [ 3GPP-GGSN- MCC-MNC ]
                 [ 3GPP-NSAPI ]
                 [ Called-Station-Id ]
                 [ 3GPP-Session-Stop-Indicator ]
                 [ 3GPP-Selection-Mode ]
                 [ 3GPP-Charging-Characteristics ]
                 [ 3GPP-SGSN-MCC-MNC ]
                 [ 3GPP-MS-TimeZone ]
```

[3GPP-CAMEL-Charging-Info]
 [Charging-Rule-Base-Name]
 [3GPP-User-Location-Info]
 [3GPP-RAT-Type]
 [PS-Furnish-Charging-Information]
 [PDP-Context-Type]

7.2.94 Quota-Consumption-Time AVP

The *Quota-Consumption-Time* AVP (AVP code 881) is of type Unsigned32 and contains an idle traffic threshold time in seconds. This AVP may be included within the Multiple-Services-Credit-Control AVP when this AVP also contains a Granted-Service-Units AVP containing a CC-Time AVP (i.e. when the granted quota is a time quota).

7.2.95 Quota-Holding-Time AVP

The *Quota-Holding-Time* AVP (AVP code 871) is of type Unsigned32 and contains the quota holding time in seconds. The client shall start the quota holding timer when quota consumption ceases. This is always when traffic ceases, i.e. the timer is re-started at the end of each packet. The Credit Control Client shall deem a quota to have expired when no traffic associated with the quota is observed for the value indicated by this AVP. The timer is stopped on sending a CCR and re-initialised on receiving a CCA with the previous used value or a new value of Quota-Holding-Time if received.

This optional AVP may only occur in a CCA command. It is contained in the Multiple-Services-Credit-Control AVP. It applies equally to the granted time quota and to the granted volume quota.

A Quota-Holding-Time value of zero indicates that this mechanism shall not be used. If the Quota-Holding-Time AVP is not present, then a locally configurable default value in the client shall be used.

7.2.96 Read-Reply-Report-Requested AVP

The *Read-Reply-Report-Requested* AVP (AVP code 1222) is of type Enumerated and indicates whether a read reply report has been requested by the originator MMS User Agent or not.

The values for whether a report was requested are:

- 0 No
- 1 Yes

7.2.97 Recipient-Address AVP

The *Recipient-Address* AVP (AVP code 1201) is of type Grouped. Its purpose is to identify the recipient of a MM.

It has the following ABNF grammar:

```
Recipient-Address ::= < AVP Header: 1201 >
                    [ Address-Type ]
                    [ Address-Data ]
                    [ Address-Domain ]
                    [ Addressee-Type ]
```

7.2.98 Reply-Applic-ID AVP

The *Reply-Applic-ID* AVP (AVP code 1223) is of type UTF8String and holds the identifier of a 'reply path', i.e. the identifier of the application to which delivery reports, read-reply reports and reply-MMs are addressed.

7.2.99 Reporting-Reason AVP

The *Reporting-Reason* AVP (AVP code 872) is of type Enumerated and specifies the reason for usage reporting for one or more types of quota for a particular category. It can occur directly in the Multiple-Services-Credit-Control AVP, or in the Used-Service-Units AVP within a Credit Control Request command reporting credit usage. It shall not be used at command level. It shall always and shall only be sent when usage is being reported.

The following values are defined for the Reporting-Reason AVP:

- | | |
|---|-----|
| THRESHOLD | (0) |
| <ul style="list-style-type: none"> This value is used to indicate that the reason for usage reporting of the particular quota type indicated in the Used-Service-Units AVP where it appears is that the threshold has been reached. | |
| QHT | (1) |
| <ul style="list-style-type: none"> This value is used to indicate that the reason for usage reporting of all quota types of the Multiple-Service-Credit-Control AVP where its appears is that the quota holding time specified in a previous CCA command has been hit (i.e. the quota has been unused for that period of time). | |
| FINAL | (2) |
| <ul style="list-style-type: none"> This value is used to indicate that the reason for usage reporting of all quota types of the Multiple-Service-Credit-Control AVP where its appears is that a normal PDP context termination has happened. | |
| QUOTA_EXHAUSTED | (3) |
| <ul style="list-style-type: none"> This value is used to indicate that the reason for usage reporting of the particular quota type indicated in the Used-Service-Units AVP where it appears is that the quota has been exhausted. | |
| VALIDITY_TIME | (4) |
| <ul style="list-style-type: none"> This value is used to indicate that the reason for usage reporting of all quota types of the Multiple-Service-Credit-Control AVP where its appears is that the credit authorization lifetime provided in the Validity-Time AVP has expired. | |
| OTHER_QUOTA_TYPE | (5) |
| <ul style="list-style-type: none"> This value is used to indicate that the reason for usage reporting of the particular quota type indicated in the Used-Service-Units AVP where it appears is that, for a multi-dimensional quota, one reached a trigger condition and the other quota is being reported. | |
| RATING_CONDITION_CHANGE | (6) |
| <ul style="list-style-type: none"> This value is used to indicate that the reason for usage reporting of all quota types of the Multiple-Service-Credit-Control AVP where its appears is that a change has happened in some of the rating conditions that were previously armed (through the Trigger-Type AVP, e.g. QoS, Radio Access Technology,...). The specific condition that has changed is indicated in an associated Trigger-Type AVP. | |
| FORCED_REAUTHORISATION | (7) |
| <ul style="list-style-type: none"> This value is used to indicate that the reason for usage reporting of all quota types of the Multiple-Service-Credit-Control AVP where its appears is that it is there has been a Server initiated re-authorisation procedure, i.e. receipt of RAR command | |
| POOL_EXHAUSTED | (8) |
| <ul style="list-style-type: none"> This value is used to indicate that the reason for usage reporting of the particular quota type indicated in the User-Service-Units AVP where it appears is that granted units are still available in the pool but are not sufficient for a rating group using the pool. | |

The values QHT, FINAL, VALIDITY_TIME, FORCED_REAUTHORISATION, RATING_CONDITION_CHANGE apply for all quota types and are used directly in the Multiple-Services-Credit-Control AVP, whereas the values THRESHOLD, QUOTA_EXHAUSTED and OTHER_QUOTA_TYPE apply to one particular quota type and shall occur only in the Used-Service-Units AVP. The value POOL_EXHAUSTED apply to all quota types using the credit

pool and occurs in the Used-Service-Units AVP. It may optionally occur in the Multiple-Services-Credit-Control AVP if all quota types use the same pool.

When the value RATING_CONDITION_CHANGE is used, the Trigger-Type AVP shall also be included to indicate the specific event which caused the re-authorisation request.

7.2.100 Requested-Party-Address AVP

The *Requested-Party-Address* AVP (AVP code 1251) is of type UTF8 String. In IMS it holds the address (SIP URI or TEL URI) of the party (Public User ID or Public Service ID) to whom the SIP transaction was originally posted. The Requested Party Address shall be populated with the SIP URI or TEL URI contained in the Request-URI of the incoming request. This field is only present if different from the Called Party Address parameter.

7.2.101 Role-of-node AVP

The *Role-Of-Node* AVP (AVP code 829) is of type Enumerated and specifies the role of the AS/CSCF.

The identifier can be one of the following:

ORIGINATING_ROLE	0	The AS/CSCF is applying an originating role, serving the calling subscriber.
TERMINATING_ROLE	1	The AS/CSCF is applying a terminating role, serving the called subscriber.
PROXY_ROLE	2	The AS is applying a proxy role.
B2BUA_ROLE	3	The AS is applying a B2BUA role.

7.2.102 SDP-Media-Component AVP

The *SDP-Media-Component* AVP (AVP code 843) is of type Grouped and contains information about media used for a IMS session.

It has the following ABNF grammar:

```
<SDP-Media-Component>:: = <AVP Header: 843 >
                           [ SDP-Media-Name ]
                           * [ SDP-Media-Description ]
                           [ Media-Initiator-Flag ]
                           [ Authorized-QoS ]
                           [ 3GPP-Charging-Id ]
                           [ Access-Network-Charging-Identifier-Value ]
```

NOTE: When populating the SDP-Media-Component, either the 3GPP-Charging-ID or the Access-Network-Charging-Identifier-Value should be present but not both. The 3GPP-Charging-ID is expected to be used for 3GPP defined IP-CANS (e.g. GPRS) while the Access-Network-Charging-Identifier-Value is used for non-3GPP defined IP-CANS.

7.2.103 SDP-Media-Description AVP

The *SDP-Media-Description* AVP (AVP code 845) is of type UTF8String and holds the content of an "attribute-line" (i=, c=, b=, k=, a=, etc.) related to a media component, as described in [406]. The attributes are specifying the media described in the SDP-Media-Name AVP.

7.2.104 SDP-Media-Name AVP

The *SDP-Media-Name* AVP (AVP code 844) is of type UTF8String and holds the content of a "m=" line in the SDP data.

7.2.105 SDP-Session-Description AVP

The *SDP-Session-Description* AVP (AVP code 842) is of type UTF8String and holds the content of an "attribute-line" (i=, c=, b=, k=, a=, etc.) related to a session, as described in [406].

7.2.106 Served-Party-IP-Address AVP

The *Served-Party-IP-Address* AVP (AVP code 848) is of type Address and holds the IP address of either the calling or called party, depending on whether the P-CSCF is in touch with the calling or the called party. This AVP is only provided by the P-CSCF.

7.2.107 Service-ID AVP

The *Service-ID* AVP (AVP code 855) is of type UTF8String and identifies the service the MRFC is hosting. For conferences the conference ID is used as the value of this parameter.

7.2.107A Service-Generic-Information AVP

The *Service-Generic-Information* AVP (AVP code 1256) is of type Grouped. Its purpose is to allow the transmission of service information elements used for all services.

The OMA specific use is defined at OMNA WSP Content Type Codes database [210].

7.2.108 Service-Information AVP

The *Service-Information* AVP (AVP code 873) is of type Grouped. Its purpose is to allow the transmission of additional 3GPP service specific information elements which are not described in this document.

It has the following ABNF grammar:

```
Service-Information ::= < AVP Header: 873>
                        [ Subscription-Id ]
                        [ PS-Information ]
                        [ WLAN-Information ]
                        [ IMS-Information ]
                        [ MMS-Information ]
                        [ LCS-Information ]
                        [ PoC-Information ]
                        [ MBMS-Information ]
                        [ Service-Generic-Information ]
```

The format and the contents of the fields inside the Service-Information AVP are specified in the middle-tier documents which are applicable for the specific service. Note that the formats of the fields are service-specific, i.e. the format will be different for the various services.

The Subscription-Id AVP in Service-Information AVP is only used on the Rf interface.

Further fields may be included in the Service-Information AVP when new services are introduced.

7.2.109 Service-Specific-Data AVP

The *Service-Specific-Data* AVP (AVP Code 863) is of type UTF8String and holds the value of the Service-Specific-Data.

7.2.109A Service-Specific-Info AVP

The *Service-Specific-Info* AVP (AVP Code 1249) is of type Grouped and holds service specific data if and as provided by an Application Server.

It has the following ABNF grammar:

```
Service-Specific-Info ::= < AVP Header: 1249 >
                        [ Service-Specific-Data ]
                        [ Service-Specific-Type ]
```

7.2.109B Service-Specific-Type AVP

The *Service-Specific-Type* AVP (AVP Code 1257) is of type Unsigned32 and holds the type of the Service-Specific-Data.

7.2.110 SGSN-Address AVP

The *SGSN-Address* AVP (AVP code 1228) is of type Address and holds the IP-address of the SGSN that was used during a report.

7.2.111 SIP-Method AVP

The *SIP-Method* AVP (AVP code 824) is of type UTF8String and holds the name of the SIP Method (INVITE, UPDATE etc.) causing a accounting request to be sent to the CDF or credit control request to be sent to the OCF.

7.2.112 SIP-Request-Timestamp AVP

The *SIP-Request-Timestamp* AVP (AVP code 834) is of type Time and holds the time in UTC format of the SIP request (e.g. Invite, Update).

7.2.113 SIP-Response-Timestamp AVP

The *SIP-Response-Timestamp* AVP (AVP code 835) is of type Time and holds the time in UTC format of the response to the SIP request (e.g. 200 OK).

7.2.114 Submission-Time AVP

The *Submission-Time* AVP (AVP code 1202) is of type Time and indicates the time at which the MM was submitted or forwarded as specified in the corresponding MM1 message.

7.2.115 Talk-Burst-Exchange AVP

The *Talk-Burst-Exchange* AVP (AVP code 1255) is of type Grouped and holds the talk burst related charging data.

It has the following ABNF grammar:

```
<Talk-Burst-Exchange>:: = < AVP Header: 1255 >
                        { PoC-Change-Time }
                        [ Number-Of-Talk-Bursts ]
                        [ Talk-Burst-Volume ]
                        [ Talk Bursts-Time ]
                        [ Number-Of-Received-Talk-Bursts ]
                        [ Received-Talk-Burst-Volume ]
                        [ Received-Talk-Burst-Time ]
                        [ Number-Of-Participants ]
                        [ PoC-Change-Condition ]
```

7.2.116 Terminating-IOI AVP

The *Terminating-IOI* AVP (AVP code 840) is of type UTF8String (alphanumeric string) and holds the Inter Operator Identifier (IOI) for the terminating network as generated by the IMS network element which takes responsibility for populating this parameter [404] in a SIP response [202].

The Terminating IOI contains the following values:

- Type 1 IOI: IOI of the home network where the S-CSCF is located.
- Type 2 IOI:
 - IOI of the home network of the terminating end user where the S-CSCF is located in case a session is initiated toward the IMS. In case of redirection by the S-CSCF, *Terminating-IOI* AVP indicates the terminating party's network operator to which the session is redirected.
 - IOI of the terminating network where the MGCF is located in case a session is initiated from the IMS toward the PSTN.
- Type 3 IOI:
 - IOI of the service provider network (originating side or terminating side) where the AS (proxy, terminating UA or redirect server or B2BUA) is located when receiving a SIP request [202].
 - IOI of the home network operator contacted by an AS when an AS (originating UA or B2BUA) initiates a SIP request [202].

For further details on the Type 1, Type 2 and Type 3 IOIs, please refer to 3GPP TS 32.240 [1].

7.2.117 Time-Quota-Threshold AVP

The *Time-Quota-Threshold* AVP (AVP code 868) is of type Unsigned32 and contains a threshold value in seconds. This AVP may be included within the Multiple-Services-Credit-Control AVP when this AVP also contains a Granted-Service-Units AVP containing a CC-Time AVP (i.e. when the granted quota is a time quota).

If received, the Credit Control client shall seek re-authorisation from the server for the quota when the quota contents fall below the supplied threshold. The client shall allow service to continue whilst the re-authorisation is progress, until the time at which the original quota would have been consumed.

7.2.118 Time-Stamps AVP

The *Time-Stamps* AVP (AVP code 833) is of type Grouped and holds the time of the initial SIP request and the time of the response to the initial SIP Request.

It has the following ABNF grammar:

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

7.2.119 Token-Text AVP

The *Token-Text* AVP (AVP code 1215) is of type UTF8String and contains extension information for the Message-Class AVP.

7.2.120 Trigger-Type AVP

The *Trigger-Type* AVP (AVP code 870) is of type Enumerated and indicates a single re-authorisation event type.

When included in the Credit Control Answer command, the Trigger-Type AVP indicates the events that shall cause the credit control client to re-authorise the associated quota. The client shall not re-authorise the quota when events which are not included in the Trigger AVP occur.

When included in the Credit Control Request command indicates the specific event which caused the re-authorisation request of the Reporting-Reason with value RATING_CONDITION_CHANGE associated.

It has the following values:

CHANGE_IN_SGSN_IP_ADDRESS (1)

- This value is used to indicate that a change in the SGSN IP address shall cause the credit control client to ask for a re-authorisation of the associated quota.

CHANGE_IN_QOS (2)

- This value is used to indicate that a change in the end user negotiated QoS shall cause the credit control client to ask for a re-authorisation of the associated quota.

NOTE 1: This should not be used in conjunction with enumerated values 10 to 23.

CHANGE_IN_LOCATION (3)

- This value is used to indicate that a change in the end user location shall cause the credit control client to ask for a re-authorisation of the associated quota.

NOTE 2: This should not be used in conjunction with enumerated values 30 to 34.

CHANGE_IN_RAT (4)

- This value is used to indicate that a change in the radio access technology shall cause the credit control client to ask for a re-authorisation of the associated quota.

CHANGEINQOS_TRAFFIC_CLASS (10)

- This value is used to indicate that a change in the end user negotiated traffic class shall cause the credit control client to ask for a re-authorisation of the associated quota.

CHANGEINQOS_RELIABILITY_CLASS (11)

- This value is used to indicate that a change in the end user negotiated reliability class shall cause the credit control client to ask for a re-authorisation of the associated quota.

CHANGEINQOS_DELAY_CLASS (12)

- This value is used to indicate that a change in the end user negotiated delay class shall cause the credit control client to ask for a re-authorisation of the associated quota.

CHANGEINQOS_PEAK_THROUGHPUT (13)

- This value is used to indicate that a change in the end user negotiated peak throughput shall cause the credit control client to ask for a re-authorisation of the associated quota.

CHANGEINQOS_PRECEDENCE_CLASS (14)

- This value is used to indicate that a change in the end user negotiated precedence class shall cause the credit control client to ask for a re-authorisation of the associated quota.

CHANGEINQOS_MEAN_THROUGHPUT (15)

- This value is used to indicate that a change in the end user negotiated mean throughput shall cause the credit control client to ask for a re-authorisation of the associated quota.

CHANGEINQOS_MAXIMUM_BIT_RATE_FOR_UPLINK (16)

- This value is used to indicate that a change in the end user negotiated uplink maximum bit rate shall cause the credit control client to ask for a re-authorisation of the associated quota.

CHANGEINQOS_MAXIMUM_BIT_RATE_FOR_DOWNLINK (17)

- This value is used to indicate that a change in the end user negotiated downlink maximum bit rate shall cause the credit control client to ask for a re-authorisation of the associated quota.

CHANGEINQOS_RESIDUAL_BER (18)

- This value is used to indicate that a change in the end user negotiated residual BER shall cause the credit control client to ask for a re-authorisation of the associated quota.

CHANGEINQOS_SDU_ERROR_RATIO (19)

- This value is used to indicate that a change in the end user negotiated SDU error ratio shall cause the credit control client to ask for a re-authorisation of the associated quota.

CHANGEINQOS_TRANSFER_DELAY (20)

- This value is used to indicate that a change in the end user negotiated transfer delay shall cause the credit control client to ask for a re-authorisation of the associated quota.

CHANGEINQOS_TRAFFIC_HANDLING_PRIORITY (21)

- This value is used to indicate that a change in the end user negotiated traffic handling priority shall cause the credit control client to ask for a re-authorisation of the associated quota.

CHANGEINQOS_GUARANTEED_BIT_RATE_FOR_UPLINK (22)

- This value is used to indicate that a change in the end user negotiated uplink guaranteed bit rate shall cause the credit control client to ask for a re-authorisation of the associated quota.

CHANGEINQOS_GUARANTEED_BIT_RATE_FOR_DOWNLINK (23)

- This value is used to indicate that a change in the end user negotiated downlink guaranteed bit rate shall cause the credit control client to ask for a re-authorisation of the associated quota.

CHANGEINLOCATION_MCC (30)

- This value is used to indicate that a change in the MCC of the serving network shall cause the credit control client to ask for a re-authorisation of the associated quota.

CHANGEINLOCATION_MNC (31)

- This value is used to indicate that a change in the MNC of the serving network shall cause the credit control client to ask for a re-authorisation of the associated quota.

CHANGEINLOCATION_RAC (32)

- This value is used to indicate that a change in the RAC where the end user is located shall cause the credit control client to ask for a re-authorisation of the associated quota.

CHANGEINLOCATION_LAC (33)

- This value is used to indicate that a change in the LAC where the end user is located shall cause the credit control client to ask for a re-authorisation of the associated quota.

CHANGEINLOCATION_CellId (34)

- This value is used to indicate that a change in the Cell Identity where the end user is located shall cause the credit control client to ask for a re-authorisation of the associated quota.

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 shall cause the credit control client to ask for a re-authorisation of the associated quota.

CHANGEINPARTICIPANTS_Number (50)

- This value is used specifically for PoC to indicate that a change in the number of active participants within a PoC session shall cause the credit control client to ask for a re-authorisation of the associated quota.

7.2.121 Trunk-Group-ID AVP

The *Trunk-Group-ID* AVP (AVP code 851) is of type Grouped and identifies the incoming and outgoing PSTN legs.

It has the following ABNF grammar:

```
<Trunk-Group-ID>:: = <AVP Header: 851>
                    [ Incoming-Trunk-Group-ID ]
                    [ Outgoing-Trunk-Group-ID ]
```

7.2.122 Type-Number AVP

The *Type-Number* AVP (AVP code 1204) is of type Enumerated and identifies the well-known media types. The values are taken from OMNA WSP Content Type Codes database [210]

7.2.123 Unit-Quota-Threshold AVP

The *Unit-Quota-Threshold* AVP (AVP code 1226) is of type Unsigned32 and contains a threshold value in service specific units. This AVP may be included within the Multiple-Services-Credit-Control AVP when this AVP also contains a Granted-Service-Units AVP containing CC-Service-Specific-Units AVP (i.e. when the granted quota is service specific).

If received, the Credit Control client shall seek re-authorisation from the server for the quota when the quota contents fall below the supplied threshold. The client shall allow service to continue whilst the re-authorisation is in progress, up to the volume indicated in the original quota.

7.2.124 User-Session-ID AVP

The *User-Session-Id* AVP (AVP code 830) is of type UTF8String and holds the session identifier. For a SIP session the *User-Session-ID* contains the SIP Call ID, as defined in [405].

7.2.125 Volume-Quota-Threshold AVP

The *Volume-Quota-Threshold* AVP (AVP code 869) is of type Unsigned32 and contains a threshold value in octets. This AVP may be included within the Multiple-Services-Credit-Control AVP when this AVP also contains a Granted-Service-Units AVP containing a CC-Total-Octets, CC-Input-Octets or CC-Output-Octets AVP (i.e. when the granted quota is a volume quota).

If received, the Credit Control client shall seek re-authorisation from the server for the quota when the quota contents fall below the supplied threshold. The client shall allow service to continue whilst the re-authorisation is in progress, up to the volume indicated in the original quota.

7.2.126 WAG-Address AVP

The WAG-Address AVP (AVP code 890) is of type Address and contains the WAG IP address.

7.2.127 WAG-PLMN-Id AVP

The WAG-PLMN-Id AVP (AVP code 891) is of type OctetString and contains the WAG PLMN id (MCC and MNC).

Coding of this AVP is same as 3GPP-SGSN-MCC-MNC coding described in 3GPP TS 29.061 [207].

7.2.128 WLAN-Information AVP

The *WLAN-Information* AVP (AVP code 875) is of type Grouped. Its purpose is to allow the transmission of additional WLAN service specific information elements. The format and the contents of the fields inside the *WLAN-Information* AVP is specified in TS 32.252 [22].

It has the following ABNF grammar:

```
WLAN-Information ::= < AVP Header: 875>
                    [ WLAN-Session-Id ]
                    [ PDG-Address ]
                    [ PDG-Charging-Id ]
                    [ WAG-Address ]
                    [ WAG-PLMN-Id ]
                    [ WLAN-Radio-Container ]
                    [ WLAN-UE-Local-IPAddress ]
```

7.2.129 WLAN-Radio-Container AVP

The *WLAN-Radio-Container* AVP (AVP code 892) is of type Grouped. The *WLAN-Radio-Container* AVP has the following format:

```
WLAN-Radio-Container ::= < AVP Header: 892>
                        [ Operator-Name ]
                        [ Location-Type ]
                        [ Location-Information ]
                        [ WLAN-Technology ]
```

7.2.130 WLAN-Session-Id AVP

The *WLAN-Session-Id* AVP (AVP code 1246) is of type Unsigned32 and contains the charging id generated by the AAA Server for the session.

Coding of this AVP is same as 3GPP-Charging-Id coding described in TS 29.061 [207].

7.2.131 WLAN-Technology AVP

The *WLAN-Technology* AVP (AVP code 893) is of type Unsigned32. Actual content of this AVP is tbd.

7.2.132 WLAN-UE-Local-IPAddress AVP

The *WLAN-UE-Local-IPAddress* AVP (AVP code 894) is of type Address and contains the UE's local IP address.

Annex A (informative): Bibliography

a) **The 3GPP charging specifications**

- 3GPP TS 32.250: "Telecommunication management; Charging management; Circuit Switched (CS) domain charging".
- 3GPP TS 32.251: "Telecommunication management; Charging management; Packet Switched (PS) domain charging".
- 3GPP TS 32.252: "Telecommunication management; Charging management; Wireless Local Area Network (WLAN) charging".
- 3GPP TS 32.260: "Telecommunication management; Charging management; IP Multimedia Subsystem (IMS) charging".
- 3GPP TS 32.270: "Telecommunication management; Charging management; Multimedia Messaging Service (MMS) charging".
- 3GPP TS 32.271: "Telecommunication management; Charging management; Location Services (LCS) charging".
- 3GPP TS 32.298: "Telecommunication management; Charging management; Charging Data Record (CDR) encoding rules description".
- 3GPP TS 32.297: "Telecommunication management; Charging management; Charging Data Record (CDR) file format and transfer".
- 3GPP TS 32.296: "Telecommunication management; Charging management; Online Charging System (OCS) applications and interfaces".
- 3GPP TS 32.295: "Telecommunication management; Charging management; Charging Data Record (CDR) transfer".

b) **Common 3GPP specifications**

- 3GPP TS 33.201: "Access domain security".

c) **other Domain and Service specific 3GPP / ETSI specifications**

-

d) **Relevant ITU Recommendations**

-

e) **Relevant IETF RFCs**

- IETF RFC 959 (1985): "File Transfer Protocol".
- IETF RFC 1350 "TFTP Protocol".

Annex B (informative): Change history

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Cat	Old	New
Dec 2005	SA_30	SP 050654	--	--	Created for reference by TISPAN	--	6.5.0	7.0.0
Mar 2006	SA_31	SP-060079	0050	--	Corrections to LCS AVPs and to Diameter application	A	7.0.0	7.1.0
Mar 2006	SA_31	SP-060079	0051	--	Correction on threshold reauthorisation trigger for service specific units	A	7.0.0	7.1.0
Mar 2006	SA_31	SP-060084	0052	--	Alignment of MBMS AVPs with 29.061	A	7.0.0	7.1.0
Mar 2006	SA_31	SP-060079	0053	--	Correction to usage of Event Charging with Unit Reservation (ECUR)	A	7.0.0	7.1.0
Mar 2006	SA_31	SP-060079	0054	--	Corrections of the usage of AVPs in CCR/CCA messages	A	7.0.0	7.1.0
Mar 2006	SA_31	SP-060079	0055	--	Corrections to online charging description	A	7.0.0	7.1.0
Mar 2006	SA_31	SP-060079	0057	--	Consistent use of the Event-Timestamp AVP in the CCR message	A	7.0.0	7.1.0
Mar 2006	SA_31	SP-060079	0058	--	Correction to bindings for offline charging	A	7.0.0	7.1.0
Mar 2006	SA_31	SP-060079	0059	--	Correction to bindings for online charging	A	7.0.0	7.1.0
Mar 2006	SA_31	SP-060086	0060	--	Add missing AVP codes for MMS Online charging	A	7.0.0	7.1.0
Mar 2006	SA_31	SP-060087	0061	--	Add missing AVP code definitions for PoC charging	A	7.0.0	7.1.0
Mar 2006	SA_31	SP-060079	0063	--	Alignment on credit pooling with 32.240	A	7.0.0	7.1.0
Mar 2006	SA_31	SP-060079	0064	--	Corrections for charging procedures description	A	7.0.0	7.1.0
Mar 2006	SA_31	SP-060079	0065	--	Correction to session termination and overload protection	A	7.0.0	7.1.0
Mar 2006	SA_31	SP-060079	0066	--	Correction to Re-authorization Request	A	7.0.0	7.1.0
Mar 2006	SA_31	SP-060080	0067	--	Correction of AVP Code - Align with IETF RFC 3588 and RFC 4006	A	7.0.0	7.1.0
Mar 2006	SA_31	SP-060079	0069	--	Consistent use of the Cost-Information AVP in the CCA message	A	7.0.0	7.1.0
Mar 2006	SA_31	SP-060080	0070	--	Correction of AVP type of Content-Length AVP	A	7.0.0	7.1.0
Mar 2006	SA_31	SP-060080	0072	--	Correction of AVP code definitions for IMS charging - Align with IETF RFC 3261	A	7.0.0	7.1.0
Mar 2006	SA_31	SP-060080	0074	--	Correction to Cause-Code AVP type - Align with IETF RFC 3588	A	7.0.0	7.1.0
Mar 2006	SA_31	SP-060080	0076	--	Correction of timestamp data types- Align with RFC 3588	A	7.0.0	7.1.0
Mar 2006	SA_31	SP-060081	0078	--	Correction of User-Name AVP	A	7.0.0	7.1.0
Mar 2006	SA_31	SP-060080	0080	--	Correction of Terminating Inter Operator Identifier (IOI) AVP	A	7.0.0	7.1.0
Mar 2006	SA_31	SP-060080	0082	--	Correction of Multiple Service Indicator - Align with IETF RFC 4006	A	7.0.0	7.1.0
Mar 2006	SA_31	SP-060081	0084	--	Correction of SIP timestamps	A	7.0.0	7.1.0
Mar 2006	SA_31	SP-060081	0086	--	Correction to Calling-Party-Address AVP description	A	7.0.0	7.1.0
Mar 2006	SA_31	SP-060080	0087	--	Alignment on Message Body occurrences in ACR	A	7.0.0	7.1.0
Mar 2006	SA_31	SP-060081	0088	--	Correction to Inter Operator Identifier (IOI) occurrences in ACcounting Request (ACR)	A	7.0.0	7.1.0
Mar 2006	SA_31	SP-060088	0089	--	Correction to AVP code definitions for WLAN charging	A	7.0.0	7.1.0
Mar 2006	SA_31	SP-060075	0091	--	Alignment of PS AVPs with 32.251	A	7.0.0	7.1.0
Mar 2006	SA_31	SP-060076	0093	--	Correction to PS-Furnish-Charging-Information AVP at MSCC level	A	7.0.0	7.1.0
Mar 2006	SA_31	SP-060075	0095	--	Align Service Identifier Type with IETF RFC 4006	A	7.0.0	7.1.0
Mar 2006	SA_31	SP-060080	0097	--	Correction to Diameter AVPs table assignments - Align with IETF RFC 3588	A	7.0.0	7.1.0
Mar 2006	SA_31	SP-060087	0099	--	Correction to re-authorization on a change in the number of participants in a PoC session	A	7.0.0	7.1.0
Mar 2006	SA_31	SP-060087	0101	--	Correction to PoC charging correlation between the different servers	A	7.0.0	7.1.0
Jun 2006	SA_32	SP-060241	0103	--	Correction on Proxy-Info AVP - Align with IETF RFC 3588	A	7.1.0	7.2.0
Jun 2006	SA_32	SP-060241	0105	--	Correction to online re-authorization due to media change	A	7.1.0	7.2.0
Jun 2006	SA_32	SP-060241	0108	--	Alignment of Message Body AVP with TS 32.260	A	7.1.0	7.2.0
Jun 2006	SA_32	SP-060241	0110	--	Correction to Calling-Party-Address AVP definition	A	7.1.0	7.2.0
Jun 2006	SA_32	SP-060241	0112	--	Implicit registration: Add 'list of associated URIs' parameter to the IMS charging information - Align with SA2's 23.228 IMS Stage 2	A	7.1.0	7.2.0
Jun 2006	SA_32	SP-060244	0114	--	Correct PoC specific information	A	7.1.0	7.2.0
Jun 2006	SA_32	SP-060241	0116	--	Alignment with IETF RFC 3588 on use of Error-Reporting-Host AVP	A	7.1.0	7.2.0
Jun 2006	SA_32	SP-060241	0118	--	Alignment on Service-Identifier AVP	A	7.1.0	7.2.0
Jun 2006	SA_32	SP-060241	0120	--	Alignment with IETF RFC 4006 on use of the Direct-Debit-Failure-Handling AVP	A	7.1.0	7.2.0
Jun 2006	SA_32	SP-060241	0122	--	Correction to Update-Record use in Offline Charging	A	7.1.0	7.2.0
Jun 2006	SA_32	SP-060240	0126	--	Correct information set used for PDP context related charging	A	7.1.0	7.2.0
Jun 2006	SA_32	SP-060241	0128	--	Correction to Called Party Address in IMS Charging	A	7.1.0	7.2.0
Jun 2006	SA_32	SP-060241	0130	--	Correction to description of "Event-Type" AVP and "SIP-Method" AVP - Align with 32.260	A	7.1.0	7.2.0
Jun 2006	SA_32	SP-060248	0106	--	Add a new field named PoC_user_role to PoC_Information - Align with OMA PoC 2.0	B	7.1.0	7.2.0
Sep 2006	SA_33	SP-060524	0132	--	Correction on definition of Event-Timestamp due to ambiguity in IETF definitions	A	7.2.0	7.3.0
Sep 2006	SA_33	SP-060517	0136	--	Correction on WLAN-Session-ID AVP code	A	7.2.0	7.3.0
Sep 2006	SA_33	SP-060517	0138	--	Correction on LCS AVP codes	A	7.2.0	7.3.0
Sep 2006	SA_33	SP-060517	0140	--	Correction on MMS AVP codes	A	7.2.0	7.3.0

Sep 2006	SA_33	SP-060518	0142	--	Correction to number of participants charging for PoC	A	7.2.0	7.3.0
Sep 2006	SA_33	SP-060517	0144	--	Correction on the type of the Number-of-Participants AVP	A	7.2.0	7.3.0
Sep 2006	SA_33	SP-060542	0145	--	Add P-Access-Network-Info to IMS-Information and CDRs	C	7.2.0	7.3.0
Sep 2006	SA_33	SP-060516	0147	--	Align description of number of participants with 32.272 (PoC-CH)	A	7.2.0	7.3.0
Sep 2006	SA_33	SP-060542	0148	--	Enhance Service-Specific-Data AVP definition	C	7.2.0	7.3.0
Dec 2006	SA_34	SP-060720	0152	--	Correction of AVP categories - Align with RFC 4006	F	7.3.0	7.4.0
Dec 2006	SA_34	SP-060706	0153	--	Correct the usage-indicators for IMS AVPs	A	7.3.0	7.4.0
Dec 2006	SA_34	SP-060720	0154	--	Correction on Service Information - Align with OMA Charging Enabler v1.0	C	7.3.0	7.4.0
Dec 2006	SA_34	SP-060713	0155	--	Add Access Network Charging Identifier Value AVP in ACR and CCR	C	7.3.0	7.4.0
Dec 2006	SA_34	SP-060720	0156	--	Add an identifier for the service initiating offline Diameter Accounting	B	7.3.0	7.4.0
Dec 2006	SA_34	SP-060720	0157	--	Add an identifier for the served user in offline Diameter Accounting	B	7.3.0	7.4.0
Dec 2006	SA_34	SP-060706	0158	--	Correction on Multiple Service Credit Control (MSCC) - Align inside 32.299	A	7.3.0	7.4.0
Dec 2006	SA_34	SP-060706	0159	--	Correct MBMS Information - Align with 23.246	A	7.3.0	7.4.0
Dec 2006	SA_34	SP-060720	0160	--	Correction on PS-Information AVP	F	7.3.0	7.4.0
Dec 2006	SA_34	SP-060720	0161	--	Correction on Service Specific Data	F	7.3.0	7.4.0
Dec 2006	SA_34	SP-060720	0162	--	Add PoC User Access Priority into PoC-information - Align with OMA-RD-PoC-V2_0	B	7.3.0	7.4.0
Dec 2006	SA_34	SP-060714	0163	--	Introduce support of event based charging for PCC - Align with 23.203	B	7.3.0	7.4.0

History

Document history		
V7.0.0	December 2005	Publication
V7.1.0	March 2006	Publication
V7.2.0	June 2006	Publication
V7.3.0	September 2006	Publication
V7.4.0	December 2006	Publication