ETSI TS 132 299 V6.1.0 (2004-12)

Technical Specification

Universal Mobile Telecommunications System (UMTS);
Telecommunication management;
Charging management;
Diameter charging applications
(3GPP TS 32.299 version 6.1.0 Release 6)

Reference
DTS/TSGS-0532299v610

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/chaircor/ETSI_support.asp

Copyright Notification

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

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 references, abbreviations, definitions, descriptions, principles and requirements, 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 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.

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*.

a) The 3GPP charging specifications

[1] 3GPP TS 32.240: "Telecommunication management; Charging management; Charging Architecture and Principles".

[2]-[9] Void.

[10] 3GPP TS 32.250: "Telecommunication management; Charging management; Circuit Switched (CS) domain charging".

[11] 3GPP TS 32.251: "Telecommunication management; Charging management; Packet Switched (PS) domain charging".

[12] 3GPP TS 32.252: "Telecommunication management; Charging management; Wireless Local Area Network (WLAN) charging".

[13]-[19] Void.

[20] 3GPP TS 32.260: "Telecommunication management; Charging management; IP Multimedia Subsystem (IMS) charging".

[21]-[29] Void.

[30] 3GPP TS 32.270: "Telecommunication management; Charging management; Multimedia Messaging Service (MMS) charging".

[31] 3GPP TS 32.271: "Telecommunication management; Charging management; Location Services (LCS) charging".

[32]-[49] Void.

[51] 3GPP TS 32.298: "Telecommunication management; Charging management; Charging Data Record (CDR) encoding rules description".

[52] 3GPP TS 32.297: "Telecommunication management; Charging management; Charging Data Record (CDR) file format and transfer".

[53] 3GPP TS 32.296: "Telecommunication management; Charging management; Online Charging System (OCS) applications and interfaces".

[54] 3GPP TS 32.295: "Telecommunication management; Charging management; Charging Data Record (CDR) transfer".

[55]-[69] Void.

b) Common 3GPP specifications

[70] 3GPP TS 33.201: "Access domain security".

[71]-[199] Void.

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

[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]-[299] Void.

d) Relevant ITU Recommendations

[300]-[399] Void.

e) Relevant IETF RFCs

[400] IETF RFC 959 (1985): "File Transfer Protocol".

[401] IETF RFC 3588: "Diameter Base Protocol".

[402] IETF Internet-Draft "Diameter Credit Control Application" http://www.ietf.org/internet-drafts/draft-ietf-aaa-diameter-cc-05.txt.

[403] IETF RFC 1350 "TFTP Protocol".

[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-13.txt

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, abbreviations and symbols

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 Abbreviations

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

ACA	ACcounting Answer
ACR	ACcounting Request
AS	Application Server
AVP	Attribute Value Pair
CCA	Credit Control Answer
CCR	Credit Control Request
CDR	Charging Data Record
ECUR	Event Charging with Unit Reservation
IEC	Immediate Event Charging
IMS	IP Multimedia Subsystem
OCS	Online Charging System
SDP	Session Description Protocol

3.3 Symbols

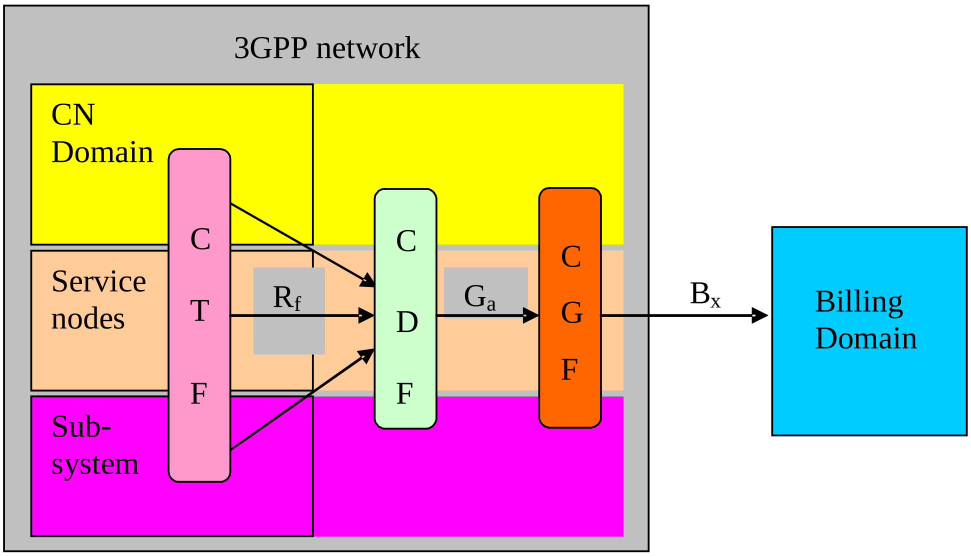
For the purposes of the present document, the following symbols apply:

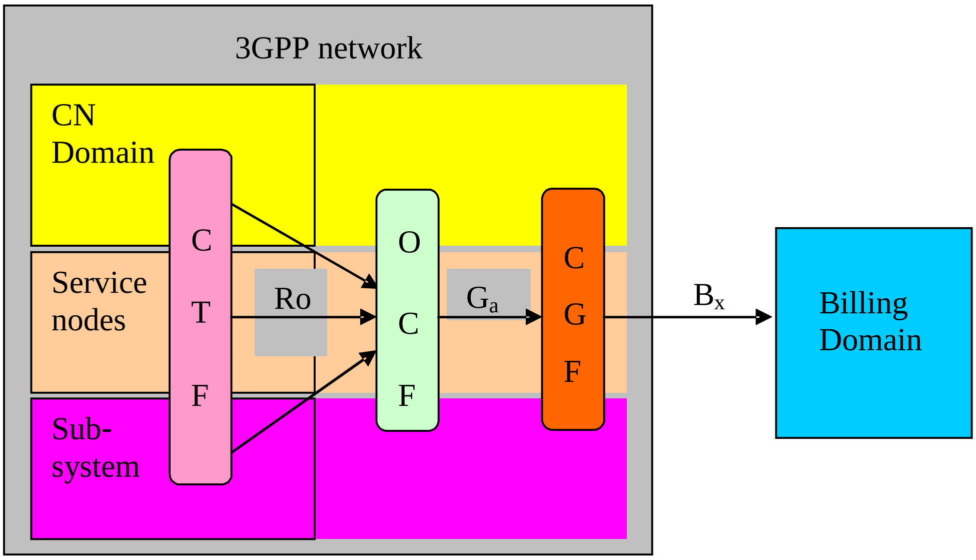
Rf	Offline Charging Reference Point between a 3G network element and the CDF.
Ro	Online Charging Reference Point between a 3G network element and the OCS.
CDF	Charging Data Function
FUI	Final-Unit-Indication
GSU	Granted-Service-Unit
CI	Cost-Information

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 offline charging architecture.





CTF:	**C**harging **T**rigger **F**unction
CDF:	**C**harging **D**ata **F**unction
CGF:	**C**harging **G**ateway **F**unction
BD:	**B**illing **D**omain. This may also be a billing mediation device / post-processing system.

Figure 4.1: Logical ubiquitous offline charging architecture

Editor"s note: Separate the figures.

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

5.1.1 Rf Reference Point

Offline charging for both events and sessions between network element and the CDF is performed using the Rf reference point. The Rf reference point supports integrity protection and authentication for the case that the network element is outside the operator domain.

5.1.2 Offline Charging Requirements

Offline charging between the CCF and each of the network element shall allow for at least the following features:

- Reliable transfer of Charging Information with acknowledgement mechanisms from the Network Element to the CDF.
- Support redundancy mechanisms as described in the Diameter Base Protocol []

5.1.3 Charging Scenarios

5.1.3.1 Event based charging (stage 2)

In the following scenario, network element asks the CCF to store event related charging data.

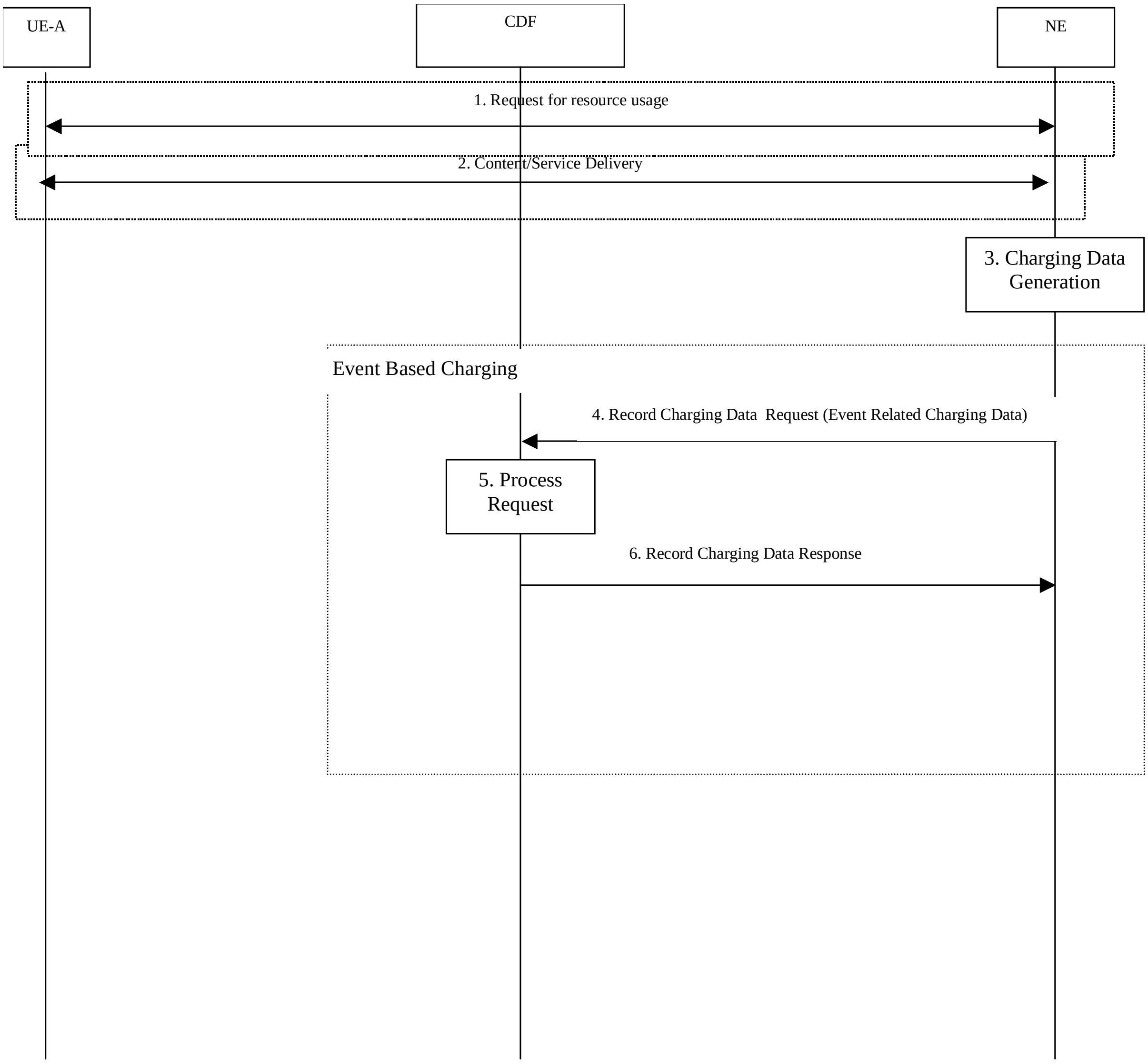

UE-A
CDF
NE
1. Request for resource usage
2. Content/Service Delivery
3. Charging Data Generation
Event Based Charging
4. Record Charging Data Request (Event Related Charging Data)
5. Process Request
6. Record Charging Data Response

Figure 5.1.3.1 : 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 network element generates charging data related to service delivery
4. **Record Charging Data Request:** the network element requests the CCF to store event related charging data for CDR generation purposes.
5. **Process Request:** CCF stores received information. Wheter the CDR is generated or not depends on CDR generation configuration.
6. **Record Charging Data Response:** the CCF informs the network element that charging data was stored.

5.1.3.2 Session based charging (stage 2)

In the following scenario, network element asks the CCF to store session related charging data.

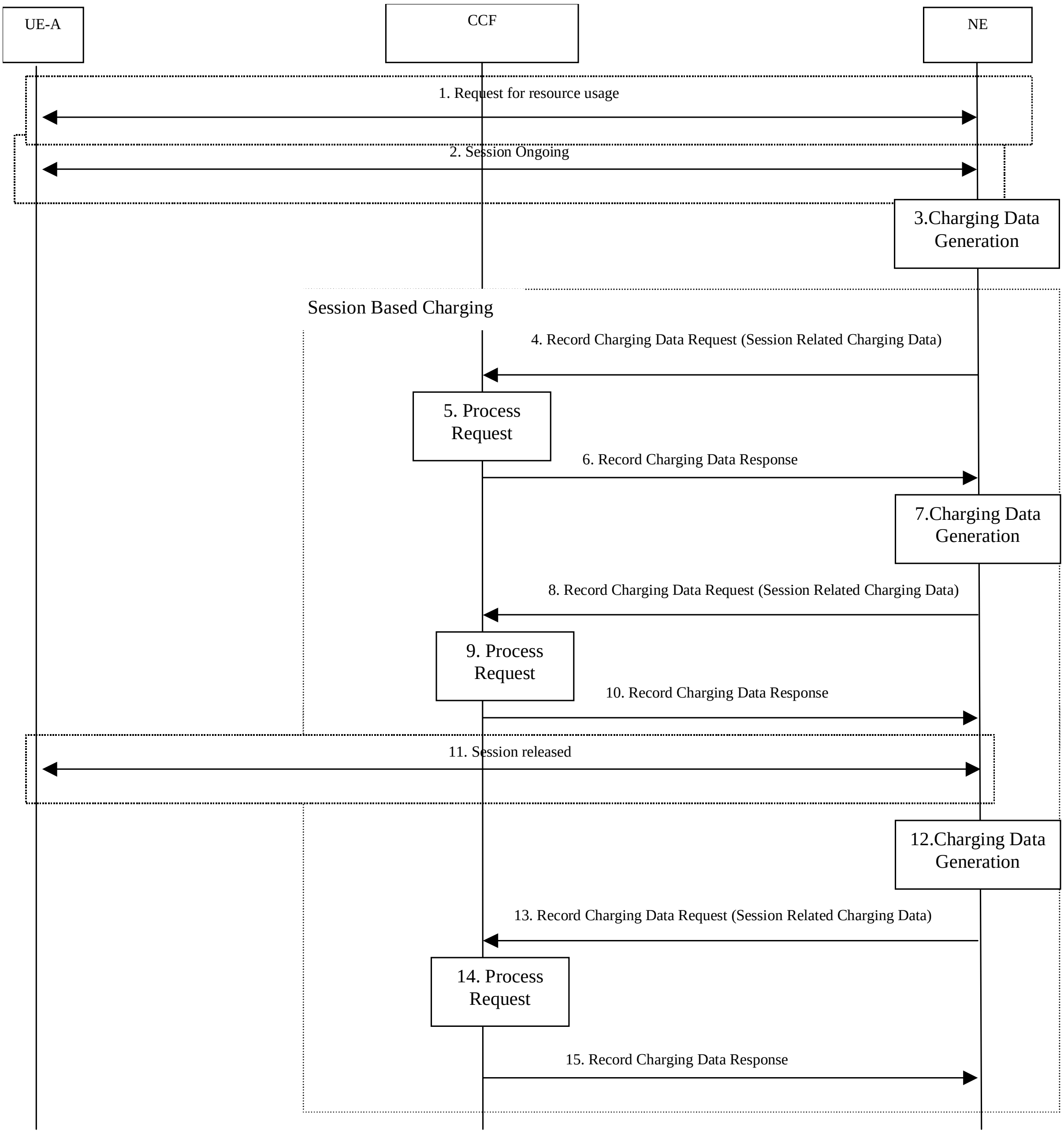

UE-A
CCF
NE
1. Request for resource usage
2. Session Ongoing
3.Charging Data Generation
Session Based Charging
4. Record Charging Data Request (Session Related Charging Data)
5. Process Request
6. Record Charging Data Response
7.Charging Data Generation
8. Record Charging Data Request (Session Related Charging Data)
9. Process Request
10. Record Charging Data Response
11. Session released
12.Charging Data Generation
13. Record Charging Data Request (Session Related Charging Data)
14. Process Request
15. Record Charging Data Response

Figure 5.1.3.2 : 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 network element generates charging data related to session.
4. **Record Charging Data Request:** the network element requests the CCF to store event related charging data for CDR generation purposes.
5. **Process Request:** CCF stores received information. Wheter the CDR is generated or not depends on CDR generation configuration.
6. **Record Charging Data Response:** the CCF informs the network element that charging data was stored
7. **Charging Data Generation:** the network element generates charging data related to session due of e.g. interimedaite timer expiry
8. **Record Charging Data Request:** the network element requests the CCF to store event related charging data for CDR generation purposes.
9. **Process Request:** CCF stores received information. Wheter the CDR is generated or not depends on CDR generation configuration.
10. **Record Charging Data Response:** the CCF informs the network element that charging data was stored

11. **Session release:** the session is released
12. **Charging Data Generation:** the network element generates charging data related to session due of session termination.
13. **Record Charging Data Request:** the network element requests the CCF to store event related charging data for CDR generation purposes.
14. **Process Request:** CCF stores received information. Wheter the CDR is generated or not depends on CDR generation configuration.
15. **Record Charging Data Response:** the CCF informs the network element that charging data was stored

5.2 Online Charging

5.2.1 Ro Reference Point

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

5.2.2 Basic principles of online charging

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 network element.

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 network element.

- With the Decentralized Unit Determination approach, the network element 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 network element. The network element is then responsible for the supervision of service delivery. Particularly, the network element 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 network element 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 network element. Consequently, network element 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.

5.2.3 Basic Operations and Scenarios

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

- "Debit Units Request"; sent from network element → OCF
  After receiving a service request from the subscriber, the network element sends a Debit Units Request to the OCF. The network element may either specify a service identifier (centralised unit determination) or the number of units requested (decentralised unit determination).

- "Debit Units Response"; sent from OCF → network element
  The OCF replies with a Debit Units Response, which informs the network element 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 in case of charging with reservation:

- "Reserve Units Request"; sent from network element → OCF
  Request to reserve a number of units for the service to be provided by an network element. In case of centralised unit determination, the network element 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 network element.

- "Reserve Units Response"; sent from OCF → network element
  Response from the OCF which informs the network element 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 network element to modify the current reservation, including the return of previously reserved units.

5.2.4 Charging Scenarios

In order to perform event charging via Ro, the scenarios between the involved entities UE-A, OCF and network element 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 – FFS

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

5.2.4.1 Immediate Event Charging

5.2.4.1.1 Decentralized Unit Determination and Centralized Rating

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

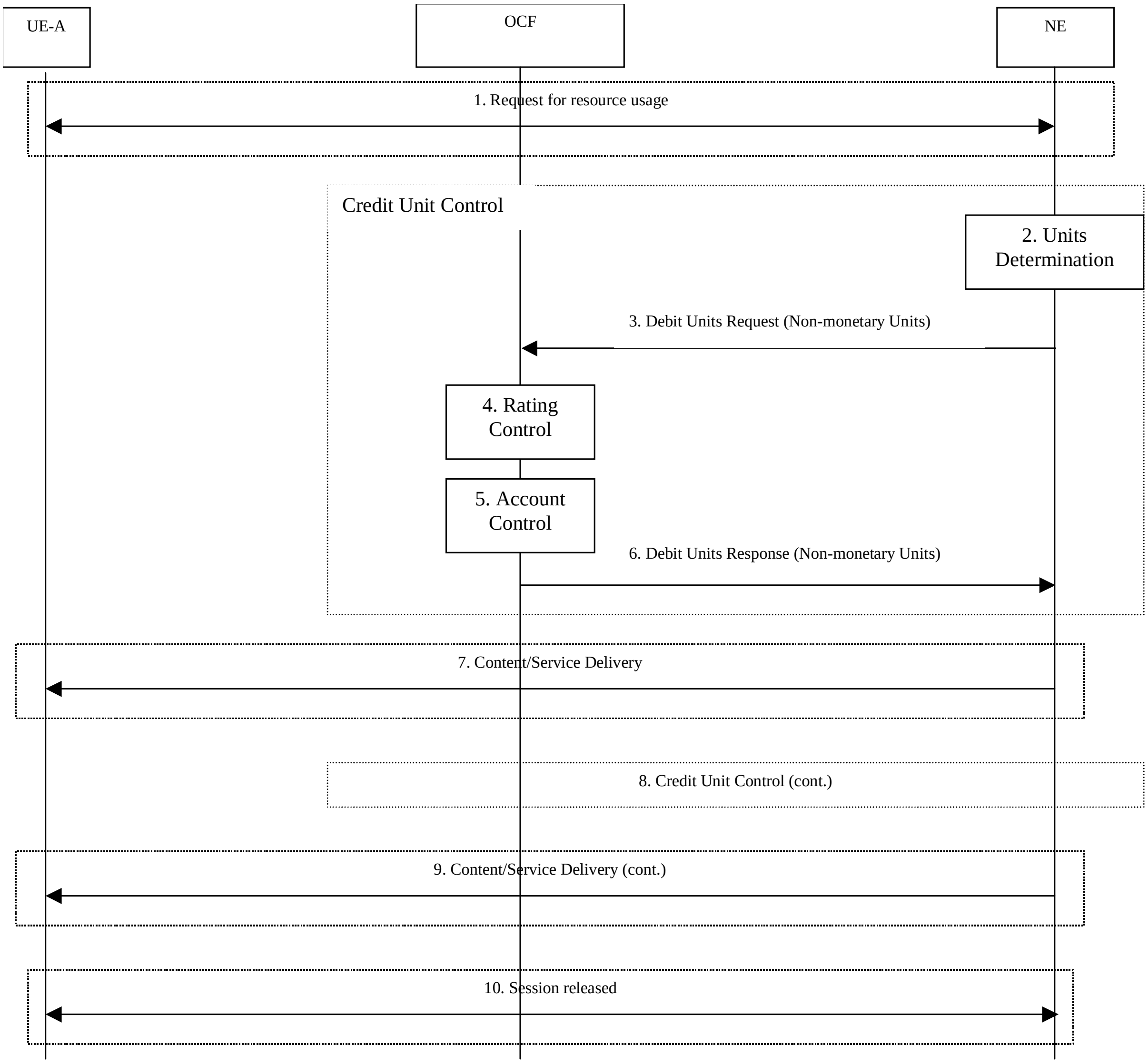

UE-A
OCF
NE
1. Request for resource usage
Credit Unit Control
2. Units Determination
3. Debit Units Request (Non-monetary Units)
4. Rating Control
5. Account Control
6. Debit Units Response (Non-monetary Units)
7. Content/Service Delivery
8. Credit Unit Control (cont.)
9. Content/Service Delivery (cont.)
10. Session released

Figure 5.2.4.1.1 : 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 network element determines the number of units accordingly.
3. **Debit Units Request:** the network element 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 network element of the number of granted units.
7. **Content/Service Delivery:** the network element 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.

5.2.4.1.2 Centralized Unit Determination and Centralized Rating

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

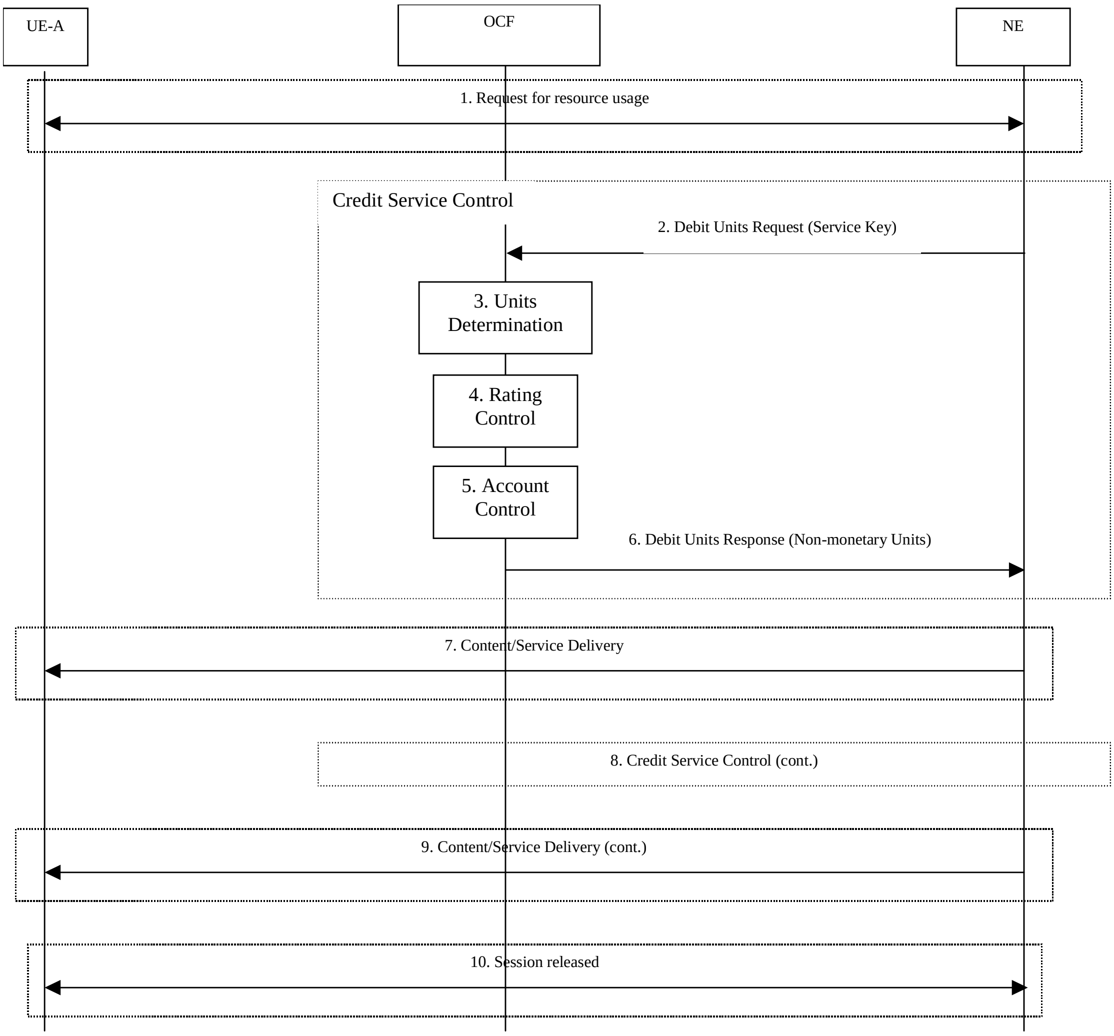

UE-A
OCF
NE
1. Request for resource usage
Credit Service Control
2. Debit Units Request (Service Key)
3. Units Determination
4. Rating Control
5. Account Control
6. Debit Units Response (Non-monetary Units)
7. Content/Service Delivery
8. Credit Service Control (cont.)
9. Content/Service Delivery (cont.)
10. Session released

Figure 5.2.4.1.2 : 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 network element 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 network element 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 network element 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.

5.2.4.1.3 Decentralized Unit Determination and Decentralized Rating

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

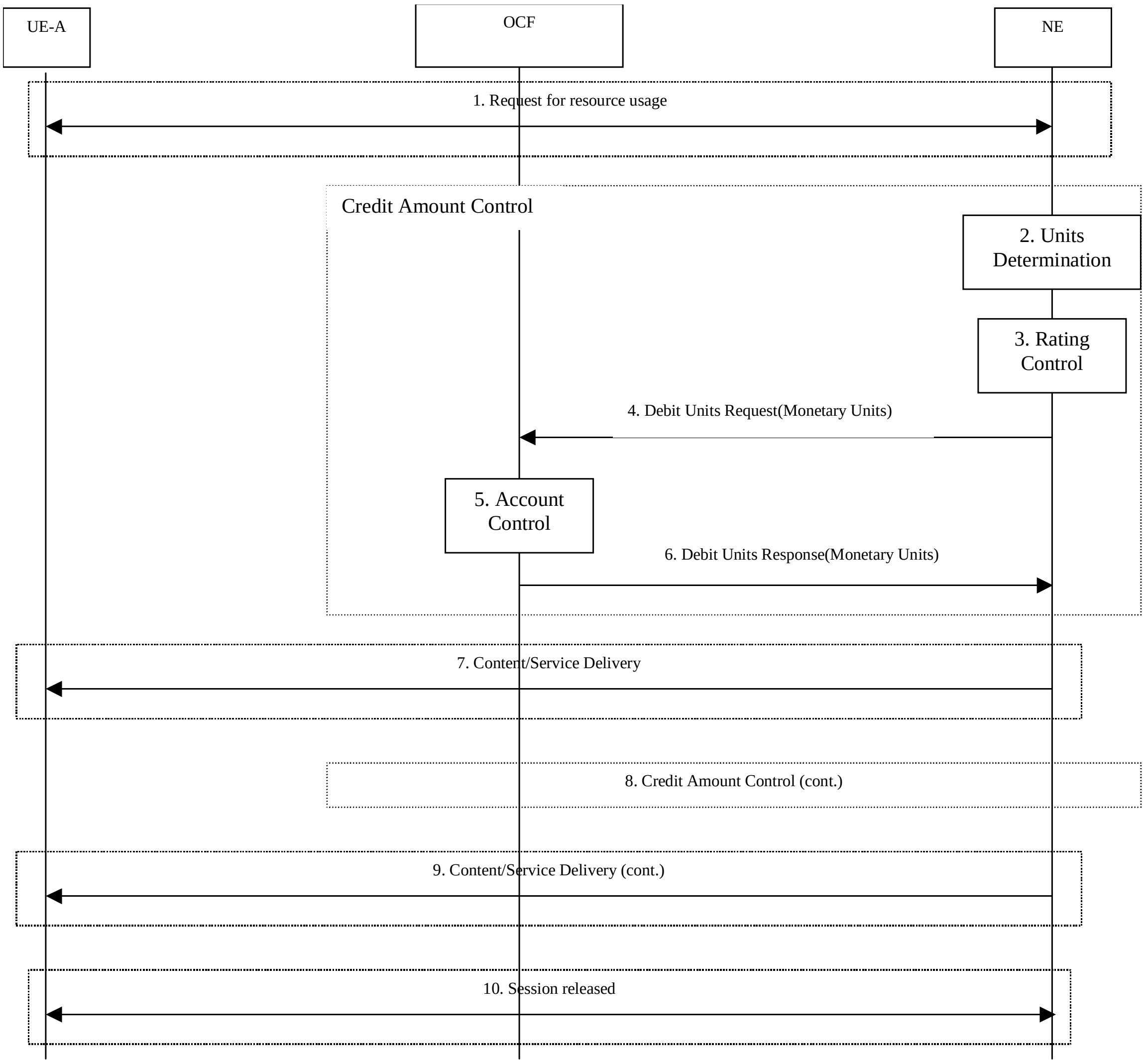

UE-A
OCF
NE
1. Request for resource usage
Credit Amount Control
2. Units Determination
3. Rating Control
4. Debit Units Request(Monetary Units)
5. Account Control
6. Debit Units Response(Monetary Units)
7. Content/Service Delivery
8. Credit Amount Control (cont.)
9. Content/Service Delivery (cont.)
10. Session released

Figure 5.2.4.1.3 : 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 network element determines the number of units accordingly.
3. **Rating Control:** the network element calculates the number of monetary units that represent the price for the number of units determined in item 2.
4. **Debit Units Request:** the network element 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 network element the number of deducted monetary units.
7. **Content/Service Delivery:** the network element 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.

5.2.4.1.4 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.

5.2.4.2 Event charging with Reservation

5.2.4.2.1 Decentralized Unit Determination and Centralized Rating

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

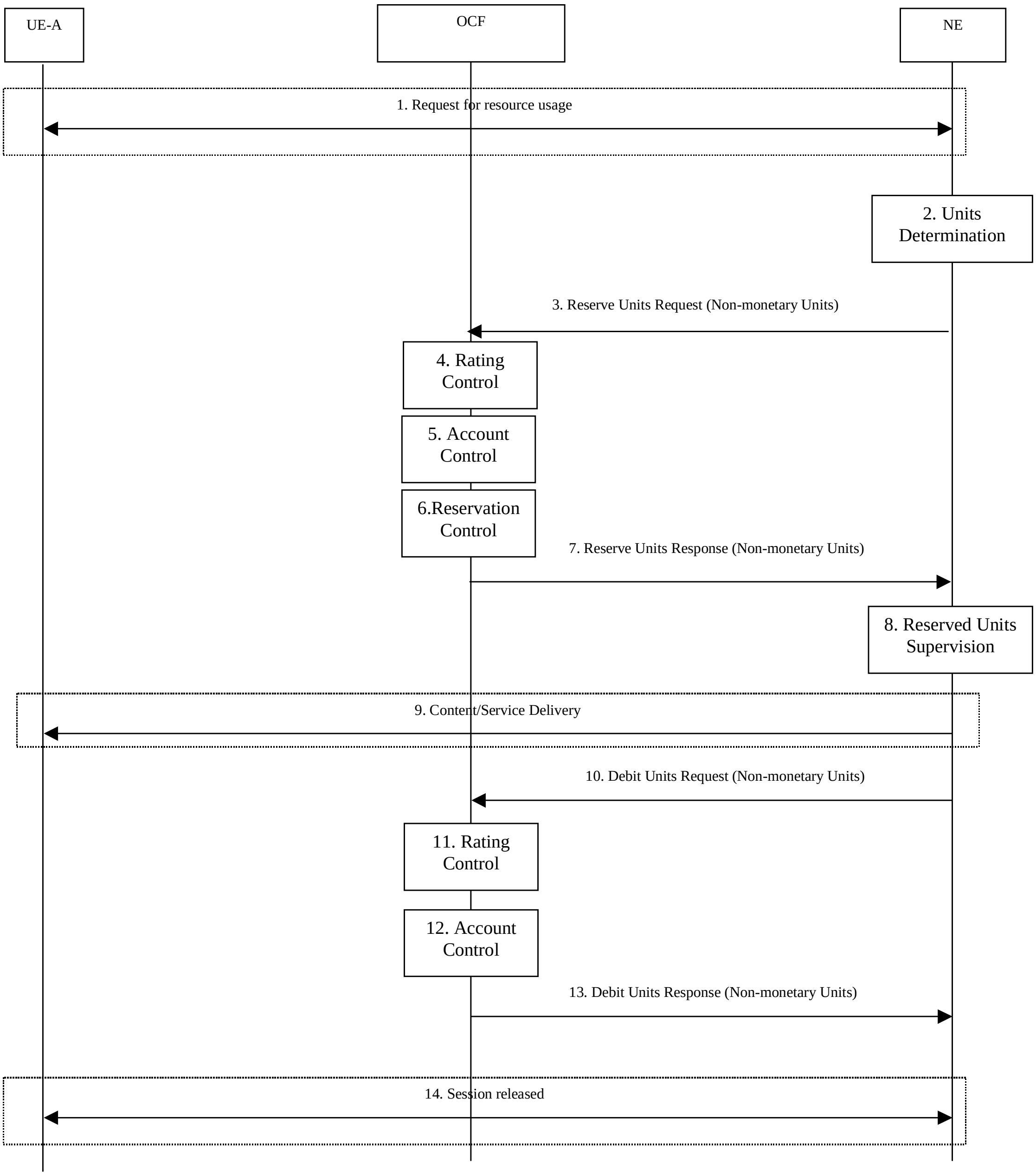

UE-A
OCF
NE
1. Request for resource usage
2. Units Determination
3. Reserve Units Request (Non-monetary Units)
4. Rating Control
5. Account Control
6.Reservation Control
7. Reserve Units Response (Non-monetary Units)
8. Reserved Units Supervision
9. Content/Service Delivery
10. Debit Units Request (Non-monetary Units)
11. Rating Control
12. Account Control
13. Debit Units Response (Non-monetary Units)
14. Session released

Figure 5.2.4.2.1 : 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 network element determines the number of units accordingly.

3. **Reserve Units Request:** the network element 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 network element 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 network element monitors the consumption of the reserved units.
9. **Content/Service Delivery:** the network element 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 network element 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 network element of the actually deducted units. Items 10 to 13 may be repeated several times.
14. **Session Release:** the session is released.

5.2.4.2.2 Centralized Unit Determination and Centralized Rating

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

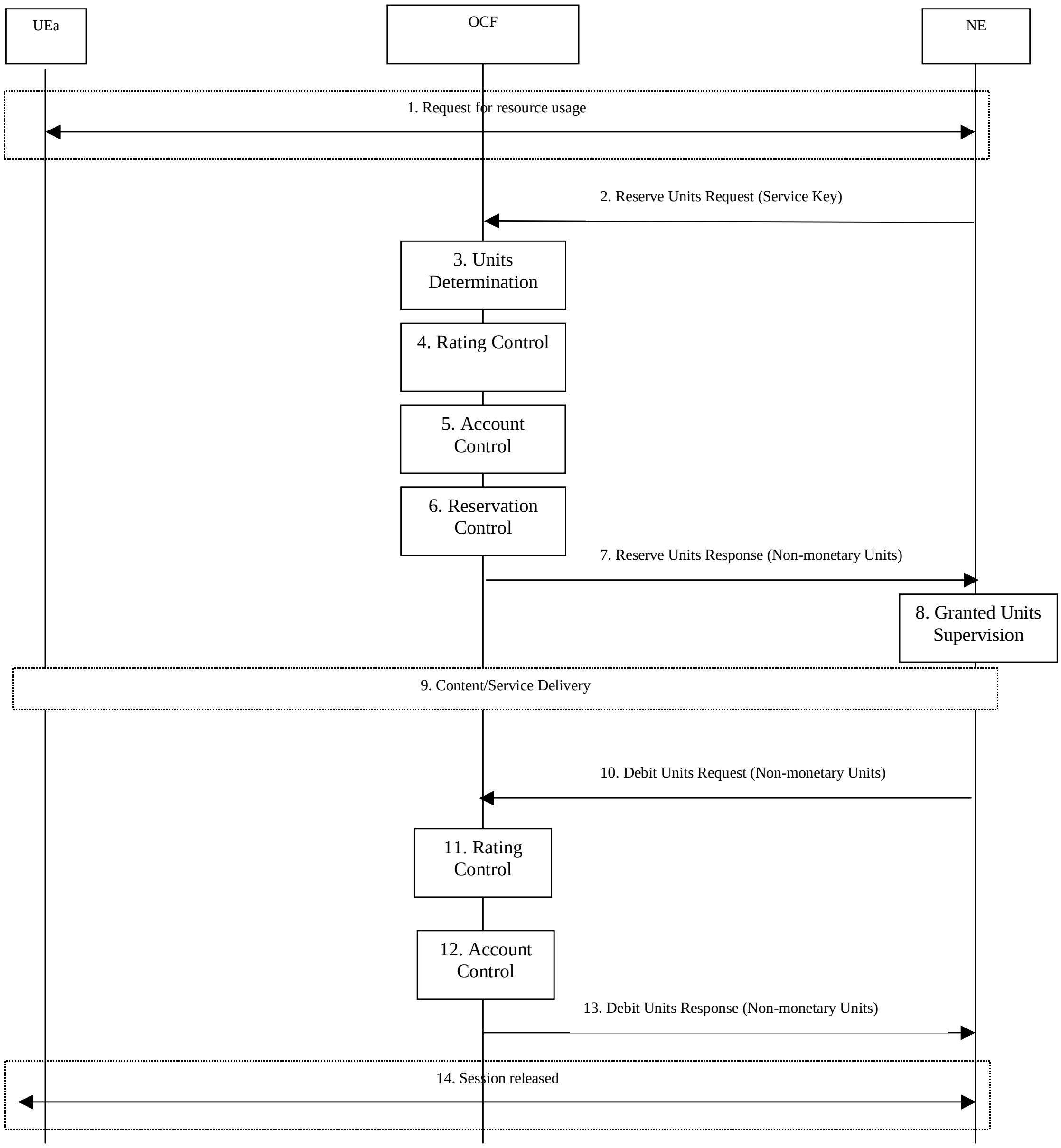

UEa
OCF
NE
1. Request for resource usage
2. Reserve Units Request (Service Key)
3. Units Determination
4. Rating Control
5. Account Control
6. Reservation Control
7. Reserve Units Response (Non-monetary Units)
8. Granted Units Supervision
9. Content/Service Delivery
10. Debit Units Request (Non-monetary Units)
11. Rating Control
12. Account Control
13. Debit Units Response (Non-monetary Units)
14. Session released

Figure 5.2.4.2.2 : Event Charging with Reservation / Centralized Unit Determination and Centralized Rating

1. **Request for resource usage:** The UE-A requests the desired content from the network element.
2. **Reserve Units Request:** depending on the service requested by the UE-A, the network element 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 network element 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 network element monitors the consumption of the reserved units.
9. **Content/Service Delivery:** the network element 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 network element 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 network element of the actually deducted units. Items 10 to 13 may be repeated several times.
14. **Session Released:** the session is released.

5.2.4.2.3 Decentralized Unit Determination and Decentralized Rating

In the following scenario, the network element 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.

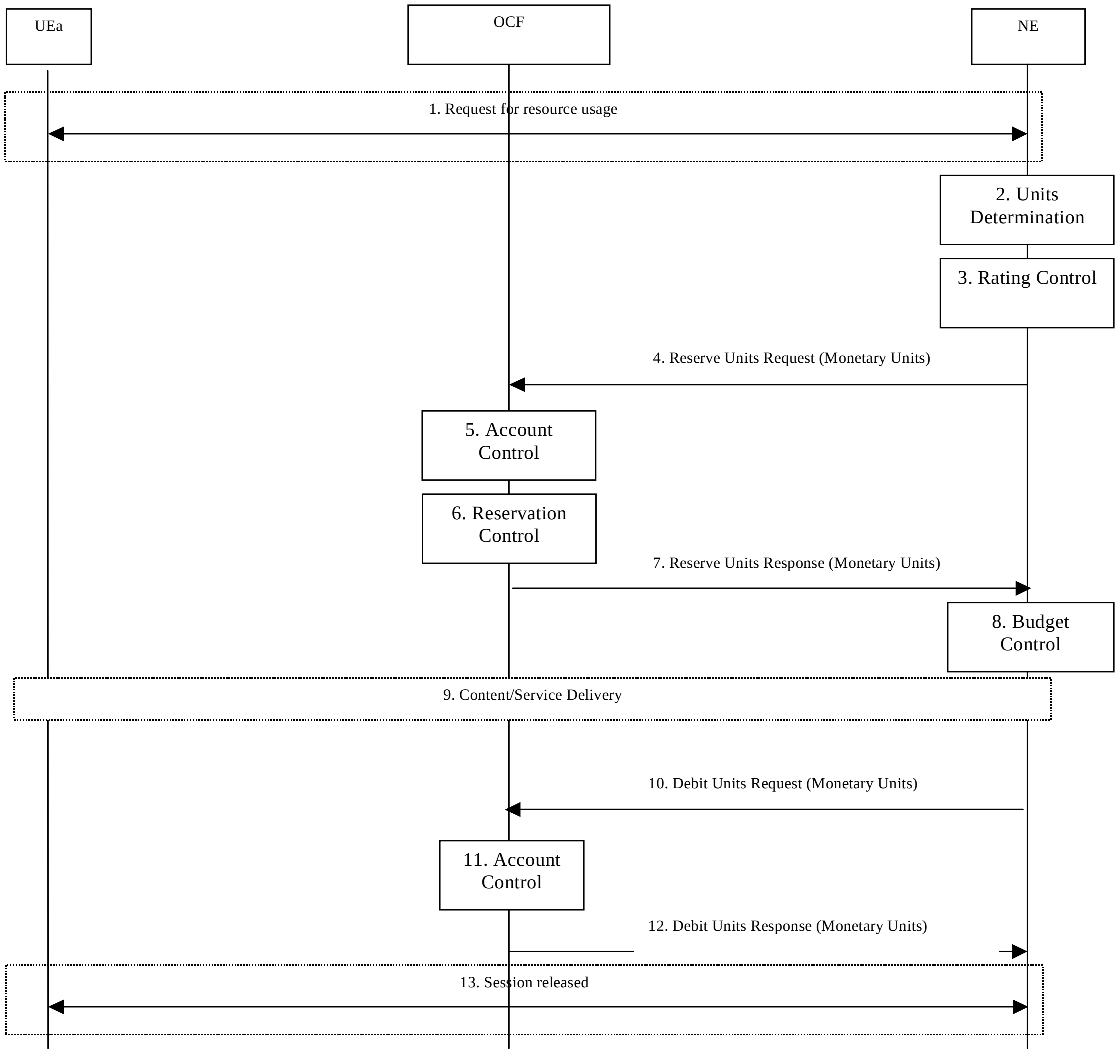

UEa
OCF
NE
1. Request for resource usage
2. Units Determination
3. Rating Control
4. Reserve Units Request (Monetary Units)
5. Account Control
6. Reservation Control
7. Reserve Units Response (Monetary Units)
8. Budget Control
9. Content/Service Delivery
10. Debit Units Request (Monetary Units)
11. Account Control
12. Debit Units Response (Monetary Units)
13. Session released

Figure 5.2.4.2.3 : Event Charging with Reservation / Centralized Unit Determination and Centralized Rating

1. **Request for resource usage:** The UE-A requests the desired content from the network element.
2. **Units Determination:** depending on the service requested by the UE-A, the network element determines the number of units accordingly.
3. **Rating Control:** the network element calculates the number of monetary units that represent the price for the number of units determined in item 2.

4. **Reserve Units Request:** the network element 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 network element 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 network element monitors the consumption of the granted amount.
9. **Content/Service Delivery:** the network element delivers the content/service at once, in fractions or in individually chargeable items, corresponding to the number of units.
10. **Debit Units Request:** the network element 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 network element 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.

5.2.4.3 Session charging with Reservation

5.2.4.3.1 Decentralized Unit Determination and Centralized Rating

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

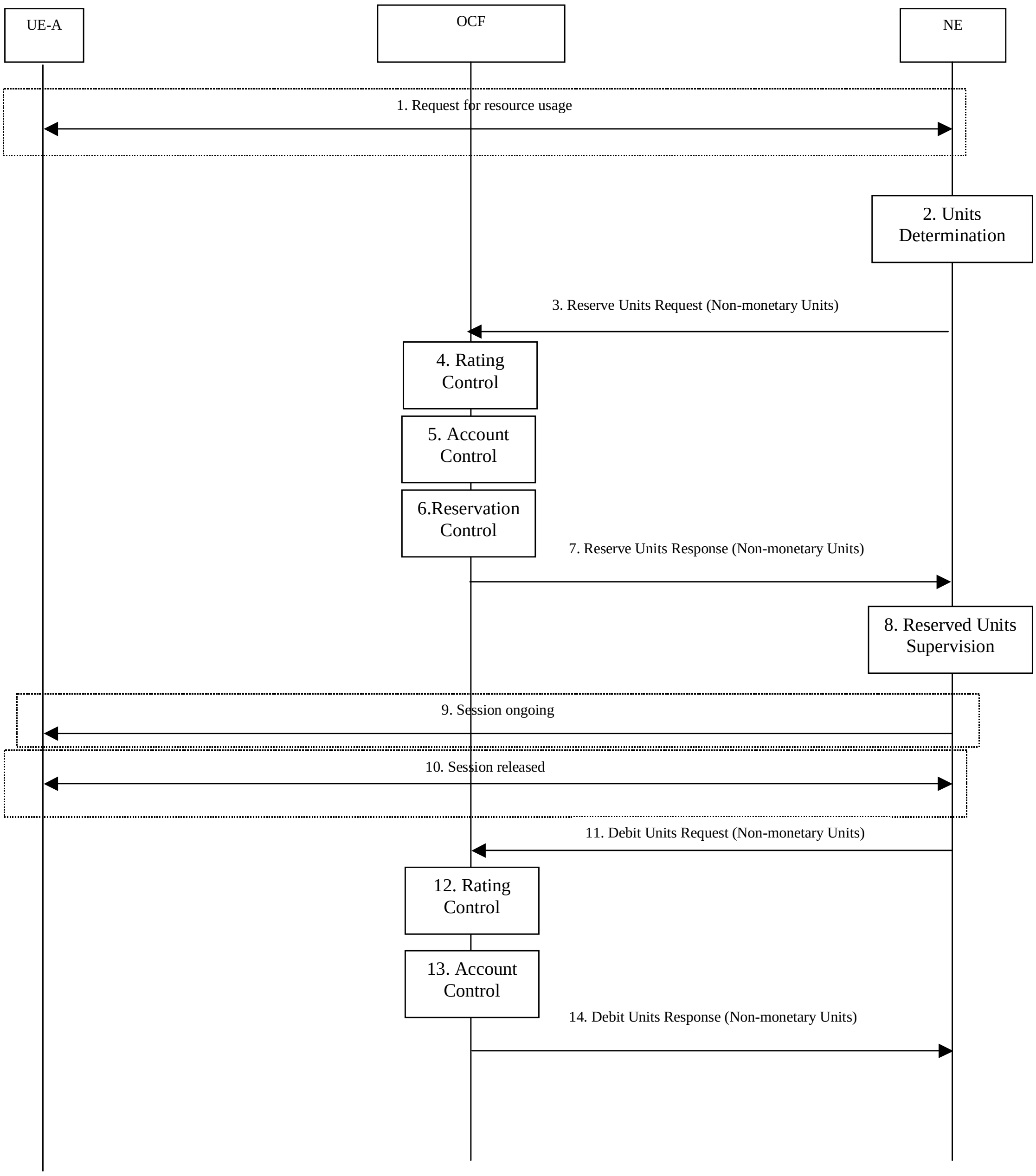

UE-A
OCF
NE
1. Request for resource usage
2. Units Determination
3. Reserve Units Request (Non-monetary Units)
4. Rating Control
5. Account Control
6.Reservation Control
7. Reserve Units Response (Non-monetary Units)
8. Reserved Units Supervision
9. Session ongoing
10. Session released
11. Debit Units Request (Non-monetary Units)
12. Rating Control
13. Account Control
14. Debit Units Response (Non-monetary Units)

Figure 5.2.4.3.1 : Session Charging with Reservation / Decentralized Unit Determination and Centralized Rating

1. **Request for resource usage**The UE-A requests session establishment from the NE.
2. **Units Determination:** depending on the requested type of the session the network element determines the number of units accordingly.
3. **Reserve Units Request:** the network element 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 network element of the reserved number of units.
8. **Reserved Units Supervision:** simultaneously with the ongoing session, the network element monitors the consumption of the reserved units.
9. **Session ongoing:** the network element maintains the session, corresponding to the reserved number of units.
10. **Session Release:** the session is released

11. **Debit Units Request:** the network element 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 network element of the actually deducted units.

5.2.4.3.2 Centralized Unit Determination and Centralized Rating

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

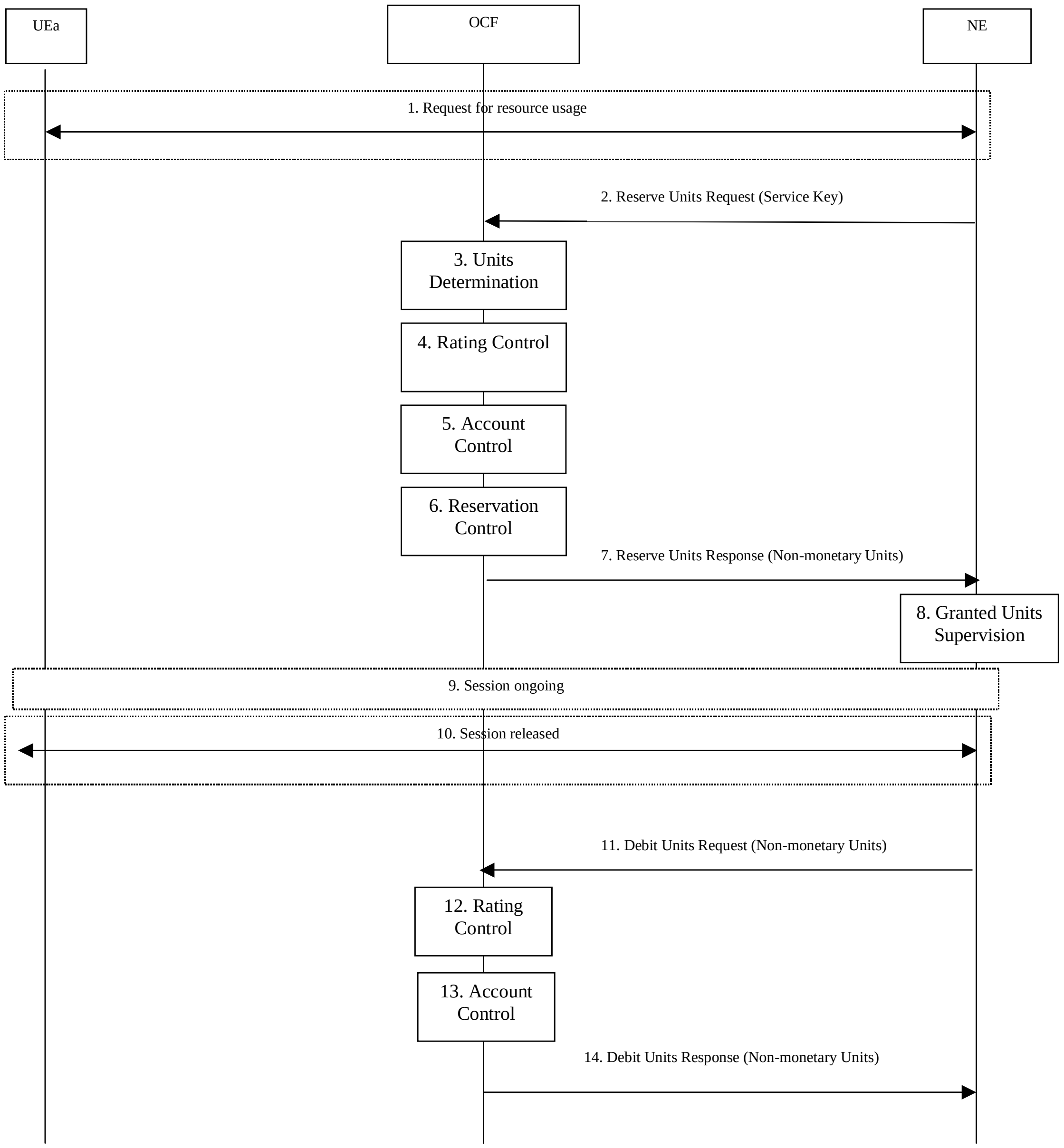

UEa
OCF
NE
1. Request for resource usage
2. Reserve Units Request (Service Key)
3. Units Determination
4. Rating Control
5. Account Control
6. Reservation Control
7. Reserve Units Response (Non-monetary Units)
8. Granted Units Supervision
9. Session ongoing
10. Session released
11. Debit Units Request (Non-monetary Units)
12. Rating Control
13. Account Control
14. Debit Units Response (Non-monetary Units)

Figure 5.2.4.3.2 : Session Charging with Reservation / Centralized Unit Determination and Centralized Rating

1. **Request for resource usage:** The UE-A requests the session establishment from the network element.
2. **Reserve Units Request:** depending on the requested type of the session by the UE-A, the network element 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 network element 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 network element monitors the consumption of the reserved units.
9. **Content/Service Delivery:** the network element maintains the session corresponding to the reserved number of units.
10. **Session ongoing:** the network element 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.
11. **Session Released:** the session is released.
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 network element of the actually deducted units.

5.2.4.3.3 Decentralized Unit Determination and Decentralized Rating

In the following scenario, the network element 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.

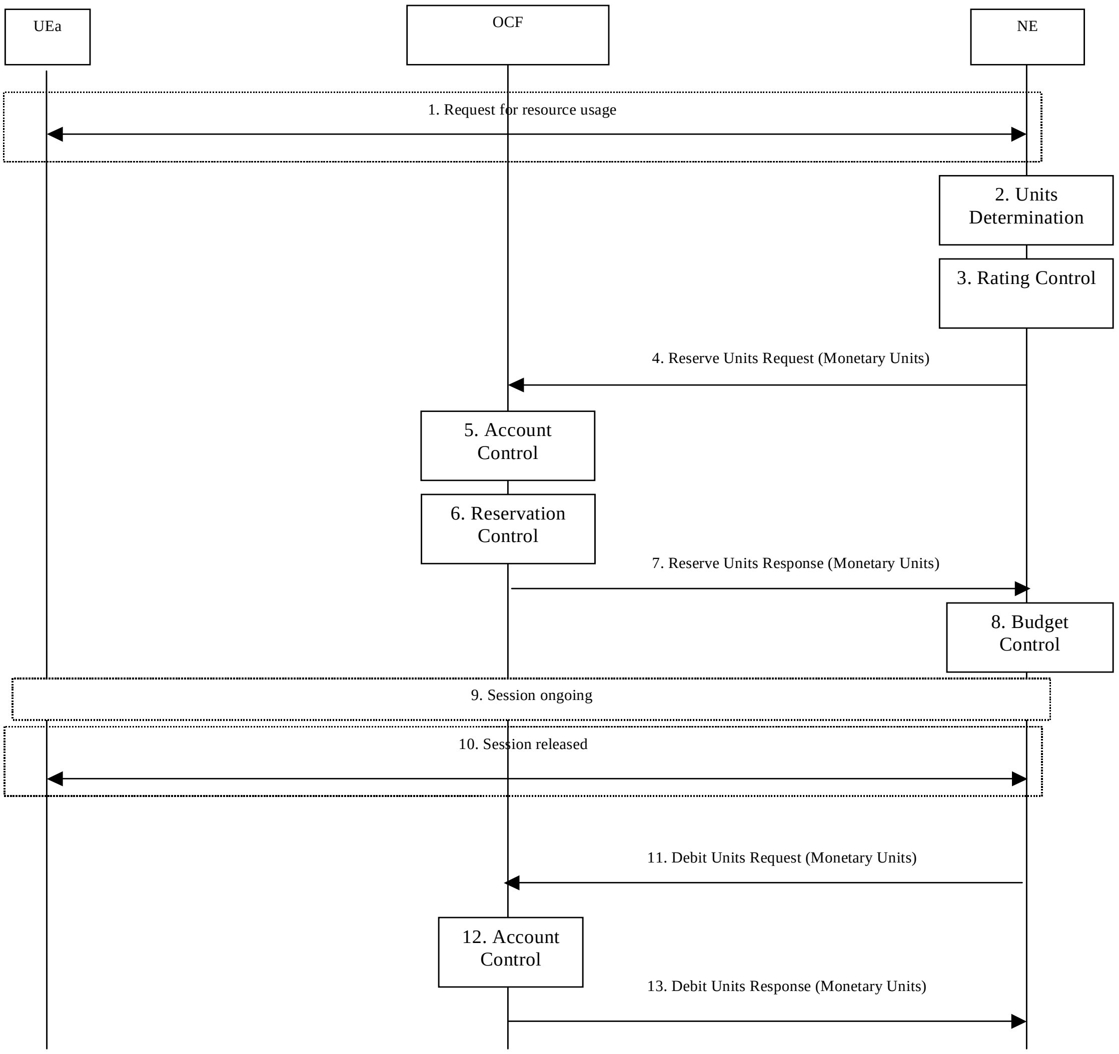

UEa
OCF
NE
1. Request for resource usage
2. Units Determination
3. Rating Control
4. Reserve Units Request (Monetary Units)
5. Account Control
6. Reservation Control
7. Reserve Units Response (Monetary Units)
8. Budget Control
9. Session ongoing
10. Session released
11. Debit Units Request (Monetary Units)
12. Account Control
13. Debit Units Response (Monetary Units)

Figure 5.2.4.3.3 : Session Charging with Reservation / Centralized Unit Determination and Centralized Rating

1. **Request for resource usage:** The UE-A requests the session establishment from the network element.
2. **Units Determination:** depending on the requested type of the session by the UE-A, the network element determines the number of units accordingly.
3. **Rating Control:** the network element calculates the number of monetary units that represent the price for the number of units determined in item 2.
4. **Reserve Units Request:** the network element 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 network element of the reserved number of monetary units.
8. **Budget Control:** simultaneously with the ongoing session, the network element monitors the consumption of the granted amount.
9. **Session ongoing:** the network element maintains the session corresponding to the number of units.
10. **Session Released:** the session is released.

11. Debit Units Request: the network element 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 network element the number of deducted monetary units.

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

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-authorisation 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 trigger, the client shall reports 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.

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..

Editor"s note: Create a relation between the CTF & the Diameter client, and, the CDF and the Diameter Server.

The charging architecture implementing Diameter adheres to the structure where all communications for offline charging purposes between the CTF and the CDF are carried out on the Diameter Rf interface, 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 interfaces 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 client 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.

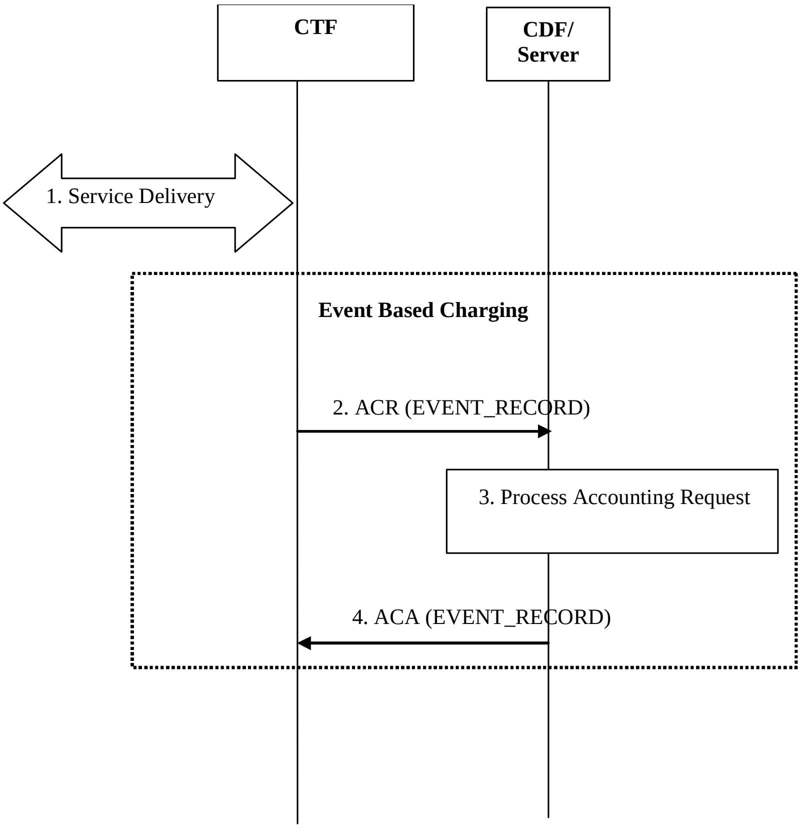


Figure 6.1.1 : Event Based offline charging

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.

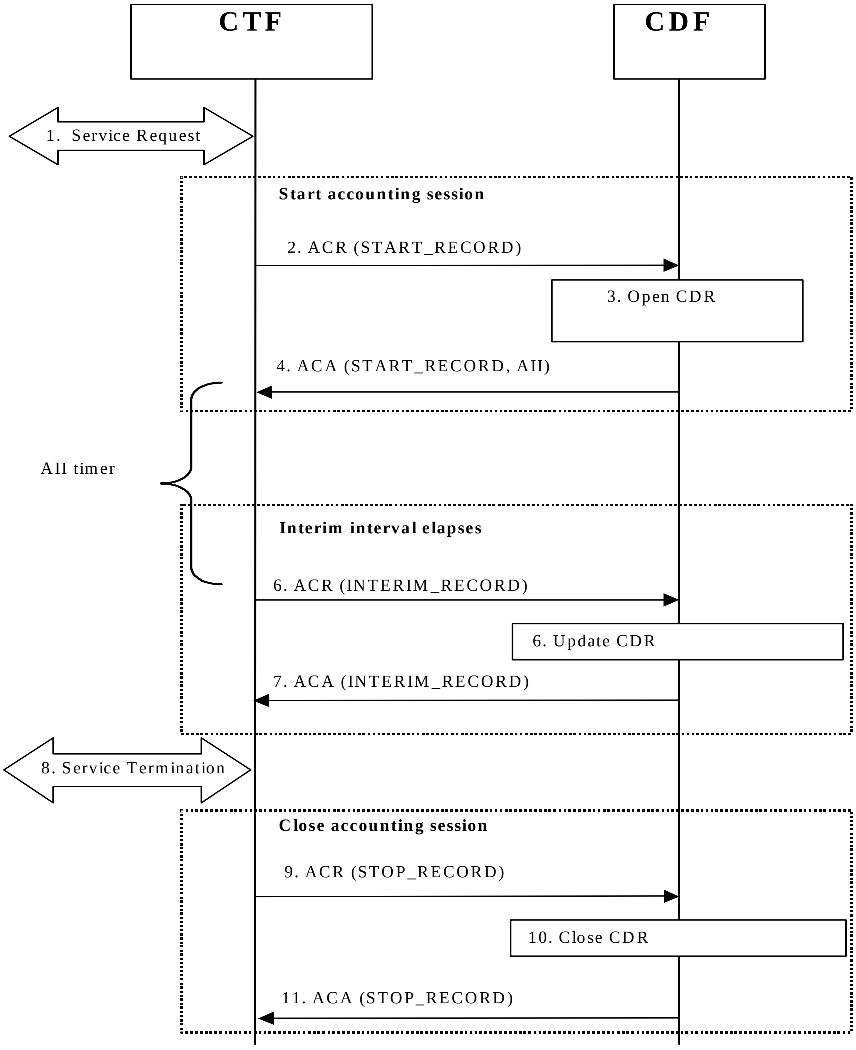


Figure 6.1.2 : Session based offline charging

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 AII elapse the network element 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 Accounting-Request Message

The following table illustrates the basic structure of a Diameter *Accounting-Request* message as used for offline charging.

Table 6.2.1 : Accounting-Request (ACR) Message Contents for Offline Charging

Diameter base protocol AVPs	
AVP	**Used in offline ACR**
<Diameter-Header:271,REQ,PXY>	Yes
<Session-Id> -- Diameter Session Id	Yes
{Origin-Host}	Yes
{Origin-Realm}	Yes
{Destination-Realm}	Yes
{Accounting-Record-Type}	Yes
{Accounting-Record-Number}	Yes
[Acct-Application-Id]	No
[Vendor-Specific-Application-Id]	Yes
[Vendor-Id]	Yes
{ Auth-Application-Id }	Yes
{ Acct-Application-Id }	Yes
[User-Name]	Yes
[Accounting-Sub-Session-Id]	No
[Accounting-RADIUS-Session-Id]	No
[Acct-Multi-Session-Id]	No
[Acct-Interim-Interval]	Yes
[Accounting-Realtime-Required]	No
[Origin-State-Id]	Yes
[Event-Timestamp]	Yes
*[Proxy-Info]	Yes
{ Proxy-Host }	Yes
{ Proxy-State }	Yes
*[Route-Record]	No
*[AVP]	No
3GPP Diameter accounting AVPs	
[Event-Type]	Yes
[Role-of-node]	Yes
[User-Session-ID]	Yes
[Calling-Party-Address]	Yes
[Called-Party-Address]	Yes
[Time-stamps]	Yes
*[Application-Server]	Only for IMS (S-CSCF)
Application Servers Involved	Only for IMS (S-CSCF)
*Application Provided Called Parties	Only for IMS (S-CSCF)
*[Application-provided-Called-Party-Address]	Only for IMS (S-CSCF)
*[Inter-Operator-Identifier]	Yes
originating IOI	Yes
terminating IOI	Yes
[IMS-Charging-Identifier]	Yes
*[SDP-Session-Description]	Yes
*[SDP-Media-Component]	Yes
SIP Request Timestamp	Yes
SIP Response Timestamp	Yes
SDP Media Components	Yes
SDP Media Name	Yes
SDP Media Description	Yes
GPRS Charging ID	Yes
Media Initiator Flag	Yes
Authorised QoS	Yes
[GGSN-Address]	Yes
[Served-Party-IP-Address]	Only for IMS (P-CSCF)
[Authorized-QoS]	Only for IMS (P-CSCF)
[Server-Capabilities]	Only for IMS (I-CSCF)
[Trunk-Group-ID]	Only for IMS (MGCF)
[Bearer-Service]	Only for IMS (MGCF)
[Service-ID]	Only for IMS (MRFC)
[UUS-Data]	Yes
Content-Type	Yes
Content-Disposition	Yes

Content-Length	Yes
Originator	Yes
[Cause]	Yes
[PS-Furnish-Charging-Information]	Yes
{GPRS-Charging-Id}	Yes
{PS-Free-Format-Data}	Yes
[PS-Append-Free-Format-Data]	Yes

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

Editor"s note: The Application Provided Called Party issue needs to be reviewed & corrected if needed.

6.2.2 Accounting-Answer Message

The following table illustrates the basic structure of a Diameter *Accounting-Answer* message as used for offline charging. This message is always used by the CDF as specified below, regardless of the network element it is received from and the ACR record type that is being replied to.

NOTE: Other AVPs would be added. Only generic AVPs should be here, so IMS specific AVPs should be removed.

Table 6.2.2 : Accounting-Answer (ACA) Message Contents for Offline Charging

Diameter base protocol AVPs	
AVP	**Used in Offline ACA**
<Diameter-Header:271,PXY>	Yes
<Session-Id>	Yes
{Result-Code}	Yes
{Origin-Host}	Yes
{Origin-Realm}	Yes
{Accounting-Record-Type}	Yes
{Accounting-Record-Number}	Yes
[Acct-Application-Id]	No
[Vendor-Specific-Application-Id]	Yes
[Vendor-Id]	Yes
{ Auth-Application-Id }	Yes
{ Acct-Application-Id }	Yes
[User-Name]	Yes
[Accounting-Sub-Session-Id]	No
[Accounting-RADIUS-Session-Id]	No
[Acct-Multi-Session-Id]	No
[Error-Reporting-Host]	No
[Acct-Interim-Interval]	Yes
[Accounting-Realtime-Required]	No
[Origin-State-Id]	Yes
[Event-Timestamp]	Yes
*[Proxy-Info]	No
{ Proxy-Host }	No
{ Proxy-State }	No
*[AVP]	No

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.

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 Diameter Base Protocol [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 Diameter Base Protocol [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 Interface

6.3.2.1 Basic Principles

For online charging the Diameter Credit Control Application defined in [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.

NOTE: To the extent possible alignment with the IETF Diameter Credit Control Application, [402], is planned. However, this can only be accomplished when the current IETF draft receives an official RFC status.

Editor"s note: Incorporate the framework from 32.200 for ECUR and IEC to this document.

Editor"s note: Include 3 scenarios. Distinguish between Event & Session.

6.3.3 Immediate Event Charging (IEC)

The following figure shows the transactions that are required on the Ro interface 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.

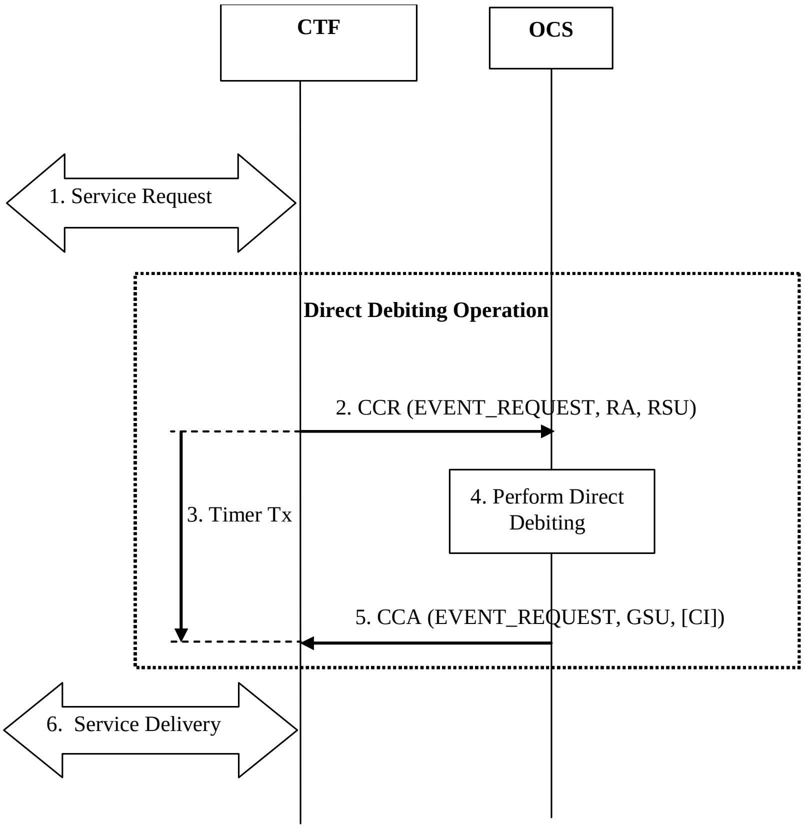

CTF
OCS
1. Service Request
Direct Debiting Operation
2. CCR (EVENT_REQUEST, RA, RSU)
3. Timer Tx
4. Perform Direct Debiting
5. CCA (EVENT_REQUEST, GSU, [CI])
6. Service Delivery

Figure 6.3.3 : IEC Direct Debiting Operation

Step 1. The network element receives a service request.
The Direct Debiting Operation is performed as described in DCCA [402].

Step 2. 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' [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 [402].

6.3.4 Event Charging with Unit Reservation (ECUR)

The following figure shows the transactions that are required on the Ro interface in order to perform the SBCC or the session based reserve and debit units operation. Multiple replications of both of these operations are possible.

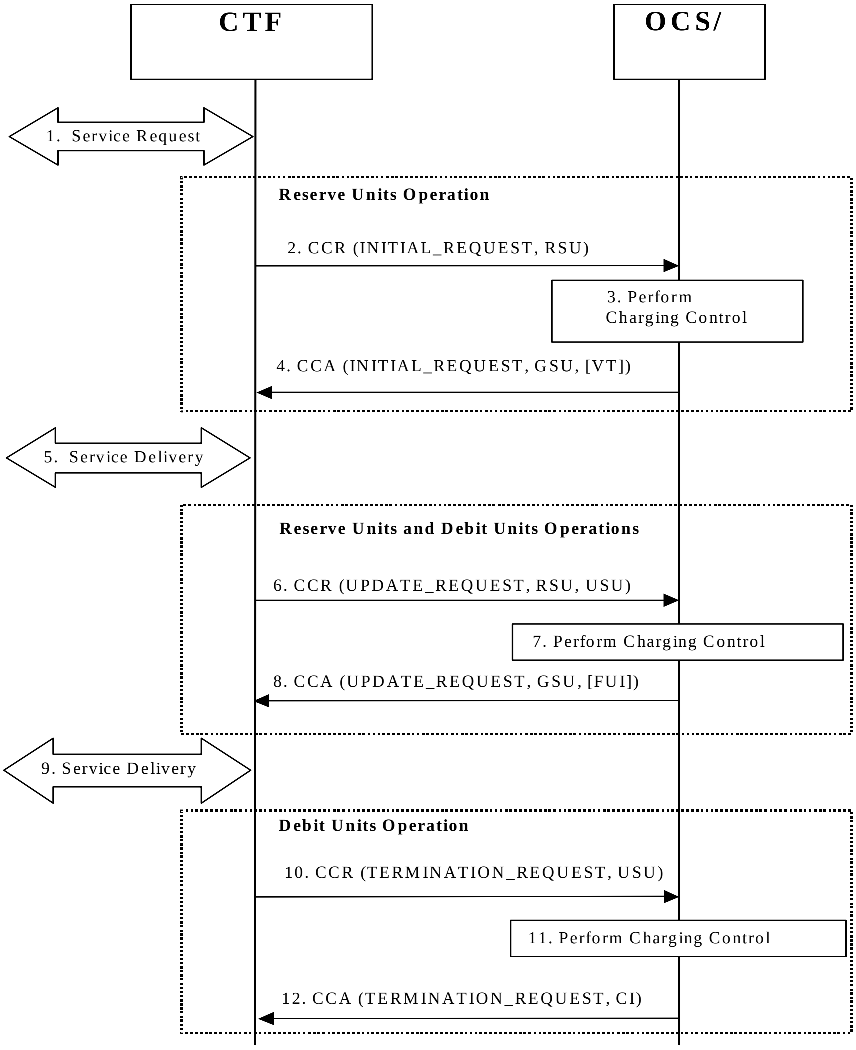

CTF
OCS/
1. Service Request
Reserve Units Operation
2. CCR (INITIAL_REQUEST, RSU)
3. Perform Charging Control
4. CCA (INITIAL_REQUEST, GSU, [VT])
5. Service Delivery
Reserve Units and Debit Units Operations
6. CCR (UPDATE_REQUEST, RSU, USU)
7. Perform Charging Control
8. CCA (UPDATE_REQUEST, GSU, [FUI])
9. Service Delivery
Debit Units Operation
10. CCR (TERMINATION_REQUEST, USU)
11. Perform Charging Control
12. CCA (TERMINATION_REQUEST, CI)

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. During content/service 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. Content/service delivery continues and the reserved units are concurrently controlled.

Step 10. When content/service delivery is completed or the final granted units have been consumed, the network element sends CCR with *CC-Request-Type* AVP set to INTERIM_REQUEST to terminate the active credit control session and report the used units.

Step 11. The OCS deducts the amount used from the account. Unused reserved units are released, if applicable.

Step 12. 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)

The follwing figure shows the transactions that are required on the Ro interface in order to perform the SCUR.

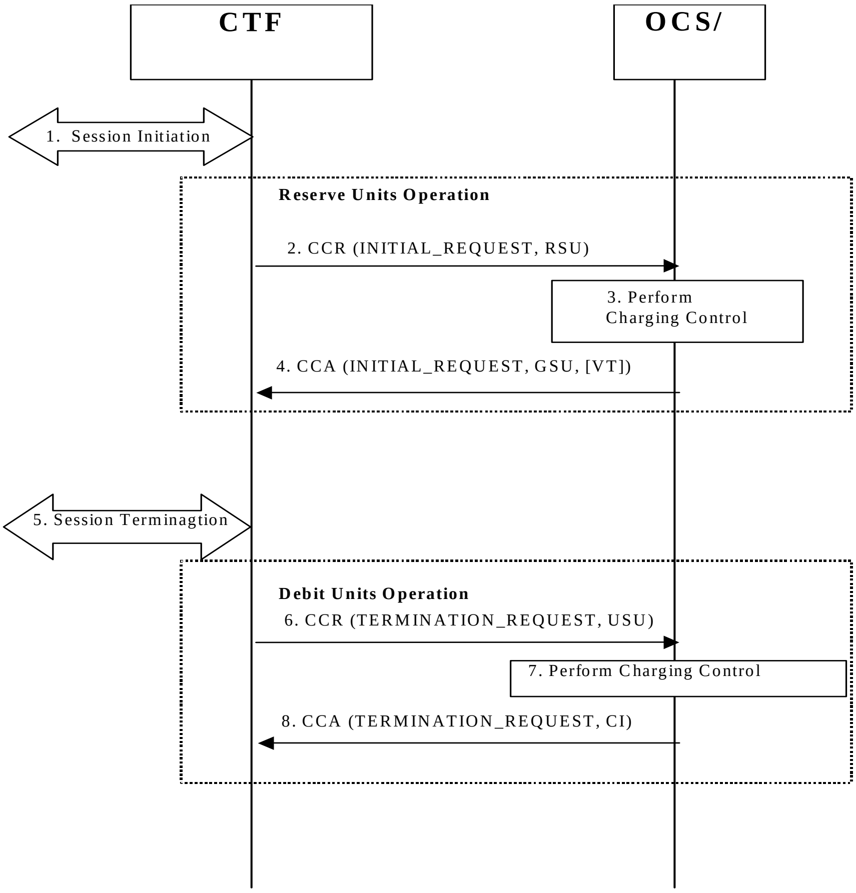

CTF
OCS/
1. Session Initiation
Reserve Units Operation
2. CCR (INITIAL_REQUEST, RSU)
3. Perform Charging Control
4. CCA (INITIAL_REQUEST, GSU, [VT])
5. Session Terminagtion
Debit Units Operation
6. CCR (TERMINATION_REQUEST, USU)
7. Perform Charging Control
8. CCA (TERMINATION_REQUEST, CI)

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. The session is terminated at the network element.

Step 7. 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 8. The OCS deducts the amount used from the account. Unused reserved units are released, if applicable.

Step 9. 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 6.3.5.

Editor"s note: Update the figure to reflect the changes made in the steps.

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' interface. 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 the Diameter Credit Control 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 [402].

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 quotas to be granted for use 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 must still 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 [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 (sub-)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 (sub-)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.

6.4 Message formats for Online

6.4.1 Summary of Online Charging Message Formats

6.4.1.1 General

The Diameter credit control application [402] 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 defined in the Diameter Credit Control Application [402] specification. 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.

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

Table 6.4.1.1 : Online Charging Messages Reference Table

Command-Name	Source	Destination	Abbreviation
Credit-Control-Request	Network Element	OCS	CCR
Credit-Control-Answer	OCS	Network Element	CCA
Re-Auth-Request	OCS	Network Element	RAR
Re-Auth-Answer	Network Element	OCS	RAA
Capabilities-Exchange-Request	Network Element/OCS	Network Element/OCS	CER
Capabilities Exchange Answer	Network Element/OCS	Network Element/OCS	CEA
Device-Watchdog-Request	Network Element/OCS	Network Element/OCS	DWR
Device-Watchdog-Answer	Network Element/OCS	Network Element/OCS	DWA

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 the Diameter Credit Control Application specification [402].

Those Diameter Credit Control AVPs that are used for online charging are marked "Yes" in tables 6.2 to 6.3. Those Diameter AVPs that are not used for online charging are marked "No" in tables 6.2 to 6.3. This implies that their content can (Yes) or can not (No) be used by the OCS for charging purposes.

The following symbols are used in the tables:

- <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.

Where the AVPs" are marked as "Yes", they are then mandatory, if marked "No", they are not used, if marked "Optional", then their use is subject to their inclusion in the relevant domain specific charging TS, if marked "Conditional", then its use is subject to condition specified in this TS, if marked as "Out of Scope" (OoS), then, the decision on its use is defined from the specification it has been derived from and is not subject to judgement within the present document.

6.4.2 Credit-Control-Request Message

The following table illustrates the basic structure of a Diameter Credit Control *Credit-Control-Request* message as used for online charging.

Table 6.4.2: Credit-Control-Request (CCR) Message Contents for Online Charging

Diameter Credit Control Application AVPs	
AVP	**Used in 3GPP**
<Diameter Header: 272, REQ, PXY>	Yes
<Session-Id>	Yes
{Origin-Host}	Yes
{Origin-Realm}	Yes
{Destination-Realm }	Yes
{Auth-Application-Id}	Yes
[Destination-Host]	Yes
[Vendor-Specific-Application-Id]	Yes
[Vendor-Id]	Yes
{ Auth-Application-Id }	Yes
{ Acct-Application-Id }	Yes
[User-Name]	Yes
[Acct-Multi-Session-Id]	No
[Origin-State-Id]	Yes
[Event-Timestamp]	Yes
* [Proxy-Info]	No
{ Proxy-Host }	No
{ Proxy-State }	No
* [Route-Record]	No
[Termination-Cause]	No
*[AVP]	Yes
{CC-Request-Type}	Yes
{CC-Request-Number}	Yes
[CC-Subsession-Id]	Yes
*[Subscription-Id]	Yes
{Subscription-Id-Type}	Yes
{Subscription-Id-Data}	Yes
[Requested-Action]	Yes
[Requested-Service-Unit]	Yes
[CC-Time]	Yes
[CC-Money]	Yes
{Unit-Value}	Yes
{Value-Digits}	Yes
[Exponent]	Yes
[Currency-Code]	Yes
[CC-Total-Octets]	Yes
[CC-Input-Octets]	Yes
[CC-Output-Octets]	Yes
[CC-Service-Specific-Units]	Yes
*[AVP]	Yes
*[Used-Service-Unit]	Yes

Diameter Credit Control Application AVPs	
[Tariff-Change-Usage]	Yes
[CC-Time]	Yes
[CC-Money]	Yes
{Unit-Value}	Yes
{Value-Digits}	Yes
[Exponent]	Yes
[Currency-Code]	Yes
[CC-Total-Octets]	Yes
[CC-Input-Octets]	Yes
[CC-Output-Octets]	Yes
[CC-Service-Specific-Units]	Yes
*[AVP]	Yes
*[Service-Parameter-Info]	Yes
[Service-Parameter-Type]	Yes
[Service-Parameter-Value]	Yes
[CC-Correlation-Id]	No
[Service-Identifier]	No
[Multiple-Services-Indicator]	Yes
*[Multiple-Services-Credit Control]	Yes
[Reporting-Reason]	Yes
*[Trigger-Type]	Yes
[Granted-Service-Unit]	No
[Requested-Service-Unit]	Yes
[CC-Time]	Yes
[CC-Money]	Yes
{Unit-Value}	Yes
{Value-Digits}	Yes
[Exponent]	Yes
[Currency-Code]	Yes
[CC-Total-Octets]	Yes
[CC-Input-Octets]	Yes
[CC-Output-Octets]	Yes
[CC-Service-Specific-Units]	Yes
*[AVP]	Yes
*[Used-Service-Unit]	Yes
[Reporting-Reason]	Yes
[Tariff-Change-Usage]	Yes
[CC-Time]	Yes
[CC-Money]	Yes
{Unit-Value}	Yes
{Value-Digits}	Yes
[Exponent]	Yes
[Currency-Code]	Yes
[CC-Total-Octets]	Yes
[CC-Input-Octets]	Yes
[CC-Output-Octets]	Yes
[CC-Service-Specific-Units]	Yes
*[AVP]	Yes
[Tariff-Change-Usage]	No
*[Service-Identifier]	Yes
[Rating-Group]	Yes
*[G-S-U-Pool-Reference]	No
[Validity-Time]	No
[Result-Code]	No
[Final-Unit-Indication]	No
*[AVP]	Yes
[User-Equipment-Info]	Yes
{User-Equipment-Info-Type}	Yes
{User-Equipment-Info-Value}	Yes
3GPP Credit control AVPs	
[ServiceInformation]	Yes
[PS-Information]	Yes
[WLAN-Information]	Yes
[IMS-Information]	Yes

Diameter Credit Control Application AVPs	
[MMS-Information]	Yes
[LCS-Information]	Yes

6.4.3 Credit-Control-Answer Message

The following table illustrates the basic structure of a Diameter Credit Control *Credit-Control-Answer* message as used for online charging. This message is always used by the OCS as specified below, independent of the receiving network element and the CCR record type that is being replied to.

Table 6.4.3: Credit Control Answer (CCA) Message Contents for Online Charging

Diameter base protocol AVPs	
AVP	**Used in 3GPP**
<Diameter Header: 272, PXY>	Yes
<Session-Id>	Yes
{Result-Code}	Yes
{Origin-Host}	Yes
{Origin-Realm}	Yes
{Auth-Application-Id}	Yes
[Vendor-Specific-Application-Id]	Yes
[Vendor-Id]	Yes
{ Auth-Application-Id }	Yes
{ Acct-Application-Id }	Yes
[User-Name]	Yes
[Acct-Multi-Session-Id]	No
*[Redirect-Host]	No
[Redirect-Host-Usage]	No
[Redirect-Max-Cache-Time]	No
[Origin-State-Id]	Yes
[Event-Timestamp]	Yes
*[Proxy-Info]	No
{ Proxy-Host }	No
{ Proxy-State }	No
*[Route-Record]	No
*[AVP]	Yes
Diameter Credit Control AVPs	
{CC-Request-Type}	Yes
{CC-Request-Number}	Yes
[CC-Subsession-Id]	Yes
[CC-Session Failover]	No
*[Subscription-Id]	Yes
[Granted-Service-Unit]	Yes
[Tariff-Time-Change]	Yes
[CC-Time]	Yes
[CC-Money]	Yes
{Unit-Value}	Yes
{Value-Digits}	Yes
[Exponent]	Yes
[Currency-Code]	Yes
[CC-Total-Octets]	Yes
[CC-Input-Octets]	Yes
[CC-Output-Octets]	Yes
[CC-Service-Specific-Units]	Yes
[Time-Quota-Threshold]	Yes
[Volume-Quota-Threshold]	Yes
*[AVP]	Yes
[Cost-Information]	Yes
{Unit-Value}	Yes
{Value-Digits}	Yes
[Exponent]	Yes
{Currency-Code}	Yes
[Cost-Unit]	Yes
[Final-Unit-Indication]	Yes
{Final-Unit-Action}	Yes
*[Restriction-Filter-Rule]	Yes
*[Filter-Id]	Yes
[Redirect-Server]	Yes
[Check-Balance-Result]	Yes
[Credit-Control-Failure-Handling]	Yes
[Validity-Time]	Yes
*[Trigger-Type]	Yes
[Direct-Debiting-Failure-Handling]	Yes
*[Multiple-Services-Credit-Control]	Yes
[Quota-Holding-Time]	Yes

[Granted-Service-Unit]	Yes
[Tariff-Time-Change]	Yes
[CC-Time]	Yes
[CC-Money]	Yes
{Unit-Value}	Yes
{Value-Digits}	Yes
[Exponent]	Yes
[Currency-Code]	Yes
[CC-Total-Octets]	Yes
[CC-Input-Octets]	Yes
[CC-Output-Octets]	Yes
[CC-Service-Specific-Units]	Yes
[Time-Quota-Threshold]	Yes
[Volume-Quota-Threshold]	Yes
*[AVP]	Yes
[Requested-Service-Unit]	No
*[Used-Service-Unit]	No
[Tariff-Change-Usage]	Yes
*[Service-Identifier]	Yes
[Rating-Group]	Yes
*[G-S-U-Pool-Reference]	Yes
{G-S-U-Pool-Identifier}	Yes
{CC-Unit-Type}	Yes
{Unit-Value}	Yes
[Validity-Time]	Yes
[Result-Code]	Yes
[Final-Unit-Indication]	Yes
{Final-Unit-Action}	Yes
*[Restriction-Filter-Rule]	Yes
*[Filter-Id]	Yes
[Redirect-Server]	Yes
{Redirect-Address-Type}	Yes
{Redirect-Server-Address}	Yes
*[AVP]	Yes
3GPP Diameter Credit Control AVPs	
[PS-Furnish-Charging-Information]	Yes
{GPRS-Charging-Id}	Yes
{PS-Free-Format-Data}	Yes
[PS-Append-Free-Format-Data]	Yes

6.4.4 Re-Auth-Request Message

The following table 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

Diameter Credit Control Application AVPs	
AVP	**Used in 3GPP**
<Diameter Header: 258, REQ, PXY>	Yes
<Session-Id>	Yes
{Origin-Host}	Yes
{Origin-Realm}	Yes
{Destination-Realm}	Yes
{Destination-Host}	Yes
{Auth-Application-Id}	Yes
{Re-Auth-Request-Type}	Yes
[User-Name]	Yes
[Origin-State-Id]	Yes
[Event-Timestamp]	Yes
* [Proxy-Info]	No
{ Proxy-Host }	No
{ Proxy-State }	No

Diameter Credit Control Application AVPs	
* [Route-Record]	No
*[AVP]	Yes
[CC-Sub-Session-Id]	Yes
[G-S-U-Pool-Identifier]	Yes
[Service-Identifier]	Yes
[Rating-Group]	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.

6.4.5 Re-Auth-Answer Message

The following table 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].

6.5 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 stoped 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.

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-authorisation 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, depeding 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-authorisation 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.

If the threshold triggers were included along with the quota granted, the Credit Control client, then, 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 original quota had been consumed.

7 Summary of used AVPs (defined in the present document)

- Defined/used cause codes.

- Detailed list of AVPs defined here.

7.1 Diameter Accounting AVPs

The use of the Attribute Value Pairs (AVPs) that are defined in the Diameter Base Protocol [401] is specified in clause 6.2 for offline charging and in clause 6.4 for online charging. The information is summarized in the following table with the base protocol AVPs listed in alphabetical order. Detailed specification of these AVPs is available in the base protocol specifications.

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

Those Diameter AVPs that are used for offline charging are marked "Yes" in the following table. Those Diameter AVPs that are not used for offline charging are marked "No" in the following table. This implies that their content can (Yes) or can not (No) be used by the CCF for charging purposes.

The following symbols (adopted from [401]) are used in the tables:

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

Table 7.1: Use Of Diameter Base Protocol AVPs

AVP name	Mechanism	Offline	
	Type	ACR	ACA
	Table #	6.1	6.2
[Accounting-Multi-Session-Id]		No	No
[Accounting-RADIUS-Session-Id]		No	No
[Accounting-Realtime-Required]		No	No
{Accounting-Record-Number}		Yes	Yes
{Accounting-Record-Type}		Yes	Yes
[Accounting-Sub-Session-Id]		No	No
[Acct-Application-Id]		No	No
[Acct-Interim-Interval]		Yes	Yes
{Auth-Application-Id}		-	-
<Diameter-Header:271,REQ,PXY>		Yes	Yes
{Destination-Host}		-	-
{Destination-Realm}		Yes	-
[Error-Message]		-	-
[Error-Reporting-Host]		-	No
[Event-Timestamp]		Yes	Yes
*[Failed-AVP]		-	-
*[Proxy-Info]		No	No
{Origin-Host}		Yes	Yes
{Origin-Realm}		Yes	Yes
[Origin-State-Id]		Yes	Yes
*[Redirected-Host]		-	-
[Redirected-Host-Usage]		-	-
[Redirected-Max-Cache-Time]		-	-
{Result-Code}		-	Yes
*[Route-Record]		No	-
<Session-Id>		Yes	Yes
[User-Name]		Yes	Yes
[Vendor-Specific-Application-Id]		Yes	Yes

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

7.1.1 Diameter Base AVP

7.1.1.1 Acct-Application-Id AVP

The *Acct-Application-Id* AVP (AVP code 259), as part of the *Vendor-Specific-Application-Id* grouped AVP, shall contain the value of 1 i.e. the same application id as used by the Cx interface protocol as defined in [204].

7.1.1.2. Result-Code AVP

This subclause defines new *Result-Code* AVP (AVP code 298) values that must be supported by all Diameter implementations that conform to the present document.

The *Accounting-Answer* message includes the *Result-Code* AVP, which may indicate that an error was present in the *Accounting-Request* message. A rejected *Accounting-Request* message should cause the user's session to be terminated.

Errors that fall within the transient failures category are used to inform a peer that the request could not be satisfied at the time it was received, but MAY be able to satisfy the request in the future.

DIAMETER_END_USER_SERVICE_DENIED 4010

The OCF denies the service request due to service restrictions 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 credit control server 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).

Errors that fall within permanent failure category are used to inform the peer that the request failed, and should not be attempted again.

DIAMETER_CREDIT_LIMIT_REACHED 4012

The credit-control server 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.

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 credit-control client that the credit-control server 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. 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.

7.1.1.3 User-Name AVP

The *User-Name* AVP (AVP code 1) contains the Private User Identity [201], if available in the node.

7.1.1.4 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'.

7.1.2 3GPP specific accountingAVPs

For the purpose of offline charging additional AVPs are used in ACR and ACA. The information is summarized in the following table along with the AVP flag rules.

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. [402]), is provided in the following table and the detailed description is not repeated.

Table 7.2: Use Of Diameter accounting AVPs

AVP Name	AVP Code	Clause Defined	Value Type	AVP Flag rules				
				Must	May	Should not	Must not	May Encr.
3GPP Diameter Accounting AVPs								
[Event-Type]	823	7.1.2.16	Grouped	V				
[SIP-Method]	824	7.1.2.34	UTF8String	V				
[Event]	825	7.1.2.15	UTF8String	V				
[Content-Type]	826	7.1.2.12	UTF8String	V				
[Content-Length]	827	7.1.2.11	UTF8String	V				
[Content-Disposition]	828	7.1.2.10	UTF8String	V				
[Role-of-Node]	829	7.1.2.27	Enumerated	V				
[User Session Id]	830	7.1.2.45	UTF8String	V				
[Calling-Party-Address]	831	7.1.2.7	UTF8String	V				
[Called-Party-Address]	832	7.1.2.6	UTF8String	V				
[Time-stamps]	833	7.1.2.39	Grouped	V				
[SIP-Request-Timestamp]	834	7.1.2.35	UTF8String	V				
[SIP-Response-Timestamp]	835	7.1.2.36	UTF8String	V				
[Application-server]	836	7.1.2.3	UTF8String	V				
[Application-provided-called-party-address]	837	7.1.2.2	UTF8String	V				
[Inter-Operator-Identifier]	838	7.1.2.22	Grouped	V				
[Originating-IOI]	839	7.1.2.25	UTF8String	V				
[Terminating-IOI]	840	7.1.2.38	UTF8String	V				
[IMS-Charging-Identifier]	841	7.1.2.20	UTF8String	V				
*[SDP-Session-Description]	842	7.1.2.31	UTF8String	V				
*[SDP-Media-component]	843	7.1.2.28	Grouped	V				
[SDP-Media-Name]	844	7.1.2.30	UTF8String	V				
*[SDP-Media-Description]	845	7.1.2.29	UTF8String	V				
[GPRS-Charging-Id]	846	7.1.2.18	UTF8String	V				
[GGSN-Address]	847	7.1.2.17	IPAddress	V				
[Served-Party-IP-Address]	848	7.1.2.32	IPAddress	V				
[Authorized-QoS]	849	7.1.2.4	UTF8String	V				
[Server-Capabilities]	[204]	[204]		V				
[Trunk-Group-Id]	851	7.1.2.40	Grouped	V				
[Incoming-Trunk-Group-Id]	852	7.1.2.21	UTF8String	V				
[Outgoing-Trunk-Group-Id]	853	7.1.2.26	UTF8String	V				
[Bearer-Service]	854	7.1.2.5	OctetString	V				
[Service-Id]	855	7.1.2. 33	UTF8String	V				
[UUS-Data]	856	7.1.2.46	Grouped	V				
[Amount-of-UUS-data]	857	7.1.2.1	UTF8String	V				
[Mime-type]	858	7.1.2.23	UTF8String	V				
[Direction]	859	7.1.2.14	Enumerated	V				
[Cause]	860	7.1.2.8	Grouped	V				
{Cause-Code}	861	7.1.2.9	Enumerated	V				
{Node-Functionality}	862	7.1.2.24	Enumerated	V				

7.1.2.1 Amount-of-UUS-Data AVP

The *Amount-Of-UUS-Data* AVP (AVP code 857) is of type UTF8String and holds the amount (in octets) of User-to-User data conveyed in the body of the SIP message with content-disposition header field equal to "render".

7.1.2.2 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 URL, E.164), if it is determined by an application server.

7.1.2.3 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.

7.1.2.4 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 interface.

7.1.2.5 Bearer-Service AVP

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

7.1.2.6 Called-Party-Address AVP

The *Called-Party-Address* AVP (AVP code 832) is of type UTF8String and holds the address (Public User ID: SIP URL, E.164, etc.) of the party to whom a session is established.

7.1.2.7 Calling-Party-Address AVP

The *Calling-Party-Address* AVP (AVP code 831) is of type UTF8String and holds the address (Public User ID: SIP URL, E.164, etc.) of the party initiating a session.

7.1.2.8 Cause AVP

The *Cause* AVP (AVP code 860) is of type Grouped. The Cause AVP includes the *Cause-Code* AVP that contains the cause value and the *Node-Functionality* AVP that contains the function of the node where the cause code was generated.

Cause has the following ABNF grammar:

```
<Cause>::=<AVP Header:   860>

          {Cause-Code}

          {Node-Functionality}
```

7.1.2.9 Cause-Code AVP

The *Cause-Code* AVP (AVP code 861) is of type Enumerated and includes the cause code value from IMS node. It is used in Accounting-request[stop] and/or Accounting-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).

"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].

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).

7.1.2.10 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 [406].

7.1.2.11 Content-Length AVP

The *Content-Length* AVP (AVP code 827) is of type UTF8String and holds the size of the of the message-body, as described in [406].

7.1.2.12 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 [406].

7.1.2.13 Direction AVP

The *Direction* AVP (AVP code 859) is of type Enumerated and indicates whether the UUS data travels in up-link or down-link direction. The following values are defined:

UPLINK	0
DOWNLINK	1

7.1.2.14 Event AVP

The *Event* AVP (AVP code 825) is of type UTF8String and holds the content of the "Event" header used in SUBSCRIBE and NOTIFY messages.

7.1.2.15 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 message is generated.

It has the following ABNF grammar:

```
<Event-Type>::=<AVP Header: 823 >

        [ SIP-Method]

        [ Event ]

        [ Content-Type ]

        [ Content-Length ]

        [ Content-Disposition ]
```

7.1.2.16 GGSN-Address AVP

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

7.1.2.17 GPRS-Charging-ID AVP

The *GPRS-Charging-ID* AVP (AVP code 846) is of type UTF8String and holds a sequence number generated by the GGSN at PDP context activation, as described in [1].

7.1.2.18 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.

7.1.2.19 Incoming-Trunk-Group-ID AVP

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

7.1.2.20 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 ]
```

7.1.2.21 Mime-Type AVP

The *Mime-Type* AVP (AVP code 858) is of type UTF8String and holds the Mime type of the User-To-User data.

7.1.2.22 Node-Functionality AVP

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

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
UE	7

7.1.2.23 Originating-IOI AVP

The *Originating-IOI* AVP (AVP code 839) is of type UTF8String (alphanumeric string) and holds the Inter Operator Identifier for the originating network as generated by the S-CSCF in the home network of the originating end user [404].

7.1.2.24 Outgoing-Trunk-Group-ID AVP

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

7.1.2.25 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 a 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.

7.1.2.26 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 ]

        [ GPRS-Charging-Id ]
```

7.1.2.27 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.

7.1.2.28 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.

7.1.2.29 SDP-Session-Description AVP

The *SDP-Media-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].

7.1.2.30 Served-Party-IP-Address AVP

The *Served-Party-IP-Address* AVP (AVP code 848) is of type IPAddress 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.

7.1.2.31 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.

7.1.2.32 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 an accounting request to be sent to the CCF.

7.1.2.33 SIP-Request-Timestamp AVP

The *SIP-Request-Timestamp* AVP (AVP code 834) is of type UTF8String and holds the time in UTC format of the initial SIP request (e.g. Invite).

7.1.2.34 SIP-Response-Timestamp AVP

The *SIP-Response-Timestamp AVP* (AVP code 835) is of type UTF8String and holds the time in UTC format of the response to the initial SIP request (e.g. 200 OK).

7.1.2.35 Terminating-IOI AVP

The *Terminating-IOI* AVP (AVP code 840) is of type UTF8String (alphanumeric string) and holds the Inter Operator Identifier for the originating network as generated by the S-CSCF in the home network of the terminating end user [404].

7.1.2.36 Time-stamps AVP

The *Time-Stamp* 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]
```

7.1.2.37 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 ]
```

7.1.2.38 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 *Session-ID* contains the SIP Call ID, as defined in [405].

7.1.2.39 UUS-Data AVP

The *UUS-Data* AVP (AVP Code 856) is of type Grouped AVP and holds information about the sent User-To-User data.

It has the following ABNF grammar:

```
<Used-Service-Unit>::=< AVP Header: 856 >
          [Amount-of-UUS-Data]
          [Mime-Type]
          [Direction]
```

7.1.2.40 PS-Furnish-Charging-Information

This information element may be received in a CCA message via the Ro interface. 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 interface. The detailed description of this AVP is provided in section 7.2.2.2.

7.2. AVPs for Credit Control

For the purpose of online charging additional AVPs are used in CCR and CCA. The information is summarized in the following table along with the AVP flag rules.

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. [402]), is provided in the following table and the detailed description is not repeated.

Table 7.3: Use Of Diameter Credit Control

AVP Name	AVP Code	Clause Defined	Value Type	AVP Flag rules				
				Must	May	Should not	Must not	May Encr.
CC-Correlation-Id	[402]	[402]	OctetString					
CC-Input-Octets	[402]	[402]	Unsigned64					
CC-Money	[402]	[402]	Grouped					
CC-Output-Octets	[402]	[402]	Unsigned64					
CC-Request-Number	[402]	[402]	Unsigned32					
CC-Request-Type	[402]	[402]	Enumerated					
CC-Service-Specific-Units	[402]	[402]	Unsigned64					
CC-Session –Failover	[402]	[402]	Enumerated					
CC-Sub-Session-Id	[402]	[402]	Unsigned64					
CC-Time	[402]	[402]	Unsigned32					
CC-Total-Octets	[402]	[402]	Unsigned64					
CC-Unit-Type	[402]	[402]	Enumerated					
Check-Balance-Result	[402]	[402]	Enumerated					
Cost-Information	[402]	[402]	Grouped					
Cost-Unit	[402]	[402]	UTF8String					
Credit-Control	[402]	[402]	Enumerated					
Credit-Control-Failure-Handling	[402]	[402]	Enumerated					
Currency-Code	[402]	[402]	Unsigned32					
Direct-Debiting-Failure-Handling	[402]	[402]	Enumerated					
Exponent	[402]	[402]	Integer32					
Final-Unit-Action	[402]	[402]	Enumerated					
Final-Unit-Indication	[402]	[402]	Grouped					
Granted-Service-Unit	[402]	[402]	Grouped					
Granted-Service-Unit -Pool-Identifier	[402]	[402]	Unsigned32					
Granted-Service-Unit -Pool-Reference	[402]	[402]	Grouped					
Multiple-Services-Credit-Control	[402]	[402]	Grouped					
Multiple-Services-Indicator	[402]	[402]	Enumerated					
Rating-Group	[402]	[402]	Unsigned32					
Redirect-Address-Type	[402]	[402]	Enumerated					
Redirect-Server	[402]	[402]	Grouped					
Redirect-Server-Address	[402]	[402]	UTF8String					
Requested-Action	[402]	[402]	Enumerated					
Requested-Service-Unit	[402]	[402]	Grouped					
Restriction -Filter-Rule	[402]	[402]	IPFiltrRule					
Service-Identifier	[402]	[402]	UTF8String					
Service-Parameter-Info	[402]	[402]	Grouped					
Service-Parameter-Type	[402]	[402]	Unsigned32					
Service- Parameter-Value	[402]	[402]	OctetString					
Subscription-Id	[402]	[402]	Grouped					
Subscription-Id-Data	[402]	[402]	UTF8String					
Subscription-Id-Type	[402]	[402]	Enumerated					
Tariff-Change-Usage	[402]	[402]	Enumerated					
Tariff-Time-Change	[402]	[402]	Time					
Unit-Value	[402]	[402]	Grouped					
Used-Service-Unit	[402]	[402]	Grouped					
User-Equipment-Info	[402]	[402]	Grouped					
User-Equipment-Info-Type	[402]	[402]	Unsigned32					
User-Equipment-Info-Value	[402]	[402]	UTF8String					
Value-Digits	[402]	[402]	Integer64					
Validity-Time	[402]	[402]	Unsigned32					
3GPP Diameter Credit Control AVPs								
Service-Information	Tbd.	7.2.2.1	Grouped					
PS-Furnish-Charging-Information	865	7.2.2.2	Grouped					
GPRS-Charging-Id	846	7.1.2.18	UTF8String					
PS-Free-Format-Data	866	7.2.2.3	OctetString					
PS-Append-Free-Format-Data	867	7.2.2.4	Enumerated					
Time-Quota-Threshold	868	7.2.2.5	Unsigned64					
Volume-Quota-Threshold	869	7.2.2.6	Unsigned64					
Trigger-Type	870	7.2.2.7						
Quota-Holding-Time	871	7.2.2.8						
Reporting-Reason	872	7.2.2.9						

7.2.1. Diameter Credit Control AVPs

tbd.

7.2.2 3GPP Specific Credit Control AVPs

7.2.2.1 Service-Information AVP

The ServiceInformation AVP is of type Grouped. Its purpose is to allow the transmission of additional service specific information elements which are not covered in this document.

The ServiceInformation AVP has the following format:

```
Service-Information :: =   < AVP Header: TBD>
                           [PS-Information]
                           [WLAN-Information]
                           [IMS-Information]
                           [MMS-Information]
                           [LCS-Information]
```

The format and the contents of the fields inside the ServiceInformation 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.

Further fields may be included in the ServiceInformation AVP when new services are introduced.

7.2.2.2 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 interface, onto the Rf interface in order to facilitate its inclusion in CDRs. The PS- Furnish-Charging-Information AVP has the following format:

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

7.2.2.3 PS-Free-Format-Data AVP

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

7.2.2.4 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.

7.2.2.5 Time-Quota-Threshold

The Time-Quota-Threshold AVP (AVP code 868) is of type Unsigned64 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.

7.2.2.6 Volume-Quota-Threshold

The Volume-Quota-Threshold AVP (AVP code 869) is of type Unsigned64 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 progress, up to the volume indicated in the original quota.

7.2.2.7 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 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.

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.

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.

7.2.2.8 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.

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.

7.2.2.9 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)

- 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)

- 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)

- 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)

- 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)

- 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)

- 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)

- 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 the rating contions 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)

- 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

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.

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.

Annex A (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
Mar 2004	SA_23	SP-040145	--	--	Submitted to TSG SA#23 for Information	1.0.0	
Sep 2004	SA_25	SP-040554	--	--	Submitted to TSG SA#25 for Approval	2.0.0	6.0.0
Dec 2004	SA_26	SP-040776	001	--	Reassign Vendor specific AVP codes - Align with CN4"s 29.230	6.0.0	6.1.0
Dec 2004	SA_26	SP-040776	002	--	Add Threshold based re-authorisation triggers	6.0.0	6.1.0
Dec 2004	SA_26	SP-040776	003	--	Add Re-authorisation triggers for flow-based online charging – Align with Stage 2	6.0.0	6.1.0
Dec 2004	SA_26	SP-040776	004	--	Add missing elements and other corrections	6.0.0	6.1.0
Dec 2004	SA_26	SP-040775	005	--	Add definition of a new 3GPP-specific AVP: PS Furnish Charging Information AVP - Align with 32.251	6.0.0	6.1.0
				--			

History

Document history		
V6.1.0	December 2004	Publication