Source:	**SA5 (Telecom Management)**
Title:	New Rel-6 TS 32.299-100: "Telecommunication management; Charging management; Diameter charging applications" - **for SA Information**
Document for:	**Information**
Agenda Item:	**7.5.3**

SP-040145 New Rel-6 TS 32.299-100: "Telecommunication management; Charging management; Diameter charging applications" - **for SA Information**

3GPP TSG-SA5 (Telecom Management) S5-044153
Meeting #37, Malaga, SPAIN, 23 - 27 Feb 2004

Presentation of Specification to TSG

Presentation to:	**TSG SA Meeting #23**
Document for presentation:	**TS 32.299, Version 1.0.0**
Presented for:	**Information**

Abstract of document:

This is a 3GPP Technical Specification for the Diameter charging applications; for online and offline charging for 3GPP networks. The technical specification in Rel 6 currently focuses on the ‘Rf’ and ‘Ro’ interface.

Changes since last presentation to TSG SA:
New

Outstanding Issues:

- Stage 2 requirements as derived from the Rel-5 specifications need to be included.
- The selection of the protocol application specification needs to be finalised.
- Addition / completion of parameter description & formal syntax.

Contentious Issues:
None.

3GPP TS 32.299 V1.0.0 (2004-03)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Service and System Aspects;
Telecommunication management;
Charging management;
Diameter charging applications;
(Release 6)

The present document has been developed within the 3rd Generation Partnership Project (3GPP ™) and may be further elaborated for the purposes of 3GPP.

The present document has not been subject to any approval process by the 3GPP Organizational Partners and shall not be implemented.
This Specification is provided for future development work within 3GPP only. The Organizational Partners accept no liability for any use of this Specification.
Specifications and reports for implementation of the 3GPP ™ system should be obtained via the 3GPP Organizational Partners' Publications Offices.

Keywords

UMTS, charging, accounting, management,
Diameter, GPRS, IMS, MMS, online, offline

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

Copyright Notification

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

© 2004, 3GPP Organizational Partners (ARIB, CCSA, ETSI, T1, TTA, TTC).
All rights reserved.

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]-[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-03.txt.

[403] IETF RFC 1350 "TFTP Protocol".

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

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 Diameter online and offline charging applications

4.1 Implementation of offline and online charging

The present document defines a 3GPP Diameter charging application, which utilizes the Diameter Base Protocol (RFC 3588 [401]). Separate applications are used online and offline charging. The generic description of the protocol is provided in the subclauses below while the portions of the protocol application associated with offline and online charging are described in clauses 5 and 6, respectively.

The charging architecture implementing Diameter adheres to the structure where all communications for offline charging purposes between the network entities and the core network charging function are carried out on the Diameter 'Rf' interface. Subsequently, all communications between the network entities and the online charging system utilize the Diameter 'Ro' interface. The above-mentioned interfaces are defined in 3GPP TS 32.240 [1].

4.2 Diameter protocol basic principles and use

4.2.1 Basic Principles

The Diameter charging applications are based on the following general principles:

The basic functionality of Diameter accounting, as defined by the Diameter Base Protocol (RFC 3588 [401]) is re-used. However, for online charging, the basic functionality as defined by the IETF Diameter Credit Control application is reused.

Editor's note: The working assumption for online charging needs to be confirmed.

For offline charging network reports accounting information to the Charging Data Function (CDF). The CDF uses this information to construct and format CDRs.

For online charging, the network elements requests resource allocation and reports credit control information to the Online Charging System (OCS).

4.2.2 Application requirement for the Diameter charging application

Editor's Note: Move the following two subclauses to the appropriate section, i.e. the stage 3 section..

4.2.2.1 Offline specific base protocol requirements

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].

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.

4.2.2.2 Online Specific Credit Control Application Requirements

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.

The online client (e.g. a GGSN, TPF or an AS, MRFC) implements the state machine described in [402] for "CLIENT, EVENT BASED" 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 [402] for the "SERVER, SESSION AND EVENT BASED" in order to support Immediate Event Charging and Event Charging with Unit Reservation.

4.2.2.3 Security Considerations

Diameter security is addressed in the base protocol RFC 3588 [401]. Network security is specified in 3GPP TS 33.201 [70].

Editor's note: Update reference

5 Offline charging

5.1 Basic Principles

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.

5.1.1 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.

Figure 5.1 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.

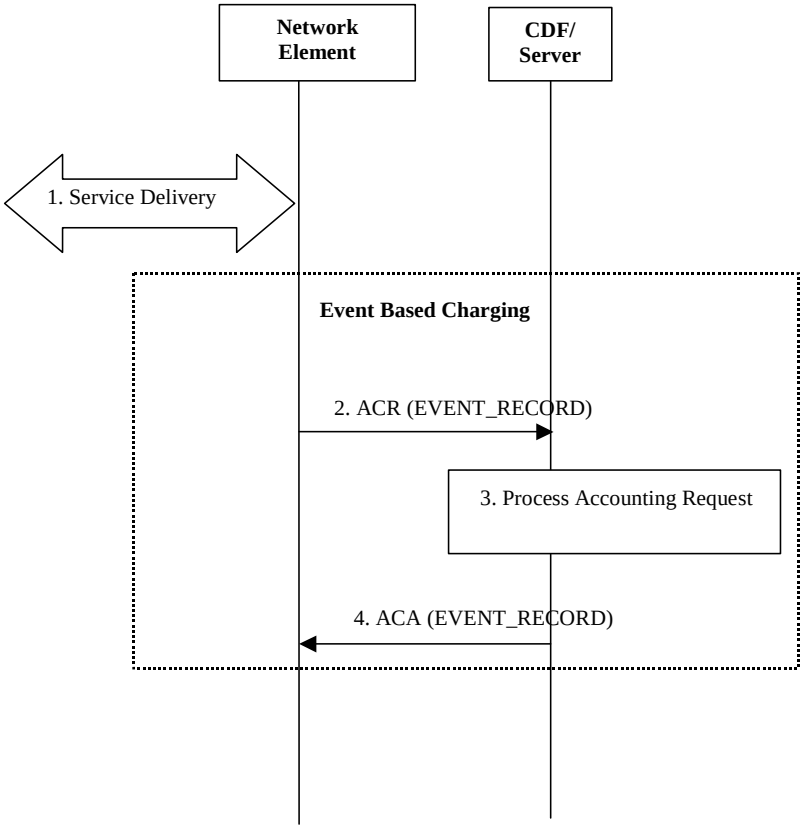

Figure 5.1: Event Based online charging

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.

5.1.2 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.

Figure 5.2 shows the transactions that are required on the Diameter offline interface in order to perform session based charging.

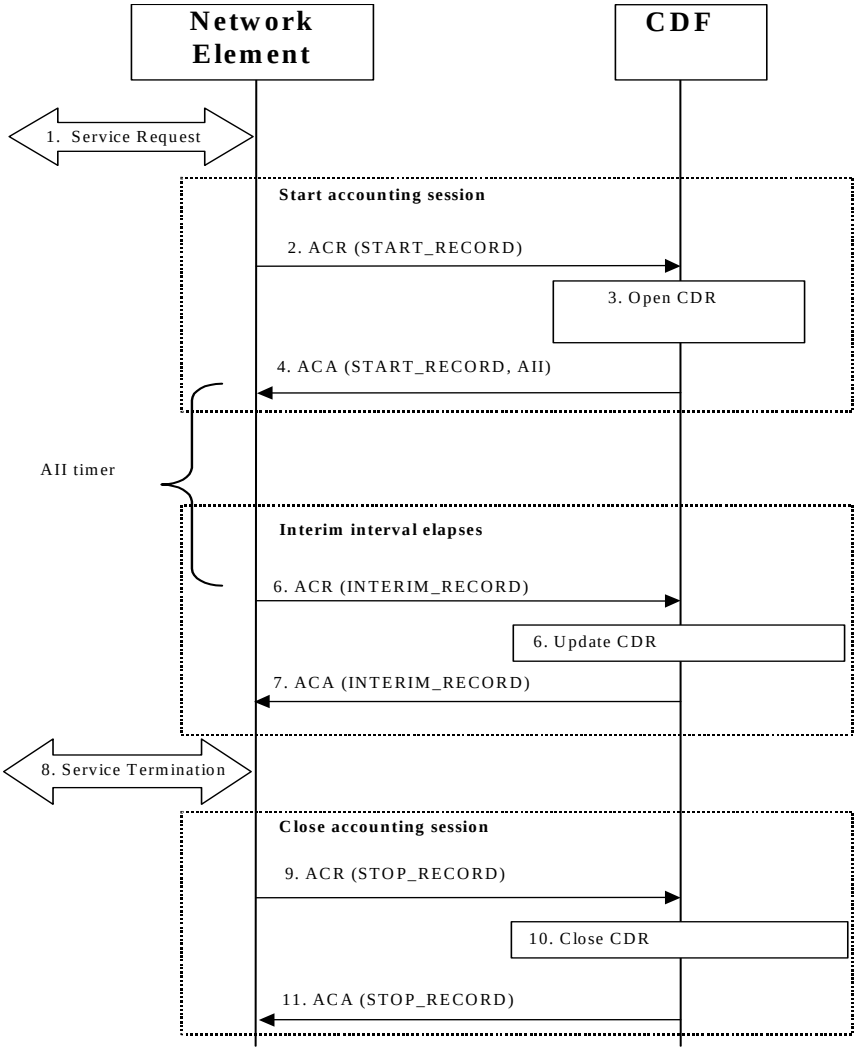

Figure 5.2: Session based offline charging

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.

5.2 Offline charging error cases - Diameter procedures

5.2.1 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.

5.2.2 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.

5.2.3 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.

5.2.4 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.

5.3 Message Contents

5.3.1 Accounting-Request Message

Table 5.1 illustrates the basic structure of a Diameter *Accounting-Request* message as used for offline charging.

Table 5.1: 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
[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]	No
*[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-provided-Called-Party-Address]	Only for IMS (S-CSCF)
*[Inter-Operator-Identifier]	Yes
[IMS-Charging-Identifier]	Yes
*[SDP-Session-Description]	Yes
*[SDP-Media-Component]	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
[Cause]	Yes

NOTE: For AVP of type "Grouped" only the group AVP is listed in table 5.1. A detailed description of the AVPs is provided in clause 7.

5.3.2 Accounting-Answer Message

Table 5.2 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 5.2: 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
[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
*[AVP]	No

6 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.

6.1 Diameter Description on the Ro Interface

6.1.1 Basic Principles

For online charging the Diameter Credit Control Application defined in [402] is used with additional AVPs defined in the present document.

Two cases for online event charging are distinguished:

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

In the case of Immediate Event Charging (IEC), granting units to the network element is performed in a single operation that also includes the deduction of the corresponding monetary units from the subscriber's account. The credit control process 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 contrast, Event Charging with Unit Reservation (ECUR) also includes the process of requesting, reserving, releasing and returning unused units. The deduction of the corresponding monetary units then occurs upon conclusion of the ECUR transaction. In this case, the *CC-Request-Type* INITIAL / UPDATE / TERMINATION_REQUEST are used to control the accounting session. During a session there can be repeated execution of unit reservation and debit operations as specified in subclause X[AvT2].

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.

6.1.2 Message Flows and Types

NOTE: This subclause describes the basic message flows for the event charging procedures on the Ro interface.

As described earlier, for online charging, two distinct cases are currently defined, IEC and ECUR. The basic procedures for these cases are conducted as explained below.

6.1.2.1 Immediate Event Charging (IEC)

Figure 6.1 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.

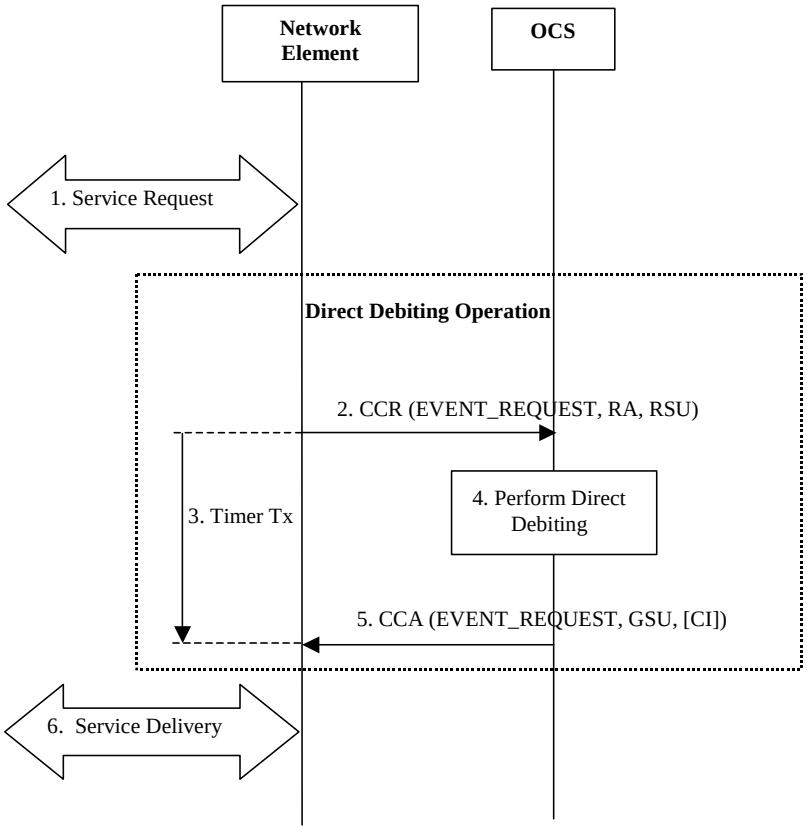

Figure 6.1: IEC Direct Debiting Operation

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].

6.1.2.2 Event Charging with Unit Reservation

Figure 6.2 shows the transactions that are required on the 'Ro' interface in order to perform the ECUR session based reserve and debit units operation. Multiple replications of both of these operations are possible.

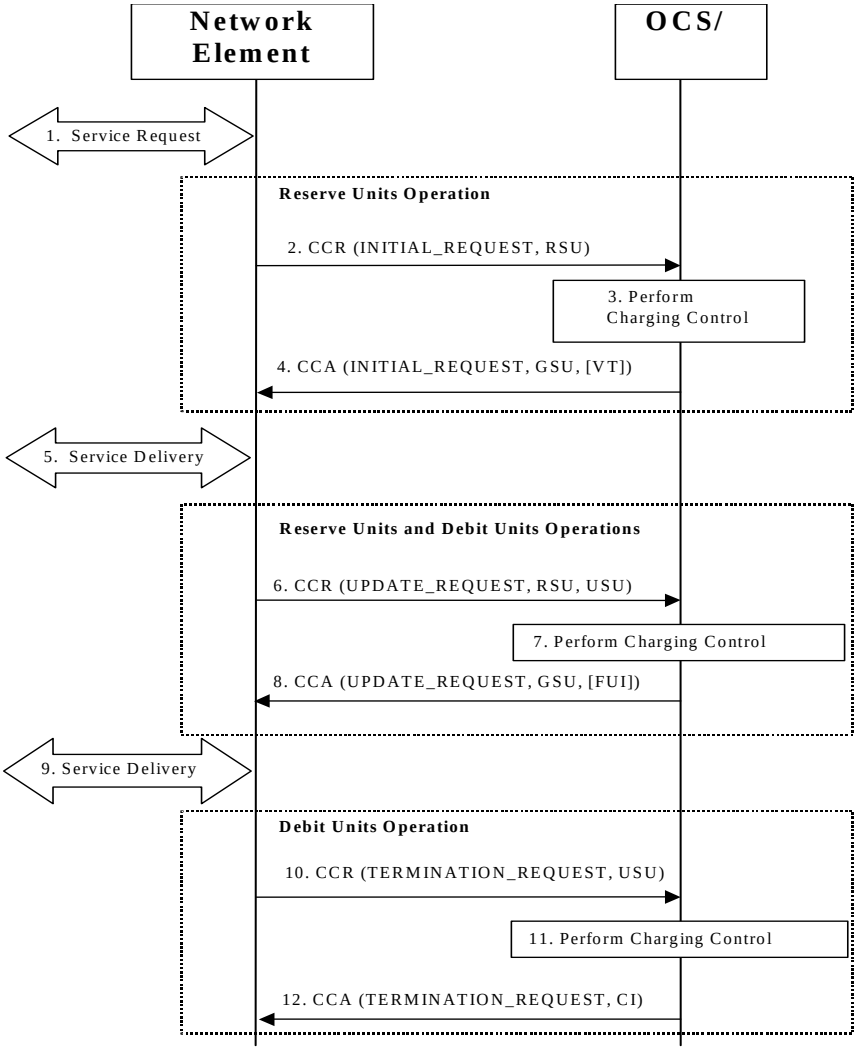

Figure 6.2: ECUR for session based credit control

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* (VI) 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 6.2.

6.1.3 Message Flows - Successful Cases and Scenarios

6.1.3.1 Online Charging 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.

6.1.3.1.1 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 IEC 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.

6.1.3.1.2 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.

6.1.3.2 Support of Tariff Switch

Changes to the tariffs pertaining to the service may be handled in the following ways.

- Tariff Changes handled using Validity-Time AVP; or
- Tariff changes handled using the Tariff Switch Time AVP.

Editor's note: This subclause should be updated according the method described in [402] It needs to be further clarified if Tariff Switch can also be applied in the case of time a the unit of measurement or only in the case of volume.

6.2 Message formats

6.2.1 Summary of Online Charging Message Formats

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.

Table 6.1 describes the use of these messages for online charging.

Table 6.1: Online Charging Messages Reference Table

Command-Name	Source	Destination	Abbreviation
Credit-Control-Request	Network Element	OCS	CCR
Credit-Control-Answer	OCS	Network Element	CCA

6.2.1.1 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 *Credit-Control-Request* and *Credit-Control-Answer* 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.

6.2.1.1.1 Credit-Control-Request Message

Table 6.2 illustrates the basic structure of a Diameter Credit Control *Credit-Control-Request* message as used for online charging.

Table 6.2: Credit-Control-Request (CCR) Message Contents for Online Charging

Diameter Base Protocol AVPs	
AVP	**Used in Online CCR**
<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
[User-Name]	Yes
[Acct-Multi-Session-Id]	No
[Origin-State-Id]	Yes
[Event-Timestamp]	Yes
* [Proxy-Info]	No
* [Route-Record]	No
[Termination-Cause]	No
*[AVP]	No
Diameter Credit Control Application AVPs	
{CC-Request-Type}	Yes
{CC-Request-Number}	Yes
{CC-Subsession-Id}	Yes
[Subscription-Id]	Yes
[Requested-Action]	Yes
*[Requested-Service-Unit]	Yes
*[Used-Service-Unit]	Yes
*[Service-Parameter-Info]	Yes
*[CC-Correlation-Id]	No
[Service-Identifier]	No
Multiple-Services-Indicator	Yes
Multiple-Services-Credit Control	Yes
G-S-U-Pool-Reference	Yes
G-S-U-Pool-Identifier	Yes
Tariff-Time-Change	Yes
Tariff-Change-Usage	Yes

Diameter Base Protocol AVPs	
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]	No
*[Application-Provided-Called-Party-Address]	Yes
*[Inter-Operator-Identifier]	Yes
[IMS-Charging-Identifier]	Yes
*[SDP-Session-Description]	Yes
*[SDP-Media-Component]	Yes
[GGSN-Address]	Yes
[Served-Party-IP-Address]	No
[Authorized QoS]	No
[Server-Capabilities]	No
[Trunk-Group-ID]	No
[Bearer-Service]	No
[Service-Id]	Yes
[UUS-Data]	Yes
[Cause]	Yes

6.2.1.1.2 Credit-Control-Answer Message

Table 6.3 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 6.3: Credit Control Answer (CCA) Message Contents for Online Charging

Diameter base protocol AVPs	
AVP	**Used in online CCA**
<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
[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
*[AVP]	No
Diameter Credit Control AVPs	
{CC-Request-Type}	Yes
{CC-Request-Number}	Yes
{CC-Subsession-Id}	Yes
[CC-Failover-Supported]	No
[Subscription-Id]	Yes
*[Granted-Service-Unit]	Yes
[Tariff-Switch-Definition]	Yes
[Cost-Information]	Yes
[Final-Unit-Indication]	Yes
[Check-Balance-Result]	Yes
[Credit-Control-Failure-Handling]	Yes
[Validity-Time]	Yes
[Direct-Debiting-Failure-Handling]	Yes
Multiple-Services-Credit-Control	Yes

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

- Defined/used cause codes.
- Detailed list of AVPs defined here.

Annex A (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
Mar 2004	S_23	SP-040145	--	--	Submitted to TSG SA#23 for Information	1.0.0	