ATIS-0300075.2018

Usage Data Management Architecture and Protocols Requirements for Packet-Based Application Services

AMERICAN NATIONAL STANDARD FOR TELECOMMUNICATIONS

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-IP transition, 5G, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

AMERICAN NATIONAL STANDARD

Approval of an American National Standard requires review by ANSI that the requirements for due process, consensus, and other criteria for approval have been met by the standards developer.

Consensus is established when, in the judgment of the ANSI Board of Standards Review, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made towards their resolution.

The use of American National Standards is completely voluntary; their existence does not in any respect preclude anyone, whether he has approved the standards or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standards.

The American National Standards Institute does not develop standards and will in no circumstances give an interpretation of any American National Standard. Moreover, no person shall have the right or authority to issue an interpretation of an American National Standard in the name of the American National Standards Institute. Requests for interpretations should be addressed to the secretariat or sponsor whose name appears on the title page of this standard.

CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken periodically to reaffirm, revise, or withdraw this standard. Purchasers of American National Standards may receive current information on all standards by calling or writing the American National Standards Institute.

Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OFMERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [http://www.atis.org/legal/patentinfo.asp] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

ATIS-0300075.2018, *Usage Data Management Architecture and Protocols Requirements for Packet-Based Application Services*

Is an American National Standard developed by the ATIS **Telecom Management and Operations Committee (TMOC)**.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

ATIS-0300075.2018

Revision of ATIS-0300075.2012

American National Standard for Telecommunications

Usage Data Management Architecture and Protocols Requirements for Packet-Based Application Services

Alliance for Telecommunications Industry Solutions

Approved March 2018

American National Standards Institute, Inc.

Abstract

This document describes a functional architecture and provides requirements intended for usage data management to be applied to various business applications for accounting and charging of packet-based telecommunications services.

Foreword

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The Telecom Management and Operations Committee (TMOC) – formerly T1M1 -- develops operations, administration, maintenance and provisioning standards, and other documentation related to Operations Support System (OSS) and Network Element (NE) functions and interfaces for communications networks - with an emphasis on standards development related to U.S.A. communication networks in coordination with the development of international standards.

ANSI guidelines specify two categories of requirements: mandatory and recommendation. The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, TMOC Secretariat, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time it approved this document, TMOC, which is responsible for the development of this Technical Report, had the following leadership:

P. Galarza, TMOC Chair (iconectiv)

Table of Contents

Table of Figures

American National Standard for Telecommunications –

Usage Data Management Architecture and Protocols Requirements for Packet-Based Application Services

1 Introduction

1.1 Background

Network Elements and Service Elements are often required to export usage information to facilitate accounting (e.g., billing functions) as well as non-accounting operations. Often usage information is stored in charging and accounting functions as log files (e.g., CDR files), and exported to external systems in batches (off-line charging). Today's rapidly evolving data networks also demand the availability of real-time and high-performance usage collection mechanisms that are related to on-line charging.

This document specifies the usage data management requirements and architecture that provide an integrated approach for meeting the demands of both on-line and offline charging for packet-based application services.

This standard was originally published as a Technical Report. Extensive revisions to the functional requirements, alignment with ITU-T Y.2233 and incorporation of revised technical content from ATIS-0300075.1 provide the rationale for promotion of this document to an American National Standard for usage data collection.

1.2 Scope & Purpose

This document specifies requirements and architecture for the collection and management of usage data for applications across packet-based networks. One purpose of this specification is to interpret and enhance ITU-T Recommendation Y.2233 in the North American context. It will additionally address protocol requirements for various reference points within the charging architecture.

Usage data is fundamental to ensuring customer charging and billing settlements reasonably correlate to the resources consumed to provide telecommunications services. Enhancements and refinements of Y.2233 will support various billing applications normally encountered in the North American context such as found in various supplier-partner relationships, including the following: retail, wholesale, and intercarrier billing settlements. Although usage data can also support non-accounting operations such as traffic management, fraud management, and market analysis, these will not be addressed in detail in this document.

The requirement to account for network and or service usage in real-time carries with it an unspoken requirement: high-performance. In this case, *high-performance* means the efficient use of capabilities of both the network and the network elements, such that the timely availability of usage records is possible even in situations where both the network and network elements are stressed by a high volume of traffic. Attaining such efficiency requires delivery protocols that minimize the overhead involved with delivering event messages and CDRs, while still enabling the reliable transfer of messages.

1.3 Target Billing Applications

The following are a service-independent set of charging applications that are considered in determining the requirements in this document. The target charging applications are:

- *Retail Billing* – The rendering of an invoice for charges due to a Service Provider by a Subscriber to their services, as per an agreed rate plan and service agreement.
- *Wholesale Billing* – The rendering of an invoice for charges due to a Network Operator from a Service Provider for access or transport services via which the Service Provider's services were delivered.
- *Intercarrier Settlement* – The process of assessing the periodic net charges due from one Service Provider to another for services rendered by each of the Service Providers on behalf of the other's Subscribers.

- *CDN Settlement* – The process of providing billing settlements between two Content Delivery Network owners.

In addition, CDRs described in this document can be used by the following management applications:

- *Internal Cost Accounting (e.g., Chargeback)* – Use of accounting information by a commercial Subscriber for separating the aggregate usage into sub-accounts associated with the enterprises' financial components.
- *Customer Care* – All those activities associated with the sustenance of satisfactory Subscriber service levels, including inquiries, account changes, restoral, and termination.
- *Marketing Information* – Demographic, financial, statistical, geographical, and temporal data used to aid in decision making and direction setting for product and services positioning and introduction by a Service Provider.
- *Law Enforcement Information Support* – Capture of targeted service usage entries, requested by a legal order for use by various agencies of law enforcement.
- *Fraud Detection* – Analysis of telecommunications service usage to identify potential abuse of network services.
- *Capacity Planning* – Predictive extension of existing usage patterns to allow for adequate resources to be staged in such a timeframe as to ensure continuity of agreed service levels.
- *Traffic Profiling* – Statistical portrayal of usage information for characterizing the patterns of usage levels and concentrations at nodal points and across transport boundaries.
- *Traffic Engineering* – Use of traffic profile information to manage the configuration of infrastructure resources so as to ensure service level continuity.
- *Performance Management* – Use of statistical data derived from network and service element telemetry to adapt the configuration of those elements to ensure service level continuity.
- *Revenue Assurance* – Any activity an organization performs to ensure that processes, practices, and procedures result in revenue that is billed and collected completely, accurately, and in a timely manner. This involves all areas of the organization, from customer care and network systems to invoicing and collections and finance, crossing all boundaries. Revenue leakage is revenue the company has earned, but has neither billed for nor collected. This revenue is lost. Revenue assurance includes *Fraud Abatement* – e.g., *Attack/Intrusion Detection*: the use of statistical and pattern recognition results to detect, prevent, and interdict in usage by Service Consumers not authorized for such usage by a Subscription agreement.
- *QoS Monitoring/SLA Management* – Use of all varieties of network and BSS data in the tracking and adaptation of network behavior to ensure service level continuity.

The generic requirements for all charging application types are specified in clauses 6 and 7.

Specific service requirements (such as VOIP) are not addressed in this document.

1.4 Relationship to Other Standards Activities

It is the intention of this standard (ATIS-0300075) to adopt the Functional Architecture and functional requirements approved by ITU-T Study Group 13 and found in ITU-T Y.2233. Exceptions are noted later in the document.

Other industry standards provide interface specifications corresponding to reference points within the Functional Architecture for which interoperable interfaces are desired. These standards are included in the reference list and noted in appropriate context within the document. In particular, for the IPDR solution of the TeleManagement Forum, informational Annex A provides a mapping between the functional architecture of Figure 5.1 and the IPDR solution.

2 Definitions, Acronyms, & Terminology

2.1 Definitions

For a list of common communications terms and definitions, please visit the *ATIS Telecom Glossary*, which is located at < http://www.atis.org/glossary >.

2.1.1 Acceptable CDR: CDRs that have been processed by a CAF without error, or where errors have been corrected by the CAF, are considered "acceptable" by the CAF for subsequent delivery to the Billing Domain. CDRs that have non-recoverable errors are not considered "acceptable" by the CAF.

2.1.2 Accounting: The process of collecting and analyzing service and resource usage metrics for the purposes of capacity and trend analysis, cost allocation, auditing, billing, etc. Accounting management requires that resource consumption be measured, rated, assigned, and communicated between appropriate business entities.

2.1.3 Call: A call is an informal term that refers to some communication between peers, generally set up for the purposes of a multimedia conversation.

2.1.4 Charging Data Record (CDR): Formatted collection of information about a potentially chargeable event (e.g., time of call set-up, duration of the call, amount of data transferred, etc.) for use in billing and accounting. For each party to be charged for parts of or all charges of a chargeable event a separate CDR is required to be generated – i.e., more than one CDR may be generated for a single chargeable event: e.g., because of its long duration, because more than one charged party is to be charged, or because more than one content-type is to be charged.

2.1.5: Chargeable Event: A collection of usage information that identifies network resources and related services for:

- User-to-user communication (e.g., a single call, a data communication session, or a short message); or
- User-to-network communication (e.g., service profile administration); or
- Inter-network communication (e.g., transferring calls, signalling, or short messages); or
- Mobility (e.g., roaming or inter-system handover); and
- Any other types of service activities the network operator may want to charge for.

At a minimum, this event not only characterizes the resource/service usage, but also indicates the identity of the involved end user(s).

2.1.6 Charging Event: Set of charging information forwarded by the Charging Trigger Function (CTF) towards the Charging Collection Function (CCF) (Offline Charging) or towards the Online Charging Function (OCF).

2.1.7 Correlation: The capability to generate an aggregated CDR by combining and analyzing chargeable events collected from the same transport/service session.

2.1.8 Error File: The logging of usage data records that cannot be processed in the normal way. The reasons records may not be processed include, but are not limited to, the following: missing mandatory data elements, attribute values outside of permitted range, and correlation failures. Error files allow subsequent processing to perform root cause analysis on high volume and high revenue impacting failures.

2.1.9 Network Element: An element in the transport stratum that is responsible for delivering bearer traffic associated with NGN services. Examples include: routers, gateways, network, and attachment systems.

2.1.10 Offline Charging: Charging mechanism where charging information does not affect, in real-time, the service rendered.

2.1.11 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 resource/session/service control is required.

2.1.12 Pull Mode: A file transfer delivery method where a “collector” requests the transfer of records from a CAF component.

2.1.13 Push Mode: A file transfer delivery method where one CAF component transmits records to another "collector/s" on a fixed, predictable schedule, or in response to an event.

2.1.14 Record Type: Indicates the purpose of the record. For example, session origination, interim recording, or session termination can be considered record types. Stand-alone events provide another example.

2.1.15 Service Element: An element in the service stratum that is responsible for providing end-users and applications with the NGN services they request. Examples include: application servers, web servers, and proxy servers.

2.1.16 Service Provider: An enterprise that provides communications-based services.

2.1.17 Service Type: Designates an NGN service category. For example, VoIP, IPTV, content delivery service, telepresence, virtual desktop, and virtual private network can be considered service types.

2.1.18 Session: From the SDP specification: "A multimedia session is a set of multimedia senders and receivers and the data streams flowing from senders to receivers. A multimedia conference is an example of a multimedia session."[1][2]

2.1.19 Template: A metadata expression defining a data structure.

2.1.20 Usage Record: The information associated with a charging event or CDR.

2.2 Abbreviations & Acronyms

3GPP	3rd Generation Partnership Project
ABMF	Account Balance Management Function
ACA	Accounting Answer (Diameter message)
ACR	Accounting Request (Diameter message)
AMA	Automatic Message Accounting
ASR	Abort Session Request (Diameter message)
ATIS	Alliance for Telecommunications Industry Solutions
AVP	Attribute Value Pair
CAF	Charging and Accounting Function
CCA	Credit-Control-Answer (Diameter message)
CCR	Credit-Control-Request (Diameter message)
CCF	Charging Collection Function
CDF	Charging Data Function
CDR	Charging Data Record
CGF	Charging Gateway Function
CTF	Charging Trigger Function
ECUR	Event Charging with Unit Reservation
FTP	File Transfer Protocol
IEC	Immediate Event Charging
IETF	Internet Engineering Task Force
IPGCF	Inter-Provider Charging Gateway Function

[1] IETF RFC 4566, *Session Description Protocol*.

[2] This differs slightly from the definition found in Y.2233: "Logical connection between parties involved in a packet-switched based communication.

NOTE – This term is used for IP connections rather than the term 'call' that is normally used for a connection over conventional (circuit switched) systems. A session can be composed of one or more unidirectional and/or bidirectional flows."

IP	Internet Protocol
IPDR	Internet Protocol usage data management specifications as defined by the TM Forum
ISO	International Standardization Organization
ITU-T	International Telecommunications Union – Telecommunications Standardization Section
NE	Network Element
NGN	Next Generation Network
OCF	Online Charging Function
QoS	Quality of Service
RAA	Re-Auth-Answer (Diameter message)
RAR	Re-Auth-Request (Diameter message)
RF	Rating Function
RFC	Request for Comment
SCUR	Session based Charging with Unit Reservation
TMF	TeleManagement Forum
TMN	Telecommunications Management Network
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VoIP	Voice over IP
XDR	External Data Representation

2.3 Requirements Terminology

The word **shall** will be understood as denoting a mandatory requirement. "Shall" will be used wherever the criterion for conformance with the specific recommendation requires that there be no deviation.

The word **should** will denote a recommendation. "Should" will be used wherever noncompliance with the specific recommendation is permissible.

The words **conditional mandatory** will denote a requirement for which the implementation is optional, but if it is implemented, shall be implemented in the exact manner specified.

The word **may** will denote an optional capability that may augment the standard. The standard is fully functional without the incorporation of this optional capability.

3 Assumptions

1. Policy management controls what usage events are accounted as chargeable events and how the chargeable events are mapped into Charging Data Records (CDRs).
2. Application of this specification may result in large numbers of usage records being generated, requiring economical storage, transport, and processing implementations. Several requirements stated below are intended to address this assumption.
3. No quantitative requirements regarding performance (end-to-end delay, transfer rate, etc.) or efficiency (message size, compression ratio, etc.) for the usage data collection processes are stated in Y.2233 or this document. These requirements will be defined by individual service operators.
4. The specification of authentication and authorization mechanisms for users is not in scope of this document.

4 Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

[1] ITU-T Recommendation Y.2233, *Requirements and framework allowing accounting and charging capabilities in NGN*.[3]

[2] TMF8000-IPDR-IIS-PS, *IPDR Streaming Protocol (IPDR/SP).*[4]

[3] 3GPP TS 32.240, *Telecommunication management; Charging management; Charging Architecture and Principles*.[5]

[4] 3GPP TS 32.295, *Telecommunication management; Charging management; Charging Data Record (CDR) transfer*.[5]

[5] 3GPP TS 32.297, *Telecommunication management; Charging management; Charging Data Record (CDR) file format and transfer*.[5]

[6] ITU-T Recommendation Y.2012, *Functional requirements and architecture of the NGN*.[3]

[7] RFC 6733, *Diameter Base Protocol.*[6]

[8] IETF RFC 3261, *Session Initiation Protocol* June 2002.[6]

[9] RFC 4006, *Diameter Credit Control Application*. [6]

[10] ATIS-0300276, *A Baseline of Security Requirements for the Management Plane*.[7]

[11] 3GPP TS 32.251, *Telecommunication management; Charging management; Packet Switched (PS) domain charging*.[5]

[12] 3GPP TS 32.296, *Telecommunication management; Charging management; Online Charging System (OCS) applications and interfaces*.[5]

[13] IETF RFC 4566, *Session Description Protocol.*[6]

[14] IETF RFC 2228, *FTP Security Extensions.*[6]

[15] TMF875-IPDR-IIS-PS, *Business Solution Requirements: Network Data Management – Usage.*[4]

[16] TMF8001-IPDR-IIS-PS, *IPDR/XDR Encoding Format*.[4]

[17] ITU-T Recommendation M.3020, *Management interface specification methodology*.[3]

[18] ITU-T Recommendation M.3010, *Principles for a telecommunications managed network*.[3]

[19] ATIS-1000018, *NGN Architecture.*[6]

[20] 3GPP TS 32.260, *Telecommunication management; Charging management; IP Multimedia Subsystem (IMS) charging*.[4]

[3] This document is available from the International Telecommunications Union. < http://www.itu.int/ITU-T/ >

[4] This document available from the TM Forum. < http://www.tmforum.org/ >.

[5] This document is available from the Third Generation Partnership Project (3GPP) at < http://www.3gpp.org/specs/specs.htm >.

[6] This document is available from the Internet Engineering Task Force (IETF). < http://www.ietf.org >

[7] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005. < https://www.atis.org/docstore/product.aspx?id=25578 >

5 Architecture Model

5.1 Architecture Components

Figure 5.1 presents the ATIS NGN Charging and Accounting Functions (CAF), architecture.[8] The NGN Service & Transport Functions, Charging and Accounting Functions, and Billing Domain indicated are presumed to belong to a single service provider.

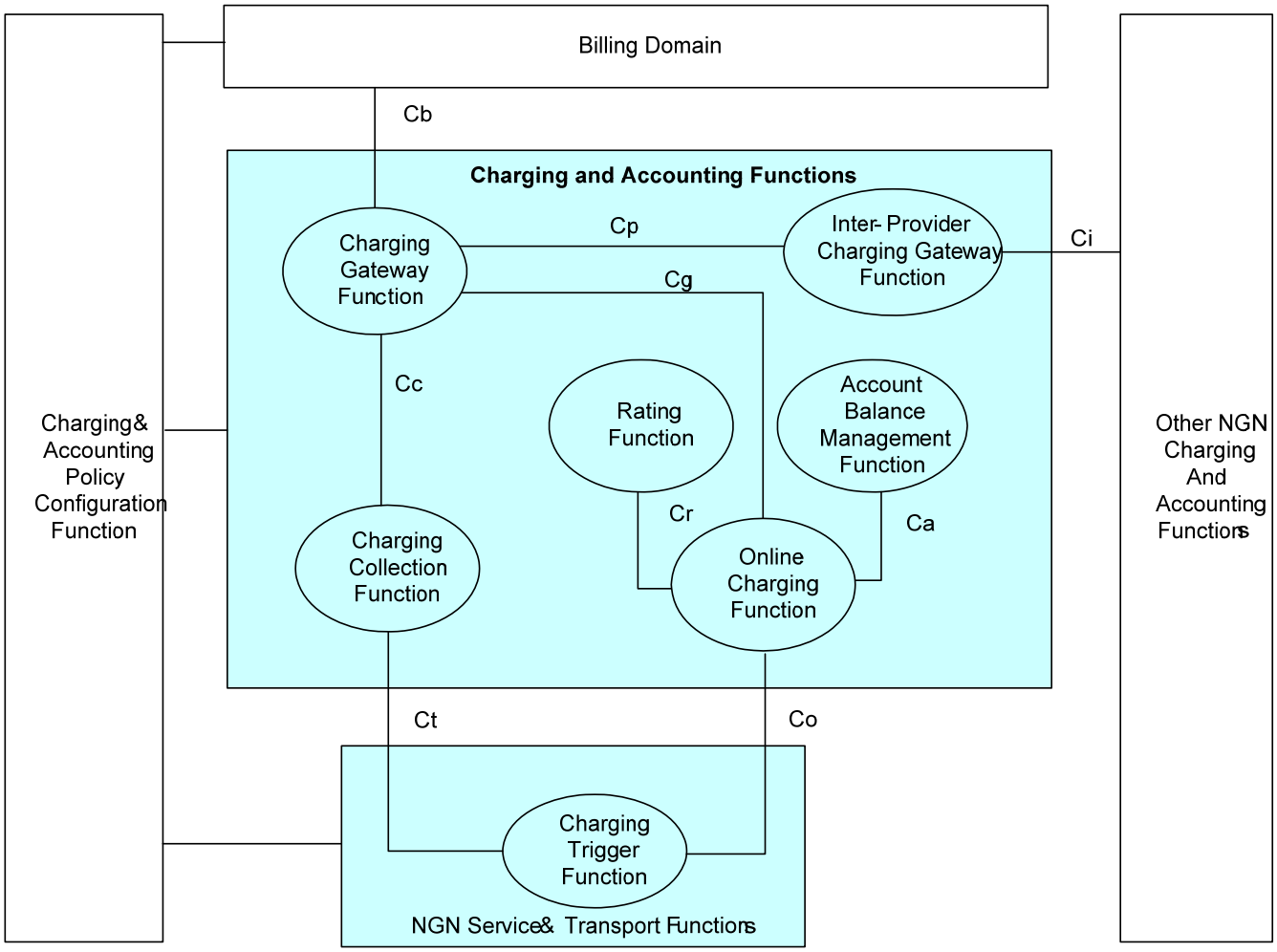

Figure 5.1 – Functional Architecture for NGN Charging and Accounting

The following is a general description of the entities that comprise the NGN CAF. Please refer to the latest versions of ITU-T Recommendations Y.2233 and Y.2012 for further descriptions.

A. Charging Trigger Function (CTF) – The CTF generates charging events based on the observation of network resource usage. In every network and service element that provides charging information, the CTF is the focal point for collecting information pertaining to chargeable events within the network element, assembling this information into matching charging events, and sending these charging events to the charging collection function for offline charging. The CTF is therefore a necessary component in all network elements that provide offline-charging functionality. It is also a necessary component for online charging since it sends charging events for real-time charging to the OCF and plays a key role in monitoring the use of network resources.

[8] This figure was originally presented in ITU-T Recommendation Y.2233 (01/2008).

B. Charging Collection Function (CCF)[9] – The CCF is used for offline charging. The CCF receives charging events from the CTF via the reference point Ct. It then uses the information contained in the charging events to construct charging data records (CDRs). The CCF also supports services which cannot simply be charged by event-based or session-based charging schemes. Some examples of additional charging schemes are data volume-based, flow-based, QoS-based, content-type-based, etc. The received data from the CTF is a record of a particular flow of user traffic that needs to be charged. Based on the received data, the CCF performs necessary analysis functions to identify the chargeable events beyond simple events and session state changes. The results of the CCF tasks are CDRs with well-defined content and format. The CDRs are later transferred to the billing domain through the CGF via the reference points Cc and Cb.

C. Online Charging Function (OCF) – The OCF supports session-based, event-based, and flow-based charging functions. The OCF receives charging events from the CTF via the Co reference point and executes in near real-time to provide authorization for the chargeable event or network resource usage requested by the authorized user. The CTF must be able to delay the actual resource usage until permission has been granted by the OCF. The OCF provides a quota for resource usage, which must be tracked by the CTF. The OCF responds to the charging requests from various users at the same time and provides a certain quota to each user. The quota is determined by default or by certain policies. Subsequent interactions may result in an additional quota being provided according to the subscriber's account balance, or they may result in no additional quota being provided, in which case the CTF must enforce termination of the end user's network resource usage.

The OCF shall have the capability to construct CDRs for delivery to the CGF for archival and post-rating purposes.

D. Rating Function (RF) – The RF specifically supports online charging. The RF determines the value of the network resource usage (described in the charging event received by the OCF from the network) on behalf of the OCF. To this end, the OCF furnishes the necessary information to the RF and receives the rating output. The RF calculates and reserves a number of non-monetary units such as service units, data volume, flow volume, time, and events. It then determines the price by calculating monetary units for a given number of non-monetary units. The RF calculates the price based on tariff information, the subscriber’s contractual terms, and the service being requested.

E. Account Balance Management Function (ABMF) – The ABMF stores the subscriber's account balance within the online charging system. The subscriber's account balance could be represented by the remaining available traffic volume (e.g., bytes), time (e.g., minutes for calling), or content (e.g., a movie), as well as credit. ABMF checks, updates, and reserves the account balance. It may also manage counters for online charging. Security and robustness should be emphasized by encrypting key data, providing backup and failure alarm capabilities, keeping detailed logs, and so forth.

F. Charging Gateway Function (CGF) – The CGF receives CDRs from the CCF and OCF via reference points Cc and Cg, respectively, in near-real time. It performs validation, consolidation, correlation, formatting, and error handling of CDRs. It manages the creation, deletion, and modifications of CDR files. It plays a gateway role between the NGN network and the billing domain or another NGN CGF. It uses the Cb reference point to transfer CDRs to the billing domain and the Cp reference point to transfer CDRs to IPCGF, which will further use that information for inter-provider charging information exchanges.

G. Inter-Provider Charging Gateway Function (IPCGF) – The IPCGF receives CDRs and other processed information from the CGF via the Cp reference point. It constructs CDRs for inter-provider charging settlement, including any additional information needed for inter-provider charging based on the settlement policy between the involved providers. It uses the Ci reference point to transfer further processed CDRs to another NGN IPCGF. The Ci reference point is used to communicate CDRs for the settlement of accounting rate between NGN service providers. It allows service providers exchange CDRs in real-time over standardized interfaces.

[9] 3GPP refers to ITU-T-defined CCF as Charging Data Function (CDF), and uses CCF to refer to combined CDF and CGF functionality. Figure 5.1 provides a logical functional architecture; combined functionality can be implemented in a single system.

In addition to these Functional Entities, revision 1 of Y.2233 (06/2010) provides further definition of logical entities that provide input to or receive information from the charging and accounting functions. These include the Billing Domain, other NGN accounting functions and policy functions. For example, the policy functions consist of policy enforcement, functional entity, policy decision functional entity, service user profile functional entity, and recharging applications.

5.2 Architecture Interfaces

The key reference points that define interfaces between the CAF entities are:

A. Reference point Ct – The Ct reference point is required to support interaction between the CTF and the CCF. The protocols crossing this reference point are required to support real-time transactions in stateless mode ("event-based charging") and stateful mode ("session-based charging") of operation. The following information flows across this reference point in real-time:

- Charging events for offline charging from the CTF to the CCF.
- Flow-based charging events for offline charging from the CTF to the CCF.
- Acknowledgements for these events from the CCF to the CTF.

B. Reference point Co – The Co reference point is required to support interaction between the CTF and the OCF. The protocols crossing this reference point are required to support real-time transactions in stateless mode ("event-based charging") and stateful mode ("session-based charging") of operation. The following information flows across this reference point in real-time:

- Charging events for online charging from the CTF to the OCF.
- Flow-based charging events for online charging from the CTF to the OCF.
- Response for these events from the OCF to the CTF. The response grants or rejects the network resource usage requested in the charging event, according to the decision taken by the OCF.

C. Reference point Cc – The Cc reference point supports interaction between the CCF and the CGF. The protocols crossing this reference point are required to support near real-time transactions by transferring one or more CDRs in a single message. The protocols should also support changeover to secondary destinations (alternate CGFs) in case of the primary CGF not being reachable. The following information flows across this reference point:

- CDRs are sent from the CCF to the CGF.
- Acknowledgements for these CDRs are returned from the CGF to the CCF.

The CDRs generated by the CCF contain the required charging information to be used for billing the customer.

D. Reference point Cg – The Cg reference point supports interaction between the OCF and the CGF. The protocols crossing this reference point are required to support near real-time transactions by transferring one or more CDRs in a single message. The protocols should also support changeover to secondary destinations (alternate CGFs) in case of the primary CGF not being reachable. The following information flows across this reference point:

- CDRs are sent from the OCF to the CGF.
- Acknowledgements for these CDRs are returned from the CGF to the OCF.

The CDRs generated by the OCF contain archival information intended to complement the real-time charging that has already occurred for the customer.

E. Reference point Cr – The Cr reference point supports interaction between the OCF and the RF in order to determine the value of chargeable events in terms of monetary or non-monetary units. The protocols crossing this reference point are required to support real-time transactions. The following information flows across this reference point:

- Price request message is sent from the OCF to the RF.
- Reply including price and usage counter information is returned from the RF to the OCF.

F. **Reference point Ca –** The Ca reference point supports the interaction between the OCF and the ABMF in order to access the account balance of the subscriber on the OCF.

G. **Reference point Cb –** The Cb reference point supports interaction between a CGF and the billing domain. The information crossing this reference point is comprised of CDR files. A common, standard file transfer protocol (e.g., FTP) is required to be used, including the transport mechanisms specified for the selected protocol.

H. **Reference point Cp –** The Cp reference point is required to support interaction between the CGF and the IPCGF. The protocols crossing this reference point are required to support near real-time transactions in stateful mode ("session-based charging") of operation. The following information flows across this reference point in real-time:
   – CDRs are sent from the CGF to the IPCGF.
   – Acknowledgements for these CDRs are returned from the IPCGF to the CGF.

I. **Reference point Ci –** The Ci reference point supports interaction between two IPCGFs in different service provider domains. The information crossing this reference point is comprised of CDR files, which are additionally processed for inter-provider settlement. A common, standard file transfer protocol or real-time protocol is required to be used, including the transport mechanisms specified for the selected protocol.

All usage accounting protocols crossing these reference points shall provide secure and reliable transport.

6 Usage Accounting Requirements Beyond Architecture Considerations

Sections 6 and 7 of ITU-T Recommendation Y.2233 provide critical functional requirements and objectives that the reader should consider to be part of this specification. The following functional requirements and objectives are provided as additional enhancements to those already contained in ITU-T Recommendation Y.2233.

6.1 Information Content

- **I-M-R001**: Information models shall be used to characterize usage attributes metered and collected on NGN Transport and Service Control resources[10].
- **I-M-R002**: The information specification shall indicate, for all usage attributes, if the information is required, optional, or conditional.

6.2 Data Modeling & Encoding

- **D-M-E-R001**: Data models for specific collection implementations shall be derived from the relevant information models according to standardized derivation for the collection protocol.
- **D-M-E-R002**: Data encoded from the information model shall preserve the semantics and typing specified in the information model.
- **D-M-E-R003**: Encoding shall employ rules amenable to computational efficiency.
- **D-M-E-R004**: Encoding shall employ rules amenable to transmission efficiency.

[10] Reference [18] provides a suitable framework to derive the requirements for the specification of TMN accounting management physical architectures from the TMN functional and information architectures. Reference [17] describes the methodology for a specification that is protocol neutral.

6.3 Data Recording

- **D-R-R001**: It shall be possible to synchronize timestamps generated by a recording process with Coordinated Universal Time (UTC). All charging events conveyed from the CTF to the CCF should include a UTC timestamp. It is an implementation decision of whether the timestamps presented in a CDR should be UTC or local time.
- **D-R-R002**: In case of an overload in the media plane, control plane, or OAM network, the recording process may change its behavior in order to cope with the lack of resources. Overload control mechanisms may include redundant collectors and local archiving. All implied configuration and behavior changes within network resources shall be accompanied with appropriate change notification(s) to management support systems.
- **D-R-R003**: The CCF and CGF mass storage should have sufficient capacity to store at least five average business days' busy season CDR data.
- **D-R-R004**: A single OCF, CCF, or CGF failure shall not cause the unrecoverable loss or corruption of more than 10,000 CDRs.
- **D-R-R005**: NE accounting functions shall be capable of creating new usage records, updating existing ones, computing usage statistics, deriving further usage properties, detecting usage expiration, and deleting usage records.
- **D-R-R006**: Where appropriate, a type of value/unit shall be specified to denote the unit of measure of an associated attribute value within the usage record or defined implicitly through a usage record template.
- **D-R-R007**:[11] Usage data shall not be overwritten or erased until acknowledged to be successfully transferred.

6.4 Data Transfer

- **D-T-R001**: Data transfer shall employ open standards-based protocol.
- **D-T-R002**: Data transfer shall account for each usage record.
- **D-T-R003**: Data transfer shall allow detection of missing usage data.
- **D-T-R004**: Data transfer shall allow for retransmission of usage data.
- **D-T-R005**: Retransmitted usage data shall either be marked so as to differentiate the retransmission from the original transmission or be known to not have been retransmitted by virtue of some implicit protocol mechanism.
- **D-T-R006**: The end-points' network resources and charging collectors can be located at different independent administrative domains. The data transfer protocol should work well and securely across multiple administrative domains.
- **D-T-R007**: The data transfer system (including charging collectors) shall be capable of detecting and removing duplicate records.
- **D-T-R008**: The data transfer solution shall provide network operator support for the monitoring of missing or duplicate usage data records through use of performance management parameters.
- **D-T-R009**: The NGN charging and accounting functions shall ensure the usage data are reliably transferred and received.
- **D-T-R010**: Data transfer shall reliably deliver usage data despite impairment or failure of underlying transport links.
- **D-T-R011**: At minimum, data transfer shall incur a loss of no more than 1 in 500,000 CDRs transferred between the CCF and the CGF, as well as between the CGF and the billing domain.

[11] When deleting usage data that has been successfully transferred, the usage data should be removed in chronological order starting with the oldest.

6.5 Security

- **S-M-R001**: Management systems and network elements of Accounting Management implementations that follow the architecture specified in this document and that comply with the requirements specified in this document shall also conform to the security standards and practices set forth in OAM&P Security Requirements for the Public Telecommunications Network: ATIS-0300276.2008, *A Baseline of Security Requirements for the Management Plane* [10].
- **S-M-R002**: Management systems and transport and control resources providing Accounting Management implementations shall support fraud management procedures and fraud control. These shall include capabilities to support establishment of limits for accumulated charges from visitors from other Telecommunications Management Network (TMN) entities, timely collection of usage charges, and authentication of end users.

6.6 Other Operations & Administrative Considerations

- **O-A-M-R001**: It shall be possible for the operator to define different time intervals for the collection and the processing of charging information (e.g., real time, short time, other regular intervals).
- **O-A-M-R002**: Accounting Management implementations and their management systems shall support the collection of performance monitoring data to validate all charging collection and forwarding functionality. Depending on implementation architectures, this includes counts for accounting messages and CDRs created, sent, received, and lost.
- **O-A-M-R003**: Accounting and Policy implementations and their management systems shall support configuration of charging policies. In particular, the implementation shall allow the provisioning of different policies according to the QoS of the call, session, or event.
- **O-A-M-R004**: The OCF, CCF, and CGF functional components shall support the creation of error files. These error files shall not be overwritten due to overload considerations unless the content has been successfully transferred to its intended destination or stored in an archive.
- **O-A-M-R005**: The maintenance of any functional component of the charging mediation layer shall not cause any loss or corruption of CDRs.
- **O-A-M-R006**: The CGF functional component shall support the creation of error files for unacceptable CDRs and performance counters that record the number of unacceptable CDRs within certain intervals of time, such as fifteen minutes, sixty minutes, and/or twenty-four hours. The CGF functional component shall also support the setting of thresholds for these counters and threshold crossing alerts when the thresholds have been exceeded.
- **O-A-M-R007**: The usage data recording, collection, and reporting functionality will adhere to federal and state/province legal and regulatory requirements.

7 Protocol Requirements & Guidelines

Protocol requirements differ based on the reference point at which the protocol will be used. The high-level requirements presented in clause 6 for information content, data modeling and encoding, and data transfer apply to all reference points within the NGN Charging and Accounting Architecture. The protocol requirements presented in this clause are specific to four reference points[12]:

a. The Ct reference point for exchanging event messages and acknowledgements between the CTF and the CCF (designated by the code “Ct” preceding the requirement number).

b. The Co reference point for exchanging event messages and acknowledgements between the CTF and the OCF (designated by the code “Co” preceding the requirement number).

[12] Protocol requirements for other NGN Charging and Accounting reference points may be added in future issues of this specification.

c. The Cc reference point between the CCF and CGF (designated by the code “Cc” preceding the requirement number).

d. The Cb reference point between the CGF and Billing Domain (designated by the code “Cb” preceding the requirement number).

In order to isolate technical aspects unique to various views of a protocol, this specification discusses the information objects intended for messages, requirements for the encoding scheme used to represent instances of information objects at each reference point, and requirements for data transfer across the specified reference point.

7.1 Protocol Requirements for the Ct Reference Point

The protocol requirements for the Ct reference point between the CTF and CCF are predominantly based on the Diameter application requirements for offline charging specified in 3GPP TS 32.299 and IETF RFC 6733, *Diameter Base Protocol*.

Ct-P-R001: Interface implementations for the Ct reference point for offline charging shall employ Diameter protocol as defined in IETF RFC 6733.

7.1.1 Information Content and Encoding: Ct Reference Point

- **Ct-I-C-E-R001**: For offline charging, event and session based charging are performed by the use of the following fundamental Diameter Accounting operations:
    - *Accounting Request (ACR)*; sent from CTF → CCF.
      After detecting a chargeable event, the CTF sends an ACR to the CCF.
    - *Accounting Answer (ACA)*; sent from CCF → CTF.
      After receiving an ACR, the CCF sends an ACA to the CTF to inform the CTF that charging data was received.
        - The ACR and ACA correspond to the 3GPP *Charging Data Request* and *Charging Data Response* operations, as specified in TS 32.299.
- **Ct-I-C-E-R002**: For offline charging purposes (Ct reference point), two cases of Charging shall be supported:
    - Session based charging; and
    - Event based charging.
- **Ct-I-C-E-R003**: The Diameter *Accounting Request (ACR)* types START, INTERIM, and STOP shall be used for accounting data related to successful sessions.
- **Ct-I-C-E-R004**: The Diameter EVENT ACR type shall be used for all event based charging. EVENT accounting data, which is unrelated to sessions, 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 following requirements (Ct-I-C-E-R005 through Ct-I-C-E-R007) describe key data elements to be included in ACR messages.

- **Ct-I-C-E-R005**: The following Diameter Accounting Attribute Value Pairs (AVPs) shall be present in each ACR message, as required per IETF RFC 6733:
- **Session-Id** (This field identifies the operation session.)
- **Origin-Host** (This field contains the identification of the source point of the operation and the realm of the operation originator.)
- **Origin-Realm** (This field contains the realm of the operation originator.)

- **Destination-Realm** (This field contains the realm of the operator domain. The realm will be addressed with the domain address of the corresponding public URI.)
- **Accounting-Record-Type** (This field defines the transfer type: event for event based charging and start, interim, stop for session based charging.)
- **Accounting-Record-Number** (This field contains the sequence number of the transferred messages.)
- **Other optional Diameter Base Protocol AVPs**, as specified in RFC 6733, may also appear in the ACR message.Ct-I-C-E-R006: In addition to the AVPs listed in Ct-I-C-E-R005, the ACR for session-based charging shall include vendor-specific AVPs to convey the following types of information:
- **Ct-I-C-E-R006**: Information:
    - Originating user identification for the session (e.g., calling party number or URL).
    - Requested user or application for the session (e.g., called party number or URL).
    - Session start time (for inclusion in the START_RECORD ACR).
    - Session end time (for inclusion in the STOP_RECORD ACR).
    - Call answer indication (for call sessions).
    - Charged party identification (if different than the originating user).
    - Release cause (for inclusion in the STOP_RECORD ACR).
        - Depending on the nature of the session, additional information, such interconnecting carrier identification or number portability indicators, might also be required.
- **Ct-I-C-E-R007**: In addition to the AVPs listed in Ct-I-C-E-R005, the ACR for event-based charging should include vendor-specific AVPs to convey the following types of information:
    - Originating user identification for the event.
    - Requested user or application for the event.
    - Service Identifier (e.g., call forwarding, toll free service query, video conferencing, video on demand).
    - Type of event (e.g., registration, activation, deactivation, interrogation/data base query, invocation).
    - Event time stamp (i.e., indication of the time that the usage event ocurred).
- **Ct-I-C-E-R008**: The following Diameter Accounting Attribute Value Pairs (AVPs) shall be present in each ACA message, as required per IETF RFC 6733:
    - Session-Id (This field identifies the operation session.).
    - Result-Code (This field contains the result of the specific query.)
    - Origin-Host (This field contains the identification of the source point of the operation and the realm of the operation originator.)
    - Origin-Realm (This field contains the realm of the operation originator.)
    - Accounting-Record-Type (This field defines the transfer type: event for event based charging and start, interim, stop for session based charging.)
    - Accounting-Record-Number (This field contains the sequence number of the transferred messages.)

Other optional Diameter Base Protocol AVPs, as specified in RFC 6733, may also appear in the ACA message.

7.1.2 Data Transfer: Ct Reference Point

- **Ct-D-T-R001**: For non-integrated solutions, each CTF shall have a CCF 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.
- **Ct-D-T-R002**: The CTF shall send charging event information to the CCF in real time as each chargeable event is detected.

- **Ct-D-T-R003**: When the connection towards the primary CCF is broken, the process of sending accounting information should continue towards a secondary CCF (if such a CCF is configured).
- **Ct-D-T-R004**: If no CCF is reachable, the network element may buffer the generated accounting data in non-volatile memory. Once the CCF connection is working again, all accounting messages stored in the buffer is sent to the CCF, in the order they were stored in the buffer.
- **Ct-D-T-R005**: 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 should execute the connection failure procedure as specified in Ct-D-T-R003 and Ct-D-T-R004.
- **Ct-D-T-R006**: If retransmitted ACRs are sent, they are marked with the T-flag as described in RFC 6733, in order to allow duplicate detection in the CCF.
- **Ct-D-T-R007**: If the CCF receives a message that is marked with the T-flag as retransmitted and this message was already received, then it shall discard the duplicate message. However, if the original of the re-transmitted message was not yet received, the CCF shall use the information in the marked message when generating the CDR. The CCF shall mark all CDRs that use information from duplicated message(s).

7.2 Protocol Requirements for the Co Reference Point

The protocol requirements for the Co reference point between the CTF and OCF are predominantly based on the Diameter application requirements for online charging specified in 3GPP TS 32.299 and IETF RFC 4006, *Diameter Credit Control Application.*

Co-P-R001: Interface implementations for the Co reference point for online charging shall employ Diameter credit control protocol as defined in IETF RFC 4006.

7.2.1 Information Content and Encoding: Co Reference Point

- **Co-I-C-E-R001**: On-line credit control shall use the following Diameter Accounting operations:
    - *Credit-Control-Request (CCR)*; sent from CTF → OCF. After receiving a service request from the subscriber, the CTF sends a CCR to the OCF. The CTF may either specify a service identifier (centralized unit determination) or the number of units requested (decentralized unit determination).
    - *Credit-Control-Answer (CCA)*; sent from OCF → CTF. After receiving a CCR, the OCF replies with a CCA, which informs the CTF of the number of units granted as a result of the CCR. This includes the cases where the number of units granted indicates the permission to render the requested service, where a reservation is made of the requested resource units, or where the requested service is denied by the OCF.

      The CCR corresponds to the 3GPP *Debits Unit Request* and *Reserve Units Request* operations, as specified in TS 32.299. The CCA corresponds to the 3GPP *Debits Unit Response* and *Reserve Units Response*, as specified in TS 32.299.
- **Co-I-C-E-R002**: Three cases for control of user credit for online charging shall be supported, as described in 3GPP TS 32.240:
    - Immediate Event Charging (IEC);
    - Event Charging with Unit Reservation (ECUR); and
    - Session Charging with Unit Reservation (SCUR).
- **Co-I-C-E-R003**: In the case of IEC, the credit control process for events is controlled by the corresponding *CC-Request-Type* EVENT_REQUEST that shall be sent with the Diameter CCR for a given credit control event.

- **Co-I-C-E-R004**: In the case of ECUR, a CCR with the *CC-Request-Type* INITIAL_REQUEST shall be used to make a reservation of service units prior to service delivery, and the usage of service units is committed on execution of a successful delivery. The *CC-Request-Type* TERMINATION_REQUEST shall be used to release unused service units that have previously been reserved.
- **Co-I-C-E-R005**: SCUR is used for credit control of sessions and shall use CCRs with the *CC-Request-Type* values of INITIAL_REQUEST, UPDATE_REQUEST, and TERMINATION_REQUEST.
- **Co-I-C-E-R006**: The Tariff-Time-Change AVP shall be used to determine the time of the tariff change as described by RFC 4006. The Tariff-Change-Usage AVP shall be used within the Used-Service-Units AVP to distinguish reported usage before and after the tariff time change. In addition to the scenarios described in RFC 4006, the Tariff-Time-Change AVP may also be used in the context of continuously time-based charging. If appropriate to the tariff policy, changes to the tariffs pertaining to the service during active user sessions may alternatively be handled using the Validity-Time AVP.
- **Co-I-C-E-R007**: When allocating resources, the OCF may instruct the CTF to re-authorize the quota upon a number of different session-related triggers that can affect the rating conditions, such as end user QoS changes or location updates. The OCF shall instruct the CTF to monitor for such events by using the Trigger AVP containing one or more Trigger-Type AVPs in the CCA command.
- **Co-I-C-E-R008**: When the CTF detects a reauthorization trigger, it shall send a Diameter Re-Auth-Request (RAR) to the OCF. The CTF shall send the RAR even if all previously granted service units have not been used and shall include a report of the current service usage quota. The basic structure and content of a Diameter RAR as used for online charging is shown in Table 6.4.4 of 3GPP TS 32.299.
- **Co-IC-E-R009**: The OCF shall respond to each RAR by sending a Diameter *Re-Auth-Answer* (RAA) to the requesting CTF. The basic structure and content of a Diameter RAA as used for online charging is shown in Table 6.4.5 of 3GPP TS 32.299.
- **Co-I-C-E-R010**: The CTF shall be able to report the quota usage on a periodic basis or under other circumstances if instructed by the OCF or through other mechanisms such as policy control. When this happens, the reason for the quota being reported is notified to the OCF through the use of the Reporting-Reason AVP in the CCR. The reason for reporting credit usage can occur directly in the Multiple-Services-Credit-Control AVP, or in the Used-Service-Units AVP, depending on whether it applies for all quota types or a particular quota type respectively. When the reason is RATING_CONDITION_CHANGE, the CTF shall include the Trigger AVP in the CCR to indicate the specific armed trigger events which caused the reporting and re-authorization request (per section 6.5.1.3 of TS 32.299).
- **Co-I-C-E-R011**: The OCF should have the capability to include an indication to the client of the remaining quota threshold that shall trigger a quota re-authorization as part of the Multiple-Services-Credit-Control AVP. See section 6.5.2 of TS 32.299 for further information concerning quota threshold parameters.
- **Co-I-C-E-R012**: Re-authorizations of multiple active resource quotas within a Diameter credit control session shall be achieved using a single Diameter *Credit Control Request/Answer* message sequence. New quota allocations received by the NE/CTF shall override any remaining held quota resources after accounting for any resource usage while the re-authorization was in progress.
- **Co-I-C-E-R013**: Instead of requesting re-authorization, the OCF may directly indicate that a service should be terminated upon reaching a quota threshold. The OCF shall have the capability to indicate the conditions under which termination occurs by including the Final-Unit-Indication AVP with the value TERMINATE in the CCA.
- **Co-I-C-E-R014**: Based on customer account balance notification, a customer may interact with a recharging application in order to increase available credit so that session termination can be avoided. The recharging application informs the account balance management function which in turn informs the OCF of the updated available credit. The OCF shall have the capability to send a reauthorization request to the CTF updating the quota units allowed.
- **Co-I-C-E-R015**: The OCF should have the capability to inform the CTF via the CCA message that the service shall be stopped after a period of end user inactivity. The OCF shall indicate the time-out period by including the Quota-Consumption-Time AVP in the CCA as described in section 6.5.4 of TS 32.299.
- **Co-I-C-E-R016**: If the OCF does not have a pending request from the CTF, and has determined that a service requires termination, the OCF shall send a Diameter Abort Session Request (ASR) message to the

CTF to terminate the session related to the service. On reception of an ASR, the CTF shall close the associated Credit-Control session and send a CCR [TERMINATE] to the OCF. (See section 6.5.5 of TS 32.299.)

- **Co-I-C-E-R017**: If the OCF has determined that a session requires termination and has a pending request from the CTF, the OCF shall return a CCA with Result-Code AVP with value DIAMETER-AUTHORIZATION-REJECTED. Upon receipt of the CCA, the CTF shall close the associated Credit-Control session. (See section 6.5.5 of TS 32.299.)

The following requirements (Co-I-C-E-R018 through Ct-I-C-E-R021) describe key data elements to be included in CCR and CCA messages.

- **Co-I-C-E-R018**: The following Diameter Accounting Attribute Value Pairs (AVPs) shall be present in each CCR message, as required per IETF RFC 6733:
    - *Session-Id* (This field identifies the operation session.)
    - *Origin-Host* (This field contains the identification of the source point of the operation and the realm of the operation originator.)
    - *Origin-Realm* (This field contains the realm of the operation originator.)
    - *Destination-Realm* (This field contains the realm of the operator domain. The realm will be addressed with the domain address of the corresponding public URI.)
    - *Auth-Application-Id* (The field corresponds to the application ID of the Diameter Credit Control Application and is defined with the value 4.)
    - *Service-Context-Id* (This field indicates the supported protocol version.)
    - *CC-Request-Type* (This field defines the transfer type: EVENT_REQUEST, INITIAL_REQUEST, UPDATE_REQUEST, or TERMINATE_REQUEST.)
    - *CC-Request-Number* (This field contains the sequence number of the transferred messages.)
    - Other optional Diameter Base Protocol AVPs, as specified in RFC 6733, may also appear in the CCR message.
- **Co-I-C-E-R019**: In addition to the AVPs listed in Co-I-C-E-R017, the CCR shall include vendor-specific AVPs to convey the following types of information:
    - Originating user identification (e.g., calling party number or URL).
    - Requested user or application (e.g., called party number or URL).
    - Timestamp for the event that has resulted in the CCR generation (charge event or session initiation, update or termination).
    - Call answer indication (for call sessions).
    - Rating Request Type (e.g., price request, tariff request).
    - Service-specific data (service-Id, QoS, etc.).
    - Service usage counters data (e.g., SMS/MMS message counts, data usage volume, used time units, etc.).
    - Release cause (for inclusion in a termination CCR).
    - Depending on the nature of the session or event related to the credit control request, additional information, such as roaming service provider identification or number portability indicators for call sessions, might also be required.
- **Co-I-C-E-R020**: The following Diameter Accounting Attribute Value Pairs (AVPs) shall be present in each CCA message, as required per IETF RFC 6733:
    - *Session-Id* (This field identifies the operation session.)
    - *Result-Code* (This field contains the result of the specific query.)

- *Origin-Host* (This field contains the identification of the source point of the operation and the realm of the operation originator.)
- *Origin-Realm* (This field contains the realm of the operation originator.)
- *Auth-Application-Id* (The field corresponds to the application ID of the Diameter Credit Control Application and is defined with the value 4.)
- *CC-Request-Type* (This field defines the transfer type: event for event based charging and initial, update, terminate for session based charging.)
- *CC-Request-Number* (This field contains the sequence number of the transferred messages.)

- **Co-I-C-E-R021**: In addition to the AVPs listed in Co-I-C-E-R020, the CCA shall include Diameter and vendor-specific AVPs to convey the following information, as appropriate to the session or event associated with the Credit Control Request:
  - Multiple-Services-Credit-Control (used for service and traffic quota management).
  - Granted service units (time, octets, message counts).
  - Low balance indication.
  - Remaining balance.

7.2.2 Data Transfer: Co Reference Point

- **Co-D-T-R001**: The CTF shall stream charging event and credit request information to the OCF in real time upon detection of each chargeable event and credit request trigger.
- **Ct-D-T-R002**: The CTF and OCF shall follow the failure handling procedures in IETF RFC 6733, *Diameter Base Protocol*, and RFC 4006, *Diameter Credit Control Application*.
  - These procedures apply to handling of error responses, recovery from connection failures, etc. The *Credit-Control-Failure-Handling* AVP as defined in RFC 4006 determines what to do if the sending of Diameter credit-control messages to the OCF has been temporarily prevented. The usage of *Credit-Control-Failure-Handling* AVP gives flexibility to have different failure handling for credit-control sessions.
- **Co-D-T-R003**: The CTF shall use the Tx timer (defined in RFC 4006) to limit the waiting time for an answer to the CCR sent to the OCF. When the Tx timer elapses, the CTF shall take action to the end user according to the value of the *Credit-Control-Failure-Handling* AVP.
- **Co-D-T-R004**: Each CTF shall have an 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 at the first address is not available (e.g., out of service), then the CTF shall send the charging information to the secondary address and so on.
- **Co-D-T-R005**: As defined in RFC 4006, if a failure occurs during an ongoing credit-control session, the CTF shall move the credit control message stream to an alternative OCF, if the primary OCF indicated FAILOVER_SUPPORTED in the *CC-Session-Failover* AVP. In case CC-Session-Failover AVP is set to FAILOVER_NOT_SUPPORTED, the credit control message stream is not moved to a backup OCF.
  - In the case of FAILOVER_NOT_SUPPORTED, the operator has the option to either specify that the service session shall be terminated or allow the session to continue without credit control based on the value of the *Credit-Control-Failure-Handling* AVP.
- **Co-D-T-R006**: When a connection failure is detected for new credit control sessions, the CTF shall perform failover to an alternative OCF if possible. For instance, if an implementation of the CTF can determine primary OCF unavailability, it can establish the new credit control sessions with a possibly available secondary OCF.
- **Co-D-T-R007**: The CTF shall mark the request messages that are retransmitted after a link fail over as possible duplicates with the T-flag as described in RFC 6733.
- **Co-D-T-R008**: The OCF shall be able to detect duplicate request messages.

- 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 (as opposed to all-against-all record checking). The OCF may perform a duplicate request check based on inspection of the *Session-Id* and *CC-Request-Number* AVP pairs and the state machine of the OCF.

7.3 Protocol Requirements for the Cc Reference Point

The protocol requirements for the Cc reference point between the CCF and CGF are based on offline charging concepts specified for 3GPP, IPDR, and Automatic Message Accounting (AMA) procedures established for usage accounting.

7.3.1 Information Content and Encoding: Cc Reference Point

- **Cc-I-C-E-R001**: The CCF shall extract information from charging event messages to create CDRs according to a specific data template based on the service type.
- **Cc-I-C-E-R002**: Each CDR shall contain a minimum set of information required data fields. These data fields shall include the following types of information:
  - Template ID or code[13] (required if a compact record format is being used).
  - Service type.
  - Requesting user identification (e.g., calling party number).
  - Requested entity identification (e.g., called party number).
  - Recording entity identification.
  - Event timestamp(s), including session "start" and "stop" timestamps (or start timestamp plus duration) when session charging applies.
  - Resource usage (e.g., packet counts, byte counts, seconds of use).
- **Cc-I-C-E-R003**: The CDR template shall be extensible, permitting the addition of data fields and service specific usage attributes as packet-based application services evolve. This would include new services, messaging, and attributes as required to support NGN services billing, fraud detection, performance management, and other aspects of OAM&P.
- **Cc-I-C-E-R004**: Meta-data should be used to describe the charging information structure irrespective of the choice of transfer protocol for the Cc reference point.
- **Cc-I-C-E-R005**: The CGF shall perform semantical and/or syntactical sanity checks on CDRs received from the CCF. If the CGF determines that a CDR parameter's value is not well formatted, or otherwise incorrect, then the defective CDR parameter value(s) shall be replaced with an appropriate flag value conforming to an agreed syntax allowed for that parameter (assuming such a flag or default value is available). Once the flag value replacement has occurred, the CDR shall be deemed acceptable by the CGF.

7.3.2 Data Transfer: Cc Reference Point

- **Cc-D-T-R001**: The CCF shall transfer CDRs to the CGF using one of the following data transport mechanisms:
  - Streaming Protocol (e.g., GTP' and IPDR, see references [4] and [2] respectively).

[13] The use of templates makes it possible for each CDR to contain only the actual data values for each usage event without having to include any data descriptors such as field names, types, and length in each usage record; this significantly reduces the volume of information sent over communication links.

- File Transfer Protocol (FTP), per RFC 959.
- FTP with secure extensions, per RFC 2228.

- **Cc-D-T-R002**: Any streaming protocol shall allow the encoding of charging information for transfer even if all the information is not yet in memory.
- **Cc-D-T-R003**: Any streaming protocol shall allow the decoding of charging information prior to reading to the end of the CDR being conveyed.
- **Cc-D-T-R004**: Any streaming protocol shall allow the transfer of different types of CDRs concurrently.
- **Cc-D-T-R005**: Any streaming protocol shall support the single collection point of charging information from sources employing multi-version and multi-CDR record structures.
- **Cc-D-T-R006**: Any streaming protocol should be backwards compatible, with reference to releases of the protocol.
- **Cc-D-T-R007**: For streaming protocols, the CCF shall continue to stream new sets of CDRs to the CGF, regardless of whether previous CDRs have been acknowledged, as long as the CGF sends intermittent CDR acknowledgements based on an established CDR transmission policy that defines acknowledgement procedures.
- **Cc-D-T-R008**: Any file transfer collection process shall support "Push Mode". The file transfer collection process shall optionally support "Pull Mode"[14].
- **Cc-D-T-R009**: Each CCF should have an O&M configurable address list of CGFs (Charging Gateways) to which it can send its CDRs. The list shall be organized in CGF address priority order. If the primary CGF is not available (e.g., out of service), then the CCF shall send the CDRs to the secondary CGF and so on.
- **Cc-D-T-R010**: The protocol shall support the association of a sequence number, or its equivalent, for every set of CDRs to be transferred. The CGF shall acknowledge each set received from the CCF. Each acknowledgement shall refer to the sequence number or its equivalent.
- **Cc-D-T-R011**: The Cc reference point shall provide a mechanism to prevent duplicate CDRs that might arise during redundancy operations, or to mark CDRs that have been retransmitted.

7.4 Protocol Requirements for the Cb Reference Point

The protocol requirements for the Cb reference point between the CGF and Billing Domain are based predominantly on CDR file transfer principles specified in 3GPP TS 32.297 and established industry procedures.

7.4.1 Information Content and Encoding: Cb Reference Point

- **Cb-I-C-E-R001**: The CGF shall be capable of transferring files with CDRs to multiple destinations within the Billing Domain.
- **Cb-I-C-E-R002**: The CGF shall determine which CDRs are placed in which CDR file based on Cb routing criteria such as CDR origin and other CDR parameters.[15] The file name shall, within the limits of the file naming conventions, contain an indication of the CDR routing filter applied.
- **Cb-I-C-E-R003**: The CGF shall package "acceptable" CDRs (those without errors or with errors that have been corrected) in files for transfer to the designated Billing Domain destination(s) via the Cb.
- **Cb-I-C-E -R004**: Each CDR file shall contain all "acceptable" CDRs received and processed by the CGF between the closure of the previous file and the closure of the current file.

[14] See definitions found in section 2.1.

[15] A routing filter is constructed from the routing criteria.

- **Cb-I-C-E-R005**: When generating a CDR file, the CGF shall close the CDR file and prepare it for transfer to the Billing Domain based on any of several conditions:
    - A configurable file size limit;
    - A configurable file closure time;
    - A configurable file lifetime ("interval");
    - A configurable number of CDRs within the file;
    - CDR release, version or encoding change;
    - Manual OAM&P actions;
    - Billing Domain requests;
    - Other system defined reasons (e.g., file system full).
- **Cb-I-C-E-R006**: Each CDR file shall contain a header section followed by a variable sized CDR data section. The CDR data section shall contain zero or more concatenated CDRs. Each CDR in a file shall include a header indicating the CDR length, encoding scheme, CDR template, and relevant release/version identifiers.
- **Cb-I-C-E-O006**: The CGF should support the customization of CDR files to be forwarded based on application logic concerning the billing application recipient.
- **Cb-I-C-E-R007**: The CGF shall identify and delete duplicate CDRs before delivering CDR files to the Billing Domain.

7.4.2 Data Transfer: Cb Reference Point

- **Cb-D-T-R001**: At minimum, the Cb Reference Point shall support use of the File Transfer Protocol (FTP) defined in RFC 959 for CDR file transport.

  NOTE: Other protocols such as the IPDR Streaming Protocol [2] may also be used.
- **Cb-D-T-R002**: The file transfer mechanism shall support “Push Mode”. The file transfer mechanism may optionally support “Pull Mode”.
- **Cb-D-T-R003**: The CGF shall transfer each CDR file to the Billing Domain under one of the following conditions, as determined based on the charging and accounting policy:
    - Immediate transfer to the Billing Domain upon file closure;
    - Transfer to the Billing Domain based on pre-defined schedule;
    - The Billing Domain has issued a command requesting file transfer;
    - OAM&P action to force CDR file transfer.
- **Cb-D-T-R004**: The CGF shall store each CDR file until one of the following occurs, based on the charging and accounting policy:
    - The Billing Domain has acknowledged receipt of the CDR file;
    - The CGF file system storage limit has been reached and notification has been transmitted;
    - The file age in the CGF has reached a configurable limit;
    - OAM&P action, scheduled or on demand.
- **Cb-D-T-R005**: The protocol shall support the association of a sequence number, or its equivalent, for every file of CDRs to be transferred. The CGF shall process acknowledgements from the Billing Domain with reference to the sequence number or its equivalent.
- **Cb-D-T-R006**: The file header shall contain at minimum the following components:
    - Identification of the CGF;

- Destination in Billing Domain;
- File sequence number;
- File creation timestamp;
- Number of records in files;
- File length;
- Identification of CDR templates used.

- **Cb-D-T-O007**: The file header should contain the following components:
  - Timestamp for most recent CDR in file;
  - Timestamp for oldest CDR in file.

Annex A

(informative)

A IPDR Reference Model

A.1 IPDR Reference Model Overview

The IPDR Reference Model defines a framework for exchanging usage records between IPDR-enabled devices or systems. The IPDR Reference Model is maintained by the TeleManagement Forum (TMF). Figure A.1 shows the key elements and interfaces found within the IPDR Reference Model (see reference [15]).

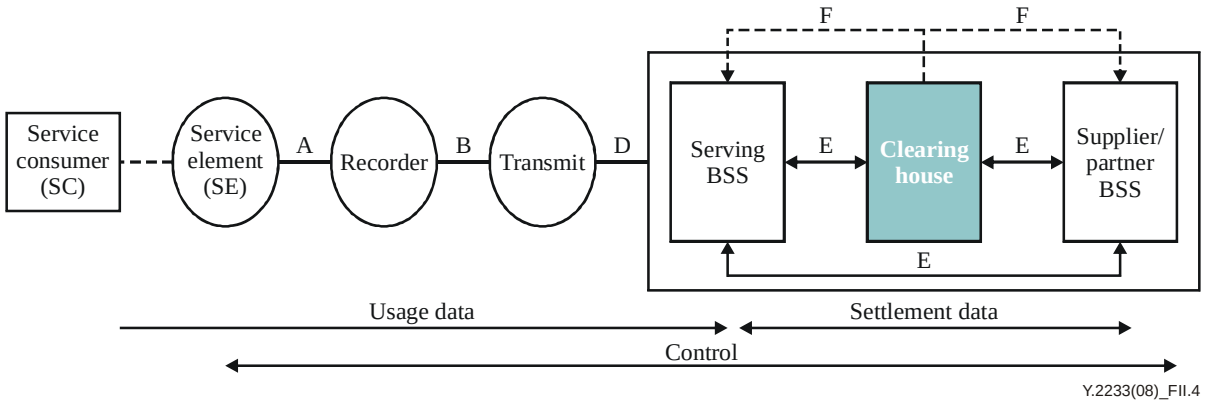

Figure A.1 – IPDR Reference Model

A.2 Mapping of the IPDR Reference Model interfaces to ITU-T Recommendation Y.2233 reference points

The following describes a mapping between major reference points of the ITU-T Y.2233 Functional Architecture of Charging and Accounting in NGN release 1 (described in clause 5 of this document) and the IPDR Reference Model interfaces shown above:

- The ITU-T Y.2233 “Ct” and “Co” interfaces between the NGN Service and Transport Functions and the Charging and Accounting Function are collectively termed "Interface A" by the IPDR Reference Model.
- The ITU-T Y.2233 “Cc” and “Cg” interface between the Charging Collection Function and Online Charging Function (collectively called “Recorder” by the IPDR Reference Model) and the Charging Gateway Function (CGF, that is termed “Transmitter” by the IPDR Reference Model) are collectively termed "Interface B" by the IPDR Reference Model.
- The ITU-T Y.2233 “Cb” interface between the CCF and the billing domain is termed "Interface D" by the IPDR Reference Model.
- The ITU-T Y.2233 “Ci” interface between the Inter-Provider CGF and the Other NGN Charging and Accounting Function is termed "Interface E" by the IPDR Reference Model.