



**Network Data Management – Usage  
(NDM-U)  
For  
IP-Based Services  
Service Specification –  
Authentication and Authorization**

**Version 2.5-A.0**

**April 13, 2001**

**© 1999-2001 IPDR, Inc.**

## Preface

### **Contacts**

For general questions regarding this document and referrals to technical experts for detailed questions, please contact:

Chief Editor: Steve Cotton  
Cotton Management Consulting  
[scotton@compuserve.com](mailto:scotton@compuserve.com)

#### **Architecture Working Group** –

Lead: Raghu Dhulipala  
Convergys Corporation  
[raghu.dhulipala@convergys.com](mailto:raghu.dhulipala@convergys.com)

Editor: Aron Heintz  
RateIntegration, Inc.  
[aheintz@rateintegration.com](mailto:aheintz@rateintegration.com)

#### **Business Requirements Working Group** –

Lead: Kelly Anderson  
SCC Communications Corp.  
[kanderson@sccx.com](mailto:kanderson@sccx.com)

Editor: Pat Walls  
TSI  
Telecommunication Services Inc.  
[pwalls@tsiconnections.com](mailto:pwalls@tsiconnections.com)

#### **Protocol Working Group**

–

Lead: Jeff Meyers  
HP  
[jeffm@cup.hp.com](mailto:jeffm@cup.hp.com)

Editor: Ken Sarno  
NARUS, Inc.  
[kensarno@narus.com](mailto:kensarno@narus.com)

### **Acknowledgements**

The following member companies contributed materially to the creation of this release of the document:

### **Abstract**

This document is a companion to NDM-U, which specifies the overall business requirements and protocol generic to all services. The content herein is compliant to those requirements and specifications and is particular to the service specified.

### **Change History**

2.5-A.0            April 13, 2001 – Initial Release

## Table of Contents

Preface.....	2
Contacts.....	2
Acknowledgements.....	2
Abstract.....	2
Change History.....	2
1. Introduction.....	4
1.1. Purpose.....	4
1.2. Scope.....	4
1.3. Compatibility.....	4
1.4. Timeline.....	<b>Error! Bookmark not defined.</b>
1.5. References.....	4
1.6. Overview.....	4
1.7. Terminology and Glossary.....	5
2. Authentication and Authorization Specification.....	7
2.1. Definition.....	7
2.1.1. Requirements.....	7
2.1.2 Usage Attribute List.....	8
2.2 Use Case.....	9
2.2.1 Basic Flow - RADIUS.....	9
2.2.2 Basic Flow (DIAMETER Type).....	10
3.0 Formal Specification.....	12
3.1 Schema.....	12
3.2 Sample Instance Document.....	13

# 1. Introduction

## 1.1. Purpose

This document is intended to specify the business use case and formal XML Schema for the IP-based service.

## 1.2. Scope

This document is limited to the discussion of issues as defined by the mission statement of IPDR.org, namely:

*The IPDR Organization (the “Organization”) is organized and operates as a non-stock not for profit organization for the following purposes:*

- (a) To develop, agree upon and publish a non-proprietary, open specification for the representation and encapsulation of Internet Protocol (IP)-based events for use by business, operations and decision support systems. Such events include, but are not limited to, IP-based network services, application services and e-commerce transactions;*
- (b) To develop, agree upon and publish a non-proprietary, open specification for the representation and encapsulation of IP-based network and service elements provisioning events;*
- (c) To promote work accomplished and uniform specifications to the industry and submit approved published specifications to the appropriate standards bodies for acceptance in the public domain;*  
*and*

To have and exercise all powers necessary or convenient to affect any or all of the purposes for which the Organization is organized.

## 1.3. Compatibility

Future revisions are expected to make every attempt to preserve investments made by service providers and solution vendors by considering backward and forward compatibility whenever it is practical.

## 1.4. References

- [1] NDM-U 2.5, IPDR.org.
- [2] XML Schema Part 1: Structures, W3C Working Draft 7 April 2000.
- [3] XML Schema Part 2: Data Types, W3C Working Draft 7 April 2000.

## 1.5. Overview

This specification is divided into two major chapters:

- Service Specification – description of the specific requirements and business use case for the service in question.
- Formal Specification – XML Schema description of the IPDR Record for this service.

## 1.6. Terminology and Glossary

### Terminology

Term	Definition
Accounting	The process of collecting and analyzing <b>service</b> and <b>resource usage</b> metrics for the purposes of capacity and trend analysis, cost allocation, auditing, and billing, etc. Accounting management requires that resource consumption be measured, rated, assigned, and communicated between appropriate business entities.
Mediation	In view of network reference model, Mediation refers to the combination of the logical entities IPDR recorder, IPDR transmitter, and IPDR store.
Resource	A quantifiable asset employed by a <b>Service Provider</b> , or on behalf of a <b>Service Provider</b> by another Service Provider, to fulfill a request of a <b>Service Consumer</b> . (Examples include: files, communications, goods, etc).
Roaming	Service usage initiated by a service consumer and provided by a service provider other than the one with which the service consumer have business relationship.
Service	Network and/or application operation that provides the <b>Service Consumer</b> with the requested <b>resource</b> .
Service Consumer	The beneficiary (human or system) of a <b>service</b> .
Service Element	Any element that is responsible for fulfilling a <b>Service Consumer</b> request. (Examples include: network equipment and system processes)
Service Provider	An enterprise that provides communications-based <b>services</b> .
Session	A set of related service usages; service usages may or may not be time based in the unit of measurement.
Usage	Consumption of <b>resources</b> and <b>services</b> by a <b>Service Consumer</b> .
Usage Attribute	A parameter whose value indicates some aspect of <b>usage</b> of a given <b>service</b> and/or <b>resource</b> .
Usage Entry <sup>1</sup>	A <b>Service</b> -specific trigger resulting in the generation by a <b>Service Element</b> of a set of <b>Usage Attribute</b> values related to <b>Usage</b> specific to a given <b>Service Consumer</b>

<sup>1</sup> Because of legacy issues, a Usage Entry from a given Service Element will not initially conform to an IPDR specification or, in some cases, may never conform. To be considered a Usage Entry the information presented or made available by inference from the Service Element must minimally contain attributes from some of the general attribute categories.

## Glossary:

ANI	- Automatic Number Identification
ASP	- Application Service Provider
BSS	- Business Support Systems
CRM	- Customer Relationship Management
DSS	- Decision Support Systems
DTD	- Document Type Definition
DSL	- Digital Subscriber Line
EP	- End Point
ESN	- Electronic Serial Number
FoIP	- Fax over IP
GK	- Gate Keeper
GPRS	- General Packet Radio Service
IETF	- Internet Engineering Task Force
IMSI	- International Mobile Subscriber Identity
IP	- Internet Protocol
IS	- IPDR Store
ISDN	- Integrated Services Digital Network
ISP	- Internet Service Provider
IT	- IPDR Transmitter
NDM	- Network Data Management
NSE	- Network Service Element
OSS	- Operations Support System
PLMN	- Public Land Mobile Network
PSTN	- Public Switched Telephone Network
QoS	- Quality of Service
RADIUS	- Remote Access Dial-In Usage Server
RAS	- Remote Access Server
SC	- Service Consumer
SE	- Service Element
SMS	- Short Message Service
SP	- Service Provider
TMF	- TeleManagement Forum
TOM	- Telecommunications Operations Map
UA	- Usage Aggregators
UC	- Usage Collectors
VoIP	- Voice over IP
VPN	- Virtual Private Network
WAP	- Wireless Application Protocol
xDSL	- Digital Subscriber Line of type x
XML	- eXtensible Markup Language

## 2. Authentication and Authorization Specification

The services described in this section are defined by IETF in a set of RFCs (for RADIUS) and in over 10 Internet Drafts (for DIAMETER and other protocols); the Internet Drafts are still under discussion in the AAA Working Group of IETF (AAA stands for Authentication, Authorization and Accounting) .

Other examples of AAA processes, such as the authentication within the framework of ITU-T's H.323 standard for VoIP, Video over IP, have not directly been used in the creation of this document.

The characteristic of authentication and/or an authorization service (“AA services”) is that of enabling other services such as dial-in service.

### 2.1. Definition

The AAA keywords have been defined by IETF as follows:

- **Authentication:** The act of verifying the identity of an entity (subject).
- **Authorization:** The act of determining whether a requesting entity (subject) will be allowed access to a resource (object).
- **Accounting:** The act of collecting information on resource usage for the purpose of trend analysis, auditing, billing, or cost allocation.

An authentication service and/or an authorization service is a service provided by an IP Network Service Provider to control access to network resources. Apart from authentication and/or authorization the AA services may include configuration of the service the user wants to use and accounting for that service.

The authentication or the authorization process itself may include generation of accounting records.

The following parties are involved in this service:

- The User, i.e. the Service Consumer,
- the Network Access Server (NAS), and the AAA Server, or Shared (Authentication, Authorization and Accounting) Server containing a single database of users, which allows for authentication and/or authorization (by verifying user ID and password), for accounting as well as for configuration information detailing the type of service to deliver to the user (for example, SLIP, PPP, telnet, rlogin, VoIP etc.).

#### 2.1.1. Requirements

- The IPDR must provide unique identification of all parties involved in the service, i.e. the User, the NAS and the AAA Server.
- If there is more than one administrative domain, some of the parties may have proxies; the IPDR must provide unique identification of those as well.
- The IPDR must contain all attributes needed for AA services for mobile wire line and mobile wireless user
- The set of attributes must reflect a state-of-art AA service protocol such as DIAMETER.

### 2.1.2 Usage Attribute List

<i>Category</i>	<b>Usage Attribute Name</b>	<b>Data Type</b>	<b>Presence</b>	<b>Possible Values</b>	<b>Remarks</b>
What	Type of AAService	String	Required	“Radius”, ”Diameter”, “H.225”, “Undefined” etc.	Type of authentication service that is invoked.
When	AARequestTime	Datetime	Required	ISO 8601 time	May be different from AAAcknowledgeTime. This will allow measuring response time.
When	AAAcknowledgeTime	Datetime	Required	ISO 8601 time	Time when authentication and/or authorization granted at NAS
Where	NAS ID	String	Required		Identification or Location of Network Access Server (NAS)
Where	AAA Server ID	String	Required		Identification or Location of Shared (Authentication/Authorization and Accounting) Server
Who	ProviderName	String	Required		Actual provider of the AA service
Who	UserLoginName (= User ID)	String	Required		Identifies a unique user in the system. Real time mapping of dynamically allocated IP addresses might be necessary

This attribute list should be completed by attributes defined in RADIUS and DIAMETER documents; see Internet Draft “Accounting Attributes and Record Formats” by Nevil Brownlee and Alan Blount, 16 June 2000; draft-ietf-aaa-accounting-attribute-04.txt.

In the case of RADIUS the usage is detailed by the following table.

<i>Category</i>	<i>Usage Attribute Name</i>	<i>Data Type</i>	<i>Presence</i>	<i>Possible Values</i>	<i>Remarks</i>
What	Acct-Status-Type		Required	“Start”, “Stop”, “Acct-on”, “Acct-off”	RADIUS Type Field 40
What	Acct-Input-Volume (octets or packets)		Required		RADIUS Type Field 42 or 47
What	Acct-Output-Volume (octets or packets)		Required		RADIUS Type Field 43 or 48
What	Acct-Session-Id		Required		RADIUS Type Field 44
What	Acct-Session-Time		Required		RADIUS Type Field 46
Why	Acct-Terminate-Cause		Optional		RADIUS Type Field 49

## 2.2 Use Case

### 2.2.1 Basic Flow - RADIUS

The description in this section is based on the RADIUS protocol (Remote Authentication Dial-in Service; see RFC 2138, RFC 2139 and related documents).

#### 2.2.1.1 Basic Flow

The RADIUS protocol provides a basic AA(A) service.

In this simplest case, the user is in the same administrative domain as the NAS and the AAA Server.

The user subscribes to an AA service with his/her IP Network Service Provider, and typically gets a user ID and a password.

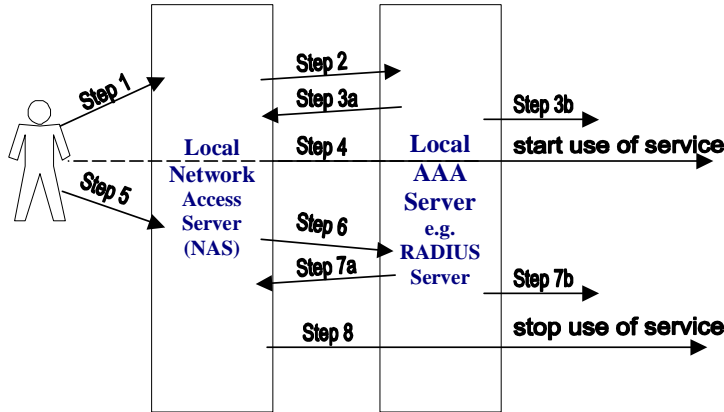
At the start of service delivery the NAS/AAA Server pair may generate an Accounting Start Record.

At the end of service delivery the NAS/AAA Server pair may generate an Accounting End Record.

Client/Server Model: A Network Access Server (NAS) operates as a client of the AAA Server. The client is responsible for passing user information to the designated AAA Server, and then for acting on the response that is returned.

#### Basic Flow on Start of Service

- 1) The User logs in and requests a service at the NAS.
- 2) The authentication request (as sent by the NAS) arrives at the AAA Server
- 3) The AAA Server acknowledges if the User ID is valid and the password is correct and the user is entitled to use the requested service.
  - a) On receiving the acknowledge message the NAS starts the service initially requested by the user.
  - b) The AAA Server generates a Accounting Start Record.
- 4) Start use of service.



**Basic Flow on End of Service**

5. The User requests termination of the service at the NAS.
6. The termination request arrives at the AAA Server
  - a) The AAA Server acknowledges receipt of the termination request, and
  - b) generates an Accounting End Record containing various parameter describing the effective use of the service (end time, duration, volume etc.).
7. NAS stops the service as requested by the user.

**Attributes for Basic Flow on End of Service**

See Table 1 above. In addition to the attributes listed in Table 1, there will be attributes describing the billable usage specific to the type of service consumed. Refer to Table 2 above for an example of the additional specific attributes for describing billable usage for a dial-in service over the IP network using the RADIUS protocol.

**2.2.1.2 Basic Flow Usage Attribute List**

See table above.

**2.2.2 Basic Flow (DIAMETER Type)**

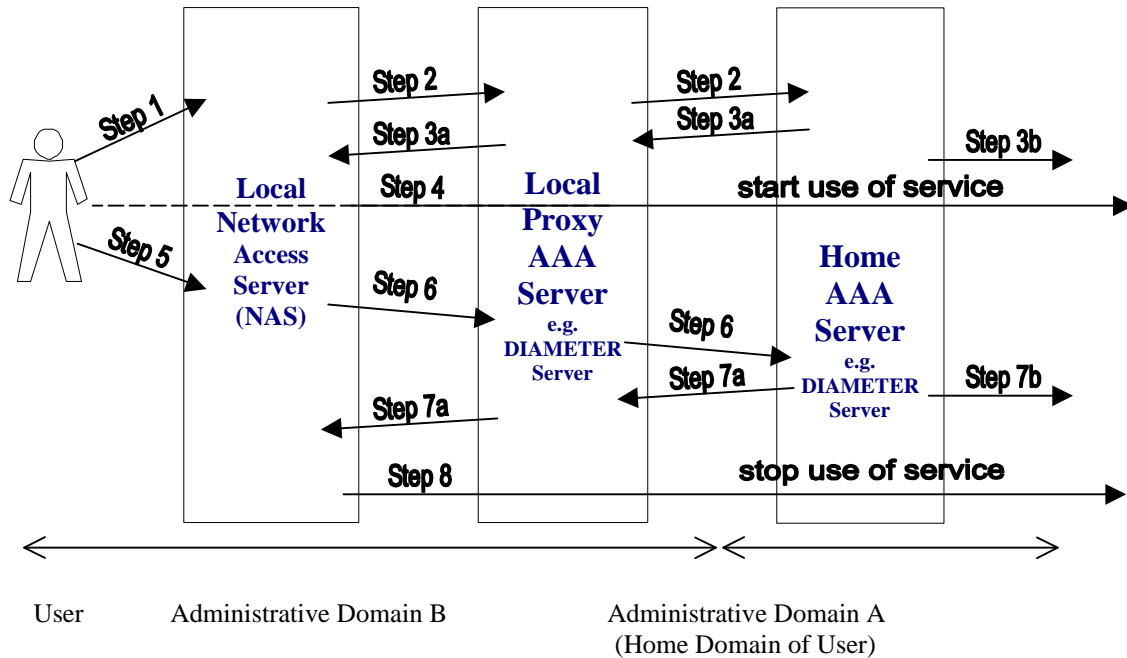
An extension of the RADIUS protocol, the DIAMETER protocol has been proposed and is now discussed in the IETF working groups (see the considerable number of pertinent Internet Drafts dated July 2000 and earlier). DIAMETER is the attempt to improve on most of the shortcomings of the RADIUS protocol. Furthermore, an additional objective is to accommodate roaming aspects of mobile wire line and wireless IP services.

**2.2.2.1 Alternate Authentication/Authorization**

The DIAMETER protocol provides an alternate flow for an AA(A) service.

The user is either in the same administrative domain as the NAS and the AAA Server or may be in another administrative domain (when roaming).

To provide AA services in the case of mobile IP and more than one administrative domain AAA Servers may have proxies in others than their original administrative domains.



DIAMETER Peer Model: A Network Access Server (NAS) operates as a peer of the AAA Server. Among AAA Servers, there is also a peer-to-peer relationship in DIAMETER.

### 2.2.2.2 Alternative/Specific Flow Usage Attribute List

See Internet Draft “Accounting Attributes and Record Formats” by Nevil Brownlee and Alan Blount, 16 June 2000; draft-ietf-aaa-accounting-attribute-04.txt; see the section on DIAMETER Attributes.

## 3.0 Formal Specification

### 3.1 Schema

```

<?xml version = "1.0" encoding = "UTF-8"?>
<!--Generated by XML Authority. Conforms to w3c http://www.w3.org/2000/10/XMLSchema-->
<schema xmlns = "http://www.w3.org/2000/10/XMLSchema"
  targetNamespace = "http://www.ipdr.org/namespaces/ipdr"
  xmlns:ipdr = "http://www.ipdr.org/namespaces/ipdr"

  version = "2.5-A.0"
  elementFormDefault = "qualified"
  attributeFormDefault = "unqualified">
  <annotation>
    <documentation>
      Referring to a local copy will normally yield significantly faster performance.
      The name of the master IPDR schema file can either be:

      http://www.ipdr.org/public/ipdr2.5.xsd

      Alternatively, it can be a local copy of this file.
      Please modify the preceding "include schemaLocation" appropriately.
    </documentation>
    <documentation>This is the master IPDR schema file for Authentication/Authorization and
Accounting</documentation>
    <documentation>The master service description documentation _SHOULD_ be found at:
      http://www.ipdr.org/public/NDM-U-ver-2-5-XXXXX-Cx.doc</documentation>
  </annotation>
  <include schemaLocation = "ipdr2.5.xsd"/>
  <!-- ***** -->

  <!-- ***** -->

  <complexType name = "SC-AA-Type">
    <complexContent>
      <extension base = "ipdr:SCType">
        <sequence>
          <element ref = "ipdr:subscriberId"/>
          <element ref = "ipdr:ipAddress"/>
        </sequence>
      </extension>
    </complexContent>
  </complexType>
  <element name = "subscriberId" type = "string"/>
  <element name = "ipAddress" type = "string"/>
  <complexType name = "SE-AA-Type">
    <complexContent>
      <extension base = "ipdr:SEType">
        <sequence>
          <element ref = "ipdr:hostName"/>
        </sequence>
      </extension>
    </complexContent>
  </complexType>
  <element name = "hostName" type = "string"/>
  <complexType name = "UE-AA-Type">
    <complexContent>
      <extension base = "ipdr:UEType">
        <sequence>
          <element name = "typeOfAAService" type = "string">
            <annotation>
              <documentation>Type of authentication service that is
invoked</documentation>
            </annotation>
          </element>
          <element name = "aRequestTime" type = "timeInstant">

```

```

                <annotation>
                <documentation>May be different from
aAAAcknowledgeTime. This will allow measuring response time.</documentation>
                </annotation>
            </element>
            <element name = "aAAcknowledgeTime" type = "timeInstant">
                <annotation>
                <documentation>Time when authentication and/or
authorization granted at NAS.</documentation>
                </annotation>
            </element>
            <element name = "nasId" type = "string">
                <annotation>
                <documentation>Identification or Location of Network
Access Server (NAS)</documentation>
                </annotation>
            </element>
            <element name = "aAAServerId" type = "string">
                <annotation>
                <documentation>Identification or Location of Shared
(Authentication/Authorization and Accounting) Server.</documentation>
                </annotation>
            </element>
            <element name = "providerName" type = "string">
                <annotation>
                <documentation>Actual provider of the AA
service</documentation>
                </annotation>
            </element>
            <element name = "userLoginName" type = "string">
                <annotation>
                <documentation>Identifies a unique user in the system.
Real time mapping of dynamically allocated IP addresses might be necessary.</documentation>
                </annotation>
            </element>
        </sequence>
    </extension>
</complexContent>
</complexType>
</schema>

```

### 3.2 Sample Instance Document