AES Call for Comment on Media Network Directory Requirements

Published by
Audio Engineering Society, Inc.

Abstract
This document is a call for comments on technical requirements for media network directories and directory-related services and mechanisms such as network discovery. From this document and the comments received on it, the AES will develop a set of requirements for media network directory standards that will work with present and future media networks over a wide range of application domains. Such standards will address at least the following areas:

1. Registration, query, and administration protocols;
2. Security mechanisms;
3. Directory data model;
4. Query language and related semantics; and
5. Scalability strategies.

Specific input is requested (see Section 4.4) on security use cases, user identity and privilege schemes as well as secure and nonsecure Directory Services.

Individuals with comments, input or questions about the draft material or issues presented in this document are encouraged to email them to x238-rfc-standards@aes.org

Contents

Introduction **4**
1 Scope **4**
2 Normative References **4**
3 Terms, definitions and abbreviations **4**
3.1 General Networking 4
3.2 Media Networks 5
3.3 Entities 5
3.4 Directories 5
3.5 Discovery 6
3.6 Namespaces 6
3.7 Media Connections 6
3.8 Network Services and Stores 6
3.9 Directory Database Services and Functions 6
4 Requirements **7**
4.1 Functionality 7
4.1.1 Registration / deregistration 7
4.1.2 Querying 7
4.1.3 Discovery 7
4.1.4 Representational capability 8
4.1.5 Storage independence 8
4.2 Namespaces 8
4.2.1 Path 8
4.2.2 Entity Name resolution 9
4.3 Data network independence 9
4.3.1 Data network type independence 9
4.3.2 Data network topology independence 9
4.3.3 Minimal effect on infrastructure 9
4.3.4 Shared data networks 9
4.4 Security and access control 10
4.4.1 Basic Security 10
4.4.2 Access Control 11
4.5 Scalability 11
4.5.1 Performance 11
4.5.2 Centralized and distributed implementations 12
4.6 Reliability and Robustness 12
4.7 Ease of use 12
4.8 Standardization 12
4.9 Data-network-type-specific features 12
4.9.1 IP Networks 12
4.9.2 USB networks 13
4.9.3 Bluetooth networks 13
4.9.4 Other types of networks 13
5 Comment Procedure **13**
5.1 Method 13
5.2 Format 13
5.3 Timing 13
5.4 Personal Involvement 13

Foreword

This AES Call for Comment on Media Network Directory Requirements was produced by the SC-02-12-N task group on AES-X238, Media network directory architecture, under the leadership of Jeff Berryman.

Members of the group that contributed to this document are: N. Amaya, F. Bergholtz, J. Berryman, H. Blum, A. Boenninghoff, J. Boqvist, P. Brightwell, R. Cabot, A. Calvanese, T. Edwards, J. Fletcher, J. Freyberger, J. Grant, K. Gross, M. Henry, E. Heurtel, A. Hildebrand, T. Johansson, S. Jones, M. Lave, M. Law, G. Linis, J. Meyer, R. Michl, B. Olson, O. Palm, S. Scott, M. Smaak, P. Stevens, N. Sturmel, P. Treleaven, P. Waddell, P. Warrington, P. Zielie.

Jeff Berryman
Chair, SC-02-12-N task group on AES-X238, Media network directory architecture
2017-07-25

Note on normative language

In AES standards documents, sentences containing the word “shall” are requirements for compliance with the document. Sentences containing the verb “should” are strong suggestions (recommendations). Sentences giving permission use the verb “may”. Sentences expressing a possibility use the verb “can”.

AES Call for Comment on Media Network Directory Requirements

Introduction

This document is a call for comments on technical requirements for media network directories and directory-related services. From this document, and the comments received on it, the AES will develop a set of requirements for media network directory standards that will work with present and future media networks over a wide range of application domains. Interested parties are encouraged to submit general and specific comments, proposed additions or changes, and responses to the specific questions posed below via the Comment Procedure described at the end of this document.

Media network directories are application-layer mechanisms that collect, store and disseminate information about devices, application services, and other elements of media networks. They are used for connection management, network supervision, and other purposes.

1 Scope

The standard that will result from this document will be aimed at directory standards that specify:

- Registration, query, and administration protocols;
- Security mechanisms;
- Directory data model;
- Query language and related semantics; and
- Scalability strategies by defining both peer-to-peer and server-supported modes.

Although directories are used by connection management mechanisms, such mechanisms are not addressed in this document. In this context, "connection management" means the protocols and processes in a media network by which signal flows are set up, monitored, and taken down.

The standard will make best use of existing standards. For example, the standard should be able to choose a query language from existing standard ones.

The target standard will not specify Directory Service implementation architectures or internal protocols the services may use to maintain the Directory data.

2 Normative References

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

RFC 2782 – *A DNS RR for specifying the location of services (DNS SRV)*, Internet Engineering Task Force

RFC 3986 – *Uniform Resource Identifier (URI): Generic Syntax*, Internet Engineering Task Force

3 Terms, definitions and abbreviations

3.1 General Networking

3.1.1 Data Network.
A telecommunications network for transport of digital data of various kinds. Synonym of computer network.

3.1.2 Subnetwork, or **Subnet**
A "logical, visible division" of a data network. For IP networks, a subnet is an IP "broadcast domain", i.e. the set of IP nodes reachable by a single broadcast message from any of those nodes.

3.2 Media Networks

3.2.1 Media Network
A network that communicates audio and video signals and related control, monitoring, data, and time-synchronization traffic.

3.2.2 Simple media network
A media network that operates entirely on a single subnet that is not shared with any other media network.

3.3 Entities

3.3.1 Network Entity or just **Entity**
Anything in a media network that can be described by a Directory. A Directory is itself an Entity, so Directories can be nested inside other Directories.

3.3.2 Entity Type
A particular kind of Entity.

3.3.3 Entity Name
The unique name of an entity within its namespace.

3.3.4 Network Device or just **Device**
An Entity Type that denotes a logical block of functionality within a networked media infrastructure, usually implemented by a physical device connected to a media network, or a software virtualization of such a device running on a computer connected to a media network.

3.3.5 Network Service or just **Service**
An Entity Type that denotes a software functionality or a set of software functionalities that can be used by network clients, together with the policies that control its usage.

3.4 Directories

3.4.1 Database
A formally organized collection of data that allows query and update.

> Note: This document uses "database" in the abstract Computing Science sense, to mean a set of objects and operations defined by a schema. No particular database management system (e.g. MySQL) is expected or implied.

3.4.2 Directory
A database that contains Directory Entries that describe a set of Entities.

3.4.3 Directory Entry or just **Entry**
The database record in a Directory that describes an Entity. Each Entity described by a Directory shall have its own Entry.

3.4.4 Entry Attribute or just **Attribute**
A data value that is part of an Entry. For example, Entity Name is an attribute.

3.4.5 Register [Entity]
Add an Entity's Entry to a Directory.

3.4.6 Deregister [Entity]
Delete an Entry from a Directory.

3.5 Discovery

3.5.1 Discovery

A set of Directory functions that support automation of directory updating. These functions typically include:

- Autonomous self-registration of Entities.
- Automatic detection of new or departing Entities.
- Support of persisting queries.
- Ongoing supervision and verification mechanisms to ensure that the Directory data is accurate at all times.

Note: Some important Directory Services do not offer discovery functions

3.6 Namespaces

3.6.1 Entity Namespace or just Namespace

An Entity Namespace is a container for a set of Entity Names. Each Entity Namespace is a scope for its Entity Names, thus making it possible to distinguish between identical Entity Names in different contexts, by associating each context with its own separate Entity Namespace.

3.7 Media Connections

3.7.1 Entity Connection Identifier or just Connection Identifier

A particular Attribute that provides data that can be used for establishing a media connection to the Entity.

3.7.2 Entity Name Resolution

The process by which an Entity Name is used to retrieve its Connection Identifier.

3.7.3 Connection Endpoint

An Entity Type that denotes a source or destination of media.

3.8 Network Services and Stores

3.8.1 Media Repository

An Entity Type that denotes a Service which stores media elements and provides them to network clients on demand.

3.8.2 Subscribe

Establish a relationship between Entities that provides automatic notifications to the initiating Entity ("subscriber") whenever certain events occur in the other Entity ("subscribee"). "Subscribe X to Y" means establish a relationship with subscribee X that produces automatic notifications to the subscriber whenever event Y occurs. For example, "Subscribe myself to Directory Additions" set up a relationship that notifies me whenever something is added to a Directory.

3.9 Directory Database Services and Functions

3.9.1 Directory Service

A network Service that provides access to a Directory. A typical Directory Service will:

- implement standard Directory data models and processing rules;
- use Entity Names as defined by the standard Entity Namespace model; and
- offer services to networks via standard Directory access protocols.

A complete Directory implementation may entail one or more Directory Services.

Note: Examples of multiple Directory Services include:

Media network protocol architectures that specify multiple services for directory access. For example, NMOS defines separate Directory Services for Registration and Query.

Directory implementations that must support legacy schemes (e.g. DNS-SD) alongside newer standards. In such cases, there will probably be separate Directory Service sets for legacy and current operation.

3.9.2 Query (noun)
A precise request for retrieving one or more Entries from a Directory.

3.9.3 Query (verb)
Apply a Query(noun) to a Directory. "Execute a Query" is a synonym.

3.9.4 Query Specification
The logical expression in a Query that specifies its selection criteria.

3.9.5 Query Language
The specification the defines the syntax and semantics of a Query Specification.

3.9.6 Persisting Query
A Query on a Directory that includes a Subscription to subsequent changes involving Entries that match the Query. Persisting Queries allow Entities to maintain continuously accurate knowledge of a Directory's population, or more precisely, knowledge of the subset of the population the subscriber cares about.

Note: Executing Queries or Persistent Queries is sometimes called "Browsing" in networking standards language.

4 Requirements

4.1 Functionality

4.1.1 Registration / deregistration

It shall be possible for Entities on the network to be registered in, and deregistered from, the Directory.

4.1.2 Querying

Querying may be used by:

- Controllers, to identify and monitor the Entities in the network; and
- Entities, in order to confirm their registration status;
- Network administrators, for purposes such as updating and reporting of Entities and editing of metadata such as security parameters and access permissions.

The Directory Service shall provide querying functions sufficient for all of these activities.

Different Directory implementations may offer differing levels of query service, but in all cases it shall be possible to retrieve sufficient information for communicating devices to attempt establishing connections with the Entities involved.

Queries shall be expressed in a query language defined by the Directory standard. The same language shall be used for all compliant implementations. However, the standard may define some query features as optional.

It is expected that the Directory query language will be based on an existing query language from standard database technology.

The Directory may support Persisting Queries. When a Persisting Query is active, changes that cause update notifications shall include creation, modification, and deletion of Entries that match the query.

4.1.3 Discovery

The Directory Service may support Discovery. Discovery shall include the following functions:

- Accept Entity self-registration and de-registration.
- Subscription-based notification of added or departed Entities.

- Query of the directory by Entities in the network, including both simple and persisting queries.
- Timely automatic detection of Entity departure.

  Note: Whether to implement automatic detection will be outside the scope of the resulting standard. Where automatic detection is implemented, the quantitative meaning of "timely" will be outside the scope of the resulting standard.

4.1.4 Representational capability

The same Directory Services shall work for all kinds of network services, including media transport, connection management, and device control.

A Directory shall be able to describe multiple Entity types.

The Directory standard shall define:

- A schema that describes the complete set of standard Entity Types;
- The minimum subset of Entity Types a Directory must be able to support in order to comply with the standard;
- A means by which implementations may extend the schema to support additional nonstandard Entity Types without compromising interoperability.

Directories shall offer flexible attribute support. Entity Types shall be capable of providing attribute names and values that can be used for presentation or client-side filtering. The schema for these shall form the definition of an Entity Type.

Entity Types, such as ACIP accounts or AES67 media streams, shall be capable of providing one or more recommended media profiles expressed as partial or full SDP documents.

4.1.5 Storage independence

Data formats and directory access protocols shall be decoupled from the Directory data model.

4.2 Namespaces

The Directory data model shall allow the collection of Entries into Namespaces. When an Entry is registered, it shall be registered in a particular Namespace called its Home Namespace.

A Namespace shall be a scope for the Entries it contains. Thus, two Entities in a Directory may have the same Entity Name as long as they are contained in different Namespaces.

By default, a Directory shall contain a single namespace that contains all its Entries. This namespace shall be called the Directory's Global Namespace.

Namespaces shall themselves be Entities and shall be registered in the Directory. A Namespace may be registered in the global namespace or in another namespace, but not in itself. A Namespace registered inside another Namespace may be referred to as a Nested Namespace.

Access to a Namespace may be subject to access controls as described in Section 4.2.

The use of Namespaces other than the Global Namespace shall an implementation option. If only a Global Namespace is used, then it shall be the Home Namespace of all the Entities in the Directory.

4.2.1 Path

A globally unique identifier of an Entity may be constructed by prepending to the Entity's Name the set of containing Namespaces, starting with the Name of the Entity's Home Namespace, proceeding to the left, and ending with the Name of the Global Namespace. Each element of the identifier shall be separated by a delimiter character. Such an identifier shall be termed Entity Path, or just Path.

Path syntax shall be defined by the IETF URI scheme described in RFC 3986. The URI scheme has various options from which the final Directory standard shall select.

For illustrative purposes, for a Directory using nested Namespaces, an example Path might be as follows:

```
ODA:/MyCompany/Operations/PagingSys/LoadingDock/Amp1
```

4.2.2 Entity Name resolution

For Entity Name Resolution, Directory Services shall provide various query functions, depending on the Query specified, as follows:

- If the Query specifies only a Path, a direct lookup shall be made in the designated Namespace(s), as specified by the elements of the Path.
- If the Query specifies only a simple Entity Name, a lookup in the client's Home Namespace shall be attempted; if it is not found there, the lookup shall fail.
- If the Query specifies multiple attributes, the lookup shall generally proceed according to the rules of the Query Language.

4.3 Data network independence

4.3.1 Data network type independence

Directory standards shall not assume a particular data network type (e.g. IP network), and shall include features that allow implementations to operate over a range of data network types, including use cases that include multiple data networks of differing types in a single application system.

> Note: An example involving multiple data network types is an IP-based network media system that includes devices connected via USB links.

4.3.2 Data network topology independence

Specific Entity Name and Path values shall not depend on the topologies of the underlying data network infrastructures, and Entity Name and Path values shall survive changes to addressing strategies and routing topologies of the data networks involved.

4.3.3 Minimal effect on infrastructure

Directory changes, including:

- Adding/changing/deleting new Directory entries, and
- Adding/changing/deleting new media networks and their Directories
- should require minimal (ideally zero) infrastructure administration (e.g. IT department) activity.

Directory operations shall not compromise the integrity of the underlying data network infrastructure.

4.3.4 Shared data networks

The Directory standard shall allow for use cases in which multiple independent media networks owned by different organizational units share a common data network infrastructure.

In such cases:

- The Directories of the respective media networks shall function independently of each other.
- One media network's Directory shall not be detectable or accessible by another media network's Entities unless specific permissions to that effect have been granted.
- Given suitable permissions, an Entity may be registered simultaneously in more than one Directory.
- Adding and deleting Entities and their Directory entries shall be secure, straightforward, and not error-prone.

> Note: When a Directory implementation supports automatic self-registration of Entities, and where multiple Directories exist in the common data network, a mechanism will be required to ensure that each new Entity joining the network registers itself in the correct Directory or Directories.

4.4 Security and access control

Directory Services shall implement basic security services that protect Directory traffic, and may additionally implement access control mechanisms that constrain Directory access, based on user identity.

4.4.1 Basic Security

The basic Directory security problem can be seen as a matrix of cases, as shown in Table 1.

Table 1. Directory security cases

Security Function →		Authentication		C. Encryption	D. Integrity Protection
Application Process ↓	Accessor ↓	A. of Server	B. of Client		
1. Registration	Device	A1	B1	C1	D1
2. Querying	Controller	A2	B2	C2	D2
3. Administration	Workstation	A3	B3	C3	D3

The security functions (columns A-D of Table 1) are as follows:

1. **Server Authentication**. This function aims to ensure to a client that the server it is accessing is indeed the server it intends to access, and not an impostor.
2. **Client Authentication**. This function aims to ensure to a server that the client accessing it is indeed the purported client, and not an impostor.
3. **Encryption**. This function aims to prevent eavesdropping on client-server traffic.
4. **Integrity Protection**. This function aims to prevent content of client-server traffic (in either direction) from being maliciously or accidentally altered in transit.

   Note: Encryption alone is not sufficient to guarantee message integrity. For example, (1) encryption does not prevent portions of messages from being deleted in transit; (2) encryption does not prevent messages from being replaced by other encrypted messages, even though the agent doing the replacing may not be able to decrypt the texts involved.

Directory systems may implement some or all of these functions.

The application processes (rows 1-3 of Table 1) are as follows:

1. **Registration**. This is the process in which an Entity joining a network enters itself in the Directory.
2. **Querying**. This is the process by which a controller maintains up-to-date knowledge of the network's Entity population. Queries may be one-time or persistent. Persistent queries automatically notify controllers of network changes.
3. **Administration**. This is the process by which humans edit the contents and operating parameters of the Directory.

The task group requests input on needs in this area. Which, if any, security cases should future directory standards support? Specific input is requested on classifying features as required, desirable, or optional (i.e. "shall", "should", or "may").

4.4.2 Access Control

Directory Services, whether secure or not, may provide access control features to avoid unauthorized modification and/or retrieval activities.

In this context, "access control" means placing constraints on the scope of user Directory interactions that depend on the user's identity. In this definition, "user" may mean a person, a device, or an instance of a software system.

Directory activities are broadly categorized as follows:

1. **Device activities**, including self-registration and deregistration (if Discovery is supported) and participation in supervision ("keep-alive") processes;
2. **Controller activities**, which are centered around querying (including persistent querying); and
3. **Administrative activities**, whose tasks may include retrieval, reporting, and update of Entities, creation and deletion of Directories, user account administration, and implementation administration tasks such as backup, file space management, performance tuning, troubleshooting, and so on.

Although access control is optional, when a Directory Service implements access control it shall implement at least the user identity and privilege scheme defined in the Standard.

The task group requests input on requirements for the basic user identity and privilege scheme. It has the following questions:

- ***Should the standard specify a password scheme, an ID+password scheme, or something more elaborate?***
- ***Should the standard specify access controls on individual Directory data elements (i.e. on the field with an Entry), or is it sufficient to control access to whole Entries at a time?***
- ***Should the standard allow access control for nonsecure Directory Services?***

4.5 Scalability

The directory standard shall be appropriate for both local and wide-area contexts, with network populations ranging from two to many thousands of entities. However, implementation details may differ between small and large cases.

Directories and their services shall be capable of accommodating network infrastructures at all levels of complexity, from simple single-subnet cases to complex cases with many subnets. The Directory standard shall define a range of mechanisms to cover all the use cases.

In general, Directories are required to work at all network scales. However, Directory Service particulars may not be the same at all scales. In particular, plug-and-play, zero-administration operation, while convenient in small networks, shall not be required to work in larger networks.

4.5.1 Performance

Quantitative Directory Service performance criteria may vary from application to application, but in general, Directory Service performance shall be satisfactory in the following functional areas:

- Distribution of an update to a large number of Persistent Query subscribers.
- Servicing a large number of simultaneous queries (this is particularly important for system startup).
- Recovering from loss of the active Directory Service.

In all cases, Directory Services shall be stable under extreme conditions, such as data network bandwidth deficiency, high data transmission error rates, and massive bursts of transaction traffic of all kinds.

4.5.2 Centralized and distributed implementations

A Directory may be implemented in a centralized or distributed manner. In this context, "distributed" shall mean implemented in multiple physical sections usually stored in diverse network hosts.

The distribution of a Directory shall generally be transparent to Directory clients.

Implementation details of Directory distribution are outside the scope of this document.

4.6 Reliability and Robustness

Directory standards shall define, but not require, high-reliability implementations that include various forms of redundancy and service distribution.

Directory reliability standards shall generally be high enough for use in life-safety and evacuation applications.

Directory implementations should provide:

- Proactive methods for instability prevention.
- Reactive methods for recovery from existing instability.
- The ability to automatically recover from loss of the active registry.

4.7 Ease of use

Setting up and managing Directory Services for simple media networks shall not require advanced network administration skills.

The Directory standard shall define, for simple media networks, a plug-and-play mode requiring zero preconfiguration by users and no dedicated Directory server.

4.8 Standardization

Directory protocols and services shall be defined by open public standards.

Directory standards shall be complete enough to ensure interoperability of directory implementations from multiple makers.

4.9 Data-network-type-specific features

> Note: The Directory Standard will generally define the data model and access methods of the Directory in a manner that does not depend on the type of underlying data network. However, there are additional data-network-type-specific requirements which particular Directory implementations must fulfill in order to guarantee interoperability.

4.9.1 IP Networks

When implemented in an IP network, a Directory service shall be capable of:

- Operating with either IPv4 or IPv6 addressing
- Using Dynamic Host Configuration Protocol (DHCP) to determine its own IP address.
- Registering its hostname in the Domain Name Service (DNS).
- Using DNS hostnames to address the Entities it registers.

The Directory Service shall provide a service name that can be used to register DNS SRV records as per RFC 2782.

When multiple Directory services share the same IP network, each such service shall have a unique DNS domain to allow harmonious coexistence. E.g. “directory1.companyname.example” and “directory2.companyname.example”.

4.9.2 USB networks

Comments are invited.

4.9.3 Bluetooth networks

Comments are invited.

4.9.4 Other types of networks

Comments are invited.

5 Comment Procedure

5.1 Method

Individuals with comments, input or questions about the draft material or issues presented in this document are encouraged to email them to x238-rfc-standards@aes.org

5.2 Format

Responses may preferably be submitted as marked up versions of this document with "Track Changes" enabled or with changes and comments highlighted or implemented in a font color other than black.

Responses may also be submitted as a new document. If this approach is used, the material should reference the section number of this document to which it applies.

5.3 Timing

Responses should be submitted by September 30, 2017 to insure that they may be considered by the SC-02-12-N task group in advance of and during their meeting at the Audio Engineering Society fall convention in New York.

5.4 Personal Involvement

Interested individuals are encouraged to join the SC-02-12-N task group and, if possible, to attend the meeting at the Audio Engineering Society fall convention in New York. Attendance at the meeting is not required in order to join the task group.

Please submit material in advance of the meeting via the x238-rfc-standards@aes.org email address, even if you plan to attend the meeting. Submitted documents are circulated to the task group members in advance of the meeting. This improves meeting efficiency and allows more thorough consideration of the submitted material.

STANDARDS

The AES Standards Committee is the organization responsible for the standards program of the Audio Engineering Society. It publishes technical standards, information documents and technical reports. Working groups and task groups with a fully international membership are engaged in writing standards covering fields that include topics of specific relevance to professional audio. Membership of any AES standards working group is open to all individuals who are materially and directly affected by the documents that may be issued under the scope of that working group.

Complete information, including working group scopes and project status is available at http://www.aes.org/standards. Enquiries may be addressed to standards@aes.org

The AES Standards Committee is supported in part by those listed below who, as Standards Sustainers, make significant financial contribution to its operation.

Standards Sustainer Gold

NETFLIX

Focusrite

XFRM Inc. Transforming the World One Idea at a Time

Olson Sound Design

Standards Sustainer Silver

LECTROSONICS

21st Century Fox

Audio precision

SENNHEISER

ADAMSON

THE TELOS ALLIANCE

BOSE

Eventide

fulcrum ACOUSTIC

COVELOZ

Standards Sustainer

AUDYSSEY

NTi AUDIO

MQA

KLIPPEL

LAWO

CLAIR

WEISS

METRIC HALO

AEA

U SOUND

THAT Corporation

NBCUniversal

DYNAUDIO

WorldCast Systems

Fraunhofer IIS

Control 4

AMERGING AUDIO FOR THE NETWORKING AGE

RAVENNA

DSPECIALISTS Digitale Audio- und Messsysteme GmbH

ARCHWAVE connecting audio

DOLBY

HARMAN A SAMSUNG COMPANY

XPERI

audio-technica

dbx-tv

This list is current as of 2017/6/30