Directory Schema Listing Procedures
<draft-ietf-schema-proc-list-01.txt>

Status of this Memo

This document is an Internet-Draft. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

To learn the current status of any Internet-Draft, please check the "id-abstracts.txt" listing contained in the Internet-Drafts Shadow Directories on ftp.is.co.za (Africa), nic.nordu.net (Europe), munnari.oz.au (Pacific Rim), or ftp.isi.edu (US West Coast).

Abstract

This memo documents procedures for listing directory service schemas in a centrally operated, administered, and maintained repository. This repository will be available as a resource to directory protocol and service implementors to facilitate schema discovery.
Table of Contents

1.0 Introduction ........................................ 3
1.1 Terms and Definitions. ............................. 3
2.0 Directory Schema Listing ............................ 5
2.1 Schema Listing Request Architecture Diagram. ...... 5
2.2 Listing Requirements .................................. 6
2.2.1 Functionality Requirements ....................... 6
2.2.2 Naming Requirements ............................... 6
2.2.3 Content Formatting and Transfer Encoding Requirements... 6
2.2.4 Security Requirements. ........................... 7
2.2.5 Usage and Implementation Non-requirements ........... 8
2.2.6 Publication Requirements ......................... 8
2.3 Listing Procedure..................................... 9
2.3.1 Announcement and Community Review. .............. 9
2.3.2 Community Review and Assessment.................. 10
2.3.3 Primary Repository Operator Listing............... 10
2.4 Comments on Schema Listings ......................... 10
2.5 Location of List of Available Schema ................. 10
2.6 Primary Repository Operator Procedures for Listing Schemas 10
2.7 Change Control ..................................... 12
2.8 Listing Request Formats. ............................ 13
2.8.1 Schema Unit Listing Request Format ................ 13
2.8.2 Schema Pak Listing Request Format ................ 14
2.9 Primary Repository Operator Responsibilities and Constraints 14
3.0 Security Considerations .............................. 14
4.0 Acknowledgements ................................. 15
5.0 References ........................................ 15
6.0 Authors’ Address .................................... 16
1.0 Introduction

There is a growing number of places where schema for Internet Directory Services are being defined, with varying degrees of documentation. This plethora of schemas is unavoidable in the light of the needs of different service communities, but it makes it difficult for directory service builders to find and make use of an existing schema that will serve their needs and increase interoperability with other systems. A listing service providing a single point of discovery for directory service schema will promote schema reuse, reduce duplication of effort, and thus promote directory service interoperability. Listed schema will be assigned a permanent, unique listing listing name as a part of the creating schema listing requests; which starts the schema listing process. This listing process was defined to ensure that directory service schema writers can publish their schema in a public forum so that they will be re-used.

The IETF schema listing service has public read access and restricted, moderated write access. Currently, this listing service is centrally operated, administered, and maintained by the Internet Directory Consortium. The schema listing repository is mirrored to ensure some level of redundancy for read access.

This document defines schema listing procedures which use the Internet Directory Consortium as the primary listing repository operator.

1.1 Terms and Definitions

Information Object - a descriptive abstraction of some real-world object

Object Attribute - a descriptive property of an information object; typically, object attributes are defined in terms of semantic and syntactic definitions

Schema - a collection of definitions for related information objects

Schema Unit - a related or grouped set of object attributes that form a discrete unit within the context of a schema for a particular protocol; examples include an LDAP object class or a WHOIS++ template

Schema Pak - a related or grouped set of schema units that collectively specify a schema associated with a particular protocol; an example of a schema pak is the set of LDAP object classes specified in [RFC2256]
Metadata - characteristics that differentiate one schema unit or schema pak from another; used to catalog listing service content; structured using a profile of [MIMEDIR]; also contains references to files stored within and outside of a listing repository

Schema Unit Content - a formal specification of a schema unit using a profile of [MIMEDIR]

Schema Unit Listing - the combination of a single schema unit content file intended for use within the context of a particular protocol and a file containing metadata describing the schema unit specified within that schema unit content file

Schema Pak Listing - a single metadata file containing information describing and referring to a set of related or grouped schema unit content files

Repository - a database in which listings are stored

Listing Request - a proposed schema unit listing or schema pak listing formatted using [MIME] constructs that is submitted for consideration as a listing to be published in a repository

Operator - an organization that administers and maintains a repository

Primary Repository - the repository that masters the schema listings database

Shadow Repository - a repository that mirrors the primary repository

Contact Person - the name of the individual who holds the authority to update a listing and who should be contacted if questions or concerns arise related to a listing or listing request

Listing Authority Contact - the name of the individual who holds authority to replace a contact person; can be either the contact person for a listing or an alternate contact within the organization to which the contact person belongs (this allows one person organizations to list schema)

The terms for specifying requirement level defined in [RFC2119] are used in this document.
Listing of a new schema starts with the construction of a listing request. Schema writers obtain a unique listing name and include it in the schema listing request sent to a moderated request review list. Following a comment period of 2 weeks, if no significant objections are raised (determined by the moderator), the moderator sends the listing request to the primary listing repository operator, subject to incorporation of relevant comments by the schema writer. Listing requests are checked to verify compliance with the requirements and conditions discussed below and the listing will be published in the primary listing repository if appropriate. A mirroring agent replicates the new listing across the primary and mirrored copies of the listing repository database.
The following sections describe the requirements and procedure.

2.2 Listing Requirements

Listing requests are all expected to conform to various requirements laid out in the following sections.

2.2.1 Functionality Requirements

Schema unit listings MUST include two different types of information:

1. metadata

2. schema unit content

Metadata will be used to catalog repository files by characteristics that differentiate listings.

Schema unit content MUST be limited to the specification of a single schema unit.

2.2.2 Naming Requirements

All listings MUST have a valid OID as their name.

The primary listing repository operator MUST provide schema writers with the following components of a listing request name:

+ a sequence number assigned to each listing by the primary repository operator

+ a version number assigned to each listing version by the primary repository operator

2.2.3 Content Formatting and Transfer Encoding Requirements

All listings MUST employ a common data format.

Metadata and schema unit content format and transfer encoding MUST utilize appropriate [MIMEDIR] profiles.

Currently, five [MIMEDIR] profiles have been defined for use in the schema listing service:

[MIMELDAP] MUST be used to format and encode LDAPv3 schema unit content.

[MIMEWHOISPP] MUST be used to format and encode WHOIS++ schema content.
unit content.

[MIMEWHOIS] MUST be used to format and encode WHOIS schema unit content.

[MIMERWHOIS] MUST be used to format and encode RWHOIS schema unit content.

[METASYN] MUST be used to format and encode metadata for all schema unit listings, schema pak listings, and listing requests.

Other [MIMEDIR] profiles MAY be defined for use in the schema listing service; this procedures document will be updated to reflect such changes.

2.2.4 Security Requirements

An analysis of security issues for listed schema SHOULD be performed prior to submitting a listing request. However, regardless of what security analysis has or has not been done, all descriptions of security issues MUST be as accurate as possible. In particular, a statement that there are "no security issues associated with this type" MUST not be confused with "the security issues associated with this type have not been assessed".

There is absolutely NO REQUIREMENT that listed schema be secure or completely free from risks. Nevertheless, all known security risks SHOULD be identified in the listing request.

The security considerations section of all requests is subject to continuing evaluation and modification, and in particular MAY be extended by use of the "comments on schema listings" mechanism described in subsequent sections.

Some of the issues that SHOULD be looked at in a security analysis of a schema listing are:

(1) A listing might include specifications mandating exposure of certain attributes which would result in compromising the privacy of an organization or individual.

(2) A listing might be intended for use by applications requiring some sort of security assurances not provided by the schema specified in the schema unit content or in the schema unit content files referenced in a schema pak listing.
2.2.5 Usage and Implementation Non-requirements

In the directory services environment, where information on the embedded schema knowledge of a directory client is frequently not available to a server, maximum interoperability is attained by restricting the schema used to those agreed upon by the large community of directory service technology developers and users. This was asserted in the past as a reason to limit the number of possible schema to one via standards processes and resulted in a change process with a significant hurdle and delay for those seeking to modify and extend standard schema to better suite their needs. Eventually, various individuals and organizations began using non-standard schema, making interoperability difficult to achieve.

The need for "common" or "meta" schema listings does not require limiting the publication of new listings. If a set of schema unit listings is recommended for a particular application, that should be asserted by an intended use statement specific for that application and/or environment within a schema pak listing metadata file. If a set of schema pak listings is recommended for a particular application, that should be asserted by a separate intended use statement specific for the application and/or environment; or an additional schema pak listing containing references to all of the relevant schema unit listings should be created, reviewed, and published.

As such, universal support and implementation of a schema is NOT a requirement for listing it. If, however, a schema is explicitly intended for limited use, this should be noted in its listing(s).

2.2.6 Publication Requirements

Requests for schema listed in the IETF schema listing service MAY be published as RFCs. The primary listing repository operator will retain copies of all schema listing requests that meet the requirements specified below and "publish" them as part of the schema listing repository.

The listing of a schema does not imply endorsement, approval, or recommendation by the IETF or even certification that the specification is adequate for the intended use of the schema. To become Internet Standards, protocol, data objects, or whatever must go through the IETF standards process. This is too difficult and too lengthy a process for the convenient listing of schema.

It is expected that applicability statements for particular applications will be published from time to time that recommend implementation of, and support for, schema that have proven
particularly useful in those contexts.

2.3 Listing Procedure

The following procedure has been implemented by the primary listing repository operator for review and approval of new listings. This is not a formal standards process, but rather an administrative procedure intended to foster re-use of directory services schema and to provide a method for collecting schema in a publicly accessible repository.

Submitting listing requests can be done via mail, treating posting of a formatted request containing the specification of schema unit content for a particular protocol and/or metadata to the mailing list

ietf-schema-review@pilot.schema.dir.reg.int

as a first step.

2.3.1 Announcement and Community Review

While listed schema are NOT REQUIRED to be published as RFCs, listing requests documenting them MUST be posted to the mailing list

ietf-schema-review@pilot.schema.dir.reg.int,

allowing a review and comment period of at least 2 weeks. This is necessary to prevent the malicious as well as unintended introduction of obviously bogus or frivolous schema into the listing repository.

Schema writers wishing to have their schema listed by the primary listing repository operator, MUST specify any such schema (may require the creation/submission of more than one request) according to one of the following [MIMEDIR] profiles: [MIMELDAP], [MIMEWHOISPP], [MIMEWHOIS], or [MIMERWHOIS]. Other such profiles may be defined elsewhere and this procedures document will be update to reflect such process changes.

Metadata, as specified in [METASYN], MUST also be included in this request. A template for listing requests is specified in paragraph 2.8. Schema writers MUST use this template.

Schema writers MUST also construct a unique listing request name for each request being created. Listing names are constructed according to the type valuetype syntax and type special notes for the ‘listingName’ MIME Directory Type [METASYN].

Once created, the listing request should be sent to ietf-schema-
2.3.2 Community Review and Assessment

Moderated discussions on the ietf-schema-review@pilot.schema.dir.reg.int mailing list will enable a means of gauging consensus as to whether or not the schema being proposed is bogus. If there is no significant reason to believe that a schema is useful or if it appears to be a bogus or malicious request, the moderator will not submit a listing request to the primary listing repository operator; otherwise, they may do so.

2.3.3 Primary Repository Operator Listing

Provided that the schema listing request meets the requirements defined in paragraph 2.1, the ietf-schema-review@pilot.schema.dir.reg.int list moderator will send that listing request to the primary repository operator, which will check this listing request for validity, and make the listing available to the community.

2.4 Comments on Schema Listings

Comments on listings may be submitted by members of the IETF community to for consideration by the rest of the community and the primary listing repository operator. These comments will be passed on to the contact person for the listing if possible. Submitters of comments may request that their comment be attached to the listing itself. If the ietf-schema-review@pilot.schema.dir.reg.int list moderator is able to gauge consensus affirming the inclusion of such a comment, it will be made accessible in conjunction with the listing itself.

2.5 Location of List of Available Schema

Listings will be posted in the anonymous FTP directory "ftp://www.pilot.schema.dir.reg.int/schema/" and all listings will be summarized in a periodically issued RFC. Schema unit content, schema pak listings, and/or other supporting material may also be published as an Informational RFC by sending it to "rfc-editor@isi.edu" (please follow the instructions to RFC authors [RFC2223]).

2.6 Primary Repository Operator Procedures for Listing Schemas

Listings will be published by the primary repository operator automatically and without any formal review as long as the following minimal conditions are met:
(1) All listings MUST have a valid OID as their name.

(2) All schema unit listing requests MUST include both metadata and schema unit content.

(3) All schema pak listing requests MUST be limited to metadata.

(4) Metadata MUST comply with [METASYN].

(5) Schema unit content MUST be compliant with at one of the following [MIMEDIR] profiles:

   + [MIMELDAP] (for LDAPv3 schema specifications)
   + [MIMEWHOISP] (for WHOIS++ schema specifications)
   + [MIMEWHOIS] (for WHOIS schema specifications)
   + [MIMERWHOIS] (for RWHOIS schema specifications)

Other [MIMEDIR] profiles may be defined in the future and this document will be updated to reflect such additional profiles.

(6) Any security considerations given must not be obviously bogus. It is neither possible nor necessary for the primary listing repository operator to conduct a comprehensive security review of listings. However, the listing request review committee (the members of the listing request review mailing list) has the authority and expertise to identify obviously incompetent material and exclude it.

(7) Schema listing requests MAY be signed using PGP/MIME as described in [RFC2015]. The primary listing repository operator MUST be able to accept listing requests in PGP/MIME messages, although they are NOT REQUIRED to validate or retain the signatures.

(8) Listing request MUST be formatted according to paragraph 2.8.

(9) If a listing request includes one or more URI-based references to information that would not be included in a resulting listing, but is associated with the schema or schema unit specified by the request, a fingerprint of this information MUST be included with each such reference as specified in [METASYN]. The schema writer MUST also include a special caveat metadata element (as specified in [METASYN]) if at least one such
2.7 Change Control

Once a listing has been published by the primary repository operator, the contact person may request a change to its definition. The contact person for a listed schema is defined to be the person or organizational role or entity who submitted the original listing request.

The change request follows the same procedure as the listing request

1. Publish the revised listing request on the ietf-schema-review@pilot.schema.dir.reg.int list.

2. Leave at least two weeks for comments.

3. Publish using the primary listing repository operator after formal review if required.

Changes MAY be requested when there are serious omissions or errors in the published listing or when other factors which would justify a change request, such as an emerging need of the user community for a listed schema which cannot be addressed by that listed schema in its present form. When review is required, a change request MAY be denied if it renders entities that were valid under the previous definition invalid under the new definition.

The primary listing repository provider SHOULD attempt to verify the authority of a person claiming to be the contact for a listing, prior to implementing such changes.

The contact person for a listing MAY pass responsibility for that listing to another person or agency by informing the primary listing repository operator and the ietf-schema-announce@pilot.schema.dir.reg.int list; this can be done without discussion or review.

The IESG may reassign responsibility for a listing. The most common case of this will be to enable changes to be made to types where the contact person for the listing has died, moved out of contact, or is otherwise unable to make changes that are important to the community.

Listings will not be deleted; listings which are no longer believed appropriate for use can be declared OBSOLETE by a change to their "intended use" field; such listings will be clearly marked in repository content summary RFCs published by the primary listing repository operator.
2.8 Listing Request Formats

2.8.1 Schema Unit Listing Request Format

To: ietf-schema-review@pilot.schema.dir.reg.int
Subject: schema unit listing request
MIME-Version: 1.0
Message-Id: <ids1@wherever.com>
Content-Type: multipart/related; start=3@foo.com; boundary="boundary"
Content-ID: top@foo.com

--boundary
Content-Type: text/directory;
    profile="schema-metadata-0";
    charset="utf-8"
Content-Transfer-Encoding: Quoted-Printable
Content-ID: 3@foo.com

(metadata elements and values as specified in [METASYN] and embedded in a text/directory MIME component of profile "schema-meta-0")

--boundary
Content-Type: text/directory;
    profile="<mimedir-profile-type>";
    charset="utf-8"
Content-Transfer-Encoding: Quoted-Printable
Content-ID: 3@foo.com

(a schema specification compliant with a profile of [MIMEDIR] corresponding to the value of <mimedir-profile-type>)

--boundary

Where:

<mimedir-profile-type> = "schema-ldap-0" / "schema-whoispp-0" / "schema-whois-0" / "schema-rwhois-0"
2.8.2 Schema Pak Listing Request Format

To: ietf-schema-review@pilot.schema.dir.reg.int
Subject: schema pak listing request
MIME-Version: 1.0
Message-Id: <ids1@wherever.com>
Content-Type: text/directory;
    profile="schema-metadata-0";
    charset="utf-8"
Content-Transfer-Encoding: Quoted-Printable

(metadata elements and values as specified in [METASYN] and embedded
in a text/directory MIME component of profile "schema-meta-0")

2.9 Primary Repository Operator Responsibilities and Constraints

The data residing in the repository is not the property of the
repository operator. Since the schema actually listed are the
intellectual property of the entities creating the listing, the
repository operator cannot claim them as intellectual property. All
metadata surrounding the system is considered to be either in the
public domain or is owned by the IANA (or some other suitable
entity). The repository operator can make no claims whatsoever of
ownership over any data in the repository.

The repository operator can also make no determinations of
appropriateness or suitability of a schema to be listed. This
responsibility rests solely with the members of the listing request
review committee (the members of the listing request review mailing
list). If the list coordinator requests that the repository operator
publish a schema listing, the repository operator MUST include the
schema listing or be relieved of the responsibility of running the
repository.

Currently, the ability to advertise products and services on the
repository web site to recoup monies used in operating the service is
allowed. At any time, the review committee make make a policy
decision on the appropriateness of ads on the repository pages.

3.0 Security Considerations

As described in [LISTRQMT], the subject of trust with respect to most
aspects of the service involving the exchange of information
(submitting a listing request, updating an existing listing, or
retrieving a listing) is not addressed in this document. However, the
primary schema listing repository operator will take reasonable steps
to ensure that information associated with the service is as accurate
and authentic as possible.
If users of the schema listing service obtain and use listings from the repository, they SHOULD verify that any fingerprints contained as a part of metadata for references to related content hosted outside of the repository are valid. This can be verified by computing the MD5 checksum [RFC1321] of the referenced content and comparing it with the fingerprint value. If this verification fails, the user of this schema information can assume that this external content has changed after the listing was published. In any case, no repository operator has control over external content referenced by URIs in the metadata. Thus the establishment of trust as it relates to the validity of fingerprints and the content which they represent is solely the user’s responsibility and is OPTIONAL.

4.0 Acknowledgements

The format and much of the content in this document is based on [RFC2048].

The engineering team for listing service requirements:

Chris Apple - AT&T Labs
Michael Mealling - NSI
Sanjay Jain - Oracle
John Strassner - Cisco
Sam Sun - CNRI
Mark Wahl - Critical Angle
Chris Weider - Microsoft

Paul Hoffman for review and comments resulting from his effort to develop a platform for the initial release of the schema listing service.

5.0 References


6.0 Authors’ Address

Chris Apple
Room 2F-165
AT&T Labs
600 Mountain Ave
Murray Hill, NJ 07974
US

Phone: +1 908 582 2409
Fax: +1 908 582 3296
Email: capple@att.com

Michael Mealling
505 Huntmar Park Drive
Herndon, VA 22070
US

Apple, Mealling

[Page 16]
This Internet-Draft expires on October 21, 1998.