Standardization Priorities for the Directory

Directory Interoperability Forum White Paper

December 2001

THE Open GROUP
... working for interoperability

Standardization Priorities for the Directory
Directory Interoperability Forum White Paper

Document Number: W012
UK ISBN: 1-85912-267-1
US ISBN: 1-931624-11-9

Any comments relating to the material contained in this document may be submitted to:

The Open Group
Apex Plaza
Forbury Road
Reading
Berkshire, RG1 1AX
United Kingdom

Management Summary

It is now generally recognized that directories form a critical part of the infrastructure necessary to support an enterprise's information and communications services. Such services are essential in order to conduct all styles of e-business. In order support consistent end-to-end e-business transactions and other processes across multiple, multi-vendor systems it is therefore necessary that directory services be integrated and unified. This requires open standards.

The Directory Interoperability Forum (DIF) was formed in July 1999 and since July 2000 has been managed by The Open Group. The primary aim of the DIF is to enable and promote open and interoperable directories based on open standards. This will make directories more usable, ensuring that any applications written to use an open directory can run with any directory without regard to the supplier, and making it easier for software developers to create such applications.

However, some problems currently exist in the area of directory standardization. Specifically:

- There are a number of different bodies each developing directory related standards.
- There is a wide range of potential areas for directory standardization, some of which are being actively progressed, some of which have been started but have stalled, and some which have simply not been undertaken yet.

The Standards Co-ordination Working Group within the DIF is taking on the challenge of attempting to provide some focus to the various directory standardization efforts and to influence which specific areas of directory services most urgently require standardization. A first step towards this goal was to undertake a survey of the DIF membership in order to determine their priorities for standardization within the directory. This White Paper reviews the results of that survey, the current state of standards efforts on the items recognized by the survey as priorities, and documents the steps agreed to by DIF members to promote the progress of standards in these areas.

In summary, the DIF membership believe that the most urgent areas for directory standardization are:

- Directory service security
- Directory synchronization
- Onward progression of existing base directory standards
- Directory server replication
- Directory and XML

This White Paper documents the intent of DIF members to implement and support some recently emerging standards, and to participate in each of the relevant directory standards bodies in order to influence and to expedite the development of open standards where the current state of the standards does not suffice to address these priorities.

Table of Contents

Introduction

In early 2001, the Standards Co-ordination Working Group within the Directory Interoperability Forum (DIF), managed by The Open Group, conducted a survey of all DIF members to establish which areas of directory standardization they considered to currently be the most urgently required. This White Paper reports the results of that survey.

The opening section provides some brief background on the various bodies involved in the development of directory standards.

Details of the survey were then recorded, including a classification of general directory standardization into 16 more specific areas, a copy of the questionnaire that was distributed, a list of the respondents, and the actual results.

It is intended that this White Paper be used by the DIF to publicize its members' priorities for directory standardization. The DIF will also approach the relevant standards bodies involved in order to promote and advance the development of standards in the areas identified.

Directory Standardization Bodies

A variety of regional and international bodies have taken responsibility for standardizing different aspects of directory services. The most important organizations are summarized briefly in this section.

IETF

The IETF (Internet Engineering Task Force) is the body that defines the standards that govern the Internet. It is a large, open, international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual.

The IETF is responsible for the Lightweight Directory Access Protocol (LDAP), which is the primary means by which directories are accessed over the Internet. The IETF currently has three working groups related specifically to LDAP related standards:

LDAPext (LDAP Extensions)

LDAP, Version 3 (LDAPv3) is defined by a core set of RFCs produced by the now dissolved IDS (Internet Directory Services) Working Group. However, LDAPv3 has been designed to be extensible and the LDAPext Working Group is responsible for standardizing LDAPv3 extensions. These extensions include features such as:

- An access control model for LDAPv3 accessible directory information
- The use of language codes with LDAPv3
- Extensions for dynamic directory services
- The LDAP Data Interchange Format (LDIF) specification
- Java and C APIs for LDAP

LDUP (LDAP Duplication/Replication/Update Protocols)

This group is standardizing the architecture, models, protocol, and procedures necessary to support the replication of directory information across multiple LDAPv3 accessible directory servers. This is needed because, as LDAPv3 becomes more widely deployed, the replication of data across servers running different implementations becomes an important part of providing a unified but distributed directory service.

LDAPbis

The primary goal of this group is to replace the existing set of core LDAPv3 RFCs, which represent an IETF Proposed Standard, with a new set of RFCs which move the core LDAPv3 specification forward to become IETF Draft Standard status.

In addition to the three working groups above, other IETF groups also have responsibility for developing LDAP-related standards within their specific sphere of interest, typically to define directory schema items. Examples of such working groups are PKIX, Policy, and IPP.

ISO/ITU-T

ISO is a worldwide federation of national standards bodies from some 130 countries, one from each country. It is a non-governmental organization established in 1947, whose mission is to promote the development of standardization and related activities in the world. Its work results in international agreements which are published as International Standards.

The ITU is an organ of the United Nations (UN) within which governments and the private sector coordinate global telecommunications networks and services. Its Telecommunications Standardization Section (ITU-T) fulfils the purposes of the ITU relating to telecommunications standardization by studying technical, operating, and tariff questions and adopting Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

ISO and the ITU-T (formerly known as the Committée Consultitatif International Téléphonique et Télégraphique – CCITT) established their Joint Technical Committee number 1 (JTC1) to develop standards for Information Technology, including standards for Open Systems Interconnection (OSI). These have largely been rendered irrelevant by the development of the Internet. However, the OSI standards for directories are still important. These are published by the ITU as the X.500 Series Recommendations, and by ISO as International Standard 9594. LDAP was originally derived from the X.500 Directory Access Protocol (DAP) and assumes many aspects of the X.500 directory model.

DMTF (DEN)

The DMTF (Distributed Management Task Force) is the industry organization that is leading the development, adoption, and unification of management standards and initiatives for desktop, enterprise, and Internet environments.

The DMTF is responsible for the Directory-Enabled Networks (DEN) specification. DEN is designed to provide the building blocks for more intelligent networks by mapping users to network services, and mapping business criteria to the delivery of network services. This will enable applications and services to transparently leverage network infrastructure on behalf of the user, empower end-to-end services, and support distributed network-wide service creation, provisioning, and management. DEN specifies a Common Information Model (CIM) with LDAP mappings from CIM to X.500. This provides a template for exchanging information and enables vendors to share a common definition of a device, application, or service, and allows for extensions that add value.

OASIS (DSML)

DSML (Directory Services Mark-Up Language) is intended to be the mark-up language for representing directory services in XML. The intention of the dsml.org Working Group is to establish DSML as an open standard, so that developers and vendors will be able to adopt it into their systems.

The dsml.org Working Group has given the DSML 1.0 draft to OASIS (the Organization for the Advancement of Structured Information Standards) for standardization. OASIS is a non-profit, international consortium that creates interoperable industry specifications based on public standards such as XML and SGML, as well as others that are related to structured information processing.

NAC

The NAC (Network Applications Consortium) is a customer-oriented consortium that does requirements analysis and other work in the area of network applications. It has produced the Lightweight Internet Person Schema (LIPS) for directory representation of information about people. More recently, it has produced a positioning paper on the exploitation of directories within e-business applications.

CEN/ISSS

The Information Society Standardization System (ISSS) of the European Committee for Standardization (Committée Européen pour Normalization – CEN) is an initiative whose mission is to provide market players with a comprehensive and integrated range of standardization-oriented services and products, in order to contribute to the success of the Information Society in Europe.

CEN/ISSS included a Directory Workshop which was the successor of the Directory Expert Group of the now dissolved EWOS (European Workshop for Open Systems), and which continued with uncompleted work items from EWOS in addition to working on some new items. Its purpose was to

promote the use of directory technologies by providing technical specifications and guidance material, and to explore and give guidance on naming issues, especially for directory names and Internet domain names. Deliverables included:

- Directory profiles
- Guidance material in the form of CEN Workshop Agreements (CWAs)
- Information provided on its web pages
- Contributions to the base X.500 standardization work

The CEN/ISSS Directory Workshop has now completed this work and the group was dissolved in May 2001.

DIF Standards Survey

Background

The primary goal of this survey was to consider the areas of directory standardization currently covered by the various bodies described above and then:

- To determine what current, emerging, or possibly new directory standards are considered by the DIF membership to be the most urgently required.
- To supply this information to the relevant directory standards bodies in order to influence the development and implementation of such standards.

The first step in this process was to attempt to classify the very wide scope of general directory standardization down into a number of specific areas (covered in the following section). A questionnaire based around these areas could then be distributed to the DIF membership to determine their particular priorities.

Areas of Standardization

Potentially, directory standardization work can cover a wide range of functionality. To assist in clarifying priorities, the DIF Standards Coordination Working Group broke directory standardization down into sixteen logical areas as follows:

1. Onward progression of existing base directory standards
2. Directory service extensions
3. Distributed directory operation
4. Directory server replication
5. Directory service security
6. Directory service administration and monitoring
7. Directory internationalization
8. Directory APIs
9. Directory-enabled networking (DEN)
10. Directory-enabled PKI
11. Other directory-enabled applications
12. Directory and XML
13. Directory schema definitions
14. Directory service discovery
15. Other service/business discovery
16. Directory synchronization

The Questionnaire

The DIF Standards Co-ordination Working Group distributed a questionnaire (based around the 16 areas introduced above) to all DIF members in early 2001. The questionnaire is reproduced in Appendix A: The Survey Questionnaire.

Respondents

The initial respondents to the survey consisted primarily of most of the world's major directory product vendors plus some other large organizations. In alphabetical order these were:

Critical Path	IBM	Nortel	SAP
DISA	iPlanet	Novell	Siemens
EDS	Microsoft	Oracle	

The collated results from these respondents were then distributed to all user organizations within the DIF for further validation. This included the recently established EMA Forum within The Open Group which contains representatives from many large-scale, national, and multi-national enterprises.

Results

As a result of this membership survey and the validation of its results by many of the world's major directory user organizations, the DIF believes that the following five areas of directory standardization (in priority order) must be addressed urgently:

1. Directory service security
2. Directory synchronization
3. Onward progression of existing base directory standards
4. Directory server replication
5. Directory and XML

Each of these five areas is expanded upon in the following sections.

Directory Service Security

This area was considered to be far and away the highest priority for directory standardization.

Although certain aspects of security such as authentication and confidentiality are already covered in base directory standards, there remains an urgent need for the definition of:

1. A standard access control model for use by LDAPv3 accessible directories
   (The DIF therefore recommends that high priority be given to successful completion of the IETF LDAPext proposed standard in this area.)
2. A standard model and procedures for the consistent use and administration of passwords within LDAPv3 accessible directories
   (The DIF therefore recommend that high priority be given to successful completion of the IETF LDAPext proposed standard covering password policy.)

In addition, the DIF Security Working Group has developed a Directory in Key Management Infrastructure (KMI) Business Scenario (see Reference Documents). The document identifies a number of requirements for standardization (all of which are KMI-related, but some of which would also apply to a wider range of applications).

Directory Synchronization

The ability to have some level of standardized functionality which could be exploited within directory synchronization and "meta-directory" solutions was considered extremely urgent.

In particular, a standardized method to generate and receive change notification events applying to LDAPv3 accessible directory information was repeatedly requested. Such a method could be exploited by specialized directory clients, agents, and other servers in order to regulate and synchronize changes being applied across disparate data sources.

The DIF therefore recommends that standardization of directory change notification be reviewed and that high priority be given to successful completion of the IETF proposed standard covering LCUP (the LDAP Client Update Protocol) currently being progressed within the LDUP group.

Onward Progression of Existing Base Directory Standards

Of equal importance to the directory synchronization work above, the DIF believes that progression of the existing base directory standards is considered extremely urgent. This covers two aspects strongly recommended by the DIF that:

1. The IETF LDAPbis work to move the core LDAPv3 standard forward to IETF Draft Standard status be given high priority.
2. The IETF and the ISO/ITU-T liaise to align the LDAPv3 and X.500 standards together wherever practically possible.

Directory Server Replication

The ability to replicate a level of LDAPv3 accessible directory information between different servers (potentially multi-vendor) in a standardized manner is considered an urgent requirement by the DIF.

A number of vendors currently provide proprietary replication in varying degrees from a straightforward master-slave model through to a full multi-master model. Also, certain directory servers can replicate information in a master-slave model using the X.500 standard DISP (Directory Information Shadowing Protocol) to a relatively sophisticated level – however, this is typically achieved in a single-vendor environment only.

In order to fulfil the requirement for standardized directory replication, the DIF strongly recommends that:

1. Completion of the IETF LDUP work to standardize replication between LDAPv3 accessible directory servers (progressing up to a full multi-master model) be given a high priority.
2. Multi-vendor testing of replication between X.500-based LDAPv3 accessible directory servers using DISP be undertaken to prove a level of standardized interoperability.

Directory and XML

The initial work done by the dsml.org Working Group for standardization as DSML 1.0 by OASIS was recognized by the DIF as an important first step to represent basic directory schema and data within an XML document format.

However, the DIF also recognizes that standardization of DSML 2.0 to provide an XML-oriented interface to information stored in one or more directories is now an urgent requirement. In particular, the capability to support standardized, XML-based access to directory schema details and associated information is considered a key requirement. The DIF will therefore attempt to influence and expedite the proposed DSML 2.0 standardization work within OASIS.

In addition to the above five key areas, the DIF membership also highlighted a number of other aspects of directory functionality where standardization is considered important. In summary, these were (in no particular priority order):

- Directory service extensions:
    - Server-side sorting of LDAPv3 search results
    - Scrolling-view browsing of LDAPv3 search results
    - LDAPv3 control for simple paged results
    - Returning matched values with LDAPv3
    - Grouping of related LDAPv3 operations
- Distributed directory operation (server-to-server referrals and chaining)
- Evolving LDAP Schema Entries (proposed ELSE Working Group in the IETF)
- LDAP service discovery using DNS
- Directory-enabled PKI (specifically the IETF PKIX schema and LDAPv3 profile)

Conclusions

The following standards are priorities for implementation, in addition to what is required to support The Open Brand for LDAP 2000. These standards offer a guide especially to LDAP server vendors, as to what may be required in future versions of the LDAP 2000 brand, and to LDAP application vendors, as to function that may be exploited in conformance with future versions of the Works With LDAP 2000 brand.

1. RFC 2829: Authentication Methods for LDAP
2. RFC 2830: Lightweight Directory Access Protocol (v3) – Extension for Transport Layer Security
3. RFC 2891: LDAP Control Extension for Server-Side Sorting of Search Results

The following items are priorities for standardization. Definition of these standards is not complete, and progress has been slow on some items, but DIF members agree to assist in the progression of these standards by active participation in standards discussions, and, where appropriate, by creating sample implementations. It is understood that these items also may be included in future versions of the LDAP 2000 and Works With LDAP 2000 brands.

1. Access Control Model for LDAP, taking as a starting point the recommendations of RFC 2820
2. Completion of and conformance to IETF LDAPbis
3. ISO/ITU-T and IETF X.500/LDAP alignment
4. Support for signed directory operations, leveraging the approach documented in RFC 2649, but extending this proposal as needed to meet known requirements
5. The DSML 2.0 standard, including interoperable implementations over standard transports such as SOAP
6. Change notification, including persistent search and event notification as specified by the LDAP Client Update Protocol (LCUP) draft
7. Uniform means for storing referral information, such as proposed in Internet draft draft-zeilenga-ldap-namedref-04.txt
8. Uniform means for storing and locating of schema information in the directory, as proposed in Internet draft draft-hahn-schemapart-00.txt
9. Scrolling view browsing of search results, as proposed in Internet draft-ietf-ldapext-ldapv3-vlv-04.txt
10. Update of RFC 2587, PKIX LDAP Schema to be based on LDAP v3 rather than LDAP v2

Reference Documents

1. Directory in the Key Management Infrastructure Business Scenario, The Open Group White Paper, Doc. No. W011
2. LDAP 2000, The Open Group Product Standard, Doc. No. X99DI
   (This document provides the functional definition of The Open Brand for LDAP 2000.)
3. IETF RFC 2587: Internet X.509 Public Key Infrastructure - LDAPv2 Schema
4. IETF RFC 2649: An LDAP Control and Schema for Holding Operation Signatures
5. IETF RFC 2820: Access Control Requirements for LDAP
6. IETF RFC 2829: Authentication Methods for LDAP
7. IETF RFC 2830: Lightweight Directory Access Protocol (v3) – Extension for Transport Layer Security
8. IETF RFC 2891: LDAP Control Extension for Server-Side Sorting of Search Results

The Open Group publications can be obtained on-line from The Open Group Publications web site at http://www.opengroup.org/publications.

IETF RFCs can be obtained on-line from the IETF RFC web site at http://www.ietf.org/rfc.html.

Refer to Appendix B: Internet Drafts for descriptions of the Internet Drafts mentioned in this White Paper.

Appendix A: The Survey Questionnaire

The DIF Standards Co-ordination Working Group has been actioned to find out what current, emerging, or possibly new directory standards are considered by the DIF membership to be the most urgently required. It is intended that this information be used by the DIF to influence and expedite the development of those standards and their implementation by directory product vendors. From the 16 general areas of directory standardization identified below, would individuals please reply with what they consider to be their 5 areas of highest priority. (No particular priority order is required.)

In order to minimize the time necessary to reply, simply list your priorities using the relevant reference numbers. As some of the areas include a lot of underlying standards work items, please also indicate which (any number) of those you consider to be particularly important. If any specific work item is important to you but outside of your 5 areas of priority, then please identify it separately.

As an example, if you consider your top 5 areas to currently be:

> **base standards progression, replication, security, XML, synchronization**

and specific work items within those areas to be:

> **LDAPbis, LDUP, access control for LDAP, LDAP authentication password attribute, password policy for LDAP, DSML 2.0, LCUP**

and you also consider further work items outside your top 5 areas to be important, such as:

> **server-side sorting, scrolling view browsing, referrals in LDAP, language codes in LDAP**

then you would simply reply:

> **"My top 5 areas (and associated work items) are:**
> **1 (1.1) 4 (4.1) 5 (5.1, 5.3, 5.4) 12 (12.2) 16 (16.2)**
> **Other important work items outside of those areas are: 2.4, 2.6, 3.1, 7.1"**

Note: If there are any further directory-related areas or features not covered below that you would like to see progressed then please describe them.

Any other comments are also welcome.

DIRECTORY STANDARDIZATION – PRIORITIES

1. Onward Progression of Existing Base Directory Standards

1. The IETF "LDAPbis" work to supersede the existing LDAPv3 client-server Proposed Standard (RFCs 2251-56 and 2829-30) by a new set of RFCs progressing towards IETF Draft Standard status.
2. Publication of the ISO/ITU-T 4th edition of X.500 (2001). This includes features such as:
    a. An extended/restructured X.509 covering PKI and PMI
    b. X.500 protocols directly over TCP/IP
    c. Subtrees of entries handled together as "families"
    d. Hierarchical groups of entries linked across the DIT
    e. Pre-configured search rules for relaxation/tightening

f. Geographical/zonal matching of entries

3. Development of an ISO/ITU-T 5th edition of X.500. Work items being proposed include:
    a. LDAP/X.500 alignment
    b. Related entries
    c. Further X.509 enhancement
    d. Distributed paged results
    e. "Friend" attributes

2. Directory Service Extensions

Specific extensions to directory base standards to provide particular functionality.

1. Connectionless LDAP (draft)
2. Using Domains in LDAP/X.500 Distinguished Names (RFC 2247)
3. Extensions for Dynamic Directory Services (RFC 2589)
4. Server Side Sorting of LDAP Search Results (RFC 2891)
5. LDAP Control for Simple Paged Results (RFC 2696)
6. Scrolling View Browsing of Search Results (draft)
7. Result Message for LDAP Controls (draft)
8. Extended Partial Response Protocol Enhancement (draft)
9. Returning Matched Values with LDAPv3 (draft)
10. Duplicate Entry Representation of Search Results (draft)
11. LDAP and X.500 Component Matching Rules (draft)
12. Extended operation to cancel/abandon an operation (draft)
13. LDAPv3: Grouping of Related Operations (draft)

3. Distributed Directory Operation

The definition of standardized mechanisms to enable client access to a logically centralized directory service (but where that service might be provided by a physically distributed set of servers).

1. Referrals in LDAP Directories (draft)
2. Named Subordinate References in LDAP Directories (draft)
3. LDAP Control to Specify Chaining Behavior (draft)
4. X.500 standard chaining

4. Directory Server Replication

Standardized mechanisms to replicate information between directory servers.

1. LDUP (Proposed IETF standard for an LDAPv3 multi-master replication model, architecture, procedures, protocol, and management)
2. X.525 master-slave replication

5. Directory Service Security

Authentication and confidentiality are covered within the base directory standards. This area relates to any other security aspects.

1. Access Control Model for LDAP (draft)
2. X.500 Access Control Model (Basic Access Control)
3. LDAP Authentication Password Attribute (draft)
4. Password Policy for LDAP Directories (draft)
5. LDAP Authentication Response Control (draft)
6. LDAP Control and Schema for Holding Operation Signatures (Experimental RFC 2649)

6. Directory Service Administration and Monitoring

This is an area which generally has not been standardized but where certain work items could still be considered to apply:

1. Data import/export: LDAP Data Interchange Format, LDIF (RFC 2849)
2. Directory Server Monitoring MIB (RFC 2605)
3. Recommendations for Recording Directory Access Data (draft)
4. ELSE – Evolving LDAP Schema Entries (proposed IETF work). This will include standards for aspects such as:
    a. The merging, updating, and removal of schema
    b. How to determine allowable changes to existing schema
    c. Object class/attribute type definition extensions
    d. Partitioning of different schema within different DIT areas

7. Directory Internationalization

Existing standards cover basic double-byte Unicode/ISO 10646 support and UTF-8 encoding. However, further related items could be considered:

1. Use of Language Codes in LDAP (RFC 2596)
2. X.500 3rd edition attribute contexts
3. Specific Chinese/Japanese/Korean-related standards handling (S-JIS, EUC, KS-5601, etc.)

8. Directory APIs

1. C LDAP API (draft)
2. Java LDAP API (draft)
3. The Java SASL API (draft)
4. JNDI

9. Directory-Enabled Networking (DEN)

This is based on the general Common Information Model (CIM) work undertaken in the DMTF with specific LDAP mappings (primarily schema) being input to the IETF.

1. Policy Framework LDAP Core Schema
2. LDAP Schema for the DMTF Core CIM Model
3. LDAP Schema for the DMTF Physical CIM Model
4. LDAP Schema for the DMTF Network CIM Model
5. LDAP Schema for the DMTF System CIM Model
6. LDAP Schema for the DMTF Device CIM Model
7. LDAP Schema for the DMTF Application CIM Model

10. Directory-Enabled PKI

For example, covering the existing and emerging IETF PKIX profiles:

1. Internet X.509 PKI Operational Protocols – LDAPv2 (RFC 2259)
2. Internet X.509 PKI LDAPv2 Schema (RFC 2587)
3. Internet X.509 PKI Operational Protocols – LDAPv3 (draft)
4. Internet X.509 PKI Additional LDAP PKI/PMI Schema (draft)

11. Other Directory-Enabled Applications

This covers any other applications work where basic directory standards, guidelines, and recommendations might be required; e.g., e-flow, mobile, etc.

1. Service Provider Directory-enabled Network Applications (SP-DNA). (The definition of a framework to support multiple directory-enabled SP network applications exploiting a single directory infrastructure.)

12. Directory and XML

Any specific standardization efforts covering XML and directory integration/exploitation. For example:

1. DSML 1.0 (basic directory schema/data representation in an XML document format)
2. DSML 2.0 (XML-oriented interface to information stored in one or more repositories/directories)

13. Directory Schema Definitions

A variety of directory schema standards and recommendations exist (some of which are covered under other areas here). Further examples include:

1. Schema for Representing Java Objects in an LDAP Directory (RFC 2713)
2. Schema for Representing CORBA Objects in an LDAP Directory (RFC 2714)
3. Definition of the inetOrgPerson LDAP Object Class (RFC 2798)
4. ACP 133 Common Content and LDAP (draft)
5. Internet Printing Protocol (IPP): LDAP Schema for Printer Services (draft)
6. Kerberos KDC LDAP Schema (draft)
7. LDAP Schema for NDS (draft)
8. LDAP vCard Schema (draft)
9. A Configuration Schema for LDAP-Based Directory User Agents (draft)

10. The following schema standards are especially important for interoperability, and therefore should be priorities for the DIF:

    a. Schema for referral information (draft-zeilenga-ldap-namedref-03.txt)

    b. An approach for identifying different schemas in effect across the directory name space (draft-hahn-schemapart-00.txt)

    c. LDAP schema update procedures (draft-poitou-ldap-schema-update-01.txt)

14. Directory Service Discovery

Standardized mechanisms and guidelines to discover directory servers and services:

1. A Taxonomy of Methods for LDAP Clients Finding Servers (draft)
2. Discovering LDAP Services with DNS (draft)

15. Other Service/Business Discovery

Any other standardization efforts in the area of directory discovery and look-up:

1. UDDI (Universal Description, Discovery, and Integration). The proposed development of standards for the registration, discovery, and use of Web e-services (based upon SOAP, XML, HTTP, TCP/IP) – underlying directory technology requirements yet to be defined.

15. Directory Synchronization

The areas of directory synchronization and "meta-directory" have not been standardized. Indeed, the nature of the problem they are attempting to solve (connecting to disparate data sources, joining and manipulating information, etc.) makes it a difficult area to standardize. However, some standards to assist in the operation and management of this area could be considered, for example:

1. Definition of an Object Class to Hold LDAP Change Records (expired draft)
2. LDAP Client Update Protocol - LCUP (draft)

Appendix B: Internet Drafts

This White Paper refers to work that is currently the subject of Internet Drafts.

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 made obsolete 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”.

The list of current Internet Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt. The list of Internet Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

Because Internet Drafts have only a limited lifetime, they are not cited as references by this White Paper. The identities and the abstracts of the drafts current at the time of publication that address areas that are priorities for standardization are given in the following sections.

The drafts are the copyright of The Internet Society, and the following copyright statement applies to them.

LDAP Client Update Protocol

[draft-ietf-ldup-lcup-01.txt]

This document defines the LDAP Client Update Protocol (LCUP). The protocol is intended to allow an LDAP client to synchronize with the content of a directory information tree (DIT) stored by an LDAP server and to be notified about the changes to that content.

Named Subordinate References in LDAP Directories

[draft-zeilenga-ldap-namedref-04.txt]

This document details schema and protocol elements for representing and manipulating named subordinate references in LDAP (RFC 2251) directories. A referral object is used to hold subordinate reference information in the directory. These referral objects hold one or more URIs (RFC 2396) contained in values of the ref attribute type and are used to generate protocol referrals and continuations. A control, ManageDsaIT, is defined to allow manipulation of referral objects as normal objects.

Approach for Identifying Different Schemas in Effect Across a Directory Name-Space

[draft-hahn-schemapart-00.txt]

IETF RFC 2251 provides a mechanism for indicating, given any particular entry in the directory tree, what entry in the directory tree holds the directory schema information for that particular entry. RFC 2251 does not, however, provide guidance on how different directory servers, each of which might have their own active directory schema, should publicize this directory schema such that the different active schemas are distinct from one another when viewing the entire directory name-space. This document describes a way to name sub-schema sub-entry entries such that different active schemas can be distinguished from one another across the entire directory name-space.

LDAP Extensions for Scrolling View Browsing of Search Results

[draft-ietf-ldapext-ldapv3-vlv-04.txt]

This document describes a Virtual List View control extension for the LDAP Search operation. This control is designed to allow the "virtual list box" feature, common in existing commercial e-mail address book applications, to be supported efficiently by LDAP servers. LDAP servers' inability to support this client feature is a significant impediment to LDAP replacing proprietary protocols in commercial e-mail systems.

The control allows a client to specify that the server return, for a given LDAP search with associated sort keys, is a contiguous subset of the search result set. This subset is specified in terms of offsets into the ordered list, or in terms of a greater than or equal comparison value.