

Directory Standardization Report

Kurt Zeilenga
Isode Limited

<http://www.isode.com>

First International LDAP Conference
6 September 2007

Outline

- ◆ A Brief History
- ◆ Current Standards
 - X.500 Series of ITU-T Recommendations
 - LDAP (and related) Standard Track RFCs
- ◆ Future of Directory Standards
- ◆ Significant Changes to LDAP Technical Specification

History

X.500 History

- ◆ ITU-T (CCITT) initiated development of a general-purpose directory in 1984, driven by X.400 Message Handling directory needs.
- ◆ ISO/IEC was also developing directory in support of OSI networking.
- ◆ These early efforts merged into a collaborative effort, know as the OSI Directory or simply X.500.

LDAP History

- ◆ LDAP arose out of efforts, in early 1990s, to provide a lightweight alternative to the X.500 Directory Access Protocol (DAP), which required (at that time) an OSI Network stack.
 - PSI's Directory Assistance Service [RFC1202]
 - U-Mich's DIXIE [RFC1479]
- ◆ LDAP is defined as a protocol for accessing an X.500 Directory Service.

LDAP History

- ◆ LDAP was originally developed by *Tim Howes* (U. of Michigan), *Steve Kille* (Isode), and *Wengyik Yeong* (PSI).
- ◆ LDAP was called the *Lightweight Directory Browsing Protocol* (LDBP) in its early stages of development, later renamed as the scope of the protocol expanded to include update operations.

Editions of X.500

- ◆ First edition - 1988
 - Basic directory operations
- ◆ Second edition - 1993
 - Refined Data Model, Replication, Access Control
- ◆ Third edition - 1997
 - Attribute contexts
- ◆ Fourth edition - 2000
 - Family of entries, TCP/IP support
- ◆ Fifth Edition - 2005 (current)
 - LDAP alignment

Versions of LDAP

◆ LDAPv1

- Development version. Not published.

◆ LDAPv2

- First Edition: “X.500 Lightweight Directory Access Protocol” [RFC1487], 1993.
- Second Edition: “Lightweight Directory Access Protocol” [RFC1777], 1995
- “LDAPv2 to Historic Status” [RFC3494], 2003.

Versions of LDAP

◆ LDAPv3

- First Edition: RFC 2251-2256, 1997. First published without SASL and TLS support.
- Authentication Methods (eg SASL), RFC 2829, 2000
- Extension for TLS, RFC 2830, 2000.
- LDAP Tech Spec, RFC 3377, 2002.
- Clarifies that RFC 2829 & 2830 are integral.
- Current Edition: RFC 4510-4519, 2006
- IANA Considerations for LDAP, BCP 64, RFC 4520
- Considerations for LDAP Extensions, BCP 118, RFC 4521

Standard Track

LDAP Extensions

- Dynamic Services [2589]
- Sorted Results [2891]
- Password Modify [3062]
- Referral [3296]
- Component Match [3687,3727]
- Collective Attrs [3671]
- Subentries [3672]
- All Op Attrs [3673]
- Addl. Match Rules [3698]
- Language Tags [3866]
- Matched Values [3876]
- Cancel Op [3909]
- LCUP [3928]
- Proxied Authz [4403]
- ;binary [4522]
- X.509 schema [4523]
- COSINE schema [4524]
- (&) (|) filters [4526]
- Read Entry [4527]
- Assertion [4528]
- entryUUID [4530]
- whoami? [4532]
- entryDN [5020]

Considerations for LDAP Extensions

- BCP 118 [RFC 4521] published
- Extensions MUST be *truly optional*

Ongoing Work

Ongoing X.500 work

- ◆ 6th Edition expected in 2008
- ◆ Federation of Privilege Management Infrastructures (PMI)
- ◆ Communication Support Enhancements
 - Extensions to use TCP/IP instead of OSI Network
 - Extensions to use IPv6
 - RFID attributes
- ◆ Miscellaneous Extensions
 - Password Policies (to be proposed by Isode)

LDAP in the IETF

- ◆ LDAPbis WG concluded in 2006 after publication of the revised LDAP tech spec.
- ◆ Extension continues to be pursued on an individual basis.
- ◆ General need to revise LDAP extension specifications.
- ◆ Apps Area review of LDAP extension specifications may move from the LDAP Directorate to the Apps Review Team.

Ongoing LDAP Work

- ◆ Using LDAP over IPC
 - draft-chu-ldap-ldapi
- ◆ X.500 Admin Model in LDAP
 - draft-legg-ldap-admin
- ◆ X.500 Access Controls in LDAP
 - draft-legg-ldap-acm-admin

Ongoing LDAP Work

- ◆ Distributed Operations
 - draft-...
- ◆ Session Tracking
 - draft-wahl-ldap-session
- ◆ AdministratorsAddress attribute
 - draft-wahl-ldap-adminaddr
- ◆ Subtree Data Source URI Attribute
 - draft-wahl-ldap-subtree-source

Ongoing LDAP Work

- ◆ Don't Use Copy Control
 - draft-zeilenga-ldap-dontusecopy
- ◆ Relax Rules (ManageDIT) Control
 - draft-zeilenga-ldap-relax
- ◆ No-Op Extended Operation
 - draft-zeilenga-ldap-noop
- ◆ X.500 Password Policies in LDAP
 - draft-zeilenga-ldap-passwords (soon)
- ◆ Transactions
 - draft-zeilenga-ldap-txn

Related Standardization Efforts

- ◆ XML Enabled Directory work continues on an individual basis, driven by Steven Legg.
 - See [draft-legg-xed-roadmap-xx.txt](#)
- ◆ SASL revision work continues. RFC 4422 to be revised to achieve draft standard status.
- ◆ vCardDAV spinning up - provides protocol to access/update vCards content

Participation

◆ X.500

- <http://www.x500standard.com>

◆ LDAP Revision (LDAPbis)

- <http://www.ietf.org/html.charters/OLD/ldapbis-charter.html>
- ietf-ldapbis@openldap.org

◆ LDAP Extensions (LDAPext)

- <http://www.ietf.org/html.charters/OLD/ldapext-charter.html>
- ldapext@ietf.org

LDAP Technical Specification Changes

- ◆ Many changes were made in the revised LDAP Technical Specification (TS)
- ◆ In general, implementations of the old and new TSs will interoperate... no version bump
- ◆ But there are a few important changes implementors should make...

Internationalization

- ◆ Servers should use LDAPprep in matching.
 - LDAPprep is a multiple step (transcode, map, normalize, prohibit, check bidi, spaces) “stringprep” algorithm for preparing text for matching in LDAP.
- ◆ Clients should prepare textual passwords.
 - Convert to Unicode, apply SASLprep, encode in UTF-8.

New MTI Authentication/Security Mechanism

- ◆ MTI = mandatory to implement
- ◆ Was SASL/DIGEST-MD5
- ◆ Now StartTLS+Simple(DN,password)

TLS Server Identity Check

- ◆ Updated to support International Domain Names
- ◆ Now includes IP address (v4 and v6) checks
- ◆ Other subject alternative name checks may be supported

Misc

- Avoid LDAPv2isms
 - DN in LDAPv3 should not contain LDAPv2isms (such as spaces after RDN separators)
- Controls
 - Okay for a server to ignore a recognized non-critical control instead of failing with `unwillingToPerform`.
- `errorMessage` now `diagnosticMessage`
 - can be returned anytime (even on success)
- return of `matchedDN` no longer restricted to particular error cases.

Q&A