THE Open GROUP

LDAP Certified: Consistent Results for LDAP Customers

A White Paper by:

The Directory Interoperability Forum (DIF)

July, 2003

LDAP Certified: Consistent Results for LDAP Customers

ISBN No.: 1-931624-34-8

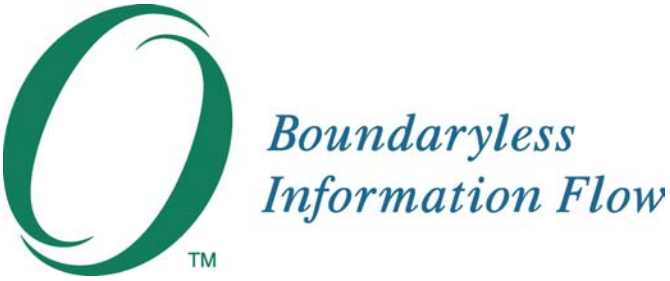
Document No.: W032

Published by The Open Group, July, 2003

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

ogspecs@opengroup.org

Table of Contents



Boundaryless Information Flow™
achieved through global interoperability
in a secure, reliable, and timely manner

Abstract

Certification of conformance with the Lightweight Directory Access Protocol (LDAP), a specification for accessing and creating directory information, addresses customers' desire for interoperable directory products. In doing so, it saves companies money and improves their ability to move information in a secure, reliable, and timely manner. This paper introduces the reader to the advantages and components of the third-party LDAP certification programs operated by The Open Group.

Executive Summary

A directory is a special-purpose dataset—not a general-purpose database—and is potentially a powerfully tool of commerce, government, and education. It can provide a standard repository for data shared by operating systems and applications. It can also give partners and customers controlled access to selected information, simplify enterprise administration, and enable massive cost savings.

LDAP Certified aims to increase customer confidence to purchase directories through the promotion of open directory standards such as LDAP.

Directory technologies can be combined with others to solve key problems related to information flow within and between enterprises. This is true only if they interoperate, however. In an effort to move toward the vision of secure, reliable, and timely information flow within and between enterprises—a vision The Open Group calls Boundaryless Information Flow—many organizations have turned to LDAP to standardize their approach to creating and accessing directory information.

LDAP is a complicated protocol, offering multiple ways to solve the same problems. The last thing an executive wants to hear from a vendor about LDAP servers or directory-enabled applications is: "You have to support us slightly differently..."

In implementing LDAP, a handful of considerations will determine the success or failure of the effort. In short, they involve architecture, security, a data strategy vision, a plan for rollout, and, at the top of the list, conformance to the LDAP specification developed by the Internet Engineering Task Force (IETF).

Many documents providing guidance say: "compliance to the IETF standard". Successful implementation, however, lies in the interoperability of LDAP products, achievable through strict *conformance* to key requirements of the standard, not just loose adherence to what the implementer believes to be its spirit.

LDAP Certified is a program of The Open Group Directory Interoperability Forum (DIF), whose aim is to increase customer confidence to purchase directories through the promotion of open directory standards such as LDAP. Members are architects, strategists, and product managers from customers and vendors of directories and directory-enabled applications.

Goal of LDAP Certification

The goal of *LDAP Certified* is straightforward: to signify guaranteed conformance of directory servers to Version 3 of the Lightweight Directory Access Protocol (LDAP).

This gives application vendors a solid base on which to build their products and know that they will interwork.

This in turn enables customers to buy LDAP products from multiple vendors with confidence.

History of LDAP and the LDAP Certification Program

LDAP is a development of the international directory standard called X.500 that preceded the need for a standard applicable to the Internet environment. The Internet Engineering Task Force (IETF) developed LDAP, also known as X.500 Lite, specifically for use in the IP networking environment.

When the IETF standard emerged, a number of vendors declared their compliance—and rightly so. Nevertheless, their systems did not interoperate because the standard allowed for a great deal of creativity in the implementation of it.

This is just one example of a pervasive problem that The Open Group has addressed through a program called Open Brand certification, which provides the means for vendors to guarantee to buyers that their products do conform to required specifications.

In June 2000, the LDAP 2000 program was launched as part of the overall Open Brand program.

On July 22, 2003, the DIF announced the launch of its *LDAP Certified* program. The *LDAP Certified* program replaces the *Open Brand for LDAP 2000* certification.

The *LDAP Certified* program was developed through a year of collaboration among the many server and application members of the DIF. Of the many protocol features in the IETF specifications, the DIF identified the ones that are commonly provided by servers and used by applications in the marketplace. These features are described in The Open Group publication *LDAP Features for Certification*[1] and the requirements for compliance are detailed in the *LDAP Certified* Product Standard. To be certified, a server must support those features, and to be sure of interoperability, an application should use only those features.

IT government and enterprise buyers have mandated more than US$56 billion worth of Open Brand certified IT products in their procurements.

Advantages of Certification for Server Vendors

The exercise of establishing interoperability through confidential Plugfests and certifying a product through The Open Group costs relatively little, while it yields enormous revenue opportunity. To give a big-picture view of this assertion, IT government and enterprise buyers have mandated more than US$56 billion worth of Open Brand certified IT products in their procurements. As of the end of 2002, the full Open Brand program included 25 major suppliers and more than 1,500 products.

[1] This document is available from: http://www.opengroup.org/products/publications/catalog/i031.htm.

Growth statistics for the directory market reveal that vendors have a potentially bright future as customers become increasingly reliant on directory technologies. The directory market is growing in terms of dollar volume. Integral to the success story is the fact that provisioning, access control, CRM, and web services are important growth drivers.

Customers want complete solutions—usually not provided by a single vendor.

But why are standards and certification important to the vendors in this burgeoning market? Once vendors find customers, they are in the business of keeping them; to keep customers, they have to satisfy them. Customers want complete solutions—usually not provided by a single vendor. They want the option of alternative vendors so they have multiple sources of products and services; therefore, they want interoperable parts and, in many cases, that means interchangeable and standardized choices.

From railroads to information technology, standards have demonstrated their worth in dramatically growing market size. The directory market is standardized, but there is no way to demonstrate that the many vendors in that market space have actually implemented the standards the same way without certification of conformance. And to serve that market well, three kinds of certification are needed:

1. Server-to-server – addressed by *LDAP Certified*
2. Application-to-server – addressed by *LDAP Ready*, to debut in Fall 2003
3. Application-to-application – in the future, but certainly part of the planning agenda. With the proliferation of XML-based technologies, customers will see more direct application-to-application capabilities, and both LDAP and Directory Service Markup Language (DSML) will have to be able to be certified to support that development. (DSML combines directory services technology; e.g., LDAP, with XML syntax.)

In short, by earning the *LDAP Certified* mark for their products, server vendors do the following:

- Demonstrate commitment to and compliance with open standards
- Give customers confidence that their products will work with directory-enabled applications, and deliver the benefits that they expect from LDAP solutions
- Promote the concept of directory interoperability through LDAP, growing the overall market for directory products

Advantages for Application Vendors

Applications must interface to directories because customers rely on directories for safe storage of, and ready access to, valued information. So applications must come into an environment "ready" to work with products

in that environment. A standard interface between applications and directories means than an application vendor:

- Has a larger market
- Has lower development costs
- Can sell products more easily, and therefore:
- Can achieve higher sales

Some application vendors operate their own certification programs for LDAP servers. For them, The Open Group offers the ability to link their programs with *LDAP Ready* certification. This gives them the additional advantages of:

- Positioning their products in the marketplace as using standard LDAP, rather than a proprietary variant
- Enabling them to test servers under their own program at Plugfests; and, as a consequence:
- Enabling them to certify more servers with less effort under their own programs

In summary, *LDAP Ready* certification gives an application vendor:

- Demonstrable standards compliance
- Increased sales
- Lower testing costs

The LDAP Ready program comprises web-based documents, processes, and legal agreements that can be completed, start to finish, via the web.

The New LDAP Certified Program

The document *LDAP Features for Certification* identifies three kinds of features:

- BASE – These are the most commonly used LDAP features. They include simple bind, search, add, delete, modify, simple cases of modify DN, and operation over SSL as well as TCP. Applications that use only features from the Base profile will be relatively simple to create, and can expect good interoperability with most LDAP servers.
- STANDARD – Together with BASE, these are the most commonly implemented LDAP features. They include Root DSE, alias de-referencing, operational attributes, controls, extended operations, referrals, continuation references, and a number of common object classes, attribute types, and syntaxes. Applications that use only BASE and STANDARD features may be relatively complex to create, but can still rely on interoperability with *LDAP Certified* servers that support the Standard profile.

- ADVANCED – Features not marked as Base or Standard in *LDAP Features for Certification* are marked as ADVANCED. They include start TLS, SASL bind, complex modify DN operations, and extensible match. These features are required by relatively few applications, generally of a specialized nature. Applications that do use these features are unlikely to interoperate with a wide range of LDAP servers.

The *LDAP Certified* program will initially cover support for BASE features. Certification of STANDARD features will be added later. The DIF will then work on certification of vertical profiles of ADVANCED features for particular application areas.

The VSLDAP test suite is the indicator of compliance for *LDAP Certified*. Vendors warrant that their products conform to all details of the Product Standard, whether those details are tested or not.

The Forthcoming LDAP Ready Program

Set for a Fall 2003 debut, the *LDAP Ready* program comprises web-based documents, processes, and legal agreements that can be completed, start to finish, via the web. Once a vendor has completed the web forms, The Open Group will list the product in the registry and grant the right to display the *LDAP Ready* logo according to the *LDAP Ready* terms and conditions, described at www.opengroup.org/dif/ldapr/conds.htm.

To obtain *LDAP Ready* certification, a vendor must do the following:

- Describe the product functions that use LDAP
- Describe any conditions that must apply to the server for the product to work
- Affirm that under those conditions the product will work with any server that conforms to the *LDAP Certified* Product Standard
- Describe the tests that have been done to prove it

The information a vendor supplies to obtain the certificate is made publicly available through the *LDAP Ready* registry.

Summary: Advantages and Participation

LDAP Certified and *LDAP Ready* offer measurable benefits to server vendors, application vendors, and customers of directory products, as follows:

- Customers can identify and purchase applications that work with the same IETF LDAP standards they are using or planning to use in their enterprise infrastructure. This significantly reduces the risk of unexpected integration, development, and maintenance costs

incurred when applications do not work with the underlying infrastructure.

- Server vendors benefit because certified applications create a pull in the market for those server vendors' products in which the associated underlying LDAP standard has been implemented. This pull creates an increased demand from customers and application vendors resulting in increased sales for server vendors.
- Application suppliers benefit because the demand from customers for certified products increases their sales volume, increases their market share, and increases customer satisfaction and retention.

Application vendors will be able to certify a product as *LDAP Ready* via the web. The *LDAP Ready* website www.opengroup.org/dif/ldapr/ explains how.

To certify a server as *LDAP Certified*, a server vendor must:

- Execute a legal agreement with The Open Group
- Obtain the VSLDAP test suite and supply a report from a test run showing that the product has passed the tests
- Complete a formal certification application, including warranting that the product conforms

The DIF provides an FAQ to address a range of vendor and customer questions at www.opengroup.org/dif/cert03/certfaq.htm.

About the Directory Interoperability Forum (DIF)

The mission of the DIF is to drive product and vendor interoperability based on open standards: interoperability between directory servers, within applications, and between the servers and applications themselves. Its members are the vendors that create these products and the enterprises that use them. By working together, they determine how these technologies can provide increasing value and help guide developers in building them. By keeping the entire directory community involved, the DIF increases the collective value of technology and expands the number of products that freely interoperate.

DIF members participate in a variety of initiatives in addition to standards development, including Identity Management, and the Mobile and Directory Challenge. More information about the DIF can be found at www.opengroup.org/dif.

About The Open Group

The Open Group is a vendor-neutral and technology-neutral consortium, committed to a vision of **Boundaryless Information Flow** achieved through global interoperability in a secure, reliable, and timely manner.

The Open Group mission is to drive the creation of **Boundaryless Information Flow** by:

- Working with customers to capture, understand, and address current and emerging requirements, establish policies, and share best practices
- Working with suppliers, consortia, and standards bodies to develop consensus and facilitate interoperability, to evolve and integrate specifications and open source technologies
- Offering a comprehensive set of services to enhance the operational efficiency of consortia
- Developing and operating the industry's premier certification service and encouraging procurement of certified products