

LDAP

White Paper

March 2000

By: V. Corey Williams

PROplus Systems, Inc.
2082 Michelson Drive # 212
Irvine, CA 92612

http://www.proplus.com

Copyright ©2000 PROplus Systems, Inc.

LDAP Whitepaper

March 29, 2000

So, what is LDAP and what can it do for you? LDAP is an acronym for lightweight directory access protocol. It is the emerging industry protocol for accessing online directories. OK… So, what is an online directory? Well to put it simply, online directories are a way to help people find things using a computer. They help us by providing a way to identify and organize the things we need to find.

The concept of a directory is by no means a new one. We often use directories whether we are aware of it or not. Whenever you have searched for a telephone number in a phone book or searched for a product in a mail order catalog, you have made use of a directory.

Telephone books, library catalogs, products catalogs, and television listings are all examples of *offline directories*. By contrast, directories that are accessed through a computer are referred to as *online directories*. Online directories are very similar to offline directories but they differ in that they are more dynamic and flexible. In addition, online directories can be personalized and secured.

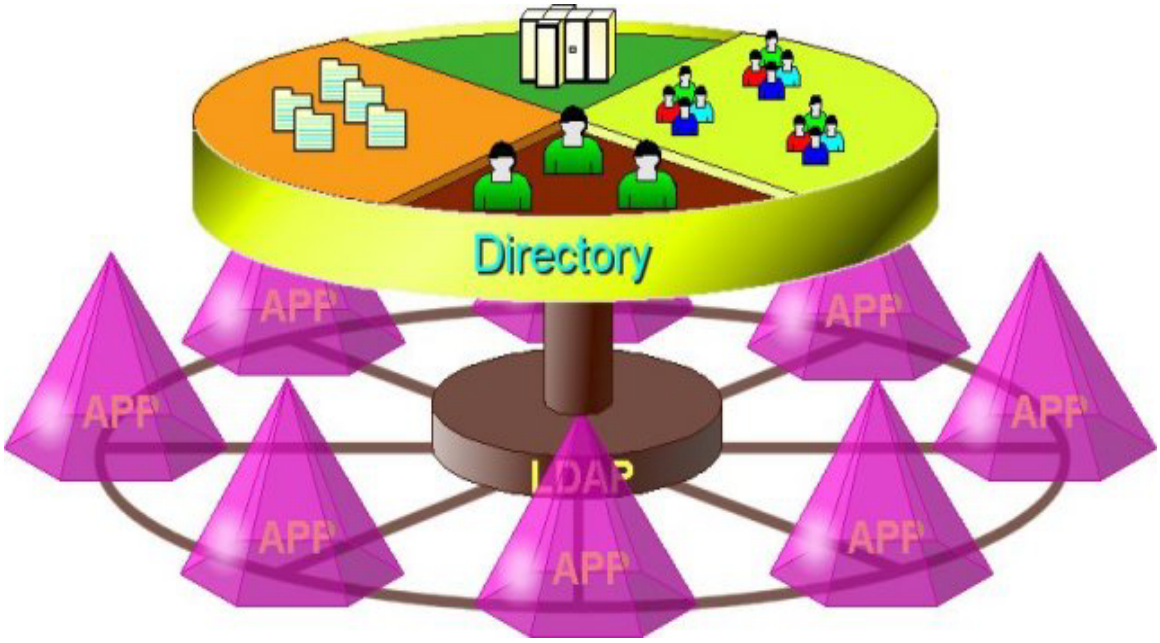

Figure 1 - Directories are used to identify and organize the things we need to find.

Copyright © PRO*plus* Systems, Inc.

Online directories are a specialized type of database. With that said, directories are significantly different than most databases in how they are used and deployed. For instance, the read-to-write ratio is usually much higher for directories than for other databases. For this reason, directories usually have very different performance characteristics than do other databases. Directories also differ from other databases in that they are more widely distributed than other databases and are often replicated to a higher degree than other databases.

Online directories are used in a variety of computer applications. Probably the most common application is online address books but the possible applications are boundless. Until recently, developers who wished to incorporate a directory into their applications were often left with only two choices: build a proprietary directory or purchase and incorporate a fully functional database into their applications. The first approach had obvious shortcomings. First, it required significant developer effort. Second, the data stored was often not accessible by other applications. Using a fully functional database also had its shortcomings. First, a fully functional database was often overkill. Directories are usually much simpler and less cost intensive than a full-blown database. Second, although the data can typically be accessed by other applications, the format of the data is typically specific to the application that created it.

LDAP based directories provide a solution to these problems. They are becoming widely available so application providers no longer need to create their own directories (some operating systems such as Windows 2000 bundle one free), they are much simpler than fully functional databases, and they store data in a standard way so that multiple applications can share the same data. Most notably, applications can share common user information such as user identifiers and credentials. This will allow application developers to implement features, like single-logon functionality, which would not be possible otherwise.

It is not only application developers that will benefit from LDAP. MIS administrators will benefit from the central administration of common application data such as user and security information. This means that an administrator will no longer need to keep these data synchronized across multiple directories. This can be very labor intensive and can also lead to errors. End users will also benefit from LDAP. All kinds of useful information will be cataloged and easily assessable to them. Printers, servers, employees, etc. will all be accessed through LDAP client applications.

LDAP is based on an older protocol, X.500, but it is much simpler to implement and use. The X.500 standard consists of a number of smaller sub-protocols that cover every aspect of directory access including naming, data format, communication, digital certificates, user authentication, etc. LDAP is a simplified subset of the X.500 protocols. It has adopted the most widely used functionality while trimming away the fat.

Like LDAP, other subsets of the X.500 protocols have found increasing popularity in recent years. For instance, the X.509 protocol that specifies digital certificates and

Copyright © PRO*plus* Systems, Inc.

public-key based authentication has celebrated widespread adoption in the Internet community. This protocol is an essential part of the secure socket layer (SSL) protocol and has found uses in other protocols including secure email communication.

The X.509 protocol presents some interesting challenges, however, dealing mostly with the management of digital certificates. LDAP is an excellent tool for addressing these challenges. Since, LDAP evolved from the same protocols as X.509 it shares the same naming conventions as the X.509 protocol. It also supports the authentication protocols defined in X.509 for authenticating directory users. This makes LDAP based directories an ideal place to store and manage digital certificates.

Another reason that LDAP is ideal for storing X.509 certificates is that it is designed to work on the Internet. As more people adopt LDAP as a means for storing digital certificates, Internet services can be created that will acquire those certificates automatically and use them for the purposes of authentication and digitally signing data. Clients that have never before been identified can be authenticated and held accountable for all information they sign. This will be particularly powerful in the world of e-commerce.

Of course, certificates are not the only kind of data that can be accessed by Internet clients through LDAP. Numerous companies including Microsoft, AT&T, Netscape, Bigfoot, Yahoo, Alta Vista, and Verisign are beginning to provide access to many kinds of data through LDAP services. Most notable among these are digital certificates, phone directories, and email directories. But as LDAP becomes more widely adopted, the number of LDAP applications on the Internet is most certainly going to increase.

LDAP has already seen tremendous success both on the Internet and LAN but it has yet to see its fullest potential. Undoubtedly, the release of Windows 2000 will spur the popularity of LDAP. This platform has made extensive use of LDAP. Every thing from system resources to security objects are cataloged in a LDAP based directory. It also provides a number of easy to use LDAP search tools for finding people and resources. Windows 2000 will expose more people to LDAP than ever before.

As more and more users and IS administrators are exposed to the benefits of LDAP, LDAP will no doubt find an ever increasing variety of applications. As I have already said, the possible applications of LDAP are boundless. So, what is LDAP and what can it do for you? We'll just have to wait and see.

Copyright © PRO*plus* Systems, Inc.