# DCL White Paper:
# DIRECTORY SERVICES - THE ROLE OF LDAP AND X.500

## CONTENTS

1. Introduction and Summary

2. What do Directory Standards Define? (What is X.500?)

3. What is LDAP?

4. The Role of LDAP

5. Is LDAP Enough?

6. Why is X.500 Necessary?

7. X.500 as a Directory Service

8. The Future of Directory Services

9. Notes and References

10. Further Information

## 1. INTRODUCTION AND SUMMARY

There is currently a huge amount of interest, comment and speculation within the industry about directory services. In particular, the Lightweight Directory Access Protocol (LDAP) is often positioned as the standard capable of providing universal directory access, as well as a mechanism of integrating separate directories into large-scale, consolidated directory services.

LDAP was originally conceived as a way to simplify access to a directory service that was modelled according to X.500 (the ISO/ITU international directory standards). Many of the recent claims for LDAP go beyond this original definition and attempt to position LDAP as the only directory protocol required - and therefore imply that the X.500 protocols are redundant.

The adoption of LDAP as a standard access protocol is to be welcomed and this is already endorsed by the leading industry players. However, LDAP is not sufficient to define a complete directory standard. The X.500 standards are needed to define all of the features required for the provision of a truly distributed directory service.

This paper aims to analyse LDAP and highlights what LDAP is capable of and how it relates to other directory standards. It concludes with a look at the likely future for directories and the role that LDAP should play in making directory technology more widely available, on the Internet, Intranet and Extranet. The key points are as follows.

- A distributed directory service is defined by both a set of protocols and also a definition of a directory model (i.e. how the directory is managed, structured and accessed).
- LDAP was designed as a directory access protocol suitable for user access. LDAP alone is not the basis for an advanced distributed network of directory servers, which must be defined by additional protocols and a directory model.
- X.500 provides the definition of a distributed directory with server to server protocols and a proven directory model. It is the only endorsed open standard to address these issues and is totally complementary to (and compatible with) the current LDAP standard.
- LDAP does not as yet address the broader requirements of a distributed directory. While some attempts are being made to rectify this, it will be several years before a "pure" LDAP directory has the same capabilities as current X.500-based implementations. And LDAP will risk losing its "lightweight" tag in the meantime!
- Mature X.500 products are now available which support LDAP and have addressed early concerns about the feasibility of implementing X.500 based solutions **[1]**.

So, in conclusion, the industry should embrace LDAP as an access protocol but demand that distributed directory products conform to the well established X.500 standards. Yes, directory services will be based on LDAP - that is how users will access the directory. However, the service has to be implemented to the X.500 standards. X.500 directories are the most powerful and advanced LDAP servers around.

## 2. WHAT DO DIRECTORY STANDARDS DEFINE? (WHAT IS X.500?)

Before considering LDAP itself it is necessary to understand a little about directory standards and, in particular, the existing industry model of X.500.

X.500 is the standard produced by the ISO/ITU defining the protocols and information model for a directory service that is independent of computing application and network platform. First released in 1988 and updated in 1993 and 1997, the X.500 standard defines a specification for a rich, distributed directory based on hierarchically named information objects (directory entries) that users can browse and search. X.500 uses a model of a set of Directory Servers (DSAs), each holding a portion of the Directory Information Base (DIB). The DSAs co-operate to provide a directory service to user applications in a way which means these applications need not be aware of the location of the information they are accessing. In other words, the user applications can connect to any Directory Server and issue queries to access information anywhere in the directory.

The X.500 standards address both the way directory information is structured and controlled within the directory service and the protocols needed to provide access to this information. The original 1988 X.500 standards focused heavily on the protocols to be implemented; there were two protocols that were crucial in providing a truly distributed service.

- Firstly, the standards specified how user applications access the directory information (the Directory Access Protocol - DAP).
- Secondly, and essentially, they specified the protocol used to propagate user directory requests between Directory Servers when the request cannot be satisfied by the local Directory Server (the Directory Service Protocol - DSP).

The 1993 standards refined the DAP and DSP protocols and addressed the key areas of the control and management of the data held in the directory. These standardised the administration of the directory, while simultaneously allowing maximum flexibility to the administrator of each portion of the directory.

- **Access Control.** The 1993 standard defined security mechanisms to protect the information in the directory and restrict user access to it (e.g. to prevent users seeing or modifying restricted information). In combination with strong authentication using public/private key technology and digital signatures (defined in the X.500 standards) this provides an extremely flexible and secure method for data protection **[2]**.
- **Schema Management.** The 1993 standard defined the way in the directory schema is held. The directory schema determines what and how information is held in the directory. X.500 allows the administrator of each portion of the directory to define how information is structured in that particular part of the directory.
- **Collective Attributes.** The 1993 standard introduced the concept of collective attributes. These allow, for example, the telephone number of a company to be stored and modified in a single place in the directory (in the directory entry of the company), while appearing, for the purposes of interrogation, in the directory entry of each employee of that company.
- **DSA Information Model.** 1993 X.500 standardised the method of storing data within each DSA. This defines how the directory's structure is held within the directory. It allows different servers to share data by replication, because they both share and communicate a definition of the structure.
- **Internationalisation.** Support for multi-byte character sets was introduced in the 1993 standards, ensuring that the X.500 model can be used to implement solutions for all countries.

The 1993 standard also addressed the substantial performance implications of supporting a very large distributed directory with only one copy of each directory entry. It introduced a third key protocol for replication allowing information mastered in one Directory Server to be shadowed to other Directory Servers (the Directory Information Shadowing Protocol - DISP). Several copies of directory data could then be used to satisfy user queries, resulting in greatly improved response times and greater resilience to failure.

The 1997 standards built on and extended the 1993 ones, but left the definition of fundamental features (such as those highlighted above) unaltered. There was in fact no need to change these significantly because the 1993 standards were generally comprehensive and self-consistent - and allowed vendors to create standards-based directory solutions of unprecedented versatility. It is particularly important that the 1993 standards provided such a stable base since it implies that implementations based on them are not greatly destabilised as they incorporate features from the 1997, and forthcoming 2001, standards.

Basing a directory service on X.500 means access to data is secure and data can be distributed or centralised. These features have significantly boosted the desirability of directories based on the 1993/1997 X.500 standards and made them more practical for mainstream implementation. X.500 not only makes it possible to query an individual's e-mail address and synchronise different e-mail directories, but it is also practical to build a single enterprise directory that possesses the access-control and security mechanisms necessary to allow unlimited internal and external access and that can hold a wide variety of data ranging from equipment inventories to a personnel database.

In conclusion, directory standards define both a directory model and directory protocols. Genuine distributed directories need both an advanced model and three protocols (user to server, server to server and server replication).

## 3. WHAT IS LDAP?

LDAP is an Internet standard to provide a lightweight directory access protocol. LDAP v2 is defined in RFC 1777 and a revised version v3 is defined in RFC 2251. For both protocols, there are other associated RFCs which refine the specifications further.

Recently, LDAP has been positioned as an open standard for Directory Services - a standard way for client applications and Internet Web servers to access on-line directory services over the TCP/IP network. The aim is to let users quickly and easily access directories of people and information such as user names, e-mail addresses, and telephone numbers.

As defined in the v2 RFC, the primary goal of LDAP is to minimise the complexity of the client so as to facilitate widespread deployment of applications capable of utilising the directory service.

As this RFC itself indicates, the LDAP protocol is "designed to provide access to directories supporting the X.500 models, while not incurring the resource requirements of the X.500 Directory Access Protocol (DAP). This protocol is specifically targeted at management applications and browser applications that provide read/write interactive access to directories".

Furthermore, the v3 RFC (December 1997) :

- "defines LDAP in terms of X.500 as an X.500 access mechanism. An LDAP server should act in accordance with the X.500 (1993) series of ITU Recommendations when providing the service. However, it is not required that an LDAP server make use of any X.500 protocols in providing this service, e.g. LDAP can be mapped onto any other directory system so long as the X.500 data and service model is supported in the LDAP interface."
- notes that LDAP "can be mapped onto a strict subset of the X.500 (1993) directory access service, so it can be cleanly provided by the DAP".

Clearly, LDAP is a directory access protocol that defines a simple means of querying data from X.500 or any other directory service that uses the X.500 data and service model. LDAP uses many of the directory-access techniques specified in the X.500 DAP standard, while at the same time being more practical for mainstream usage when working over a TCP/IP link because it requires less client resource.

LDAP v3 also defines a number of improvements to enable client access to the server to be more efficiently implemented and more suitable for the Internet model (e.g. the use of sort keys and paged responses to support type-down addressing). This is essential work, needed to facilitate directory application development and deployment. Importantly, LDAP has so far defined these new functions so that they can be implemented on top of the standard X.500 DAP mechanisms (i.e. without compromising the relationship with X.500).

As a lightweight access protocol, LDAP is to be welcomed and encouraged as it should become the standard way to access directory services.

## 4. THE ROLE OF LDAP

The motivation behind LDAP v2 was to provide lightweight access to directory services which use the X.500 data and information model. That means that while LDAP does not demand a service supporting X.500 protocols, it does require a directory service that uses the X.500 data and information model.

This approach was endorsed in the v3 specification with the exposure through LDAP of many of the new features introduced in the X.500 (1993) standard (such as operational attributes and new protocol elements like modify DN support).

LDAP should continue to grow as the basis for access to directory services, just as tone dialling for telephones gives universal access to the telephone service. LDAP could become the standard access protocol to all directory services.

However, the telephone service is not restricted to primitive tone dialling protocols within the telephone network. More advanced peer-to-peer protocols are used to provide a fast, resilient and manageable service. Similarly, complex directory services cannot be defined simply by the access protocol. The service itself will use more advanced protocols to provide the underlying directory network. X.500 is currently the only standard available.

Thus, X.500 complements the LDAP protocol, but there are two areas of possible concern that need to be addressed.

- In the quest for a truly Internet driven directory service and access protocol there is a desire among some parties to remove any associations with X.500 because of the perceived negative effect this will have - X.500/OSI has historically conjured up thoughts of complexity, over-engineering and high resource overhead.
- Accordingly, there are proponents of the idea that X.500 should be discarded, and directory services based on LDAP alone. This may be very harmful because this solution fails to recognise the requirements of a managed, distributed global directory.

There is a real danger that LDAP may end up re-inventing the wheel if it grows into providing more that just an access protocol. The X.500 standards provide a solid, proven blueprint for a standards-based distributed directory. The key is to give the industry confidence in X.500, show why it is important and actively promote it as a solution. This is addressed in subsequent sections of this paper.

## 5. IS LDAP ENOUGH?

To examine whether good, distributed directory services could feasibly be built on LDAP alone, we need to look more closely at the characteristics of current LDAP implementations. In as much as LDAP is an access protocol only, it does not define the behaviour of server to server communication. In other words, directory servers in a network are assumed to be "standalone". When one server receives a directory request it provides the answer either from its local database or not at all. The only support for a distributed directory is by use of referrals, or proprietary replication mechanisms. Each of these features is reviewed below.

### Referrals

This is an optional feature of most directory services that allows a directory server to return information to a client indicating alternative servers that might hold the required information. This can be quite effective when the client is in fact a user that is happy to trawl a network searching for information. The alternative, not supported by LDAP, is for the directory server to itself make requests of other servers to resolve the directory request (this is called "chaining"). There are several obvious benefits of this approach.

- For many users and applications it is far simpler to make one directory request and know that the directory service, accessed through the local server, will provide the answer. This in fact facilitates development of lightweight clients.
- In particular, a user is not exposed to misconfigurations where each of a set of servers refers to another, resulting in the user eventually returning to the original server without finding an answer to the original request.
- For search operations it is far preferable to make a request of a single server, rather than to make a series of requests to each directory that holds some of the data to be searched. An added benefit is that, by use of chaining, the local server can remove any duplicate entries that are returned by more than one of the servers used to satisfy the search.
- Finally, the use of chaining allows the service to manage its operations to meet the time limits set by the client. For a complex search the service will return all results found "so far", ensuring that the use of chaining does not lead to unacceptable response times.

### Replication

Most LDAP servers implement replication using processes known as SLAPD and SLURPD. The SLAPD process produces an update log of the modification operations performed against the local directory and writes out this log in a file format called LDIF. SLURPD is then used to replay the LDIF update log against another server using LDAP. This is an implementation using the client LDAP protocol to "replicate" information between SLAPD servers. Using this architecture results in a very basic distributed directory service.

- The result is two independent LDAP servers holding equivalent copies of the information (so it is not possible to selectively replicate key information at the expense of large, less frequently accessed information such as a photo).
- There is no mechanism to identify which server holds the master entry data and which has the shadow replica copy (so a user cannot ensure the data is up to date and it is very hard to manage the system to ensure concurrent updates do not cause conflict).
- All information in each SLAPD server needs to be fully replicated between servers to ensure user requests are to be satisfied (otherwise users are forced to go through the cumbersome process of following referrals).

Basically, the architecture of this implementation supports a distributed directory service by copying individual directories to provide multiple server copies or by forcing directory clients to trawl multiple servers to locate information. This does provide improved user access to large directories. However, this use of LDAP to synchronise information between separate directory servers falls well short of what is required to provide a managed, distributed and potentially replicated service, and makes for deployments that are expensive to run and administer. This is an area where the use of complete directory specifications such as X.500 is necessary.

## 6. WHY IS X.500 NECESSARY?

Although the X.500 standards define an access protocol (DAP), we have seen that this is only one aspect of the standard. The vast majority of the specification addresses the directory model and the protocols required to provide a fully distributed service. This service is based on a model of co-operating directory servers each responsible for a portion of the overall Directory Information Base (DIB), linking together to provide a single logical directory for users accessing the service.

To support this model, the X.500 standards address many aspects of a directory implementation:

- how the directory information is represented in entries (the schema defining, for example, object classes and attributes)
- how entries are organised and named - the Directory Information Tree and hierarchical naming model
- how information within entries is protected from unauthorised access - the access control model
- the protocol needed to chain user requests between directory servers (DSP) and the knowledge information needed to accomplish this
- the protocol (DISP) needed to replicate information between servers in a managed way such that, for example, access control is preserved and the information doesn't become stale.

These are the key features that a distributed directory service needs to exhibit. Furthermore, these individual features need to relate to each other and work well in harmony. For example, it is no use defining a sophisticated standard and protocol for replication if that standard doesn't take into account replication of access control information - access control must function equivalently on copies of data as on the original source. The X.500 standards have been designed so that each feature is fully compatible with each other - the pieces all fit snugly together like a jigsaw puzzle.

The complexity of this task should not be underestimated. Although the directory is fundamentally a simple concept, finding a consistent self-referential model for implementation is very difficult. Work started on the X.500 standards in the mid-1980s and it wasn't until 1993 that success was achieved in this respect.

Currently, LDAP is purely a lightweight alternative to the X.500 access protocol. It doesn't address how the directory service itself is structured, or how features like access control and server to server communication should operate. There are Internet working groups in place which are trying to plug these gaps and turn LDAP into a complete directory standard, but it may be in vain.

- Each group tends to specialise, and focus on refining one particular area of the LDAP specification. Without any real overall coherence to their efforts, it will be far harder to find solutions that are all mutually compatible like X.500's.
- X.500 has had a considerable head start on this difficult task, and is now gaining a real foothold where scalable, distributed directory solutions are needed. By the time a good distributed LDAP standard appears, and vendors have implemented it, it may well be too late.

In summary, LDAP is purely a lightweight alternative to the X.500 access protocol. It doesn't address how the directory service itself is structured. This is why X.500 is important - it provides a proven blueprint for implementing a directory service. It is precisely this sort of service that is needed to provide a good LDAP server.

## 7. X.500 AS A DIRECTORY SERVICE

There is a move within some members of the LDAP community to de-emphasise the X.500 relationship because they perceive a negative effect of an association with X.500. Certainly there is a tendency within the industry to see de-facto Internet standards as better than OSI standards.

However, if the industry and the Internet need a solution with the power of X.500, and this paper argues strongly that it does, then the substance of these concerns must be addressed. Close analysis shows many of the concerns to be unfounded. Indeed the main objections raised against X.500 are that (a) it is too complex and over-engineered, (b) it is OSI and therefore too resource intensive, and (c) X.500 products are not mature and easy-to-use.

Addressing each of these issues in turn.

- It is most certainly true that implementing X.500 is a challenge and requires advanced engineering skills. This is because of the problems it has to solve - advanced propriety directories are also complex. The key is that the complex implementation can lead to simple applications and intuitive easy-to-use administrative tools. There is a direct analogy with operating systems. These implementations are complex, but need to be so to make application development and system configuration simpler.
- X.500 is part of the OSI family of standards and assumes the use of OSI communications which are certainly not widespread. If X.500 were inextricably linked to X.25 or OSI connectionless transport protocols then, with the growth of the Internet, it would be quite unacceptable to advocate its use. However, all major implementations of X.500 run over the Internet (using RFC 1006). The overhead of the remaining elements of OSI communications used in server-to-server is very low and could even be removed completely [3].
- It is true that in the early years of X.500 the technology was often viewed as an engineering tool, not a real shrink-wrapped product. As with X.400 the propagation of public domain technology, which was developed in a research project, led many people to associate the restrictions of that implementation with limitations of the standard. Several vendors are now selling directory products, based on the X.500 standards, which are addressing the real needs of corporate users [4]. These products compete on the basis of their directory capability, not simply by adherence to a standard. Furthermore, support of the X.500 standard ensures a high level of function and dramatically simplifies the integration problems of companies that deploy products from more than one vendor.

## 8. THE FUTURE OF DIRECTORY SERVICES

The momentum behind the LDAP protocol is a very positive move towards helping product vendors and users alike to provide powerful directory services. It must be encouraged.

LDAP must retain its focus as an access protocol and continue to be refined and improved. At all times the aim must be to preserve the X.500 data and information model for the server.

X.500 is the open standard for co-operating directories handling distributed operations and directory replication. If necessary the industry can endorse lightweight DSP and DISP (operating directly over TCP/IP) to reduce the server overhead, but X.500 itself must be retained.

Use of X.500 will guarantee that directories can really support the demands of a customer base that is growing at a phenomenal rate. By supporting LDAP as the access protocol, X.500 products will ensure that other competing and proprietary standards do not proliferate. This will ensure that:

- there is compatibility between vendor products
- there are few limitations in distributed directory capability (rather than frustrating users who just want a solution to their problems by implementing very limited functions based on LDAP alone)
- we do not create a market in directory backbones and gateways, creating huge software and administrative costs for directory users [5].

## 9. NOTES AND REFERENCES

[1] Data Connection Limited (DCL) provides an advanced directory server - part of the DC Directory product suite - on Windows NT, IBM AIX, HP UX and Sun Solaris.

[2] Strictly speaking, strong authentication was supported in the 1988 version of X.500, but it is only alongside the other 1993 X.500 extensions that its use has become accepted.

[3] Lightweight versions of DSP and DISP, under consideration for the X.500 2001 standards, pass requests directly over TCP/IP and remove the use of an OSI communications stack.

[4] Data Connection Limited (DCL) has released a directory product suite, DC Directory, which supports LDAP, web access and administration, a Windows directory browser, advanced GUI administration, directory synchronisation and security integration (PKI).

[5] Ironically, these directory backbones and gateways will inevitably be satisfied by the more powerful X.500 products, hence ensuring that X.500 protocols are essential, after all, for distributed directory services.

## 10. FURTHER INFORMATION

For further information on Data Connection's messaging and directory products and services, please contact Graeme MacArthur at the address below.

Data Connection Ltd
100 Church Street
Enfield
Middlesex
EN2 6BQ
UK

Tel: +44 (0) 20 8366 1177
Fax: +44 (0) 20 8363 1039
E-mail: directories@datcon.co.uk
Web: http://www.datcon.co.uk

This white paper is for informational purposes only. Data Connection makes no warranties, express or implied, as to the accuracy of the content. Data Connection is a registered trademark of Data Connection Limited. All other brand and product names are trademarks or registered trademarks of their respective owners.

Back to Directories page
Back to Data Connection Home Page