INTERNET-DRAFT

December 1995
Barbara Jennings
Sandia National Laboratory

Building an X.500 Directory Service in the US
Filename: draft-ietf-ids-jennings-00.txt

Status of this Memo

Abstract
This document provides definition and recommends considerations that must be undertaken to operate a X.500 Directory Service in the United States. This project is the work performed for the Integrated Directory Services Working Group within the Internet Engineering Task Force, for establishing an electronic White Pages Directory Service within an organization in the US and for connecting it to a wide-area Directory infrastructure.

Establishing a successful White Pages Directory Service within an organization requires a collaborative effort between the technical, legal and data management components of an organization. It also helps if there is a strong commitment from the higher management to participate in a wide-area Directory Service.

The recommendations presented in the document are the result of experience from participating in the Internet White Pages project.

Table of Contents

Introduction

1.1 Purpose of this Document

This document provides an introduction for individuals planning to build a directory service for an organization in the US. It presents an introduction to the technical, legal, and organizational aspects of a directory service. It describes various options to organizations who want to operate an X.500 Directory service and illustrates these with examples of current X.500 service providers.

1.2 Introduction to Directory Services

An electronic directory server is an electronic process that provides a list of information provided via electronic access. This information is variable in content, however it should be explicitly defined by the directory purpose. Information about people, organizations, services, network hardware are just a few examples of data content that a directory service can provide. The aim of an X.500 Directory service is to make using the directory intuitive and as easy to use as calling for directory assistance. The X.500 Directory service is an international standard ratified by the International organization for Standardization (IS) and the ITU-T International Telecommunication Union formerly (CCITT) in 1988 [1].

The Directory is intended to be global service comprised of independently operated and distributed Directory Service Agents (DSAs), that provide information in the form of a White Pages Phone Directory.

Electronic mail communication benefits from the existence of a global electronic White Pages to allow network users to retrieve addressing information in an intuitive fashion. Manual searching for names and addresses, specifically electronic addresses, can take a great deal of time. A White Pages directory service can enable network users to retrieve the addresses of communication partners in a user friendly way, using known variables such as common name, surname, and organization to facilitate various levels of searches.

In order to make global communication over computer networks work efficiently, a global electronic White Pages service is indispensable. Such a directory service could also contain telephone and fax numbers, postal addresses as well as platform type to facilitate in translation of documents between users on different systems. An electronic White Pages may prove to be useful for specific local purposes; replacing paper directories or improving quality of personnel administration for example. An electronic directory is much easier to produce and more timely than paper directories which are often out of date as soon as they are printed.

The Internet White Pages Project provides many companies in the US with an opportunity to pilot X.500 in their organizations.   Operating as a globally distributed directory service, this project allows organizations in a wide variety of industry type to make themselves known on the Internet and to provide access to their staff as desired.

Some organizations, such as ESnet agreed to manage directory information for other organizations. ESnet maintains data at their site for all the national laboratories. They provide assistance to organizations in defining their directory information tree (DIT) structure. They also provide free access to the X.500 Directory via Gopher, WWW, DUAs, whois and finger protocols.

The InterNIC is another directory services provider on the Internet. To date [June 1995] they hold X.500 directory data for 52 organizations and provide free access to this data via various protocols: X.500 DUA, E-Mail, whois, Gopher and WWW.

To find the most current listing of X.500 providers see RFC 1632 - Catalog of Available X.500 Implementations [2].

The X.500 Protocol

2.1 Introduction

This chapter provides the basic technical information necessary for an organization to begin deploying an X.500 Directory Service. It provides a brief introduction to the X.500 protocol and the possibilities that X.500 offers.

2.2 The Directory Model

X.500 Directory Model is a distributed collection of independent systems which cooperate to provide a logical data base of information to provide a global Directory Service. Directory information about a particular organization is maintained locally in a Directory System Agent (DSA). This information is structured within specified standards. Adherence to these standards makes the distributed model possible. It is possible for one organization to keep information about other organizations, and it is possible for an organization to operate independently from the global model as a stand alone system. DSAs that operate within the global model have the ability to exchange information with other DSAs by means of the X.500 protocol.

DSAs that are interconnected form the Directory Information Tree (DIT). The DIT is a virtual hierarchical data structure. An X.500 pilot using QUIPU software introduced the concept of a "root" DSA which represents the world; below which "countries" are defined. Defined under the countries are "organizations". The organizations further define "organizational units" and/ or "people". This DIT identifies the DIT for the White Pages X.500 services.

Each DSA provides information for the global directory. Directories are able to locate in the hierarchical structure discussed above, which DSA holds a certain portion of the directory. Each directory manages information through a defined set of attributes and in a structure defined as the Directory Information Base (DIB).

A DSA is accessed by means of a Directory User Agent (DUA). A DUA interacts with the Directory by communicating with one or more DSAs as necessary to respond to a specific query. DUAs can be an IP protocol such as whois or finger, or a more sophisticated application which may provide Graphical User Interface (GUI) access to the DSA. Access to a DSA can be accomplished by an individual or automated by computer application.

2.3 The Information Model

In addition to the Directory Model, the X.500 standard defines the information model used in the Directory Service. All information in the Directory is stored in "entries", each of which belong to at least one "object class". In the White Pages application of X.500 object classes are defined as country, organization, organizational unit and person.

The object classes to which an entry belongs defines the attributes associated with a particular entry. Some attributes are mandatory others are optional. System administrators may define their own attributes and register these with regulating authorities, which will in turn make these attributes available on a large scale.

Every entry has a Relative Distinguished Name (RDN), which uniquely identifies the entry. A RDN is made up of the DIT information and the actual entry.

The Directory operates under a set of rules know as the Directory schema. This defines correct utilization of attributes, and ensures an element of sameness throughout the global Directory Service.

Under the White Pages object class "Person" there are three mandatory attributes: objectClass, commonName, surName. These attributes along with the DIT structure above, define the RDN.

An example of an entry under Sandia National Laboratory is shown here:
@c=US@o=Sandia National Laboratory@ou=Employees@cn=Barbara Jennings

```
                                          root
                                  /                      \
                                  c=US                    c=CA
                               /   \
o=Sandia National Laboratory      o=ESnet
|                    \
|                     \
ou=Employees  ou=Guests
        /              \
cn=Barbara Jennings   cn=Paul Brooks
```

Organizations may define the best structure suited for their DIT. Typically an organizations DIT will look very much like the organizations structure itself. A DIT structure is determined by naming rules and as such, becomes the elements unique Relative Distinguished Name (RDN). The DIT structure may also be dependent on whether the DSA information is administered by a flat file or a database. Extra consideration to designing of the DIT structure should be taken when using flat files versus a database, as it takes longer to search through a flat file if the tree structure becomes too complex or intricate. To obtain information on recommended schema for DIT structuring see RFC1274[3].

2.4 Benefits and Uses for X.500 Directory Service

The nature of the X.500 Directory makes it suitable for independently operated segments that can be expanded to global distribution. The benefits for local directory use are:

- with the distributed nature of the service, an organization may separate the responsibility for management of many DSAs and still retain the overall structure; - the robustness of this service allows it to provide information to a wide range of applications. Whereas globally integrated projects must conform to a specific DIT, independent X.500 operations may define unique DITs, object classes and attributes as per their specific needs; - X.500 is a good alternative for paper directories, offering the ability to update and modify in an interactive mode. This allows a company to provide the most current information with less cost and effort; - because of the electronic base of X.500, other electronic applications may interact with the application without human intervention.

The benefits for global directory use are:

- the distributed nature of X.500 is well suited for large global applications such as the White Pages Directory. Maintenance can be performed in a distributed manner; - X.500 offers good searching capabilities from any level in the DIT. Also with "User Friendly Naming" in place, searches are very intuitive; - there are DUA interfaces for the White Pages service available for all types of workstations. For an overview of X.500 software reference RFC1632. - X.500 is an international standard. Using such a standard ensures interoperability within the worldwide base.

2.5 Other Applications of X.500

In addition to the White Pages, X.500 can be used as a source for any type of information that needs a distributed storage base.

The University of Michigan is using X.500 for electronic mail routing. Any mail coming to the university domain, umich.edu; gets expanded out to a local address that is stored in the rfc822Mailbox attribute. The University also operates a standard X.500 name server which provides name lookup service of over 200,000 names. They use the Lightweight Directory Access Protocol (LDAP)[11].

An implementation of the X.500 Standard directory service has been incorporated into the Open Software Foundation (OSF) Distributed Computing Environment (DCE). This component, known as the Global Directory Service (GDS), provides an area where distributed application clients can find their application servers. The GDS, in response to requests made by other clients, provides the unique network address for a particular DCE resource. Because it is based on a international standard, GDS can offer access to resources among users and organizations worldwide. This scalable service can be performed in DCE environments that range in size from the very small to the very large.

Lookup services can be implemented into a variety of applications. Cambridge University in Great Britain implemented the X.500 directory service into an employee locator application. Based on badge sensors at strategic locations, this application can determine the whereabouts of an employee on the campus. As the individual moves about, the sensors register their location in an X.500 Directory.

Digital Signature Service (DSS) and Privacy Enhanced Mail (PEM) work on the principal of a directory key server which generates and provide users with "public" codes that match previously registered "private" codes. Only the recipient can decipher messages sent in this fashion. The X.509[4] standard for key certificates easily fits within the structure of the X.500 Directory Service.

Legal Issues

3.1 Introduction

Currently in the United States, there are no specific legal rules for the information that is provided via an electronic directory service. Various organizations and groups associated with usage of the Internet, noting a need to address privacy and data integrity issues, have prepared directives to address this issue. Two such areas addressed are those of the rights of registrants included in the directory and the responsibility of administrators to guarantee the integrity of such data.

Registries containing information that is related to an individual is freely transferred and unregulated in the US, unless the provider of the data is an agency or an holder of sensitive information as defined by federal legislation and further may differ for each state. An agency is defined as: any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency. Sensitive data can be financial records, medical records, and certain legal documents. As previously noted, each state has their own legislation on sensitive or private data.The registered persons have little recourse to control list information short of filing a lawsuit against the information provider.

For individuals who transfer data across country boundaries, it is important to understand that other countries may have legislation to regulate data. Prior to requesting list information from these countries, an administrator should review applicable legislation and have some mechanism in place to ensure how data will be handled once it is crosses the border. Policy Statements for some countries have been prepared and are provided for via Code of Conduct papers.

3.2 Purpose of the Directory

The operational intent including presentation data and list registrants and access rights must be clearly defined and stated. Initially this provides the skeleton of the DIT. Eventually a statement such as this may provide a basis legally justifying the directory.

All data presented must be defined in the purpose. If for example, a directory is for the sole purpose of providing professional addressing information - an entry would include name, postal address, office telephone, facsimile number, electronic mail address and company name. Private address information listing the home address or phone would be prohibited as would any other information not directly related to addressing.

3.3 User Rights

The North American Directory Forum (NADF) has published a document that defines the User Bill of Rights[5]. This document defines an individuals rights regarding the public release of personal or private information. Among other issues stated, the user has the right to be notified regarding the inclusion of their information in a data registry as well as the right to examine and have incorrect information changed.

This paper is specifically written for the North American Directory Forum and recommends compliance with US or Canadian laws regulating privacy and access information.

Although current US legislation does not include all the suggestions in this document, it is the responsibility of the controller of the data to respect the rights of the individuals. These recommended rules can be seen as respect for the individual and the considerate controller will follow these guidelines within any boundaries that they may be mandated by.

3.4 Data Integrity

An information provider has the responsibility to guarantee the data that they make available to users. The integrity of a data source is heavily weighted by the accuracy and timeliness of the contents. Interoperable data sources must have concurrence of these factors as well. The degree to which an information provider can guarantee the validity of the data that they present, reflects on the validity of the provider in general. RFC 1355[6], suggests that a data source enable accuracy statements describing the process that the individual NIC will use to maintain accuracy in the database.

In the European community, it is a legal requirement that the information provider guarantee accurate data.

The controller of the information needs to be certain of the primary source of data. When possible, the controller should develop routines of random checks to validate the registry data for correctness.

3.5 Data Security

A Directory Service with non-authenticated access from the Internet is difficult to protect from unauthorized use. Unauthorized use being defined by each organization within the directory purpose statement. Typical misuse being by individuals who attempt to duplicate the directory for unauthorized purposes. Other security measures include: Access Control Lists (ACLs), limitations on number of entries returned to a query, and time to search flags. The result of such controls will affect the legitimate user as well as the user they are intended to block.

An alternative that may provide protection from misuse is to create and display an attribute with each entry stating non-approved usage. This feature will also provide evidence of restricted use in the event that a legal case is necessary to stop unauthorized access.

The responsibility again falls on the data provider/implementor of the directory service. Astute programmers will create or make use of existing tools to protect against data destruction, falsification, and misuse.

3.6 Conclusions

User Rights, Data Integrity and Protection of data should not be considered merely in an effort to abide by legal rulings; they should be the intention of a good data source. A successful Directory Service must be aware of the requirements of those individuals inclusive in the list as well as those of the directory users.

In general, at the minimum the following conditions should be observed:

1. Define the purpose of the Directory.
2. Initially inform all registrants of their inclusion in a Directory.
3. Prevent the use of data beyond the stated purpose.
4. Limit the attributes associated to an entry within boundaries of the purpose.
5. Work towards a suitable level of security.
6. Develop a mechanism to correct/remove faulty data or information that should not be in the Directory.

Infrastructure

4.1 Introduction

The White Pages Project, currently operated by Performance Systems International (PSI) provides a reliable QUIPU infrastructure for sites wishing to provide their own X.500 directory. Started in 1989 as the NYSERNet White Pages Pilot Project it was the first production-quality field test of the Open Systems Interconnection (OSI) technology running on top of TCP/IP suite of protocols[7]. This pilot X.500 Directory, provided a real-time testbed for a variety of administrative and usage issues that arise. Today, more than 30 countries participate in the globally distributed project with over 1 million entries. The White Pages pilot is one of 37 other pilots cooperating to provide information in the Nameflow-PARADISE directory; an European project.

Initially the software was public domain, QUIPU X.500[8]. This "shareware" application in conjunction with administrative services provided free of charge by PSI, allowed for a truly distributed X.500 Directory Service to operate.

In keeping with the Internet rules of operation, the lack of the US regulations, the suggestions of North American Directory Forum and the Internet Engineering Task Force (IETF), the complications that arise from multi-distributed data as a service can be overwhelming. PSI took on the challenge to provide such a service, and continues to ensure operations today.

4.2 A Well Maintained Infrastructure

This distributed information service involves the cohesive effort of all of the participating organizations. The ISO Development Environment (ISODE) implementation of the OSI Directory, provided the attributes and uniformity to facilitate this effort.

The primary DSA for the PSI Project is named Alpaca. Operating on a Sun Sparc 10 with 120 megabytes of memory, this host serves as the Master for the DSAs of 117 organizations under c=US. Redundancy for Alpaca is provided by two sources, Fruit Bat operated by PSI and Pied Tamarin operated by the InterNIC. Slave updates to this host are provided on a nightly basis from the individual DSAs.

The data presentation is hierarchical in nature and emulates the common white pages telephone book. The information provided contains at minimum: a common name, voice phone listing, and electronic mail addressing. Each entry has a uniqueness associates with it; the relative distinguished name which is comprised of the entire directory information tree. The DITs may vary slightly, but each must contain an organization, and a person. The nature of the directory and the structure of the actual organization for whom the directory is being provided contribute to the overall DIT structure. The following is a list of commonly used attributes:

commonName	physicalDeliveryOfficeName	stateOrProvinceName
description	photo	streetAddress
userid	postOfficeBox	surname

favouriteDrink	postalAddress	telephoneNumber
title	rfc822Mailbox	facsimileTelephoneNumber

4.3 DUA Interfaces for End Users

There are a variety of user interfaces on the market today that will provide Directory User Agent access to the X.500 Directory. Standard protocols such as fred, whois, whois++, finger, are used widely. Interfaces are also available via World-wide Web browsers and electronic mail.

Vendors providing DUAs include ISODE Consortium, NeXor, and Control Data Corporation. These applications operate in conjunction with the vendor provided DSAs.

Historically DUA interfaces were difficult to implement and required the entire OSI stack. Implementing such a product on a PC or Apple platform required skillful programming. The executable for these platforms were usually very large. The IETF has since defined and standardized the Lightweight Directory Access Protocol (LDAP)[11]; a protocol for accessing on-line Directory services which offers comparable functionality to the Directory Access Protocol (DAP). It runs directly over TCP and is used by nearly all X.500 clients. LDAP does not have the overhead of the various OSI layers and runs on top of TCP/IP.

The functionality varies by specific DUA. Each offers access to the X.500 Directory. Most offer the ability to make modifications to entries. There are a few that offer Kerberos authentication.

Further information on LDAP clients for specific platforms can be found on the University of Michigan WWW server: http://www.umich.edu/~rsug/ldap.

Another interface that has been tested and recommended for users by our Dutch (Surfnet) colleagues is Directory Enquiry (DE). Originally developed by University College London for the Paradise project in Europe, the engineers at Surfnet have selected DE as the best interface for "dumb" terminals. They have also translated the interface into Dutch for their local users[12].

Ideally, users should be able to access X.500 directly from their electronic mail applications. Vendors (other than the ones mentioned above) have been slow to incorporate the X.500 Standards into their electronic mail applications.

Datamanagement & Pilot Projects

5.1 Simple Internet White Pages Service

A wide variety of directory services retrieval protocols has emerged in the time since the original Internet White Pages was begun in 1989. To ensure that decentralized implementations will have interoperability with other providers, the IETF Integrated Directory Services Working Group, is working to create a draft focusing on the common information and operational modeling issues to which all Internet White Pages Services (IWPS) must conform to.

Utilizing current information servers, the conceptual model described includes issues regarding naming, schema, query and response issues for a narrowly defined subset of directory services. The goal of this paper is to establish a simple set of information objects, coupled with a basic set of process requirements that will form a basis which can lead to ubiquitous IWPS. With this goal in mind, it will be easier to proved a consistent User view of the various directory services.

5.2 InterNIC

The InterNIC[9] is a collaborative project of two organizations working together to offer the Internet community a full scope of network information services. Established in January 1993 by the National Science Foundation, the InterNIC provides registration services and directory and database services to the Internet. (Internet a global network of more than 13,000 computers networks, connecting over 1.7 million computers and used by an estimated 13 million people.) In keeping up with the exponential growth of the Internet, the InterNIC provides a guide to navigate the maze of available resources.

InterNIC provides two types of services; InterNIC directory and database services and registration services. AT&T provides the directory and database services, acting as the pointer to numerous resources on the network offering X.500 to help users easily locate other users and organizations on the Internet.

5.3 ESnet

The Energy Sciences Network[10], is a nationwide computer data communications network whose primary purpose is support multiple program, open scientific research. As part of this support, ESnet offers networking services including information access and retrieval, directory services, group communications series, remote file access services and infrastructure services. As a early member of the White-Pages Pilot Project, ESnet continues to be a part of the worldwide distributed directory service based on the ISO/OSI X.500 standard. There are over nineteen ESnet organization represented in the directory, comprising over 120,000 entries. ESnet provides access to seven other sites via the X.500 DSAs.

Recommendations

6.1 General

The X.500 Directory technology is available through several options. Vendors can provide consultation for schema design as well as supply, install, and support the software to perform the operations required. For smaller organizations or companies who do not want to administer their own DSA, there are providers available who will maintain the DSAs remotely and provide this service to the Internet. Those with network and management expertise, can either operate independently or join one of several white pages directory projects. Careful consideration must be given to the initial investment required and the required maintenance process.

6.2 Getting Started

Successful initialization of a directory service requires a systematic approach. The complexity of offering this type of service becomes more apparent as implementation progresses. Several aspects must be considered as this service becomes a cooperative effort among the technical, administrative, organizational, and legal disciplines. Procedures must be defined and agreed to at the initial phase of implementing an X.500 Directory service.[13] The following are issues that should be addressed in these procedures.

6.3 Who are the Customers?

Defining the customer and the customer requirements will determine the scope of service to offer. What is the primary purpose for the directory service? A company may find it desirable to do away with a paper directory while simultaneously providing the current directory information. The directory may be for internal use only or expanded to any users with Internet access. Will the customer use the directory for e-mail address only or is other locational information such as postal address and telephone number a requirement?

The directory may provide information to electronic customers such as distributed computing applications as well. In this case, the data must be provided in machine readable format.

Will the customers extend across country boundaries? Information may be considered private by one country and not by another. It is necessary to be aware of the legalities and restrictions for the locality using the data. Some counties have published a Code of Conduct with the IETF, explicitly stating the legal restrictions on directory and list data. Check the archives to determine if the country with whom information will be shared has presented such information.

6.4 What are the contents of the Directory?

The information presented in the directory is tightly coupled with the purpose. If the purpose is to provide addressing information for individuals, then customary information would include: Name, address, phone, e-mail address, facsimile number, pager, etc. If the use of the directory is to facilitate electronic mail routing then the destination mail address needs to be included for each user. No other information should be presented in the directory if it is not directly related to the purpose.

If the directory is internal only, it may be desirable to include the registrants title as well. Remember that information available on the Internet is generally open to anyone who wants to access it. Individuals wishing to target a specific market may access directories to create customer mailing lists.

The structure or schema of the X.500 Directory must be an initial consideration. Will the hierarchy follow the company structure or is a different approach more practical? How many entries will there be in the directory five or 50,000? A complex hierarchy for thousands of users may affect the efficiency of queries.

6.5 What are the rights of the individuals?

The subjects included in the directory shall have well defined rights. These may be mandated by company policy, legal restrictions, and the ultimate use of the directory. For a basic Internet White Pages Service these rights may include:

1. the option of inclusion in the directory
2. the right of access to the information
3. the right to have inaccurate entries corrected

The terms and conditions for employees of an organization may affect these rights. On becoming an employee of any organization, an individual inevitably agrees to forego certain personal privacies and to accept restrictions.

Every organization should develop and publish the "rights" that can be expected by the list registrants.

6.6 Data Integrity

Information that needs to be included in the directory may come from various sources. Demographic information may originate from the human resources department. Electronic mail addresses may be provided by the computer network department. To guarantee data integrity, it is advised that the data be identified and maintained as corporate information.

The required timeliness of the data is unique for each DSA. Updates to the data may be a frequent as once a day or once a month. Updates to the data must be provided on a regular basis. In cases where data is time sensitive, an attribute should be included to display the most recent maintenance date.

A regular check for data accuracy should be included in the directory administration. Faulty information may put an organization in breach of any data protection laws and possibly render the company as unreliable.

6.7 Data Security

Securing networked information resources is inherently complex. Attempts must be made to preserve the security of the data. These may include access control lists (ACLs), limiting the number or responses allowed to queries, or internal/external access to the directory.

The 1993 recommendations have added a complex access control model that is designed to tightly restrict the access that users may have to the information in the Directory. Local protection is configured by the implementor. A secure X.500 Directory should provide tools to protect against destruction, falsification, and loss of data.

There is not a tool yet that will protect against the misuse of data. There are flags and limits that can be set from within the application that will serve somewhat as a barrier to such unwanted use. Any restrictions however, also will affect the legitimate users. One suggestion is to post a notice of illegitimate use within each entry. This of course will only serve as a deterrent and as an asset should legal action be required.

Again, caution must be taken when transferring data between country and state borders. In the US data regulations differ from state to state.

6.8 Data Administration

The decentralized nature of the X.500 Directory service means that each organization has complete control over the data. As part of a global service however, it is important that the operation of the DSA be monitored and maintained in a consistent manner. Authorization must be given to the local manager of the information and in some cases, the subjects included in the directory may also have modification privileges.

Once the service is running, the importance of guaranteed operation can not be overstated. Maintenance of the local Directory will be an integral part of normal administrative procedures within the organization and must be defined and agreed upon in the initial stages of development.

6.9 Conclusion

Establishing a Directory service within an organization will involve a great deal of cooperative effort. It is essential to get commitment from the integral parties of an organization at the onset. This includes the technical, legal, and data managements components of the organization. Executive level commitment will make it much easier to get the cooperation necessary.

Operational procedures must be clearly defined, as the inclusion in a globally distributed service has wide visibility. Adherence to these procedures must be maintained to the highest degree possible as misinformation may result in unintentional legal violations and unreliable access or data can adversely affect on a companys reputation.

An X.500 Directory can be extremely useful for an organization if it operates as designed. It may serve as the "hub" of the information routing and the basis for several everyday activities. A successful service will be one of the most important tools for communication in the computer network environment. For people to make use of the service, they must be able to rely on consistent and accurate information.

References

1. CCITT Blue Book, Volume VIII - Fascicle VIII.8, November 1988
2. RFC 1632; A Revised Catalog of Available X.500 Implementations. A. Getchell; ESnet, S. Sataluri; AT&T.
3. RFC 1274; The COSINE and Internet X.500 Schema. P. Barker & S. Kille.
4. CCITT Blue Book, Volume VIII - Fascicle VIII - Rec. X.509, November 1988.
5. RFC 1295; User Bill of Rights for entries and listing in the Public Directory. Networking Working Group; IETF, January 1992.
6. RFC 1355; Privacy and Accuracy Issues in Network Information Center Databases. Curran, Marine, August 1992.
7. RFC 1006, ISO Transport Class 2 Non-use of Explicit Flow Control over TCP RFC 1006 extension. Y. Pouffary, June 1995.
8. Colin Robbins, NEXOR Ltd., Nottingham, London. c.robbins@nexor.co.uk
9. InterNIC; Collaborative effort of General Atomics, AT&T and Network Solutions; info@internic.net
10. ESnet; Managed and funded by the US Department of Energys Energy Research Office in Scientific Computing (DOE/ER/OSC).
11. RFC 1777; Lightweight Directory Access Protocol, W. Yeong, T. Howes, S. Kille, March 1995.
12. Building a Directory Service, Final Report test phase SURFnet X.500 pilot project, June 1995.
13. The X.500 Directory Services: a discussion of the concerns raised by the existence of a global Directory, Julia M. Hill, Vol.2/No.1 Electronic Networking, Spring 1992.
14. Directory Services and Privacy Issues, E. Jeunik and E. Huizer.
15. The Little Black Book; Mail Bonding with OSI Directory Services, Marshall T. Rose, Simon & Schuster Company, 1992.
16. NYSERNet White Pages Pilot Project: Status Report; NYSERNet Technical Report #89-12-31-1, Marshall T. Rose, December 1989
17. RFC 1798, Connection-less Lightweight Directory Access Protocol, A. Young, June 1995.
18. RFC 1781; Using the OSI Directory to Achieve User Friendly Naming, S. Kille, March 1995.
19. draft-ietf-pds-iwps-design-spec-01.txt, Tony Genovese; Microsoft, July 1995.
20. draft-ietf-ids-privacy-00.txt, B. Jennings; Sandia National Laboratories, S. Sataluri; AT&T, November 1994.

Glossary

ACL	Access Control List; a mechanism to restrict access to data stored in an X.500 Directory Service
Attribute	A collection of attributes belong to an entry in the Directory Service, and contain information belonging to that entry.
c=	countryName; Object class definition, specifies a country. When used as part of the directory name, it identifies the country in which the named object is physically located.
cn=	commonName; Attribute defining common name for individuals included in a directory. In 1988 standards can be up to 64 characters.
CCITT	The International Telegraph and Telephone Consultative Committee.
DAP	Directory Access Protocol; the protocol between a DUA and a DSA.
DIB	Directory Information Base; a collection of information objects in the Directory.
DIT	Directory Information Tree; the hierarchy of the distributed database that makes up an X.500 service.
DSA	Directory System Agent; an application that offers the Directory service, this is the database for the Directory.
DUA	Directory User Agent; an application that facilitates User access to a DSA
E-Mail	Electronic Mail.
Entry	A Directory Service contains entries on people, organizations, countries, etc. Entries belong to a certain class, and information on entries is stored in attributes.
ESnet	Energy Sciences Network; nationwide computer data communications network.
GUI	Graphical User Interface.
IETF	Internet Engineering Task Force; an internationally represented task force of Internet Activities Board charged with solving the short-term needs of the Internet
Internet	A collection of connected networks, international, running the Internet suite of protocols.
InterNIC	Directory of Directories, a collaborative project between AT&T, General Atomics, and Network Solutions, Inc.
IP	Internet Protocol; the network protocol offering a cone4ctionless- mode network service in the Internet suite of protocols.
ISODE	ISO Development Environment, a research tool developed to study the upper-layers of OSI and deploy network applications according to the ISO OSI standards and ITU X series of recommendations.
ITU	International Telecommunication Union; formerly the CCITT.
LDAP	Lightweight Directory Access Protocol, an Internet Standard for a lightweight version of DAP running over TCP/IP.
Object Class	Entries in a Directory Service belong to an Object Class to indicate the type and characteristic; e.g. Object Class "person".
OSI	Open Standards Interconnection, An international standardization program, facilitated by ISO and ITU to develop standards for data networking.
o=	organization; An attribute defining the company or organization that the person works for.

ou=	organizational unit; An attribute found under organization. Denotes the department, division, or other such sub-unit of the organization that the person works in.
PEM	Privacy Enhanced Mail; and Internet Standard for sending secure Electronic mail.
PSI	Performance Systems International, Inc.; operator of the Internet White Pages Project
QUIPU	X.500 Directory implementation developed by Colin Robbins while at the University College of London.
RDN	Relative Distinguished Name; a unique identifier for each list subject, defined by the hierarchy of the DSA.
RFC	Request For Comments; Internet series publications
sn=	surname; Attribute defining the surname of the person in the directory.
TCP/IP	Transmission Control Protocol and Internet Protocol; two internet protocols.
White-Pages	Electronic directory, accessible via Internet suite of protocols.
Whois	An Internet standard protocol.
Whois++	An Internet Directory Services protocol; a possible alternative for X.500
WPS	White Pages Service; a Directory Service that contains information on people and organizations.
X.500	A series of recommendations as defined by the ITU, that specify a Directory Services protocol.