

What is an X.500 Directory?

"A Lot More than Communications & Email"

Introduction

The International Standards Organization (ISO) started development on the X.500 standards in the 1980s, to support the X.400 Message Handling System standards - X.400 and the Telephone/Telex networks. It is for this reason that X.500 has until recently been thought of only as an electronic "white pages" or messaging address look-up facility, or even "as just a set of protocols". The standard has evolved and this narrow perspective has been greatly expanded. It is now understood, as the developers of the standard recognized, that X.500 can be the distributed information repository for all IT and voice services as well as a tool to search, retrieve and manage information.

The basic engineering components of X.500 comprise:

- ◆ an object-oriented data model;
- ◆ use of common schema for organizational, postal, telecommunications, locality, messaging and security information;
- ◆ a set of protocols which provide access, distribution and replication facilities;
- ◆ security and access control mechanisms; and a global naming paradigm.

In essence, X.500 was and is still seen to be the world's directory information infrastructure standard.

It is unfortunate that some (who generally have a communications view of the world) have seen X.500 as a set of protocols. A common view of directories is that they serve as information repositories for one's

own internal use of information. Actually the more comprehensive use of directories is to publish or externalize one's information for others to use and access.

General

When used primarily as an email and organizational look up facility similar to the Telephone Directory, X.500 has been used to search for a particular recipient and gather information on names, addresses, phone numbers and email addresses.

The X.500 standard has a number of parts which describe the information model, access control, protocols and information sets. One part of the X.500 standards is very prominent, and describes how security (authentication, etc.) is applied through the use of the directory. This particular standard is X.509, and it defines the authentication processes and the associated certificate specification. The X.500 standards also describe access controls for the directory and its data. When both are applied, the user can be strongly authenticated and has the ability to use confidentiality and non-repudiation services. In addition, the information within the directory is protected through the use of Access Control regimes. X.509 has been adopted worldwide by most vendors for digital key certificates.

X.500 is the only internationally recognized directory paradigm with a standardized access method. IT vendors are currently incorporating two versions of the Directory

Access Protocol (DAP) - a full specification (DAP) and a lightweight version of DAP servers (LDAP).

This process helps enforce common information sets, global naming and inter-connected directory systems used by all.

Globalization and the Internet are making directories the information search and management tool of the future. The requirements for Data and Voice Service integration, Distributed Computing, the provision of global services to mobile users and Electronic Commerce and Digital Signatures are the driving force behind the directory paradigm.

Current Uses

White Pages

Traditional White Pages or an “upgraded White Pages” service is one of a Directory’s main applications. Most small, medium and large organizations have details on people which are published internally and/or externally. Details may include names, telephone numbers, facsimile numbers, location, email addresses and in some cases, audio messages, video and images.

An X.500 Directory allows a common and standard access method which dedicated address books and integration software packages can’t provide to external users. In some instances, the X.500 Directory permits internal users with different applications to gain indirect access to information on proprietary systems.

Most developers are enabling their client-based programs to use the Directory Access Protocols (DAP) and Lightweight Directory Access Protocols (LDAP) to work with the Internet. This provides the user the ability to look up information on a global basis from desktop (and proprietary) applications.

An X.500 Directory “White Pages” service is implemented by a major life insurance company in the USA. All their offices have a security lookup and “White Pages” application. Names, photos and details on 9,000 employees are held in the CA eTrust Directory ***DXserver*** (DSA). When employees enter an office other than their own, they give their name and the security office or receptionist looks them up on the directory against a stored JPEG photo for visual ID check. This use of the directory could be performed from any DAP/LDAP-enabled application. At the same time as this check on the ID is performed, the employee can also be given their appropriate network access rights to internal and external network connections.

Other common “White Pages” activities are phone, fax and email address lookup by email applications or through browsers.

Catalogue

The use of an X.500 Directory as a catalogue has not been widely appreciated. The directory has the ability to store any piece of information, which can then be searched upon. A catalogue may contain photographs, serial numbers, product descriptions, price availability, etc. An X.500 Directory may also be used as a Library catalogue or electronic brochure for Electronic Commerce activities. Visit the OpenDirectory web site to see a simple product catalogue demonstration example.

X.509 Certificate Repository

An important function of the directory is its use as the standard repository for holding security Key material within the Public Key Infrastructure (PKI). A majority of financial institutions are applying X.509 certificates for Electronic Commerce activities and secure Internet transactions. The X.509 standard specifies precisely the format of the certificate, its verification process and how it should be managed.

Key Management

The Public Key Material for an individual or device is stored in a public X.500 Directory

system, whereas the Private Key Material may be embedded in a smart card, software application or a secure and trusted X.500 Directory/Certification Authority (CA) infrastructure.

The CA eTrust Directory **DXserver** has been deployed to provide this functionality because it has proven access control processing and world-class distributed operations capabilities. It is also being utilized by military and other government agencies, because the eTrust Directory provides the robustness required for such systems. An example is the Australia Post - KeyPost Certificate Authority (CA).

Large organizations generally have a number of databases, which have entries on people, locations, etc. These entries may be common to a number of databases, but their data definitions may be described differently across those databases. *Another important aspect of the Directory is to provide the unique and consistent data definitions that are required, often throughout an operationally dispersed organization.* Having determined a common specification for these data definitions through the Directory-defined schema standards, many organizations now have the ability to consolidate the data definitions used across their organization.

In addition, through the use of the directory service, they now have a vehicle for the synchronization of their databases and therefore can achieve information consistency for users and customers. The Directory is seen as the prime core source of data and therefore when new entries are added this is done through the Directory, and the information is either exported or synchronized to these other systems.

In essence the Organization has a single, uniformly protected information publishing point for both internal and external IT systems.

Document and Information Environments

All organizations, small or large, need to disseminate information to their employees and to external users. This may take the form of policy documents, brochures etc. Large organizations have major publishing systems. Smaller organizations tend to have just word processing systems. However, all are trying to automate the publishing process as a means to reduce costs while providing timely and up-to-date information.

For most organizations, it is better to leave the development and ownership of documents with the appropriate person/area responsible, but still publish documents from a central resource.

Large organizations are using Intranets and the Internet to get documents distributed to the interested parties. However, managing the source of the information and its filing is becoming an operational nightmare. In particular, user indexing between Search and Retrieval systems, the Internet, and document management systems needs to be seamless.

The CA eTrust Directory Server, through the Directory User Agent (DUA), has the ability to store "launchable" attributes. This allows the Directory to point to the source of information, say a Word document and its location, and run the target application. This allows the users direct access to up-to-date information via the directory system and the ability to edit and print it, etc. The directory may point to a URL, publishing system or other specialty application, rather than holding the whole document within the directory. This then gives the organization the flexibility to choose the most appropriate mechanism for document retrieval and publication of its information.

In addition, by holding pointers to information and pointers to applications which deal with information, the directory can, under its access control regimes,

provide different information environments for different users according to their role or privileges.

Information Warehouse - Information Pointers

Using a directory for Information Warehousing has similarities to the above, in that the directory can hold the information, instead of references that just point to it. The directory is used as the central repository of all information an organization uses. This may be the versions of software, hardware, assets, financial information, reference pointers to other information not held directly by the organization, but which it deems important for its operation.

For instance, the directory can be used in this way by storing documents which are being developed and then these can be moved (or renamed) to indicate that they are public or ready for publishing. In this application, the directory access control mechanisms protect the draft document until it is moved to a directory area that is public.

Directory-stored documents can be supplemented with specific attributes such as a "subject", "author", etc, which enables rapid selection and sorting. It can be seen in this case that the directory has far greater importance than a database, as a database is more specific in its operation. The directory is the organization's total information reference point. Being all pervasive, such information needs protection. This is one of the strong points that a directory can apply to an organization's information - Security.

The information may be protected at many levels - at an individual, an object, group or profile level. Users are allowed access to the information deemed viewable only if the security rights of the user are accredited by the directory for that individual/group doing the search or retrieval.

Conversion and Address Resolution

The CA eTrust Directory server and client/browser can be used to convert email addresses from one format to another. This has become an issue for large organizations with heterogeneous email packages running on different proprietary integrated software environments. In such situations, a user may be known by a common name in the directory; however, his email address may reflect the software environment to which he has to communicate, e.g. SMTP, LOTUS, Exchange, X.400 etc. This mechanism requires continual updates by appropriate system administrators when changes occur or by the user ID access rights granted.

If another user is looking up an individual in the directory, the client, or DUA, uses the common name email address specified (which could be different from the email environment) and converts it to a Lotus or Microsoft Exchange format, for example, to allow local Intranet email to occur within the proprietary environment. This "conversion" mechanism is transparent, as the DUA is configured to suit the operating environment.

Security

Security deserves more attention than it is given in most applications, even in other directories. However, this is one of the strongest features which directories bring to any organization. It has been touched upon above, in that you can protect some or all of the information for all entries held in the Directory through the use of Access Controls.

Organizations have an internal and external network capability that governs the whole organization's information covering people, financial status and equipment. However, not all this information can be made visible internally or externally.

Each directory user is authenticated with the directory at logon time and access rights are granted to information, if allowed. So, if a user is in finance, they may have rights to see some or all of the financial information up to a certain level. In the case of basic access, an anonymous user might be able to view the business phone and fax number but not the home address and phone number attributes of entries. An anonymous outside user may only see name, phone, FAX, email and postal address and that information which the organization wishes the public to view.

Secure messaging and Electronic Commerce require a directory, because X.509 certificates, which are required for Public Key Infrastructure (PKI), are essential. The directory holds an individual's or device's Public Key certificate. The Private Key is held securely in a trusted directory, known as a Certification Authority (CA).

The current trend is for all IT network services to become X.509-enabled, including those of banking and financial institutions. Smart cards, carried by all in the near future, will hold one's X.509 certificate for financial and company-to-company transactions. This same card can also hold one's other primary certificates that allow secure email, building access and network access etc.

The basis for all of the above is naming properties. And as X.509 requires both the User's name (the subject) and the Card issuer's name (the issuer), and these are "directory names" and global. – it is natural to conclude that without directories, electronic commerce on a global scale may well be impossible.

Conclusion

It is inevitable and essential that organizations consolidate their information, develop some information doctrine and view their information as a highly valued

asset. Organizations will require their internal information repositories to be consolidated, and the customer/service data (the external data) to be integrated. Not dealing with this issue leaves an organization exposed to major inefficiencies and loss of information assets – i.e. revenue. The direction towards directory systems is the first link in the process of introducing information doctrine, and globalizing information service provisioning rather than debating directory protocols or other low level issues. This step is fundamental.

Thanks to Alan Lloyd of CA eTrust Directory/OCSP Development Labs in Mooroolbark, Australia, and Kim Fenley of CA eTrust Directory/OCSP Sales in Australia.