



Directories and Public –Key Infrastructure (PKI)



CONTENTS

| | |
|---|----------|
| Directory Technology Overview | 1 |
| X.500 – The ISO Standard Directory Architecture | 2 |
| LDAP – Internet Standard for Directory Access | 3 |
| The Schema – How a Directory Represents Information | 3 |
| Scaling via References and Replication | 4 |
| Directory Gateways | 5 |
| The Directory-PKI Relationship | 5 |
| Use of Directories by PKI | 5 |
| Applications that Use PKI and Directories | 5 |
| Securing LDAP Directory Access | 6 |
| Directory-Dependent PKI vs Directory-Linkable PKI | 7 |
| Directories and VeriSign Managed PKI | 7 |
| The Managed PKI Directory Integration Module | 7 |
| Public Directory | 8 |
| For Further Information... | 9 |

VeriSign provides a PKI solution that complements— not dictates—an enterprise’s directory strategy

Are you considering an enterprise-wide network security solution for such purposes as secure e-mail or secure Web access by employees, customers, or partners? Do you have or are you considering acquiring an enterprise directory? If so, this paper is for you.

You may have your own questions, such as: Just what is the state-of-the-art in PKI-compatible directory technology? To what extent can an enterprise directory help leverage investment in a single application security solution to produce an enterprise wide solution? How can I be sure that a PKI installation will not derail my enterprise directory plans by imposing thorny requirements upon an already-complex undertaking? To what extent does my choice of PKI solution impact the ease of PKI-directory integration?

This paper addresses these questions. We start with an overview of today’s directory technology, followed by discussion of how an enterprise directory supports enterprise security needs, and conclude with discussion of how VeriSign’s approach to enterprise PKI averts the directory integration concerns that may arise in other approaches.¹

Directory Technology Overview

A directory makes an information source available to a user community—for example, information about employees, such as names, telephone numbers and e-mail addresses, or information about network resources such as printers and routers. Many network applications and utilities rely upon directory services of some type.

Many enterprises today operate multiple independent directory services based on separate proprietary protocols, requiring separate administration and maintenance of each service. As the number of applications and utilities relying on directories has increased, the task of maintaining these separate directories has become increasingly difficult. The ideal solution is clearly a single directory service supporting the enterprise as a whole, accessed by an industry standard access protocol (Figure 1). As a recent Microsoft White Paper put it, “*The directory service is the hub around which a large distributed system turns*”².

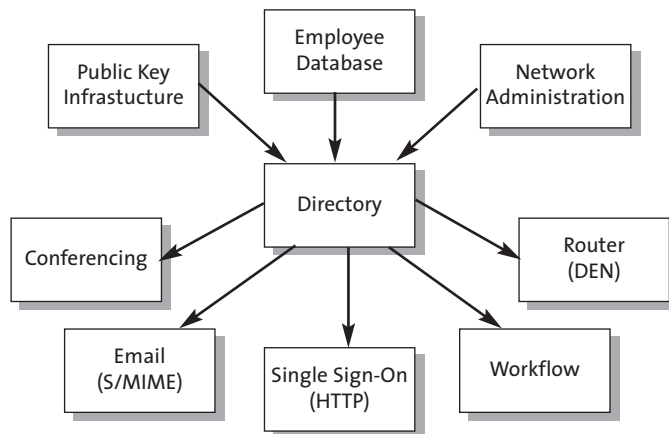


Figure 1: The directory service is the hub of a large distributed system.

The goal of establishing the directory as the unified information source for the enterprise can only be met if all the applications relying on the directory support a common means of accessing and interpreting the information stored therein. Open standards are clearly essential.

A directory is essentially a database but, unlike more general purpose databases, the information in a directory is generally read much more often than it is changed. Updates to a directory are typically simple changes to a single entry rather than read-then-modify transactions affecting many entries as is typical of other databases. As a result, a directory does not, in general, require the complex transaction management or roll back schemes supported by database products designed to support a high volume of complex updates. A general purpose database is designed to balance many different requirements. A directory is tuned to give quick response to high volumes of queries.

A fully featured directory allows information to be replicated amongst multiple servers to increase availability and reliability. Unlike a database application which relies on absolute consistency across all database replicas, a directory application is typically tolerant of transient inconsistencies. This tolerance leads to a significant decrease in the complexity of the replication protocols. This in turn can make the deployment of large directory systems simpler than deployment of a replicated database system of the same scale.

X.500 – The ISO Standard Directory Architecture

X.500 is a comprehensive directory architecture designed under the auspices of ISO and other international standards organizations. In the X.500 model, the basic unit of data is a directory entry which consists of one or more attribute-value pairs. Each attribute contains a particular data item associated with the entry; for example, the 'e-mail' attribute contains the e-mail address of the entry.

Here is an example of a directory entry for Alice Cryptographer who works for VerySecure Inc.:

| | |
|--------------------------------|-----------------------------|
| C=US | Country |
| O=VerySecure Inc. | Organization |
| OU=Security | Organizational Unit |
| CN=Alice Cryptographer | Common Name |
| alice@verysecure.com | E-mail address |
| Telephone=(666) 123 4567 | Telephone number |
| UserCertificate= <binary data> | Alice's digital certificate |

Directory entries are arranged in a tree using a subset of attributes called the Distinguished Name. For example, the *Distinguished Name* of the directory entry for Alice might be:

C=US; O=VerySecure Inc.; OU=Security; CN=Alice Cryptographer

The attributes used to construct the Distinguished Name define what is referred to as the *Directory Information Tree* (DIT) (Figure 2).

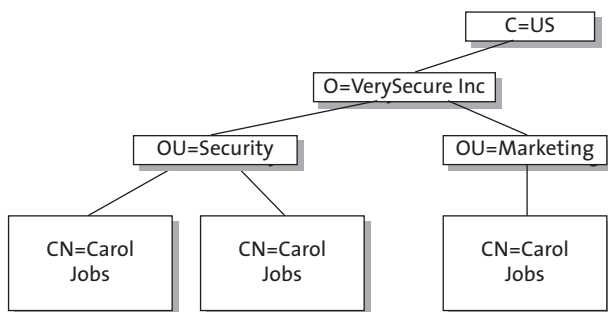


Figure 2: A Directory Information Tree

X.500 directories are accessed using the X.500 Directory Access Protocol (DAP). DAP, being a legacy ISO protocol, suffers from the shortcoming that it is not compatible with the Internet's TCP/IP protocol.

LDAP – Internet Standard for Directory Access

Lightweight Directory Access Protocol (LDAP) is a simplified version of DAP, providing an alternative interface to an information source which uses the X.500 data model. Unlike DAP, LDAP operates over TCP/IP and, consequently, is considerably simpler to implement and deploy.

LDAP was originally developed at the University of Michigan. In 1995, the Internet Engineering Task Force (IETF) chartered an LDAP working group and issued an 'Informational' RFC specifying version 2 of the LDAP protocol (LDAPv2). In December 1997, the IETF issued the version 3 LDAP protocol specification and endorsed it as a proposed Internet standard.

The Schema – How a Directory Represents Information

Like a database schema, a directory schema defines how data is represented in the directory; for example, which attributes are supported (mail, telephone, office number), the type of the value associated with each attribute (a mail attribute value has character string type), and how they are interpreted (the mail attribute stores an e-mail address).

In order for the directory to serve as a repository for the many different types of information an enterprise might need, the directory schema should be open and extensible. Each application must refer to the same type of data in the same way. The role of the directory as a unified information service thus creates a tension between the need to support schema customization for custom applications and the need for compatibility.

For example, if a data provider adds information to a directory entry using particular attribute identifiers (such as mail and userCertificate), clients will be unable to retrieve it unless they use the same attribute identifier (Figure 3).

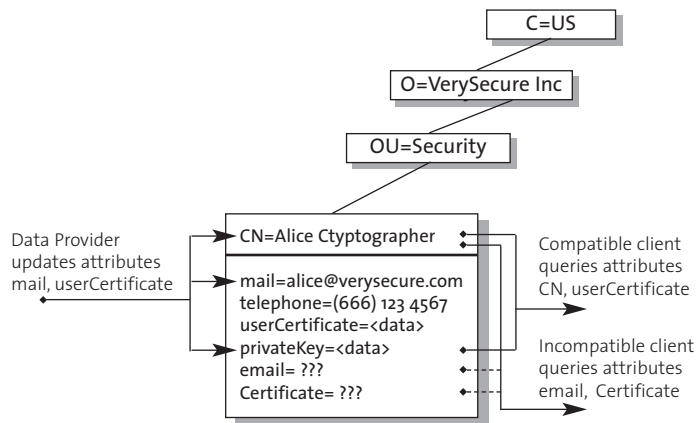


Figure 3: Data Producers and Consumers must support a common schema

The VeriSign Managed PKI Directory Integration Module supports the use of standard schema attributes, or alternatively may be configured to meet customer specific needs.

Scaling via Referrals and Replication

As with any enterprise-wide network resource, scaling is a major concern. Directories achieve scale through two mechanisms, referral and replication:

Referral: Separate parts of the directory are stored in different servers. A server receiving a request for information that it does not store locally refers the request to another server.

Replication: Copies of the same information are made available from multiple directory servers.

To support replication, X.500 defines a complete replication protocol. In an LDAP directory service, there are three main approaches to replication:

- Use an X.500 backbone to exchange information between servers;
- Use the LDAP protocol to exchange information between servers; and
- Use a proprietary directory update protocol.

Each approach is viable and has advantages and disadvantages in different environments.

Directory Gateways

The deployment of an enterprise directory across a large enterprise can be a daunting task. However, establishing an enterprise LDAP or X.500 service need not require the wholesale replacement of a legacy infrastructure. This infrastructure may be reused through a directory gateway or meta-directory.

A *directory gateway* allows an LDAP client to use an existing directory service by means of a protocol conversion or by translating LDAP requests to calls to an API supported by the legacy directory. A *meta-directory* is simply an exceptionally flexible directory gateway designed to make a large number of disparate enterprise information services act like a single directory service.

The latest release of Microsoft Exchange, for example, provides an LDAP directory gateway.

The Directory-PKI Relationship

Use of Directories by PKI

Where a PKI is deployed, a directory can be used to distribute:

- Certificates, for applications such as e-mail in which an end user certificate must be obtained before an encrypted message is sent.
- Certificate status information, such as *certificate revocation lists* (CRLs).³
- Private keys, when portability is required in environments where users do not use the same machine each day. The directory stores encrypted private keys which are decrypted at the remote workstation using a password provided by the user.

Not all PKI applications require directories. Furthermore, there is no inherent reason for using any particular directory technology with PKI. LDAP tends to be the most common directory access protocol used with PKI-enabled products, but other directory technologies may be equally appropriate in certain environments, e.g., where there is already legacy directory technology in place.

Applications that Use PKI and Directories

Examples of applications that leverage both PKI and Directories are e-mail, access control to information resources, and single sign-on.

E-mail

Many e-mail clients support access to contact information stored in one or more LDAP directories. Most S/MIME applications automatically include the sender's certificate with a signed message. However, when an encrypted message is to be sent, the certificate of each recipient must be obtained before the message is sent. Leading e-mail clients which offer

S/MIME encryption, such as Microsoft's Outlook Express and Outlook 98 and Netscape Messenger can retrieve recipients' certificates from an LDAP directory.

Access Control to Enterprise Information Resources

Access control consists of authentication (determining that the end user is the person claimed) and authorization (determining what the user is permitted to do). Certificates allow users to be authenticated using their public keys and can also carry signed authorization information. However, since the contents of a certificate must be known at the time the certificate is issued and remain valid for the entire lifetime of the certificate, certificates are not always suitable for conveying authorization information.

A directory may be used to store authorization information such as group membership and access rights. If the directory service is secured and is considered trusted, authorization data may be authenticated by authenticating the directory which provided it through a protocol such as SSL. In other cases the directory may not be itself a trusted entity but merely contain attributes signed by a trusted entity.

Single Sign-on

Another area in which directories are being used today is to support *single sign-on*. In a single sign-on environment, a user does not need to repeatedly enter passwords to access resources across a network. Instead the user signs on once using a password, smartcard, or other authentication mechanism, and thereby obtains access to multiple resources on different machines. Ideally every resource on the network should be available in this manner. In practice, however, the deployment of a single sign-on solution is a gradual process.

Netscape's Enterprise and Messaging servers support single sign-on using digital certificates and authorization information (group membership) stored in an LDAP directory. Microsoft will provide a single sign-on solution based on the LDAP compliant Active Directory when Windows NT 5.0 is released.

Securing LDAP Directory Access

Access to an LDAP server may be secured using SSL to ensure the confidentiality and integrity of queries and responses.

To enable SSL, a server certificate is required. This may be obtained from the VeriSign Digital ID center or through a local enterprise VeriSign Managed PKI for SSL installation. Note that an SSL server certificate authenticates the machine—not the application. A server supporting multiple services may use a single certificate provided the server applications themselves are compatible. For example, a certificate installed with Netscape Enterprise Server may be used with Netscape Directory Server on the same machine.

Certificate-based client authentication using, for example, client certificates issued through VeriSign Managed PKI, is also supported with appropriately configured LDAP directory servers such as Netscape Directory Server. This restricts access to the directory to only authenticated individuals.

Directory-Dependent PKI vs Directory-Linkable PKI

Different PKI implementations relate to directories in different ways. For example, Entrust is a directory-dependent PKI which requires an X.500/LDAP directory in order to function. VeriSign Managed PKI, on the other hand, is a directory-linkable PKI, which does not depend upon a directory for its basic operation but is designed to be linked to external directories of any type for distributing certificates or CRLs as required.

A directory-dependent PKI suffers from several shortcomings. The directory supporting the PKI must have particular features and a particular schema. This means that, more likely than not, it is infeasible to arrange for the PKI's directory to be the same as an enterprise-wide directory owing to feature and schema incompatibilities. The enterprise is faced with either force-fitting the PKI schema requirements on its enterprise directory schema or of operating two directories. A directory-linkable PKI does not have these shortcomings.

Directories and VeriSign Managed PKI

VeriSign Managed PKI is a directory-linkable PKI—not a directory-dependent PKI. This averts the problems experienced by enterprises trying to deploy directory-dependent PKI, where the schema and protocol requirements of the PKI product and the enterprise directory are rarely aligned.

Managed PKI includes a directory integration module that allows any directory or database system (whether X.500, LDAP, SQL, or legacy database) to be interfaced to Managed PKI such that certificates are downloaded to it. This approach facilitates ready integration with any enterprise directory, without imposing any schema requirements upon it. Enterprises also have the option of using the VeriSign central LDAP directory if they choose to join the VeriSign Trust Network.

The Managed PKI Directory Integration Module

The optional Managed PKI Directory Integration Module automatically enters certificates into an enterprise directory as they are issued.

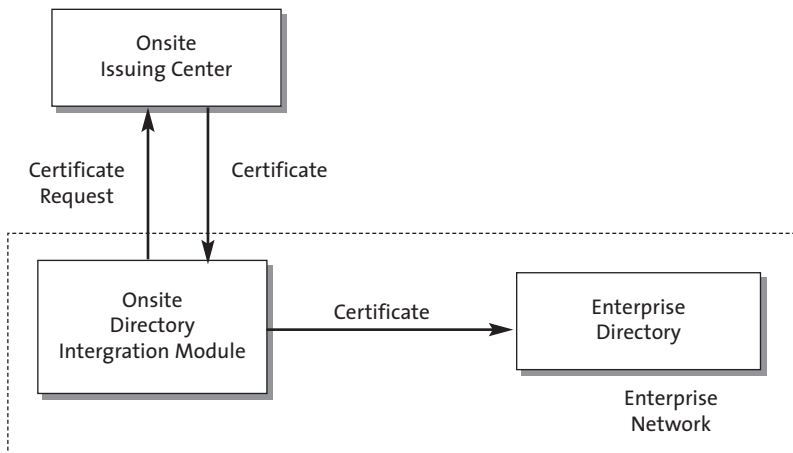


Figure 4: The Managed PKI Directory Integration Module

In accordance with the philosophy that a PKI should complement, not dictate directory strategy, the Directory Integration Module is configurable to support a wide range of site specific schema and naming conventions.

The Directory Integration Module, as shipped, may be used directly with any LDAP compliant directory that supports the ADD operation. VeriSign has partnership arrangements with several directory product vendors, including Netscape, ICL, Siemens, and ISOCOR, that ensure these vendors' respective products interoperate seamlessly with VeriSign Managed PKI. Microsoft Exchange Directory is also supported and Microsoft Active Directory will be supported when released. If required, a non-LDAP compliant directory may be accommodated provided it exposes an Application Programming Interface (API) or implements a standard directory or database access protocol. VeriSign Professional Services specialists will perform any necessary software integration work, if desired.

Deploying a PKI should not force an enterprise to adopt a particular directory strategy. VeriSign Managed PKI adapts to a customer's installed directory/ database technology, including LDAP, X.500, SQL, or legacy technology. Standalone PKI software that requires a particular directory interface protocol and/or dictates a particular directory schema will not integrate easily with pre-existing directory systems due to feature and schema conflicts.

Public Directory

VeriSign has deployed one of the largest LDAP directories on the Internet for distributing VeriSign Trust Network certificates to the public. Providing access to over two million certificates, the VeriSign LDAP server responds to over 40,000 queries per day. VeriSign Managed PKI customers have the option of having their CA join the VeriSign Trust Network or of being private and independent; in the former case, enterprise certificates are distributed via the VeriSign directory.

Popular email clients including Microsoft Outlook Express, Outlook 98 and Netscape Messenger may be configured to automatically search the VeriSign LDAP directory using the following parameters:

| | |
|-------------|------------------------|
| Hostname | Directory.verisign.com |
| Search root | NULL |
| TCP port | 389 |

For Further Information...

On VeriSign Managed PKI:

See the VeriSign website at www.verisign.com, contact your local VeriSign Account Representative, or call VeriSign at (650) 961-7500.

On LDAP:

The following book is recommended:

Tim Howes and Mark Smith, LDAP: Programming Directory-Enabled Applications with the Lightweight Directory Access Protocol, Macmillan Technical Pub, March 1997

The LDAPv2 protocol is described in the following standards documents which may be obtained from www.rfc-editor.org/rfc.html:

Lightweight Directory Access Protocol (RFC 1777)

The String Representation of Standard Attribute Syntaxes (RFC 1778)

A String Representation of Distinguished Names (RFC 1779)

Connection-less Lightweight Directory Access Protocol (RFC 1798)

A String Representation of LDAP Search Filters (RFC 1960)

The LDAP Application Program Interface (RFC 1823)

The LDAP v3 protocol is described in the following documents available from the same address.

Lightweight Directory Access Protocol (v3) (RFC 2251)

LDAPv3 Attribute Syntax Definitions (RFC 2252)

UTF-8 String Representation of Distinguished Names (RFC 2253)

The String Representation of LDAP Search Filters (RFC 2254)

The LDAP URL Format (RFC 2255)

A Summary of the X.500(96) User Schema for use with LDAPv3 (RFC 2256)

¹For an overview of the different approaches to implementing enterprise PKI, and discussion of VeriSign's approach, see "Public-Key Infrastructure – The VeriSign Difference," VeriSign White Paper #98-01, 1998

²Active Directory Technical Summary, Microsoft, 1998

³See: "Certificate Revocation with VeriSign Managed PKI," VeriSign White Paper #98-03, 1998