FEDERAL PUBLIC KEY INFRASTRUCTURE

DIRECTORY PROFILE

Version 2.5 (Draft)

October 8, 2002

[contract title and number]

Prepared By:

Booz | Allen | Hamilton
900 Elkridge Landing Road
Linthicum, Maryland 21090

Table of Contents

Table of Figures

1.0 INTRODUCTION

This profile defines the requirements for the initial operational Federal Public Key Infrastructure (FPKI) directory system. The FPKI will use the Federal Bridge Certification Authority (FBCA) that cross-certifies with agency Principal Certification Authorities (CAs) to provide trust paths between the agencies. A directory server within the FBCA will handle X.500 chained operations with agency border directories, and will also provide referrals to agency Lightweight Directory Access Protocol (LDAP) directory servers. These operations are explained in detail within later sections of this document. The Border CA concept is described in [1].

The FPKI builds upon the Federal Bridge Certification Authority (FBCA) prototype that was successfully demonstrated during the Electronic Messaging Association (EMA) Challenge in April 2000. This prototype supported S/MIME messaging among several disparate Public Key Infrastructure (PKI) domains using several different CA products, X.500 and LDAP-based directory products, and S/MIME e-mail clients. This demonstration illustrated interoperability on several levels – between CAs, between directories, and between e-mail clients. Each client created, and then processed a certificate trust path between the domain of the recipient and the domain of the sender in order to validate the signer's digital signature on the e-mail. Trust paths up to seven certificates were constructed and validated. Directories were chained using the X.500 Directory Services Protocol (DSP), while LDAP was employed by the e-mail client to access its local directory [2].

This profile addresses the minimum required directory schema, naming conventions, directory protocols supported, security considerations, alternatives to consider, and issues to bear in mind in order to adapt to this evolving technology. Familiarity with PKI technology, concepts and general terms of the directory service is assumed.

The draft is based on several sections of the following documents:

- The Evolving Federal Public Key Infrastructure [2]
- Governmentwide Directory Support 2 Technical Series, updated US Gold Schema document [3]
- The Bridge CA Demonstration Repository Requirements Draft 4/8/1999 [4]
- NSA Bridge Certification Authority Demonstration Phase II - Directory Requirements and Architecture, 7/3/2000 [5]

2.0 SCHEMA REQUIREMENTS

This section addresses the minimum schema requirements for agency directories to interoperate with the FPKI directory. The schema is limited to just the objects needed to support the PKI. At a minimum, the directories are required to store and disseminate the following PKI related attributes:

- Certification Authority Certificates
- Certificate Revocation Lists
- Authority Revocation Lists
- Cross Certificates
- End-entity certificates
- RFC822MailUser

In the Internet X.509v3 Public Key Infrastructure LDAPv2 Schema [6], these attributes are:

- cACertificate
- certificateRevocationList
- authorityRevocationList
- crossCertificatePair
- userCertificate
- rfc822Mailbox

This schema is used in some commercial CA products.

Some agencies may wish to make other information available externally to support their PKI applications. However, this profile does not address or impose requirements on application-specific data in agency directories.

The *cACertificate* and *crossCertificatePair* attributes require special attention when accessing the directory to build the certificate path. Neither the Public Key Infrastructure (X.509) "PKIX" specification nor the X.509 standards explicitly provide an algorithm to construct a certificate path. The PKIX LDAP-V2-schema provides guidance on what can be stored in the specific attributes. The draft states the following about the *cACertificate* attribute and the *crossCertificatePair* attribute:

> The *cACertificate* attribute of a CA's directory entry shall be used to store self-issued certificates (if any) and certificates issued to this CA by CAs in the same realm as this CA.

The forward elements of the *crossCertificatePair* attribute of a CA's directory entry shall be used to store all, except self-issued certificates issued to this CA. Optionally, the reverse elements of the *crossCertificatePair* attribute of a CA's directory entry may contain a subset of certificates issued by this CA to other CAs. If a CA issues a certificate to another CA, and the subject CA is not a subordinate to the issuer CA in a hierarchy, then the issuer CA must place that certificate in the reverse element of the crossCertificatePair attribute of its own directory entry. When both the forward and the reverse elements are present in a single attribute value, issuer name in one certificate shall match the subject name in the other and vice versa, and the subject public key in one certificate shall be capable of verifying the digital signature on the other certificate and vice versa.

When a reverse element is present, the forward element value and the reverse element value need not be stored in the same attribute value; in other words, they can be stored in either a single attribute value or two attribute values.

In the case of V3 certificates, none of the above CA certificates shall include a *basicConstraints* extension with the cA value set to FALSE.

A path development algorithm must consider that the CA's certificate must be stored in the *crossCertificatePair* attribute, but the algorithm may consult the *cACertificate* attribute first, for performance reasons.

The following sections define the attributes and object classes that are required for end entities and CAs.

2.1 End Entities

2.1.1 Attributes

End entity (EE) directory entries shall contain, as a minimum, the following attributes:

userCertificate as defined in 1997 X.509v3 [7] (OID: 2.5.4.36)

commonName as defined in 1997 X.521 [8] (OID: 2.5.4.3)

surname as defined in 1997 X.521 (OID: 2.5.4.4)

Note**:** The EE relative distinguished name (RDN) shall consist of the *commonName* attribute type and value. For example: cn=John Smith

Optionally, EEs may include the following object attributes:

attributeCertificate as defined in 1997 X.509v3 (OID: 2.5.4.58)

2.1.2 Object Classes

EE entries shall be made up of the following object classes:

person as defined in 1997 X.521 (OID: 2.5.6.6)

pkiUser as defined in RFC 2587: LDAPv2 Schema (OID: 2.5.6.21)

Optionally, EEs may include the following object classes:

securePkiUser as defined in Allied Communications Publication (ACP) 133 Edition B [9] (OID: 2.16.840.1.101.2.2.3.66). This auxiliary object class includes *attributeCertificate* and *supportedAlgorithms* as optional attribute types.

organizationalPerson as defined in 1997 X.521 (OID: 2.5.6.7)

inetOrgPerson as defined in Internet Engineering Task Force (IETF) Request for Comment (RFC) 2798 [10] (OID: 2.16.840.1.113730.3.2.2)

2.2 Certification Authorities

2.2.1 Attributes

CA entries in the directory, including Policy Creation Authorities (PCAs) and Policy Approving Authorities (PAAs), shall contain at a minimum the following attributes:

commonName OR *organizationalUnitName* as defined in 1997 X.509v3 (OIDs: 2.5.4.3 and 2.5.4.11 respectively)

cACertificate as defined in 1997 X.509v3 (OID: 2.5.4.37). As per the LDAPv2 Schema (RFC 2587), the cACertificate attribute shall be populated as follows:

> "The *cACertificate* attribute of a CA's directory entry shall be used to store self-issued certificates (if any) and certificates issued to this CA by CAs in the same realm as this CA."

certificateRevocationList as defined in 1997 X.509v3 (OID: 2.5.4.39)

crossCertificatePair as defined in 1997 X.509v3 (OID: 2.5.4.40). As per the LDAPv2 Schema (RFC 2587), the *crossCertificatePair* shall be populated as follows:

> "The forward elements of the *crossCertificatePair* attribute of a CA's directory entry shall be used to store all, except self-issued certificates issued to this CA. Optionally, the reverse elements of the *crossCertificatePair* attribute of a CA's directory entry may contain a subset of certificates issued by this CA to other CAs. When both the forward and the reverse elements are present in a single attribute value, issuer name in one certificate shall match the subject name in the other and vice versa, and the subject public key in one certificate shall be capable of verifying the digital signature on the other certificate and vice versa.
>
> "When a reverse element is present, the forward element value and the reverse element value need not be stored in the same attribute value; in other words, they can be stored in either a single attribute value or two attribute values."

CAs entries in the directory may optionally contain the *authorityRevocationList* attribute as defined in 1997 X.509v3 (OID: 2.5.4.38).

> Note: The CA RDN shall consist of either the *commonName* attribute type and value or the *organizationalUnitName* attribute type and value. For example: *cn=NSA CA* -- OR -- *ou=ECA1*

2.2.2 Object Classes

CA entries shall be made up of the following object classes:

pkiCA as defined in RFC 2587: LDAPv2 Schema (OID: 2.5.6.22)

The base object class of CAs shall be one (or more) of the following:

person as defined in 1997 X.521 (OID: 2.5.6.6)

organizationalPerson as defined in 1997 X.521 (OID: 2.5.6.7)

inetOrgPerson as defined in IETF RFC 2798 (OID: 2.16.840.1.113730.3.2.2)

organizationalUnit as defined in 1997 X.521 (OID: 2.5.6.5)

3.0 NAMESPACE CONTROL AND DIRECTORY TREE STRUCTURE

Public key infrastructure certificates and related objects are defined by the X.509 specification, which is a portion of the overall X.500 information model. These PKI objects are made available to relying parties by a directory service. The FBCA directory service acts as a bridge between various agency directory services, allowing relying parties to retrieve certificates to construct trust paths and Certificate Revocation Lists (CRLs) to ensure that the certificate has not been revoked.

The X.500 information model is used by both X.500- and LDAP-based directory servers, and forms the basis for interoperability between directory services. Objects within the federal directory service are located using the object's Distinguished Name (DN), which specifies both the Relative Distinguished Name (RDN) of the object and it's location within the overall federal directory.

The federal directory service can be thought of as a tree – a logical hierarchical structure composed of all the various directory services operated by federal agency directory services, and made possible by general agreement on naming schemes and directory structures. An agency's "namespace" refers to the individual directory, or subtree, controlled by that specific agency.

3.1 Agency Directory Service Requirements

Agencies are not required to conform to any specific directory protocol internally. However, in order to interoperate with the FBCA, an agency's directory service must conform to the following requirements:

- The agency must register their directory service as in Section 3.1.1 with the FBCA in order to establish interoperability.
- The agency's PKI information must conform to the X.500 information model and X.509.
- The agency's directory service must support 1993 X.500 chained operations, 1993 X.500 referrals, or LDAP v3 referrals.
- The agency's PKI information must conform to the namespace strategies stated in Sections 3.2, 3.3, and 3.4, below.

The agency may choose to employ a Border Directory Server Agent (DSA) to provide for protocol conversion, enforce security, and restrict access to internal directory services. Alternate approaches are discussed in Appendix B, along with relevant security implications and considerations. Examples of how to connect various directory services to the FBCA Directory are illustrated in Appendix C.

3.1.1 Registration

In order to support connectivity between the FBCA and agency directory services, each agency participating in the FPKI must register their directory service or Border DSA with the FBCA Operational Authority (OA). Appendix A contains a worksheet to aid you in collecting this information prior to registration.

The following information must be provided:

- Name and address of agency desiring to interoperate with the FBCA directory
- Name, address and contact information for that agency's directory administrator
- Distinguished Name, Network Address, and Host Name of directory service
- Naming Context(s) (i.e., namespace) provided by this directory server (see Sections 3.2, 3.3, and 3.4)

- Protocols supported (X.500 and/or LDAP)

3.2 X.500 Directory Services

If the agency chooses to use an X.500-based directory service, its directory must conform to the name space as defined for the Federal Government [3] (Figure 3-1). This namespace contains the U.S. Government level of the global X.500 Directory Information Tree (DIT) and all governmental agencies and departments. In X.500 terms, this namespace includes directory servers with the naming context of:

c=us; o=U.S. Government

The U.S. Government is registered as an *organization* (o) object in the Global DIT, directly subordinate to the *country=us* object (the national U.S. country level object). Agencies and departments occupy *organizationalUnit* (ou) objects immediately beneath the o=*U.S. Government* entry. Agency and department names in the Federal Government namespace must conform to agency and department names as stated in The United States Government Manual (*http://www.access.gpo.gov/nara/nara001.html*). This publication cites official names for agencies and departments (*organizationalUnit*s) of the Federal Government. For instance, Transportation and Treasury would be:

c=us; o=U.S. Government; ou=Department of Transportation

c=us; o=U.S. Government; ou=Department of the Treasury

The Federal Aviation Administration and Internal Revenue Service have been assigned the following directory naming contexts based on their official names and parent agencies:

c=us; o=U.S. Government; ou=Department of Transportation; ou=Federal Aviation Administration

c=us; o=U.S. Government; ou=Department of the Treasury; ou=Internal Revenue Service

Each agency or department is free to define and manage the namespaces for organizational units within that agency. It is highly suggested, however, that the organizational unit names listed under that agency in The United States Government Manual be used for consistency.

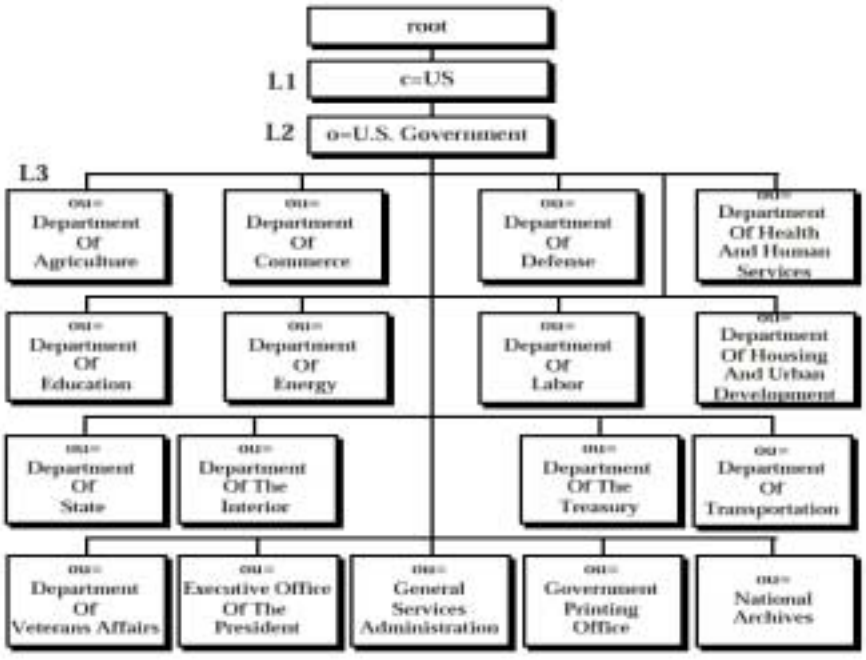


Figure 3-1. Federal Government Top Level Directory Naming

Abbreviations are allowed, but must be negotiated with the FBCA Registrar (as in Section 3.1.1 above) to ensure uniqueness within the U.S. Government namespace. Potential conflicts on abbreviations may occur, and will be solved as follows.

Any number of *organizationalUnitNames* may be registered to aid in directory searches. For example, the Department of Transportation directory entry might have the following names (if authorized by the FBCA Registrar):

c=us; o=U.S. Government; ou=Department of Transportation (e.g.; the "official" name)

c=us; o=U.S. Government; ou=DOT (the unofficial name, as approved by the registrar)

Both entries in the FBCA directory will "point to" (e.g. will have a subordinate reference or LDAP referral to) the directory server being operated by the agency.

3.2.1 DNs versus RDNs

Each object stored in an LDAP or X.500 directory is identified by a Relative Distinguished Name (RDN). The RDN is the value that uniquely identifies an entry within the current node (or "container") of the directory. For instance, if the Relative Distinguished Name is a person's full name (e.g. their *commonName* or *cn*), each directory entry within a specific level will have a unique RDN. At a given level of the directory, there can exist only one, single entry with a RDN of *cn=John Smith*.

Since the directory contains several levels (nodes or containers), there might exist multiple nodes that contain a RDN of *cn=John Smith* throughout the directory tree. But within each individual directory node or container, there can exist only one such entry.

An entry in the directory is specified by its full Distinguished Name (DN), which is composed of all the RDNs starting with the top of the tree and moving downward to the specific entry. In the original X.500 syntax, the RDNs that composed a full DN were separated from each other by an @ sign, and listed beginning at the top of the tree. The @ sign has been replaced by a comma in most X.500 products for readability. A full X.500 DN would look like:

c=US@o=U.S. Government@ou=General Services Administration@cn=John Smith, or

c=US, o=U.S. Government, ou=General Services Administration, cn=John Smith

LDAP typically reverses the order, like this:

cn=John Smith, ou=General Services Administration, o=U.S. Government, c=US

Functionally, both DNs are the same. The DN describes the path through the directory tree, which contains the following objects:

- A *country* object with a RDN of *c=us*
- An *organization* object with a RDN of *o=U.S. Government*, which is subordinate to the *c=us* object.
- An *organizationalUnit* object with a RDN of *ou=General Services Administration*, which is subordinate to the *o=U.S. Government* object.
- The targeted person entry with a RDN of *cn=John Smith*

3.2.2 Advantages and Disadvantages of X.500

The X.500 naming scheme is well understood. It is supported in current PKI products, which have been successfully demonstrated in the PKI FBCA and the EMA challenge demonstrations. The drawback of this naming scheme is that it is little used by anyone other than for PKI. Most users do not understand nor care about the finer distinctions of the Federal X500 directory naming structure. Hence, distinguished names with organizational structure embedded in them are generally difficult for users to comprehend or remember.

Many agencies have adopted a very "flat" namespace, where all the organization's users are listed directly underneath the agency object or within a single subtree, regardless of location or organizational structure.

Another recurring debate, which occurs with X.500- and LDAP-based systems, lies in the directory tree structure within the agency. There are three basic approaches:

- Put all the directory entries into a single, flat namespace (usually requires a single DSA serving the entire agency or replication of this information to geographically located directory servers).
- Divide the tree to mirror organizational structure (which may create problems if the directory servers are located in multiple geographic locations).
- Divide the tree to mirror geographical or network infrastructure (presents issues related to interactive searching and use).

The Federal Bridge CA has no preference and issues no guidance as to the tree structure of internal agency directory services. This area is clearly outside the scope of this document.

3.3 Internet Domain Name Based Naming

With the global acceptance of Internet and technologies such as the Domain Name System (DNS) and RFC822-based e-mail, many portions of the government have ignored older technologies such as X.500 and have implemented Internet-based infrastructures. These infrastructures are used primarily for e-mail and web-based delivery of services and information.

The Internet DNS provides a hierarchical naming and locating system based on domain name components. For instance, the Internal Revenue Service is registered as *irs.treas.gov*. The U.S. Federal government "owns" the *gov* "top-level domain", and is responsible for assigning and administering domain component names underneath that domain. Department of the Treasury (Treasury) has registered the domain component of "*treas*", underneath *gov*. Therefore, any e-mail user at the Department of the Treasury would have an e-mail address something like *user@treas.gov*, and the main Treasury web page would be found at *www.treas.gov*.

The Internal Revenue Service has been assigned the domain component of "irs" by Treasury, such that a user within IRS should have an email address of *user@irs.treas.gov*. However, IRS has also registered directly underneath .gov, meaning that most IRS personnel use email addresses like *user@irs.gov* and the main IRS web page is found at *www.irs.gov*.

This DNS-style of naming was originally developed to support hierarchical management and searching of computer system names (e.g. "hostnames"). Each computer attached to the Internet has an Internet Protocol (IP) address, which consists of four numbers between 0 and 255, separated by periods. These addresses look something like 192.248.32.14. Clearly, this is hard for users to comprehend, much less remember. Who wants to address an email message to *john.smith@192.248.32.14*? (Actually, this style address will work on many Internet-connected systems). DNS maps this numeric IP address into a human-readable system name, called a Fully Qualified Domain Name (FQDN). This allows a user to

send email to *john.smith@company.com* instead of trying to remember the IP address. The computer looks up *company.com*, finds the numeric address, and makes the connection. In this sense, IP addresses are like telephone numbers, and DNS is like a giant, worldwide electronic phone book.

X.500 is a completely separate directory system from DNS. However, a proposed Internet Standard as described in RFC 2247 [11] and RFC 2377 [12] provides a method of representing Domain Name System domain components using the X.500 information model. This allows both X.500 and LDAP-based directory services to store information in a structure familiar to Internet-literate users.

RFC 2247 defines an attribute, *domainComponent (dc)*, which can be used to store a domain component such as "*gov*". It also defines two objects, *domain* and *dcObject*. The *dcObject* object can be added to existing objects so that they can contain a *dc* attribute. The *domain* object allows the addition of new entries that contain a *dc* attribute.

Using *domain* objects, it is possible to accurately represent the DNS "tree" within an X.500 or LDAP directory service (Figure 3-2). The user specified by the email address *john.smith@irs.treas.gov* would be represented by the X.500 DN:

dc=gov; dc=treas; dc=irs; cn=john.smith

LDAP allows a relaxed form of DN in reverse order, which looks like:

cn=john.smith, dc=irs, dc=treas, dc=gov

The information in the directory is the same either way. Searching based on this DNS-style naming can be very intuitive to users who are familiar with Internet email addresses. The Federal Bridge CA will allow agencies to choose to implement naming in this fashion, instead of (or in addition to) the X.500-style Federal Government naming set forth in Section 3.1.

Additionally, the *dcObject* object could be used to add the *dc* attribute to other X.500 objects. Therefore it could allow for construction of DNs which look very much like X.500, but which are actually composed of *DomainComponent* attributes. This sort of DN would look like:

dc=us; dc=U.S. Government; dc=treas; dc=irs; cn=john.smith (or)

cn=john.smith, dc=irs, dc=treas, dc=U.S. Government, dc=us

The Federal Bridge CA will <u>not</u> support this style naming. Its similarity to pure X.500 naming can cause significant confusion. Since it doesn't map to the Internet-style e-mail addresses, it is not intuitive to use and therefore provides no discernable benefit. As DNS evolves in the future, country-based naming may come into use. If so, this decision will be revisited at that time.

3.3.1 Drawbacks of DNS-Style Naming

RFC 2247, the document that proposes this style of addressing, is a proposed Internet Standard. It therefore is fairly stable and not subject to major changes. However, it may not be widely implemented in applications and commercial software products yet.

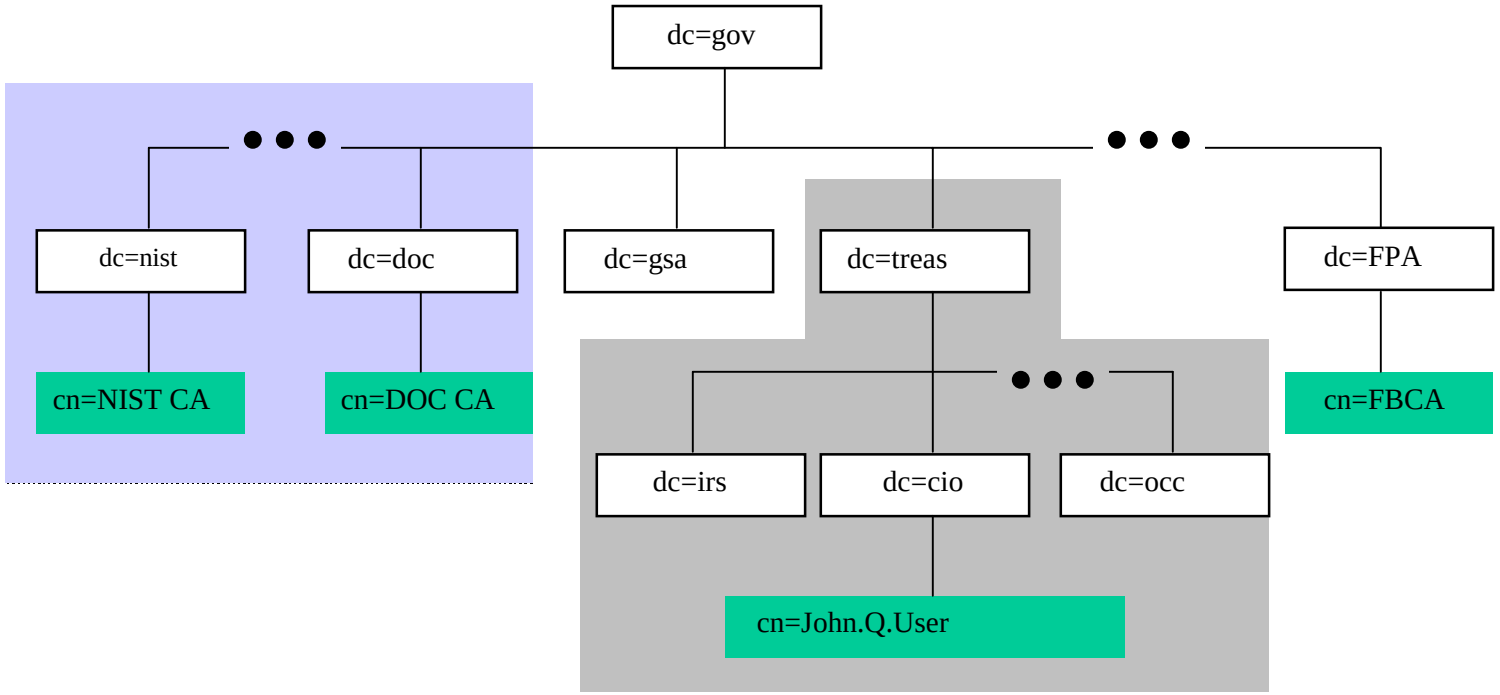
The *.gov* domain is owned by the U.S. Government. Registration of government agencies and operation of the government-level DNS is outsourced to a vendor. There is little guidance relating to the creation of DNS-style domain information for government agencies. This leads to several confusing situations:

Internet domain name components are typically short and cryptic. Many times, all users appear directly underneath the organization with no clue as to organizational structure or geographic location. Also, many agencies have registered domain names that don't reflect the actual Federal departmental structure.

This may be because of grandfathering (e.g., an agency registered the name before any official policy was established), or because the public is neither interested in nor knowledgeable about the government's departmental structure, and would simply be confused by domain names that reflect actual structure. Examples include:

faa.gov	is more understandable than	*faa.dot.gov*
nist.gov	is more understandable than	*nist.doc.gov*
cg.mil	is more understandable than	*cg.dot.gov*

Figure 3-2. Domain Component Naming DIT



It may be fairly clear that the FAA should be a part of the Transportation Department, but does the public generally know that NIST is a part of the Commerce Department, or that the Coast Guard, a uniformed service, is actually under the Department of Transportation rather than the Department of Defense?

Another potential problem can be confusion between the government and the private sector because of the Top Level Domain Names. The U.S. Government only has authority over domain names ending with *.gov*. Sites such as *www.irs.com* and *www.fbi.com* play off of this confusion for purposes of commerce, social satire, political commentary, and worse.

And lastly, there is no automatic synchronization between X.500 and the DNS. When a domain component is registered in the DNS, it will require a second action to have it manually entered into the X.500 directory. This presents the potential for the X.500 or LDAP-based directory to get out of synchronization with the current state of the DNS. Within government, the changes are infrequent enough that this should be a manageable problem.

3.4 Combined Domain Component Names with X.500 Names

Recently the Higher Education community, in a part of the **Internet II** effort [13], has taken a slightly different approach to the use of domain component names, and asked the FPKI directory profile support this option. This community advocates combining domain component names with traditional X.500 names in the *subjectName* field of a certificate to enforce name uniqueness. This requires no new registration or management, and it may facilitate directory service discovery via DNS SRV records [14]. No rule in X.500 prohibits this, and recent changes to the FBCA CP will also allow for this flexibility. New infrastructures are being designed in the Internet2/EDUCAUSE arenas to meet the needs of academia and a myriad of applications [13]. Allowing this flexibility will facilitate interoperability between institutions of higher education and the federal government, and foster the use of the FBCA model outside the US government.

The Federal PKI Technical Working Group has discussed this proposal extensively and tentatively agreed to support this option as a reasonable basis for interoperable naming. The FBCA directory server will hold 2 (or 3) roots for [o=US Government, c= US], [dc=gov], and, possibly, [dc=mil]. Agencies would be encouraged to use only one name form or the other (Figure 3.1 and Figure 3.2). However, agencies have autonomy over the content of their own directory services and could therefore choose to include the combined name form in entity certificates. In this case, the agency must choose whether to use [o=US Government, C= US] (Figure 3.3) or [dc=gov] (Figure 3.4) as the most significant part of their name.

Using this scheme, some naming examples would be:

> *cn=John Smith, dc=irs, ou=Internal Revenue Service, dc=treas, dc=gov,* ***ou=Department of Treasury***, ***o=U.S. Government***, ***c=US***
>
> *cn=John Smith, ou=Internal Revenue Service, dc=irs, dc=treas, dc=gov,* ***ou=Department of Treasury***, ***o=U.S. Government***, ***c=US***

Or, starting with the ".gov" domain name:

> *cn=John Smith, ou=Internal Revenue Service, o=U.S. Government,* ***dc=irs***, ***dc=gov***
>
> *cn=John Smith, ou=Internal Revenue Service, o=U.S. Government, c=US,* ***dc=irs***, ***dc=gov***

Figure 3-3. Combined Domain Naming with X.500 Names

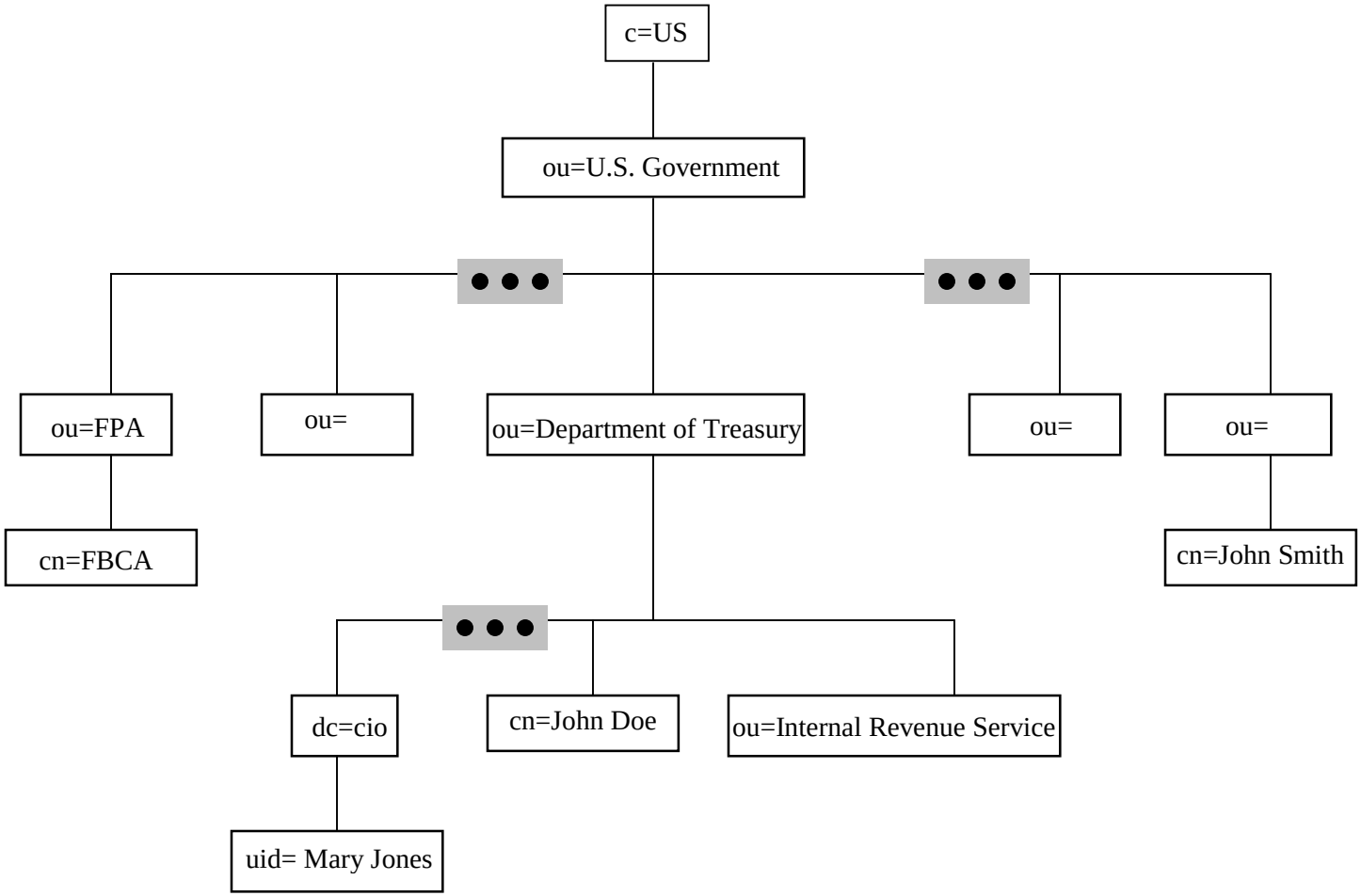
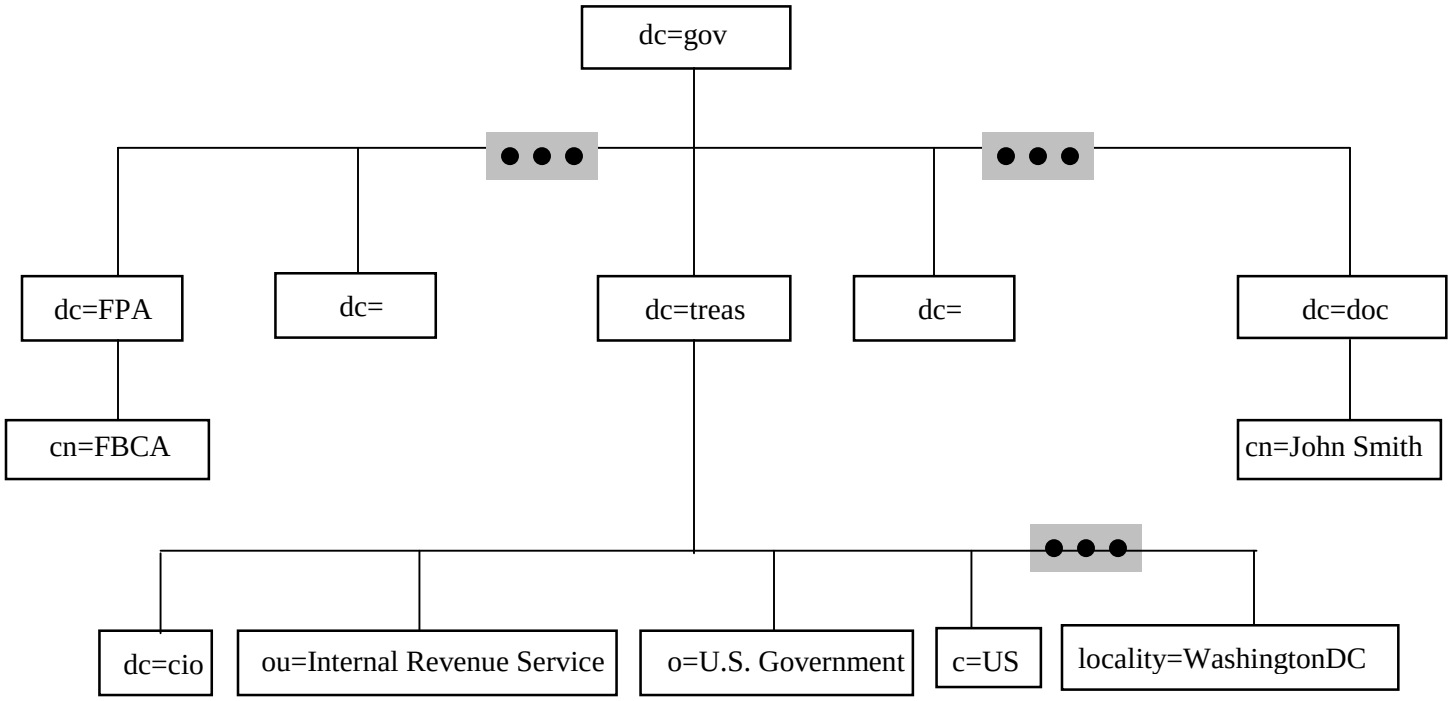


Figure 3-4. Combined Domain Component and X.500 Naming (alternate)



Several issues have been raised regarding this combined naming scheme. It is unknown how any specific vendor's products (directory, client, or PKI) will react to this naming scheme. Any agency contemplating use of such combined naming schemes is ***strongly encouraged*** to fully test such a naming scheme, both internally and with other agencies and entities with whom

3.5 The U.S. Government Directory Server

In order to promote interoperability between various agency and department directory services, the Federal Bridge CA program will operate a Directory Server that supports both the Federal Bridge CA, and the U.S. Government level of the X.500 DIT.

In support of the U.S. Government level, the FBCA program will provide the following services:

- Registration of directory services for agencies that wish to (a) participate in the Bridge CA program, and/or (b) interoperate with other government directory services.
- The DSA will provide knowledge references to all registered directory services, and also to international government and the private sector, as required in order to promote Electronic Government initiatives.
- Coordination with E-gov and international interoperability initiatives.

The DSA will support the traditional X.500 DIT for the U.S. Government (Figure 3.1), and the "de-facto" Internet DNS directory structure (Figure 3.2). It will be able to provide connectivity among these namespaces, promoting interoperability among agencies that have implemented traditional X.500 naming, those that rely upon the DNS structure, and those supporting both.

4.0 DIRECTORY PROTOCOLS

Two broad categories of directory servers are currently in use – X.500 DSAs, and LDAP servers. Both use the same X.500 directory information model and the LDAP client directory access protocol. X.500 DSAs also support Directory Service Protocol (DSP) for chaining of information between directory servers. An LDAP server typically supports the LDAPv3 [15] client interface and LDAPv3 referrals. At the present time, if chaining between LDAP servers is offered, it is a proprietary implementation. LDAP-based chaining has not yet become a standardized protocol.

The FBCA will maintain an X.500 DSA holding the roots for *c=US*, *o=U.S. Government*; *dc=gov*; and possibly *dc=mil*. This FBCA DSA will be available for chaining with agency X.500 DSAs.

Although this profile does not preclude chaining internal X.500 directory servers to the FBCA directory server, most agencies will choose to operate with the Federal PKI through a border directory server located outside the agency firewall, as described in Appendix B and C.

For agencies that use X.500 for their directory service or their border directory, it is not necessary to specify the client to directory server access protocol. Typically, it will be some version of LDAP, but the older X.500 Directory Access Protocol (DAP) is also acceptable. All that is required is that agency clients are compatible with agency servers. Agency servers will obtain needed external certificates and CRLs for their clients via DSP chaining, and this is transparent to the clients. Each X.500 agency Border DSA will be chained to the FBCA directory, via DSP chaining.

Agencies that choose to use LDAP servers internally may make external agency certificates available to clients in several ways:

- The agency may stand up an X.500 DSA as a border directory and chain it to the FBCA DSA;
- Alternatively, if agency clients support LDAP v3 with referrals, then the LDAP servers may refer clients to the FBCA DSA for external certificates (or may make direct referrals to the border directories of other agencies).

Agencies that choose to use LDAP servers internally may make internal agency certificates and CRLs available externally by:

- Standing up an X.500 DSA chained to the FBCA DSA and posting externally available certificates and CRLs to it. This may be achieved by purchasing directory services from a 3rd party supplier. This is the preferred or recommended method of interoperating with other agencies through the FBCA DSA.
- Standing up a Sacrificial LDAP Server (with a replicated subset of the agency's information) or Reverse Proxy, in order to allow users to retrieve needed certificates and CRLs.
- Alternatively, if no X.500 border DSA is set up, users may include a certificate list beginning with the certificate issued by the FBCA to their agency PCA and ending with the user's signature certificate in the header of signed S/MIME messages. This does not directly support encryption, but it allows an external relying party (who interoperates through the FBCA) to validate S/MIME signatures.

As the Federal PKI develops, the FBCA directory may incorporate a meta-directory or "meta-connector" capability to transparently resolve the queries of X.500 DSAs for information contained in LDAP servers. In principle, the choice to use X.500 style or Domain component names is independent of the choice to use X.500 DSAs or LDAP servers. In practice, it appears likely that those who choose to use domain component names will probably choose to use LDAP servers. It is possible to chain through the FBCA DSA from an agency that uses Domain Component names to one that uses X.500 style names. The

FBCA directory shall hold the root for both *c=US; o=U.S. Government* and *dc=gov*, and support chaining of both name types.

4.1 Authentication Requirements

For the initial version of the Federal PKI, agency directories will be allowed to connect to the Federal Bridge CA with no authentication.

4.1.1 Client Authentication

FPKI directory clients that read the FPKI directory (read, list, search directory operations) require no authentication (i.e. anonymous binds to the directory are acceptable). This profile does not address directory access control requirements to update FPKI directory servers. Agencies must ensure that only authorized parties can update their own agency PKI directory information.

4.1.2 Server Authentication

Initially, the FPKI directory service will not require authentication between agency servers and the FBCA directory server for DSP chained operations. The FBCA directory server is protected by a firewall that will be configured to allow only DSP operations between the FBCA directory and specified agency directories. Since the entries contained within the FBCA directory is public information, these firewalls will offer sufficient protection. The identity of LDAP clients querying the FBCA's LDAP directory server will be anonymous.

Future enhancements to the FPKI directory structure may allow for strong credential-based authentication between servers. However, the state of technology is such that this is capability is not possible at the present time given the fact that different vendors' products do not provide for seamless interoperability of security functionality.

4.2 Disclaimer

The FBCA directory service is being provided to promote full interoperability between government agencies, in support of the Federal Bridge CA. Every attempt will be made to ensure that information contained in the directory service is correct (as provided by the individual agencies), and that this information is protected from unauthorized access and modification. However, each agency or department must consider the possible consequences of unintended disclosure of information provided due to error or attack. It is the responsibility of each agency or department to establish their own policy and security posture with regard to directory-based information, and to implement whatever protocols and protection that they deem sufficient to protect critical systems, including their internal directory services.

APPENDIX A – NAME REGISTRATION WORKSHEET

If your agency is deploying an X.500 directory service and desires to use the X.500-style naming, you should register your directory with the FBCA Operational Authority (OA). To register, complete the following information and forward it to:

Name (FBCA Contact Information goes here)
Street Address
City, State Zip
Phone Number:
Fax Number:
Email address:

Agency Information	
Agency Name	
Mailing Address	
City, State & Zip	
Main Phone #	
Main Fax #	
Directory Administrator Information	
Administrator Name	
Mailing Address	
City, State & Zip	
Telephone #	
Fax #	
Email Address	
Alternate Contact	
Mailing Address	
City, State & Zip	
Telephone #	
Fax #	
Email Address	
Directory Service Information	
Type of Service	[ ] X.500 [ ] LDAP v2 [ ] LDAP v3 [ ] Other_____
Server Host Name	
Server IP Address	
Directory Port #	
DN of DSA entry (if applicable)	
Naming Context(s) and Protocols Supported	

Does this directory support chained operations using X.500 DSP?	[ ] Yes [ ] No
Is this directory server a Border DSA?	[ ] Yes [ ] No
Does this directory server support user access via X.500 DAP?	[ ] Yes [ ] No
Does this directory server support user access via LDAP v2?	[ ] Yes [ ] No
Does this directory server support user access via LDAP v3?	[ ] Yes [ ] No
Does this directory server allow access from other Federal Agencies?	[ ] Yes [ ] No
Does this directory server allow access from anonymous / untrusted users?	[ ] Yes [ ] No
What are the naming contexts supported by this directory server?	*e.g. ou=Bureau of XYZ, ou=Department of ABC, ou=U.S. Government, c=us*
Naming Context #1	
Naming Context #2	
Naming Context #3	
Naming Context #4	

APPENDIX B – ESTABLISHING AN AGENCY DIRECTORY SERVICE

This document presumes that your agency already has an established organizational directory service that can be connected to the FBCA. If this is not the case, an official directory service must be established that can serve as the connection point between your agency, the FBCA, and other agencies. The general steps involved in setting up such a directory service are:

1. Decide which directory technology and/or product that your agency is going to support. It is highly suggested that you use either X.500 or an LDAP directory server. Proprietary directory services such as Active Directory or NDS may already be in use within your agency. If so, it should be possible to connect them to the FPKI directory service, but it may require that your agency implement a border DSA, sacrificial LDAP server, or metadirectory technology.

2. Decide upon the naming convention that your agency is going to support, whether full X.500-based naming or Internet-style domain naming. A full discussion of these options can be found in Section 3. The FBCA supports both styles for agency naming contexts.

3. Register your directory service with the FBCA OA. Instructions for doing so can be found in Appendix A.

4. Plan the directory architecture – how many servers, where located, alternate / fallback service.

5. Plan the security architecture for the directory. The following sections of this appendix discuss security related threats and mitigation strategies that can affect the directory architecture.

6. Begin the process for registering for connection to the FBCA, as outlined in Appendix D of this document.

B.1 Security Considerations

All of the information contained within the FBCA directory server is considered public information. However, because agency directory services support operational requirements, they often need to contain information of a sensitive or For Official Use Only (FOUO) nature that should not be revealed to persons outside of the agency. Therefore, an agency may have issues with the security implications connecting their directory service with an external directory service such as the FBCA.

Agencies are normally faced with conflicting goals with regard to an agency directory service. On one hand, they want their directory service to contain many different kinds of information and be readily available to all agency users who need access to that information. On the other hand, they generally want to identify a very small portion of their overall directory information as public information (a controlled set of phone numbers and email addresses, PKI certificates and CRLs, etc.), and they want to restrict access so that non-agency users cannot gain access to the rest of the information in their directory. At the same time, they want to protect their directory service from attack, denial of service, and unauthorized disclosure of information. And, they want to use the directory service to obtain needed information from other agency directory services.

Therefore, as agencies begin to allow connectivity with other directory services and access by non-agency users, they find that additional security capabilities must be added in order to provide accessibility and connectivity while ensuring survivability and availability, and protecting sensitive information from unauthorized disclosure.

B.2 LDAP vs. X.500

LDAP has a different security model than X.500. In LDAP, the client authenticates to the local server and this serves as proof of identity. The server uses that identity as the basis for all subsequent operations during that session. LDAP can use Secure Socket Layers (SSL) or Transport Layer Security (TLS) in order to protect from unauthorized disclosure by encrypting the data flowing between the server and client. If this information were not encrypted, passwords and other directory information could be intercepted by capturing the information flowing between the client and server using network "sniffers".

LDAP is a client-server protocol that allows user applications to retrieve and update directory-based information. It was originally based on a subset of the ITU X.500 recommendations, and has always been an Internet proposed standard. LDAP version 3 diverges from the pure X.500 in a few specific details, but still follows the X.500 "information model". Almost all directory-aware clients use the LDAP protocol to access directory services, and nearly every X.500 directory vendor provides an intrinsic LDAP server within their product. More accurately, this server is usually an LDAP-to-DAP gateway, converting the user's LDAP requests to X.500 query operations, converting X.500 responses to a series of LDAP responses, and sending the responses back to the client. Therefore, the client application doesn't know or care whether the directory being accessed is X.500-based, LDAP-based, or an Oracle database.

LDAP-based directory services (e.g. non-X.500) are becoming quite scaleable and robust, and are being implemented by the majority of federal agencies. It is fairly straightforward to set up a large LDAP directory to serve an agency's user population. Unfortunately, having that directory server interoperate with another organization is not so simple, even if the other organization has implemented LDAP.

LDAP directory servers tend to be isolated islands of information. Users within the organization cannot easily access directory information within other agencies, whether LDAP-based or X.500. And, users outside of the organization cannot access information maintained in the organizational directory. While this may be an inconvenience when the directory information consists of email addresses and phone numbers, it is a severe problem when the information to be retrieved includes public key certificates and certificate revocation lists. Relying parties outside of the organization must be able to retrieve these objects in order to validate digital signatures, or to obtain encryption certificates.

Pure X.500 directory servers can also require that the client authenticate to the local X.500 DSA. In addition, each directory request carries the identity of the requestor. If the local DSA doesn't hold the requested information it will chain the operation onward. When the performing DSA receives the request, it can prove the identity of the requestor. In X.500, requests can be digitally signed, thereby providing non-repudiable proof of identity of the requestor. The DSA that performs the requested directory operation can check this digital signature in order to prove the requestor's identity, and can use that identity when enforcing access controls that may apply to the requested information.

This incompatibility presents a couple of difficulties related to trust when creating hybrid X.500-LDAP directory services:

- LDAP has become the universal client-to-directory access protocol, and LDAP clients cannot create signed directory requests. LDAP servers base their trust on the fact that credentialed authentication may have been performed between the client and server at initial bind. However, this trust in the client's identity is only held by the LDAP server and cannot be provided to another server as part of a chained operation. This is likely to change in future versions of LDAP, but it is not possible with LDAP v3 and earlier implementations.
- If the client is using LDAP to connect to an X.500 DSA, any chained requests forwarded from that DSA could contain the user's identity (DN). However, the requests cannot be signed because the DSA doesn't hold the user's private key (which is required to create a digital signature). Therefore, the performing DSA (the one that eventually does the requested operation) cannot trust

the user's identity. The security policy and at the performing DSA would normally treat such requests as untrusted, or anonymous.

This discontinuity in security generally leads agencies to implement additional security technology and techniques to protect the agency directory from unauthorized use and attack. These can include techniques such as compartmentalization, selective replication, border directories, and proxy servers – all of which are described in some detail below.

B.2.1 PKI Users With LDAP-Based Directories

In order to validate a digital signature, a PKI-aware client must construct a trust path and must check to see that the certificate has not been revoked. The certificates and CRLs needed to perform these tasks are generally obtained via LDAP from a directory service. If the issuing authority and client are both within the same agency and served by the same directory service, this means that the client can simply issue repeated requests to the organizational directory until it has all the objects it needs.

However, if the signature was created by someone in a different agency, the PKI-aware client must construct a trust path that includes the Bridge CA, and must check the revocation status of a certificate that was issued by a completely different organization. Not only will the client need access to information in their own agency's directory service, but they will also need information that is found in the Bridge Directory and in the issuing agency's directory service.

If the agency uses an X.500 directory infrastructure, this is relatively straightforward. The user simply queries their directory server using LDAP. The query is converted to X.500 DSP and chained to whatever X.500 directory holds the required information. The response is chained back to the agency directory, converted to LDAP, and sent to the client. The client is not even aware that the query and responses were automatically chained through multiple directory servers in order to satisfy their query.

But, if the agency uses a pure LDAP server, all it can do is return a referral. LDAP v3 provides a referral capability similar to that provided by X.500. If an LDAP server does not contain the information requested, it can return a referral pointing to another LDAP server that might be better able to respond to the query. The LDAP client can then choose to disconnect from the current LDAP server and try the one referenced in the referral instead, if it is capable of handling referrals.

However, some existing LDAP clients are not able to follow LDAP referrals. Even if they were, every federal agency directory server would have to be configured with referral information about all the other agencies. This is sometimes referred to as the N*(N-1) problem. If you only have two agencies, two referrals are required. Three directories require six referrals. Four directories require twelve referrals. One hundred directories would require that 9,900 referrals be maintained. Some estimates place the number of directory services within federal agencies at over 1,000 – requiring nearly a million referrals, posing a bit of an issue with regard to scalability!

The initial operating capability of the FBCA directory service didn't allow direct access by LDAP clients. When available, however, client requests could be converted to X.500 DSP and chained by the FBCA directory to other agencies. From that point, the client will not have to handle any further referrals unless the issuing agency was also using an LDAP-based directory service.

In this manner, the FBCA directory service would become the defacto standard directory server to which the majority of agency referrals could point.

B.2.2 X.500 Access to Agency LDAP Directories

Certificates and revocation information must be obtained from the issuing agency in order to validate a digital signature. If the relying party's organization uses an X.500 directory and the issuing agency uses

an LDAP-based directory service, there is no way to chain the X.500 DSP queries to the agency's LDAP-based directory service. One possible approach would be for the agency to provide directory information such as certificates and CRLs to the FBCA, which would "publish" them, adding them to the FBCA directory base so other agencies could find them. However, this will require that updated information be provided by the agency on a regular (probably daily) basis. Each agency providing this kind of information will have to convert their data to a standardized format (probably LDIF) so that it can be posted into the FBCA Directory.

Currently, it is planned that the FBCA directory service will provide LDAP v3 referrals to non-X.500 agency directory services. If the client's local agency directory does not contain the needed information, it will receive a referral to the FBCA Border Directory. It will then connect to the FBCA and request the information again. The FBCA would return an LDAP v3 referral to the target agency directory. The client would then connect to the target directory and request the information again.

B.3 Types of Threats

An agency's directory service should be designed such that it is resistant to common types of attacks. The most common types of threats are noted below.

B.3.1 Loss of Service

An agency directory should be available to the users and applications that rely upon it. Not only must it support the agency's own users, but it will be needed in order to obtain validate PKI-based digital signatures. The two basic issues to be addressed are availability and survivability.

Availability means that the directory service must be able to handle the expected usage load and that the agency network infrastructure can reliably connect users to the directory. Strategies for ensuring availability include monitoring the directory service's performance and ensuring that network infrastructures are sufficiently robust, with fallback or failover capability.

Survivability means that the directory service is resistant to intentional attack or systems failure. Strategies include protecting agency systems with firewalls, compartmentalization (segregated networks for infrastructure components and servers), active monitoring, and distribution/replication of directory information across multiple systems.

B.3.2 Unauthorized Disclosure

As noted earlier, much of the information contained in agency directory services might be considered sensitive and therefore not suitable for access by unknown persons. Methods of gaining unauthorized access to directory information can include social engineering (usually by tricking support personnel to grant access to an untrusted party), bird-dogging (accessing an authorized user's terminal when they aren't aware), snooping (watching the data move across the network), spoofing (providing false identification and credentials to the directory service), and directly accessing the data held by the directory (usually by hacking into the network and gaining access to the directory server itself).

Social engineering and bird-dogging must be addressed by training both users and support staff. Snooping can be mitigated to some degree by using SSL or TLS to encrypt data flowing between LDAP clients and servers. If the agency directory service is X.500-based, communication between DSAs can be protected using link encryption or virtual private network technology in order to prevent snooping. Spoofing is a more difficult problem to prevent, and requires establishing a method whereby a user's identity can be proven by some sort of credentials (such as a PKI private key) before being allowed to access the directory service. X.500 (and some LDAP) directories can implement access controls that restrict access to information based on the user's identity.

B.3.3 Unauthorized Modification

FPKI information should only be modified by authorized parties within each agency. Each agency is responsible for ensuring that unauthorized modifications of the information in the agency directory do not occur – especially PKI-related information that will be relied upon by users outside that agency.

If FPKI information is to be extracted from an agency directory and provided to the FBCA, the agency must ensure that only public information is included in the extract. In addition, a method of securing the information (such as a digital signature) must be agreed upon between the agency and the FBCA OA. A digital signature would provide proof that the extracted information had not changed in transit.

Obviously, directory information can also be modified by unauthorized access to the computer system the directory is running on. This sort of data alteration may not be detected immediately, if the information is cached for performance reasons or accessed infrequently.

B.4 Protection Strategies

The following strategies can be employed to protect an agency directory service. Many strategies can help mitigate multiple threats. Often, multiple strategies will be employed in conjunction with each other in order to create stronger protection architectures.

B.4.1 Publication to Bridge CA

It is quite likely that some agencies will not allow unrestricted access to their directories and are unable or unwilling to put up a border or "sacrificial" directory service. These agencies may ask the Bridge CA to publish this information for them. In this type of arrangement the agency will provide a file – probably in Lightweight Directory Interchange Format (LDIF) format – containing to the information to the Bridge Operating Authority on a regular (probably daily) basis. Automated scripts would extract this information and provide it to the Bridge directory server.

This capability must be negotiated on a case-by-case basis with the FBCA OA.

B.4.2 Authentication and Access Controls

The LDAP v3 core standard provides for no access control capability. However, most vendor products offer some sort of access control – usually a subset or variant of the X.500-style Access Control Information (ACI) functionality. When selecting an LDAP server, you should ensure that you understand the method by which access control is implemented in the product you are considering.

Most directory servers support either anonymous access (no authentication) or simple authentication (passwords). Simple authentication provides only limited assurance of the user's identity because passwords can be guessed or intercepted by network snooping. SSL or TLS encryption should always be employed when simple authentication is used.

Strong authentication uses credentials such as a PKI digital signature in order to establish the identity of the user. Both X.500 and many LDAP products can perform strong authentication of users, but most vendors' implementations are not compatible with each other.

Access controls are based on who you are (your identity) and what you are permitted to do (access rights). X.500 style access controls are based on a user's identity as expressed by the full distinguished name in the directory request. LDAP access controls are usually based on the user's identity or computer address, provided when the user first binds to the directory server. Using access controls, an agency can allow external users to view public information while restricting access to sensitive information such that only agency users can view it. Since access controls are enforced based on the user's identity, strong

assurance (e.g. credentials such as digital signatures) are the only way to be assured that the user's identity has been proven.

Access controls are important to restrict unauthorized access to directory information, but they may not provide sufficient protection. For instance, your agency may base access control decisions on the user's Distinguished Name in the directory request, allowing organizational users to list and read all the information in the directory. If a bad player can create a directory request containing a name that you trust, they can gain access to directory information. That request can come from anywhere on the Internet, so most organizations believe that it's a good idea to protect their directory from outside access by use of other techniques such as firewalls and Border DSAs.

Most LDAP servers implement an inherited access control model. When access controls are implemented on a container, any objects further down in the directory tree will typically inherit the higher-level access controls. As an example, if you apply a policy that any anonymous user can read objects in the top level of the directory, all objects within this entire directory tree will normally inherit this access control. It can be over-ridden further down the directory tree if needed. For instance, you might want to severely restrict access to a lower level of the directory. An access control statement applied to that container would over-ride the inherited access control definition set higher in the directory tree. Some LDAP servers ship with default access controls already defined, while others require you to define all access control information.

Replication brings another set of problems with regard to inherited access controls. Since inherited access controls flow downward from higher levels of the directory, some of the applicable access control information may not exist in the portion of the directory that is being replicated. The answer is generally to add additional replication agreements such that access control information is replicated in addition to the directory data. Some vendors have implemented product-specific methods of replicating this data.

B.4.3 Compartmentalization

Using X.500, it is possible to divide the agency directory into segments while organizing these segments into a logical agency DIT. The portions of the directory can be deployed on different network segments, separated by intelligent routers. For instance, if part of the directory tree contained public information, the directory server that held that portion might be located in the same network segment that holds the agency web server. If the directory server holding sensitive information is only to be accessible by agency users, it could be placed in the organizational network and routers configured such that directory traffic could not pass between the agency network and the Internet.

In the same manner, the "master" copy of the directory information could be held on a protected directory server located within a very secure network environment. Directory data can be updated by directory administrators operating within this secure network. When complete, the directory data would be replicated outward to servers operating in the lower assurance network. The main disadvantage to this architecture is that directory updates cannot be accomplished directly by end users. Requests for changes must be sent to the directory administrators, the updates accomplished, and the modified information replicated back outward to the production directory servers.

B.4.4 Encryption

If your agency is worried about interception of directory information traveling across the network, various forms of encryption can be employed. Not only can a bad actor discover information held by the directory, but they can also intercept information such as passwords, server network addresses, and chaining history (in X.500 requests) can be intercepted.

The original LDAP v3 specification lacks a definition of security services. To fill this gap, the Simple Authentication and Security Layer (SASL) was defined in RFC 2222. SASL is a method for adding authentication support to connection-based protocols such as LDAP. In a SASL-protected session, the

client issues an authentication command that includes a SASL mechanism name. Every SASL mechanism name must be registered with the Internet Assigned Numbers Authority (IANA), whose web site can be found at *http://www.iana.org*; RFC 2222 gives instructions for registering new authentication mechanisms with IANA. If the server supports the requested SASL mechanism, it initiates an *authentication protocol exchange* - a series of server challenges and client responses specific to that particular security mechanism. During this authentication protocol exchange, the client transmits the user's identity and negotiates for the use of a mechanism-specific security "layer".

The transmitted authorization identity may actually be different from the client's identity, to permit agents such as proxy servers to authenticate using their own credentials, followed by requesting access privileges belonging to the identity for which they are proxying. Once a security layer is requested / negotiated, it is used to protect all subsequent data sent between client and server.

Secure Socket Layers (SSL) and Transport Layer Security (TLS) are methods of encrypting information flowing between computer systems. SSL is the older of the two and is used extensively in securing access to sites on the World Wide Web. SSL encrypts the data carried within the "packets" flowing between the two computers. Any stream of information flowing across the Internet is actually busted into little chunks, called packets. These packets flow independently from the sending computer to the receiving computer. The receiving computer stores up the packets and re-assembles the data stream – all without the user's knowledge. The information carried in these packets for LDAP is text, and can easily be viewed by hardware and software tools known as "sniffers" – hence the term "packet-sniffing". SSL encrypts the information contained within the packets so that only the receiver can decode it.

TLS is a relatively recent standard, and as of this writing has not been implemented in a great many products. It provides similar functionality to SSL, but at the transport layer rather than the packet layer. In other words, the data stream itself is encrypted in TLS before being broken into packets, whereas SSL breaks up the data stream first and then encrypts each packet.

Both SSL and TLS allow mutual authentication using strong authentication, and can use X.509-based certificates issued by various commercial PKI systems.

B.4.5 Border and "Sacrificial" DSAs

A Border DSA is an application level firewall that typically sits just inside the corporate firewall, or possibly in a DMZ (demilitarized zone) network segment with your email and web servers. External directory requests are received by this DSA, which either returns information based on the DIT that it holds (usually a subset of your overall directory information), or perhaps chains the query inward. You can use just about any X.500 product to create an effective Border DSA for civilian government agencies. Simply replicate information into the Border DSA, and do not configure it to chain queries inward. It will enforce access control information on the replicated entries, and return any applicable information from the replica that it holds. The Border DSA should not master any part of the DIT.

Sacrificial DSAs are nearly the same as Border DSAs, except for two regards. First, they almost always exist outside the corporate firewall, albeit perhaps within a DMZ. Second, the data that they hold is usually refreshed on a regular basis, sometimes by a proprietary method (such as via FTP or an LDIF update). A Sacrificial DSA will normally assume that all requests are anonymous, and will not hold any information of a sensitive nature. If the Sacrificial DSA is attacked, it holds no sensitive information that would be of use to the attacker. Because its data replication is one-way and it doesn't support chaining, a Sacrificial DSA provides no additional information that could be used to compromise the corporate directory service.

Border and Sacrificial DSAs typically contain only that subset of the information in the protected directory that is considered public information. This subset is extracted via various means from the protected directory and populated onto the border/sacrificial directory. The intent is to provide a layer of

protection that prevents disclosure of the non-public information. If the border/sacrificial directory is compromised, the attacker can only discover the public information. If there is no direct connection back to the internal directory for the attacker to follow in order to gain access to the protected directory's full content.

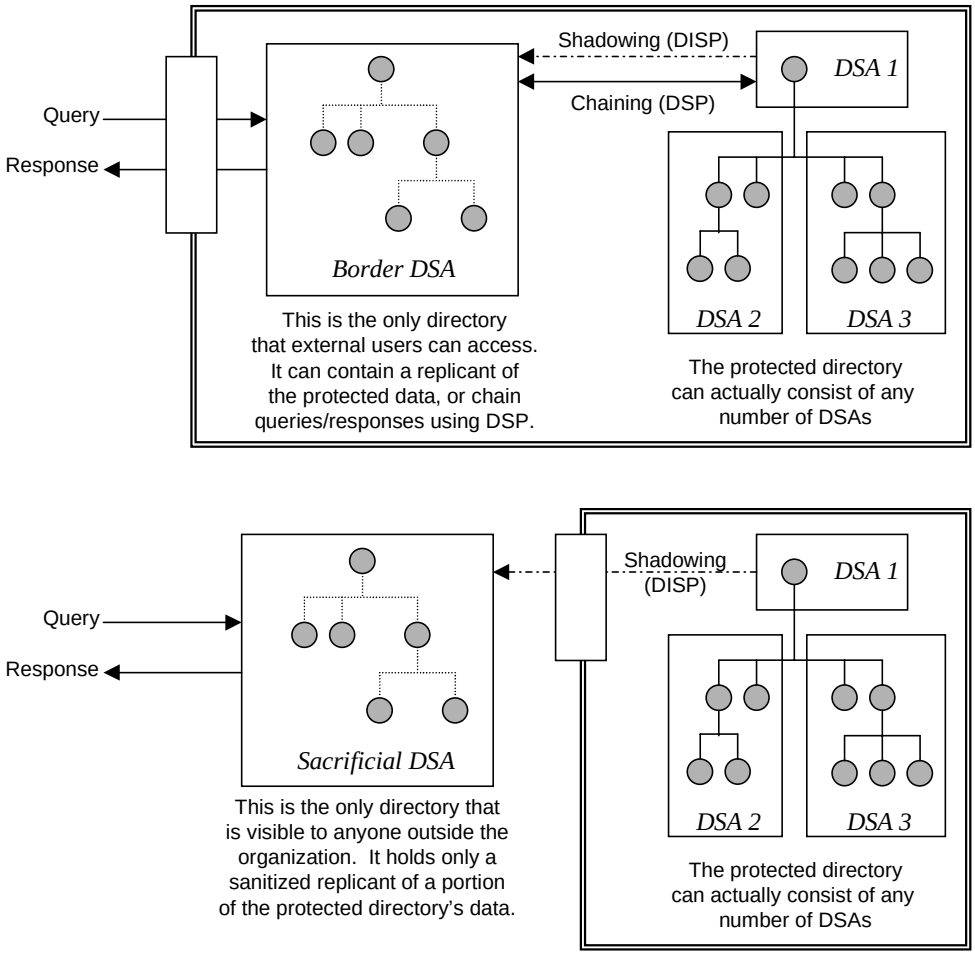


Figure B-1. Border and Sacrificial DSAs

B.4.6 LDAP Reverse Proxies

LDAP presents significant challenges when securing the corporate network, because it does not (yet) implement any sort of chaining. Users from all over the world expect to be able to directly contact your LDAP-based directory. If that directory exists within your corporate network, you will have to open your firewalls to allow this access. Most firewalls are not able to act as an application-level LDAP gateway. The only thing you could do to restrict access is to deny connectivity to all systems inside your organization except the LDAP server, and restrict access such that only LDAP operations and results can be passed between the LDAP server and users across the Internet. However, this configuration is still extremely worrisome to most security administrators, especially since most external LDAP access will be anonymous.

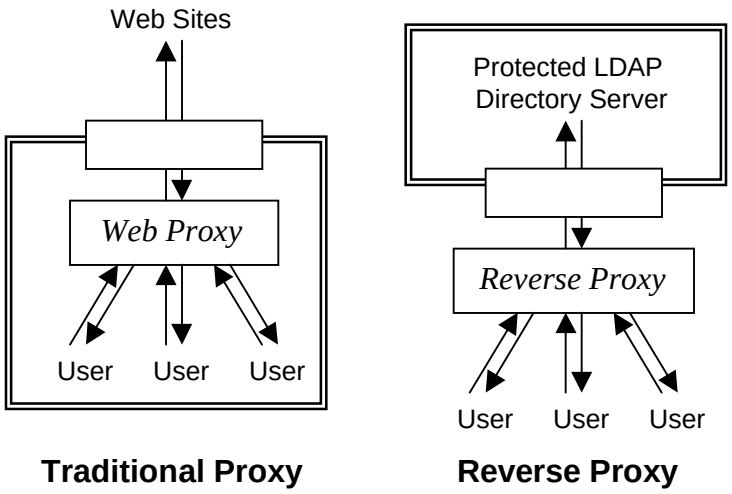


Figure B-2. Traditional and Reverse Proxy Servers

A new technology, the *reverse proxy server*, addresses a great deal of the security concern regarding LDAP in this type of environment. For a traditional service like Web access, a proxy server is deployed inside the corporate firewall. Users are not allowed to access the Internet, but they *can* connect to the proxy server. The proxy server is allowed to connect to Web servers outside the corporate networks *on behalf of* the user. Responses come back to the proxy server, which then forwards them to the appropriate user. A reverse proxy, like the iPlanet Directory Access Router (IDAR), places the proxy server backwards, outside the corporate firewall. Any user from the Internet can connect to the server. A single hole through the corporate firewall allows the reverse proxy to connect to the corporate LDAP server to send LDAP operation requests and receive results on behalf of the originating user.

APPENDIX C – FBCA CONNECTIVITY DIAGRAMS

Agency PKI Certificate Authorities will issue certificates to users within the agency. Revocation information will be contained in Certificate Revocation Lists (CRLs) that are also maintained within the agency. The FBCA Directory provides the connectivity needed for users outside the agencies to find the agency's CRLs, in order to determine whether agency-issued certificates are still valid. It also provides the connectivity needed to find the CA certificates needed to construct trust paths between the relying party and your agency's PKI.

The following diagrams discuss the methods by an agencies can connect with the Federal Bridge Certification Authority and the Federal PKI system. Functionality provided to both internal and external PKI users is discussed, along with any suggested restrictions or suggested enhancements. This Appendix is divided into two sections – Directory Services (C.1) and Directory Users (C.2). Agencies wishing to connect to the Federal Directory Service should consult both sections in order to determine the best method of establishing connectivity and providing full access to their user communities.

C.1 Directory Services

The Federal Bridge directory supports connectivity with X.500-based directory services using the Directory Services Protocol (DSP). Agency directories connected in this manner can perform chained operations with the Bridge directory. Alternately, for agencies with non-X.500 directory services, the Bridge directory can provide LDAP v3 referrals to the agency's LDAP directory server. Both types of connectivity are shown in Figure C-1.

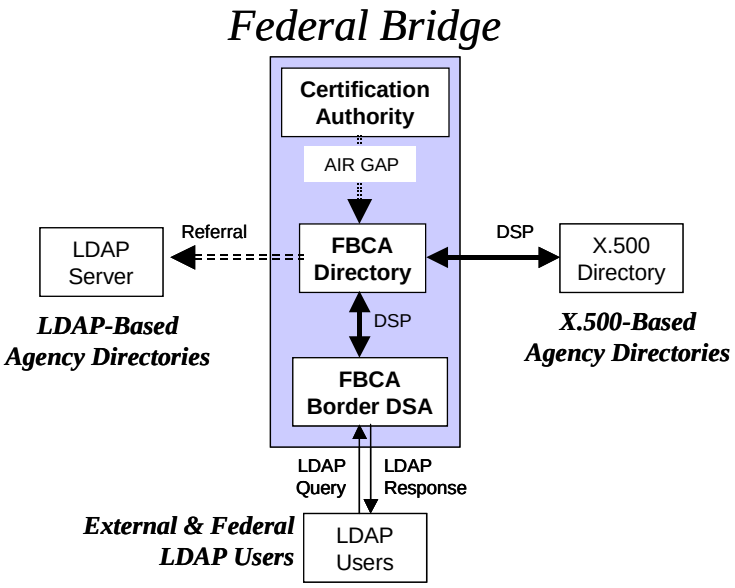


Figure C-1. Basic FBCA Directory Connectivity

C.1.1 Agencies with X.500 Directories

Agencies with X.500 directories can connect directly to the Federal Bridge DSA using the Directory Services Protocol (DSP) as in Figure C-1, above. User queries are *chained* from the agency's X.500 directory to the FBCA DSA. Normally, the FBCA DSA will not contain the needed information, but rather will chain the request onward to the particular agency DSA that does hold the needed information (called the *performing DSA*). The answer is then chained back to the agency DSA (called the *originating DSA*). Chained directory operations such as this are completely invisible to the user.

If the requested information is held in an LDAP server, the FBCA DSA will only be able to return a referral to that LDAP server. The referral is chained back to the originating DSA, which returns it to the user. The user agent would then contact the referenced LDAP server and request the information again.

C.1.2 Agencies with LDAP Directory Servers

The majority of Federal agencies will have implemented an LDAP-based directory service. Agencies with LDAP-based directory services do not "connect to" the FBCA DSA in the same sense as X.500 directories. Rather, connection information for these directories will be stored in the FBCA DSA in the form of LDAP v3 referrals. When users request information held by within these directories, the FBCA DSA returns the referral to the requestor, either directly if the user contacts the FBCA directly, or within an X.500 chained response via DSP.

C.1.3 Agencies with X.500 Border DSAs

Many agencies implement Border DSAs, in order to insulate protected internal directory servers from outside access and attack. Typically, the Border DSA will permit queries by internal users to the outside world and will allow responses to those queries to pass back through it. However, queries from outside the agency will be blocked by the Border DSA. It could be configured to allow access to a very small set of information that is deemed public, but block queries to everything else. Border DSAs usually hide all information about the directory services they are protecting, so that attackers can't gain information like network addresses or types of systems and software deployed.

If an agency has implemented an X.500 DSA as a border DSA, that DSA can be connected to the FBCA DSA via DSP just as any other X.500 DSA. Figure C-2 illustrates this connectivity. Note that it doesn't matter where the information is held, so long as the agency's Border DSA can provide it to requestors via X.500 DSP chained operations. Agencies can even replicate information from proprietary sources into a Border DSA, which would then service requests chained from the FBCA DSA.

The security policy implemented by the Border DSA must allow external users to "find" your agency's CRLs and CA certificates. Either it must allow access to those items by external user queries, or it must hold a replica of those items. Each Border DSA product will provide slightly different functionality, so offering specific implementation guidance is outside the scope of this document.

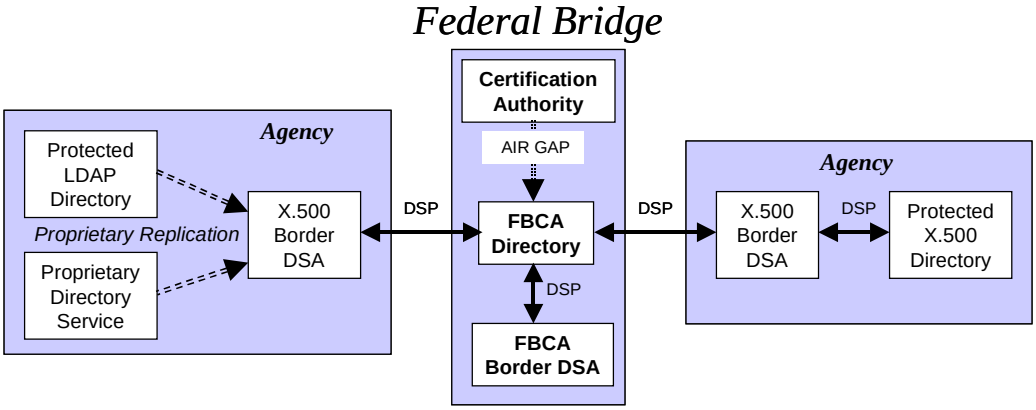


Figure C-2. Connecting an X.500 Border DSA to the FBCA

C.1.4 Agencies with X.500 Sacrificial DSAs

Some agencies do not allow *any* inbound access to their internal directory services. Such agencies may operate a "sacrificial" DSA in order to provide publicly accessible directory information without jeopardizing their internal directory services. This sacrificial DSA is usually a Border DSA that is located

outside of the agency firewalls (or in a "no-man's land") and is accessible to the general public. It only holds a copy of the subset of the agency's directory information that is public information. If it is subverted, its information can quickly be refreshed. Since the information in the sacrificial DSA is the only version available to external users, it should be updated regularly and monitored often in order to ensure that it hasn't been compromised.

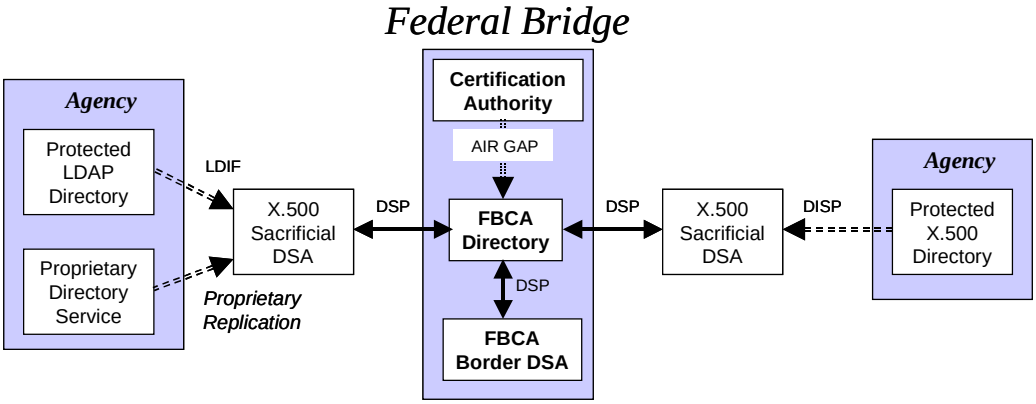


Figure C-3. Connecting a Sacrificial X.500 DSA to the FBCA

All PKI information required to validate agency digital signatures must be pushed outward into the sacrificial DSA on a timely basis. External users will obtain the needed information from the sacrificial DSA rather than the protected directory services.

Agency information can be replicated into the Sacrificial DSA via whatever means or protocol is available; e.g. X.500 Directory Information Shadowing Protocol (DISP), LDAP Lightweight Directory Interchange Format (LDIF), or other proprietary means. Since this replication process is invisible to the Bridge, it is outside the scope of this document.

C.1.5 Agencies with External LDAP Directory Servers

Agencies with LDAP-based directory servers may choose to set up external LDAP servers in order to restrict access to internal agency directory services. This type configuration is shown in Figure C-4, below. As noted in C.1.2, above, LDAP Servers do not connect to the FBCA DSA directly. Rather, knowledge references are provided to the Bridge, which holds LDAP v3 referrals to the directory service. When information is requested that is held by the agency's external LDAP server, the Bridge DSA returns the LDAP v3 referral that references the external server.

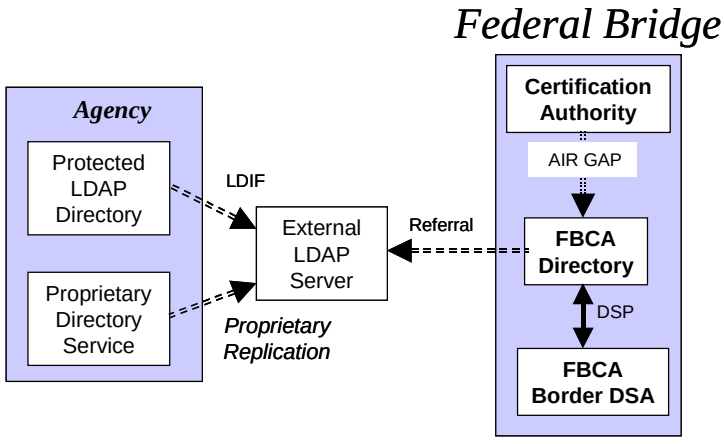


Figure C-4. Using an Agency External LDAP Server with the FBCA

All PKI information required to validate agency digital signatures must be pushed outward into the agency's External LDAP Server on a timely basis. External users will obtain the needed information from the External LDAP Server rather than the protected agency directory services.

Agency information can be replicated into the External LDAP server via whatever means or protocol is available; e.g., LDAP Lightweight Directory Interchange Format (LDIF) or other proprietary means. Since this replication process is invisible to the Bridge, it is outside the scope of this document.

C.1.6 Agencies with Reverse Proxy Servers

A few vendors provide reverse proxy servers, which appear to users as an External LDAP Server. However, information is not replicated outward onto an external server. Rather, the Reverse Proxy Server "funnels" all external LDAP requests together, so that they appear (to the internal protected directory) to be coming from one, single user. The advantage is that firewalls can be configured to disallow LDAP queries and responses except between the Proxy Server and the protected internal directory. This arrangement removes the complexity of maintaining replication between the protected directory and an external LDAP server. Information such as certificates and CRLS are immediately available to relying parties outside the agency, because the Proxy Server allows real-time access to this information, whereas replication is normally performed on a periodic basis.

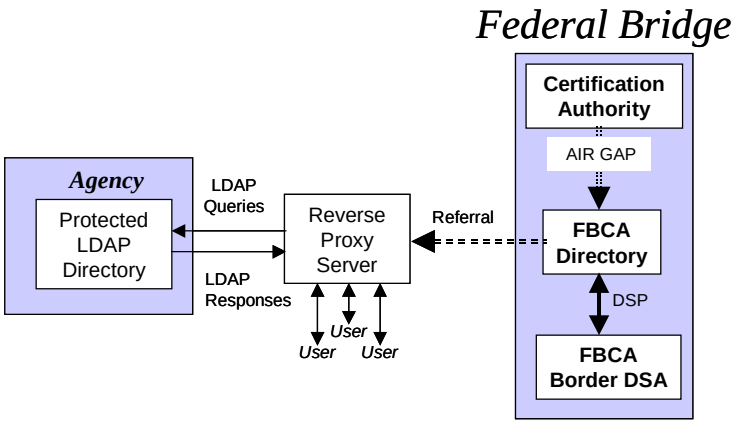


Figure C-5. Using a Reverse Proxy Server with the FBCA

From the view of the FBCA, the Reverse Proxy Server is simply another LDAP server. The FBCA DSA will maintain LDAP v3 referrals to the Proxy Server, and provide them to users requesting information from that agency.

C.2 Directory Users

The following sections describe how relying users will obtain needed information from the Federal PKI Directory Services, including certificates and CRLs needed to validate digital signatures created with certificates issued by an agency.

C.2.1 X.500 DAP Users

There are few, if any, user agents that use the X.500 Directory Access Protocol (DAP). It is very unlikely that any such user agents will have the ability to construct trust paths with the information provided by the FBCA. Therefore, such user agents are considered to be outside the scope of this document, unless otherwise requested by agencies that have deployed X.500 DAP user agents with this capability.

C.2.2 X.500 LDAP Users

Most, if not all, X.500 directory products allow users to connect to the directory service via LDAP. This allows any LDAP-aware user agent to access the information held in the X.500 directory. This arrangement is depicted in Figure C-6.

Most products convert the user's LDAP query into X.500 and route it onward using DSP. X.500 directories that receive the query via DSP are not aware that the original request was made via LDAP. If the directory containing the requested information is another X.500 directory, the query is chained to the performing DSA via DSP, and the response is chained back to the originating DSA which converts it to an LDAP response.

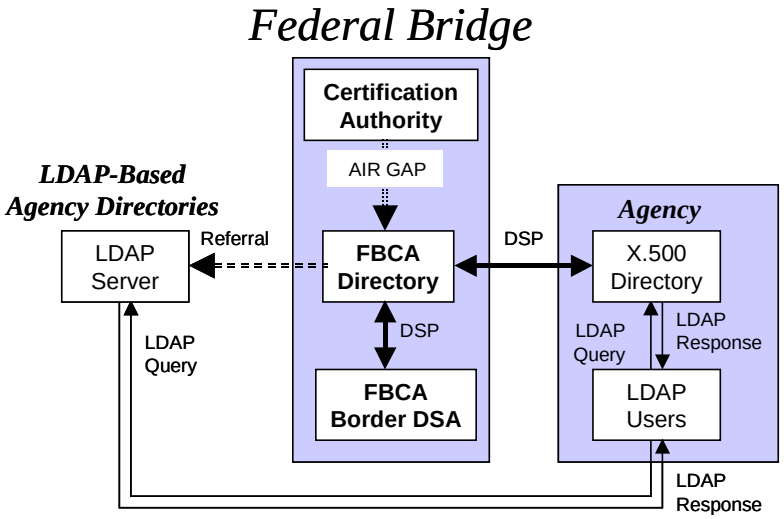


Figure C-6. LDAP User Agents within an Agency with X.500 Directory Service

However, if the directory holding the requested information is an LDAP server, the FBCA directory will return an LDAP v3 referral. It is the responsibility of the originating X.500 DSA to provide the referral to the user agent, which will follow the referral – connecting to the agency LDAP server that holds the needed information.

It is presumed that the originating DSA can correctly convert the referral and provide it to the user agent, and it is also presumed that the user agent can follow LDAP v3 referrals. If either is not the case, the user will not be able to find the information needed to validate digital signatures.

C.2.3 X.500 LDAP Users with LDAP Proxy

Some agencies with X.500-based directories may have difficulties with the above architecture, in that they do not allow their users to freely access the Internet. In this case, it would be impossible for users to follow LDAP referrals. An LDAP Proxy, as illustrated in Figure C-7 below, can provide the needed functionality.

When the user agent receives an LDAP v3 referral, it will be redirected to the LDAP Proxy that will make the request on the user's behalf. The response will be received by the Proxy, and forwarded to the user. In this manner, the firewalls that protect the agency's network from unauthorized access (both inward and outward) must only be configured to allow LDAP queries and responses from and to the LDAP Proxy.

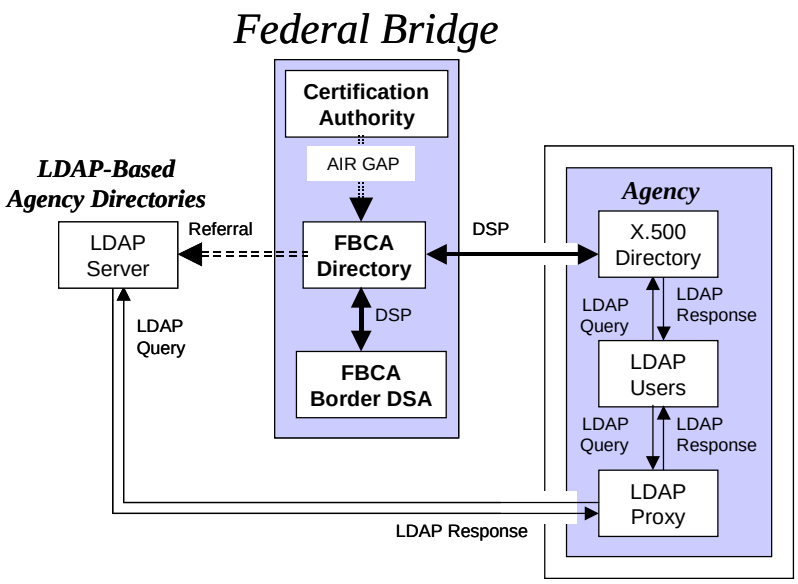


Figure C-7. LDAP User Agents and Proxy with X.500 Directory Service

C.2.4 LDAP Server

When a directory user requests information that is not held by their agency's LDAP-based directory service, they will receive an LDAP v3 referral to the FBCA Border DSA (1). They will then connect to the FBCA Border DSA using LDAP, and make the same request (2).

If the directory service containing the desired information is an X.500-based directory, the user's query is converted to DSP and chained onward to the performing DSA. The response is chained back, and converted back into an LDAP response that is provided to the requesting user.

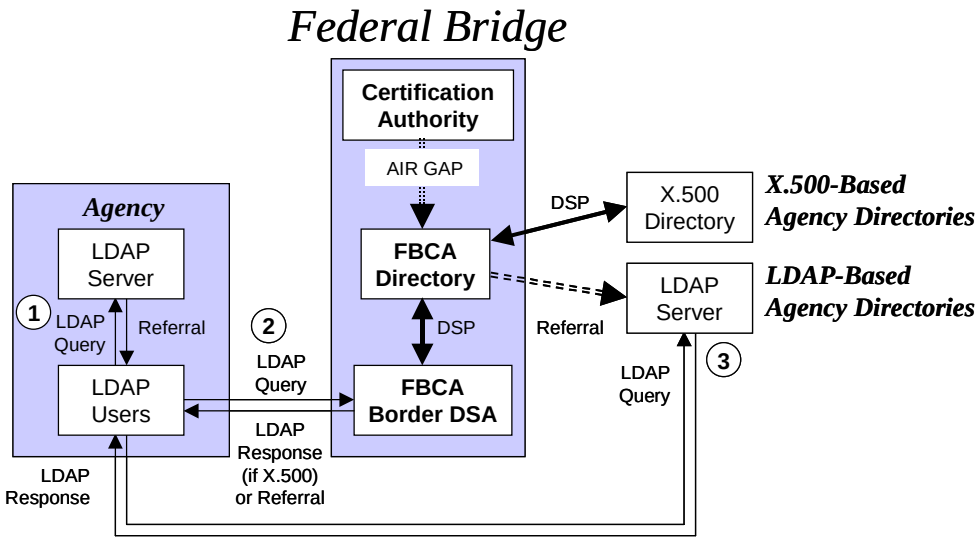


Figure C-8. LDAP User Agents with LDAP-Based Agency Directory Service

However, if the agency directory containing the needed information is an LDAP server, the FBCA Border DSA will return another LDAP v3 referral to the user agent. It will then connect to the target agency's LDAP server (3) and request the needed information.

C.2.5 LDAP Server and Border X.500 DSA

A few agencies with LDAP-based directory services have considered putting up an X.500-based Border DSA in order to facilitate connectivity with the Federal Bridge and other agencies, as shown in Figure C-9, below. Although this arrangement facilitates interoperability with agencies that have X.500 directory services, it has significant limitations that must be considered by an agency.

If the agency's LDAP server does not contain the requested information, it should return a referral (1) to the agency's Border DSA (which would also support LDAP inquiries from internal users). The Border DSA will then chain the query to the FBCA DSA (2). If the target directory that holds the requested information is an X.500 directory, the query will be chained onward to the performing DSA, the response will be chained back to the Border DSA, and it will be converted into an LDAP response.

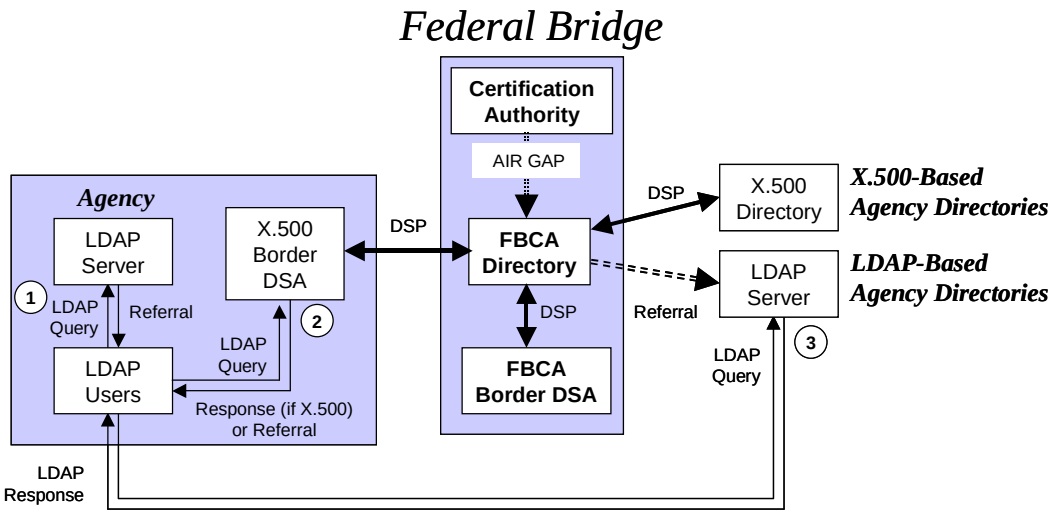


Figure C-9. LDAP User Agents with LDAP Server and X.500 Border DSA

However, if the target directory service is another LDAP server, the FBCA will return an LDAP v3 referral. In order to obtain the needed information, the LDAP user agent must connect to the referenced LDAP server and repeat the request (3). This means that the users must be allowed access to the Internet in order to follow this last referral, and that would probably be viewed as circumventing the security for which the Border DSA was employed in the first place.

C.2.6 LDAP Server and LDAP Proxy

An LDAP Proxy can solve the problems noted in C.2.5, above. When the user requests information not held by the agency's LDAP server, they receive a referral to their agency's LDAP Proxy (1). They connect to the LDAP Proxy and request the information (2). The LDAP Proxy connects to the FBCA Border DSA and makes the request on behalf of the user (3). If the target agency has an X.500-based directory service, the query is converted to X.500 DSP and chained to the performing DSA, the response is chained back, converted to LDAP and returned to the LDAP Proxy (which returns it to the user). If the target agency has an LDAP-based directory, the FBCA DSA returns a referral (4), and the LDAP Proxy follows the referral to make the request of the target directory.

Referring back to Figure C-8, consider the case where an LDAP user agent may not be able to follow LDAP v3 referrals. Although some commercial products are able to follow referrals, many products already deployed do not yet have this capability. In this case, the LDAP v3 referral returned by the agency's LDAP server or the FBCA would be completely useless.

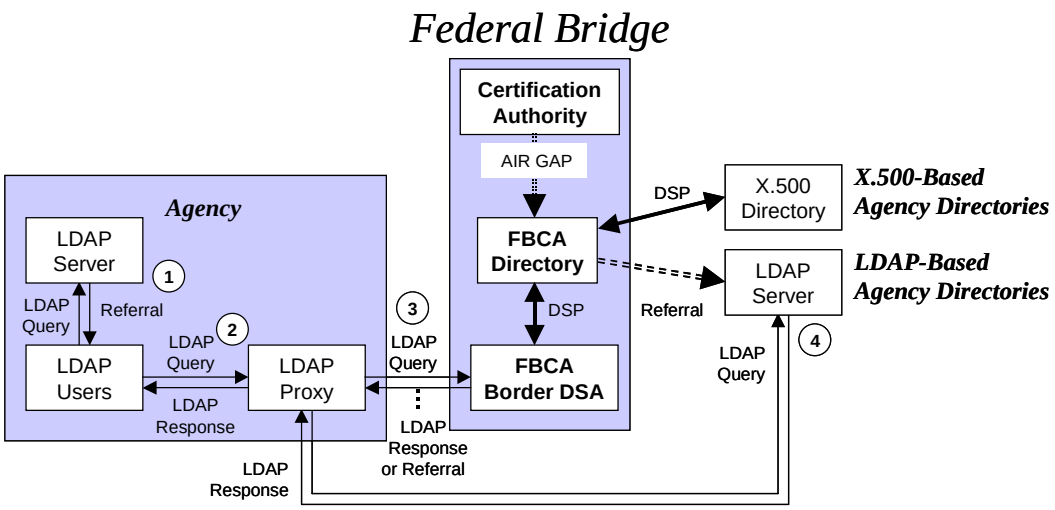


Figure C-10. LDAP User Agents with LDAP Server and LDAP Proxy

The LDAP Proxy solution solves this problem fairly neatly, assuming that it is capable of following LDAP v3 referrals. In this situation, the LDAP user agent would be configured with the agency's LDAP Server as the primary server, but with the LDAP Proxy as the only alternate. When the answer is not provided by the agency's LDAP Server, the User Agent would fall back to request the same information from the LDAP Proxy. The LDAP Proxy would handle all transactions from that point, and simply provide the requested information back to the user when found.

C.3 Suggested Configurations

The following diagrams illustrate recommended configurations for agencies with X.500 based directory services and LDAP based directory services. These configurations provide the best functionality for both directory service interoperability and user function, and also provide good security and protection of the agency's internal directory services.

C.3.1 Agency with X.500 Directory Service (high-security version)

Figure C-11, below, shows a recommended high-security configuration for agencies that have X.500-based directory services. This configuration features both a sacrificial DSA and an LDAP Proxy. Users within the agency are presumed to be using LDAP-enabled user agents, not X.500 DAP, to access the internal directory service.

Information that is deemed to be public is pushed outward from the protected agency directory to the sacrificial X.500 DSA, which is probably located in a demilitarized zone. The sacrificial DSA handles all outside requests for information, either via X.500 DSP or direct connection by external LDAP users. Since a replica of the approved subset of information is held within the sacrificial DSA, no directory requests are passed inward to the protected agency directory service.

If the agency's X.500 directory does not contain the information requested by an agency user, it returns a referral to the FBCA Border DSA. The user agent connects to the LDAP Proxy, which in turn requests the information from the FBCA Border DSA on behalf of the user.

If the target directory is X.500, the query is converted to X.500 and chained to the performing DSA, the response is chained back to the FBCA Border DSA, converted into and LDAP response, and returned to the user. If the target directory is an LDAP Server, the FBCA returns an LDAP v3 referral, the LDAP Proxy follows the referral to the target LDAP directory, and the response is sent back to the requesting user.

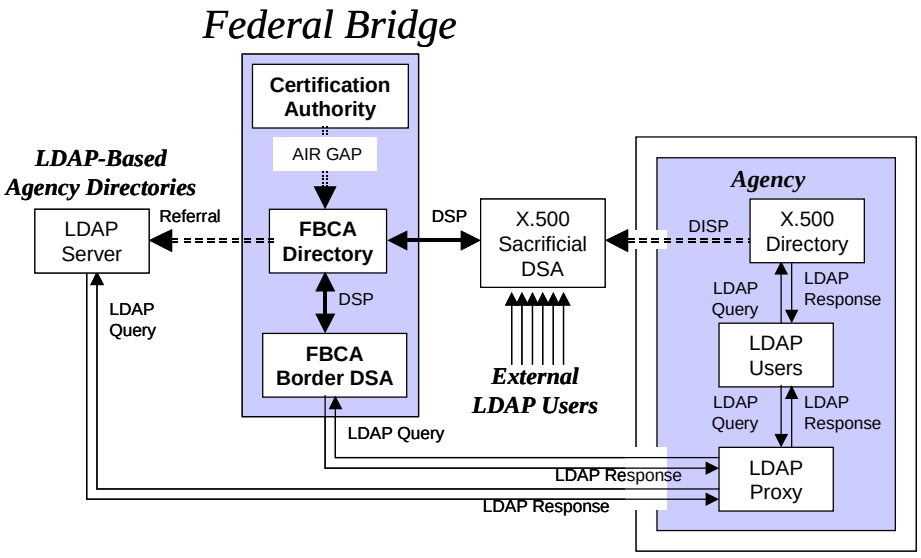


Figure C-11. Suggested High-Security Connectivity for X.500 Directory Services

C.3.2 Agency with X.500 Directory Service (medium security)

Figure C-12 shows a recommended medium-security configuration for agencies that have X.500-based directory services. This configuration features both a Border X.500 DSA and an LDAP Proxy.

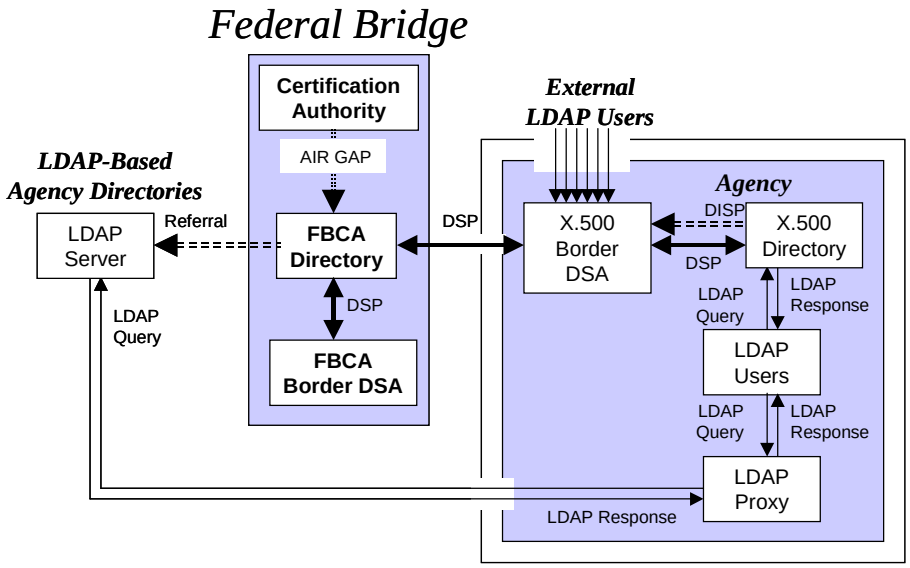


Figure C-12. Suggested Medium-Security Connectivity for X.500 Directory Services

A Border DSA within the agency (or within a "no-man's land") provides X.500 connectivity to the outside world for agency users. It also contains a replica of information that is deemed to be public. The Border DSA responds to DSP queries from outside the agency, but does not chain requests onward to the protected agency directory service. It may also handle LDAP requests from outside users.

If the agency's X.500 directory does not contain the information requested by an agency user, the Border DSA will chain the request to the FBCA DSA. If the target directory is X.500 based, the query will be chained to the performing DSA and the response will be chained back to the originating agency DSA.

However, if the target directory is an LDAP server, an LDAP v3 referral will be returned. At that point, the LDAP user agent will connect to the LDAP Proxy as in C.3.1 above. The LDAP Proxy will connect to the target LDAP Server, make the query on behalf of the user, and return the answer to the user.

C.3.2 Agency with LDAP Directory Service

Figure C-13 shows a recommended configuration for interoperability between an agency with an LDAP-based directory service and the Federal Bridge. It features a Sacrificial LDAP Server to handle queries from outside the agency, and an LDAP Proxy Server to allow internal users access to other agency LDAP servers without exposing the protected agency networks.

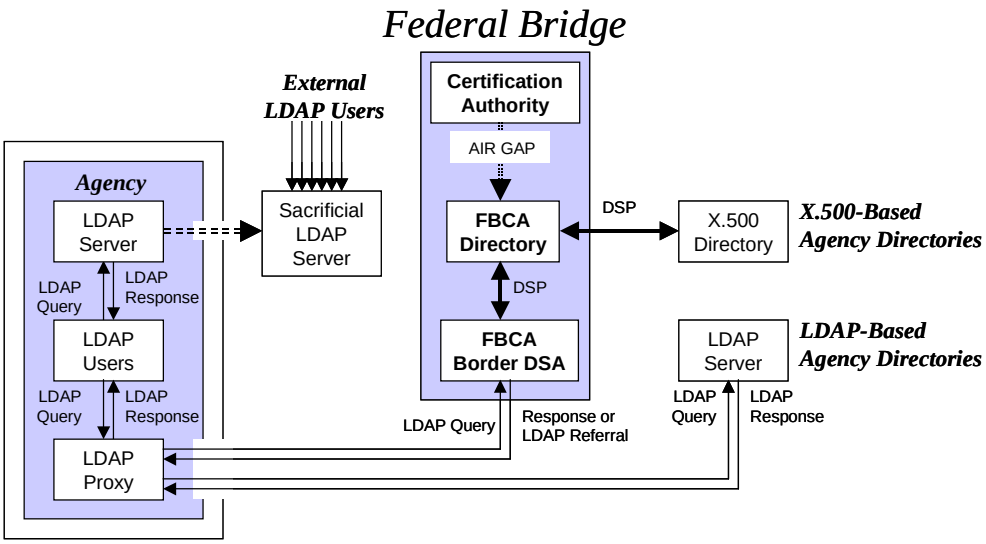


Figure C-13. Suggested Connectivity for Agency with LDAP Directory Servers

A Sacrificial LDAP Server outside the agency's protected networks (or within a "no-man's land") contains a replica of information that is deemed to be public. The Sacrificial LDAP Server handles LDAP requests from external users, without allowing those external users to access protected agency directory servers.

If the agency's directory service does not contain the information requested by an agency user, it returns an LDAP v3 referral to the FBCA Border DSA. The user agent connects to the LDAP Proxy, which in turn requests the information from the FBCA Border DSA on behalf of the user.

If the target directory is X.500, the query is converted to X.500 and chained to the performing DSA, the response is chained back to the FBCA Border DSA, converted into and LDAP response, and returned to the user. If the target directory is an LDAP Server, the FBCA returns an LDAP v3 referral, the LDAP Proxy follows the referral to the target LDAP directory, and the response is sent back to the requesting user.

It would also be possible to replace the LDAP Sacrificial DSA with a LDAP Reverse Proxy Server, described earlier.

C.4 Security Implications

For the directory architectures shown above, all queries from outside the agency should be considered to be anonymous. Even though X.500 DSP queries contain the identity (distinguished name) of the requestor, it is not possible to prove that identity given the wide variety of products and directory server configurations in use by different Federal agencies and the private sector.

The Federal PKI directory service does not require "strong authentication" of directory requests (which could provide a digital signature by which the requestor's identity could be proven). In the vast majority of instances, the original directory request will have been submitted via the LDAP protocol, which has a slightly different security mechanism than X.500. Since most accesses to agency information will be via LDAP, one cannot count on the assurance of the user's identity.

In an X.500 query, the user's identity is recorded in the directory request and accompanies the request as it is chained throughout a distributed directory service. LDAP queries don't provide this information because the user's identity is validated when they first bind to the LDAP directory, and LDAP does not provide for chained operation between directory servers. This is not a problem when an LDAP user connects to the FBCA Border Directory, because they provide their identity at that time.

However, when a user binds to an X.500 directory service using LDAP they are actually binding to an LDAP gateway that converts their LDAP queries into X.500, and converts the X.500 responses back into LDAP. If this gateway is constructed properly, it will remember the user's identity and place it into the X.500 queries in order to be used by performing DSAs. X.500-style access controls use the identity of the requestor in order to determine whether the requested operation should be allowed.

Most directory services do not require any sort of cryptographic proof of identity when the user binds to the directory service. It is possible that the application forming the request could have been subverted, or that the identity of the requestor could have been changed (or perhaps not even initially created correctly). Therefore, all directory requests from outside of your agency should be treated as anonymous. At a minimum, appropriate access controls should be implemented to restrict access by users outside of your agency. However, since (as noted) it is not possible to completely trust the identity expressed in directory requests, it would be prudent to examine your agency's security posture with regard to directory-based information. You may need to implement a Border DSA or sacrificial DSA in order to protect sensitive agency-based information from unauthorized disclosure.

C.5 A Note About Appropriate Directory Usage

The Federal Directory service described in this document is primarily being implemented as part of the Federal Bridge Certification Authority, in order to promote interoperability of Federal PKI credentials. To this end, it presumes two things about "normal" usage of the Federal Directory:

- Applications will perform directory queries on behalf of users. The FBCA Directory is not designed to handle interactive browsing by directory users. The FBCA Directory is able to provide LDAP referrals to other LDAP directory servers, but users will not connect to the FBCA Directory in order to chain interactive queries to other agency directory services.

- The FBCA facilitates validation of digital signatures created by PKI certificates issued by other agencies. In allows PKI-enabled applications to find the certificates and CRLs needed to construct trust paths between agencies and ascertain that the signing certificate is still valid. It is not designed to provide encryption certificates or support any other sort of interactive use. The CA Certificate and CRL information for each agency should consist of only a few directory entries, whereas an agency might issue tens of thousands of encryption certificates. If relying users wish to obtain encryption certificates or other personal information, they must contact the issuing agency's directory service directly or obtain the certificates by some other means.

C.6 DOD Connectivity and Interoperability

The US Department of Defense has a more complicated directory services architecture than noted in the above diagrams. Each Service operates their own directory service, and these directory services send updated information to the DISA Global Directory Service (GDS). When a user or application cannot find required information in their Service's directory service, they request it from the GDS. This supports

interoperability between the Services within DoD, but does not provide for interoperability with other Federal agencies and the private sector. Most of the directory products used by the Services are LDAP-based, but a few have deployed X.500-based directories. To make matters more complicated, PKI certificates and CRLs will be issued by the Key Management Initiative (KMI) for all of DoD, rather than by each Service. Methods of connecting all of these into the Federal Bridge are described below, not only as guidance for DoD Services, but also to provide ideas that might be useful when connecting large agencies with many separate organizational units, departments, bureaus, modes, or branches (the exact terminology varies from agency to agency).

C.6.1 Connecting the DoD GDS to the Federal Bridge

DISA is planning to implement a Border DSA, which will connect to the FBCA Directory using the X.500 DSP protocol. Information from Service directories is replicated into the DISA GDS so that it becomes available to other Services. PKI information held within the GDS will be replicated to the GDS Border DSA, as needed. Users outside of the DoD will only see information that has been replicated into the GDS Border DSA.

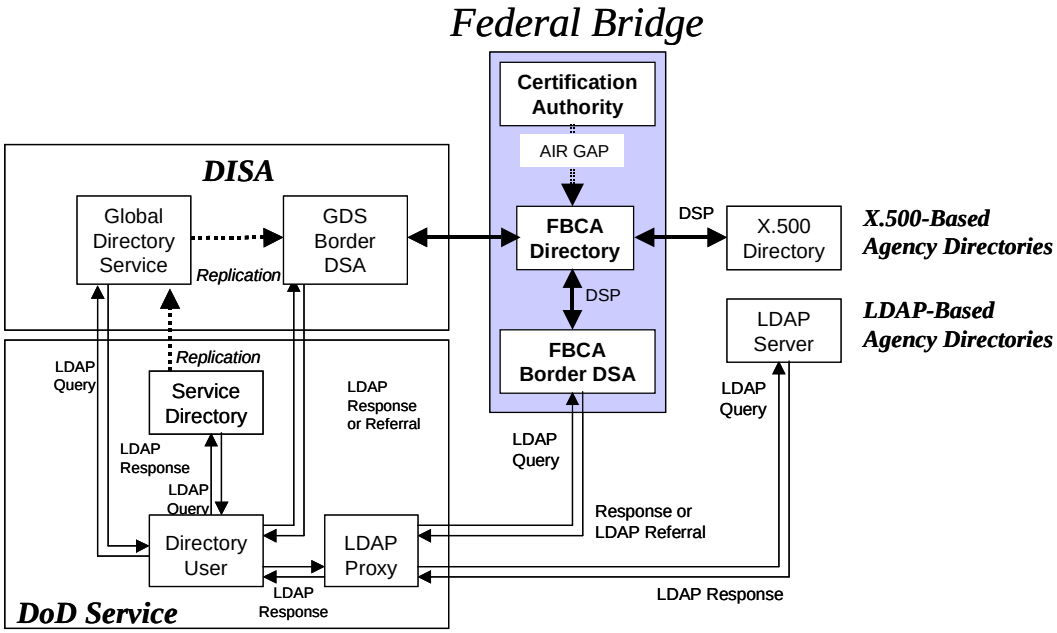


Figure C-14. Connection of the DISA GDS to Federal Directory

Service users will first contact their own Service Directory. If the data requested doesn't exist within the Service Directory, there are variations as to what might occur next.

- The user's application may connect to the DISA GDS and request the information. If it doesn't exist in the GDS, a referral would be returned to the user.
- If the user's application can determine that the GDS will not contain the information, it may connect to the GDS Border DSA and request the information. The Border DSA would chain the request to the Bridge directory.

Each service will have their own policy dictating whether and how users can connect to the Internet. One suggested approach is to deploy an LDAP Proxy to control user access to the Internet. Firewall policies may further restrict access, but should at the very least allow LDAP communications to and from the Service's LDAP Proxy Server.

If the user's query cannot be satisfied by the GDS or GDS Border DSA, the user will receive a referral and would then make the request of the FBCA Border DSA. The FBCA Border DSA will likely receive

a referral and would follow the referral to the target agency LDAP directory, request the needed information on behalf of the user, and return the response to the user.

Services that have already implemented X.500 directories can establish DSP connectivity between their internal directory service (or Border DSA) and the FBCA Directory. Queries for information not held in their Service Directory would automatically be chained to the FBCA Directory for resolution. This would be invisible to the user, and would not require any modification or configuration of user agents and applications. Again, if the target directory were an LDAP Server, the FBCA Directory would chain back a response that contained a query to the appropriate directory. The user agent would follow the referral, as outlined above.

C.6.2 Connecting the DoD KMI to the Federal Bridge

Currently, it is planned that the KMI will include an X.500 directory server in order to facilitate interoperability with DoD Services and agencies. Key materials and certificates generated by the KMI will be posted to this KMI Directory, which will forward them to the GDS. At this time, it is unclear whether the KMI directory will allow DSP connectivity with the FBCA Directory (as shown in Figure C-7, below). If not, then external users will access the information held within the GDS Border DSA (as shown in figure C-6, above).

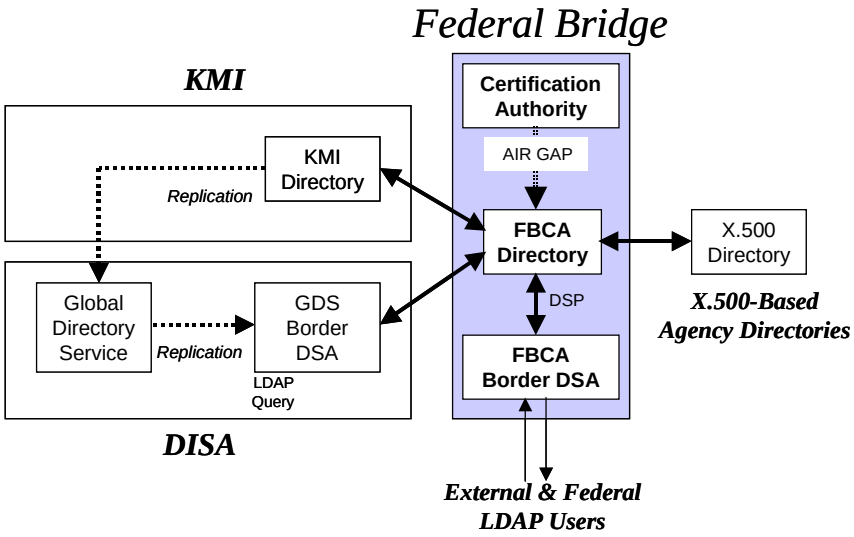


Figure C-15. Connection of the DISA KMI to Federal Directory

If the KMI establishes direct X.500 DSP connectivity with the FBCA Directory, it is expected that KMI will deploy an X.500-based Border DSA between itself and the Bridge.

C.7 A Few Words About MetaConnectors

Earlier drafts of this document contained information about X.500 “metaconnectors”. These are essentially reverse LDAP gateways. Instead of converting LDAP requests into DAP queries, they convert DSP queries into LDAP requests. Their purpose in life is to connect established X.500 directory services to various LDAP “islands” that might exist in a large corporation. However, it is unclear whether X.500 vendors can currently supply robust versions of this technology, or even whether the technology will be commercially viable and supportable in the future. Therefore, a consensus to remove this technology was reached by the Federal PKI Technical Working Group. The main functionality of such a product would be to allow X.500-based agency directories to retrieve information from LDAP servers, rather than forcing the user applications to follow referrals in order to obtain the needed information.

APPENDIX D – CONNECTING TO THE FBCA DIRECTORY

This section briefly describes the steps that an organization must complete in order to connect to: the Federal Bridge Certification Authority (FBCA or "Bridge").

D.1 Overview

The Federal Bridge CA (FBCA) is operated by the Federal Bridge CA Operational Authority (FBCA OA) under the guidance and oversight of the Federal PKI Policy Authority (FPKI PA). The FBCA facilitates trust between your organization and other organizations by providing a certification path between your PKI and other government PKIs. This path is created by issuing cross-certificates between your organization and the FBCA, and connecting your organization's directory service to the FBCA's directory. This allows your PKI-aware applications to verify digital signatures created by certificates issued by other organizations, and to verify that those certificates are still valid (and haven't been revoked). Obviously, your organization must already have an operational PKI in order to make use of the Bridge.

D.2 Where to find additional information and assistance

Information on the Bridge, including the most current version of this Getting Started guide, will be found at *http://www.cio.gov/fbca*. Information on the FPKI Policy Authority will be found at *http://www.cio.gov/fpkipa*. Information on the FPKI Steering Committee will be found at *http://www.cio.gov/fpkisc*. Information on Internet standards can be found at *http://www.ietf.org*. A glossary of common security terms used in this and related documents can be found in RFC 2828 [1] (below).

D.3 Documents

You will need the following documents, all of which are available on-line.

[1] Shirey, R. RFC 2828: Internet Security Glossary (May 2000). [Online] http://www.ietf.org/rfc/rfc2828.txt

[2] Federal PKI Policy Authority. X.509 Certificate Policy for the Federal Bridge Certification Authority (14 Jun 2001). [Online] http://www.cio.gov/fpkisc/ documents/fbca_cp_06-14-01.pdf

[3] Chokhani, S. RFC 2527: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (March 1999). [Online] http://www.ietf.org/ rfc/rfc2527.txt

[4] Federal PKI Policy Authority. Application for Interoperability with the Federal Bridge Certification Authority (TBD). [Online] http://www.cio.gov/fbca/docs/Application.doc.

[5] Federal PKI Steering Committee. Federal PKI Directory Profile (TBD). [Online] http://www.cio.gov/fbca/docs/DirectoryProfile.doc.

D.4 How to get connected to the Federal Bridge CA

Your organization must complete the following steps before your PKI can be interconnected to the FBCA.

1. Create an Agency Certificate Policy (CP) – Your organization's formal Certificate Policy (CP) must be included in your *Application for Interoperability* [4] (see “Documents”, above) with the Bridge. If you have an existing CP, you should review it for equivalence with the Bridge CP [2]. Your application must describe how the assurance levels in your CP map to those provided by the

Bridge. General guidance for creating a Certificate Policy and Certification Practices Statements can be found in RFC 2527 [3].

2. Create an Agency Certification Practice Statement (CPS) – Your CPS must provide specific details of how your PKI implementation meets the requirements stated in your CP. The CPS must be included as supporting documentation in your *Application for Interoperability* [4] with the Bridge.

3. Have Your PKI and CPS Audited for Compliance with Your CP – A third party must perform an independent audit of your organization's PKI implementation, to ensure that it meets the requirements set forth in your CP. The resulting Compliance Audit report must be included in your organization's *Application for Interoperability* [4] with the Bridge.

3. Submit Your Application for Interoperability to the FPKI PA – You must submit an *Application for Interoperability* [4] to the Bridge. This application must include your CP, CPS, Compliance Audit, and contact information. A discussion of the information to be provided as part of the application follows in a later section of this document.

   After being reviewed by the FPKI PA for completeness, the application will be referred to the Federal Certificate Policy Working Group (FCPWG). The FCPWG will evaluate the application, work with your organization to resolve any Certificate Policy issues that might prevent a favorable recommendation for cross-certification, and return their recommendation to the FPKI PA. The FPKI PA will then approve the application and issue an authorization for your organization's PKI to be cross-certified with the FBCA at a specific Certificate Policy level.

4. Negotiate a Memorandum of Agreement (MOA) with FPKI PA – After your *Application for Interoperability* [4] has been submitted to the FPKI PA, you can negotiate a Memorandum of Agreement (MOA) between your organization and the FPKI PA. This MOA can be drafted during the time that the FCPWG is reviewing your application, but it cannot be signed and put into effect until the FPKI PA approves your application.

5. Perform Interoperability Testing with the Prototype Bridge CA – Once the application has been submitted, you can also begin to perform interoperability testing. The FBCA OA maintains a prototype FBCA facility to support interoperability testing, so that initial testing can be performed without adverse impact to the production FBCA. Your PKI cannot be cross-certified with the production FBCA until you receive approval from the FPKI PA. Your directory system may not establish interoperability with the operational BCA Directory System until interoperability testing with the FBCA prototype facility has been completed, and the FBCA Operational Authority authorizes the connection.

6. Conduct Live Test with the Production Bridge CA – After you receive approval, create an MOA with the FPKI PA, and perform initial connectivity testing, you can connect to the production BCA Directory Service and set up cross-certification between your Principal CA and the Bridge CA. Once your agency is connected, you will conduct some initial functional tests to ensure that everything works as expected. Then you can begin working with all the other organizations connected to the Bridge!

D.5 Filling Out the Application

The *Application for Interoperability* [4] can be obtained from the FBCA website. After completing the application, you will submit it to the FPKI PA in written form or in Microsoft Word format to the Federal PKI Policy Authority. The information you must provide includes:

1. Organizational Information – You must include Organization Name and Address; Name, Title, Address and Contact Information for Designated Agent and Secondary Contact(s).

2. Certificate Policy – You must attach a copy of your organization's Certificate Policy (CP) to the application. Your agency CP must be in RFC 2527 [3] format. If your CP was not developed to this format, you must convert it to this format before submitting it to the FBCA Policy Authority.

3. Compliance Audit – You must describe how the organization PKI, the Principal CA, and any other CA that has a trust relationship with the organization PKI, is audited – including the frequency and the identity of the organization who performs the audit. You must attach a copy of your organization's latest PKI Compliance Audit, documenting your organization's PKI's compliance with your CP. This audit must demonstrate that all aspects of the agency PKI Certificate Policy are being complied with, and must be conducted by an independent third party.

4. Certificate Policy Mapping – You must describe the mapping that your agency proposes between the certificate levels covered under your CP, and those set forth in the FBCA CP. You must explain the basis for the proposed mapping by comparing the two CPs and providing any other relevant information or justification.

5. PKI Information – You must provide information regarding the PKI that will be cross-certified with the FBCA. This information must include:

   a) You must provide information about the PKI system implemented within your organization, including:

      - PKI product being used,
      - Version implemented,
      - Signature algorithms supported, and
      - Encryption algorithms supported.

   b) You must identify at the Principal Certification Authority (CA) to be cross-certified with the FBCA. Information to be provided about this CA will include:

      - Distinguished Name (DN) of the Principal CA that will cross-certify with the FBCA,
      - The X.500 Name Space in which the PKI operates; and
      - Contact information for the manager of the Principal CA,

   c) If any CA with a trust relationship to the Principal CA provides certificates that assert object identifiers not covered in the organization's CP, you must identify those OIDs and provide a copy of the relevant CP under which those OIDs are defined.

6. Directory Information – Currently, the initial configuration of the Bridge supports interconnection to X.500-based directory services using the Directory Services Protocol (DSP). Your directory must support X.500 DSP in order for your PKI to interoperate with the Bridge. You must provide information regarding your organization's directory service, including:

   a) A statement regarding the level of conformance of your agency directory with the Federal PKI Directory Profile [5],

   b) DSA Distinguished Name, product, version, network address, and confirmation that the DSA supports1993 X.500 DSP;

   c) The naming context supported by this DSA, e.g., the X.500 "prefix" that identifies your organization's directory information tree (DIT). For instance, Treasury has an X.500 naming context of: *c=us, o=U.S. Government, ou=Department of the Treasury*;

   d) Information about any secondary DSAs that also support that naming context;

   e) The knowledge references that must be established between the BCA's directory and your agency's directory – e.g. cross, superior, or subordinate references – as noted in the Federal PKI Directory Profile.

f) Contact information for your directory and host system administrators.

Important note: If your organization's directory is *not* X.500 compliant, it will not be able to interoperate with the BCA Directory Service using the Directory Services Protocol (DSP). If so, you must utilize a Border DSA that has the ability to service directory requests from your users using whatever protocol is supported within your organization (such as LDAP or NDS) and can communicate with the FBCA using X.500 DSP.

D.6 Testing with the Prototype Bridge

After application has been made to the FPKI PA, you can begin interoperability testing with the prototype Bridge CA. This testing can proceed in parallel with the FPKI PA's approval of the application. The purpose of testing with the prototype Bridge CA is to identify and solve any technical or connectivity issues prior to connecting to the production Bridge CA. The steps involved include:

1. Establish and test network connectivity to the prototype FBCA facility. When this is accomplished, you will be able to *ping* the prototype BCA Directory service host computer from your primary directory server, and vice versa. Your technical people will work with technical staff from the FBCA OA to accomplish this task.
2. Next, establish and test connectivity between your agency's X.500 directory service (or Border DSA) and the prototype BCA Directory. This will involve configuring knowledge references between the prototype Bridge's directory and your directory service, and testing to ensure that directory queries and responses can flow between the directories using the DSP protocol. Your technical people will work with technical staff from the FBCA OA to accomplish this task.
3. Exchange cross-certificates between your Principal CA and the prototype Bridge CA, and install the Bridge CA's cross-certificate in your agency's directory.
4. Perform end-to-end testing to ensure that your PKI-aware application is able to verify digital signatures created by an application in the FBCA OA, and vice versa.

D.7 Connecting to the Production Bridge

You can establish interoperability with the production Bridge CA after the FPKI PA has approved your agency for connection to the Federal Bridge CA, and you have executed a MOA with the FBCA OA. To connect to the production Bridge CA, you will perform essentially the same steps as when you set up interoperability with the prototype Bridge CA.

APPENDIX E – REFERENCES

[1] Burr, W., "Public Key Infrastructure (PKI) Technical Specifications: Part A-Technical Concept of Operations", September 1998

[2] The Evolving Federal Public Key Infrastructure, Federal Public Key Infrastructure Steering Committee, Federal Chief Information Officers Council, *http://gits-sec.treas.gov*.

[3] Governmentwide Directory Support 2 Technical Series, the Updated US Gold Schema document, 7/14/1997, by Booz Allen & Hamilton.

[4] The Bridge CA Demonstration Repository Requirements Draft 4/8/1999 by Chromatix, Inc.

[5] NSA Bridge Certification Authority Demonstration Phase II - Directory Requirements and architecture, 7/3/2000, by Entigrity Solutions.

[6] Boeyen, S., Howes, T., and P. Richard, "Internet X.509 Public Key Infrastructure LDAPv2 Schema", RFC2587, June 1999.

[7] ITU-T Recommendation X.509 (1997) | ISO/IEC 9594-8: 1997, “Information technology - Open Systems Interconnection - The Directory: Authentication framework”, June 1997.

[8] ITU-T Recommendation X.521 (1997) | ISO/IEC 9594-7: 1997, “Information technology - Open Systems Interconnection - The Directory: Selected object classes”.

[9] Common Directory Services and Procedures, ACP (Allied Communication Publication) 133 Edition B, March 2000.

[10] M. Smith, "Definition of the inetOrgPerson LDAP Object Class", RFC 2798, April 2000.

[11] Kille, S., Wahl, M., Grimstad, A., Huber, R., and S. Sataluri, "Using Domains in LDAP Distinguished Names", RFC 2247, January 1998.

[12] Grimstad, A., Sataluri, S., and M. Wahl, "Naming Plan for Internet Directory-Enabled Applications", RFC 2377, September 1998.

[13] The Middleware Architecture Committee for Education (MACE) *http://middleware.internet2.edu/MACE/*

[14] Armijo, M., Esibov, L., Leach, P., and R. Morgan, “Discovering LDAP Services with DNS”, Work in Progress.

[15] Wahl, M., Howes, T., and S. Kille, "Lightweight Directory Access Protocol (v3)", RFC 2251, December 1997.

APPENDIX F – ACRONYMS

ACP	Allied Communications Publication
c	country
CA	Certification Authority
cn	commonName
dc	domainComponent
DIT	Directory Information Tree
DN	Distinguished Name
DNS	Domain Naming System
DSA	Directory Service Agent
DSP	Directory Services Protocol
EE	End Entity
EMA	Electronic Messaging Association
FBCA	Federal Bridge Certification Authority
FOUO	For Official Use Only
FPKI	Federal Public Key Infrastructure
FQDN	Fully Qualified Domain Name
IETF	Internet Engineering Task Force
LDAP	Lightweight Directory Access Protocol
o	organization
OA	Operational Authority
OID	Object IDentifier
ou	organizationalUnit
PAA	Policy Approving Authority
PCA	Policy Creation Authority
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (X.509)
RDN	Relative Distinguished Name
RFC	Request For Comment
S/MIME	Secure Multipart Internet Messaging Extensions
SSL	Secure Socket Layer
TLS	Transport Layer Security
uid	userID
X.500	ITU specification for directory services