Federal Public Key Infrastructure (FPKI) Architecture Technical Overview

October 2005

Federal PKI Operational Authority

REVISION HISTORY

Document Date	Revision Details
March 2005	First publication by FPKI OA
August 2005	FPKI OA Clarified statement on distinguished naming conventions in section 2.5.1.
October 2005	FPKIOA Amended and clarified description of interrelations between elements of the FPKIA (i.e., Certification Authorities) in section 2.2

TABLE OF CONTENTS

SECTION **PAGE**

LIST OF FIGURES

FIGURE **PAGE**

LIST OF TABLES

TABLE **PAGE**

SECTION 1

INTRODUCTION

1.1 BACKGROUND

The E-Authentication Initiative is an important component of the President's Management Agenda (PMA) item for expanding e-Government. It was established to assist the agency system owners in developing trust relationships with their user communities through the use of electronic identity credentials. To accomplish this objective, the E-Authentication Initiative will leverage identity credentials across multiple trust environments to enable identity assurance services for Federal electronic business processes, which will enable trust and confidence in e-Government transactions through the establishment of an integrated policy and technical infrastructure for identity management.

The governance structure of the E-Authentication Initiative includes the Office of Management and Budget (OMB), the Federal Chief Information Officers Council (CIOC), the Federal Enterprise Architecture Program Management Office (FEAPMO), and the E-Authentication Service Component. The chart below depicts the governance structure.

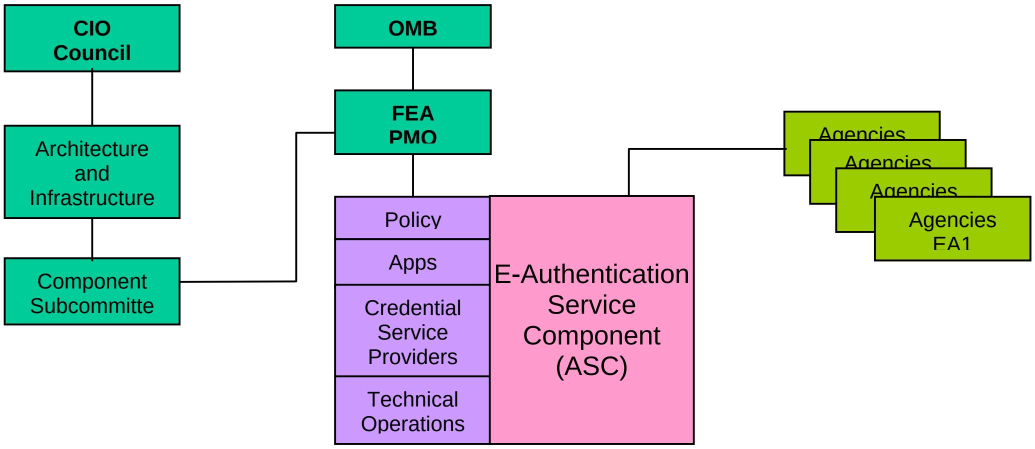

Figure 1.1-1 E-Authentication Initiative

The E-Authentication Component is responsible for providing uniform authentication services across the government. This is accomplished by working directly with agencies to assist them in determining their E-Authentication needs (compliant with assurance level policy and technical standards) and solving technical interoperability challenges.

Within the technical operations of the E-Authentication Service Component, the architectural framework is defined that includes a Federal PKI.

The E-Authentication initiative has defined four assurance levels to accommodate varying levels of risk. For certificate based credentials, the FPKI will solve the technical interoperability challenge of melding individual entity initiatives that use PKI products from a variety of commercial vendors into a Federal PKI and supports entity (i.e., state and local governments, foreign governments, businesses, and the public) business processes using certificate based credentials.

The principal reason for this distinction is that certificate based transactions require a cryptographic binding between the authentication and transaction, which is widely available using client certificates over Secure Socket Layer (SSL).

1.2 PURPOSE AND SCOPE

This document provides a high level description of the FPKI architecture and its role in the E-Authentication initiative.

The reader should have an understanding of PKI. Section 2.4 assumes the reader being quite familiar with directory services technology. The reader will gain an understanding of the FPKIA and its supporting directory. The document is organized as follows.

Section 1 – Introduction – This section.

Section 2 – FPKI Architecture – Provides an overview and description of the initial and current FPKIA architecture, encompassing CAs as well as the supporting directory high level architectures (off-line and on-line).

SECTION 2

FPKI ARCHITECTURE

Similarly to any PKI, the implementation of the FPKIA, encompasses Certificate Authorities (CAs) as well as a directory/repository architectural structures. The underlying directory infrastructure architecture enables the implementation of the CA architecture by providing the information publishing service.

The FPKIA incorporates multiple cross-certified CAs that have demonstrated interoperability among each other. This set of CAs is off-line (i.e., disconnected from the Internet). The publishing service architecture of the FPKIA encompasses an off-line and an on-line directory services, separated by an a one-way internal firewall.

This section describes both CA and directory architectural aspects as well as their evolution path followed from the initial implementation to its present state.

2.1 INITIAL CONCEPT AND OPERATION

The initial conceptual architecture included the Federal Bridge Certification Authority (FBCA). Because the FBCA concept was quite innovative with respect to the market place at that time, the FBCA initial operation began by deploying one CA (i.e., Entrust) that successfully passed the interoperability and compliance testing conducted in the pilot test environment.

The Federal Bridge Certification Authority (FBCA) is an information system that implemented the Federal PKI. It continues to solve the technical interoperability challenge of the Federal PKI to meld individual entity initiatives that use PKI products from a variety of commercial vendors into a Federal PKI.

Concurrent to supporting the Federal PKI with the aforementioned initial operating capability, the FBCA featured multiple CAs by disparate vendors that cross-certified successfully with all current membrane members and entered the FBCA architecture. These vendors are Betrusted (formerly Baltimore Technologies), RSA, and Microsoft.

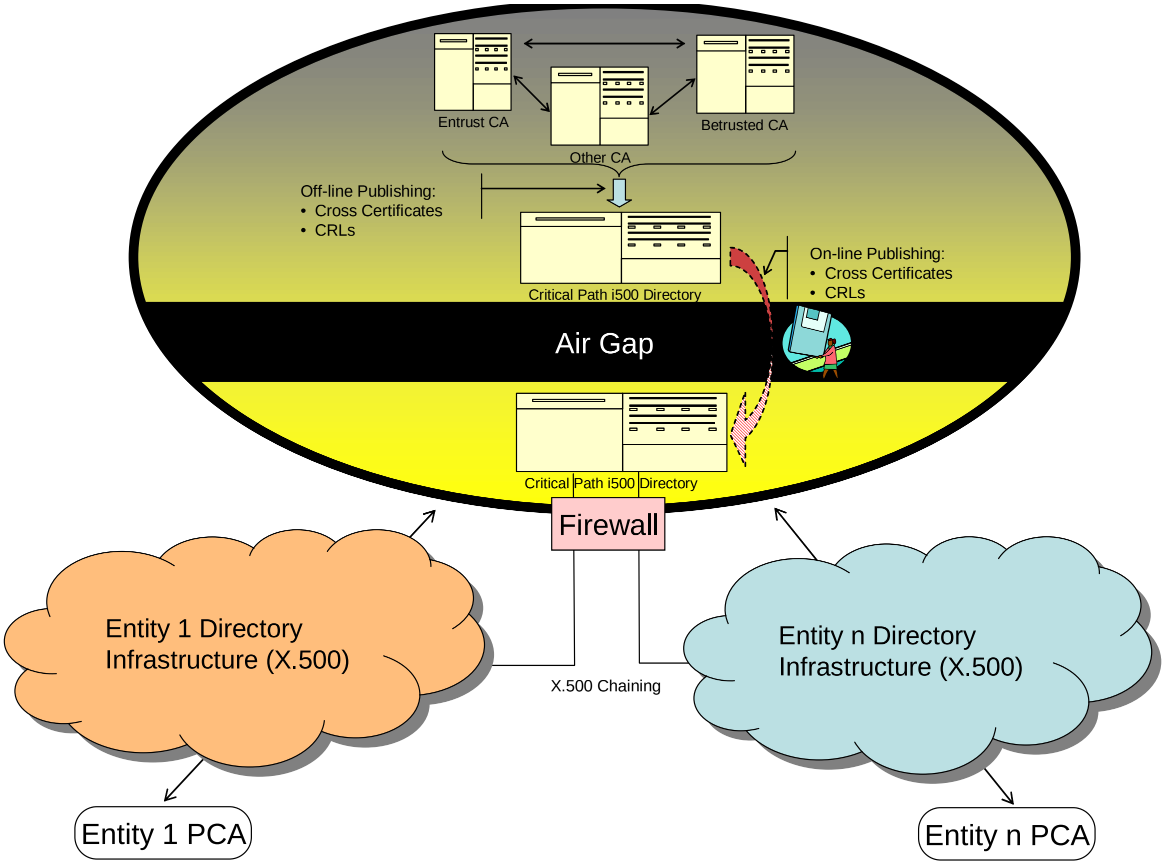

Figure 2.1-2 Initial Concept and Operation of the FBCA

2.2 EVOLVED OPERATION

Since its initial conceptualization and operation, the FBCA membrane has ceased from incorporating cross-certified CAs by multiple vendors that have demonstrated interoperability among one another. It has evolved into the FPKI architecture that emcompasses CAs by multiple vendors designating each CA to support a different FPKI policy and function.

The Federal PKI enabling policy CAs are: (1) FBCA, (2) the Federal PKI Common Policy Framework (FCPF) Root CA, and (3) Citizen and Commerce Class Common (C4) Root CA. The evolved operation also incorporates the e-Governance CAs used to issue SSL/TLS certificates supporting assertion-based credentials for Security Assertion Markup Language (SAML) data exchanges.

All the FPKIA CAs are off-line (i.e., isolated from the Internet) and automatically publish to an internal off-line directory. Off-line posted information is periodically (daily) manually published to the on-line (i.e., connected to the Internet) FBCA directory system to provide universal X.500 and Lightweight Directory Access Protocol (LDAP) accessibility.

Figure 2.2-1 depicts: (1) a notional view of the current FPKI architecture; (2) the FBCA (i.e., multiple cross-certified CAs cross certified to various entities) is now represented and accomplished by a single CA; (3) that the FBCA now additionally cross-certifies with FCPF Policy CA but not with C4 Policy CA (there are still discussions on whether the C4 Policy CA might be one-way cross certified to the FBCA at Rudimentary, two-way, or not at all – this is shown in the diagram by the gray-ed out arrows and labels between the FBCA and the C4 Policy CA); and (4) the absence of a cross-certification between the E-Governance CAs and the FBCA.

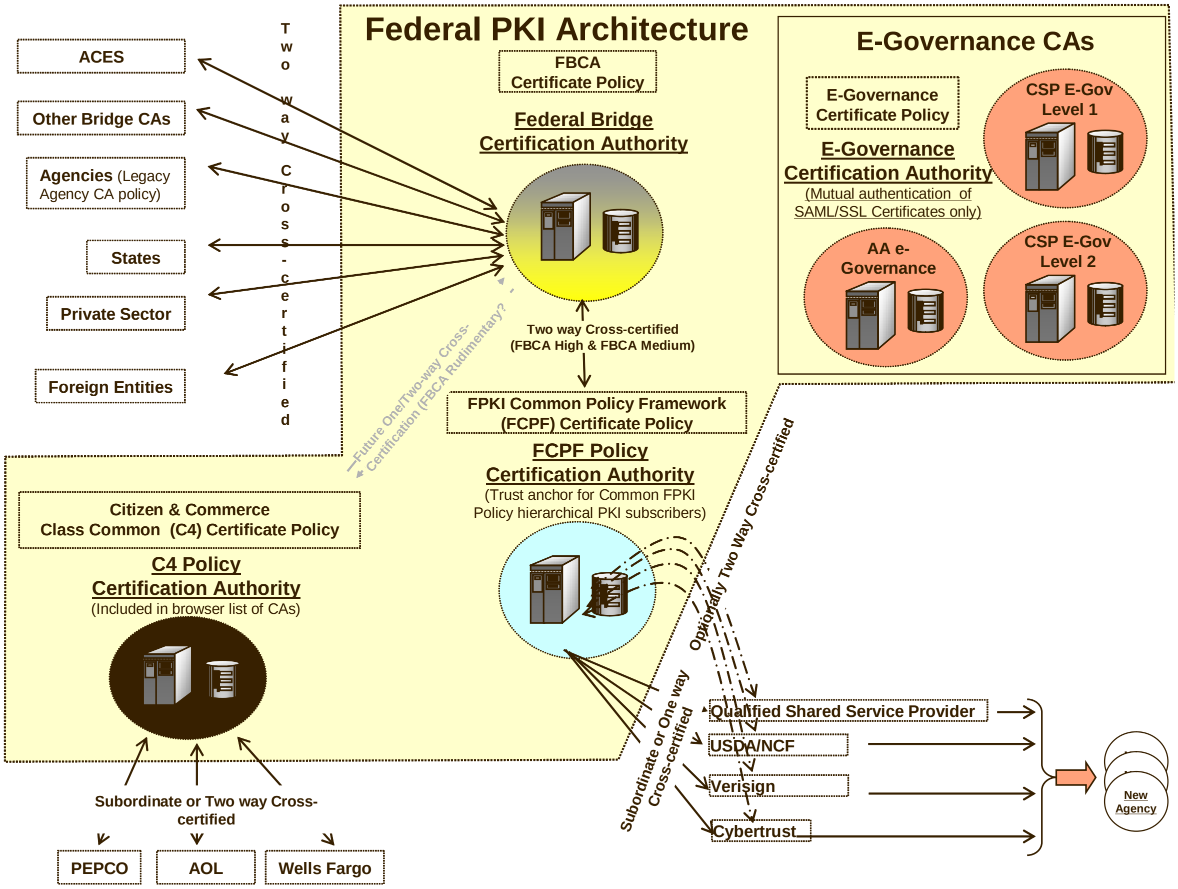
Federal PKI Architecture
FBCA Certificate Policy
Federal Bridge Certification Authority
ACES
Other Bridge CAs
Agencies (Legacy Agency CA policy)
States
Private Sector
Foreign Entities
Two way Cross-certified
Two way Cross-certified (FBCA High & FBCA Medium)
Future One/Two-way Cross-Certification (FBCA Rudimentary?
E-Governance CAs
E-Governance Certificate Policy
E-Governance Certification Authority
(Mutual authentication of SAML/SSL Certificates only)
CSP E-Gov Level 1
AA e-Governance
CSP E-Gov Level 2
FPKI Common Policy Framework (FCPF) Certificate Policy
FCPF Policy Certification Authority
(Trust anchor for Common FPKI Policy hierarchical PKI subscribers)
Optionally Two Way Cross-certified
Subordinate or One way Cross-certified
Qualified Shared Service Provider
USDA/NCF
Verisign
Cybertrust
New Agency
Citizen & Commerce Class Common (C4) Certificate Policy
C4 Policy Certification Authority
(Included in browser list of CAs)
Subordinate or Two way Cross-certified
PEPCO
AOL
Wells Fargo

Figure 2.2-1   CA Functions Within the FPKI Architecture

2.2.1 FBCA Function

The FBCA is an information system that solves the technical interoperability challenge of the Federal PKI to meld individual entity initiatives that use PKI products from a variety of commercial vendors into a Federal PKI and implements certificate based assurance.

The FBCA functions as a non-hierarchical hub allowing entities to create a certificate trust path from its domain back to the domain of the entity that issued the certificate, so that the levels of assurance honored by disparate PKIs can be reconciled. The FBCA function is depicted in Figure 2.2.1-1.

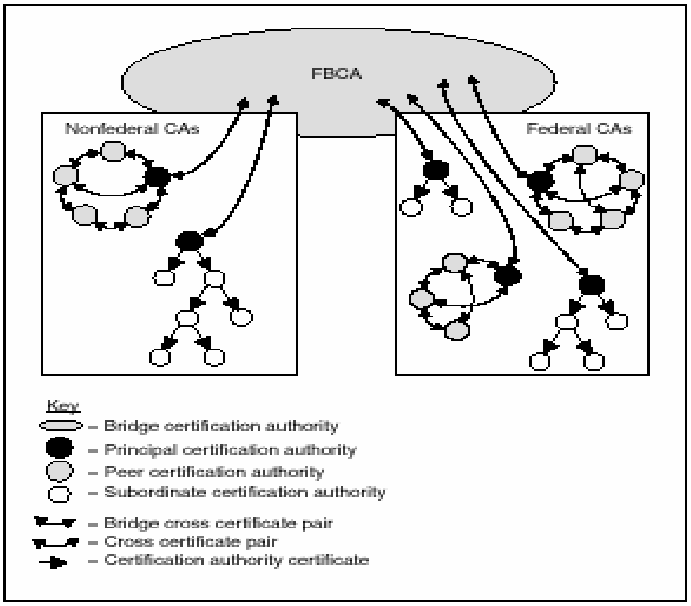
FBCA
Nonfederal CAs
Federal CAs
Key
= Bridge certification authority
= Principal certification authority
= Peer certification authority
= Subordinate certification authority
= Bridge cross certificate pair
= Cross certificate pair
= Certification authority certificate

Figure 2.2.1-1FBCA Function in the Federal PKI

As depicted in Figure 1.1-2, the unifying Federal PKI architecture applies a hub-and-spoke model where each PKI cross-certifies with FBCA, allowing certification paths to be built between any two PKI systems. This is accomplished by following the cross-certificate pairs through the FBCA. In other words, the FBCA enables transitive trust among the cross-certified trust domains. The number of cross certificates required for this architecture is $n = x \times 2$, where *x* is the number of PKI systems and *n* the number of cross-certificates to be maintained

2.2.2 EGCAs Function

While the role of the FBCA remains central in the FPKI architecture, the e-Governance CAs fulfill and support the E-Authentication Service Component requirements as they relate to the associated technical aspects.

There are three separate e-Governance CAs; the first two CAs, each associated with a different policy and assurance level that will issue Transport Layer Security (TLS) certificates to government approved Credential Services (CSs) provided by Credential

Service Providers[1]; the last CA will issue to approved Agency Applications (AAs) irrespective of assurance level. For more information on the E-Authentication initiative baseline technical architecture the reader should refer to the E-Authentication technical document suite published at http://www.cio.gov/eauthentication/library.htm

2.2.3 FCPF CA Function

The E-Government Act (Public Law 107-347) of 2002 and Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA) mandate a "buy not build" paradigm, whereby Federal agencies are strongly recommended to acquire PKI services from Shared Service Providers (SSPs) instead of acquiring and implementing their own infrastructure. SSPs include federal agencies (e.g., DoA/USDA/NFC) as well as commercial vendors. Figure 2.2-1 shows that federal agencies may elect to follow such guidance by participating via an SSP (strongly recommended), or, upon OMB approved justification, acquire their own PKI and cross-certify with the FBCA CA. The FCPF CA is the trust anchor for the federal workforce that participates in the FPKI by acquiring PKI services from a shared service provider. The FCPF CA reduces the number of cross certifications (and associated policy mapping activity) between the FBCA and the federal agencies to just the one between it and the FBCA. The shared service provider CAs are subordinate to the FCPF CA, therefore inherently cross-certified with the FBCA.

2.2.4 C4CA Function

C4 is a streamlined process based on memorandum of agreement rather than detailed review of CP and CPS for compliance. The C4 policy is modeled against the FBCA Rudimentary level of assurance and defines requirements for certificates accepted by the U.S. Federal Government for the purpose of authenticating citizens and commercial enterprises for many electronic services. Certification authorities and credential services by citizens and companies (e.g., AOL, Wells Fargo, PEPCO) conducting business with the federal government are subordinate to, or have the option to two-way cross-certify with, the C4 CA.

[1] CSPs are sometimes referred to as Electronic Credential Providers in other documents

2.3 FBCA INITIAL DIRECTORY CONFIGURATION

The initial FBCA directory configuration included one internal off-line directory and one on-line directory connected to the Internet via a firewall. Both directories were implemented on the Critical Path i500 server.

The initial FBCA directory configuration required agencies to establish a X.500 directory that would enable them to chain to the FBCA online directory. Since there are many more LDAP repository than X.500 based implementations, this configuration was deemed non compliant to the FBCA requirement to provide universal access to the posted data. Furthermore, it created a budget burden to Federal agencies since it required acquisition of a X.500 directory for the sole purpose of implementing chaining to the FBCA.

Since the expected LDAP traffic would be much greater than the X.500, the current FBCA directory online configuration required a separate dedicated LDAP server to handle it.

LDAP architectures rely on clients being capable of understanding and acting upon LDAP referrals, as well as, on organizations establishing LDAP proxy servers to comply with strict IT security policies. The current FBCA Directory sought to address such issues by implementing a directory architecture that implements “LDAP chaining” (i.e., outgoing LDAP requests), thereby avoiding the referral mechanism.

The FPKIA CAs rely on the current directory now known as the FPKIA directory to provide certificate and certificate revocation list (CRL) accessibility to relying parties. CAs publish certificates and CRLs by posting them into the FPKIA directory system. Relying parties then access the FPKIA directory during certificate validation. The FPKIA operational practice ensures that the internally posted information is also posted, daily, to the on-line (i.e., connected to the Internet) FBCA directory via a one way internal firewall push mechanism.

2.3.2 FPKIA Current Directory Configuration

The current directory architecture underlying the FPKIA contains three full-function X.500 directory servers supporting the publishing of cross-certificates, CA certificates, and revocation lists by the off-line CAs. The off-line directory server supports the internal/off-line publishing by the FPKIA CAs. The internal directory is implemented by the Critical Path i500 server. The internally published data is copied onto the on-line directory system via one-way pushing mechanism.

The on-line FPKIA directory system connects to clients or (border) directory services. The on-line FPKIA directory is made up of two ISODE M-Vault directory chained[2] X.500 directories both implementing meta-connector technology to reach out to LDAP (non-X.500) repositories (i.e., “LDAP chaining”).

The server dedicated to provide FPKIA LDAP directory access is set up to be a shadow of the server dedicated to FPKIA DSP directory function; however the only DSP/DISP requests allowed to this directory are ones that originate from the FPKIA DSP directory. The firewall is configured to allow anonymous access from any IP address to the LDAP directory (via LDAP). On the other hand, the firewall only allows trusted entities to DSP chain to the FPKIA DSP directory. Both directories can make LDAP requests to trusted directories; however, only the FPKIA DSP directory is allowed to make DSP requests to trusted directories. All other access to and from this network is restricted.

The “on-line” directories have the same structure, including schema and attributes as described in section 2.4. However, the ISODE M-Vault product is capable of providing “LDAP chaining” which enables entities using pure LDAP directories to interoperate with the FBCA using LDAP instead of DSP notwithstanding any local IT security policy or client LDAP referral aware capability. The “on-line” directories are built at the c=US context prefix, allowing entities to chain to these directories using a superior reference. More information on superior references can be found in section 2.3.1.

[2] The term “chained” refers to the ITU-T X.500/IS 9594 Directory Service Protocol (DSP) connecting two directory service agents (DSAs).

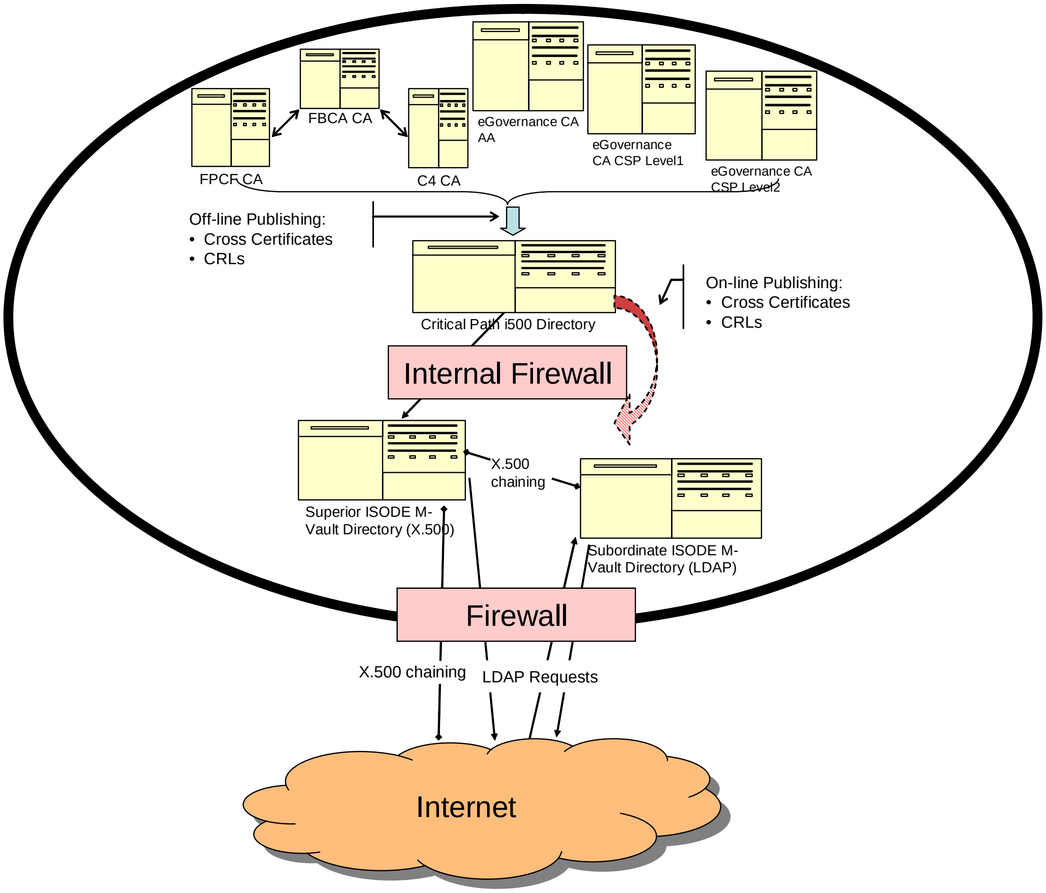

Figure 2.3.2-1FPKIA Directory Architecture (off-line and on-line)

2.4 DIRECTORY CONNECTIVITY

Figure 2.4-1 depicts the directory connectivity.

In the first scenario, an LDAP client (or, not depicted, a directory server) generates (i.e., path 1) an anonymous LDAP request (resulting, or not, from a LDAP referral) to the FPKIA. The firewall allows passage and the LDAP request reaches the FPKIA LDAP server. The FPKIA LDAP server either responds with the information, generates (i.e., path 2.1) a LDAP query to another LDAP repository, or generates (i.e., path 2.2) a DSP chaining request to the FPKIA X.500 directory. In turn, the FPKIA X.500 directory either responds with the information or (i.e., path 2.3) chains to another X.500 directory.

The second scenario describes (i.e., path a) an X.500 chaining request by an authorized party allowed by the firewall to reach the FPKIA X.500 directory. The FPKIA X.500 directory either replies with the data, chains (i.e., path b.1) to another X.500 Directory, or (i.e., path b.2) generates a LDAP request to a LDAP repository.

The aforementioned two scenarios and any combination of them fulfill the FPKIA requirement for universal accessibility of the data published.

The firewalls protecting the online directories must be opened up to allow DSP chaining and/or LDAP to take place on the correct port. Load balancers must be configured (much like firewalls) to allow DSP chaining and/or LDAP to take place on the proper directories and port.

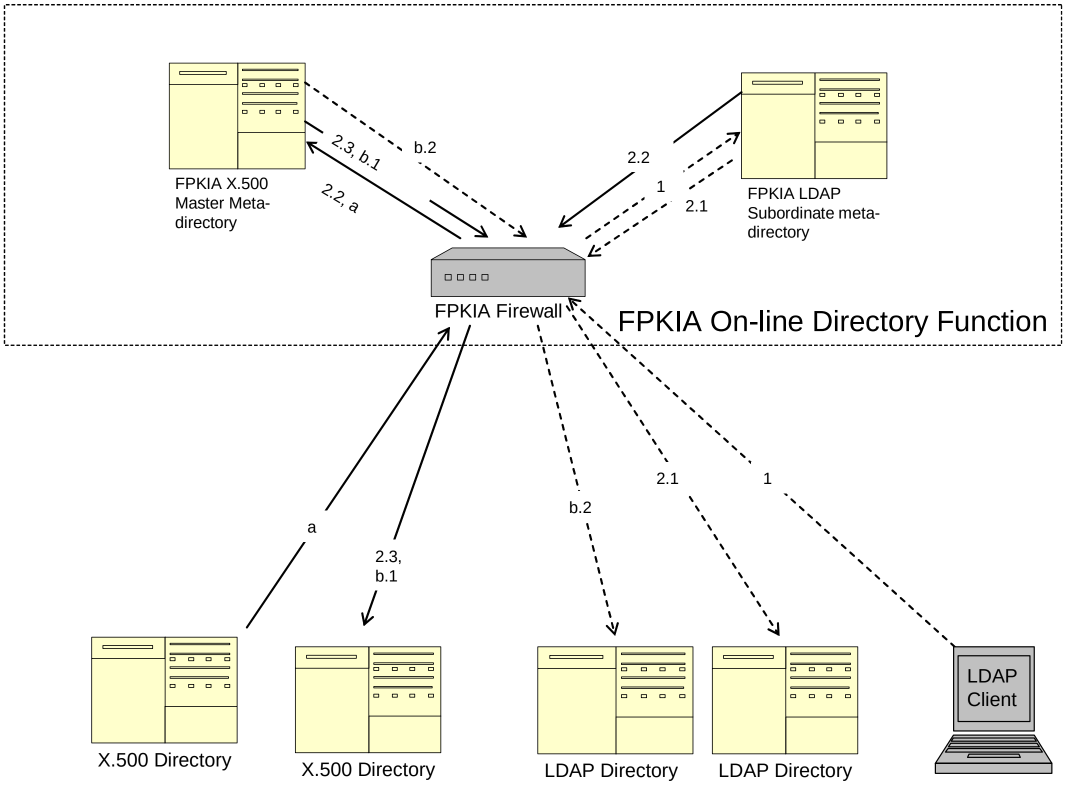

Figure 2.4-1 FPKIA On-line Directory Function Connectivity Diagram

2.4.1 X.500 DSA

Entity PKIs that publish Certificates and CRLs in a X.500 (border) directory chain to the FPKIA ISODE M-Vault setup as the master online directory. It is recommended that entities setup a superior or “parent” chaining agreement to the FPKIA “online” directory. This will allow entities to only include one reference for all cross-certified PKIs, rather than adding an entry for each trusted PKI.

2.4.2 LDAP Servers

Entity PKIs that do not publish to X.500 (border) directories use instead LDAP (border) repositories to distribute the CRL and certificates. Where the entity PKI enforces a tight IT security policy, it might also use LDAP proxy servers to limit the number of IP addresses directly querying the (border) LDAP server. Notwithstanding the above, entity LDAP directory servers are reachable by any FPKIA on-line directory using the meta-connector capabilities to implement “LDAP chaining”.

2.4.3 Clients

FPKIA-aware clients make use of their own PKI system and certificate publishing (directory/repository) service. The CAs within those systems publish certificates, cross-certificates, and revocation lists into that FPKIA-aware client’s own directory service.

The FPKIA-aware client builds a certificate validation path (i.e., path discovery) between its trust anchor (e.g., the entity issuing CA) and the authority that issued the certificate to verify a digital signature. In order to build this certificate validation path, the client must obtain certificates and revocation lists from other trust domains that are cross-certified with the FBCA. These certificates and revocation lists will have been published by the PKI systems that exist in each trust domain.

FPKIA-aware clients are strongly encouraged to comply with the requirements for path discovery and path validation that are currently being developed by the Path Discovery and Validation Working Group, an FPKIA working group. These will ensure seamless interoperability among FPKIA-aware clients and the FPKIA online repository. The requirements address two types of client base, namely those that are LDAP referral handling capable, and those that ignore LDAP referrals:

LDAP Referrals Aware Clients The FPKIA Path Discovery and Validation Working Group is currently developing the requirements that govern these clients.

LDAP Referrals Agnostic Clients The FPKIA online directory architecture, utilizing a double directory with meta-connector capability design, implements a “LDAP chaining” capability that, similarly to the X.500 DSP chaining, generates outgoing LDAP requests to retrieve the data from an LDAP repository, and then providing it to the LDAP referral-agnostic client still waiting for the response.

.

Figure 2.4.3-1 depicts an example of FPKIA-aware clients scenario belonging two separate trust domains cross-certified with the FBCA that operate in a signed SMTP/MIME based secure transaction.

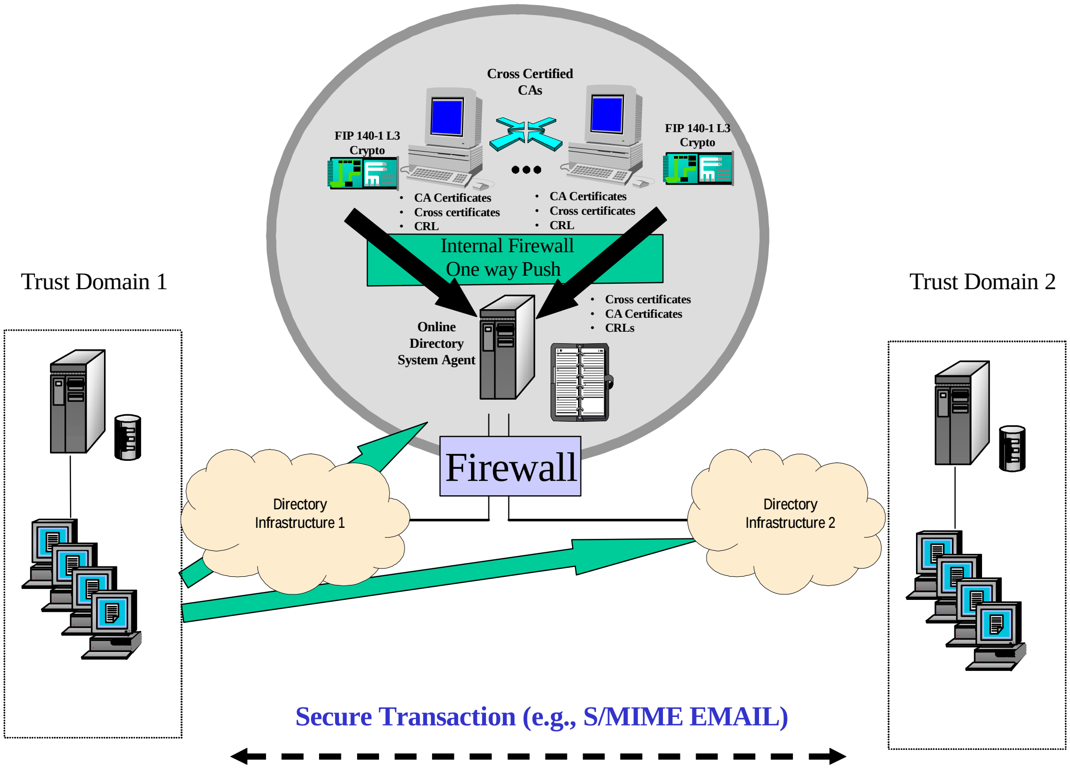

Figure 2.4.3-1 Concept of FPKIA-aware Applications (e.g., S/MIME email)

2.5 FPKIA DIRECTORY ARCHITECTURE

This section includes high-level technical information that enables applicant entities to plan and set up their interoperability testing activity. More detailed information, such as port numbers and IP addresses, requires entities to adhere to the application process controlled by the FPKIPA.

The FPKIA directory contains information required to perform cross-certifications between the FBCA and entity Principal CAs. The FPKIA Directory Information Tree (DIT) is based on the government-wide X.500 DIT. This section describes the FBCA DIT.

The structure of the FPKIA DIT is shown in Figure 2.4-1. The FBCA level of the directory is located directly underneath the U.S. Government level of the X.500 DIT.

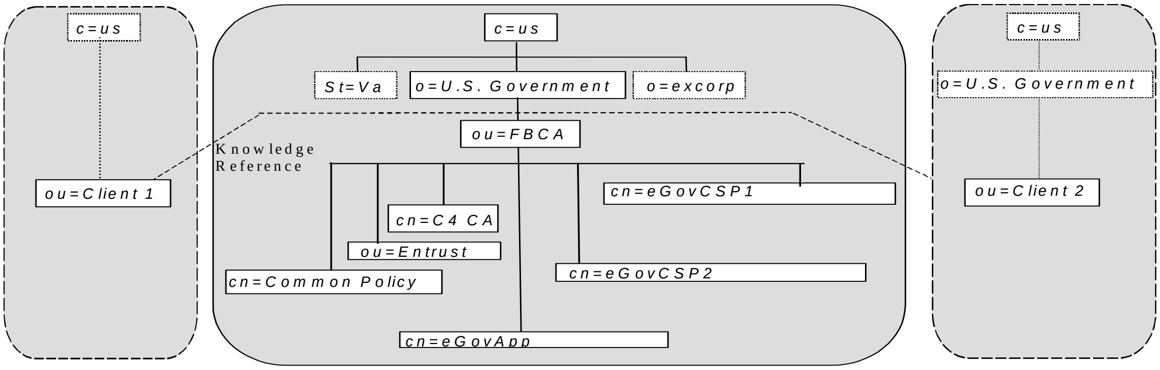

Figure 2.5-1 FPKIA Directory Information Tree

2.5.1 U.S. Government and United States Levels

Currently there is no organization in the Federal government appointed to operate the U.S. Government and United States levels. However, to ensure correct operation of the FBCA and the FPKI, such DIT levels must exist, hence the FPKIA has established its DIT at the c=US level. This will enable correct and proper implementation of X.500 chaining knowledge references and LDAP requests.

One of the distinguished naming conventions for all Federal PKI CAs is, o=U.S. Government, c=US (other naming conventions are domain component naming [see section 2.5.2], c=US with o=name of the agency, or a combination thereof). The FPKIA will include the additional RDN ou=FBCA (and, for the FBCA, also ou=Entrust,) in its DN. Similarly, the other FPKIA CAs add to ou=FBCA an RDN linked to their policy (e.g., ou=Entrust, cn=C4 CA, cn=Common Policy, cn=eGovCSP1, cn=eGovCSP2, and cn=eGovApp.)

Therefore, the complete naming context for the six FPKIA CAs is:

c=us, o=U.S. Government, ou=FBCA, ou=Entrust
c=us, o=U.S. Government, ou=FBCA, cn=Common Policy
c=us, o=U.S. Government, ou=FBCA, cn=C4 CA
c=us, o=U.S. Government, ou=FBCA, cn=eGovCSP1
c=us, o=U.S. Government, ou=FBCA, cn=eGovCSP2

c=us, o=U.S. Government, ou=FBCA, cn=eGovApp

Note: Because the DIT has evolved from supporting a FBCA-only function to supporting the FPKIA, the current FPKIA schema has retained the ou=FBCA level instead of relabelling that level to ou=FPKIA. Such relabelling would have required conducting costly key-generation and re-issuing all certificates activities, therefore the FPKIA naming space remains as ou=FBCA.

2.5.2 Schema

The FPKIA Directory requires a rather minimal schema. Basically, the following schema must be supported as a minimum:

- X.520/X.521 standard objects and attributes
- RFCs 1777, 2251, 2559, and 2587
- PKIX
- Entrust Technologies Schema

Most vendors implement PKI utilizing the standard schema specified by the IETF PKIX specifications. Entrust implementations used an enhanced version of the standard schema elements. Therefore the FPKIA schema, since it includes Entrust products, will require the support of the Entrust schema in addition to the standard one. The major objects and attributes required are anticipated to be as follows.

X.500 Standard Objects

The following object classes and attributes are defined in X.520/X.521 and are generally assumed to be mandatory as a minimum schema definition. Several of the objects are used to define the structure of the DIT and to connect the DSA to parents, peers, and subordinates.

Table 2.5.2-1 X.500 Standard Object Classes

ObjectClass	Attributes	Notes
Top	aci	required
country (c)	countryName aci searchguide description	only used for *c=us* or for connectivity to other countries
organization (o)	**o** aci businesscategory description	used by organizational entries directly under the country level

ObjectClass	Attributes	Notes
	destinationindicator facsimiletelephonenumber internationalisdnnumber physicaldeliveryofficename postofficebox postaladdress postalcode preferreddeliverymethod registeredaddress searchguide seealso st street telephonenumber teletexterminalidentifier telexnumber userpassword x121address	
organizationalUnit (ou)	**ou** aci businesscategory description destinationindicator facsimiletelephonenumber internationalisdnnumber l physicaldeliveryofficename postofficebox postaladdress postalcode preferreddeliverymethod registeredaddress searchguide seealso st street telephonenumber teletexterminalidentifier telexnumber userpassword x121address	All agencies underneath *o=U.S. Government* are organizational unit entries in the x.500 directory. *ou* divisions can also exist within other organizations such as the private sector, but are controlled by the organization
state (s)	stateOrProvinceName aci description	States are listed under the *c=us* level. [Note: need a full definition of this object]
locality (l)	localityName aci description searchguide	Localities are further divisions within states, organizations, or organizational units

ObjectClass	Attributes	Notes
	seeAlso stateOrProvinceName streetAddress	
person (pn)	**sn** **cn** aci description seealso telephonenumber userpassword	
organizationalPerson	**sn** **cn** aci description seealso telephonenumber userpassword destinationindicator facsimiletelephonenumber internationalisdnnumber ou physicaldeliveryofficename postofficebox postaladdress postalcode preferreddeliverymethod registeredaddress st street teletexterminalidentifier telexnumber title x121address	
alias	aliasedObjectName aci	
applicationEntity	commonName aci description localityName organizationName organizationalUnitName presentationAddress seeAlso supportedApplicationContext	
applicationProcess	commonName aci description localityName	

ObjectClass	Attributes	Notes
	organizationalUnitName seeAlso	
device	commonName description localityName organizationName organizationalUnitName owner seeAlso serialNumber	
dSA	commonName description knowledgeInformation localityName organizationName organizationalUnitName presentationAddress seeAlso supportedApplicationContext	
groupOfNames	businessCategory commonName member description organizationName organizationalUnitName owner seeAlso	

FBCA Schema Elements

The following information is drawn from the Draft FPKI Directory Profile version 2.5, dated 8 October 2002.

Table 2.5.2-2 End Entity (EE) Entries

Attributes	
Minimum Mandatory	*userCertificate* as defined in 1997 X.509v3 (OID: {2 5 4 36})
	commonName as defined in 1997 X.521 (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
Optional	*attributeCertificate* as defined in 1997 X.509v3 (OID: {2 5 4 58})

Object Classes	
Minimum Mandatory	*person* as defined in 1997 X.521 (OID: {2 5 6 6})
	*pkiUse*r as defined in RFC 2587: LDAPv2 Schema (OID: {2 5 6 21}) for non-Entrust EEs – OR – *entrustUser* (Entrust Directory Schema Requirements)
Optional:	*securePkiUser* as defined in Allied Communications Publication (ACP) 133 Edition B (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 (OID: {2 16 840 1 113730 3 2 2})

Table 2.5.2-3 Certification Authority (CA) Entries

Attributes	
Minimum mandatory	*commonName* OR *organizationalUnitName* as defined in 1997 X.509v3 (OIDs: {2 5 4 3} and {2 5 4 11} respectively) 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
	cACertificate as defined in 1997 X.509v3 (OID: {2 5 4 37}).
	certificateRevocationList as defined in 1997 X.509v3 (OID: {2 5 4 39})
	crossCertificatePair as defined in 1997 X.509v3 (OID: {2 5 4 40})
Optional	*authorityRevocationList* attribute as defined in 1997 X.509v3 (OID: {2 5 4 38})
Object Classes	
Minimum Mandatory	*pkiCA* as defined in RFC 2587: LDAPv2 Schema (OID: {2 5 6 22}) OR *entrustCA* (defined in Entrust Directory Schema Requirements) OR *certificationAuthority* OR certificationAuthorityv2**
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 Internet Engineering Task Force (IETF) Request for Comment (RFC) 2798 (OID: {2 16 840 1 113730 3 2 2})
	organizationalUnit as defined in 1997 X.521 (OID: {2 5 6 5})

**certificationAuthority* and *certificationAuthorityv2* have been deprecated. pkiCA is the preferable object class.

Table 2.5.2-4 Attributes Authority (AA) Entries

Attributes	
Minimum Mandatory	*userCertificate* (X.509 – OID: {2 5 4 36})
	spif (SDN.702 – OID: {2 16 840 1 101 2 1 5}).
	commonName as defined in 1997 X.521 (OID: {2 5 4 3})
	surname as defined in 1997 X.521 (OID: {2.5 4 4})
Optional	*attributeCertificate* as defined in 1997 X.509v3 (OID: {2 5 4 58})
Object Classes	
Minimum Mandatory	*person* as defined in 1997 X.521 (OID: {2 5 6 6})
	*pkiUse*r as defined in RFC 2587: LDAPv2 Schema (OID: {2 5 6 21}) for non-Entrust EEs – OR – *entrustUser* (Entrust Directory Schema Requirements)
	organizationalRole (X.521 – OID: {2 5 6 8})
Optional:	*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 (OID: {2 16 840 1 113730 3 2 2})
	NOTE: FBCA Directory Servers containing AA entries shall implement the *dMSOrganizationalRoleRule*.Content Rule (which is based on the *organziationalRole* structural object class) as defined in ACP 120 dated April 1999. This content rule includes *spif* as an optional attribute

Entrust Schema

The following objects and attributes are specified by Entrust Technologies, in order to support their PKI products. These are defined in the Entrust Technologies White Paper, *Entrust Directory Schema Requirements*; Chris Oliva; August 1998.

Table 2.5.2-5 Entrust Schema

ObjectClass	Attribute	Notes
entrustUser	userCertificate	
entrustCA	cACertificate certificateRevocationList authorityRevocationList crossCertificatePair userPasssword attributeCertificate	
organizationalPerson	(none)	
cRLDistributionPoint	(none)	
uniquelyIdentifiedUser	serialNumber	
simpleAuthObject	userPassword	
rfc822MailUser	rfc822Mailbox	
emailAddressUser	emailAddress	
msMailUser	msMailFullname msMailID msMailNetwork msMailPostOffice	
ccMailUser	ccMailComments ccMailName ccMailPostoffice	
qmMailUser	qmUserName qmMailCenter qmZone	
trustTypes	smimetrust ssltrust objsigntrust	
pKCS10Device	serialNumber	
cEPDevice	unstructuredName unstructuredAddress	

Domain Component (DC) Naming

Internet Standards track RFC 2247 and RFC 2377 define a method of representing Domain Name System (DNS) domain components using the X.500 information model, thus enabling X.500 and LDAP-based directory services to store information in “Internet-familiar” manner. RFC 2247 defines:

domainComponent (dc), attribute that can be used to store a domain component such as “gov”, “mil”,“com”, “edu”, “nist”, “gsa”, etc.;

domain object class allowing the addition of new entries that contain a *dc* attribute; and

dcObject object class that might be added to existing objects to include a *dc* attribute.

The use of *domain* objects enables to accurately represent DNS structures within an X.500 or LDAP directory service. Therefore a directory entry specified by the email address john.smith@irs.treas.gov might be characterized 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

LIST OF REFERENCES

1. Draft Federal Public Key Infrastructure Directory Profile, Version 2.5 (draft), 8 October 2002, http://www.cio.gov/fbca/documents/fpki_directory_profile.pdf
2. Draft Authentication and Identity Policy Framework For Federal Agencies, version 6, http://www.cio.gov/ficc/documents.htm
3. International Telecommunications Union – Telecommunications Sector (ITU T) Recommendation X.509 (1997) | ISO/IEC 9594 8: 1997, “Information technology - Open Systems Interconnection - The Directory: Authentication framework”, June 1997.
4. International Telecommunications Union – Telecommunications Sector (ITU T) Recommendation X.521 (1997) | ISO/IEC 9594-7: 1997, “Information technology - Open Systems Interconnection - The Directory: Selected object classes.
5.

The following Internet RFCs have been identified as sources of schema information:

6. RFC 1777: Lightweight Directory Access Protocol. W. Yeong, T. Howes, S. Kille. March 1995. (Format: TXT=45459 bytes) (Obsoletes RFC1487) (Status: DRAFT STANDARD)

7. RFC 2251: Lightweight Directory Access Protocol (v3). M. Wahl, T. Howes, S. Kille. December 1997. (Format: TXT=114488 bytes) (Status: PROPOSED STANDARD)

8. RFC 2559: Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2. S. Boeyen, T. Howes, P. Richard. April 1999. (Format: TXT=22889 bytes) (Updates RFC1778) (Status: PROPOSED STANDARD)

9. RFC 2587: Internet X.509 Public Key Infrastructure LDAPv2 Schema. S. Boeyen, T. Howes, P. Richard. June 1999. (Format: TXT=15102 bytes) (Status: PROPOSED STANDARD)

10. RFC 2798: Definition of the inetOrgPerson LDAP Object Class. M. Smith. April 2000. (Format: TXT=32929 bytes) (Status: INFORMATIONAL)

11. RFC 3494: Lightweight Directory Access Protocol version 2 (LDAPv2) to Historic Status. K. Zeilenga. March 2003. (Format: TXT=9225 bytes) (Obsoletes RFC1484, RFC1485, RFC1487, RFC1777, RFC1778, RFC1779, RFC1781, RFC2559) (Status: INFORMATIONAL)

The following RFCs are included by reference in the above mentioned RFCs:

12. RFC 1274: The COSINE and Internet X.500 Schema. P. Barker, S. Kille. November 1991. (Format: TXT=92827 bytes) (Status: PROPOSED STANDARD)

13. RFC 2079: Definition of an X.500 Attribute Type and an Object Class to Hold Uniform Resource Identifiers (URIs). M. Smith. January 1997. (Format: TXT=8757 bytes) (Status: PROPOSED STANDARD)

14. RFC 2256: A Summary of the X.500(96) User Schema for use with LDAPv3. M. Wahl. December 1997. (Format: TXT=32377 bytes) (Status: PROPOSED STANDARD)

15. RFC 3377: Lightweight Directory Access Protocol (v3): Technical Specification. J. Hodges, R. Morgan. September 2002. (Format: TXT=9981 bytes) (Updates RFC2251, RFC2252, RFC2253, RFC2254, RFC2255, RFC2256, RFC2829, RFC2830) (Status: PROPOSED STANDARD)

16. RFC 3280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile. R. Housley, W. Ford, W. Polk, D. Solo. April 2002. (Format: TXT=278438 bytes) (Obsoletes RFC2459)(Status: PROPOSED STANDARD)