



**FBCA Cross-Certification  
Technical Guide**

**for**

**Certificate Authority Vendors & Applicants**

November 13, 2003

**Prepared by:**

**Mitretek Systems**

3150 Fairview Park Drive

Falls Church, VA 22042

**Prepared For:**

**General Services Administration**

## Table of Contents

<b>1.</b>	<b>BACKGROUND .....</b>	<b>1</b>
<b>2.</b>	<b>EXCHANGE OF PKI CERTIFICATES.....</b>	<b>1</b>
<b>3.</b>	<b>DIRECTORY INTEROPERABILITY .....</b>	<b>3</b>
<b>3.1</b>	<b>DSP CHAINING.....</b>	<b>3</b>
<b>3.2</b>	<b>LDAP .....</b>	<b>3</b>
<b>4.</b>	<b>VALIDATION OF CA CERTIFICATES AND CROSS-CERTIFICATES.....</b>	<b>4</b>
<b>5.</b>	<b>LESSONS LEARNED AND SUMMARY OF COMMON ISSUES .....</b>	<b>4</b>

## 1. Background

The General Services Administration, as the Federal Bridge Certification Authority Operational Authority (FBCA OA), has contracted with Mitretek Systems to perform cross-certification testing in the Prototype FBCA to: 1) identify and resolve potential incompatibilities between the Public Key Infrastructure (PKI) technologies of the FBCA and the candidate, and 2) to minimize the risk of cross-certified Certification Authorities already in the Production FBCA.

In order to attain technical interoperability with the FBCA, the Applicant PKI and the FBCA OA undertake a cross-certification test with the Prototype FBCA. This process must demonstrate:

- a. Successful exchange of PKI certificates,
- b. Directory interoperability, and
- c. The ability of each party to validate the other's Certificate Authority (CA) certificates and cross certificates (this is an end-entity activity, for which the FBCA OA may, at the applicant's request, offer assistance).

## 2. Exchange of PKI Certificates

For full cross-certification to be completed, the FBCA and the Applicant PKI must send a cross-certificate request to each other and sign them respectively. The entire process is shown in Figure 1.

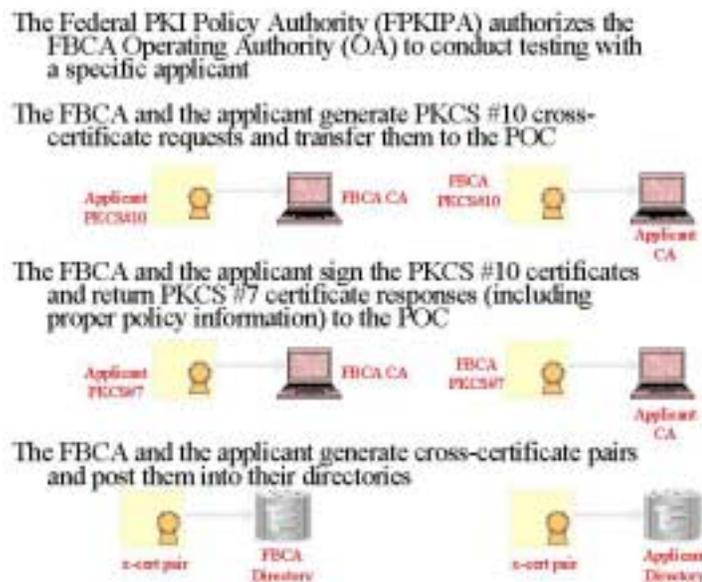


Figure 1. Cross-Certification Process

When signing the request, the following information will be used:

**Certificate Polices:** (These OIDS are for testing purposes only)

2.16.840.1.101.3.2.1.48.1

2.16.840.1.101.3.2.1.48.2

**Policy Mapping:** (These OIDS are for testing purposes only)

2.16.840.1.101.3.2.1.48.1 to

2.16.840.1.101.3.2.1.48.7

and

2.16.840.1.101.3.2.1.48.2 to

2.16.840.1.101.3.2.1.48.8

**Name Constraints:** (These values are for testing purposes only)

Permitted Subtrees:

"c=us, o=U.S. Government, ou=Commerce"

"dc=commerce, dc=gov"

"dc=nist, dc=gov"

Excluded Subtrees:

"c=us, o=U.S. Government, ou=Commerce, ou=PTO"

"dc=pto, dc=gov"

Once cross-certification is complete in both directions, the Applicant PKI will create a cross-certificate pair to post into their directory. The Applicant PKI may request the FBCA OA to generate a cross certificate pair. Updated Certificate Revocation Lists (CRLs) and CA Certificates must also be published to this directory. In order to post these attributes to the directory, at a minimum, the following object classes are required:

*pkICA* (defined in RFC 2587), or

*entrustCA* (defined in Entrust Directory Schema Requirements)

BCA CA (including PCAs and PAAs) entries in the directory shall contain at a minimum the following attributes:

*commonName* OR *organizationalUnit* (defined in X.509 – OIDs: 2.5.4.3 and 2.5.4.11)

*cACertificate* (X.509 – OID: 2.5.4.37)

*certificateRevocationList* (X.509 – OID: 2.5.4.39)

*crossCertificatePair* (X.509 – OID: 2.5.4.40)

CAs entries in the directory may optionally contain:

*authorityRevocationList* (X.509 – OID: 2.5.4.38).

### **3. Directory Interoperability**

A paramount component of the cross-certification test requires that Applicant and FBCA directories be either Directory Service Protocol (DSP) chained or be accessible via Lightweight Directory Access Protocol (LDAP).

#### **3.1 DSP Chaining**

In order for Applicants to chain to the FBCA directory, the following is needed:

1. IP address of the directory: 141.156.158.79
2. DSP port number: 102
3. DSP Transport Selector (TSEL) value: 1001 (text)
4. The base Distinguished Name (DN) of the directory: "c=us"
5. The base Distinguished Name (DN) of the CA: "ou=FBCAProto, ou=fbca, o=u.s. government, c=us"
6. DSA name: "cn=dsa, ou=fbca, o=u.s. government, c=us"

It is recommended that the Applicant's directory use a superior reference when chaining to the FBCA (provided the directory base DN is under the c=US namespace). A superior reference will allow Applicants to make one reference to the FBCA directory for any unknown DNs (e.g., other cross-certified entities). Otherwise, an Applicant's directory may make a reference to the FBCA directory for each of the cross-certified entities (depending on the product limitations).

In order for directories to chain via DSP, the Applicant must send the FBCA OA the following information:

1. IP address of the directory
2. DSP port number
3. DSP Transport Selector (TSEL) value (if applicable)
4. The base Distinguished Name (DN) of the directory

#### **3.2 LDAP**

Applicants that do not have X.500 (DSP capability) directories must interoperate with the FBCA using the Lightweight Directory Access Protocol (LDAP). When using LDAP directories, Applicants must have a method to query the FBCA directory following unsuccessful queries to its default directory. This is generally accomplished by referrals or by a directory that is capable of "LDAP chaining".

The FBCA directory information that is necessary for the Applicant is as follows:

1. IP address of the directory: 141.156.158.78
2. LDAP port number: 389
3. The base Distinguished Name (DN) of the FBCA directory: "c=us"

4. The base Distinguished Name (DN) of the FBCA CA: "ou=FBCAProto, ou=fbca, o=u.s. government, c=us"

In order for the directories to chain via LDAP, the Applicant must send the FBCA OA the following information:

1. IP address of the entity directory
2. LDAP port number of the entity directory
3. The base Distinguished Name (DN) of the entity directory

#### **4. Validation of CA Certificates and Cross-Certificates**

The FBCA OA uses a tool called CAM (Certificate Arbitrator Module) to ensure that validation can occur across the FBCA. This tool is used for each applicant after the cross-certification test has been completed. Applicants are encouraged to use other applications to check the validation process; as on occasion, CAM is not able to validate certificates. If CAM is not able to complete the validation, the applicant may optionally decide to conduct testing on their own (with the authorized support of the FBCA OA).

The FBCA OA team has been working on a production validation service that can be used for this task; however, this has not been completed at this time.

#### **5. Lessons Learned and Summary of Common Issues**

During cross-certification tests with Applicants, a number of issues have been encountered, often requiring a lot of time and/or support in order to be resolved.

The following list identifies those common issues and briefly describes their resolution. Applicant entities are strongly encouraged to review this list prior to testing, in order to assure a smooth and rapid test:

1. **Firewall settings regarding directory interoperability**

The firewalls protecting the directories must be opened up to allow chaining to take place on the correct DSP and/or LDAP port.

2. **Load Balancing issues regarding chaining**

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

3. **PKCS #10 cross-certificate request**

Some CAs do not produce properly formatted PKCS #10 cross-certificate requests. In this case, a PKCS #10 request must be manually generated.

4. **Directory chaining issues**

Each directory uses different formatting when inputting directory chaining information. It often takes technical support from the directory vendor to determine proper implementation of a chaining agreement.