FBCA and C4CA Cross-Certification Technical Guide

March 2007

Prepared by:

Noblis, Inc

3150 Fairview Park Drive

Falls Church, VA 22042

Prepared For:

General Services Administration

Table of Contents

1. Background

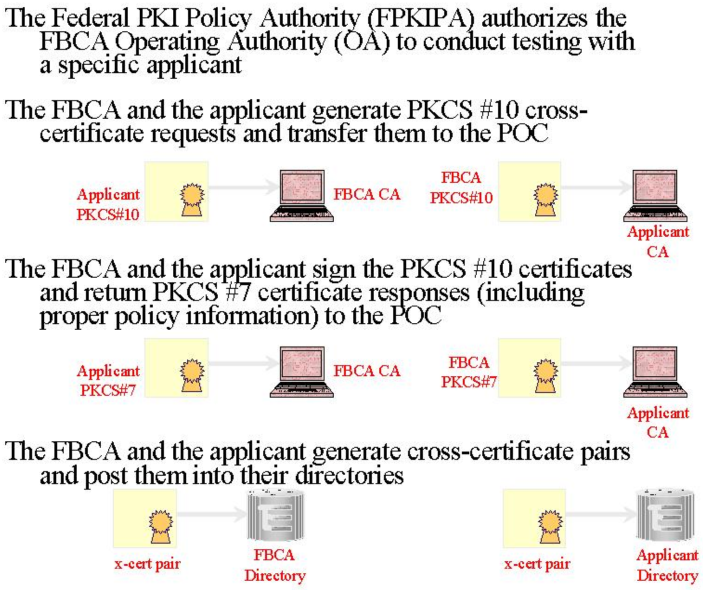
The General Services Administration, as the Federal Public Key Infrastructure Operational Authority (FPKI OA) performs cross-certification testing in the Lab FPKIA (Federal Public Key Infrastructure Architecture) to: 1) identify and resolve potential incompatibilities between the PKI technologies of the FBCA/C4CA and the candidate, and 2) to minimize the risk to other cross-certified Certification Authorities already in the Production FPKIA.

In order to attain technical interoperability with the FBCA or C4CA, the Applicant PKI and the FPKI OA undertake a cross-certification and directory tests with the FPKIA Lab's FBCA or C4CA, respectively. 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 FPKI OA may, at the Applicant PKI's request, offer assistance).

2. Exchange of PKI Certificates

For full cross-certification to be completed, the FBCA or C4CA and the Applicant PKI must send a cross-certificate request to each other and sign them respectively. The entire process for the FBCA is shown in Figure 1; this is the same process for the C4CA.



The Federal PKI Policy Authority (FPKIPA) authorizes the FBCA Operating Authority (OA) to conduct testing with a specific applicant

The FBCA and the applicant generate PKCS #10 cross-certificate requests and transfer them to the POC

The FBCA and the applicant sign the PKCS #10 certificates and return PKCS #7 certificate responses (including proper policy information) to the POC

The FBCA and the applicant generate cross-certificate pairs and post them into their directories

Figure 1. Cross-Certification Process

The following information will be used by the FPKI OA to construct the test cross-certificate issued to the entity (based on the appropriate requested policy levels):

Certificate Polices: The FPKIA lab will use test policy OIDs in all cross-certificates. The applicable policy OIDs from the below list will be used:

2.16.840.1.101.3.2.1.48.1 (FBCA Rudimentary Test OID)
2.16.840.1.101.3.2.1.48.2 (FBCA Basic Test OID)
2.16.840.1.101.3.2.1.48.3 (FBCA Medium Test OID)
2.16.840.1.101.3.2.1.48.4 (FBCA Medium Hardware Test OID)
2.16.840.1.101.3.2.1.48.5 (FBCA Medium CBP Test OID)
2.16.840.1.101.3.2.1.48.6 (FBCA Medium Hardware CBP Test OID)
2.16.840.1.101.3.2.1.48.7 (FBCA High Test OID)
2.16.840.1.101.3.2.1.48.17 (Citizen & Commerce Provisional Test OID)
2.16.840.1.101.3.2.1.48.18 (Citizen & Commerce Approved Test OID)

Policy Mapping: Each policy OID in the FPKIA Lab-issued test cross-certificate will have at least one corresponding policy mappings below. A policy mapping states how the test FBCA or the test C4CA views the equivalency of the Applicant PKI's policy, and consists of the "issuerDomainPolicy" and "subjectDomainPolicy" OID values. The subjectDomainPolicy OID in each set will be provided by the Applicant PKI as the entity's "test OID". If an entity does not have a test OID, the FPKI OA will work with the National Institute of Standards and Technology (NIST) to have one assigned. A cross-certificate containing two policy mappings will have the following form:

issuerDomainPolicy: 2.16.840.1.101.3.2.1.48.1
subjectDomainPolicy: 2.16.840.1.101.3.2.1.48.xx

and

issuerDomainPolicy: 2.16.840.1.101.3.2.1.48.2
subjectDomainPolicy: 2.16.840.1.101.3.2.1.48.yy

Name Constraints: The following name constraints will appear in FPKIA Lab issued test cross-certificates (typically the issuer's subtree is included in the name constraints "Excluded Subtrees" to ensure that trust within the domain is handled internally)

Excluded Subtrees:

"c=US, o=U.S. Government, ou=FBCA"
"dc=gov"

Authority Information Access (AIA): The following values will be present in all test cross-certificates issued by the FPKIA Lab CAs:

For FBCA:

```
ldap://fbcadir.mitretek.org/cn=FBCAProto,ou=FBCA,o=U.S.%20Government
,c=US?cACertificate;binary,crossCertificatePair;binary
http://fbcadir.mitretek.org/FBCAproto/CAcertsIssuedToFBCAproto.p7c
```

For C4CA:

```
ldap://fbcadir.mitretek.org/cn=C4CA,ou=FBCA,o=U.S.%20Government,c=US
?cACertificate;binary,crossCertificatePair;binary
```

Subject Information Access (SIA): This value will be present in all test issued cross-certificates. The value will be provided by the Applicant PKI, and should match the LDAP-URI in the AIA field of the Applicant PKI-issued cross-certificate. It should have the form:

```
ldap://ApplicantDir.Applicant.gov/cn=ApplicantCAcnRDN,ou=Applicant%2
0CA,o=U.S.%20Government,c=US?cACertificate;binary,crossCertificatePa
ir;binary
```

Certification Revocation List (CRL) **Distribution Point** (CDP): The CDP field must contain an LDAP URI. The FPKIA Lab-issued test cross-certificate additionally contains option HTTP URI and DN entries:

```
DirName:/C=US/O=U.S. Government/OU=FBCA/OU=FBCAProto/CN=CRL1
URI:ldap://fbcadir.mitretek.org/ou=FBCAProto,ou=FBCA,o=U.S.%20Govern
ment,c=US?certificateRevocationList
URI:http://fbcadir.mitretek.org/CRL/FBCAproto1.crl
```

The Applicant PKI will be expected to create a test cross-certificate back to the FPKIA Lab CA using the reverse values, for example:

Certificate Polices: It is strongly encouraged that the Applicant PKI use test policy OIDs and not production[1] policy OIDs in this phase of interoperability testing. If the Applicant PKI does not have their own set of test policy OIDs, the FPKI OA will work with NIST to provide test policy OIDs under the 2.16.840.1.101.3.2.1.48 arc.

Policy Mapping: Each certificate policy OID in the Applicant PKI issued test cross-certificate should have at least one corresponding policymappings. The issuerDomainPolicy will hold an Applicant PKI's test policy OID and the subjectDomainPolicy will hold an FPKI test policy OID. Therefore, the policy mapping should have the general format:

issuerDomainPolicy: 2.16.840.1.101.3.2.1.48.xx

[1] Certificate policy OIDs represent the terms and conditions under which the certificates were issued and the CA operates. Since the Applicant PKI's testing environment is usually not operated in as stringent conditions as their production environment, it would be inappropriate to express production policy OIDs in the testing environment CA.

subjectDomainPolicy: 2.16.840.1.101.3.2.1.48.1

and

issuerDomainPolicy: 2.16.840.1.101.3.2.1.48.yy
subjectDomainPolicy: 2.16.840.1.101.3.2.1.48.2

Name Constraints: The Applicant PKI may wish to express permitted DN subtrees or excluded DN subtrees. The following examples are for testing purposes only and are used to demonstrate functionality:

Permitted Subtrees:
"c=US, o=U.S. Government"
"dc=gov"

Excluded Subtrees:
"c=US, o=U.S. Government, ou=Applicant CA"
"dc=applicant, dc=gov"

Authority Information Access (AIA): This value must be present in all test cross-certificates issued by the Applicant PKI's CA. An LDAP URI is required:

```
ldap://ApplicantDir.Applicant.gov/cn=ApplicantCAcnRDN,ou=Applicant%2
0CA,o=U.S.%20Government,c=US?cACertificate;binary,crossCertificatePa
ir;binary
```

Subject Information Access (SIA): This value will be present in all test cross-certificates issued by the Applicant PKI CA and should match the LDAP URI value in the FPKIA CA's AIA field:

For FBCA:

```
ldap://fbcadir.mitretek.org/cn=FBCAProto,ou=FBCA,o=U.S.%20Government
,c=US?cACertificate;binary,crossCertificatePair;binary
```

For C4CA:

```
ldap://fbcadir.mitretek.org/cn=C4CA,ou=FBCA,o=U.S.%20Government,c=US
?cACertificate;binary,crossCertificatePair;binary
```

CRL Distribution Point (CDP): The Applicant PKI issued test cross-certificate must contain a LDAP URI entry in the CDP field. It is also strongly recommended that a DN entry also be included. Thus, a representative CDP extension would have the values:

```
URI:ldap://ApplicantDir.applicant.gov/cn=ApplicantCAcnRDN,ou=Applica
nt%20CA,o=U.S.%20Government,c=US?certificateRevocationList
DirName:/c=US/o=U.S. Government/ou=Applicant CA/cn=ApplicantCAcnRDN/
cn=CRL1
```

Once cross-certification is complete in both directions, the Applicant PKI will create a test cross-certificate pair to post into their certificate directory. (Optionally, the Applicant PKI may request the FPKIA Lab test FBCA or test C4CA to generate a test cross certificate pair for posting in the Applicant certificate directory.) Updated Certificate Revocation Lists (CRLs) and CA Certificates must also be published in this certificate 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)

FBCA 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).

* If the Applicant PKI CA is Entrust, the KeyIDMode must be set to 1 before signing the PKCS#10. Assistance will be provided on how this is accomplished upon request. Also, please provide the KeyIDMode that was used when generating the CA (using ‘db get keyidmode’ at the Entrust Command Shell prompt).

3. Directory Interoperability

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

3.1 DSP Chaining

In order for Applicant PKIs to chain to the FPKIA Lab directory, the following is needed:

1. DNS name of the directory: fbcadir.mitretek.org
2. DSP port number:
    a. Geopolitical naming (serving the “c=US” DSA) - 102
    b. Domain Component Naming (serving the “dc=gov” DSA) - 19999
3. DSP Transport Selector (TSEL) value: 1001 (text)
4. The base Distinguished Name (DN) of the directory (root:
    a. Geopolitical naming – "c=US"
    b. Domain Component naming – “dc=gov”

5. The base Distinguished Name (DN) of the FBCA: "ou=FBCAProto, ou=FBCA, o=U.S. Government, c=US" or the base Distinguished Name (DN) of the C4CA: "ou=C4CA, ou=FBCA, o=U.S. Government, c=US"
6. DSA name:
    a. Geopolitical naming – “cn=dsa, c=US”
    b. Domain Component naming – “cn=dsa, dc=gov”

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

In order for directories to chain via DSP, the Applicant PKI must send the FPKI 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

Applicant PKIs 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, Applicant PKIs must have a method to query the FPKIA lab 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 FPKIA lab directory information that is necessary for the Applicant PKI is as follows:

1. IP address of the directory: fbcadir.mitretek.org
2. LDAP port number:
    a. 389 for queries under “c=US”;
    b. 19389 for queries under “dc=gov”
3. The base Distinguished Name (DN) of the FPKIA Lab directory:
    a. Geopolitical naming – "c=US"
    b. Domain Component naming – “dc=gov”
4. The base Distinguished Name (DN) of the FBCA: "ou=FBCAProto, ou=FBCA, o=U.S. Government, c=US" or the base Distinguished Name (DN) of the C4CA: "ou=C4CA, ou=FBCA, o=U.S. Government, c=US"

In order for the directories to chain via LDAP, the Applicant PKI must send the FPKI 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. Application Testing

The FPKI OA will assist the Applicant PKI with testing path discovery and/or validation applications upon request.

5. Lessons Learned and Summary of Common Issues

During cross-certification tests with Applicant PKIs, 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 PKI entities are strongly encouraged to review this list prior to testing, in order to assure a smooth and rapid test:

1. **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, and should contain, at a minimum, the full DN of the CA, the CA's public key, the CA-generated Subject Key Information (SKI) extension, and a signature enveloping certificate request.

2. **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.

   Complications with directory interoperability may occur if subordinate/superior references cannot be created.

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

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

   If the prospective entity directory uses LDAP technology (and does not support X.500 DSP chaining or other proprietary "LDAP chaining") then there must be some mechanism supplied to their users to gain access to the FPKIA Directory.

3. Path Discovery and Validation issues

SubjectKeyIdentifier/authorityKeyIdentifier (SKI/AKI) matching – in many known instances, SKI /AKI doesn’t match in cross-certificates which will cause path discovery to be arduous.

Full URI extensions - *authorityInformationAccess* (AIA), *subjectInformationAccess* (SIA) and *cRLDistributionPoint* (CDP) should contain properly encoded full URIs in order to support path discovery and path validation functionality.

Some applications (including Microsoft CAPI) require cross-certificates to be included in the *cACertificate* attribute, rather than the *crossCertificatePair* attribute. A good practice is to place the Cross-Certificates in both attributes and set the AIA and SIA extensions accordingly.

4. Certificate Profile Conformance

Some CAs do not have documentation to assist with including extensions such as the *SubjectInformationAccess* field. This extension can be included in certificates issued from a Microsoft CA using the following process:

Once a request has been submitted to the Microsoft CA, at a command prompt, enter the command:

```
certutil.exe -setextension <Request-ID> 1.3.6.1.5.5.7.1.11 0
@DerEncodedValue.txt
```

where “DerEncodedValue.txt” is a file in the same folder that contains the DER encoded value of the SIA extension to be included in the issued certificate.