

APPLICATION

FOR

CROSS CERTIFICATION

WITH THE

FEDERAL BRIDGE CERTIFICATION

AUTHORITY

Instructions for Completing Form

Applicant should submit the information requested in this form either using separate pieces of paper, or in an electronic format (Microsoft Word format). The completed application should be mailed to the Chair, Federal Public Key Infrastructure Policy Authority, Michelle Moldenhauer, 1500 Pennsylvania Avenue, NW, Room 3090 Annex, Washington DC 20220. Applications can also be accepted electronically through michelle.moldenhauer@do.treas.gov and through fpki.webmaster@gsa.gov.

1. INFORMATION ON THE APPLICANT'S ORGANIZATION

Applicant Organization Name

Applicant Organization Address

Applicant Organization's Representative or Designated Agent

Name and Title

Postal Address with Zip Code

Office Phone Number

Office E-mail Address

Applicant Organization's Secondary Contact(s) (to be used if Representative or Designated Agent cannot be reached)

Name(s) and Title(s)

Postal Address with Zip Code

Office Phone Number

Office E-mail Address

2. INFORMATION ON THE APPLICANT'S CERTIFICATE POLICY AND CERTIFICATION PRACTICES STATEMENT

(The Applicant's Certificate Policy and Certification Practices Statement for the Certification Authority to be cross-certified with the FBCA (hereinafter referred to as the "Principal CA"), must be attached for this application to be considered. The Applicant may also include any other relevant documentation deemed appropriate.)

Please indicate whether the attached Certificate Policy conforms with the X.509 standard and is in PKIX part IV format. If not, please explain how the Certificate Policy differs from the X.509 standard, and how its contents map to the elements contained in the PKIX part IV format.

For the Principal CA, please ensure the following information is provided either as part of the CP, CPS or separately:

Principal CA product employed including configuration information

Principal CA hardware platform including operating system configuration

Signature and encryption algorithms supported

Directory product employed including configuration information

3. INFORMATION ON THE APPLICANT'S PKI ARCHITECTURE

For applications involving interoperability at the "Basic," "Medium," or "High" levels of assurance:

a. Provide a list of those CAs under the Applicant's control which are either subordinate to, or have any other trust relationship with, the Applicant's Principal CA. If any of those CAs provides certificates asserting object identifiers not covered in the attached CP, provide a copy of the relevant CP under which those OIDs are defined.

b. Provide a list of those CAs not under the Applicant's control which have any trust relationship (e.g., cross-certificate) with the Applicant's Principal CA or any CA under the Applicant's control that is subordinate to, or has any other trust relationship with, the Applicant's Principal CA.

c. Briefly describe each application within the Applicant's organization currently supported by the Applicant's PKI as encompassed within the attached CP and CPS. This should include any CAs under the control of the Applicant which are subordinate to or have any other trust relationship with the Applicant's Principal CA.

4. INFORMATION ON APPLICANT'S DIRECTORY ARCHITECTURE

Describe the Applicant's directory structure and how the Applicant will accomplish interoperability with the FBCA directory. For applications involving interoperability at the "Basic," "Medium" or "High" levels of assurance, describe how the Applicant will ensure proper namespace control for distinguished naming.

5. INFORMATION ON THE APPLICANT'S AUDITING PRACTICES

For applications involving interoperability at the "Basic," "Medium," or "High" levels of assurance, describe how the Principal CA, and any other CA under the control of the Applicant which is subordinate to or has any other trust relationship with the Principal CA, is audited. This should include who performs the audits, and their frequency. Attach a copy of the latest audit report attesting to compliance with the Applicant's CP and CPS.

6. INFORMATION ON CERTIFICATE POLICY MAPPING

State what mapping(s) the Applicant proposes between the certificate levels of assurance covered under the Applicant’s CP, and those set forth in the FBCA CP. For any proposed mapping at the “Basic,” “Medium,” or “High” levels of assurance, explain the basis for the proposed mapping(s) by comparing the two CPs and providing whatever other information the Applicant deems relevant.

7. INFORMATION ON TECHNICAL CONFIGURATION

For applications involving interoperability at the “Basic,” “Medium,” or “High” levels of assurance:

a. Please indicate whether the Applicant’s Principal CA, and any other CA under the control of the Applicant which is subordinate to or has any other trust relationship with the Principal CA, employs digital signature key generation and signing operations in a hardware cryptographic module meeting FIPS 140, and if so, at what level of assurance. If a module is used that does not meet FIPS 140, please describe in detail the nature of the module and why it should be considered as acceptable.

b. Please indicate whether the Applicant is producing or has the ability to produce certificates conforming to the Federal PKI Certificate Profile respecting extensions, available at http://www.cio.gov/fbca/documents/product_guidance_rev9-26.pdf or http://www.cio.gov/fbca/documents/product_guidance_rev9-26.doc.

c. Please indicate which algorithms are used by the Applicant’s Principal CA, and any other CA under the control of the Applicant which is subordinate to or has any trust relationship with the Principal CA, for signature and encryption. Please indicate whether the signature algorithms are executed in conformance with FIPS 186; if not, please explain how they are performed so as to provide a comparable or superior level of assurance.

The above information is true and correct to the best of my knowledge and belief.

Signed: _____
Applicant’s Authorized Official
(Print name and title)

Date: _____