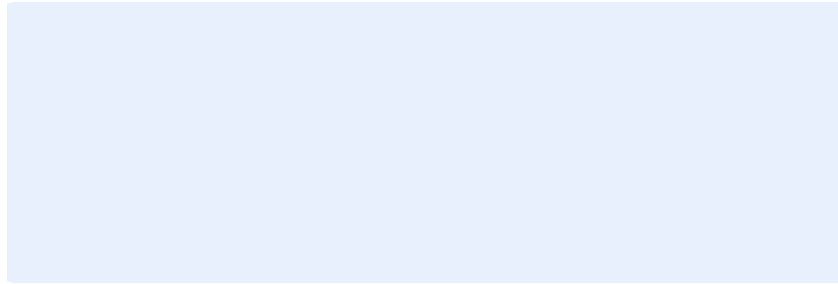


**Application For
Membership in the
CertiPath Trust Community
via
Cross-certification with the CertiPath Bridge CA
or
Subordination under the CertiPath Root CA**



Applicant's Date of Submission: [Click here to enter a date](#)

Approved by CertiPath PMA on: [Click here to enter a date](#)

CertiPath
www.certipath.com

1. Information on the Applicant's Organization

Applicant Organization

Organization's Legal Name

**(Optional) Reason for
Interest in Becoming a
Member of the
CertiPath Trust
Community**

**Applicant's Primary
Contact**

Name and Title
Postal Address with Zip Code
Office Phone Number
Office E-mail Address

**Applicant's Secondary
Contact**

Name and Title
Postal Address with Zip Code
Office Phone Number
Office E-mail Address

2. Information on the Applicant's Service Level Request

Type of Service Applied for:

Standard Service - Subordination to CertiPath's CRCA

CP Title, Version #, Effective Date *Please attach your CP as Appendix A*

Premium Service - Cross-certification to CertiPath's CBCA

CP Title, Version #, Effective Date *Please attach your CP as Appendix A*

Bridge Service - Cross-certification of a Bridge CA to the CBCA

CP Title, Version #, Effective Date *Please attach your CP as Appendix A*

Is this request for IceCAP (PIV-I) Certification?

Yes No

Does this request include CertiPath Certified Credential Provider (3CP) Certification?

Yes No

Encryption/Escrow Functionality: *Are you interested in encryption/escrow functionality compliant with CertiPath requirements as detailed in the CertiPath Key Recovery Policy?*

Yes

We desire the ability to issue encryption certificates and will perform key escrowing in conformance with CertiPath requirements. KRPS will be submitted to CertiPath for review.

No

We do not wish to issue encryption certificates at this time. We agree not to issue encryption certificates with an OID that has been or will be mapped to a CertiPath OID.

3. Information on the Applicant's PKI Architecture

Please attach a diagram of your CA architecture as Appendix B

Technical Considerations: *List specific technical aspects of your CA*

CA Software utilized with an overview of the configuration

CA OS and hardware utilized

Directory product utilized and any relevant configuration information

Security Considerations: *Provide information concerning the security architecture protecting your CA*

List all CAs that are subordinated to your Primary CA and to what degree they are under your direct control

List all CAs that are cross-certified to your Primary CA and to what degree they are under your direct control

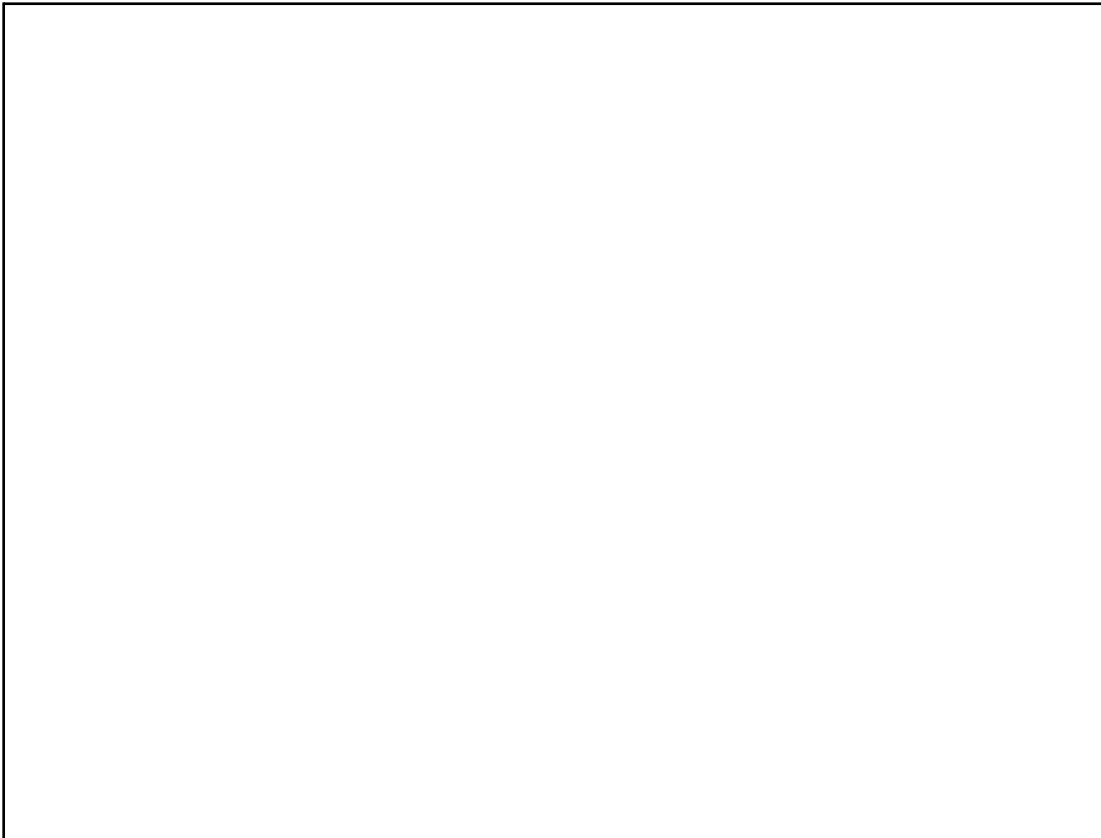
Describe network services and controls protecting your CAs

4. Information on the Applicant's Directory Architecture

Describe your directory structure and how you will accomplish interoperability with CertiPath's directory. *Please attach a Diagram of the Directory Schema as Appendix C*



Describe how you will ensure proper namespace control for distinguished naming.



5. Information on the Applicant's Credential Management Architecture (IceCAP Applications only)

This section is applicable to organizations seeking IceCAP certification. All others should mark this section N/A, and proceed to section 6.

Premium and Standard Service Applicants

Describe your identity management and credential issuance system architecture (inclusive of, but not limited to, the CMS) and how it ensures issuance of conformant IceCAP credentials.

Describe how your identity management and credential issuance system will ensure interoperability of your issued credentials with all other IceCAP credential issuers.

Describe the linkage of the CMS to identity information sources and how these two systems are maintained such that all appropriate systems remain synchronized.

At a minimum, include:

1. CMS vendor and version levels
2. Hardware security module for IceCAP-contentSigning keys
3. Hardware security module for card management keys
4. Smart card vendor and version levels
5. A list of all the products from the GSA FIPS 201 APL that are included in your architecture
6. System interface diagram for all connections between the CMS and related data sources
7. Network services and controls protecting your Credential Management capabilities

Bridge Service Applicants

Provide a plan for approval by CertiPath that:

1. Describes the procedures and practices that ensure that the Applicant Bridge's clients maintain identity management and credential issuance system architectures conformant with IceCAP mapped policies.
2. Provides your Test Plan and Procedures for interoperability at IceCAP LOA. This must describe the interoperability testing procedures that will maintain interoperability between the Bridge's clients and CertiPath's CBCA and CRCA clients.

6. Information on the Applicant's Auditing Practices

- We will employ the services of an Independent Third Party Audit Firm

- We will utilize the services of a Corporate Internal Auditor sufficiently organizationally independent as to meet the requirements of the CertiPath CP Section 8.3.

**Audit Organization
Name**

Organization's Legal Name

Lead Auditor

Name, Title of Lead Auditor
Lead Auditor Certifications (e.g. CISSP, CISA, CSCIP, etc.)
Domain expertise in IT Security
Domain expertise and practical experience in PKI
Years of experience performing IT audits
Years of experience performing security audits
Detail experience performing audits involving PKI or security key management processes
Detail a demonstrable knowledge of PKI CP and CPS
Detail a demonstrable knowledge of IdM-CIS and CMS systems integrated with CA systems

Staff Auditor(s)

Provide details as described above for any additional staff auditors that participate in the audit of your PKI.

Relationship

For Third Party Independent Auditors - Please attest that the compliance auditor works for a separate 3rd party operating entity, which is independent from your organization and any other affiliated entity that may be subject to audit in association with your PKI. See CertiPath CP Section 8 for details concerning independence.

For Enterprise Organizations utilizing a Corporate Independent Auditor, provide an organizational diagram showing points of intersection between the organization administering the PKI and the Corporate Independent Auditor and an attestation that the corporate internal auditor is organizationally independent.

7. Information on the Certificate Policy Mapping

Please select the mapping(s) you wish to pursue between the certificate levels of assurance covered under your CP, and those set forth in CertiPath's CP and listed below:

SHA 1 Infrastructure	SHA 256 Infrastructure
<input type="checkbox"/> Medium Software - id variant	<input type="checkbox"/> Medium Software

Medium Hardware - id variant

High Hardware - id variant

Medium Software CBP - id variant

Medium Hardware CBP - id variant

High Hardware CBP - id variant

Medium Hardware

High Hardware

IceCAP Hardware

IceCAP Card Authentication

IceCAP Content Signing

Medium Software CBP

Medium Hardware CBP

High Hardware CBP

8. Documents Attached (Please verify your CP/CPS is in RFC 3647 Format)

- Appendix A: *Premium and Bridge Applicants* - Certificate Policy**
- Appendix A: *Standard Applicants* - Certification Practices Statement**
- Appendix B: CA Architecture Diagram**
- Appendix C: Directory Schema**
- Appendix D: Key Recovery Practices Statement (optional)**
- Appendix E: *Bridge Applicants Only* – Applicant Bridge Criteria and Methodologies**

9. Signature

The undersigned is a duly authorized official of the Applicant's Organization and by signing this application confirms that all information within is correct and accurate.

X

Name

Title

Date: _____