

**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:

Approved by CertiPath PMA on:

CertiPath
www.certipath.com

1. Information on the Applicant's Organization

Applicant Organization

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

Applicant's Primary Contact

Applicant's Secondary Contact

2. Information on the Applicant's Service Level Request

Type of Service Applied for:

Standard Service - Subordination to CertiPath's CRCA

Please attach your CPS as Appendix A

Premium Service - Cross-certification to CertiPath's CBCA

Please attach your CP as Appendix A

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

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?*¹

Yes²

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.

¹ You can find the CertiPath Key Recovery Policy at https://certipath.com/pdfs/PMA/20220222_CertiPath-KRP_v1.6_signed.pdf

² If this option is elected, your audit must include an audit of the implementation of the KRPS. This option can be added at a later date (after cross-certification is achieved) if desired.

Bridge Service applicants should provide their Key Recovery Policy (if supported) for implementation of encryption certificates. Clearly describe mechanisms used to enforce KRP/KRPS capabilities. If Key Recovery is not supported by the Bridge, state that KRP/KRPS is not applicable.

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*



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



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*



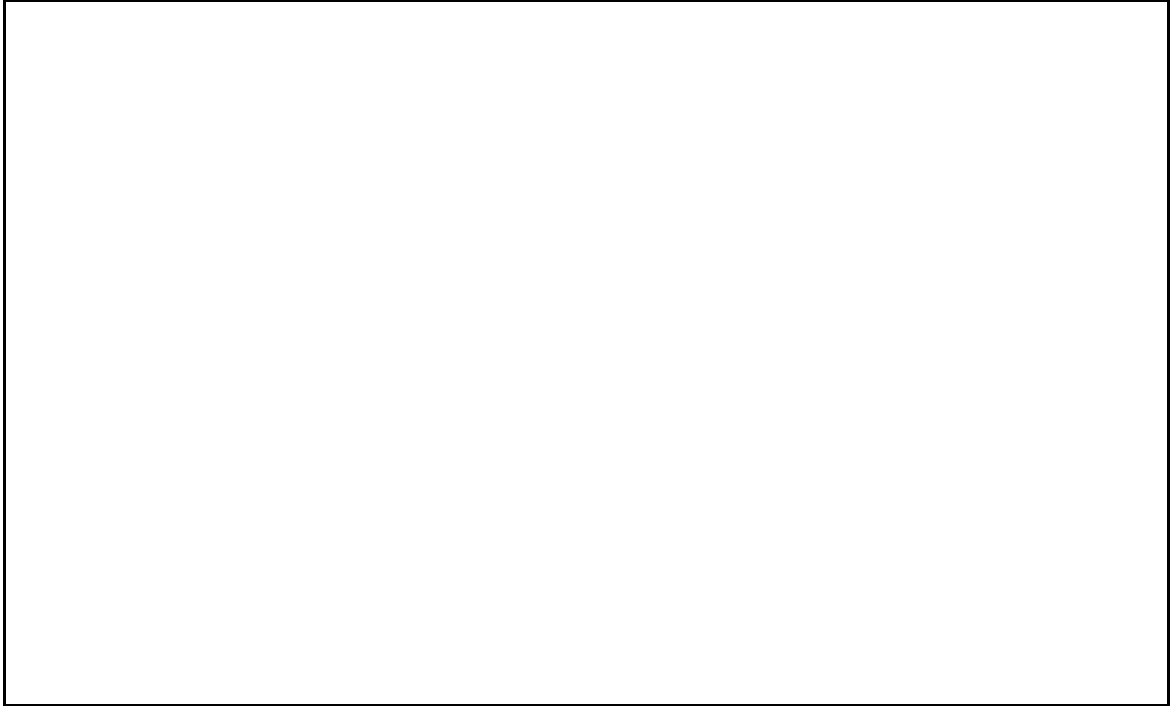
Describe how you will ensure proper namespace control for distinguished naming.



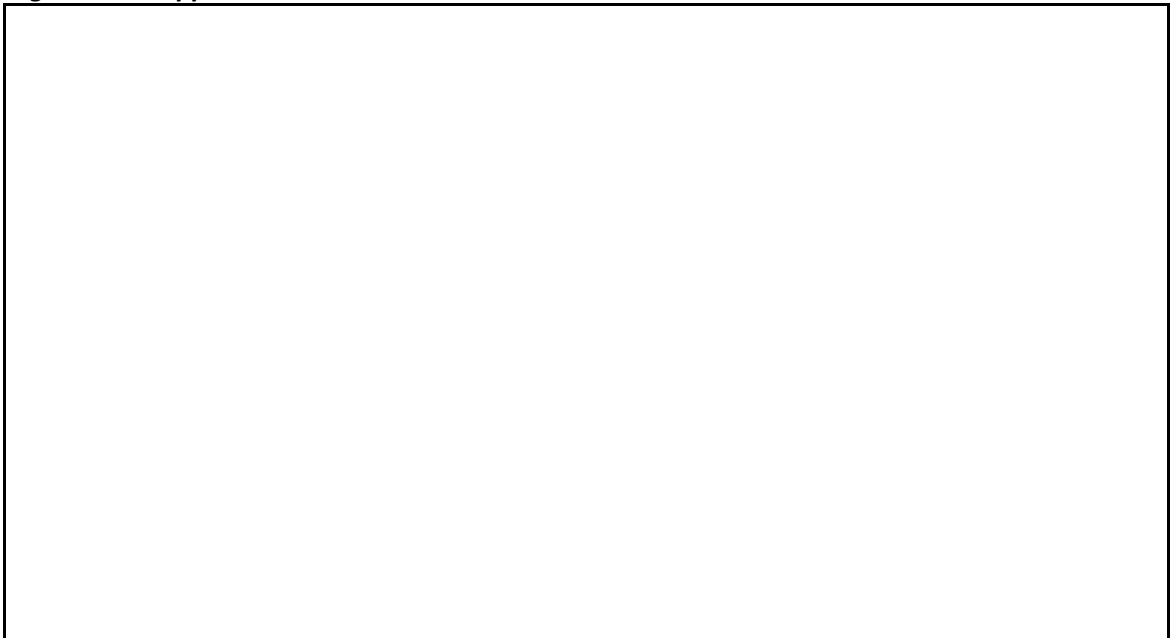
**5. Information on the Applicant's Credential Management Architecture
(IceCAP Applications only)**

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

A large, empty rectangular box with a black border, intended for providing information on the applicant's credential management architecture for Premium and Standard Service Applicants.

Bridge Service Applicants

A large, empty rectangular box with a black border, intended for providing information on the applicant's credential management architecture for Bridge Service Applicants.

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

Lead Auditor

Staff Auditor(s)

Relationship

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 or CPS, and those set forth in CertiPath's CP and listed below:



<input type="checkbox"/> Medium Software	<input type="checkbox"/> IceCAP Hardware
<input type="checkbox"/> Medium Hardware	<input type="checkbox"/> IceCAP Card Authentication
<input type="checkbox"/> High Hardware	<input type="checkbox"/> IceCAP Content Signing
<input type="checkbox"/> Medium Software CBP	
<input type="checkbox"/> Medium Hardware CBP	
<input type="checkbox"/> High Hardware CBP	
<input type="checkbox"/> Medium Device Software	
<input type="checkbox"/> Medium Device Hardware	

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

Check all that apply

- 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 _____

Date: _____