CertiPath
www.certipath.com

CertiPath PKI Criteria and Methodologies

Revision 1.2

August 27, 2014

Table of Contents

Change history:

Date	Version	Author	Reason
8/20/2012	v.1.0	J. Spencer	First Release of Document
4/22/2013	v.1.1	J. Spencer	Annual Review/Update
8/27/2014	v.1.2	J. Spencer	Annual Review/Update

1 Introduction

1.1 Objective

This document lists the criteria and methodologies used by CertiPath for cross certifications to the CertiPath Bridge Certification Authority (CBCA) and subordination to the CertiPath Root Certification Authority (CRCA). In addition, the criteria and methodologies address life cycle management of the cross certification and subordination relationships.

1.2 Background

Identity and Access Management present significant challenges for medium to large size organizations. These challenges are further complicated in a multi-enterprise environment where external parties are relying on computer based identities for enabling supply chain or extranet applications. Policy drivers addressing this space include U.S. government-wide mandates such as HSPD-12, which in turn spawned the National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 201, Office of Management and Budget requirements for two-factor access control to Federal government resources, the proliferation of technical requirements for strong identity credentials including NIST Special Publications and the Federal Chief Information Officers' (CIO) Council's *Personal Identity Verification Interoperability for Non-Federal Issuers* guidance, and the series of increasingly stringent access requirements coming from the U.S. Department of Defense (DOD) for government employees and contractors. Taken together, these documents describe a high-assurance Identity and Access Management strategy for use in both physical access and logical access environments. Organizations external to the U.S. Federal Government that wish to emulate the high-assurance Identity and Access Management strategy of the government must be cognizant of the contents of these documents and requirements stated therein.

Central to any high-assurance Identity and Access Management strategy is the use of Public Key Infrastructure (PKI) solutions. A PKI is comprised of one or more Certification Authorities (CA), which are used to issue Public-Key Certificates to an organization's employees and contractors, devices and even software components. In smaller organizations, this may be best accomplished by working with a managed service provider but for medium to large organizations, owning and operating a distinct PKI domain is typically economically and strategically advantageous. However, the real value of a public-key certificate cannot be fully realized unless it is used to verify identities during the normal conduct of business both inside and outside of the organization. This requires cross-organizational trust between the organization that issued the public-key certificate and the organization that is accepting it - a process known as Federation. It also requires the ability for the public-key enabled application to accept public-key certificates from multiple PKIs and is sometimes referred to as PKI or PK-enabled interoperability. The CRCA and CBCA leverage and extend organizational investments in PKI, establishing a federated environment by providing external interoperability and trust through the dual mechanisms of subordination and cross-certification of PKIs.

1.3 CertiPath Policy Management Authority

The CertiPath Policy Management Authority (CPMA) is comprised of the organizations cross-certified with the CBCA or subordinated to the CRCA. It is responsible for managing and maintaining the *CertiPath X.509 Certificate Policy* and approving new members for cross-certification with the CBCA or subordination to the CRCA.

The CPMA is an advisory group created by CertiPath, and CertiPath reserves the right to override CPMA decisions related to (i) policy, technical and business practices and issues related to the CBCA and/or

CRCA; and (ii) approval of applicants for cross-certification with the CBCA or subordination to the CRCA. In such instances, CertiPath will provide an explanation in writing to the CPMA.

1.4 Certificate Policy Working Group

The Certificate Policy Working Group (CPWG) is comprised of the CertiPath PKI Support Team. It performs day-to-day activities associated with the maintenance of cross certification and subordination relationships as well as performing document review and interoperability testing for cross certification and subordination, and annual renewal of both. The CPWG is primarily responsible for ensuring that the CertiPath documentation and guidelines promote secure federation of the PKIs; and secondarily that they maximize interoperability. The CPWG provides its work products to the CPMA for review and final disposition.

1.5 Intended Audience and Scope

This document is the intellectual property of CertiPath and is intended for the CertiPath membership, organizations interested in joining the CertiPath community, and the relying party community at large.

These cross certification and subordination guidelines should be read in conjunction with the *CertiPath X.509 Certificate Policy* [CertiPath CP].

1.6 General Principles

Subject to this document, CertiPath and the CPMA will consider applications for cross certification or subordination from any entity operating a CA.

Cross-certificates are issued and revoked by the CBCA at the sole discretion of CertiPath based on guidance from the CPMA. Any review by CertiPath and the CPMA of information from an applicant PKI is for use in determining whether or not cross certification is possible and appropriate – in short, whether the applicant PKI conforms to the requirements of the CertiPath CP for trust and interoperability.

Subordination CA certificates are issued and revoked by the CRCA at the sole discretion of CertiPath based on guidance from the CPMA. Any review by CertiPath and the CPMA of information from an applicant PKI is for use in determining whether or not subordination is possible and appropriate – in short, whether the applicant PKI meets the requirements of the CertiPath CP.

For CBCA cross certification, the CertiPath CPWG will conduct a review of the applicant's Certificate Policy in relation to the CertiPath X.509 Certificate Policy at the assurance levels requested in the application.

Similarly, applicants for CBCA cross certification should determine whether to reciprocally issue a cross certificate to CertiPath by conducting a review of the CertiPath X.509 Certificate Policy in relation to the applicant's own. The applicant must determine if the CertiPath CP provides criteria that meet the applicant's policy and legal requirements. CPWG review and mapping plus the CPMA acceptance of an applicant certificate policy is not a substitute for due care and mapping of certificate policies by the applicant.

For CRCA subordination, the CertiPath CPWG will conduct a review of the applicant's Certification Practices Statement (CPS) for conformance to the CertiPath CP. The CPS is reviewed by CertiPath for compliance with the CP and for the level of detail and the level of specificity to ensure that the controls used by the PKI operator will meet the CertiPath X.509 CP security and interoperability requirements. No reciprocal action is required on the part of the subordinating PKI.

Applicants for cross certification or subordination must provide independent third-party attestation to the adherence of the applicant's PKI operations to its certificate policy and CPS.

In addition, applicants for cross certification or subordination must successfully complete interoperability testing conducted by CertiPath, the results of which are shared with the CPMA and used in making the final determination to cross certify or subordinate.

Finally, all applicants for cross-certification must obtain unique policy Object Identifiers (OIDs) in the standard ISO object identifier registry from the appropriate commercial or national registration authorities.

2 Cross Certification Process

CertiPath offers two distinct federation opportunities to potential affiliates:

- Standard service, involving subordination to the CRCA; and
- Premium service, involving peer-to-peer cross certification with the CBCA. The Premium service is further separated into two categories:
    - Principal CA service and
    - Bridge CA service.

In addition, applicants for both services may elect the CertiPath Certified Credential Provider (3CP) option, for those applicants that wish to issue end user credentials on behalf of other organizations; and/or the IceCAP option, for those wishing to be certified as PIV-I providers.

Figure 1 below shows the process an organization requesting CertiPath's Standard Service would undertake to subordinate to the CRCA, and Figure 2 shows the process an organization requesting CertiPath's Premium Service would undertake to cross certify with the CBCA.

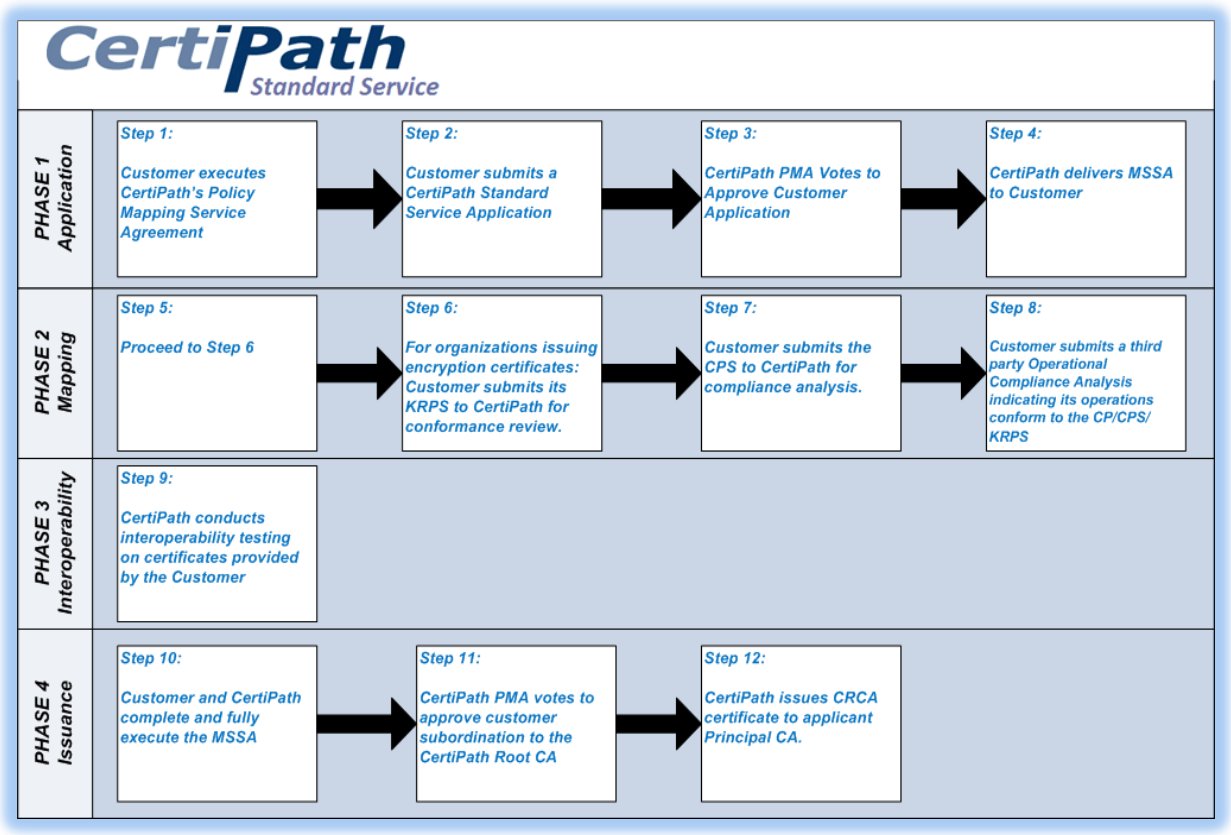

Figure 1: CertiPath Applicant CA Certification Process: Standard Service

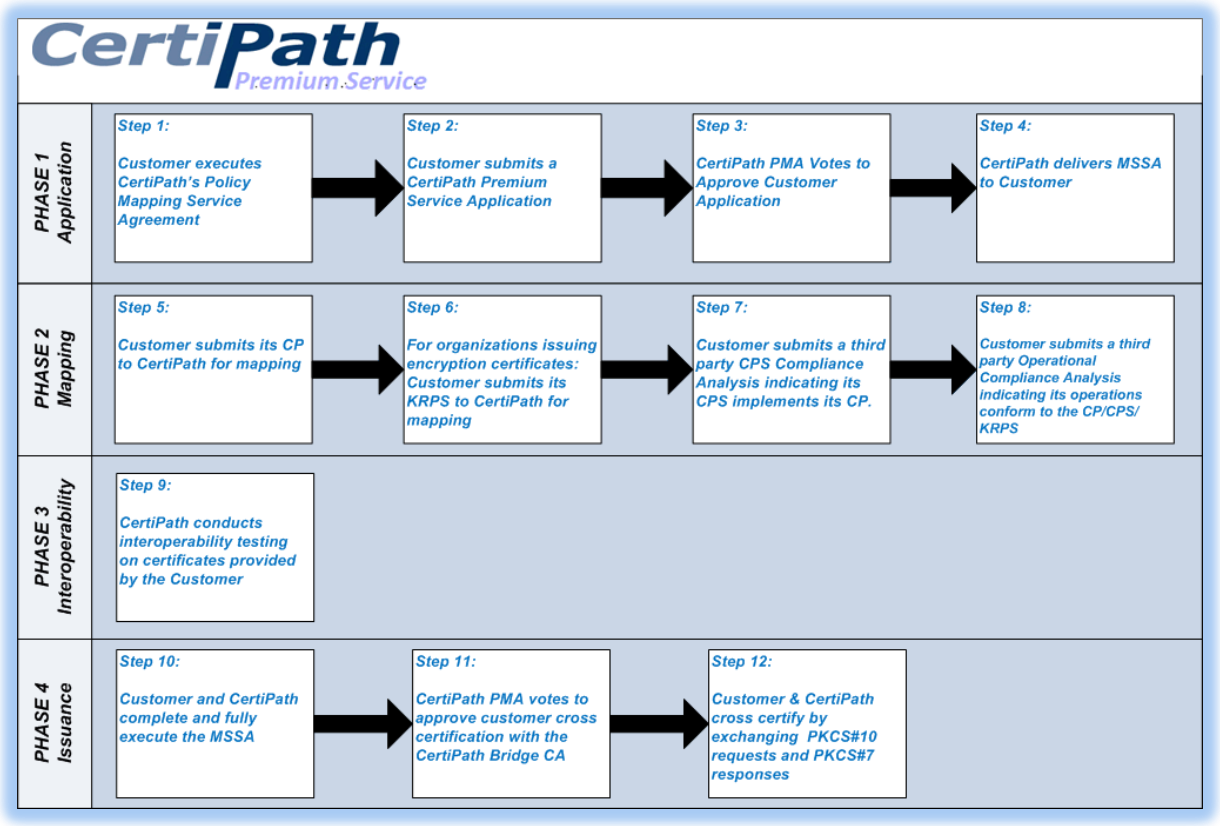

Figure 2: CertiPath Applicant CA Certification Process: Premium Service

2.1 Phase One: Application

2.1.1 Step 1: Executed Policy Mapping Service Agreement

CertiPath's Policy Mapping Service Agreement (PMSA) must be executed by the applicant before the application can be submitted to CertiPath's Policy Management Authority for approval. The PMSA includes an obligation of funds for the cross certification or subordination activities, which must be paid prior to application approval by the CPMA.

2.1.2 Step 2: Application

Once the PMSA has been executed, the next step for both Standard and Premium services applicants is submission of a formal application. An application template is provided for convenience on the CertiPath website (http://www.certipath.com/library/application-documents). The application must contain the following information:

2.1.2.1 Information on the Applicant's Organization

- The organization's legal name
- (Optional) Short description of the organization
- Two organization representatives: name and title, postal address, office phone and office e-mail address. These representatives should occupy positions in the organization whose primary responsibility relates to PKI and/or Identity Management for the organization. In addition, at least one should be a member of senior management within the organization, with oversight

responsibilities for PKI and/or Identity Management activities within the organization and authority to speak to issues pertaining to this subject on behalf of the organization. Upon successful completion of the cross certification process, it is expected that one of these individuals would be the designated CPMA voting member, while the other would be the alternate CPMA voting member.

2.1.2.2 Information on the Applicant's Service Level Request

Organizations must:

- Select the type of service they are applying for:
    - Standard Service – Subordination of a signing CA to CertiPath's CRCA.
    - Premium Service – Cross certification of a Principal CA by CertiPath's CBCA.
    - Bridge Service – Cross certification of a Bridge CA by CertiPath's CBCA.
- Declare whether they are also applying for 3CP recognition.
- Declare whether they are also applying to be an IceCAP (PIV-I) service provider.
- Declare whether the applicant organization will issue encryption certificates, and make an assertion concerning escrow functionality compliant with the CertiPath Key Recovery Policy (KRP). Entities applying for the IceCAP level of assurance *must* issue encryption certificates, for all others encryption certificates are optional:
    - If yes, the applicant must develop a Key Recovery Practices Statement (KRPS) that implements escrow functionality that is compliant with CertiPath standards as detailed in the CertiPath KRP.
    - The KRPS must be submitted to CertiPath as part of the application package for review during the mapping process. The submission of this document is covered by the confidentiality agreement between CertiPath and the applicant. It will not be shared with the CPMA or any other entity outside the CPWG.
    - The applicant must include KRPS compliance in the third party audit covering PKI operations before final approval will be granted.

  Note: Bridge applicants must clearly indicate whether or not they will support key recovery. In the event they do support key recovery, they must submit the Bridge's KRP.

2.1.2.3 Information on the Applicant's PKI Architecture

A diagram of the PKI Architecture and an in-depth description should be attached as Appendix B to the application. In addition, at a minimum, the following information should be provided in the application:

- Technical Considerations – An account of the specific technical aspects of the applicant organization's PKI, including:
    - CA software utilized with an overview of the configuration.
    - Hypervisor (if applicable) and Operating System the CA is running on and hardware utilized (including Hardware Security Module (HSM)).
    - Directory product utilized and any relevant configuration information.

- Online Certificate Status Protocol (OCSP) Responder product utilized and any relevant configuration information. An OCSP Responder is mandatory for the IceCAP assurance level, otherwise it is optional.

- Security Considerations – An account of the security architecture protecting the applicant organization's CAs, including:
  - A list of all CAs subordinate to or cross certified with the organization's Principal CA and to what degree the organization has control over these related CAs.
  - A list of all CAs cross certified with the Primary CA and to what degree they are under the applicant organization's direct control.
  - Network services and controls protecting the applicant organization's CAs.

2.1.2.4 Information on the Applicant's Directory Architecture

A diagram of the applicant organization's Directory Architecture should be attached as Appendix C to the application. In addition, at a minimum, the following information should be provided:

- The applicant must describe the organization's directory structure and how interoperability with CertiPath's directory requirements will be accomplished.
- The applicant must describe how namespace control will be achieved for ensuring unique distinguished naming within its PKI enterprise.

2.1.2.5 (IceCAP applicants only) Information on the Applicant's Credential Management Architecture

This section applies only to applicants seeking certification at the IceCAP levels of assurance. All others should mark this section N/A and proceed to Section 6 of the application.

Applicants for IceCAP Level of Assurance must:

- Describe the identity management and credential issuance system architecture (inclusive of but not limited to the Card Management System (CMS) and how it ensures issuance of conformant IceCAP credentials.
- Describe the ways the CMS will ensure the interoperability of credentials issued by the applicant with all other IceCAP conformant credential issuers.
- Describe the linkage of the CMS to identity information sources and how these two systems are maintained to ensure all appropriate systems remain synchronized.

At a minimum, the following information must be included:

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

Bridges seeking IceCAP approval must provide a plan for approval by CertiPath that:

- 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.
- Provides the applicant Bridge's test plan and procedures for interoperability at the IceCAP LOA. The Test Plan must describe the interoperability testing procedures that will maintain interoperability between the end relying parties served by the Bridge and the end relying parties served by CertiPath's CBCA and CRCA.

2.1.2.6 Information on the Applicant's Auditing Practices

Applicants must employ the services of an auditor to provide an independent analysis of the compliance of the applicant's Certification Practices Statement to the governing Certificate Policy and an assessment of whether the PKI operations implement the Certification Practices Statement. The auditor may be either an independent third party entity with no relationship to the Applicant's organization or a Corporate Internal Auditor provided the organization can demonstrate sufficient separation and independence to ensure no conflict of interest. In both cases, the auditor must have sufficient experience and training to perform in the function of independent auditor. CertiPath will make the determination of auditor suitability based on the responses in Section 6 of the application.

Auditor information must cover the following three major areas:

- Identity and experience of the Lead Auditor.
- Identity and experience of the Staff Auditors.
- Attestation of auditor independence.
    - For Third Party Auditors – Attestation that the compliance auditor works for a separate third party operating entity, independent of the applicant's organization and any of its affiliates.
    - For Corporate Independent Auditors – 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.

2.1.2.7 Information on Applicant's Certificate Policy Mapping

The applicant must select the level(s) of assurance offered by the CertiPath CP to which cross certification or under which subordination is requested.

The applicant's CP or CPS (as applicable) must support the requested level(s) of assurance.

2.1.2.8 Attached Documentation

Applicants must attach the following required documentation to the application depending on the type of service requested:

- Standard Service
    - Appendix A – Applicant's CPS. CPS must be in RFC 3647 format.
    - Appendix B – A detailed diagram of the applicant's CA architecture with explanation of its operational processes.

- Appendix C – The directory schema of the applicant's PKI.
- Appendix D – Key Recovery Practices Statement (if applicable).

- Premium Service
  - Appendix A – Applicant's CP. CP must be in RFC 3647 format.
  - Appendix B – A detailed diagram of the applicant's CA architecture with explanation of its operational processes.
  - Appendix C – The directory schema of the applicant's PKI.
  - Appendix D – Key Recovery Practices Statement (if applicable).
  - Appendix E (Bridge applicants only) – the Criteria and Methodology pertaining to the applicant Bridge.

Note: the applicant's CP (Premium Service) or CPS (Standard Service) *must* be provided in electronic form as a Microsoft *WORD* document for CertiPath review. The CP will be shared with the CPMA membership. The CPS will be protected by CertiPath and not shared with any parties outside the CertiPath CPWG. In addition, the contents of Appendix B will be protected by CertiPath and not shared with any parties outside the CertiPath CPWG.

Organizations may submit additional documentation with the application at their discretion. These additional documents must be identified here and provided as additional Appendices.

2.1.2.9 Authorized Signature

The application must be signed by a senior official form the applicant's organization who is authorized to commit the organization to CertiPath's cross certification process.

2.1.3 Step 3: CPMA Vote on Application

Upon completion of Steps 1 and 2, the application is submitted to the CPMA for approval.

The CPMA performs Charter Vote #7 requiring approval by 75% of the CPMA membership to pass.

7. Acceptance of initial Application for CertiPath Interoperation	75% Majority

2.1.4 Step 4: Master Services and Subscription Agreement

To avoid delays in the cross certification or subordination process, the CertiPath Master Services and Subscription Agreement (MSSA) will be delivered to the applicant as soon as the PMSA has been signed. While the fully executed MSSA is not required until the mapping process is complete and credential issuance has been approved by the CPMA, the MSSA represents a contractual commitment between the parties; therefore requiring legal review and bilateral agreement, which can be a lengthy process. CertiPath legal counsel is available to work with the applicant's legal counsel to iron out any areas of concern and reach mutual agreement. Cross certificate issuance will not occur until the MSSA has been fully executed and any outstanding fees have been paid.

2.2 Phase Two: Mapping

2.2.1 Step 5: Certificate Policy Mapping

Certificate Policy Mapping pertains to cross certification only, and commences on after a vote to approve the application has been attained from the CPMA.

Standard Service: Standard Service applicants skip this step and proceed to *Step 6: KRPS Compliance Analysis.*

Premium Service:

- The CPWG will map the applicant's Certificate Policy to the CertiPath CP.
- The resulting Certificate Policy Mapping Report will identify areas where the applicant's CP does not contain the detail necessary to map successfully and which may require modifications to the applicant's CP.
- The CPWG will make itself available to discuss the specific mapping report findings at the applicant's discretion.
- The applicant will submit a revised CP that addresses the CPWG mapping report findings. The CPWG requires both a marked up version showing the revisions made as a result of the findings using *Track Changes*, as well as a "clean" version that contains no editorial marks or comments.
- The above process may repeat several times until both the CPWG and the applicant are satisfied at which time, the CPWG will prepare a final mapping report for consideration by the CPMA, indicating the applicant's CP has been mapped successfully to the CertiPath CP.

CertiPath Certified Credential Provider

In order for a CertiPath affiliate to operate as a 3CP, the cross certificate issued by CertiPath to the affiliate will not contain any name constraints. However, absence of name constraints requires additional diligence on the part of the affiliate to ensure accuracy of organization naming and prevention of name collision within the affiliate's community of users and with other names assigned by other CertiPath partners. Therefore, applicants whose intent is to act as a credential provider to other organizations must satisfy the provisions associated with 3CP certification; specifically, they must describe how they will manage name uniqueness across subscriber enterprises and across CertiPath community.

In addition to all other requirements for cross certification, 3CP applicants must provide additional documentation that identifies how they ensure uniqueness of names across their customer base and with the CertiPath community: both organizational and individual naming. Name conflicts must be identified and dealt with in a consistent and positive manner that is documented in the CPS or related documentation. At a minimum, the applicant should be prepared to share Section 3.1.5 of its CPS. The 3CP applicant will be required to provide a presentation of the processes employed to the CertiPath CPWG, and be prepared to answer CPWG questions and revise the process until the CPWG is satisfied that the name meaningfulness and name uniqueness are adequately addressed.

2.2.2 Step 6: KRPS Compliance

The applicant's KRPS will be compared to the CertiPath KRP for any Standard or Premium Service applicant that intends to issue encryption certificates to end users. All others will skip Step 6. See Section 2.1.2.2 above to determine applicability of this step.

- CertiPath's CPWG will review and analyze the applicant's KRPS to determine if the KRPS provides sufficient information in terms of meeting CertiPath's KRP requirements. See the *KRPS Guideline* for additional information on developing a KRPS.
- The resulting KRPS Compliance Analysis will identify areas where the applicant's KRPS does not meet the requirements of the CertiPath KRP or does not contain sufficient details, and require modifications to the applicant's KRPS.
- The CPWG will make itself available to discuss the specific mapping report findings, at the applicant's discretion.

The applicant will submit a revised KRPS that addresses the CPWG report findings in a marked up version using *tracked changes*, as well as a "clean" version that contains no editorial marks or comments.

The above process may repeat several times until both the CPWG and the applicant are satisfied, at which time, the CPWG will issue a final KRPS Compliance Analysis for consideration by the CPMA, indicating the applicant's KRPS has successfully demonstrated compliance to the CertiPath KRP.

Bridge CAs will undergo KRP mapping instead of KRPS compliance analysis.

2.2.3 Step 7: CPS Compliance Analysis

CPS Compliance Analysis is required for both Standard and Premium Service applicants.

Standard Service: For Standard Service applicants, the CPS must be submitted to CertiPath for review and compliance analysis, as follows:

- CertiPath's CPWG will review and analyze the applicant's CPS to determine if the CPS provides sufficient information in terms of meeting CertiPath's CP requirements.
- The resulting CPS Compliance Analysis will identify areas where the applicant's CPS does not meet the requirements of the CertiPath CP or does not contain sufficient details, and require modifications to the applicant's CPS.
- The CPWG will make itself available to discuss the specific mapping report findings, at the applicant's discretion.

The applicant will submit a revised CPS that addresses the CPWG report findings in a marked up version using *tracked changes*, as well as a "clean" version that contains no editorial marks or comments.

The above process may repeat several times until both the CPWG and the applicant are satisfied, at which time, the CPWG will issue a final CPS Compliance Analysis for consideration by the CPMA, indicating the applicant's KRPS has successfully demonstrated compliance to the CertiPath CP.

Premium Service: For Premium Service Applicants, the applicant must engage the services of a third party auditor (identified in Section 6 of the application to perform a compliance analysis of the CPS in relation to the applicant's CP (submitted with the application and revised during the CP Mapping process). The compliance auditor must return an opinion indicating that "the CPS complies with the

requirements of the CP" in order for the CPS compliance analysis to be accepted by the CPMA. The applicant will provide the auditor opinion to CertiPath for consideration by the CPMA.

Upon successful completion of the CPS Compliance Analysis, the applicant proceeds to *Step 8: PKI Compliance Audit*, and the CertiPath Operations Manager will move forward with *Step 9: Technical Interoperability Testing.*

2.2.4 Step 8: PKI Operational Compliance Audit

The third party auditor must complete an operational compliance audit. This compliance audit pertains to both Standard and Premium service applicants and assesses whether the credentialing infrastructure is implemented in accordance with the CPS and KRPS (where applicable). The audit may take one of two forms, as follows:

- If the audit is being performed on an existing fully functioning CA, a full operational audit will be performed.
- If the audit is being performed on a new CA that is not yet fully functioning (i.e. production certificates have not been issued in quantity), a pre-operational audit will be performed. The following applies to a pre-operational audit:
    - The pre-operational audit is valid for six months, at which time an operational audit must be performed.
    - In the event an operational audit cannot be completed within the six month timeframe due to an insufficient number of production certificates, the organization may request one, and only one, six month extension.
    - The extension request must indicate the reason for the extension with an assertion from the auditor that use of the operational environment is insufficient to perform a meaningful audit.
    - The extension is granted at the sole discretion of CertiPath.
    - In the event an extension is not granted and the organization does not complete an operational audit, the cross certificate issued by the CBCA or subordinate CA certificate issued by the CRCA will be revoked, effectively disabling the service.
- Regardless of the operational environment, the annual audit, due twelve months following the last successful audit must be completed.

The following applies to all types of audits:

- The applicant will provide the Auditor with a set of management assertions concerning the operations of the PKI in relation to the CP/CPS and KRPS (where applicable).
- The Auditor will prepare an opinion letter summarizing the audit findings.
- The Audit must address all of the requirements identified in the *CertiPath Audit Letter Template*.
- The applicant will submit the audit opinion letter, along with the statement of management assertions to CertiPath for consideration by the CPMA.
- Audit opinion letters pertaining to applicants for CBCA cross certification or CRCA subordination must be free of any findings.

2.3 Phase Three: Interoperability

2.3.1 Step 9: Technical Interoperability Testing

Interoperability testing is required for both Standard and Premium Service applicants. CertiPath's interoperability testing focuses on the proper construction of certificates, CRLs, OCSP responses, and PKCS-10 requests with respect to the PKI's infrastructure. This testing does not include running PK-enabled applications, such as TLS or secure E Mail.

Prior to initiation of interoperability testing the applicant organization will identify a technical point of contact to work with CertiPath during the interoperability testing:

- The designated individual must have knowledge of the operational environment of the organization's PKI and will act as the liaison between the applicant organization and CertiPath for the duration of the interoperability testing.
- The organization must provide the name, title, postal address, office phone and office e-mail address for the technical point(s) of contact.

In order to run interoperability testing, CertiPath maintains a test infrastructure that emulates the production environment. The applicant must establish a test environment that emulates its own production PKI environment in order to support interoperability testing. Two options for the test environment are available:

- The test environment may use the applicant's production PKI issuing Test level policy OIDs, or
- The applicant may stand up a Test PKI specifically for this testing.

The CertiPath Test Environment must be cross certified with the Applicant's Test Environment before testing can begin. To accomplish this, both CertiPath and the Applicant must:

- Fill out a naming application form:
    - These forms provide the details of certificate construction.
    - The policy mappings must use the *test* OIDs defined in the CertiPath ARC.
    - The *Production* policy mappings specified must be per the CPMA Approved Application in *Step 3: CPMA Vote on Application*.
- Exchange Certificate Signing Requests (CSR) in PKCS#10 format with Subject Key Identifier (SKID) specified – this process exchanges the public keys that are to be signed by the respective Test CAs.
- Sign the CSR using the appropriate Test CA – this generates a certificate.
- Send the certificate to the other party using PKCS#7.
- Install the received certificate in the Test CA Directory.

Interoperability testing details are provided in the CertiPath Interoperability Testing document, which is updated from time to time by CertiPath to comply with known interoperability issues. In addition to the Baseline Interoperability Testing required of all applicants, CertiPath conducts enhanced testing for applicants requesting IceCAP approval.

- CertiPath will conduct all applicable interoperability testing using the CertiPath lab facilities.

- Upon completion, an interoperability report will be prepared identifying areas where the tested artifacts are not conformant and/or interoperability may be affected.
- CertiPath will make itself available to discuss the specific interoperability report findings, at the applicant's discretion.
- The applicant will submit revised artifacts that address the interoperability report findings for retesting.

The above process may repeat several times until both CertiPath and the applicant are satisfied, at which time, CertiPath will issue a final interoperability report for consideration by the CPMA, indicating the applicant has successfully demonstrated interoperability in the CertiPath Federated PKI environment.

2.3.1.1 Baseline Interoperability Testing

Baseline Interoperability Testing is conducted for all Standard and Premium Service applicants. This testing requires examination of PKI artifacts such as the following for conformance to certificate profiles and interoperability:

- All CA certificates, including the self-signed root and cross certificate(s).
- One sample of each type of certificate issued by each CA in the applicant's PKI.
- One sample of each type of CRL issued by each CA in the applicant's PKI.
- PKCS#10 cross certificate request.
- All OCSP Responder certificates.
- One sample OCSP request and response from each OCSP Responder.
- All pointers in the certificates and CRLs such as CRL DP and CA Issuers field in AIA.
- Status response of certificates from the OCSP Responders.

Additional examination and testing may be required depending on the complexity of the applicant's PKI.

For Bridge CAs, only the PKI objects produced by the Bridge itself and associated OCSP Responders, if applicable, are examined.

2.3.1.2 IceCAP Credential Interoperability Testing

IceCAP interoperability Testing is performed for organizations interested in achieving *PIV-Interoperability* as defined by the Federal PKI.

Interoperability testing for IceCAP requires the issuance of fully populated hardware tokens by the applicant's IdM-CMS using the IceCAP PKI OIDs. There must be at least one hardware token issued from each CA planning to issue end entity certificates that meet IceCAP assurance. In addition to the Baseline Interoperability testing conducted according to *section* **Error! Reference source not found.**, CertiPath performs specific tests unique to IceCAP conformant credentials. Interoperability testing for IceCAP includes:

- Visual verification – ensure that the printed topology is distinct from federally issued PIV credentials.
- Data model – ensure the traditional interoperability testing of the credentials personalized on the card meet current PKI interoperability testing.

- PACS application testing – ensure that IceCAP credentials actually work in representative relying party applications.

Details are provided in the *CertiPath Bridge Certification Authority IceCAP Interoperability Testing* document.

For Bridge CAs, there is no IceCAP Credential Interoperability Testing.

2.4 Phase Four: Issuance

2.4.1 Step 10: Executed Master Services and Subscription Agreement

Before CertiPath takes the results of the cross certification activities to the CPMA for a vote, the applicant must complete and fully execute the Master Certificate Services and Subscription Agreement (MSSA) provided in **Error! Reference source not found.**.

Upon execution of the MSSA, the CPWG will place the request for approval for cross certification on the CPMA agenda for the next meeting. See *Step 11: CPMA Vote to approve cross certification or subordination*.

2.4.2 Step 11: CPMA Vote to approve cross certification or subordination

Once the MSSA has been executed, and upon satisfactory completion of the mapping, compliance analysis, compliance audit, and interoperability testing, the documentation is gathered and presented to the CPMA for final review and vote.

For Standard Service applicants, the following documentation is required:

- CertiPath report concerning compliance of applicant CPS with CertiPath CP.
- Compliance auditor's opinion letter concerning conformance of applicant operations to the CPS and KRPS, where applicable, with management assertions attached. This may be based on either a pre-operational audit or full operational audit.
- Baseline Interoperability test results summary.
- IceCAP Interoperability test results, where applicable.
- KRPS compliance analysis, where applicable.

For Premium Service applicants, the following documentation is required:

- CertiPath report concerning mapping of applicant CP to CertiPath CP.
- Latest version of the applicant CP, with changes resulting from the mapping activity included.
- Compliance auditor's assertion letter concerning the applicant's CPS conformance to the applicant's CP.
- Compliance auditor's opinion letter concerning conformance of applicant operations to the CPS and KRPS, where applicable, with management assertions attached. This may be based on either a pre-operational audit or full operational audit.
- Baseline Interoperability test results summary.
- IceCAP Interoperability test results, where applicable.
- KRPS compliance analysis, where applicable.

The CPMA Chair schedules a vote to approve cross certification based on these results at the next CPMA meeting.

The CPMA performs Charter Vote #9, which requires a 75% majority of the voting members to pass:

9. Approval of New Member Cross Certification/Subordination recommendation including: a. policy mapping b. compliance audits; c. interoperability testing d. KRP/KRPS mapping (where appropriate); and e. issuance of a cross certificate or subordination certificate	75% majority

Upon approval by the CPMA for applicant cross certification or subordination, the applicant is welcomed as a full voting member of the CPMA. The CPMA Chair issues the Letter of Authorization to the Operations Manager to issue a cross certificate or subordinate CA certificate to the newly approved affiliate CA as described in **Error! Reference source not found.**/*Subordination.*

2.4.3 Step 12: Cross Certification/Subordination

The first step in issuing a cross certificate (Premium Service) or subordinate CA certificate (Standard Service) is completion of the Naming Application Form. CertiPath will assist the affiliate with completion of this form which provides details of certificate construction and will be used in generating the certificate. In filling out the Naming Application Form, the following must be observed:

- For Standard Service affiliates, the certificate policies *must* use the policy OIDs defined in the CertiPath CP.
- For Premium Service affiliates, the policy mappings specified must be per the CPMA approved Application (see *Step 3: CPMA Vote on Application*) and subsequently confirmed by the CP mapping performed by the CPWG in *Phase 2: Mapping*.

For Premium Service affiliates to achieve cross certification, both CertiPath and the affiliate must:

- Securely[1] exchange CSRs in PKCS#10 format with SKID specified (the correct PKCS #10 certificate profile can be found in the CertiPath CP Section 10). This process exchanges the public keys that are to be signed by the respective CAs. As an alternative to the CSR, the affiliate may securely provide the certificate of the CA that is being cross certified.
- Sign the CSR/CA certificate using the appropriate CA – this generates a certificate.
- Send the certificate to the other party through digitally signed e-mail or on a write-only media such as a CD.
- Install the received certificate in the appropriate CA Directories.

For Standard Service affiliates to achieve subordination to the CRCA, the following process applies:

- The affiliate will securely submit a CSR in PKCS#10 format with SKID specified to CertiPath (the correct PKCS#10 certificate profile can be found in the CertiPath CP Section 10). This process provides the public key that is to be signed by the CRCA.

[1] Examples of secure submission include hand carrying, FedEx, certified postal mail, and a digitally signed electronic file that can be verified by CertiPath.

- CertiPath will sign the CSR using the CRCA – this generates a certificate.
- CertiPath will send the certificate to the affiliate using digitally signed e-mail or on a write-only media such as a CD.
- The certificate will be installed in the appropriate CA Directories by both CertiPath and the affiliate.

3 Maintenance of Affiliate PKI Relationship with CertiPath

It is important to ensure that, once in place and for its duration, the cross-certification arrangement continues to guarantee the agreed-upon level(s) of trust between CertiPath and the Affiliate PKI.

The maintenance phase provides mechanisms both for managing the relationship between cross-certified entities and for terminating the arrangement. The following activities are inherent to the maintenance of CertiPath cross certification and subordination relationships:

- Participation in the CPMA.
- Annual recertification of the CertiPath relationship.
- Problem resolution.
- Termination.

3.1 Participation in the CPMA

Upon approval of an organization for cross certification or subordination, the organization becomes a CertiPath affiliated organization and is invested with full rights as a member of the CPMA. To this end the newly affiliated organization must provide, as part of the MSSA, the name and contact information for the primary voting member that will represent the organization at CPMA meetings, and the name and contact information for an alternate to represent the organization when the primary voting member is unavailable. These representatives must be employees of the affiliated organization and hold positions with oversight responsibilities for PKI and/or Identity Management activities within the organization. Member organizations are required to participate in the monthly CPMA meetings or provide a voting proxy when absence is unavoidable. Proxy may be assigned to the Chair or to any other voting member.

In the event an organization wishes to replace its voting member or alternate, this must be communicated to the CPMA Chair in a written notification on company letterhead and duly signed by an individual authorized to act on behalf of the organization.

3.2 Annual Recertification of the CertiPath Relationship

Cross certificates issued by the CBCA and subordinate CA certificates issued by the CRCA expire twelve months from date of issuance. In order to continue as a CertiPath member, the cross certified and subordinated organizations must undergo recertification. The following activities are performed *annually* during the recertification process to maintain an affiliate's cross certification status with the CBCA or subordinate relationship to the CRCA:

- Renewal of the *MSSA Service Level Agreement* between the affiliate and CertiPath.
- *Differential Policy Mapping* (Premium Service only).
- *CPS Differential Compliance Analysis* (Standard Service only).
- *Interoperability Testing* (Standard and Premium Service).
- *Annual Compliance Audit* (Standard and Premium Service).
- Review and vote by the CPMA to continue CBCA or CRCA relationship.
- Reissuance of CBCA cross certificate or CRCA subordination certificate.

In addition, a *KRPS Differential Compliance Analysis* is conducted biannually, where applicable.

In the event a CertiPath Affiliated Organization wishes to make changes to the cross certification or subordination relationship (e.g. implement new policy OID mappings, undergo 3CP or IceCAP certification, etc.), an "Application for Credential Modification" must be completed in addition to the above.

3.2.1 Renewal of the MSSA Service Level Agreement

The Service Level Agreement (SLA) associated with the MSSA must be renewed annually. Recertification activities (mapping, interoperability testing, etc) will not be undertaken until the SLA has been renewed and any outstanding fees have been paid.

Failure to complete the MSSA SLA renewal in a timely manner to allow completion of recertification activities before the expiration date of the current cross certificate or subordinate CA certificate may result in its cross/subordination certificate lapsing and suspension of the organization's CPMA voting membership.

3.2.2 Differential Policy Mapping (Premium Service Only)

Premium Service affiliates complete a Certificate Policy Differential Policy Mapping each year in order to renew their cross certification with the CBCA. This mapping reduces the risk of policy drift between the affiliate's CP and the CertiPath CP as these documents change over time. This mapping also helps CertiPath ensure that any CertiPath CP change requests the CPMA has approved over the past twelve months were adopted by the affiliate. The affiliate's agreement with CertiPath obligates them to adopt changes within the timeframe specified in the change request; generally, three months. To assist affiliated organizations in preparing for the differential policy mapping, CertiPath will provide a red-lined CertiPath CP that indicates the changes that have taken place between the CertiPath CP version previously used to map the Affiliate's CP and the current version of the CertiPath CP.

The Differential Policy Mapping is accomplished by reviewing the changes in the affiliated organization's CP since the last approved policy mapping and mapping these to the current CertiPath CP. To this end, the affiliated organization must supply:

- A current CP in *WORD* document format.
- A current CP in *WORD* document format that highlights (with *Track Changes*) all changes from the last approved policy mapping.

CertiPath's CPWG will:

- Verify the submitted CP is consistent with the last cross certified CP, with track changes showing all new modifications.
- Perform a differential policy mapping against the current CertiPath CP that examines the changes to the affiliated organization's CP to ensure changes made to the CertiPath CP have been adopted, where appropriate, and no other changes made are detrimental to cross organizational trust.
- Generate a mapping report that identifies areas where the affiliated organization's CP does not appear to map successfully and which may require additional modifications to the CP.
- Be available to discuss the policy mapping report at the affiliated organization's discretion.

Based on the report and subsequent discussion, the affiliate will submit a revised CP that addresses the CPWG mapping report findings in a marked up version using tracked changes, as well as a "clean" version that contains no editorial marks or comments. Each revised document must be assigned a new

version number and date of creation to ensure effective version control. This is an iterative process which may repeat several times until both the CPWG and the affiliate are satisfied, at which time the CPWG will issue a final mapping report indicating the affiliate's CP has been mapped successfully to the CBCA CP.

Once the affiliate's CP is accepted by the CPWG, the affiliate must ensure its CPS is amended as appropriate.

If the modifications to the affiliate's CP as a result of the mapping process are considered "significant", an updated third party compliance analysis and audit must be supplied by the affiliate. CertiPath with notify the affiliate when this is the case.

3.2.3 Differential Compliance Analysis

CertiPath conducts Differential Compliance Analysis annually on the CPS of Standard Service Affiliates.

In addition, Differential Compliance Analysis is conducted bi-annually on the KRPS of all affiliates whose relationship with CertiPath includes encryption certificates.

The Certification Practices Statement and the Key Recovery Practices Statement are considered sensitive documents, therefore, CertiPath will not share these documents with any party outside the CPWG and will protect the documents at all times while in CertiPath control.

3.2.3.1 CPS Differential Compliance Analysis (Standard Service Only)

Standard Service affiliates will have to complete a Certification Practices Statement Differential Policy Mapping each year in order to renew their subordination certificate with the CertiPath Root. This compliance analysis reduces the risk of drift between an affiliate's CPS and the CertiPath CP as these documents do change over time. This mapping also helps CertiPath ensure that any CP change requests the CPMA has approved over the past twelve months were implemented by the affiliate. The affiliate's agreement with CertiPath obligates them to keep the CPS in compliance with the CertiPath CP at all times, therefore all applicable changes must be reflected in the CPS within three months of CPMA approval. To assist Standard Service affiliated organizations in preparing for the differential CPS compliance analysis, CertiPath will provide a red-lined CP that indicates the changes that have taken place between the CertiPath CP version previously used to conduct compliance analysis of the Affiliate's CPS and the current version of the CertiPath CP.

The Differential Compliance Analysis is accomplished by reviewing the changes in the affiliated organization's CPS since the last approved compliance analysis and ensuring these comply with the current CertiPath CP. To this end, the affiliated organization must supply:

- A current CPS in *WORD* document format.
- A current CPS in *WORD* document format that highlights (with *Track Changes*) all changes from the last approved compliance analysis.

CertiPath's CPWG will:

- Verify the submitted CPS is consistent with the last approved CPS, with track changes showing all new modifications.
- Perform a differential compliance analysis against the current CertiPath CP that examines the changes to the affiliated organization's CPS to ensure changes made to the CertiPath CP have been adopted, where appropriate, and no other changes made are detrimental to the affiliate's subordinate status.

- Generate a compliance analysis report that identifies areas where the affiliated organization's CPS does not comply with the CertiPath CP or does not contain sufficient details and which will require additional modifications to the CPS.
- Be available to discuss the policy mapping report at the affiliated organization's discretion.

The affiliate will submit a revised CPS that addresses the CPWG compliance analysis findings in a marked up version using *tracked changes*, as well as a "clean" version that contains no editorial marks or comments. Each revised document must be assigned a new version number and date of creation to ensure effective version control. This is an iterative process which may repeat several times until both the CPWG and the affiliate are satisfied, at which time the CPWG will issue a final compliance analysis indicating the affiliate's CPS complies with the CertiPath CP.

If the modifications to the affiliate's CPS as a result of the compliance analysis are considered "significant", an updated third party compliance audit must be supplied by the affiliate. CertiPath will notify the affiliate when this is the case. Note that this compliance audit may be in addition to the compliance audit discussed in **Error! Reference source not found.**5, since the annual compliance audit may not have accounted for the changes to the CP and the CPS.

3.2.3.2 KRPS Differential Compliance Analysis

Standard and Premium Service affiliates that issue encryption certificates to end users are required to undergo review of their KRPS every two years. To assist in the process, CertiPath will provide a red-lined KRP that indicates the changes that have taken place between the CertiPath KRP version previously used in review of the affiliate's KRPS and the current version of the CertiPath KRP.

The KRPS compliance review is accomplished by examining the changes in the affiliated organization's KRPS since the last approved KRPS compliance review with the current CertiPath KRP for reference. To this end, the affiliated organization must supply:

- A current KRPS in *WORD* document format.
- A current KRPS in *WORD* document format that highlights (with *Track Changes*) all changes from the last approved KRPS mapping.

CertiPath's CPWG will:

- Examine the affiliate's KRPS for conformance with CertiPath KRP.
- Generate a KRPS compliance audit report identifying areas where the affiliate's KRPS does not meet the requirements of the CertiPath KRP.
- Determine whether modifications to the affiliate's KRPS are needed.
- Be available to discuss the specific compliance report findings, at the affiliate's discretion.

The affiliate will submit a revised KRPS that addresses the CPWG compliance report findings in a marked up version using tracked changes, as well as a "clean" version that contains no editorial marks or comments. Each revised document must be assigned a new version number and date of creation to ensure effective version control.

The above process may repeat several times until both the CPWG and the affiliate are satisfied, at which time, the CPWG will issue a final KRPS compliance report indicating the affiliate's KRPS has been reviewed successfully for compliance with the CertiPath KRP for consideration by the CPMA.

3.2.4 Interoperability Testing

The affiliated organization's CPMA representative is responsible for keeping the contact information concerning the technical resource current. The technical resource must have knowledge of the operational environment of the organization's PKI and will act as the liaison between the affiliated organization and CertiPath for the duration of the interoperability testing.

Interoperability testing is required for annual recertification of both Standard and Premium Service affiliates. CertiPath's interoperability testing focuses on the proper construction of certificates, CRLs, OCSP responses, and PKCS-10 requests with respect to the affiliate PKI's infrastructure. This testing does not include running PK-enabled applications such as TLS or secure E Mail.

Organizations that stand up a test infrastructure cross certified with the CertiPath test infrastructure during the application phase will use this same test infrastructure for annual interoperability testing. All others must issue certificates containing test level policy OIDs during annual interoperability testing.

Interoperability testing details are provided in the *CertiPath Interoperability Testing* document, which is updated from time to time by CertiPath to address known interoperability issues. In addition to the Baseline Interoperability Testing required of all affiliates, CertiPath conducts enhanced testing for applicants cross certified at the IceCAP level of assurance.

- CertiPath will conduct all applicable interoperability testing using the CertiPath lab facilities.
- Upon completion, an interoperability report will be prepared identifying areas where the tested artifacts are not conformant and/or interoperability may be affected.
- CertiPath will make itself available to discuss the specific interoperability report findings, at the affiliate's discretion.
- The affiliate will submit revised artifacts that address the interoperability report findings for retesting.

The above process may repeat several times until both CertiPath and the affiliate are satisfied, at which time, CertiPath will issue a final interoperability report for consideration by the CPMA, indicating the affiliate has successfully demonstrated interoperability in the CertiPath Federated PKI environment.

For interoperability findings that cannot be addressed immediately, the affiliate may submit a mitigation plan indicating the modifications that will be made to the certificates it issues in order to address the findings, and the timeframe for accomplishing these modifications. CertiPath may accept all or parts of the mitigation plan at its discretion; the affiliate must rectify the remaining issues immediately.

3.2.4.1 Baseline Interoperability Testing

Baseline Interoperability Testing is conducted for all Standard and Premium Service affiliates annually. This testing requires examination of PKI artifacts such as the following for conformance to certificate profiles and interoperability:

- All CA certificates, including the self-signed root and cross certificate(s).
- One sample of each type of certificate issued by each CA in the affiliate's PKI.
- One sample of each type of CRL issued by each CA in the affiliate's PKI.
- PKCS#10 cross certificate request.
- All OCSP Responder certificates.

- One sample OCSP request and response from each OCSP Responder.
- All pointers in the certificates and CRLs such as CRL DP and CA Issuers field in AIA.
- Status response of certificates from the OCSP Responders.

Additional examination and testing may be required depending on the complexity of the affiliate's PKI.

For Bridge CAs, only the PKI objects produced by the Bridge itself and associated OCSP Responders, if applicable, are examined.

3.2.4.2 IceCAP Credential Interoperability Testing

Annual IceCAP interoperability Testing is performed for affiliated organizations cross certified at the IceCAP level of assurance.

Interoperability testing for IceCAP requires the issuance of fully populated hardware tokens by the affiliate's IdM-CMS using the IceCAP PKI OIDs. There must be at least one hardware token issued from each CA that issues end entity certificates that meet IceCAP assurance. In addition to the Baseline Interoperability testing conducted in accordance with *section 3.2.4.1,* CertiPath performs specific tests unique to IceCAP conformant credentials. Interoperability testing for IceCAP includes:

- Visual verification – ensure that the printed topology is distinct from federally issued PIV credentials.
- Data model – ensure the traditional interoperability testing of the credentials personalized on the card meet current PKI interoperability testing.
- PACS application testing – ensure that IceCAP credentials actually work in representative relying party applications.

Details are provided in the *CertiPath Bridge Certification Authority IceCAP Interoperability Testing* document.

For Bridge CAs, there is no IceCAP Credential Interoperability Testing.

3.2.5 Annual Compliance Audit

All affiliated organizations cross certified with the CBCA or subordinated to the CRCA must undergo an annual audit that covers the previous 12 months, and is completed on or before the anniversary date of the previous audit. The Compliance Audit must be conducted by an approved auditor who has demonstrated competence in PKI audits. The auditor may be either an independent third party entity with no relationship to the affiliate's organization or a Corporate Internal Auditor provided the affiliated organization can demonstrate sufficient separation and independence to ensure no conflict of interest. When a Corporate Internal Auditor is used, the affiliate must engage the services of an independent third party auditor every third year, at a minimum.

In the event the affiliate changes audit companies, the individuals conducting the audit on behalf of the third party independent audit company change, elects to use corporate internal auditors, or the corporate internal auditor personnel change, the affiliate must notify CertiPath and provide information concerning the new audit company, organizational separation, and/or personnel in accordance with the application template, described in Section 2.1.2.6 above.

The annual compliance audit is comprised of two parts: the CP/CPS compliance analysis and the Operational Compliance assessment.

3.2.5.1 CP/CPS Compliance Analysis

For Standard Service affiliates, the annual CPS Compliance Analysis is conducted by CertiPath and is addressed in Section 3.2.3.1, above.

For Premium Service affiliates, compliance analysis of the CPS in relation to the affiliate's CP is performed by the third party or corporate internal auditor. The compliance auditor must return an opinion indicating that "the CPS complies with the requirements of the CP" in order for the CPS compliance analysis to be accepted by the CPMA. The affiliate will provide the auditor opinion to CertiPath for consideration by the CPMA.

3.2.5.2 Operational Compliance Assessment

The operational compliance assessment pertains to both Standard and Premium service affiliates and assesses whether the credentialing infrastructure is operating in accordance with the CPS and KRPS (where applicable).

- The affiliated organization will provide the Auditor with a set of management assertions concerning the operations of the PKI in relation to the CP/CPS and KRPS (where applicable).
- The Auditor will prepare an opinion letter summarizing the audit findings and identifying the areas of non-compliance, if any.
- The audit opinion must address all of the requirements identified in the *CertiPath Audit Letter Template.*
- The affiliate will submit the audit opinion letter, along with the statement of management assertions and a mitigation plan, with milestones, for the identified areas of non-compliance, if any, to CertiPath for consideration by the CPMA.

3.2.6 CPMA Vote on Recertification

Upon satisfactory completion of the mapping/compliance analysis, interoperability testing, and compliance audits, the documentation is gathered and presented to the CPMA for final review and vote.

For Standard Service recertification, the following documentation is required:

- CertiPath CPS Compliance Analysis Report.
- Compliance auditor's opinion letter concerning conformance of affiliate PKI operations to the CPS and KRPS, where applicable, with management assertions attached.
- Affiliate's mitigation plan, if required by compliance audit results.
- Baseline Interoperability test results summary.
- IceCAP Interoperability test results summary, where applicable.
- KRPS compliance analysis, where applicable.

For Premium Service applicants, the following documentation is required:

- CertiPath CP Mapping Report.
- Latest version of the affiliate CP, with changes resulting from the mapping activity included.
- Compliance auditor's assertion letter concerning the affiliate's CPS conformance to the affiliate's CP.

- Compliance auditor's opinion letter concerning conformance of affiliate PKI operations to the CPS and KRPS, where applicable, with management assertions attached.
- Baseline Interoperability test results summary.
- IceCAP Interoperability test results summary, where applicable.
- KRPS compliance analysis, where applicable.

The CPMA Chair schedules a vote to approve cross certification based on these results at the next CPMA meeting.

The CPMA performs Charter Vote #10, which requires a 75% majority of the voting members (with recusal of the concerned affiliate) to pass:

10. Approval of CBCA/CRCA Recertification including: a. policy mapping; b. compliance audits; c. interoperability testing; d. KRPS mapping (where appropriate); and e. reissuance of a cross certificate or subordination certificate	75% majority exclusive of concerned party. (Requires recusal of concerned member.)

Upon approval of the vote by the CPMA, the CPMA Chair will instruct the Operational Authority to issue a new cross certificate to the customer.

3.2.7 Reissuance of Cross Certification/Subordination Certificate

The first step in reissuing a cross certificate (Premium Service) or subordinate CA certificate (Standard Service) is completion of the Naming Application Form. CertiPath will assist the affiliated organization with completion of this form to ensure the details of certificate construction are accurate. In filling out the Naming Application Form, the following must be observed:

- For Standard Service affiliates, the certificate policies *must* use the policy OIDs defined in the CertiPath CP.
- For Premium Service affiliates, the policy mappings specified must be in accordance with the findings of the CP Mapping Report described in *Section 3.2.2, Differential Policy Mapping* and approved by the CPMA as described in *Section 3.2.6 CPMA Vote on Recertification*.

For Premium Service affiliates to continue the cross certified relationship, both CertiPath and the affiliate must:

- Securely exchange CSRs in PKCS#10 format with SKID specified (the correct PKCS #10 certificate profile can be found in the CertiPath CP Section 10). This process exchanges the public keys that are to be signed by the respective CAs. As an alternative to the CSR, the affiliate may securely provide the certificate of the CA that is being cross certified.
- Sign the CSR/CA certificate using the appropriate CA – this generates a certificate.
- Send the certificate to the other party through digitally signed e-mail or on a write-only media such as a CD.
- Install the received certificate in the appropriate CA Directories.

For Standard Service affiliates to continue subordination to the CRCA, the following process applies:

- The affiliate will securely submit a CSR in PKCS#10 format with SKID specified to CertiPath (the correct PKCS#10 certificate profile can be found in the CertiPath CP Section 10). This process provides the public key that is to be signed by the CRCA.
- CertiPath will sign the CSR using the CRCA – this generates a certificate.
- CertiPath will send the certificate to the affiliate using digitally signed e-mail or on a write-only media such as a CD.
- The certificate will be installed in the appropriate CA Directories by both CertiPath and the affiliate.

3.3 Problem Resolution

Either CertiPath or the Affiliated Organization may notify the other of problems and request resolution.

For Technical problems, the Affiliate PKI technical resource will work with the CertiPath Operations Manager to resolve the issue(s).

For situations where CertiPath or the CPMA has reason to believe that the affiliated PKI is not operating in compliance with its MSSA or CP, either CertiPath or the CPMA may request an aperiodic compliance audit and a compliance audit letter specifically addressing the concern. All such requests will be made for cause, and the cause will be disclosed at the time of the request.

For CA key compromise, the affected organization will take action immediately as required in the CP Section 5.7, to include immediate notification to the CPMA Chair.

CertiPath reserves the right to join the affiliate's internal incident response team if deemed necessary.

3.3.1 Notification

3.3.1.1 CertiPath Responsibilities

CertiPath will promptly advise the CPMA membership:

- In the event of any material problem or inability to operate the CBCA or CRCA in accordance with the CertiPath CP or CPS.
- In the event that CertiPath becomes aware of a material non-compliance on the part of any other party that is within the name constraints in the cross-certificate issued by the CBCA or CA certificate issued by the CRCA and that interoperates with the CBCA or CRCA.
- In the event that CertiPath takes any action to terminate or limit such other party's interoperability with the CBCA or CRCA.
- In the event of a CBCA or CRCA private key compromise or loss, or another affiliated entity's Principal CA private key compromise or loss. A CRL shall be published at the earliest feasible time by the CertiPath Operational Authority.
- In the event of a disaster where the CBCA or CRCA or an affiliate Principal CA installation is physically damaged and all copies of the CBCA or CRCA or affiliate Principal CA signature keys are destroyed.

Any such notification will occur as follows:

- The CPMA Chair or the CertiPath Operations Manager shall notify the CPMA Member points of contact.
- Notification will be done by telephone, by digitally signed and encrypted e-mail, or by any other mechanism agreed upon and documented in official correspondence between the CPMA Members and CertiPath.
- Additional procedures in accordance with CertiPath CP Section 5.7 will be followed.

3.3.1.2 Affiliate Organization Responsibilities

The affiliate organization will promptly advise the CPMA Chair and the CertiPath Operational Authority:

- In the event of any material problem or inability to operate the Principal CA in accordance with the Affiliate CP, CPS or Supplemental Requirements.
- In the event that the affiliate becomes aware of a material non-compliance on the part of any other party that is within the name constraints in the cross-certificate issued by the CBCA or CA certificate issued by the CRCA and that interoperates with the Principal CA.
- In the event that the affiliate takes any action to terminate or limit such other party's interoperability with the CBCA or CRCA.
- In the event of an Affiliate Principal CA private key compromise or loss. A CRL shall be published at the earliest feasible time by the affiliate CA.
- In the event of a disaster where the Affiliate Principal CA installation is physically damaged and all copies of the affiliate Principal CA signature keys are destroyed.

Any such notification will occur as follows:

- The Affiliate shall notify the CPMA Chair and the CertiPath Operational Authority.
- Notification will be done by telephone, by digitally signed and encrypted e-mail, or by any other mechanism agreed upon and documented in official correspondence between CertiPath and the affiliated organization.
- The affiliate shall follow all procedures specified in CertiPath CP Section 5.7, Affiliate CP Section 5.7, and Affiliate Principal CA CPS Section 5.7.

3.3.2 CPMA Problem Resolution

CertiPath reserves the right to take necessary immediate action to resolve problems within the CertiPath community, followed by appropriate notification to the CPMA as soon as deemed practicable. However, in accordance with the legal provisions provided in the MSSAs between CertiPath and its Customers and when circumstances permit, problem resolution may be referred to the CPMA.

Problem resolution within the CertiPath community is routinely carried out by the CPMA through CPMA votes #5, #6, #11, and #12.

5. Approve CPMA procedures for actions/remedies to address non-compliance.	Majority
6. Directions to CertiPath OA to revoke cross certificates or subordinate certificates.	75% Majority exclusive of the concerned party (requires recusal of concerned member)
11. Determination of remedies/actions to be taken for unacceptable risk to the CertiPath trust fabric.	75% Majority
12. Determination to restore CertiPath interoperability following cross-certification revocation	75% Majority

3.3.3 Termination

CertiPath has the right to terminate, modify, suspend or discontinue the CBCA or CRCA or individual affiliate's agreements due to:

- Government regulation or requirement.
- To avoid material liability to a third party.
- Revocation of an affiliate's certificate
- CertiPath's relationships with its service providers or licensors so require
- To avoid violations of the law or regulations

The relationship between CertiPath and an affiliate PKI may be terminated by either party.

3.3.4 Notice of Termination

In the event the Affiliate PKI initiates termination, the Affiliate PKI POC must notify CertiPath in writing of its intent to terminate the MSSA, the reason(s) for seeking termination, and the desired termination date.

Should CertiPath become aware that there has been a failure in the integrity of an Affiliate PKI, CertiPath will revoke the cross-certificate of the Affiliated PKI. CertiPath will inform the Affiliate PKI POC of the revocation and provide a resolution date after which the MSSA will be terminated if the issue is not resolved. CertiPath will inform the other CPMA members of the issue, the revocation, and the timeframe provided for resolution.

CertiPath will inform the Affiliate PKI in writing of its intent to terminate the MSSA at least 10 days before the effective date of termination.

3.3.5 Revocation of CBCA/CRCA-issued Certificates

CertiPath will revoke a cross certificate issued by the CBCA or a subordinate CA certificate issued by the CRCA if it can be proven or it is reasonable to believe key compromise has occurred or if the certificate needs modification.

In addition, CertiPath will revoke a cross certificate or subordinate CA certificate at the request of the organization to which it was issued.

3.3.5.1 Who Can Request Revocation of a Certificate

Any CPMA voting member may request revocation of its own CBCA/CRCA-issued certificate at any time.

In addition, any CPMA member may request revocation of any other organization's CBCA/CRCA-issued certificate for cause. The CPMA chair will call for a CPMA meeting to inform the CPMA membership of the request to revoke a certificate issued by the CBCA or CRCA and upon confirmation of the request by the CPMA members issue a request to the CertiPath Operational Authority to revoke the certificate.

In accordance with legal provisions provided in service agreements with Affiliates, CertiPath may revoke any cross certificate issued by the CBCA or subordinate CA certificate issued by the CRCA at any time. CertiPath may request revocation of a certificate issued by the CBCA or CRCA if any of the following are true:

- The affiliate is in default with respect to its financial obligations to CertiPath.
- The affiliate has fallen out of compliance with its CP/CPS (or the CertiPath KRP, where applicable). This requires proof or must be reasonable to believe is the case before revocation action is taken. The Operational Authority Manager will be responsible for reporting this action and the justification to the CPMA immediately following the action.
- There is a compromise in the trusted roles at an affiliate's CA. This requires proof or must be reasonable to believe is the case before revocation action is taken. The Operational Authority Manager will be responsible for reporting this action and the justification to the CPMA immediately following the action.
- The affiliate's CA key has been compromised.

For additional guidance, see Sections 4.9.1 and 4.9.2 of the CertiPath or Affiliate CP.

3.3.5.2 Revocation Request Grace Period

There is no revocation grace period. Responsible parties must request revocation as soon as they identify the need for revocation.

3.3.5.3 Certificate Suspension

In accordance with legal provisions provided in service agreements with affiliates, CertiPath may suspend any certificate issued by the CBCA or CRCA at any time. CertiPath will suspend a certificate if it is reasonable to believe key compromise has occurred or the certificate needs modification.

CertiPath will remove the suspended certificate from the CRL if investigation findings confirm that a key compromise has not occurred and the certificate does not need modification.

4 Acronyms and Abbreviations

3CP	CertiPath Certified Credential Provider
CA	Certification Authority
CBCA	CertiPath Bridge Certification Authority
CMS	Card Management System
CP	Certificate Policy
CPMA	CertiPath Policy Management Authority
CPS	Certification Practice Statement
CPWG	CertiPath Policy Working Group
CRCA	CertiPath Root Certification Authority
CRL	Certificate Revocation List
CSR	Certificate Signing Request
HSM	Hardware Security Module
KRP	Key Recovery Policy
KRPS	Key Recovery Practice Statement
MSSA	Master Services and Subscription Agreement
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIV-I	Personal Identity Verification – Interoperable
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PMSA	Policy Mapping Service Agreement
SKID	Subject Key Identifier
SLA	Service Level Agreement