Criteria and Methodology for Cross-certification with the STRAC Bridge Certification Authority (STRAC BCA)

Version 1.0

August 6, 2014

Signature Page

2/3/2015

Chair, STRAC Public Key Infrastructure Policy Authority — DATE

Revision History Table

Date	Version	Description	Author
August 6, 2014	1.0	First Version Built from FBCA Crits and Methods Ver. 3.0, Jan. 25, 2012	SPKIPA

TABLE OF CONTENTS

1 INTRODUCTION

1.1 OBJECTIVE

This document identifies the criteria for determining Applicant suitability, and defines the methodology for implementing and maintaining cross-certification with the Southwest Texas Regional Advisory Council (STRAC) Bridge Certification Authority (STRAC BCA) by external entity certification authorities (CAs).

1.2 BACKGROUND

The STRAC BCA's goal is to enable entities serving the public safety and health care communities to issue standardized credentials that meet federally trusted standards without obtaining federal certification from the Federal Bridge Certification Authority (Federal BCA) directly. Instead, the STRAC BCA, using the STRAC public key infrastructure (SPKI), intends to obtain that federal certification from the Federal BCA, and, by establishing trust with non-federal issuers consistent with federal requirements, enable those entities to issue credentials that can also be trusted not only among each other, but by federal entities as well.

As part of the process of cross-certifying with the Federal BCA, the STRAC BCA's governing body, the SPKI Policy Authority (SPKIPA), adopted "*X.509 Certificate Policy for the STRAC Bridge Certification Authority*" (STRAC BCA CP). The policy defines the STRAC BCA as an interoperability mechanism for ensuring trust across disparate PKI domains. Successful cross-certification with the STRAC BCA asserts that the Applicant operates in accordance with the standards, guidelines and practices of the SPKIPA.

1.3 STRAC PKI POLICY AUTHORITY (SPKIPA) AND THE STRAC PKI MANAGEMENT AUTHORITY (SPKIMA)

The SPKIPA sets policy governing operation of the STRAC BCA. It also approves Applicants for cross-certification with the STRAC BCA. The "*STRAC Public Key Infrastructure Policy Authority Charter*" (SPKIPA Charter) identifies the governance and operations of the SPKIPA.

The SPKIPA identifies the personnel and directs the work of the SPKIMA. The SPKIPA and SPKIMA are separate but related bodies; the SPKIPA is made up of representatives of the entities that have CAs cross-certified to the STRAC BCA, and the SPKIMA is selected, tasked, and overseen by the SPKIPA.

1.4 INTENDED AUDIENCE AND SCOPE

This document, issued under the authority of the SPKIPA, is intended for the use of entities wishing to pursue cross-certification of a CA with the STRAC BCA ("Applicant"). These cross-certification guidelines should be read in conjunction with the STRAC BCA CP.

1.5 GENERAL PRINCIPLES

Cross-certification with the STRAC BCA is not a right, nor should any discussions be considered a commitment to issue cross-certificates. The SPKIPA will determine which applications for STRAC BCA cross-certification to accept, and which to reject, following a decisional process set out in the SPKIPA Charter. This document describes the criteria and methodology upon which the SPKIPA will base its decision.

Subject to this document, the SPKIPA will consider applications for cross-certification from any entity operating a CA if such cross-certification is in the service of state, local or tribal governments or healthcare entities, though the SPKIPA will consider and accept cross-certification applications in service of other interests, as well, in the sole discretion of the SPKIPA.

1.5.1 Discretion of the SPKIPA, and Binding Nature of This Document

Cross-certificates issued by the STRAC BCA are issued, renewed, modified, and revoked at the sole discretion of the SPKIPA. *If the STRAC BCA elects to issue, renew, modify, or revoke a cross-certificate, it shall do so in compliance with this Methodology and Criteria document.*

The SPKIPA can elect at any time and for any or no reason to pause or discontinue the processing of an application for cross-certification or the renewal or modification of a cross-certificate. Accordingly, any action required of or ascribed to the SPKIPA or SPKIMA in this Criteria and Methodology (other than providing notice of decision to terminate the cross-certification application process) is subject to the SPKIPA's ongoing election to proceed with the application or maintain the resulting cross-certificate.

If the SPKIPA elects to proceed on an application for cross-certification to the STRAC BCA or the renewal or modification of a cross-certificate, it shall conduct a review of the Applicant's CP at the requested assurance levels as provided herein.

1.5.2 Cross-certification Process Is the Same Regardless of Entity Use of SPKIPA Support Services

In order to reduce the cost and complexity of obtaining the benefits of identity credentials that are interoperable with and trusted by federal partners, particularly for those within the public safety and healthcare communities, the SPKIPA intends to help applicants for cross-certification to the STRAC BCA by providing them with suggested CP language ("CP Template") to include in their CPs. This CP Template will be created by the SPKIPA specifically to comply with the STRAC BCA CP.

If the SPKIPA elects, in its sole discretion, to proceed with a cross-certification application, it will follow the processes set forth in this Criteria and Methodology—including but not limited to those applicable to CP mapping—regardless of the extent to which the Applicant adopts the provisions of the Template CP.

In order to gain further efficiencies and better ensure compliance for entities cross-certified to the STRAC BCA, the SPKIPA could, in its sole discretion, allow cross-certified CAs to co-locate at STRAC-identified facilities and to be operated on the cross-certified CA's behalf by STRAC-identified personnel; this support ("Support Services") could include co-location with the STRAC BCA and operation by personnel also involved in operation of the STRAC BCA.

If the SPKIPA elects, in its sole discretion, to proceed with an application for a new, renewed, or modified cross-certification, it will follow the processes set forth in this Criteria and Methodology—including but not limited to those applicable to audit and technical testing—regardless of the extent to which the Applicant avails itself of any support offered by STRAC or the SPKIPA, including CA co-location and operations services.

All Applicants for cross-certification must obtain unique policy Object Identifiers (OIDs) in the standard International Organization of Standardization (ISO) or similar object identifier registry from the appropriate commercial or national registration authority.

1.6 DEFINITIONS

The following terms are used in this guideline.

Affiliate PKI: An approved Applicant PKI that has successfully completed all steps required to become cross-certified and has been issued a cross-certificate by the STRAC BCA.

Applicant: An entity requesting cross-certification of a CA it operates or will operate with the STRAC BCA.

Bridge CA: A CA that itself does not issue certificates to end entities (except those required for its own operations) but establishes unilateral or bilateral cross-certification with other CAs.

Certification Authority (CA): An entity that issues certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate.

Certificate Policy (CP): A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. A PKI could adopt more than one CP.

Certificate Revocation List (CRL): A data structure that enumerates digital certificates that have been invalidated by their issuer prior to the certificates' scheduled expiration.

Certification Practice Statement (CPS): A declaration by a CA of the details of the system and practices it employs in its certificate management operations. A CPS is usually more detailed and procedurally oriented than a CP.

Cross-Certificate: A certificate issued by one CA to another CA for the purpose of establishing a trust relationship between the two CAs.

Cross-certification: The act or process by which a CA certifies a public key of another CA, issuing a public-key certificate to that other CA.

Digital Signature: A value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity.

Directory: A database server or other system that provides information, such as a digital certificate or CRL, about an entity whose name is known.

Federal Bridge Certification Authority (Federal BCA or FBCA): The U.S. Federal Government's mechanism for enabling trust domain interoperability at a level of assurance satisfying E-Authentication levels 1 through 4 using public key certificates.

Public Key Certificate: A digital certificate that binds a system entity's identity to a public key value, and possibly to additional data items; a digitally-signed data structure that attests to the ownership of a public key.

Public Key Infrastructure (PKI): A system of one or more CAs that perform some set of certificate management, archive management, key management, and token management functions for a community of users in an application of asymmetric cryptography. As used in this document, PKI also includes the entire set of policies, processes, and CAs used for the purpose of administering certificates and keys. The term also designates the person or organizational unit within an entity responsible for the following:

(a) Operation of a Certification Authority trusted by one or more users to issue and manage public key certificates and certificate revocation mechanisms; or

(b) Management of:

  (i) Any arrangement under which an entity contracts for the provision of services relating to the issuance and management of public key certificates and certificate revocation lists on its behalf; and

  (ii) Policies and procedures within the entity for managing public key certificates issued on its behalf.

Note: *A PKI remains at all times responsible and accountable for managing the public key certificates it issues or arranges to be issued on behalf of its organization.*

Repository: A system for storing and distributing digital certificates and related information (including CRLs, CPSs, and certificate policies) to certificate users.

STRAC: The Southwest Texas Regional Advisory Council, a Texas non-profit that focuses on the provision of trauma care services, including the credentialing of hospital personnel and first responders in the greater San Antonio region.

STRAC Bridge Certification Authority (STRAC BCA): STRAC's mechanism for enabling trust domain interoperability at a level of assurance satisfying E-Authentication levels 1 through 4 using public key certificates.

STRAC Public Key Infrastructure Management Authority (SPKIMA): The body responsible for operating the STRAC Bridge Certification Authority at the direction of the STRAC Public Key Infrastructure Policy Authority.

STRAC Public Key Infrastructure Policy Authority (SPKIPA): The body responsible for setting, implementing, and administering policy decisions regarding PKI interoperability that uses the STRAC Bridge Certification Authority. The STRAC Public Key Infrastructure Policy Authority directs the STRAC Public Key Infrastructure Management Authority and delegates work to it.

Subscriber: An entity other than a CA whose public key is contained in a certificate bound to the entity.

1.7 SPKIPA ACTIVITIES AND DELEGATION

Activities and tasks assigned in this document to the SPKIPA will, where appropriate and in the sole discretion of the SPKIPA, be accomplished by SPKIPA staff or a duly appointed subcommittee or working group of the SPKIPA, such as a certificate policy working group (if the SPKIPA should elect to create one). Where this document calls for the SPKIPA to vote, however, the SPKIPA will do so without delegation.

1.8 APPLICABILITY TO FEDERAL BRIDGE CERTIFICATION AUTHORITY

The STRAC BCA's primary function is to facilitate state, local and healthcare entities in their efforts to adopt the credentials that can be trusted not only among each other, but by federal entities as well. Cross-certification with the Federal BCA is a key avenue for gaining that federal trust.

Cross-certification with the Federal BCA is governed by the Federal PKIPA via a standing and documented methodology, a methodology that is also the basis for the STRAC BCA cross-certification process described in this document. As a result, treating the Federal PKIPA as "Applicant" to cross-certify the Federal BCA with the STRAC BCA would include a number of redundant, unnecessary steps.

Because the STRAC BCA intends to undergo a Federal BCA cross-certification process which is substantially similar to the STRAC BCA's own cross-certification processes, and because a central purpose of the STRAC BCA is to provide state, local and healthcare entities a link to the Federal BCA that enables federal trust up to and including Level of Assurance 4, the cross-certification of the Federal BCA to the STRAC BCA need not follow the full process described in this document. Specifically, the methodology applied to the Federal BCA-STRAC BCA cross-certification (where the Federal PKI is the "Applicant" PKI) must include the following provisions of this document:

Cross-certification Process: Compliance Audit Review (Sec. 2.4)

Cross-certification Process: Negotiation of MOA (Sec. 2.8)

Cross-certification Process: Cross-certification (Sec. 2.9)

Maintenance of Affiliate PKI Relationship with the STRAC BCA (Sec. 3)

1.9 APPLICABILITY TO BRIDGES OTHER THAN THE FEDERAL BCA

The STRAC BCA does not intend to cross-certify with any bridge CAs other than the Federal BCA. Accordingly, this document does not provide a methodology for other bridges to cross-certify

with the STRAC BCA. Should the STRAC BCA determine to cross-certify with a bridge CA other than the Federal BCA, the SPKIPA will revise this document accordingly.

2 CROSS-CERTIFICATION PROCESS

Cross-certifying entity PKIs with the STRAC BCA is a nine-step process. For Applicants seeking cross-certification at Personal Identity Verification – Interoperable (PIV-I), additional documentation and actions are required for steps 1-6. Specifics on what is required are described at each step. The nine steps are:

Step 1: Application Submission
Step 2: Applicant Further Documentation Submission
Step 3: SPKIPA Policy Mapping
Step 4: Compliance Audit Review
Step 5: Analysis of Operational Parameters
Step 6: Technical Review and Testing
Step 7: Application Approval
Step 8: Negotiation Of Memorandum of Agreement (MOA)
Step 9: Cross-certification

Once a completed application has been submitted (Step 1), the SPKIPA votes to accept or reject the application. If the application is accepted, the Applicant submits any further required documentation (Step 2). If the application is rejected, the SPKIPA notifies the Applicant in writing of the decision and provides the reasons (if any) why the application has been rejected.

Once the CP and any additional documentation has been submitted, the SPKIMA and SPKIPA then complete steps 3, 4, 5, and 6. The SPKIMA and the SPKIPA bring any significant concerns raised in completing Steps 3-6 to the attention and possible vote of the SPKIPA. These steps can be worked in parallel, but all must be completed prior to the SPKIPA vote to approve or deny the application (Step 7). If the SPKIPA decides to terminate the cross-certification process, it notifies the Applicant in writing of the decision and provides the reasons why the application has been rejected, if any. If the application is approved, the Applicant and the SPKIPA negotiate an MOA (Step 8), and the Applicant cross-certifies (Step 9) with the STRAC BCA.

2.1 STEP 1: APPLICATION SUBMISSION

To initiate the process of cross-certification with the STRAC BCA, an Applicant must submit a formal application to cross-certify. The application must contain the following:

Name and contact information (email address, phone number and address) for a principal point of contact (POC) and for a secondary POC.
Information on the Applicant's PKI and Repositories (CA product, PKI architecture, and directory product for repository).
The proposed STRAC BCA level(s) of assurance at which cross-certification is sought.
A statement of the benefit to the public that cross-certification would serve.

For non-government Applicants, evidence of the corporate status of the entity responsible for the Applicant PKI and the entity's financial capacity to manage the risks associated with the operation of the PKI. The nature and sufficiency of the corporate status and financial capacity will be determined at the discretion of the SPKIPA on a case-by-case basis.

The signature of an appropriate senior official (an officer or executive) of the organization responsible for the Applicant who is authorized to commit the organization to completing the cross-certification process. Such a commitment would include bearing any expenses incurred by the organization during the cross-certification process, and the authorization of any submission of information or statement required from the Applicant.

Impact of Applicant Adoption of Template CP Language and Intent to Use Support Services

The extent to which Applicant's CP includes language from the Template CP and the extent to which Applicant intends to use Support Services has no impact upon the process described in this Step 1: Application Submission. Applicant must submit the required information and the SPKIPA shall undertake the activities described herein, regardless of the extent to which Applicant's CP includes language from the Template CP and Applicant intends to use intends to use Support Services.

Activities

1. Applicant submits a formal written application to cross-certify with the STRAC BCA to the SPKIPA Chair at an address posted at http://pki.strac.org/bridge/contact. The application will be signed by an appropriate senior official of the Applicant organization.
2. For non-government Applicants, if the SPKIPA elects to proceed with the application, it shall consider the legitimacy and authority of the Applicant organization and representation.
3. The SPKIPA schedules a review of the application at the next available SPKIPA Meeting.
4. The SPKIPA reviews the application.
5. Following review, the SPKIPA votes whether to accept or reject the application. A record of the discussion, and vote, and a copy of the application are kept in the minutes of the SPKIPA meeting. The SPKIPA decision to accept or reject the application is entirely at the discretion of the SPKIPA; the SPKIPA can reject or cease to process the application at any time for any lawful reason, or for no reason, at its sole discretion.
6. The SPKIPA Chair communicates the decision to proceed or not to proceed to the Applicant POC and to the SPKIPA members.
    a. If the decision is to proceed,

The Applicant is instructed to provide any additional documentation to the SPKIPA Chair as specified in Section 2.2, Step 2: FURTHER Documentation Submission,

The SPKIPA prepares to undertake mapping of the Applicant's CP(s), review of compliance audit information, and analysis of any additional Applicant documents, policies, or practices requested by the SPKIPA.

The SPKIPA Chair authorizes the SPKIMA to initiate technical review and testing, and to initiate PIV-I Card testing if the application includes a request for PIV-I.

At the behest of Applicant, the SPKIPA could, in its sole discretion, execute a Non-Disclosure Agreement (NDA) to ensure that information presented during the application process will be treated in compliance with the terms of the agreement.

b. If the decision is not to proceed,

The SPKIPA Chair notifies the Applicant POC in writing and provides the reasons why the request has been rejected, if any.

2.2 STEP 2: FURTHER DOCUMENTATION SUBMISSION

The Applicant must submit any further documentation requested by the SPKIPA to support policy, audit compliance, operational analysis, and technical reviews. All documentation must be submitted in electronic format to the SPKIPA Chair at an address posted at http://pki.strac.org/bridge/contact. Signed documents should be submitted in PDF format. Other documents can be submitted in either Adobe Acrobat PDF or Microsoft Office compatible formats. A checklist of documents to be submitted is also provided as Appendix A.

The SPKIPA will review Applicant documentation to ensure that the Applicant PKI is operated to a level of assurance comparable to the requirements in the STRAC BCA CP. To support this process, the SPKIPA will use a mapping approach as described in Section 2.3, below. Evidence of compliant operation must also be provided through an independent compliance audit performed by a qualified evaluator/auditor, as described in detail below. Therefore, Applicants must submit the following:

CP in the IETF RFC 3647, "*Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*" [RFC 3647] format, unless prior approval to submit in other format has been granted.

Identification of which of the Applicant's OIDs are to be considered for cross-certification at which assurance levels.

Principal CA Certification Practice Statement (CPS).

Other documentation needed to show evidence of comparability between the Applicant PKI and the requirements in the STRAC BCA CP, as identified by the SPKIPA.

A signed third-party Auditor Letter of Compliance summarizing the results of an audit of Applicant's PKI operations that attests to the Applicant's claim that its PKI is operated in accordance with its CPS, and that the CPS implements the requirements of the CP.

Any additional Applicant POC information necessary to support the remaining steps of the application process.

The Applicant must demonstrate that its PKI is technically compatible with the STRAC BCA. This technical information includes the architecture of the PKI and all URIs and repositories included to support the configuration of certificates issued by the Applicant. Applicants must submit the following documentation to support the technical review:

Applicant PKI Architecture including a designated Principal CA and a list of subordinate CAs or cross-certified CAs within the PKI.

List of CAs that have any other trust relationship with the Applicant PKI Principal CA, such as cross-certifications with other PKIs external to the Applicant PKI and the SPKI.

Hierarchical DN relationships, if any, with other existing Affiliate PKIs (PKIs already cross-certified with the SPKI).

Any additional repositories to support URLs in Applicant PKI certificates.

Any additional certificate status mechanisms in the Applicant PKI.

Configuration of certificates issued by the Applicant PKI.

Capability of Applicant PKI to produce certificates conforming to the "*STRAC PKI Certificate and CRL Extensions Profile*" [STRAC PKI-Prof].

- For PIV-I policy level, Applicant conformance with "*X.509 Certificate and Certificate Revocation List Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards*" [PIV-I Profile] is also required.

Statement of whether algorithms used by the Principal CA or by any other CA in the Applicant PKI architecture are executed in conformance with the "Digital Signature Standard" [FIPS 186]. If not, specify the standard with which it complies.

Impact of Applicant Adoption of Template CP Language and Intent to Use Support Services

The extent to which Applicant's CP includes language from the Template CP and the extent to which Applicant intends to use Support Services has no impact upon the process described in this Step 2: Further Documentation Submission. Applicant must submit the required information and the SPKIPA shall undertake the activities described herein, regardless of the extent to which Applicant's CP includes language from the Template CP and Applicant intends to use Support Services.

Activities

1. Applicant submits required documents to the SPKIPA.
2. SPKIPA uses policy and compliance audit documents to conduct Steps 3, 4, and 5, which can be conducted in parallel.
3. SPKIPA Chair forwards technical documents to the SPKIMA. These documents are used by the SPKIMA to conduct Step 6, which can be conducted in parallel with Steps 3, 4, and 5.

2.3 STEP 3: POLICY MAPPING

Policy mapping is the process of comparing and contrasting the Applicant CP to the STRAC BCA CP and evaluating the extent to which the Applicant demonstrates policies, practices, and procedures consistent with those of the STRAC BCA CP. As noted in Section 1.5, above, the SPKIPA intends to help applicants for cross-certification to the STRAC BCA by providing them with suggested CP language for their adoption. This Template CP will be created by the SPKIPA specifically to comply with the STRAC BCA CP.

Where the Applicant generally adopts the suggested CP language, the SPKIPA will use a mapping approach such as a redline comparison of Applicant's CP to the suggested CP language to identify differences for specific compliance analysis by the SPKIPA. Where the Applicant's CP varies so substantially from the suggested CP language that a redline approach is unworkable, the SPKIPA will develop a mapping matrix document to aid the Applicant in demonstrating that each provision of the STRAC BCA CP maps to the Applicant CP, and the SPKIPA will perform a white space review of the Applicant's entire CP to ensure the absence of non-compliant provisions.

In any event, regardless of the content of the Applicant's CP, it is the Applicant's responsibility to demonstrate to the SPKIPA's satisfaction that Applicant's policies, practices, and procedures are consistent with those of the STRAC BCA CP. If a STRAC BCA CP requirement is not contained in the Applicant CP, but rather is contained in other documents maintained by the Applicant, the Applicant CP must reference the associated document to ensure that it will be included in any compliance audits, and must submit the associated documents containing the requirements to the SPKIPA to be included in the policy mapping. When conducting the policy mapping exercise, the SPKIPA will:

Analyze the Applicant's CP and documentation referenced in the Applicant's CP that is necessary to fulfill a requirement of the STRAC BCA CP.

Identify any STRAC BCA CP requirements not met by the Applicant CP and associated documentation and suggest any changes as appropriate.

If the Applicant submits a revised CP, review the revisions. When the SPKIPA and Applicant agree the mapping is comparable, the SPKIPA will review the final Applicant CP (sometimes called a "white space review") to:

1. Ensure the CP matches the Applicant's self-assertions; and
2. Ensure there are no contradictions or inconsistencies in the Applicant's CP.

At the conclusion of the mapping exercise, the SPKIPA prepares a report identifying any remaining discrepancies and identifying any additional documentation used in the mapping process, and forwards it to the SPKIPA Chair.

Impact of Applicant Adoption of Template CP Language and Intent to Use Support Services

The extent to which Applicant's CP includes language from the Template CP and the extent to which Applicant intends to use Support Services will impact the process described in this Step 3: Policy Mapping as follows:

1. If the Applicant largely adopts the language of the Template CP, the SPKIPA will use a textual comparison approach, such as a redline, to indicate the differences between the Applicant CP and the Template CP.
2. Where the Applicant's CP varies so substantially from the Template CP that a redline approach is unworkable, the SPKIPA will develop a mapping matrix document to aid the Applicant in demonstrating that each provision of the STRAC BCA CP maps to the Applicant CP, and the SPKIPA will perform a white space review of the Applicant's entire CP to ensure the absence of non-compliant provisions.

With the exception of the two items listed above, the extent to which Applicant's CP includes language from the Template CP and the extent to which Applicant intends to use Support Services will have no impact upon the process described in this Step 3: Policy Mapping. Applicant must submit the required information and the SPKIPA shall undertake the activities described herein, regardless of the extent to which Applicant's CP includes language from the Template CP and Applicant intends to use Support Services.

Activities

Note: *This is a participatory process. The Applicant will be required to make a knowledgeable and authorized representative available to the SPKIPA for the Certificate Policy mapping process. This representative shall not be the compliance auditor.*

1. The SPKIPA reviews and evaluates the Applicant's CP and associated documentation as described in this section and determines the extent to which the Applicant demonstrates policies, practices, and procedures consistent with those of the STRAC BCA CP.
2. The SPKIPA provides the Applicant POC with a summary of the review identifying any discrepancies.
3. The Applicant addresses identified discrepancies by updating its CP or including additional documents and returns the updated documentation to the SPKIPA. If additional documentation is offered, the documentation must be referenced in the appropriate sections of the CP. Applicant must specify any changes its updated documents make to earlier-submitted documents.
4. Steps 1-3 shall be repeated as necessary until the SPKIPA determines either that the Applicant has addressed all discrepancies or that the Applicant is not able or willing to address remaining discrepancies.
5. Upon completion of the mapping process, the SPKIPA prepares a mapping report identifying any remaining discrepancies, identifying additional documentation used in the mapping process, and containing a recommendation for acceptance or rejection.

6. If the SPKIPA recommends rejection or the mapping report identifies significant discrepancies, the SPKIPA will hold a discussion and vote. If no significant discrepancies are reported, the policy mapping step is complete.
7. If a vote is to be held, the SPKIPA reviews the mapping report and votes whether to accept or reject the mapping step as complete. A record of the discussion and vote are kept in the Minutes of the SPKIPA meeting.
    a. If the decision is to accept, the SPKIPA Chair provides the mapping report to the SPKIMA for archival.
    b. If the decision is to reject,
        - The SPKIPA Chair notifies the Applicant POC in writing of the decision.
        - No further cross-certification steps will be completed unless the Applicant satisfactorily resolves any identified issues.

2.4 STEP 4: COMPLIANCE AUDIT REVIEW

The trustworthiness of an Applicant PKI must be evaluated for the purposes of cross-certification. This evaluation must be performed by an independent third party who has demonstrated knowledge of PKI systems using explicitly-defined and appropriate auditing methodologies. Specific SPKIPA qualification requirements for the evaluator/auditor can be found in the STRAC BCA CP, Section 8.2, *Identify and Qualifications of Assessor*, and Section 8.3, *Assessor's Relationship to Assessed Entity*.

The SPKIPA can request the bona fides of any third-party compliance auditor indicating that the auditor meets the specified requirements.

This evidence must include a statement that audit reports showing compliance are on file for all CA components of the Applicant PKI. Evidence could include additional audit letters for various components of the Applicant PKI such as subordinate CAs and Registration Authorities (RAs) if these components are not covered in the PKI's Auditor Letter of Compliance.

The Auditor Letter of Compliance required by the SPKIPA must meet the requirements of the Federal PKIPA for cross-certification to the Federal BCA, as identified in the Federal BCA Audit Letter Template, provided as Appendix B to the Federal PKIPA's April 10, 2012 audit guidance ("FPKI Compliance Audit Requirements"). In addition, the Audit Letter of Compliance must indicate whether the audit met the requirements reflected in the FPKIPA's "Compliance Audit Requirements," Version v2.0.0 (Apr. 10, 2012).

Impact of Applicant Adoption of Template CP Language and Intent to Use Support Services

The extent to which Applicant's CP includes language from the Template CP and the extent to which Applicant intends to use Support Services has no impact upon the process described in this Step 4: Compliance Audit Review. Specifically:

- The SPKIPA is comprised of diverse entities (those with CAs cross-certified to the STRAC Bridge CA) pursuant to its Charter and is not controlled by STRAC, though STRAC is a member of the SPKIPA.
- The SPKIMA, which includes individuals associated with STRAC, is directed by and answers to the SPKIPA, which is not controlled by STRAC.
- Any individual helping via Support Services to operate Applicant's CA on behalf of Applicant will be associated with the STRAC Bridge CA only through the SPKIMA.
- The STRAC Bridge CA's audit and Auditor Letter of Compliance are prepared by an independent auditor, including an assessment of the performance of SPKIMA personnel; they are reviewed and evaluated by the SPKIPA.
- The Applicant CA's audit and Auditor Letter of Compliance are prepared by an independent auditor, including an assessment of the performance of any individuals operating Applicant's CA via Support Services who also serve on the SPKIMA; the Auditor Letter of Compliance is reviewed and evaluated by the SPKIPA.

Applicant must submit the required information and the SPKIPA shall undertake the activities described herein, regardless of the extent to which Applicant's CP includes language from the Template CP and Applicant intends to use Support Services.

Activities

1. The SPKIPA reviews the Applicant's Auditor Letter of Compliance and determines whether it does the following:
    a. States whether the audit met the requirements reflected in the FPKIPA's "Compliance Audit Requirements," Version v2.0.0 (Apr. 10, 2012).
    b. Identifies the individuals performing the audit.
    c. Identifies the experience these individuals have in auditing PKI systems.
    d. Describes the relationship between the auditor and the Applicant.
    e. States when the audit was performed.
    f. States whether a particular methodology was used, and if so, what methodology.
    g. Specifies which documents were reviewed as a part of the audit, including document dates and version numbers.
    h. States that the Applicant's Principal CA CPS conforms to the requirements of the Applicant CP.
    i. States that the Applicant's Principal CA is being operated in conformance with its CPS.
    j. For PKIs with multiple CAs, states that audit reports showing compliance were on file for additional CA components of the Applicant PKI, or are an included part of the report.
2. If the Applicant's Auditor Letter of Compliance is not sufficient, the SPKIPA will provide feedback to the Applicant POC.

3. If the Applicant submits an updated Auditor Letter of Compliance and/or additional information to address any SPKIPA feedback, review the revised letter.
4. Activities 1-3 shall be repeated as necessary until the SPKIPA determines either that the Applicant PKI has met the compliance audit requirements or that the Applicant is not able or willing to address remaining issues.
5. The SPKIPA provides the final version of the Auditor Letter of Compliance received from the Applicant along with a recommendation as to its sufficiency in a compliance review report to the SPKIPA Chair.
6. If the SPKIPA determines that the Auditor Letter of Compliance is not sufficient or identifies other significant discrepancies, the SPKIPA could hold a discussion and vote. If no significant discrepancies are reported, the compliance audit review step is complete.
7. If a vote is to be held, the SPKIPA reviews the compliance review report and votes whether to accept or reject the Applicant's Auditor Letter of Compliance as adequate. A record of the discussion and vote are kept in the Minutes of the SPKIPA meeting. If the decision is to reject,
    a. The SPKIPA Chair notifies the Applicant POC in writing of the decision. The notification provides the reasons, if any, why the Applicant's Auditor Letter of Compliance has been found inadequate.
    b. No further cross-certification steps will be completed unless the Applicant satisfactorily resolves the identified issues.
8. If the decision is to accept the Applicant's Auditor Letter of Compliance as adequate, the Compliance Audit Review step is complete. The SPKIPA Chair provides the Auditor Letter of Compliance and the compliance review report to the SPKIMA for archival.

2.5 STEP 5: ANALYSIS OF OPERATIONAL PARAMETERS

Applicants must demonstrate that their operational parameters are consistent with the parameters of the STRAC BCA CP and will not have an adverse effect on the SPKIPA or on relying parties that rely on certificates based on cross-certificate trust paths. In this Criteria and Methodology, "operational parameters" refers to any policies, processes, or practices not addressed in other steps of the STRAC BCA cross-certification process; this Step 5 is intended to ensure the SPKIPA has flexibility to address any miscellaneous issues it determines are pertinent to its decision on the application.

If the SPKIPA identifies concerns with language contained in the Applicant's CP or other documentation, or with any information received by the SPKIPA, the SPKIPA will request further or updated documentation or information addressing the identified concerns. Upon completion of the analysis, the SPKIPA documents its findings in the operational parameters analysis report and forwards it to the SPKIPA Chair.

Impact of Applicant Adoption of Template CP Language and Intent to Use Support Services

The extent to which Applicant's CP includes language from the Template CP and the extent to which Applicant intends to use Support Services has no impact upon the process described in this Step 5: Analysis of Operational Parameters. Applicant must submit the required information and the SPKIPA shall undertake the activities described herein, regardless of the extent to which Applicant's CP includes language from the Template CP and Applicant intends to use Support Services.

Activities

1. The SPKIPA performs an analysis of the Applicant CP, any other associated documentation provided by the Applicant, and other relevant information to ensure that the policies, processes, and practices of Applicant's PKI are consistent with those of the STRAC BCA.
2. The SPKIPA informs the Applicant of any identified concerns and requests further or updated documentation or information to address those concerns.
3. Activities 1-2 shall be repeated as necessary until the SPKIPA determines either that the Applicant has addressed all concerns or that the Applicant is not able or willing to address remaining concerns.
4. Upon completion of the operational parameters analysis, the SPKIPA prepares an operational parameters analysis report.
5. If the SPKIPA identifies significant discrepancies in the operational parameters analysis report, the SPKIPA schedules the matter for a discussion and vote. If no significant discrepancies are reported, the analysis of operational parameters step is complete.
6. If a vote is to be held, the SPKIPA reviews the operational parameters analysis report and votes whether to accept or reject the operational parameters step as complete. A record of the discussion and vote are kept in the Minutes of the SPKIPA meeting.
    a. If the decision is to accept, the SPKIPA Chair provides the operational parameters analysis report to the SPKIMA for archival.
    b. If the decision is to reject,
        - The SPKIPA Chair notifies the Applicant POC in writing of the decision. The notification could provide the reasons, if any, why the request for cross-certification has been rejected and any Applicant recourse.
        - No further cross-certification steps will be completed unless the Applicant satisfactorily resolves the identified issues.

2.6 STEP 6: TECHNICAL REVIEW AND TESTING

Applicants must demonstrate that its PKI is technically compatible with the STRAC BCA. Technical compatibility is determined through a review of the technical information submitted

by the Applicant and through interoperability testing. Applicants for PIV-I policy levels are also required to go through PIV-I Card Testing.

The SPKIMA reviews the Applicant PKI architecture, any existing trust relationships that the Applicant PKI has entered into, and the conformance of the Applicant PKI certificates to the requirements set out in the STRAC BCA CP.

Technical interoperability testing is used to ensure technical interoperability between the STRAC BCA and the Applicant PKI. The objective of this step is to determine whether there can be a successful generation and exchange of conformant cross-certificates, to identify and resolve any incompatibilities between the technologies of the STRAC BCA and Applicant PKI products, and to minimize the risk of introducing incompatibilities with Affiliate PKIs.

Technical personnel representing the Applicant will be required to work with the SPKIMA to complete the technical interoperability testing. Technical interoperability testing at a minimum will demonstrate:

- Network connectivity can be achieved using all required protocols.
- The cross-certificate is correctly constructed by the STRAC BCA, and exchanged and recognized by the Applicant PKI CA.
- The cross-certificate is correctly constructed by the Applicant PKI CA, exchanged with the STRAC BCA, and recognized by the STRAC BCA.
- That a test transaction using a test subscriber of the Applicant PKI can be successfully validated.
- The STRAC BCA and the Applicant PKI can share revocation information, such as via appropriate repositories.

If PIV-I is requested, and federal PIV-I card testing is required, the Applicant will provide a PIV-I Card to the FICAM Test Lab or other testing entity identified by the Federal PKI Policy Authority (Federal PKIPA) for logical testing and Physical Access Control System (PACS) testing. PACS testing requires the person whose biometrics are on the Card to be present during testing. The Applicant must authorize the Federal PKIPA's testing entity to share with the SPKIMA all aspects of the testing procedure and results; and the Applicant must provide those results to the SPKIMA. The SPKIMA, at the SPKIPA's discretion, will accept testing performed by the Federal PKIPA's testing entity.

The SPKIMA documents the results of the interoperability testing, including a description of any deficiencies identified during the test, in a technical analysis report and forwards the report to the SPKIPA Chair. Deficiencies will include technical interoperability deficiencies and potential performance issues that were not specifically identified by the test criteria. The report will also include the anticipated consequences of the deficiencies and a recommendation by the SPKIMA.

The SPKIMA documents the results of the PIV-I Card Testing in a PIV-I card test report and provides the report to the SPKIPA Chair.

Impact of Applicant Adoption of Template CP Language and Intent to Use Support Services

The extent to which Applicant's CP includes language from the Template CP and the extent to which Applicant intends to use Support Services has no impact upon the process described in this Step 6: Technical Review and Testing. Specifically, with regard to testing, PIV-I Card Testing will be accomplished by the Federal PKIPA's designated testing entity as described above, and interoperability testing will occur among the STRAC BCA and the Applicant CA regardless of the location of the Applicant CA and usage of Support Services by Applicant. Applicant must submit the required information and the SPKIPA shall undertake the activities described herein, regardless of the extent to which Applicant's CP includes language from the Template CP and Applicant intends to use Support Services.

Activities

1. The SPKIMA and the Applicant determine if any constraints need to be placed in any cross-certificates issued between the STRAC BCA and the Applicant PKI.
2. The SPKIMA schedules an initial meeting with the Applicant to discuss the technical interoperability process. The following occurs at this initial meeting.
    a. The SPKIMA provides the Applicant information on the technical testing process used by the SPKIMA,
    b. The Applicant provides the SPKIMA with information on the technical configuration of the Applicant PKI to permit it and the SPKIMA testing facility to interoperate at a technical level.
3. Having shared their respective technical data, the Applicant and the SPKIMA undertake a test cross-certification between their respective environments. The SPKIMA reviews the certificates provided against [STRAC PKI-Prof] and [PIV-I Profile] for conformance.
4. Upon completion of the interoperability testing, the SPKIMA prepares a technical analysis report identifying any concerns from the documentation review, a description of any deficiencies identified during the testing, the anticipated consequences of the deficiencies, and a recommendation for acceptance or rejection.
5. If the SPKIMA identifies significant deficiencies, no further cross-certification steps will be completed unless the Applicant satisfactorily resolves the identified issues. When no significant discrepancies remain, the SPKIMA notifies the SPKIPA of the completion of the technical review step.
6. If the Applicant is seeking cross-certification as a PIV-I Issuer, the Applicant provides a test Card to the Federal PKIPA's testing entity to perform PIV-I Card testing.
    a. PIV-I Applicants must demonstrate that PIV-I Cards they issue at a minimum conform to all the requirements the Federal PKIPA imposes on cards issued by CAs cross-certified directly with the Federal Bridge CA.
    b. Applicant provides test cards to the Federal PKIPA's testing entity that reflect a cross-certification of the Applicant CA with the STRAC BCA test environment.

c. Testing is performed by the Federal PKIPA's testing entity. There are three (3) categories of PIV-I Card testing (Sub-activities associated with testing of PIV-I cards are set by the Federal PKIPA's testing entity.):

   - PIV-I Card validation;
   - PIV-I Data Model Validation; and
   - PIV-I Application Interoperability Validation.

d. The Applicant authorizes the Federal PKIPA's testing entity to share with the SPKIMA all aspects of the testing procedure and results and must provide those results to the SPKIMA.

e. The SPKIMA prepares a PIV-I Card Testing report including the results from the testing performed by the Federal PKIPA's testing entity.

2.7 STEP 7: APPLICATION APPROVAL

The objective of this step is for the SPKIPA to review the results of the previous steps and determine whether to approve the issuance of a cross-certificate to the Applicant PKI. This step is performed after the completion of Steps 3-6, regardless of the order of completion of those steps.

The overall evaluation of the Applicant PKI's comparability and trustworthiness involves an assessment of the information collected during the previous steps, as provided in the following documents.

- Certificate policy mapping report
- Auditor Letter of Compliance and compliance review report
- Operational parameters analysis report
- Technical analysis report
- For PIV-I Applicants only, a PIV-I Card test report

The SPKIPA reviews this information and any other concerns or other issues discussed during SPKIPA meetings regarding the application, including the results of any requested interim votes. Once the SPKIPA has completed review and discussions, the SPKIPA votes whether to cross-certify with the Applicant.

Impact of Applicant Adoption of Template CP Language and Intent to Use Support Services

The extent to which Applicant's CP includes language from the Template CP and the extent to which Applicant intends to use Support Services has no impact upon the process described in this Step 7: Application Approval. The SPKIPA shall undertake the activities described herein, regardless of the extent to which Applicant's CP includes language from the Template CP and Applicant intends to use Support Services.

Activities

1. The SPKIPA reviews the results from Steps 3-6 as identified in the certificate policy mapping report, Auditor Letter of Compliance and compliance review report, operational parameters analysis report, technical analysis report, and (if applicable) PIV-I Testing report, and discusses any remaining issues.
2. If required, the SPKIPA discusses remaining issues with representatives of the Applicant, such as conditions identified in previous reports and votes associated with the Application.
3. Following discussion, the SPKIPA votes whether to cross-certify with the Applicant. The documentation provided by the SPKIMA and SPKIPA and a record of the discussion and vote are kept in the Minutes of the SPKIPA meeting.
    a. If the decision is to cross-certify with the Applicant, the SPKIPA Chair notifies the Applicant by formal letter.
    b. If the decision is to deny the Applicant's request for cross-certification,
4. The SPKIPA Chair notifies the Applicant POC in writing of the decision. The notice provides the reasons, if any, why the request for cross-certification has been rejected.
5. No further cross-certification steps will be completed unless the Applicant satisfactorily resolves the identified issues.

2.8 STEP 8: NEGOTIATION OF MEMORANDUM OF AGREEMENT (MOA)

The relationship between the SPKIPA and an entity with a cross-certified CA will be governed by the cross-certification MOA to be signed by a cognizant authority from the entity and by the SPKIPA Chair (or designee on the SPKIPA) on the recommendation of the SPKIPA.

To facilitate the construction of similar MOAs for use in connection with cross-certification with the Federal BCA, the Federal PKIPA has produced the "Template for use by the U.S. Federal PKI Policy Authority for Cross-certifying with U.S. federal agencies and other U.S. Federal Entities, with U.S. state and local governments and U.S. private sector Entities, and with Governments of other Nations;" the SPKIPA could use this document as a starting point for negotiations regarding the terms of the SPKIPA MOA with the Applicant for cross-certification with the STRAC BCA. If during the application process, the documents used during the mapping process change, or new SPKIPA or Applicant conditions are introduced, those changes must be incorporated into the MOA negotiation.

The negotiated MOA must ensure the following elements:

- The Applicant accepts the obligations and other terms of the STRAC PKIPA Charter.
- The obligations imposed on the SPKI and its members are acceptable.
- The Applicant commits to meet the obligations the SPKIPA imposes upon Affiliates, including compliance with the STRAC BCA CP.
- Any obligations imposed upon relying parties of SPKI member PKIs are acceptable.

- Any conditions identified during the application review process have been included.
- Applicant documentation, including the CP and any other documents used to complete the mapping process, are incorporated by reference and the Applicant is obligated to submit advance notice of any changes to these documents to the SPKIPA.

The SPKIPA reviews the MOA language and works to achieve agreement with the Applicant. Any unresolved issues will be reviewed and decided by the SPKIPA. When no issues remain unresolved, the MOA is signed by the SPKIPA Chair and a senior, authorized official from the Applicant.

Impact of Applicant Adoption of Template CP Language and Intent to Use Support Services

The extent to which Applicant's CP includes language from the Template CP and the extent to which Applicant intends to use Support Services has no impact upon the process described in this Step 8: Negotiation of Memorandum of Agreement (MOA). The SPKIPA and the Applicant shall undertake the activities described herein, regardless of the extent to which Applicant's CP includes language from the Template CP and Applicant intends to use Support Services.

Activities

1. The SPKIPA and Applicant POC negotiate the MOA. The SPKIPA ensures that all referenced documentation described in the certificate policy mapping report is included in the MOA.
2. If the SPKIPA identifies issues with the MOA, the following steps are completed.
    a. The SPKIPA convenes a meeting of the SPKIPA subject matter experts to discuss and resolve identified issues.
    b. If necessary, the SPKIPA works with the Applicant POC to resolve issues and revise the MOA.
    c. The SPKIPA subject matter experts provide their review and the revised MOA to the SPKIPA.
    d. The SPKIPA reviews the updated MOA and votes whether to accept or reject the MOA. A record of the discussion and vote are kept in the Minutes of the SPKIPA meeting.
3. If no issues are identified by the SPKIPA or if the SPKIPA votes to accept the revised MOA, the following steps are completed.
    a. The SPKIPA Chair (or designee on the SPKIPA) signs two (2) originals of the MOA and provides them to the Applicant POC.
    b. The senior, authorized official from the Applicant signs the two (2) originals of the MOA and returns one original to the SPKIPA Chair.

        Note: *These two tasks can be completed in either order – i.e., the Applicant senior official can sign first.*

c. One original is provided to the SPKIMA for archival; any remaining originals are returned to or retained by the Applicant POC.

4. If the SPKIPA votes to reject the revised MOA, the following steps are completed.
    a. The SPKIPA Chair notifies the Applicant POC in writing of the decision. The notice provides the reasons, if any, why the updated MOA has been rejected.
    b. No further cross-certification steps will be completed unless the Applicant satisfactorily resolves the identified issues.

2.9 STEP 9: CROSS-CERTIFICATION

Once the MOA has been signed by the Applicant and the SPKIPA Chair (or designee on the SPKIPA), the remaining step for cross-certification is to issue the cross-certificates themselves. The SPKIPA requests technical and POC information from the Applicant for the cross-certification. Using this information, the SPKIPA Chair issues a Letter of Authorization to the SPKIMA to initiate cross-certification with the Applicant PKI. This Letter of Authorization contains:

- Information identifying key personnel including primary and alternate technical and managerial contacts for the Applicant and the SPKI.
    - Level(s) of assurance of cross-certificates to be issued.
    - Policy OID(s) for inclusion in the cross–certificate.
    - Directory information tree for subject names in certificates issued by the Applicant PKI.
    - Distinguished Name (DN) of the CA.

This information is used to populate the cross-certificate requests and perform the cross-certification process. Following a satisfactory review of the technical data, the production cross-certificates are issued and posted to the appropriate repositories.

Impact of Applicant Adoption of Template CP Language and Intent to Use Support Services

The extent to which Applicant's CP includes language from the Template CP and the extent to which Applicant intends to use Support Services has no impact upon the process described in this Step 9: Cross-Certification. The SPKIPA and the Applicant shall undertake the activities described herein, regardless of the extent to which Applicant's CP includes language from the Template CP and Applicant intends to use Support Services.

Activities

1. The SPKIPA requests technical and POC information from the Applicant for cross-certification.
2. The Applicant provides the requested technical and POC information to the SPKIPA.

3. The SPKIPA prepares and issues a Letter of Authorization to the SPKIMA to initiate cross-certification with the Applicant PKI.
4. The SPKIMA and the Applicant take the necessary procedural and technical steps to issue the production cross-certificate(s).
5. The SPKIMA verifies the extensions in the cross-certificate issued and the cross-certificate received against the information provided by Applicant to verify everything is correct. The SPKIMA also verifies the Subject Key ID is the same as the Subject Key ID provided in the Letter of Authorization.
6. The SPKIMA and Applicant (now an Affiliate) post the cross-certificate(s) to the SPKI and Affiliate PKI Repositories, respectively.
7. The SPKIMA notifies the SPKIPA of the completion of the cross-certification process in the respective production environments.

3 MAINTENANCE OF AFFILIATE PKI RELATIONSHIP WITH THE STRAC BCA

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 the STRAC BCA and the Affiliate PKI.

The maintenance phase provides mechanisms both for managing the relationship between cross-certified entities as required for the proper operation of the arrangement, and for terminating the arrangement if either party contravenes its terms and conditions, or at the desire of either party. The tasks described in this phase are not sequential and they apply as circumstances warrant. They include:

1. Participation in the SPKIPA pursuant to the terms of the SPKIPA Charter.
2. Submission and review of an annual compliance audit report.
3. Renewal of cross-certificate(s).
4. Update of cross-certificate(s).
5. Update of Affiliate PKI documentation referenced in the MOA.
6. Update of STRAC BCA documentation.
7. Problem resolution.
8. Termination.

3.1 PARTICIPATION IN THE SPKI POLICY AUTHORITY

Active participation in the SPKIPA by Affiliates helps to ensure that decisions made by the SPKIPA benefit the entire SPKI member community. All SPKIPA members are expected to participate at all SPKIPA meetings and discussions. Participation in SPKIPA meetings will ensure that Affiliates have a voice in proposed changes to the STRAC BCA. All Affiliates are encouraged to participate in any working groups formed by the SPKIPA, especially those dealing with the development of PKI policies and with technical PKI issues.

Impact of Affiliate Adoption of Template CP Language and Intent to Use Support Services

The extent to which Affiliate's CP includes language from the Template CP and the extent to which Affiliate intends to use Support Services has no impact upon the process described in this Sec. 3.1: Participation in the SPKI Policy Authority. The SPKIPA and the Affiliate shall undertake the activities described herein, regardless of the extent to which Affiliate's CP includes language from the Template CP and Affiliate intends to use Support Services.

Activities:

1. Affiliate identifies one or more POCs to the SPKIPA for inclusion on the SPKIPA mailing list to receive notice of meetings and items up for discussion.
2. Affiliate attends regular SPKIPA meetings in person, via conference call, or via proxy (for voting members), as specified in the SPKIPA Charter.
3. Affiliate provides feedback on topics presented to the SPKIPA.

3.2 SUBMISSION AND REVIEW OF ANNUAL COMPLIANCE AUDIT REPORT

Independent compliance audits are required of the STRAC BCA and all Affiliate PKIs. The SPKIPA must receive from the Affiliate or the auditor an Auditor Letter of Compliance summarizing the successful completion of the annual compliance audit prepared by an independent auditor for each Affiliate. Specific requirements for what the Auditor Letter of Compliance must address are the same as those required in the application process, described in Section 2.4. It is the Affiliate's responsibility to ensure that the Affiliate meets the compliance audit due date; the SPKIPA is not obligated to provide the Affiliate a notification of the compliance audit requirement. The following table indicates how often compliance audits are required.

Assurance Level	Frequency
STRAC BCA Rudimentary	N/A
STRAC BCA Basic	Once every 2 years
STRAC BCA Medium and above	Once every year

Impact of Affiliate Adoption of Template CP Language and Intent to Use Support Services

The extent to which Affiliate's CP includes language from the Template CP and the extent to which Affiliate intends to use Support Services has no impact upon the process described in this Sec. 3.2: Submission and Review of Annual Compliance Audit Report. As in Sec. 2.4, the SPKIPA and the Affiliate shall undertake the audit-related activities described herein, regardless of the extent to which Affiliate's CP includes language from the Template CP and Affiliate intends to use Support Services.

Activities:

1. At the SPKIPA's discretion, it sends a reminder to the Affiliate POC 90-120 days prior to the Affiliate's Annual Auditor Letter of Compliance is due, though such reminder is not guaranteed; it is the Affiliate's obligation to meet the Auditor Letter of Compliance requirements.
2. The Affiliate POC or qualified auditor provides the Annual Auditor Letter of Compliance to the SPKIPA no more than two months after the end of the frequency period for the previous Auditor Letter of Compliance.
3. The SPKIPA reviews the Annual Auditor Letter of Compliance and develops a compliance review report recommending whether the letter is satisfactory.
4. The SPKIPA, following review of the Annual Auditor Letter of Compliance and the compliance review report, determines whether the report is acceptable.
5. The SPKIPA Chair communicates the decision of acceptability of the Annual Auditor Letter of Compliance to the Affiliate POC.
    a. If the Annual Auditor Letter of Compliance is acceptable, the Chair notifies the Affiliate POC that it is acceptable and forwards a copy of the Letter and the report to the SPKIMA.
    b. If the Annual Auditor Letter of Compliance is not acceptable, the Chair notifies the Affiliate POC in writing of the rejection. The notice provides the reason, if any, for rejection, along with a deadline for the Affiliate POC or auditor to submit an updated Annual Auditor Letter of Compliance. Failure of the Affiliate or auditor to provide an acceptable Annual Auditor Letter of Compliance within the specified time could be grounds for termination of the MOA and revocation of the cross-certificate, at the SPKIPA's discretion. Therefore, issues regarding the audit will be brought to the attention of the SPKIPA for discussion and possible vote.

3.3 RENEWAL OF CROSS-CERTIFICATE(S)

Cross-certificates must be re-issued as a result of normal expiration.

Impact of Affiliate Adoption of Template CP Language and Intent to Use Support Services

The extent to which Affiliate's CP includes language from the Template CP and the extent to which Affiliate intends to use Support Services has no impact upon the process described in this Sec. 3.3: Renewal of Cross-Certificate(s). The SPKIPA and the Affiliate shall undertake the renewal activities described herein, regardless of the extent to which Affiliate's CP includes language from the Template CP and Affiliate intends to use Support Services.

Activities:

1. It is the responsibility of the Affiliate to contact the SPKIPA and SPKIMA for cross-certificate renewal 90 - 120 days prior to expiration of an existing cross-certificate. Upon such contact, the SPKIMA will provide the SPKIPA and Affiliate notice containing a summary of all relevant issues and information from various documents, including:
   - The most recent MOA between the SPKIPA and the Affiliate.
   - The most recent compliance review reports (the most recent Affiliate Report for review by the SPKIPA Chair, and the most recent STRAC BCA Report for review by the Affiliate).
   - For PIV-I Issuers only, the most recent report regarding PIV-I card interoperability.
   - All Problem Resolution Reports related to the Affiliate since the cross-certificate was last renewed, if any.
   - All Change Management Reports since the cross-certificate was last renewed tracking the technical changes made to the STRAC BCA that could affect interoperability, if any.
2. The SPKIPA will review the documentation and provide a report to the Chair for decision or referral to the full SPKIPA for a vote.
   a. If the Chair has no concerns,
      i. The Chair reviews the MOA with the Affiliate and updates the MOA as appropriate (POC information as well as policy OIDs might have changed since the last certificate issuance.)
      ii. The Chair authorizes the SPKIMA in writing to re-issue the cross-certificate.
   b. If the Chair does not believe the cross-certificate should be renewed,
      i. The Chair convenes a meeting of the SPKIMA and SPKIPA.
      ii. The SPKIMA and SPKIPA develop a report identifying issues (if any) and proposed resolutions and provides this report to the SPKIPA.
      iii. The SPKIPA votes to renew or not renew the cross-certificate. At the SPKIPA's discretion, failure to resolve any open issues could be grounds for terminating the MOA and permitting the cross-certificate be to expire, or the SPKIPA could vote to immediately revoke the current cross-certificate.
3. Upon receipt of the authorization, the SPKIMA arranges with the Affiliate to renew the cross-certificate.

3.4 UPDATE OF TECHNICAL ARCHITECTURE OR CROSS-CERTIFICATE(S)

If an Affiliate chooses to update its technical architecture, including its Identity Management Card Management System, updates must be provided to the SPKIPA for a determination if the

updated architecture affects the terms of the MOA or the technical interoperability between the STRAC BCA and the Affiliate PKI. Examples of changes to an architecture that must be provided to the SPKIPA include but are not limited to the addition of new CAs, changes to Affiliate PKI repositories that introduce or eliminate support for different protocols or that might affect interoperability, and changes that would require the Issuers to retest their PIV-I card compatibility.

If the SPKIMA chooses to make significant changes to the SPKI infrastructure, updates must be provided to the SPKIPA and all Affiliates for a determination as to whether the updated architecture affects the terms of the MOA or technical interoperability between the SPKI and any Affiliate PKIs.

Updating of cross-certificates can be requested by the SPKIPA, the SPKIMA, or the Affiliate to modify information contained in the certificate. All requests for modification to cross-certificates are provided to the SPKIPA for review and approval.

Impact of Affiliate Adoption of Template CP Language and Intent to Use Support Services

The extent to which Affiliate's CP includes language from the Template CP and the extent to which Affiliate intends to use Support Services has no impact upon the process described in this Sec. 3.4: Update of Technical Architecture or Cross-Certificate(s). The SPKIPA and the Affiliate shall undertake the cross-certificate update activities described herein, regardless of the extent to which Affiliate's CP includes language from the Template CP and Affiliate intends to use Support Services.

Activities:

1. If an Affiliate desires to modify its technical architecture,
    a. The Affiliate notifies the SPKIPA of the desired modification.
    b. If applicable, the SPKIPA notifies the SPKIMA of the desired change and solicits feedback on the impact of the change to the STRAC BCA relationship.
    c. The SPKIPA reviews the desired changes and any feedback from the SPKIMA, and determines whether the desired technical architecture changes will bring the Affiliate out of compliance with its MOA and/or its cross-certification mapping. In such a case, the SPKIPA will alert the Affiliate of the findings.
    d. If a new MOA is required, the Affiliate POC submits a revised MOA to the SPKIPA.
        i. The SPKIPA, at its discretion, negotiates with the Applicant POC to agree upon a revised MOA. The SPKIPA ensures that all relevant documentation is included in the MOA, and the SPKIPA Chair (or designee on the SPKIPA) and a senior authorized official from the Affiliate would sign the revised MOA.
        ii. At the SPKIPA's discretion, failure to resolve any open issues could be grounds for termination of the MOA, and the cross-certificate will be

allowed to expire, or the SPKIPA could vote to immediately revoke the current cross-certificate. The SPKIPA will notify the Affiliate of the results of any vote.

2. If the SPKI technical architecture is to be modified, the SPKIMA documents the changes in a Change Request. For any significant change that might affect the relationship between the SPKI and Affiliate PKIs, the SPKIMA will provide the Change Request to the SPKIPA and all Affiliates for a determination as to whether the updated architecture affects the terms of the MOA or technical interoperability between the SPKI and any Affiliate PKIs.

3.5 UPDATE OF AFFILIATE PKI DOCUMENTATION

Affiliates can update their CPs or other documentation referenced in their SPKIPA MOAs. Since the approval to cross-certify with the STRAC BCA is based on the information contained in this documentation, changes to Affiliate PKI documentation, with the exception of maintaining compliance with changes to the STRAC BCA CP, require a review by the SPKIPA and possible acceptance vote by the SPKIPA to ensure that the changes do not affect Affiliate PKI compliance with STRAC BCA CP requirements. This review should take place prior to implementing any changes.

In addition to updates to CP information, Affiliate Bridges (the STRAC BCA intends only to cross-certify with one Bridge: the Federal BCA), must notify the SPKIPA if any of the following changes:

- Affiliate Bridge criteria and methodology or equivalent.
- Affiliate Bridge charter.
- Community served by the Affiliate Bridge.
- Any waivers issued by the Affiliate Bridge to any of its member PKIs.
- Affiliate PKI Technical Interoperability Testing process or document.
- For PIV-I Issuers only, PIV-I Card Interoperability Test process or document.

Impact of Affiliate Adoption of Template CP Language and Intent to Use Support Services

The extent to which Affiliate's CP includes language from the Template CP and the extent to which Affiliate intends to use Support Services has no impact upon the process described in this Sec. 3.5: Update of Affiliate PKI Documentation. The SPKIPA and the Affiliate shall undertake the Affiliate documentation update activities described herein, regardless of the extent to which Affiliate's CP includes language from the Template CP and Affiliate intends to use Support Services.

Activities:

1. The Affiliate provides proposed document changes to the SPKIPA for review and discussion. Even if Affiliate provides a draft copy to the SPKIPA for review prior to

finalizing the changes, the Affiliate must still provide the final accepted version of the document to the SPKIPA.

2. The SPKIPA reviews the proposed document changes and determines whether the changes have an effect on Affiliate compliance.
3. The SPKIPA Chair communicates the decision to the Affiliate POC.
    a. If the determination is that the changes have no effect on compliance, the Chair notifies the Affiliate POC and provides a copy of the updated documentation to the SPKIMA for archival.
    b. If the determination is that the changes affect the compliance of the Affiliate PKI, the Chair informs the Affiliate POC. If the Affiliate POC addresses the SPKIPA concerns, no further action is necessary. Failure to resolve any open issues, at the SPKIPA's discretion, could be grounds for termination of the MOA, and the cross-certificate will be allowed to expire, or the SPKIPA could vote to immediately revoke the current cross-certificate.

3.6 UPDATE OF SPKI DOCUMENTATION

The SPKIPA could deem it necessary to update the STRAC BCA CP or other governance documentation (including this document), thereby placing new requirements on Affiliate PKIs. The extent of the impact on the Affiliate PKIs will be determined prior to implementation of the proposed change, a determination that and could result in postponing proposed changes until Affiliate PKIs can come into compliance, a modification to the proposed change, or a decision not to make the proposed change. Failure to resolve any open issues could result in termination of the MOA, and the cross-certificate will be allowed to expire, or the SPKIPA could vote to immediately revoke the current cross-certificate.

Proposed changes to the STRAC BCA CP will be provided to Affiliates. Affiliates will be required to indicate compliance actions to be taken and proposed timeframes, or objections to the proposed change.

Impact of Affiliate Adoption of Template CP Language and Intent to Use Support Services

The extent to which Affiliate's CP includes language from the Template CP and the extent to which Affiliate intends to use Support Services has no impact upon the process described in this Sec. 3.6: Update of SPKI Documentation. The SPKIPA and the Affiliate shall undertake the SPKI documentation update activities described herein, regardless of the extent to which Affiliate's CP includes language from the Template CP and Affiliate intends to use Support Services.

Activities:

1. The SPKIPA, Affiliates, or Applicants can request changes to the STRAC BCA CP or other governance documentation. Changes must be requested in writing and submitted to the SPKIPA, accompanied with a justification for making the change and the anticipated impact of the change.

2. The SPKIPA reviews the change request(s) and develops a recommendation for each request to accept it, accept it with changes, or reject it.
3. The SPKIPA forwards the change proposal to representatives from all Affiliate PKIs along with a response date. Affiliate responses should be sent to the SPKIPA and all Affiliates.
4. Each Affiliate must provide a response to the CP change proposal to the SPKIPA by the specified response date. The response shall include suggested modifications or an objection to the CP change proposal, where applicable. The Affiliate shall determine:
    a. If the Affiliate PKI documentation currently complies with the proposed change to the STRAC BCA CP,
    b. If the current Affiliate PKI documentation does not specify compliance but Affiliate PKI practices do comply, the estimated level of effort to bring the documentation into compliance and the time frame required,
    c. If the Affiliate PKI does not currently comply but would require changes to come into compliance, the estimated level of effort to bring the documentation and practices into compliance and the time frame required,
    d. If the proposed changes would not be applicable to the Affiliate PKI, and would therefore not require changes of the Affiliate,
    e. If the Affiliate PKI is unwilling or unable to comply with the proposed change, intends to oppose it, and understands that if the change is ultimately accepted, its MOA could become noncompliant, potentially leading to a decision to terminate the cross-certified relationship.

    Each Affiliate is encouraged to send a representative to the SPKIPA meeting scheduled to review the CP Change Proposal and present the Affiliate position in regards to the above bullets. In lieu of a representative, the Affiliate PKI could send a written position to the SPKIPA in advance of the scheduled meeting.
5. Once the Affiliate responses have been received, the SPKIPA reviews the responses and updates the CP Change Proposal as it deems appropriate.
6. The SPKIPA votes to accept, reject, or modify the CP Change Proposal.
7. The SPKIPA informs all Affiliates of the approved CP Change Proposal and the date by which compliance with the change becomes mandatory so that Affiliates can update their documentation and/or practices as needed to remain in compliance with STRAC BCA CP requirements.
8. The SPKIPA updates the STRAC BCA CP documentation with the approved change, including the implementation date, and publishes the updated CP. Notification of the publication is sent to all Affiliates.
9. After a CP Change Proposal's implementation date, the Affiliate's next annual audit report shall include documentation stating whether the Affiliate is compliant. In addition, any applicable mapping documents and CP must be updated, as appropriate.

10. With its next annual audit report, the SPKIPA will review any Affiliate PKI for which there are not updated mapping documents demonstrating compliance with the changes, including any Affiliate PKI that has requested an extension, and makes a determination whether to terminate the Affiliate PKI's MOA and revoke its cross-certificate.

3.7 PROBLEM RESOLUTION

Either party to the cross-certification arrangement can notify the other of problems and request resolution. Problem resolution procedures are specific to the problem encountered and the method of resolution will be agreed upon between the parties.

For technical problems, the Affiliate technical POC will work with the SPKIMA to resolve the issue(s). Any identified technical issues are documented in a monthly Problem Resolution Report.

For situations where the SPKIPA has reason to believe that the STRAC BCA and/or an Affiliate PKI is not operating in compliance with its MOA or CP, the SPKIPA in its discretion can request the Affiliate to perform an aperiodic audit and provide the resulting compliance audit letter specifically addressing the SPKIPA's concerns. All such requests shall be made for cause, and the cause shall be disclosed at the time of request.

Impact of Affiliate Adoption of Template CP Language and Intent to Use Support Services

The extent to which Affiliate's CP includes language from the Template CP and the extent to which Affiliate intends to use Support Services has no impact upon the process described in this Sec. 3.7: Problem Resolution. The SPKIPA and the Affiliate shall undertake the problem resolution activities described herein, regardless of the extent to which Affiliate's CP includes language from the Template CP and Affiliate intends to use Support Services.

3.8 TERMINATION

The relationship between the SPKIPA and an Affiliate can be terminated by either party.

In the event the Affiliate initiates termination, the Affiliate POC notifies the SPKIPA in writing of its intent to terminate the MOA, the reason(s) for seeking termination, and the desired termination date.

The SPKIPA can initiate termination of the MOA with an Affiliate with or without cause. Should the SPKIMA or the SPKIPA become aware that there has been a failure in the integrity of an Affiliate PKI, the SPKIPA shall, in its sole discretion, determine whether to terminate the MOA and revoke the cross-certificate of the Affiliate PKI. The SPKIPA informs the Affiliate POC of the termination and revocation and notifies all Affiliate PKIs. Alternatively, and at its sole discretion, the SPKIPA shall notify the Affiliate of the issue and provide a resolution date after which the MOA will be terminated if the issue is not resolved. The SPKIPA informs the other Affiliate PKIs of the issue and the timeframe provided for resolution.

Impact of Affiliate Adoption of Template CP Language and Intent to Use Support Services

The extent to which Affiliate's CP includes language from the Template CP and the extent to which Affiliate intends to use Support Services has no impact upon the process described in this Sec. 3.8: Termination. The SPKIPA and the Affiliate shall undertake the termination activities described herein, regardless of the extent to which Affiliate's CP includes language from the Template CP and Affiliate intends to use Support Services.

APPENDIX A DOCUMENTATION SUBMISSION CHECKLIST

Policy Documents

- ☐ Certificate Policy (CP) in the IETF RFC 3647, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" [RFC 3647].
- ☐ Identification of which of the Applicant's CPs are to be considered for cross-certification at which assurance levels.
- ☐ Identification of any areas in which Applicant CP requirements differ from those of the STRAC BCA CP.
- ☐ Other documentation needed to show evidence of comparability between the Applicant PKI and the requirements in the STRAC BCA CP.

Compliance Audit Documents

- ☐ Signed third-party Auditor Letter of Compliance summarizing the results of an audit of the PKI operations that attests to the Applicant's claim that its PKI is operated in accordance with its CPS, and that the CPS implements the requirements of the CP.

Technical Documents

- ☐ Applicant PKI Architecture including a designated Principal CA and a list of subordinate CAs or cross-certified CAs within the PKI.
- ☐ List of CAs that have any other trust relationship with the Applicant PKI Principal CA, such as cross-certifications with other PKIs external to the Applicant PKI and the SPKI.
- ☐ X.500/LDAP directory relationships and hierarchical DN relationships, if any, with other existing Affiliate PKIs (PKIs already cross-certified with the SPKI).
- ☐ Information about repositories used by the Applicant PKI to support the configuration of certificates issued by the Applicant.
- ☐ Configuration of certificates issued by the Applicant PKI.
- ☐ Capability of Applicant PKI to produce certificates conforming to the "*STRAC PKI Certificate Profile*" [STRAC PKI-Prof].
- ☐ For PIV-I policy level, Applicant conformance with "X.509 Certificate and Certificate Revocation List Extensions Profile for Personal Identity Verification Interoperable Cards" [PIV-I Profile] is also required.
- ☐ Statement of whether algorithms used by the Principal CA or by any other CA in the Applicant PKI architecture are executed in conformance with the "Digital Signature Standard" [FIPS 186]. If not, specify the standard with which it complies.