FPKIPA

Federal Public Key Infrastructure Policy Authority

Testing Requirements and Guidelines For Commercial PKI Bridges Cross-Certified With the FBCA

Version 1.0

December 18, 2017

Abstract

This document provides Certificate Testing guidelines and PIV-I Card Testing guidelines, for the Commercial PKI Bridge organizations that are cross-certified with the FBCA.

Table of Contents

1 Introduction

1.1 Background

The Federal Public Key Infrastructure (FPKI) Policy Authority (FPKIPA) is responsible for ensuring the appropriate execution of specific policies and practice requirements by all cross certified and subordinated members, in order to provide corresponding levels of trust to its relying parties. This is accomplished through various forms of evaluations (audits, testing, and artifact review/analysis), by which the FPKIPA can ascribe the appropriate level of trust for each of the FPKI members and the FPKI as a whole.

Commercial PKI Bridge organizations that maintain a relationship with the FPKI – i.e., are cross certified with the Federal Bridge Certification Authority (FBCA) – are required to oversee their member organizations in a similar manner, to include interoperability testing. Interoperability testing falls into two categories:

1. Certificate Testing
    - All cross-certified PKI Bridge organizations shall test all certificate types, from all member CAs with a trust path leading to their Bridge CA; and provide the results to the FPKIPA for all Bridge policies that map to FBCA policies.
2. Personal Identity Verification Interoperable (PIV-I) card Testing
    - All cross-certified PKI Bridge organizations with members that issue PIV-I Cards shall ensure every PIV-I Card type is compliant with all applicable federal policies and requirements via PIV-I Card Testing.

1.2 Purpose

This document describes the Certificate and PIV-I Card Testing requirements that cross certified PKI Bridge organizations must implement in their test plans and testing processes.

1.3 Scope

This document is limited to Certificate and PIV-I Card Testing guidance. Other forms of credentials (such as PIV Cards), credential issuing and management systems, applications, and validation systems are not addressed, although it may be necessary to leverage some of these components to support the execution of certificate and PIV-I card testing.

1.4 Audience

This document is intended for Commercial PKI Bridge organizations cross-certified with the FBCA. The sections regarding PIV-I Card Testing pertain to the Commercial PKI Bridge organizations with members that issue PIV-I Cards.

2 Certificate Testing

Certificate Testing verifies that all of the certificates issued under FPKI policies are in compliance with applicable x.509 requirements, Certificate Policy requirements, and certificate profile requirements. PKI Bridge organizations are responsible for annually testing all certificate types from each of their member CAs that assert or map to any of the bridge's policies, which in turn are mapped to a policy defined in the FBCA CP.

2.1 Certificate Testing Scope

All certificates and CRLs issued by members of a PKI Bridge trust community containing one or more certificate policies that map to the Bridge's certificate policies, which in turn map to certificate policies defined in the FBCA CP are in scope. Certificate Testing includes evaluations of:

- All end entity certificate types (including OCSP Responder certificates),
- All CA certificates, and
- All CRLs in the validation paths of the PKI Bridge's trust community

To ensure all appropriate certificates and certificate types are tested, the following shall be collected from each member:

1. A list identifying all CAs with a trust path to the Bridge CA
2. A list identifying all certificate types issued by each of the identified CAs that assert or map to any bridge policy that is mapped to FBCA policies
3. A current CA certificate that corresponds to each CA identified in 1. above.
4. A valid production certificate issued within the past 12 months that corresponds to each of the certificate types identified in 2. above.

2.2 Certificate Requirements

The Certificate Testing shall test each of the certificates and CRLs for compliance with:

- RFC 5280 Internet X.509 PKI Certificate and CRL Profile (aka X.509 or PKIX)
- The applicable CP, which has been mapped (directly or indirectly) to the FBCA CP
- The applicable certificate profile(s), as required by the applicable CP
- For PIV-I certificates, compliance is always tested against the FPKI Certificate and CRL Profile for PIV-I Cards

In order to demonstrate interoperability among the community and maximize certificate acceptance by federal relying parties, each certificate shall be tested for a valid path to the Federal Common Policy Root CA as its trust anchor. CRLs shall be collected dynamically during validation testing (verifying valid CRLDP extensions), and included as artifacts to test and evaluate. CA certificates shall be included in the member organization's submission, but each CA certificate necessary to build the validation paths shall be collected dynamically as part of the testing process, verifying valid AIA extensions and ensuring there are no conflicts with the CA certificates submitted by the organization under testing.

2.3 Certificate Testing Method(s)

Testing methods shall include manual review and evaluations of certificate contents in addition to the use of automated tools. Where available, automated utilities should be used for evaluation purposes. However, this is not a substitute for manual verification of the results. In addition, an automated utility capable of testing against every policy and profile requirement associated with the FPKI may not be available; therefore, some level of manual testing will be required.

The following tools have been validated for certificate testing:

- PKI Interoperability Test Tool (PITT)
- Certificate_validate (a command line utility created by NIST)
- Microsoft CAPI Certificate Viewer
- Microsoft CAPI certutil

In addition, a Bridge may utilize any application that complies with RFC5280/PKIX, and has demonstrated the ability to pass the NIST Public Key Interoperability Test Suite (PKITS) testing.

2.4 Certificate Test Reporting

Test results shall be captured in a report. The report shall be submitted to the FPKIPA as part of the PKI Bridge's Annual Review Package.

The report title, introduction, and identification information must include:

- The PKI Bridge organization responsible for testing
- The member PKI organization being tested
- The date of the report
- The date of the annual evaluation period (i.e., the member organization asserts that all production certificate types that were issued during this period have been included in the testing)
- The version number and date of the associated Certificate Test Plan
- The member PKI's list of CAs with a trust path to the Bridge CA
- The member PKI's list of certificate types (that assert or map to any Bridge policy that is mapped to any of the FPKI policies found in the FBCA CP) issued by each of the identified CAs

The report must provide the following:

- a short description of the testing methods used, including any tools, utilities, or applications used to execute the testing process.
- an explanation of the rating system used. It must cover at least the following three categories, but can be more granular if desired:
    - No issues.
    - Acceptable issues. A finding of non-conformance that has been determined acceptable (at least temporarily) by a policy decision or by exception. These issues do not require correction by the member organization prior to receiving a "passing" report. In general, they are issues that can be corrected when the associated certificate expires or by the next annual testing date. In rare cases, it

    may be determined that it is acceptable not to comply with a particular associated requirement. In these cases, the decision must be documented and an explanation provided. In addition, FPKI interoperability must be maintained and agreement from the FPKIPA is required.
    - Unacceptable issues. A finding of non-conformance that causes a “failed” testing result. These issues must be corrected before the member organization receives a “passing” report.
- a Test Results Summary section, which indicates an overall “Pass” or “Fail” and includes:
    - all of the unacceptable issues and which certificate types are implicated.
    - any acceptable issues that must be corrected prior to the next annual testing.
    - any exceptions that have been accepted by policy and do not require remediation along with an explanation of each.
    - a request for a mitigation strategy from the entity undergoing testing, with a stated deadline based on the severity of the issues.
- a certificate/CRL status section, which lists every certificate and CRL that was tested, along with its result [no issues, acceptable issue, or unacceptable issue] and an explanation of any issues. This section shall be in table format.
- a detailed table for each certificate and CRL, displaying all of its contents (fields, extensions, criticality settings). These tables must include:
    - The FPKI policies that are successfully mapped
    - Informational notes that are worthy of mentioning, but are not necessarily “issues” and do not carry any negative judgement
    - Issues that have been identified

See Appendix A for a sample Certificate Test Report, which may be used as a template.

2.5 Certificate Test Plan

Each Bridge PKI organization shall submit a Certificate Test Plan to the FPKIPA for approval. In addition, a copy of the latest Certificate Test Plan must be submitted with the annual review package. The test plan shall address in detail the implementation of the requirements in section 2 of this document. The test plan shall include:

- The detailed steps of the entire testing process, including roles and responsibilities, from initial communication with the member organization through finalizing the Certificate Test Report
- Testing methods and procedures employed, and a description of how these procedures ensure conformance with each of the requirements cited in section 2.2
- A list of automated tools, utilities, or applications used in the testing process
- Procedures used to determine findings
- Criteria used to evaluate findings, identify issues and determine their severity
- A sample Certificate Test Report

3 PIV-I Card Testing

PKI Bridge organizations must be approved by the FPKIPA to perform PIV-I Card Testing prior to implementing such testing.

All applicant PIV-I Card Issuers must undergo PIV-I Card Testing utilizing an FPKIPA-approved testing system (organization, facility, and test plan), prior to receiving approval to issue. In addition, PIV-I Card Testing is required annually, in order to maintain approval status. Annual PIV-I Card Testing verifies that PIV-I Cards are continuing to be issued in compliance with applicable FPKI PIV-I requirements. All PKI Bridge organizations cross-certified with the FBCA are responsible for carrying out PIV-I Card Testing for any of their member PKIs that issue PIV-I Cards.

3.1 PIV-I Card Testing Scope

PIV-I Card Testing is performed with production PIV-I Cards. The Card holder must be present during testing to interact with the card for authentication purposes.

PIV-I Card Testing is required for every card type issued by the PIV-I Card Issuer. PIV-I Card type is defined as a unique combination of:

- Manufacturer and model of Cardstock
- Card Management System (CMS) configuration used to issue and manage the card
- CA configuration used to issue and manage certificates on the card
- Customer organization (agency, department, or company) to which the PIV-I Card is issued, if the card profile and/or card management practices vary per customer.

3.2 PIV-I Requirements

The *Personal Identity Verification Interoperability For Issuers* guidance defines PIV-I and establishes the requirements associated with the issuance of a PIV-I Card. The PIV-I Card Testing must verify that the requirements set forth in the *Personal Identity Verification Interoperability For Issuers* guidance and referenced documentation are met. Documentation referenced in the *Personal Identity Verification Interoperability For Issuers* guidance include:

- FIPS 201
- NIST SP 800-73
- NIST SP 800-76
- NIST SP 800-78
- The FBCA CP
- FPKI Certificate and CRL Profile for PIV-I Cards (Referenced by the FBCA CP)

Additional information related to the PIV-I requirements associated with these documents can be found in the requirements tables in Appendix A, Appendix B, and Appendix C of the *Federal Identity, Credentialing, and Access Management Personal Identity Verification Interoperable (PIV-I) Test Plan* (Version 1.2.0; October 18, 2016).

3.3 PIV-I Testing Method(s)

PIV-I Card Testing methods shall include a combination of manual review, automated test tool(s), and production applications. There are three categories that must be covered during PIV-I Card testing:

1. PIV-I Card Validation –The PIV-I Card must be examined manually to ensure that it has the appropriate markings (e.g. the cardholder's facial image and name printed on the card) and uses approved card stock and smartcard applets. At a minimum, test procedures shall address the requirements found in Appendix A of the *Federal Identity, Credentialing, and Access Management Personal Identity Verification Interoperable (PIV-I) Test Plan* (Version 1.2.0; October 18, 2016).

2. PIV-I Data Model Validation – The PIV-I Card data model (i.e., the structure and contents of the smart card) is defined in Appendix A of the FBCA CP. At a minimum, test procedures shall address the requirements found in Appendix B of the *Federal Identity, Credentialing, and Access Management Personal Identity Verification Interoperable (PIV-I) Test Plan* (Version 1.2.0; October 18, 2016). Use the automated test tool, PIV-I Data Model Tester, or equivalent to conduct this category of the testing. The PIV-I Data Model Tester is based on the NIST SP 800-85B PIV Data Model Test Tool with specific modifications to determine conformance with the PIV-I standard.

3. PIV-I PACS Interoperability Validation – The PIV-I Card must interface correctly with applications known to be capable of processing PIV and PIV-I. At a minimum, test procedures shall be developed to ensure proper interoperability with real PACS implementations and address the requirements found in Appendix C of the *Federal Identity, Credentialing, and Access Management Personal Identity Verification Interoperable (PIV-I) Test Plan* (Version 1.2.0; October 18, 2016). These test procedures shall evaluate PIV-I Cards in two or more distinct approved PACS solutions consisting of different products from on the GSA Approved Product List.

3.4 PIV-I Test Reporting

Test results shall be captured in a PIV-I Test Report. For new PIV-I issuers, the reports shall be submitted to the FPKIPA for review, prior to approval to issue PIV-I Cards. Annual PIV-I Test Reports shall be submitted to the FPKIPA as part of each PKI Bridge organization's Annual Review Package. There shall be a separate report for each card type tested.

The report title, introduction, and identification information must include:

- The PKI Bridge organization responsible for testing
- The member PKI organization (PIV-I Issuer or potential PIV-I Issuer) being tested
- The date of the report
- The date of the testing
- The version number and date of the associated PIV-I Test Plan
- The distinguished name of the PIV-I issuing CA(s)

- A short description of the card type

The report must provide the following:

- a short description of the PIV-I Card, PIV-I Data Model, and interoperability testing methods used, including any tools, utilities, or applications used to execute the testing process.
- an explanation of the rating system used. It must cover at least the following three categories, but can be more granular if desired:
  - No issues.
  - Acceptable issues. A finding of non-conformance that has been determined acceptable (at least temporarily) by a policy decision or by exception. These issues do not require correction by the member organization prior to receiving a "passing" report. In general, they are issues that can be corrected prior to the next annual testing date. In rare cases, it may be determined that it is acceptable not to comply with a particular associated requirement. In these cases, the decision must be documented and an explanation provided. In addition, FPKI interoperability must be maintained and agreement from the FPKIPA is required.
  - Unacceptable issues. A finding of non-conformance that causes a "failed" testing result. These issues must be corrected before the member organization receives a "passing" report.
- a Test Results Summary section, which indicates an overall "Pass" or "Fail" and includes:
  - all of the unacceptable issues and which components of the PIV-I card are implicated.
  - any acceptable issues that must be corrected by the next annual testing.
  - Any exceptions that have been accepted by policy and do not require remediation along with an explanation of each.
  - A request for a mitigation strategy from the entity undergoing testing, with indicated stated deadline based on the severity of the issues.
- detailed test results in table format, broken down into sections for each of the three categories described in section 3.3 above. The table must include:
  - The specific requirements or groups of requirements being tested
  - the results of each [no issues, acceptable issue, or unacceptable issue]
  - an explanation of any issues found and any informational notes that are worthy of mentioning.

See Appendix B for a sample PIV-I Test Report, which may be used as a template.

3.5 PIV-I Test Plan

Each Bridge PKI organization shall submit a PIV-I Test Plan to the FPKIPA for approval. In addition, the PIV-I Test Plan must be submitted whenever it is updated. The test plan shall address in detail the implementation of the requirements in section 3 of this document. The test plan shall include:

- The detailed steps of the entire testing process, including roles and responsibilities, from initial communication with the member organization through finalizing the PIV-I Test Report
- Testing methods employed, and a description of how they ensure each of the requirements cited in section 3.2 are addressed
- A list of automated tools, utilities, or applications used in the testing process
- Specifications of the testing facility, including identification of the PACS applications available for use in the testing process
- Procedures used to determine findings
- Criteria used to evaluate findings, identify issues and determine their severity
- A sample PIV-I Test Report

3.6 PIV-I Operational Capabilities Demonstration (OCD)

As a component of the approval process for the PIV-I Test Plan, a PKI Bridge organization must undergo an Operational Capabilities Demonstration (OCD) of its PIV-I Testing processes prior to implementation. The FPKIPA will require a refresh of the OCD every three years. The OCD will be conducted via in person evaluation and approval by FPKIPA Representatives.

The OCD shall demonstrate the entire PIV-I Card Testing process, as detailed in the corresponding PIV-I Test Plan. The evaluator will assess the procedures, the personnel, the hardware, and the software used in the execution of the OCD, ensuring compliance with the approved PIV-I Test Plan.

The PIV-I Test Plan must be submitted and approved by the FPKIPA before an OCD will be scheduled.

4 Test Plan Submission

Each Bridge shall submit its certificate test plan and PIV-I test plan, if applicable, to the FPKIPA for review and approval. For organizations submitting both test plans, they shall be provided together as a single submission. All content and supporting artifacts to be considered must be included with the submission, shall be clearly identified, and shall be consistently cross-referenced within the documentation. Submissions that are not well-articulated, or easy-to-process, may be returned to the submitting bridge for further clarification.

Each Bridge will be allowed to submit its test plan(s) for approval no more than twice per fiscal year. Failure to secure FPKIPA approval for the test plan or related operational capabilities demonstration may result in the loss of the cross-certified relationship with the Federal Bridge Certificate Authority.

See Appendix C for a sample FPKI Submission Cover Letter, which may be used as a template.

Appendix A: Certificate Test Report Template

The ABC Trust Bridge

PKI Certificate Compliance Test Report For:

The XYZ PKI Credential Issuing Company

Review Period: *Month DD, YEAR to Month DD, YEAR*

Report Date: *Month DD, YEAR*

TEST PLAN: *ABC Certificate Test Plan, Version X.X, Month DD, YEAR*

Report Introduction

Brief explanation of certificate testing and the purpose of this report. Example below:

This document lists the results of annual certificate testing for The ABC Trust Bridge Participants. Certificate testing is comprised of path validation testing as well as certificate and CRL profile conformance mapping.

Testing Methods Summary

Provide a short description of the testing methods used, including any tools, utilities, or applications used to execute the testing process. Example below:

The ABC Trust Bridge uses an internal certificate parsing and export tool called “ABC cert-2-table” to build a table for each certificate and CRL evaluated. These tables allow certificate testers to more easily evaluate certificate and CRL contents visually, to ensure they comply with requirements specific to the applicable CPs and Certificate and CRL Profiles that the automated tools may not test for. The tables also provide space to record comments and issues throughout the testing process. Microsoft’s “certutil –verify,” NIST’s certificate_validate, and the PKI Interoperability Test Tool (PITT) [http://pkif.sourceforge.net/pitt.html], are used for automated conformance testing with x.509 standards, federal requirements, and Full Path Discovery and Validation (PD-Val) testing up to the federal trust anchor: Federal Common Policy CA.

Report Rating Guidelines

Include an explanation of the rating system used, in testing each certificate and CRL. Example below (rating system may be more granular if desired):

The following guidelines should be used when interpreting report results/comments:

- No issues. Requirements have been met.
- Acceptable issues. A finding of non-conformance that has been found acceptable (at least temporarily) by a policy decision or by exception. These are issues that do not require the member organization to correct before receiving a “passing” report. These are issues that can be corrected when the associated certificate expires or by the next annual testing (and do not require a retest before then), or it has been determined that it is acceptable to not comply with the particular associated requirement. In these cases, FPKI interoperability must be maintained and agreement from the FPKIPA will ultimately be required.
- Unacceptable issues. A finding of non-conformance that causes a “failed” testing process. These issues must be corrected before the member organization will receive a “passing” report.

Certificate Test Results Summary

This section indicates an overall "Pass" or "Fail." When the report indicates that the organization has failed, all of the unacceptable issues (causing the failure) shall be identified in this section. This section shall also include any acceptable issues that must be corrected prior to the next annual testing. A mitigation strategy shall be requested within this section, with an indicated deadline (based on the severity of the issues). Example below:

The XYZ certificate testing was mostly successful, but the resulting overall status is "Failed" due to the four issues called out below:

- The XYZ Root CA Delegated OCSP Responder certificate only asserts the devices policy OID, but it is used to validate other certificate policies.
- An unexpected tag was detected in the ocsp-nocheck extension of the XYZ Root CA OCSP Responder certificate. It should have a value of NULL.
- The applicable Certificate & CRL Extensions Profile requires the AuthorityInfoAccess (AIA) extension for end entity signature certificates, but the AIA extension is not present in the XYZ Sub CA1 code-signing certificate.
- The Certificate Policy requires CRL validity periods of no more than 180 hours. The XYZ Sub CA2 CRL is valid for almost 7 weeks (1110+ hours).

Please respond within 30 days with a timeline for remediation of these issues.

<u>CAs and certificate types in the testing scope, as identified and provided by *XYZ PKI Credential Issuing Company*:</u>

List all the issuing CAs and certificate types within the testing scope. Example below:

- XYZ Root CA
  - Self-Signed Certificate
  - Delegated OCSP Responder Certificate
  - Cross-certificate issued to a Subordinate CA (XYZ Sub CA1)
  - Cross-certificate issued to a Subordinate CA (XYZ Sub CA2)
- XYZ Sub CA1
  - Delegated OCSP Responder Certificate
  - Subscriber Signature Certificate
  - Subscriber Key Management Key Certificate
  - Code Signing Certificate
  - Device Certificate
- XYZ Sub CA2
  - Delegated OCSP Responder Certificate
  - PIV-I Content Signing Certificate
  - PIV-I Authentication Certificate
  - PIV-I Card Authentication Certificate
  - PIV-I Subscriber Signature Certificate
  - PIV-I Subscriber Key Management Key Certificate

<u>Certificate/CRL Status Dashboard:</u>

Provide a table identifying every certificate and CRL that was tested, along with an indication of its status (no issues, acceptable issue, or unacceptable issue) and an explanation of the issues. Example below:

Table 1-1: Summary of Certificate/CRL Status

Certificate Profile		Result/comments
XYZ Root CA> Self-Signed Certificate	🟩	
XYZ Root CA> Delegated OCSP Responder Certificate	🟥	• Certificate Status Servers shall assert all the policy OIDS for which it is authoritative. The XYZ Root CA Delegated OCSP Responder certificate only asserts the XYZ Medium Device policy OID, but it is used to validate many other certificate policies (mapped to federal policies). • An unexpected tag was detected in the ocsp-nocheck extension. It should have a value of NULL.
XYZ Root CA> Cross-certificate to Subordinate CA (XYZ Sub CA1)	🟦	• The ABC Bridge X.509 Certificate and CRL Extensions Profile and RFC 5280 both require that the PolicyConstraints extension be set as Critical. However, to support legacy applications that cannot process PolicyConstraints, it has been set to non-critical. This is permitted by the FPKI X.509 Certificate and CRL Extensions Prolife.
XYZ Root CA> Cross-certificate to Subordinate CA (XYZ Sub CA2)	🟩	
XYZ Root CA> CRL	🟩	
XYZ Sub CA1> Delegated OCSP Responder Certificate	🟩	
XYZ Sub CA1> Subscriber Signature Certificate	🟩	
XYZ Sub CA1> Subscriber Key Management Key Certificate	🟩	
XYZ Sub CA1> Code Signing Certificate	🟥	• The applicable Certificate & CRL Extensions Profile requires the AuthorityInfoAccess (AIA) extension for end entity signature certificates, but the AIA extension is not present.
XYZ Sub CA1> Device Certificate	🟩	
XYZ Sub CA1> CRL	🟩	
XYZ Sub CA2> Delegated OCSP Responder Certificate	🟩	
XYZ Sub CA2> PIV-I Content Signing Certificate	🟦	• Invalid character (a space ‘ ‘ instead of %20) detected in the LDAP address of the AIA extension. LDAP is only used internally to XYZ. The HTTP address is valid.
XYZ Sub CA2> PIV-I Authentication Certificate	🟩	
XYZ Sub CA2> PIV-I Card Authentication Certificate	🟩	
XYZ Sub CA2> PIV-I Subscriber Signature Certificate	🟩	
XYZ Sub CA2> PIV-I Subscriber Key Management Key Certificate	🟩	

Certificate Profile		Result/comments
XYZ Sub CA2> CRL	🟥	- The Certificate Policy requires CRL validity periods of no more than 180 hours. This CRL is valid for almost 7 weeks (1110+ hours).

Full Certificate/CRL Analysis:

Provide a table for every certificate and CRL, displaying all of its contents (fields, extensions, criticality settings). These tables should also have an area to detail:

- *The FPKI policies that are successfully mapped*
- *Informational notes that are worthy of mentioning, but are not necessarily "issues" and do not necessarily carry any negative judgement*
- *Issues that have been identified*

Example below:

Table 2-2: XYZ Root CA> *Delegated OCSP Responder Certificate*

Field	Description	Critical Extension	Certificate Analysis (Actual Contents)
Version	V3 (2)		3
Serial Number	Must be unique		41 d9 cb 01
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}		sha1withRSAEncryption (1.2.840.113549.1.1.5)
Issuer Distinguished Name	Unique Issuing CA DN as specified in Section 3.1.1 of the CP		CN=XYZ OCSP001, OU=Components, OU=Public Key Services, O=XYZ Credential Issuing Company, C=US
Validity Period	Valid usage period as specified in section 6.3.2 of the CP; Expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter		Thu Jun 24 13:50:55 EDT 2003 , Sat Jun 24 14:20:55 EDT 2033
Subject	Unique subject DN as specified in Section 3.1.1 of the CP		CN=XYZ Root CA, OU=Certification Authorities, OU=Public Key Services, O=XYZ Credential Issuing Company, C=US
Subject Public Key Information	2048 bit modulus, rsaEncryption {1 2 840 113549 1 1 1}		RSA(2048 Bits) , Modulus: 30820122300d06092a576891f70d01010105000382010f003082010a0264010100b9365fb3b105da4ae26bc3977f4a5c10d90a29afd96f9a55afa5196eb4f4a5ed7e43839592c94d95d2efbe244d2ea6b3a1b3e648f564b6ogc2be6b7d8e98ccd383a1d5ce93b772ead188cfe1e5f26b00405815e5e8babd28507605c16702862d64d2666432b6f858ef7e5a9a5316522ff5bess4a068ea07e544d4344e4700c30380f5501a722cc7295fb45ee2902ca5458e4defae070cb7657f3c368f44479f59ed130daad29a7abc66c137dfd13e1f7bacea89aca22bde2784e01cf0ddbfa0005e329a370a3a2825da58a1f0f246e59a6e1a63f03a659787eae6c27cc033aa50987a7fc570c83ea271e61bd37e838ab0984189e3e0c1039cd1b95882c5ccee7

			0203010001 , Public Exponent: 65537
Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}		2C08730299F8B19A5BD866EFAF78318DE641D98F50B497047012AD7515AFEDDC49CF69AFFC1160BA6193B013BACA7CF7221CE2481A32101A82F4BBAA5B92FD2AAEDE25F1DD0A7994BCD2A3195374E96695162AB251FC1F9F467F386CF19C18AB6E6E166851AEA4AB2AE92DDBEFC2436F09288E2734AF3691D95995549BA05880EAE4532E0A4372ED293A61C06967FA6F17FBD619E099CE868DD5883A3748858013F27C525A66F82C149EDD3B31873C1F2E055A830D4187FCFB64FA271EBAAE65EE773DB410C53144DB9E6304821192F4B03210576C8CB9429E9A2E5C0474D1FE12A1B2C33F724602379DC0D7116784055B454E834430F053CF5A2539821B4F24
Extension	Description	Critical Extension	Certificate Analysis (Actual Contents)
KeyUsage	c=yes; Approved use for key pair (e.g., digitalSignature or keyEncipherment)	TRUE	digitalSignature
BasicConstraints	Used to idenify CAs vs. End Entities and depth of certification paths		Subject Type=End Entity Path Length Constraint=None
OCSP No Revocation Checking	Required for OCSP Responder certificates		30 0f 06 09 2b 06 01 05 0...+... 05 07 30 01 05 04 02 05 ..0..... 00 .
SubjectKey Identifier	c=no; Octet String		89 56 30 02 ee ac 32 c7 81 bb 9a f8 5e a0 0b b9 0a 22 94 30
PrivateKeyUsage Period	Valid usage period for the corresponding private key		30 22 80 0f 32 30 31 37 0"..2017 30 31 32 37 31 36 31 39 01271619 33 31 5a 81 0f 32 30 31 31Z..201 37 30 32 32 38 30 35 30 70228050 30 30 30 5a 000Z
CRLDistribution Points	c = no; location of CRL		[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://xyz.pki.com/repos/xyzroot.crl
CertificatePolicies	c=optional; Applicable certificate policies		Policy Identifier= 9.99.999.9.999.9.9.1.3.37
AuthorityKey Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)		8d 83 fe 82 50 64 65 77 3e fd df 03 9a ce 29 d1 2f 30 cc ec
Extendedkey usage	c=no; Approved use for key pair (extended definition)		OCSP Signing (1.3.6.1.5.5.7.3.9)

Notes:

- Evaluating against:
  - The ABC Trust Bridge Certificate & CRL Extensions Profile (Worksheet 9: Delegated OCSP Responder Profile)
  - XYZ PKI CP
- BasicConstraints, PrivateKeyUsagePeriod, and CRLDistributionPoints are not listed as required or optional extensions for the OCSP Responder worksheet in the ABC Trust Bridge Certificate & CRL Extensions Profile)
- Maps to the following federal policy: certpcy-mediumDevice

Issues:

- Certificate Status Servers shall assert all the policy OIDS for which it is authoritative. This one only asserts medium device. It has been confirmed that the XYZ Root CA OCSP does support/validate other certificate policies (including other policies that map to federal policies).
- (Detected by certificate_validate) An unexpected tag was detected in the ocsp-nocheck extension. It should have a value of NULL.

Appendix B: PIV-I Card Test Report Template

The ABC Trust Bridge

PIV-I Test Report For:

The XYZ PKI Credential Issuing Company

PIV-I Card Type Description: Standard PIV-I Card for ACME Enterprises
Report Date: *Month DD, YEAR*

TEST PLAN: *ABC PIV-I Test Plan, Version X.X, Month DD, YEAR*

Report Introduction

A short description of PIV-I, PIV-I Card Testing, and the purpose of this report. Example below:

Personal Identity Verification (PIV) Interoperability for Non-Federal Issuers [PIV-I NFI] (version 2.0.1 July 27, 2017), provides information for non-federal organizations interested in issuing identity credentials that are technically interoperable with the Federal PIV Card and issued in a manner that facilitates trust. Subsequently, the Federal Identity, Credential, and Access Management (ICAM) community determined that the establishment of specific Public Key Infrastructure (PKI) certificate policy requirements for Personal Identity Verification Interoperable (PIV-I) would further facilitate this trust. These PIV-I policy requirements were added to the *X.509 Certificate Policy for the Federal Bridge Certification Authority* [FBCA CP] in May 2010. As a result, commercial PKI providers within the Federal Bridge Certification Authority (FBCA) trust fabric may provide PIV-I credentials to their subscribers. PIV-I Card issuance requires PIV-I Card interoperability testing in order to demonstrate that the PIV-I Card conforms to the policy requirements and can technically interoperate with elements of the Federal smart card infrastructure.

This report lists the results of the PIV-I testing performed in accordance with the test plan identified above, for a specific organization and specific PIV-I credential configuration.

Testing Methods Summary

Provide a short description of the testing methods used, including any tools, utilities, or applications used to execute the testing process. Example below:

The testing entails manual/visual evaluations, the automated test tool [PIV-I Data Model Tester] based on the NIST SP 800-85B PIV Data Model Test Tool, and live interface testing with real Physical Access Control System (PACS) test lab implementations.

Report Rating Guidelines

Include an explanation of the rating system used, in testing each PIV-I Card requirement/component. Example below (rating system may be more granular if desired):

The following guidelines should be used when interpreting report results/comments:

- No issues. Requirements have been met.
- Acceptable issues. A finding of non-conformance that has been found acceptable (at least temporarily) by a policy decision or by exception. These are issues that do not require the member organization to correct before receiving a “passing” report. These are issues that can be corrected when the associated certificate expires or by the next annual testing (and do not require a retest before then), or it has been determined that it is acceptable to not comply with the particular associated requirement. In these cases, FPKI interoperability must be maintained and agreement from the FPKIPA will ultimately be required.
- Unacceptable issues. A finding of non-conformance that causes a “failed” testing process. These issues must be

corrected before the member organization will receive a “passing” report.

PIV-I Card Test Results Summary

This section indicates an overall “Pass” or “Fail.” When the report indicates that the organization has failed, all of the unacceptable issues (causing the failure) shall be identified in this section. This section shall also include any acceptable issues that must be corrected prior to the next annual testing. A mitigation strategy shall be requested within this section, with an indicated deadline (based on the severity of the issues). Example below:

The ABC Trust Bridge has completed PIV-I Card Testing for the Standard PIV-I Card for ACME Enterprises, issued by The XYZ Credential Issuing Company. The testing has “failed” due to the following issues discovered:

- Expiration Date printed on the card is 6 years and 3 months from time of testing; PIV-I cards shall be issued with a maximum 6 year validity period.
- The UUID is not included in the Subject Alternative Name (SAN) extension of the PIV-I Authentication certificate, as it is required to be.
- The only policy OID in the certificate policy extension of the PIV-I Content Signing certificate is an “XYZ Credential Issuing Company” policy for device certificates and it is not mapped to the FBCA PIV-I Content Signing Policy OID.

Please respond within 30 days with a mitigation timeline for correcting these issues.

Test Details:

Test Details	Description
PIV-I Card Type Description	Standard PIV-I Card for ACME Enterprises
Subscribing Organization of the PIV-I Cards	ACME Enterprises
Issuing Organization (Certificates)	The XYZ PKI Credential Issuing Company
Issuing Certification Authority (CA) Distinguished Name	CN=XYZ Sub CA2, OU=Certification Authorities, OU=Public Key Services, O=XYZ Credential Issuing Company, C=US
Card Management System (CMS) and registration details	CMS is operated and maintained by the XYZ Credential Issuing Company. Registration and card printing is onsite with ACME Registration Authorities (RAs) using ACME RA Workstations.
Testing Date	Month DD, YEAR
Tester	PIV-I Card and Data Model Validation: Joseph D. Tester PACS Interoperability Testing: Robert D. Tester
Issues / Comments	Unacceptable Issues: • Expiration Date printed on the card is 6 years and 3 months from time of testing. Certificate issuance dates imply that the card was issued with a 6 year and 6 month validity period. • The UUID is not included in the Subject Alternative Name (SAN) extension of the PIV-I Authentication certificate, as it is required to be. • The only policy OID in the certificate policy extension of the PIV-I Content Signing certificate is an “XYZ Credential Issuing Company” policy for device certificates and it is not mapped to the FBCA PIV-I Content Signing Policy OID. Acceptable Issues: • The PIV-I Card Authentication certificate has a validity period 3 years + 1 day, instead of 3 years (or less). CA configuration should be modified to issue with a maximum of 3 years for the validity period. • Fingerprint template on card meets minimum size requirements, and fingerprint was validated successfully during registration with PACS Test

	Solution #1. However, fingerprint mismatch occurred during time of access. Too few minutiae were extracted to make a successful match. Although there's an interoperability issue with this PACS solution, we believe the issue lies with the PACS solution. Testing with PACS Test Solution #2 was successful. Comments: - Deprecated Card applet version used, but GSA approved extension until 6/30/18
Recommendation (Pass / Fail)	Fail

PIV-I Card Validation Results:

Configuration Specifications	
PIV-I Card Holder:	Carrie D. Badge
Smartcard Data Model:	Oberthur Technologies ID-One Cosmo v7.0
Smartcard Applet Version:	Oberthur PIV Applet Suite 2.3.2

Test ID	Test Description	Pass, Fail, or N/A	Comments
PIV-I-A.1	Card Visually Distinct from PIV	Pass	
PIV-I-A.2	Card Printed Information	Pass	
PIV-I-A.3	Card Printed Expiration Date within six (6) years	Fail	**Unacceptable Issue:** Expiration Date is 6 years and 3 months from time of testing.
PIV-I-A.4	Card Data Model listed on GSA APL	Pass	Listed #587 on GSA APL
PIV-I-A.5	Approved Card Applet Version	Pass	**Note:** Oberthur Applet Suite 2.3.2 is a deprecated applet version according to NIST's Validation List for PIV Card Applications. However, GSA has approved extended use until 6/30/18.
PIV-I-A.6	Mandatory Data Element: Asymmetric Card Authentication Key	Pass	
PIV-I-A.6	Optional Data Element: Key History Object	N/A	
PIV-I-A.6	Optional Data Element: Retired Key Management Keys	N/A	
PIV-I-A.7	Cardholder Facial Image printed on card	Pass	
PIV-I-A.8	Manual Review of Card Elements	Pass	

PIV-I Data Model Validation Results:

Configuration Specifications	
PIV-I Data Model Tester version:	PIV-I Data Model Tester 1.1 (based on NIST SP 800-85B PIV Data Model Test Tool version 6.2.0)

Test ID	Test Description	Pass, Fail, or N/A	Comments
PIV-I-B.01 to PIV-I-B.55	Data Model Tests using PIV-I Data Model Tester	Fail	**Unacceptable Issue**: The UUID is not included in the Subject Alternative Name (SAN) extension of the PIV-I Authentication certificate, as it is required to be.

Digital Signature	Optional Data Element: Digital Signature Key without PIV-I Hardware OID	N/A	
PIV-I Digital Signature	Optional Data Element: Digital Signature Key with PIV-I Hardware OID	Pass	
Key Management	Optional Data Element: Key Management Key without PIV-I Hardare OID	N/A	
PIV-I Key Management	Optional Data Element: Key Management Key with PIV-I Hardware OID	Pass	
PIV-I Card Authentication Key	Mandatory Data Element: Asymmetric Card Authentication Key. Supports card authentication for an interoperable environment	Fail	**Acceptable Issue**: Card Auth certificate has a validity period 3 years + 1 day. CA configuration should be modified to issue with a maximum of 3 years for the validity period.
PIV-I Authentication Key	Mandatory Data Element: PIV-I Authentication Key	Fail	**Unacceptable Issue**: The UUID is not included in the Subject Alternative Name (SAN) extension of the PIV-I Authentication certificate, as it is required to be.
Content Signer Key	Mandatory Data Element: Content Signer Key	Fail	**Unacceptable Issue**: The only policy OID in the certificate policy extension is an "XYZ Credential Issuing Company" policy for device certificates and it is not mapped to the FBCA PIV-I Content Signing Policy OID.
Printed Information	Optional Data Element: Printed Information	Pass	
Retired Key Management Keys	Optional Data Element: Retired Key Management Keys	N/A	

PIV-I PACS Application Interoperability Validation Results:

PACS Test Solution #1 (*Complete all the PACS Solution specifications and test information below***)**

Manufacturer	Product	Version	Purpose	Issues/Comments
			PACS Head-end Software	
			PACS Panel	
			PACS Panel	
			Validation System	
			Validation System	
			Validation System	
			Validation System	
			Trusted Controller	
			Reader	"Driver Error" occurred when trying to do a successful fingerprint match.

Test ID	Test	Pass, Fail, or N/A	Comments
PS1T1	Enrollment, PDVal with AIA	Pass	
PS1T2	CHUID Mode	Pass	
PS1T3	CAK Mode (Asymmetric only)	Pass	
PS1T4	PKI + PIN Mode	Pass	
PS1T5	PKI + PIN + Fingerprint Mode	Fail	Fingerprint template on card meets minimum size requirements, and fingerprint was validated successfully during registration. However, fingerprint mismatch occurred during time of access. Too few minutiae were extracted to make a successful match. Although there's an interoperability issue with this PACS solution, we believe the issue lies with the PACS solution. Testing with PACS solution #2 was successful.
PS1T6	PKI + PIN Mode, Access Denied	Pass	
PS1T7	PKI + PIN + Fingerprint Mode, Access Denied	Fail	Fingerprint template on card meets minimum size requirements, and fingerprint was validated successfully during registration. However, fingerprint mismatch occurred during time of access. Too few minutiae were extracted to make a successful match. Although there's an interoperability issue with this PACS solution, we believe the issue lies with the PACS solution. Testing with PACS solution #2 was successful.

PACS Test Solution #2 (*Complete all the PACS Solution specifications and test information below*)

Manufacturer	Product	Version	Purpose	Issues/Comments
			PACS Head-end Software	
			PACS Panel	
			PACS Panel	
			Validation System	
			Validation System	
			Validation System	
			Validation System	
			Trusted Controller	
			Reader	

Test ID	Test	Pass, Fail, or N/A	Comments

PS1T1	Enrollment, PDVal with AIA	Pass	
PS1T2	CHUID Mode	Pass	
PS1T3	CAK Mode (Asymmetric only)	Pass	
PS1T4	PKI + PIN Mode	Pass	
PS1T5	PKI + PIN + Fingerprint Mode	Pass	
PS1T6	PKI + PIN Mode, Access Denied	Pass	
PS1T7	PKI + PIN + Fingerprint Mode, Access	Pass	

Appendix C: FPKI Submission Cover Letter Template

The ABC Trust Bridge

Testing Materials Submission for the FPKI:

Test Results for Member PKIs *- Delete this line if it's not applicable -*
The ABC Trust Bridge Test Plan(s) *- Delete the above line if it's not applicable -*
Date: *Month DD, YEAR*

Test Results for Member PKIs in the ABC Bridge Community

(In support of The FPKI Annual Review Package for ABC Trust Bridge)

Delete this entire section if it's not applicable to this submission (e.g., if this is an initial test plan submission, seeking initial approval)

Enclosed you will find:

- ➢ Certificate Compliance Test Reports for the following member PKI organizations
    1) XYZ Credential Issuing Company
    2) *List each member PKI organization (with a Certificate Test Report enclosed)*
- ➢ PIV-I Card Test Reports for the following PIV-I Card Types

  (Delete this bullet, and sub-bullets, if no PIV-I cards are issued/tested in this bridge community)
    1) XYZ Credential Issuing Company
        - A. Standard PIV-I Card for ACME Enterprises
        - B. PIV-I Card for ACME Enterprises United Kingdom Office
        - C. Standard PIV-I Card for Federal IT Consulting Peeps, Inc.
        - D. *List each Card Type issued by this member PKI organization (with a PIV-I Test Report enclosed)*
    2) *List each member PKI organization (with a corresponding PIV-I Card Test Report enclosed)*

Provide any other pertinent comments here. If there are any reports missing, indicate here and explain why.

The ABC Trust Bridge Test Plan(s)

(For FPKIPA review and approval)

Delete this entire section if it's not applicable to this submission (e.g., if this is a submission of test results for the annual review package, and the associated test plan hasn't been updated since the last approval)

Enclosed you will find:

Select only one applicable bullet below, and delete the other three

- ➢ The following (single) Test Plan, covering Certificate Compliance Testing and PIV-I Card Testing
    1) The ABC Trust Bridge Test Plan for Certificate Testing and PIV-I Testing, Version X.X, Month DD, Year
- ➢ The following (separate) Certificate Compliance Test Plan and PIV-I Card Test Plan
    1) The ABC Certificate Testing, Test Plan, Version X.X, Month DD, YEAR
    2) The ABC PIV-I Card Testing, Test Plan, Version X.X, Month DD, YEAR
- ➢ The following Certificate Compliance Test Plan
    1) The ABC Certificate Testing, Test Plan, Version X.X, Month DD, YEAR
- ➢ The following PIV-I Card Test Plan
    1) The ABC PIV-I Card Testing, Test Plan, Version X.X, Month DD, YEAR

Indicate whether the test plan(s) identified above has been updated since the last version was approved, or if you're

seeking initial approval. If seeking initial approval of a PIV-I Test Plan, include a reminder that you need to schedule an OCD and provide any supporting details regarding scheduling.
Provide any other pertinent comments here as well.