



Federal PKI
Management Authority
Enabling Trust

Path Discovery and Validation (PD-VAL)

Product Conformance Testing Process

VERSION 1.0.0

March 28, 2013

TABLE OF CONTENTS

1	INTRODUCTION.....	1
1.1	BACKGROUND.....	1
1.2	PURPOSE.....	2
1.3	AUDIENCE.....	2
1.4	SCOPE.....	2
2	THE FPKI PD-VAL PRODUCT CONFORMANCE TEST SUITES.....	3
2.1	PATH VALIDATION TESTING PROGRAM.....	3
2.2	PATH DISCOVERY TESTING PROGRAM.....	3
3	CATEGORIZATION AND APPROVAL CRITERIA.....	5
3.1	THE FOUR CONFORMANCE TESTING CATEGORIES.....	5
3.2	REQUIRED TEST CASES.....	6
3.3	OPTIONAL TEST CASES.....	6
3.4	APPROVAL SPECIFICATIONS.....	8
4	ROLES AND RESPONSIBILITIES.....	9
4.1	FPKI POLICY AUTHORITY (FPKIPA).....	9
4.2	FPKI MANAGEMENT AUTHORITY (FPKIMA).....	9
4.3	FPKI TECHNICAL WORKING GROUP (TWG).....	9
4.4	PD-VAL PRODUCT VENDOR.....	9
5	THE TESTING PROCESS.....	11
5.1	PRE-APPLICATION ACTIVITIES.....	12
5.2	FPKI PD-VAL PRODUCT CONFORMANCE TESTING APPLICATION.....	12
5.3	APPLICATION REVIEW.....	12
5.4	TEST PLANS AND EXECUTION.....	12
5.5	PRELIMINARY RESULTS.....	13
5.6	FPKI PD-VAL PRODUCT CONFORMANCE TECHNICAL TEST REPORT.....	13
5.7	FPKI TWG REVIEW AND RECOMMENDATION.....	14
5.8	APPROVAL AUTHORIZATION.....	15
	APPENDIX A: PRODUCT CONFORMANCE TESTING APPLICATION.....	16
	APPENDIX B: PATH VALIDATION TESTING PROGRAM – TEST CASE DETAILS.....	23
	APPENDIX C: PATH DISCOVERY TESTING PROGRAM – TEST CASE DETAILS.....	35

1 INTRODUCTION

1.1 BACKGROUND

The Federal Public Key Infrastructure (FPKI) is the foundation for secure e-government certificate-based transactions at unclassified levels of assurance 1 through 4¹. There are many communities of interest participating in the FPKI, which offers a variety of capabilities (a) across federal agencies, and (b) between federal agencies and outside bodies such as universities, state and local governments, commercial entities, shared service providers, and community-of-interest bridges. The FPKI unifies disparate PKI domains by creating trust paths among the participating PKI domains. Certificates issued from FPKI domains and the associated trust paths are validated by Relying Parties (RPs) internal and external to the FPKI.

Due to the complexity of the FPKI certificate trust paths and the interconnected relationships within the FPKI Community, proper validation of FPKI certificates is critical, albeit challenging. Certificate validation consists of two phases: path discovery and path validation, more simply known as Path Discovery and Validation (PD-VAL). Path discovery is the process of discovering a chain of certificates running between the RP's trust anchor and the certificate being validated, as well as the associated Certificate Revocation Lists (CRLs) and/or Online Certificate Status Protocol (OCSP) responses. Path validation is the process of examining each certificate and CRL and/or OCSP response in the path, and determining validation status of the path at a given moment and within the parameters being enforced by the PD-VAL product.

A path may be discovered dynamically as needed, or it may be made up of stored (or "cached") data. Vendors may vary in how they choose to implement PD-VAL in their products, but the PD-VAL process discussed in this document expects that the entire trust path is validated in real-time with each transaction (even if the trust path is cached).

To help ensure the quality of certificate path validations in the complex FPKI environment, the FPKI Management Authority (FPKIMA) has been given the responsibility to execute FPKI PD-VAL Product Conformance Testing. This conformance testing is applicable for any software product that performs path discovery and/or path validation on X.509 certificates. The tests can be used to ensure a product conforms to the PD-VAL requirements appropriate for the FPKI environment. This conformance testing is a prerequisite for FPKI PD-VAL Product List (PPL) approval. The FPKI PPL gives FPKI members assurance that listed PD-VAL products support the needs of the FPKI Community.

¹ Levels of assurance defined by [Office of Management and Budget \(OMB\) M-04-04](#).

1.2 PURPOSE

This document provides the necessary details and guidance to all parties involved in FPKI PD-VAL Product Conformance testing.

1.3 AUDIENCE

This is a public document intended for the entire FPKI community, RPs, PD-VAL product vendors, and anyone else who may be interested.

1.4 SCOPE

The scope of this document is limited to the FPKI PD-VAL Product Conformance Testing Process. This includes, but is not limited to the identification and description of the test suites, testing categorization and approval criteria, roles and responsibilities, and the steps involved in the testing process.

This document does not discuss FPKI PPL maintenance responsibilities.

2 THE FPKI PD-VAL PRODUCT CONFORMANCE TEST SUITES

The FPKI PD-VAL Product Conformance Testing Process uses the National Institute of Standards and Technology (NIST) [Public Key Infrastructure \(PKI\) test suites](#), consisting of the path validation testing program and the path discovery testing program.

These two test suites enable developers and validation laboratories to test a PKI product's conformance to the path processing rules as specified in [X.509](#) and [RFC 3280](#)². The test suites entail sets of certificates, CRLs, and supporting documentation. The certificates and CRLs contain a variety of content and relationships, forming certification paths that are valid in some cases and not valid in other cases. Each test case is an attempt to validate a particular certificate, including its full certification path, using the product being tested. The input to each test case is a single end-entity certificate. The supporting documentation explains the intent and expected results of each test case.

2.1 PATH VALIDATION TESTING PROGRAM

The Public Key Interoperability Test Suite (PKITS) is a comprehensive path validation test suite that covers most of the features specified in [X.509](#) and [RFC 3280](#)². This test suite emulates a complex PKI environment, including various end-entity certificates, intermediate Certification Authority (CA) certificates, a trust anchor certificate, and all associated CRLs.

[Public Key Interoperability Test Suite \(PKITS\) for Certification Path Validation; Version 1.0.1; April 14, 2011](#) contains descriptions of the test cases in the test suite.

[NIST Recommendation for X.509 Path Validation](#) specifies the set of functionality that NIST believes is necessary for path validation.

2.2 PATH DISCOVERY TESTING PROGRAM

The path discovery test suite consists of three sample PKI architectures: one with Lightweight Directory Access Protocol (LDAP) URIs in the certificates indicating where certificates and CRLs may be found, one with Hypertext Transfer Protocol (HTTP) URIs in the certificates indicating where certificates and CRLs may be found, and one that does not include any information in the certificates regarding where certificates and CRLs may be found (but the certificates and CRLs may be obtained from [smime2.nist.gov](#) using LDAP as specified in [RFC 4523](#)).

The PKI architectures are designed to test a product's ability to perform path discovery:

- When end-entity certificates are issued by CAs that are hierarchically subordinate to the trust anchor CA; and

² The [FPKI X.509 Certificate and CRL Extensions Profile](#) and the [X.509 Certificate and CRL Extensions Profile for the Shared Service Providers \(SSP\) Program](#) have not been updated for [RFC 5280](#) compliance.

- When end-entity certificates are issued by CAs that are connected to the trust anchor CA by a mesh PKI architecture, leveraging bridge CAs.

[Path Discovery Test Suite; Version 0.1.1; June 3, 2005](#) contains descriptions of the test cases in the test suite.

3 CATEGORIZATION AND APPROVAL CRITERIA

3.1 THE FOUR CONFORMANCE TESTING CATEGORIES

The FPKI PD-VAL Product Conformance Testing Process allows for the path validation test suite to be executed using one or both of two methods:

1. Using online test repositories for dynamic data retrieval; and/or
2. Using static test data stored within the product

The FPKI PD-VAL Product Conformance Testing Process allows for the path discovery test suite to be executed using one or both of two methods:

1. Using path discovery functionality only (no validation); and/or
2. With revocation validation functionality

This results in four possible test execution combinations, which have four corresponding conformance categories as detailed in Table 1. A product can be approved for one, two, three, or all four conformance categories.³

TABLE 1. TEST EXECUTION COMBINATIONS AND CONFORMANCE CATEGORIES

Test Suite / Test Method Combination	Conformance Categories
Test Suite: Path Validation Testing Program Test Method: Using online test repositories for dynamic data retrieval.	Dynamic Path Validation: Products that perform validation of a certificate and its associated certification path using online repositories to dynamically retrieve the CA certificates and CRLs to build the certification path to the trust anchor.
Test Suite: Path Validation Testing Program Test Method: Using static test data stored within the product.	Static Path Validation: Products that perform validation of a certificate and its associated certification path when the CA certificates and CRLs in the certification path are already imported and stored with the product.
Test Suite: Path Discovery Testing Program Test Method: Using path discovery functionality only (no validation).	Path Discovery with No Validation: Products that perform dynamic discovery of certificates and CRLs that make up hierarchical and mesh certification paths using HTTP URIs, LDAP URIs, and/or no URIs (using LDAP as specified in RFC 2587).

³ The FPKI PD-VAL Product Conformance Testing Process requires that the path validation test suite is always executed with full path validation functionality, and that the path discovery test suite is always executed using online test repositories for dynamic data retrieval.

Test Suite / Test Method Combination	Conformance Categories
<p>Test Suite: Path Discovery Testing Program Test Method: With revocation validation functionality.</p>	<p>Path Discovery with Revocation Validation: Products that perform dynamic discovery and validation of certificates and CRLs that make up hierarchical and mesh certification paths using HTTP URIs, LDAP URIs, and/or no URIs (using LDAP as specified in RFC 2587).</p>

Within each test suite there are a number of required test cases and optional test cases. Although not every test case is required, every test case is executed within each conformance category applied for.

3.2 REQUIRED TEST CASES

Each test suite has a number of required test cases. These test cases support what is considered to be the Baseline FPKI PD-VAL Service. Products are required to pass all of these test cases without exception in order to achieve approval for the corresponding conformance category. Appendix B: **Path Validation Testing Program – Test Case Details** and Appendix C: **Path Discovery Testing Program – Test Case Details** detail each test case in the Path Validation Test Suite and the Path Discovery Test Suite respectively, including identification of the test cases that support the Baseline FPKI PD-VAL Service (i.e., the required test cases).

3.3 OPTIONAL TEST CASES

Each test suite also includes a number of optional test cases. These test cases support various optional FPKI PD-VAL services. Products are not required to pass these optional test cases in order to achieve approval for the corresponding conformance category, but all test cases are executed for each conformance category selected. This is to ensure that the product gracefully handles requests associated with non-supported services, category wide. That is, the optional test cases still require an appropriate response, ensuring the product’s relying parties do not trust untrustworthy certificates. The FPKIMA will use technical analysis and expertise, with support from the FPKI Technical Working Group (TWG) if necessary, to determine if the product responses associated with non-supported services are graceful. In many cases, the product should simply provide an invalid path response when it cannot definitively support a particular validation service (just as a product should do if it cannot locate a CRL to determine revocation status).

Products are required to pass all test cases corresponding to a specific optional PD-VAL service in order to achieve approval for that optional PD-VAL service.

3.3.1 PATH VALIDATION TESTING PROGRAM

The path validation test suite includes 40 optional test cases categorized into 12 optional FPKI PD-VAL services, as summarized in Table 2.

TABLE 2. NUMBER OF PATH VALIDATION TEST CASES PER OPTIONAL FPKI PD-VAL SERVICE

Number of Test Cases	Optional FPKI PD-VAL Service
9	Products that support delta-CRLs
3	Products that can process a nameRelativeToCRLIssuer in the cRLDistributionPoint and issuingDistributionPoint
12	Products that process indirect CRLs
1	Both: <ul style="list-style-type: none"> - Products that process indirect CRLs - Products that can process a nameRelativeToCRLIssuer in the cRLDistributionPoint and issuingDistributionPoint
6	Products that process the onlySomeReasons field of the issuingDistributionPoint extension
2	Products that can set initial-policy-set to "any-policy" when initial-explicit-policy is set
1	Products that support DSA signatures
1	Products that support DSA signatures and parameter inheritance
1	Products that support the mixed use of UTF8String encoding & PrintableString encoding in the certificates
1	Products that support case insensitive matching between the issuer field of an end entity certificate and the corresponding subject field of the CA certificate, using UTF8String encoding
1	Products that support: dnQualifier, serialNumber, & ST in the certificate Subject Name
1	Products that support: T (Title), generationQualifier, pseudonym, SN, initials, givenName, and L (Locality) in the certificate Subject Name
1	Products that gracefully handle User Notice Qualifier text with more than 200 characters

In addition to the 40 optional test cases listed in Table 2, there are 7 required tests that have an optional portion to the expected results. The expected validation response (valid or invalid) is required for these tests in support of the Baseline FPKI PD-VAL Service. However, there are expected user notification messages in response to these tests, which are optional. These notification messages are only necessary for products that process User Notice Qualifiers.

Appendix B: details the corresponding FPKI PD-VAL service for each specific path validation test case.

3.3.2 PATH DISCOVERY TESTING PROGRAM

The path discovery test suite includes only 1 optional test case assigned to 1 corresponding optional FPKI PD-VAL service:

TABLE 3. NUMBER OF PATH DISCOVERY TEST CASES PER OPTIONAL FPKI PD-VAL SERVICE

Number of Test Cases	Optional FPKI PD-VAL Service
1	Products that support mesh environments with a mix of URI types in the certificates, including no AIA or SIA in the certificates and CRLs issued by the CAs closest to the trust anchor

Appendix C: details the corresponding FPKI PD-VAL service for each specific path discovery test case.

3.4 APPROVAL SPECIFICATIONS

FPKI PPL approvals are specific to:

- The conformance categories;
- The optional FPKI PD-VAL services, if any, per category; and
- Any conditional details upon which the associated test results depend.

4 ROLES AND RESPONSIBILITIES

4.1 FPKI POLICY AUTHORITY (FPKIPA)

The FPKIPA presides over the FPKI PD-VAL Product Conformance Testing Process as the Process Owner. The FPKIPA owns and manages the FPKI PPL, and is the Approval Authority for each product on the PPL.

The FPKIPA is notified of all applications for product conformance testing that the FPKI TWG accepts or rejects, and all tested products that the FPKI TWG recommends for inclusion on or exclusion from the FPKI PPL. The FPKIPA gives final approval for listing a product on the PPL by the FPKIPA Chair signing the associated FPKI PD-VAL Validation Report. The FPKIPA may publish the technical test report and the FPKI PD-VAL Validation Report for each product on the FPKI PPL.

4.2 FPKI MANAGEMENT AUTHORITY (FPKIMA)

The FPKIMA maintains and administers the FPKI Conformance Testing Process as the Process Manager. The FPKIMA supports conformance testing inquiries, accepts product conformance testing application submissions, executes the testing, and acts as the liaison between the PD-VAL product vendor, the FPKI TWG, and the FPKIPA.

The FPKIMA is responsible for drafting:

- The preliminary test results;
- The FPKI PD-VAL Product Conformance Technical Test Report; and
- The FPKI PD-VAL Validation Report

4.3 FPKI TECHNICAL WORKING GROUP (TWG)

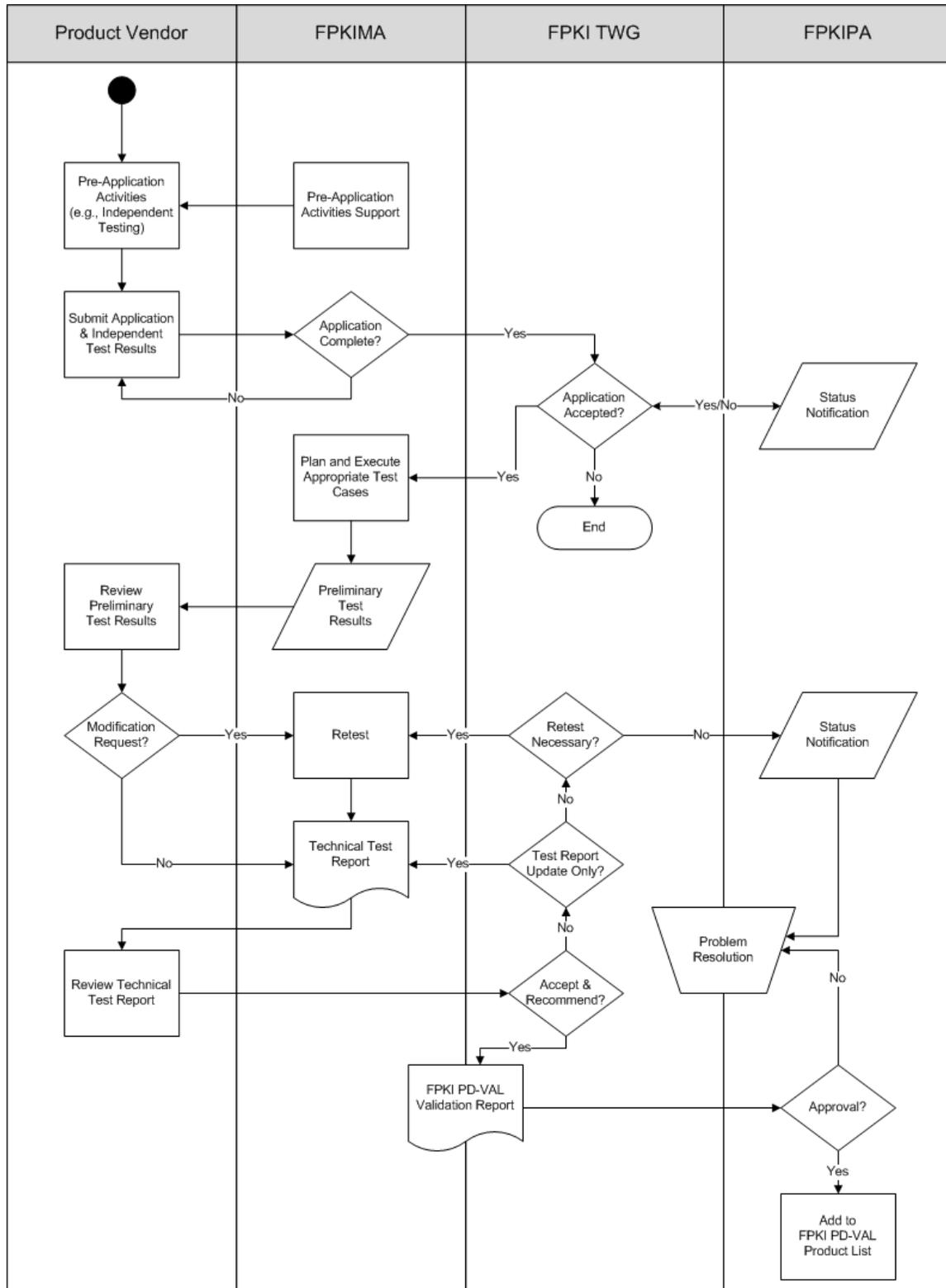
The FPKI TWG reviews each product conformance testing application provided through the FPKIMA. The FPKI TWG reviews the technical test report presented by the FPKIMA and determines whether or not to recommend listing of the product on the FPKI PPL. For a recommended product, the FPKI TWG reviews and finalizes the FPKI PD-VAL Validation Report before the report is presented to the FPKIPA for approval. For a rejected product, the FPKI TWG works with the FPKIPA to determine appropriate problem resolution steps.

4.4 PD-VAL PRODUCT VENDOR

The PD-VAL product vendor independently executes conformance testing prior to submitting an application to the FPKIMA. The vendor completes and submits a conformance testing application, which includes the independent test results. The vendor provides all required software, licenses, installation and operational procedures, and technical support to the FPKIMA during the execution of the testing process.

The PD-VAL product vendor reviews the FPKIMA's preliminary test results and determines if any tests should be re-executed with a modification (e.g., procedural, configuration, software patch). The vendor may provide one software patch in response to the preliminary test results.

5 THE TESTING PROCESS



5.1 PRE-APPLICATION ACTIVITIES

There are prerequisite activities that occur after a potential FPKI PD-VAL Product Conformance Testing candidate has been identified, but before an application is submitted. The FPKIMA provides the product vendor with the support needed during the pre-application activities. In addition, the FPKIMA provides the product vendor with all necessary resources including a kickoff information sharing meeting (conference call), documentation, and internet links.

Prior to submitting an application, the product vendor executes the test cases internally and independently. Internal testing helps product vendors determine which conformance categories and optional services to seek approval for, and allows the product vendor to identify and resolve issues prior to starting the official testing process. The product vendor confirms all necessary software to provide the FPKIMA for executing the tests, and the FPKIMA uses the product vendor's independent test results to assist in evaluating the official test results.

5.2 FPKI PD-VAL PRODUCT CONFORMANCE TESTING APPLICATION

The FPKIMA provides the product vendor with the product conformance testing application (or a link to the application) and any support needed to complete the application. The product vendor initiates the FPKI PD-VAL Product Conformance Testing process when they submit their application and independent test results. The independent test results should demonstrate that the product is capable of achieving the PD-VAL product conformance criteria selected in the application.

Appendix A: is a sample FPKI PD-VAL Product Conformance Testing Application form. The currently-published form may not be identical to this sample.

5.3 APPLICATION REVIEW

The FPKIMA reviews the application upon submission. If necessary, the FPKIMA sends the application back to the product vendor and assists the vendor with submitting a complete application.

The FPKIMA presents completed applications to the FPKI TWG for review and acceptance. Whether the application is accepted or rejected by the FPKI TWG, the status is reported to the product vendor and the FPKIPA. If the FPKI TWG rejects the application, the FPKIMA informs the product vendor of the reason(s). The product vendor may submit another application.

5.4 TEST PLANS AND EXECUTION

If the FPKI TWG accepts the application, the FPKIMA prepares a test plan based on the information provided in the application. The FPKIMA executes the test cases and records the results. The FPKIMA compares its test results to the product vendor's independent test results.

This assists with identifying potential anomalies and identifying potential configuration or procedural errors.

5.5 PRELIMINARY RESULTS

The FPKIMA records preliminary results and provides them to the product vendor for review. For each preliminary test result recorded, the product vendor determines if they would like to:

1. Agree and accept the result as detailed by the FPKIMA;
2. Request the execution of the test(s) again with a configuration or procedural modification in place; or
3. Request the execution of the tests again with a software modification in place (i.e., patch).

All requests for a modification and retest must be made by the product vendor within 10 business days of receiving the preliminary results. If the product vendor wishes to provide a software patch, the patch must be provided within 40 business days of receiving the preliminary results. If a software patch is provided by the product vendor, the FPKIMA executes all test cases after the patch is applied (not just the test cases that the patch is intended to address) to ensure that the patch doesn't have any unintended effects. The FPKIMA does not accept more than one patch per application for product approval. If the patch does not provide the product vendor's desired results, the product vendor has three options:

1. Continue the process with the current results as they are;
2. Continue the process with the pre-patched product version and the associated results;
or
3. Cancel the current testing process; the product vendor may submit another application for product approval in the future.

5.6 FPKI PD-VAL PRODUCT CONFORMANCE TECHNICAL TEST REPORT

If the product vendor agrees to and accepts all preliminary results, or the second round of testing has completed, the FPKIMA formalizes the test results in a Technical Test Report. The Technical Test Report captures and summarizes the versions and specifications of the test suite(s), the product, the testing conditions, and the results. The technical test report includes factual details and technical analysis. The report does not include any recommendations or approvals.

The Technical Test Report is provided to the product vendor for review. The product vendor has 5 business days to provide comments before the FPKIMA presents the report to the FPKI TWG. The FPKIMA is not obligated to modify the technical test report, or delay or alter the process any further due to the product vendor's comments.

The Technical Test Report should include the following information:

- Scope and Specifications
 - Test Suite(s) used, including dates and version numbers
 - Identification of the product, including the complete name, description, version, build and patch numbers
 - Identification of supporting software (e.g., client validation utilities, test tools), including name, description, build, and patch numbers.
 - Hardware and operating system specifications of all servers and client systems used to execute the tests
 - Any unique scoping details about the product's functionality
- Path Validation Testing Program Report (*if applicable*)
 - Any unique details about the product or methods used to test the product with respect to Path Validation test cases
 - The results for all test cases, including details of any failed tests or anomalies
 - Results for the Conformance Category: Dynamic Path Validation (*if applicable*)
 - Results for the Conformance Category: Static Path Validation (*if applicable*)
- Path Discovery Testing Program Report (*if applicable*)
 - Any unique details about the product or methods used to test the product with respect to Path Discovery test cases
 - The results for all test cases, including details of any failed tests or anomalies
 - Results for the Conformance Category: Path Discovery with No Validation (*if applicable*)
 - Results for the Conformance Category: Path Discovery with Revocation Validation (*if applicable*)

5.7 FPKI TWG REVIEW AND RECOMMENDATION

The FPKIMA presents the Technical Test Report to the FPKI TWG for review⁴. Based on the Technical Test Report, the FPKI TWG determines whether or not to recommend the product for the FPKI PPL. If the product vendor provided comments on the Technical Test Report, the FPKI TWG takes those comments into consideration.

The FPKI TWG makes its FPKI PPL recommendation based on the approval criteria detailed in Section 3.

⁴ If requested by the product vendor, FPKI TWG review and recommendation session(s) include federal government participants only.

If the FPKI TWG does not recommend the product for listing on the FPKI PPL, one of the following approaches is taken:

- The Technical Test Report is updated per FPKI TWG guidance and reviewed again;
- The test case(s) are executed again per FPKI TWG guidance, and the Technical Test Report is updated accordingly (if applicable) and reviewed again; or
- The FPKIPA is notified that the FPKI TWG does not recommend listing of the product on the FPKI PPL, and the FPKI TWG works with the FPKIPA to determine the appropriate problem resolution steps. If the problem(s) cannot be solved during the current testing cycle, the product vendor may submit another application for product approval in the future.

If the FPKI TWG recommends the product for listing on the FPKI PPL, the FPKIMA drafts the FPKI PD-VAL Validation Report in coordination with the FPKI TWG.

5.7.1 FPKI PD-VAL VALIDATION REPORT

The FPKI PD-VAL Validation Report details the product's FPKI PPL approval as recommended by the FPKI TWG. The report is drafted by the FPKIMA as an FPKI TWG tasking, but it is an FPKIPA document ready for approval and signature by the FPKIPA Chair. The report includes the following information:

- Identification of the approved product, including the complete name, description, version, build and patch numbers;
- Identification of the associated Technical Test Report upon which the approval is based;
- Any conditional details upon which the associated test results depend (and therefore a required condition for FPKI PPL approval);
- The FPKI PD-VAL conformance categories; and
- The optional FPKI PD-VAL services, if any, per each category

5.8 APPROVAL AUTHORIZATION

The FPKI PD-VAL Validation Report and associated Technical Test Report are provided to the FPKIPA for review and approval. The FPKI PPL approval criteria are detailed in Section 3.

If approved, the FPKIPA Chair signs the FPKI PD-VAL Validation Report and the product is added to the FPKI PPL. If not approved, the FPKIPA works with the FPKI TWG to determine the appropriate problem resolution steps.

The FPKI PD-VAL Validation Report identifies the applicable product version, the testing process version, and the test suite version(s). To obtain FPKI PPL approval for subsequent versions, product vendors should apply for retesting upon major upgrades to their products, the testing process, or the test suite(s). Product vendors will be notified of all upgrades to the PD-VAL Product Conformance Testing Process or the associated test suite(s).

APPENDIX A: PRODUCT CONFORMANCE TESTING APPLICATION

1. Product Vendor/Organization Name:
2. Product Vendor/Organization Contact Information (Website URL, Mailing Address, Telephone):
3. Point(s) of Contact (Name, Email Address, Telephone, Mailing Address):
4. Product Identification (Full Name: Suite Name/Edition Name/Release Name, Version #, Build #):
5. In the table below, check the “Baseline PD-VAL Service” box for each of the four conformance testing categories being applied for (the independent test results should demonstrate compliance with all of the required tests corresponding to each of the selected categories). In addition, check all of the optional FPKI PD-VAL Services being applied for, for each of the requested conformance categories (the independent test results should demonstrate compliance with all of the optional tests corresponding to each of the selected FPKI PD-VAL Services). Review Section 3 of the FPKI PD-VAL Product Conformance Testing Process for more details.

FPKI PD-VAL Supported Services	Conformance Testing Category			
	Dynamic Path Validation	Static Path Validation	Path Discovery	Path Discovery and Validation
Baseline FPKI PD-VAL Service				
Optional FPKI PD-VAL Services				
Products that support delta-CRLs			N/A	N/A
Products that can process a nameRelativeToCRLIssuer in the cRLDistributionPoint and issuingDistributionPoint			N/A	N/A
Products that process indirect CRLs			N/A	N/A
Products that process the onlySomeReasons field of the issuingDistributionPoint extension			N/A	N/A
Products that can set initial-policy-set to "any-policy" when initial-explicit-policy is set			N/A	N/A
Products that support DSA signatures			N/A	N/A
Products that support DSA signatures and parameter inheritance			N/A	N/A
Products that support the mixed use of UTF8String encoding & PrintableString encoding in the certificates			N/A	N/A
Products that support case insensitive matching between the issuer field of an end entity certificate and the corresponding subject field of the CA certificate, using UTF8String encoding			N/A	N/A
Products that support: dnQualifier, serialNumber, & ST in the certificate Subject Name			N/A	N/A
Products that support: T (Title), generationQualifier, pseudonym, SN, initials, givenName, and L (Locality) in the certificate Subject Name			N/A	N/A
Products that gracefully handle User Notice Qualifier text with more than 200 characters			N/A	N/A
Products that support mesh environments with a mix of URI types in the certificates, including no AIA or SIA in the certificates and CRLs issued by the CAs closest to the trust anchor	N/A	N/A		

6. Product details (Check the appropriate selections and answer sub-questions accordingly):

A. Select the type of product being tested and answer any associated questions (if testing a combination of supplementing products, select all that apply):

(1) A Server that performs centralized PD-VAL for other applications

i. Is this a hosted service provider?

Yes

No

ii. Identify the client software that was used to execute the independent testing and being provided to the FPKIMA for testing:

iii. Identify the available client products that are known to successfully interoperate with this server (include separate attachment, if necessary):

iv. What protocol (e.g., SCVP), and draft version, is used to communicate with clients?

v. Does the server perform (check one):

Path Discovery only

Path Discovery AND Path Validation

(2) A product that performs its own PD-VAL

i. Is the product (check one):

An independent application?

A plug-in that performs or supplements PD-VAL capabilities for applications?

a. Identify the software that was used to execute the independent testing and being provided to the FPKIMA for testing:

b. Identify the available software applications that are known to successfully interoperate with this plug-in (include separate attachment, if necessary):

- A Tool Kit used to enable custom applications to perform PD-VAL?
 - a. Identify the software (e.g., test tool) that was used to execute the independent testing and being provided to the FPKIMA for testing:

- (3) A Product that relies on a server to perform or supplement PD-VAL capabilities
 - i. Identify the server that was used to execute the independent testing and being provided to the FPKIMA for testing:

 - ii. Identify the available PD-VAL server products that are known to successfully interoperate with this product (include separate attachment, if necessary):

 - iii. What protocol (e.g., SCVP), and draft version, is used to communicate with server products?

 - iv. Does the product (check one):
 - Perform Path Validation while relying on a server product to perform Path Discovery?
 - Rely on a server product for both Path Discovery and Path Validation (If so, and the server product is not included in this conformance testing application, stop here – questions B through G are not relevant)

- B. The OCSP responder architectures that the product can support and integrate with include (check all that apply):
 - Integrated OCSP Responder – The CA signs and provides the revocation status information
 - Designated OCSP Responder – A separate OCSP Responder, authorized by the CA, signs and provides the revocation status information
 - Locally Trusted OCSP Responder – The product can locally configure the OCSP Responders that it trusts
 - None – The product does not support OCSP

Comments:

C. The Path Processing module can obtain the CRL needed to validate a certificate when (check all that apply):

- The certificate does not include a cRLDistributionPoints extension, but the relevant CRL is in the authorityRevocationList or certificateRevocationList attribute of the certificate issuer's directory entry (where the CRL is obtained by using LDAP to query a directory whose DNS name or IP address is known from local configuration information)
- The certificate includes a cRLDistributionPoints extension with a distribution point name that is of the directoryName name form, and the relevant CRL is in the authorityRevocationList or certificateRevocationList attribute of the directory entry specified by the directoryName (where the CRL is obtained by using LDAP to query a directory whose DNS name or IP address is known from local configuration information)
- The certificate includes a cRLDistributionPoints extension with a distribution point name that is an HTTP URI that points to a file containing the CRL
- The certificate includes a cRLDistributionPoints extension with a distribution point name that is an LDAP URI where the LDAP URI specifies the LDAP server's name (IP address or DNS name), the directory entry in which the CRL is located, and the attribute (authorityRevocationList or certificateRevocationList) that holds the CRL
- The certificate is as described in any of the four options above, but the CRL is retrieved from a local cache file

Comments:

D. When building certification paths from the end entity certificate towards the trust anchor, the path processing module can find the preceding certificate in the certification path by (check all that apply):

- Obtaining the CA certificates located in a certs-only CMS message that is pointed to by an HTTP URI in an authorityInfoAccess extension (if the implementation examines the file extension, it must accept and process both .p7c and .p7b files)
- Obtaining the CA certificates located in Distinguished Encoding Rules (DER) encoded or Base64 encoded certificate files that are pointed to by an HTTP URI in an authorityInfoAccess (AIA) extension

- Obtaining CA certificates located in an LDAP accessible directory that is pointed to by an LDAP URI in an authorityInfoAccess extension that specifies the LDAP server's name (IP address or DNS name), the directory entry in which the certificates are located, and the attributes (cACertificate and/or crossCertificatePair) within which the certificates may be found
- Obtaining certificates from the cACertificate and crossCertificatePair attributes of the certificate issuer's directory entry by querying a locally configured directory (when a certificate does not include an authorityInfoAccess extension)
- Obtaining certificates from implementation-specific sources (e.g., an application certificate trust store) or from protocol messages (e.g., TLS certificate chains) – if yes, identify each potential source in the comments area below

Comments:

E. The path processing module constructs certification paths by (check one):

- Always starting with the end certificate and building towards the trust anchor (If so, stop here – question G is not relevant)
- Building from both the end certificate and the trust anchor depending on the PKI architecture that is encountered

(NOTE: Always building from the trust anchor towards the end entity is not an option since the information required to build in this direction may not be available. See [RFC 4523](#) for more information.)

Comments:

F. If the path processing module sometimes builds certification paths from the trust anchor towards the end entity, the path processing module can find the following certificate in the certification path by (check all that apply):

- Obtaining CA certificates located in a certs-only CMS message that is pointed to by an HTTP URI in a subjectInfoAccess extension (if the implementation examines the file extension, it must accept and process both .p7c and .p7b files)
- Obtaining the CA certificates located in Distinguished Encoding Rules (DER) encoded or Base64 encoded certificate files that are pointed to by an HTTP URI in a subjectInfoAccess extension (SIA) extension
- Obtaining CA certificates located in an LDAP accessible directory that is pointed to by an LDAP URI in a subjectInfoAccess extension that specifies the LDAP server's

name (IP address or DNS name), the directory entry in which the certificates are located, and the attributes (cACertificate and/or crossCertificatePair) within which the certificates may be found

- Obtaining certificates from the cACertificate and crossCertificatePair attributes of the certificate subject's directory entry by querying a locally configured directory (when a certificate does not include a subjectInfoAccess extension)
- Obtaining certificates from implementation-specific sources (e.g., an application certificate trust store) or from protocol messages (e.g., TLS certificate chains) – if yes, identify each potential source in the comments area below

Comments:

APPENDIX B: PATH VALIDATION TESTING PROGRAM – TEST CASE DETAILS

Path Validation Testing Program			
Test #	Test Case Description	Corresponding FPKI PD-VAL Service	Expected Validation Test Result
4.1	Signature Verification		
4.1.1	Valid Signatures	Baseline FPKI PD-VAL Service	Valid
4.1.2	Invalid CA Signature	Baseline FPKI PD-VAL Service	Invalid
4.1.3	Invalid EE Signature	Baseline FPKI PD-VAL Service	Invalid
4.1.4	Valid DSA Signatures	Baseline FPKI PD-VAL Service	If DSA Signatures supported, path should validate; If not, path must be rejected
4.1.5	Valid DSA Parameter Inheritance	Optional FPKI PD-VAL Service: Products that support DSA signatures and parameter inheritance	Valid
4.1.6	Invalid DSA Signature	Optional FPKI PD-VAL Service: Products that support DSA signatures	Invalid
4.2	Validity Periods		
4.2.1	Invalid CA notBefore Date	Baseline FPKI PD-VAL Service	Invalid
4.2.2	Invalid EE notBefore Date	Baseline FPKI PD-VAL Service	Invalid
4.2.3	Valid pre2000 UTC notBefore Date	Baseline FPKI PD-VAL Service	Valid
4.2.4	Valid GeneralizedTime notBefore Date	Baseline FPKI PD-VAL Service	Valid
4.2.5	Invalid CA notAfter Date	Baseline FPKI PD-VAL Service	Invalid
4.2.6	Invalid EE notAfter Date	Baseline FPKI PD-VAL Service	Invalid
4.2.7	Invalid pre2000 UTC EE notAfter Date	Baseline FPKI PD-VAL Service	Invalid
4.2.8	Valid GeneralizedTime notAfter Date	Baseline FPKI PD-VAL Service	Valid
4.3	Verifying Name Chaining		
4.3.1	Invalid Name Chaining EE	Baseline FPKI PD-VAL Service	Invalid
4.3.2	Invalid Name Chaining Order	Baseline FPKI PD-VAL Service	Invalid
4.3.3	Valid Name Chaining Whitespace	Baseline FPKI PD-VAL Service	Valid
4.3.4	Valid Name Chaining Whitespace	Baseline FPKI PD-VAL Service	Valid
4.3.5	Valid Name Chaining Capitalization	Baseline FPKI PD-VAL Service	Valid
4.3.6	Valid Name Chaining UIDs	Baseline FPKI PD-VAL Service	Valid

Path Validation Testing Program			
Test #	Test Case Description	Corresponding FPKI PD-VAL Service	Expected Validation Test Result
4.3.7	Valid RFC3280 Mandatory Attribute Types	Optional FPKI PD-VAL Service: Products that support: dnQualifier, serialNumber, & ST in the certificate Subject Name	Valid
4.3.8	Valid RFC3280 Optional Attribute Types	Optional FPKI PD-VAL Service: Products that support: T (Title), generationQualifier, pseudonym, SN, initials, givenName, and L (Locality) in the certificate Subject Name	Valid
4.3.9	Valid UTF8String Encoded Names	Baseline FPKI PD-VAL Service	Valid
4.3.10	Valid Rollover from PrintStrg to UTF8Strg	Optional FPKI PD-VAL Service: Products that support the mixed use of UTF8String encoding & PrintableString encoding in the certificates	Valid
4.3.11	Valid UTF8String Case Insensitive Match	Optional FPKI PD-VAL Service: Products that support case insensitive matching between the issuer field of an end entity certificate and the corresponding subject field of the CA certificate, using UTF8String encoding	Valid
4.4	Basic Certificate Revocation Tests		
4.4.1	Missing CRL	Baseline FPKI PD-VAL Service	Invalid
4.4.2	Invalid Revoked CA	Baseline FPKI PD-VAL Service	Invalid
4.4.3	Invalid Revoked EE	Baseline FPKI PD-VAL Service	Invalid
4.4.4	Invalid Bad CRL Signature	Baseline FPKI PD-VAL Service	Invalid
4.4.5	Invalid Bad CRL Issuer Name	Baseline FPKI PD-VAL Service	Invalid
4.4.6	Invalid Wrong CRL	Baseline FPKI PD-VAL Service	Invalid
4.4.7	Valid Two CRLs	Baseline FPKI PD-VAL Service	Valid
4.4.8	Invalid Unknown CRL Entry Extension	Baseline FPKI PD-VAL Service	Invalid
4.4.9	Invalid Unknown CRL Extension	Baseline FPKI PD-VAL Service	Invalid
4.4.10	Invalid Unknown CRL Extension	Baseline FPKI PD-VAL Service	Invalid
4.4.11	Invalid Old CRL nextUpdate	Baseline FPKI PD-VAL Service	Invalid
4.4.12	Invalid pre2000 CRL nextUpdate	Baseline FPKI PD-VAL Service	Invalid
4.4.13	Valid GeneralizedTime CRL nextUpdate	Baseline FPKI PD-VAL Service	Valid
4.4.14	Valid Negative Serial Number	Baseline FPKI PD-VAL Service	Valid

Path Validation Testing Program			
Test #	Test Case Description	Corresponding FPKI PD-VAL Service	Expected Validation Test Result
4.4.15	Invalid Negative Serial Number	Baseline FPKI PD-VAL Service	Invalid
4.4.16	Valid Long Serial Numbeerr	Baseline FPKI PD-VAL Service	Valid
4.4.17	Valid Long Serial Number	Baseline FPKI PD-VAL Service	Valid
4.4.18	Invalid Long Serial Number	Baseline FPKI PD-VAL Service	Invalid
4.4.19	Valid Separate Cert and CRL Keys	Baseline FPKI PD-VAL Service	Valid
4.4.20	Invalid Separate Cert and CRL Keys	Baseline FPKI PD-VAL Service	Invalid
4.4.21	Invalid Separate Cert and CRL Keys	Baseline FPKI PD-VAL Service	Invalid
4.5	Verifying Paths with Self-Issued Certificates		
4.5.1	Valid Basic Self-Issued Old With New	Baseline FPKI PD-VAL Service	Valid
4.5.2	Invalid Basic Self-Issued Old With New	Baseline FPKI PD-VAL Service	Invalid
4.5.3	Valid Basic Self-Issued New With Old	Baseline FPKI PD-VAL Service	Valid
4.5.4	Valid Basic Self-Issued New With Old	Baseline FPKI PD-VAL Service	Valid
4.5.5	Invalid Basic Self-Issued New With Old	Baseline FPKI PD-VAL Service	Invalid
4.5.6	Valid Basic Self-Issued CRL Signing Key	Baseline FPKI PD-VAL Service	Valid
4.5.7	Invalid Basic Self-Issued CRL Signing Key	Baseline FPKI PD-VAL Service	Invalid
4.5.8	Invalid Basic Self-Issued CRL Signing Key	Baseline FPKI PD-VAL Service	Invalid
4.6	Verifying Basic Constraints		
4.6.1	Invalid Missing basicConstraints	Baseline FPKI PD-VAL Service	Invalid
4.6.2	Invalid cA False	Baseline FPKI PD-VAL Service	Invalid
4.6.3	Invalid cA False	Baseline FPKI PD-VAL Service	Invalid
4.6.4	Valid basicConstraints Not Critical	Baseline FPKI PD-VAL Service	Valid
4.6.5	Invalid pathLenConstraint	Baseline FPKI PD-VAL Service	Invalid
4.6.6	Invalid pathLenConstraint	Baseline FPKI PD-VAL Service	Invalid
4.6.7	Valid pathLenConstraint	Baseline FPKI PD-VAL Service	Valid
4.6.8	Valid pathLenConstraint	Baseline FPKI PD-VAL Service	Valid
4.6.9	Invalid pathLenConstraint	Baseline FPKI PD-VAL Service	Invalid
4.6.10	Invalid pathLenConstraint	Baseline FPKI PD-VAL Service	Invalid
4.6.11	Invalid pathLenConstraint	Baseline FPKI PD-VAL Service	Invalid
4.6.12	Invalid pathLenConstraint	Baseline FPKI PD-VAL Service	Invalid
4.6.13	Valid pathLenConstraint	Baseline FPKI PD-VAL Service	Valid

Path Validation Testing Program			
Test #	Test Case Description	Corresponding FPKI PD-VAL Service	Expected Validation Test Result
4.6.14	Valid pathLenConstraint	Baseline FPKI PD-VAL Service	Valid
4.6.15	Valid Self-Issued pathLenConstraint	Baseline FPKI PD-VAL Service	Valid
4.6.16	Invalid Self-Issued pathLenConstraint	Baseline FPKI PD-VAL Service	Invalid
4.6.17	Valid Self-Issued pathLenConstraint	Baseline FPKI PD-VAL Service	Valid
4.7	Key Usage		
4.7.1	Invalid keyUsage Critical keyCertSign False	Baseline FPKI PD-VAL Service	Invalid
4.7.2	Invalid keyUsage Not Critical keyCertSign False	Baseline FPKI PD-VAL Service	Invalid
4.7.3	Valid keyUsage Not Critical	Baseline FPKI PD-VAL Service	Valid
4.7.4	Invalid keyUsage Critical cRLSign False	Baseline FPKI PD-VAL Service	Invalid
4.7.5	Invalid keyUsage Not Critical cRLSign False	Baseline FPKI PD-VAL Service	Invalid
4.8	Certificate Policies		
4.8.1	All Certs Same Policy - 1	Optional FPKI PD-VAL Service: Products that can set initial-policy-set to "any-policy" when initial-explicit-policy is set	Valid
4.8.1	All Certs Same Policy - 2	Baseline FPKI PD-VAL Service	Valid
4.8.1	All Certs Same Policy - 3	Baseline FPKI PD-VAL Service	Invalid
4.8.1	All Certs Same Policy - 4	Baseline FPKI PD-VAL Service	Valid
4.8.2	All Certs No Policies - 1	Baseline FPKI PD-VAL Service	Valid
4.8.2	All Certs No Policies - 2	Baseline FPKI PD-VAL Service	Invalid
4.8.3	Different Policies - 1	Baseline FPKI PD-VAL Service	Valid
4.8.3	Different Policies - 2	Optional FPKI PD-VAL Service: Products that can set initial-policy-set to "any-policy" when initial-explicit-policy is set	Invalid
4.8.3	Different Policies - 3	Baseline FPKI PD-VAL Service	Invalid
4.8.4	Different Policies	Baseline FPKI PD-VAL Service	Invalid
4.8.5	Different Policies	Baseline FPKI PD-VAL Service	Invalid
4.8.6	Overlapping Policies - 1	Baseline FPKI PD-VAL Service	Valid
4.8.6	Overlapping Policies - 2	Baseline FPKI PD-VAL Service	Valid
4.8.6	Overlapping Policies - 3	Baseline FPKI PD-VAL Service	Invalid
4.8.7	Different Policies	Baseline FPKI PD-VAL Service	Invalid
4.8.8	Different Policies	Baseline FPKI PD-VAL Service	Invalid

Path Validation Testing Program			
Test #	Test Case Description	Corresponding FPKI PD-VAL Service	Expected Validation Test Result
4.8.9	Different Policies	Baseline FPKI PD-VAL Service	Invalid
4.8.10	All Certs Same Policies - 1	Baseline FPKI PD-VAL Service	Valid
4.8.10	All Certs Same Policies - 2	Baseline FPKI PD-VAL Service	Valid
4.8.10	All Certs Same Policies - 3	Baseline FPKI PD-VAL Service	Valid
4.8.11	All Certs AnyPolicy - 1	Baseline FPKI PD-VAL Service	Valid
4.8.11	All Certs AnyPolicy - 2	Baseline FPKI PD-VAL Service	Valid
4.8.12	Different Policies	Baseline FPKI PD-VAL Service	Invalid
4.8.13	All Certs Same Policies - 1	Baseline FPKI PD-VAL Service	Valid
4.8.13	All Certs Same Policies - 2	Baseline FPKI PD-VAL Service	Valid
4.8.13	All Certs Same Policies - 3	Baseline FPKI PD-VAL Service	Valid
4.8.14	AnyPolicy - 1	Baseline FPKI PD-VAL Service	Valid
4.8.14	AnyPolicy - 2	Baseline FPKI PD-VAL Service	Invalid
4.8.15	User Notice Qualifier	Baseline FPKI PD-VAL Service	Valid (The User Notice display is only required for products that process User Notice Qualifiers)
4.8.16	User Notice Qualifier	Baseline FPKI PD-VAL Service	Valid (The User Notice display is only required for products that process User Notice Qualifiers)
4.8.17	User Notice Qualifier	Baseline FPKI PD-VAL Service	Valid (The User Notice display is only required for products that process User Notice Qualifiers)
4.8.18	User Notice Qualifier - 1	Baseline FPKI PD-VAL Service	Valid (The User Notice display is only required for products that process User Notice Qualifiers)

Path Validation Testing Program			
Test #	Test Case Description	Corresponding FPKI PD-VAL Service	Expected Validation Test Result
4.8.18	User Notice Qualifier - 2	Baseline FPKI PD-VAL Service	Valid (The User Notice display is only required for products that process User Notice Qualifiers)
4.8.19	User Notice Qualifier	Optional FPKI PD-VAL Service: Products that gracefully handle User Notice Qualifier text with more than 200 characters	Conditional (The User Notice display is optional)
4.8.20	CPS Pointer Qualifier	Baseline FPKI PD-VAL Service	Valid
4.9	Require Explicit Policy		
4.9.1	Valid RequireExplicitPolicy	Baseline FPKI PD-VAL Service	Valid
4.9.2	Valid RequireExplicitPolicy	Baseline FPKI PD-VAL Service	Valid
4.9.3	Invalid RequireExplicitPolicy	Baseline FPKI PD-VAL Service	Invalid
4.9.4	Valid RequireExplicitPolicy	Baseline FPKI PD-VAL Service	Valid
4.9.5	Invalid RequireExplicitPolicy	Baseline FPKI PD-VAL Service	Invalid
4.9.6	Valid Self-Issued requireExplicitPolicy	Baseline FPKI PD-VAL Service	Valid
4.9.7	Invalid Self-Issued requireExplicitPolicy	Baseline FPKI PD-VAL Service	Invalid
4.9.8	Invalid Self-Issued requireExplicitPolicy	Baseline FPKI PD-VAL Service	Invalid
4.10	Policy Mappings		
4.10.1	Valid Policy Mapping - 1	Baseline FPKI PD-VAL Service	If policy Mappings supported, path should validate; If not, path must be rejected
4.10.1	Valid Policy Mapping - 2	Baseline FPKI PD-VAL Service	Invalid
4.10.1	Valid Policy Mapping - 3	Baseline FPKI PD-VAL Service	Invalid
4.10.2	Invalid Policy Mapping - 1	Baseline FPKI PD-VAL Service	Invalid
4.10.2	Invalid Policy Mapping - 2	Baseline FPKI PD-VAL Service	Invalid
4.10.3	Valid Policy Mapping - 1	Baseline FPKI PD-VAL Service	Invalid
4.10.3	Valid Policy Mapping - 2	Baseline FPKI PD-VAL Service	Valid
4.10.4	Invalid Policy Mapping	Baseline FPKI PD-VAL Service	Invalid
4.10.5	Valid Policy Mapping - 1	Baseline FPKI PD-VAL Service	Valid
4.10.5	Valid Policy Mapping - 2	Baseline FPKI PD-VAL Service	Invalid

Path Validation Testing Program			
Test #	Test Case Description	Corresponding FPKI PD-VAL Service	Expected Validation Test Result
4.10.6	Valid Policy Mapping - 1	Baseline FPKI PD-VAL Service	Valid
4.10.6	Valid Policy Mapping - 2	Baseline FPKI PD-VAL Service	Invalid
4.10.7	Invalid Mapping From anyPolicy	Baseline FPKI PD-VAL Service	Invalid
4.10.8	Invalid Mapping To anyPolicy	Baseline FPKI PD-VAL Service	Invalid
4.10.9	Valid Policy Mapping	Baseline FPKI PD-VAL Service	Valid
4.10.10	Invalid Policy Mapping	Baseline FPKI PD-VAL Service	Invalid
4.10.11	Valid Policy Mapping	Baseline FPKI PD-VAL Service	Valid
4.10.12	Valid Policy Mapping - 1	Baseline FPKI PD-VAL Service	Valid
4.10.12	Valid Policy Mapping - 2	Baseline FPKI PD-VAL Service	Valid
4.10.13	Valid Policy Mapping	Baseline FPKI PD-VAL Service	Valid (The User Notice display is only required for products that process User Notice Qualifiers)
4.10.14	Valid Policy Mapping	Baseline FPKI PD-VAL Service	Valid (The User Notice display is only required for products that process User Notice Qualifiers)
4.11	Inhibit Policy Mapping		
4.11.1	Invalid inhibitPolicyMapping	Baseline FPKI PD-VAL Service	Invalid
4.11.2	Valid inhibitPolicyMapping	Baseline FPKI PD-VAL Service	Valid
4.11.3	Invalid inhibitPolicyMapping	Baseline FPKI PD-VAL Service	Invalid
4.11.4	Valid inhibitPolicyMapping	Baseline FPKI PD-VAL Service	Valid
4.11.5	Invalid inhibitPolicyMapping	Baseline FPKI PD-VAL Service	Invalid
4.11.6	Invalid inhibitPolicyMapping	Baseline FPKI PD-VAL Service	Invalid
4.11.7	Valid Self-Issued inhibitPolicyMapping	Baseline FPKI PD-VAL Service	Valid
4.11.8	Invalid Self-Issued inhibitPolicyMapping	Baseline FPKI PD-VAL Service	Invalid
4.11.9	Invalid Self-Issued inhibitPolicyMapping	Baseline FPKI PD-VAL Service	Invalid
4.11.10	Invalid Self-Issued inhibitPolicyMapping	Baseline FPKI PD-VAL Service	Invalid

Path Validation Testing Program			
Test #	Test Case Description	Corresponding FPKI PD-VAL Service	Expected Validation Test Result
4.11.11	Invalid Self-Issued inhibitPolicyMapping	Baseline FPKI PD-VAL Service	Invalid
4.12	Inhibit Any Policy		
4.12.1	Invalid inhibitAnyPolicy	Baseline FPKI PD-VAL Service	Invalid
4.12.2	Valid inhibitAnyPolicy	Baseline FPKI PD-VAL Service	Valid
4.12.3	inhibitAnyPolicy - 1	Baseline FPKI PD-VAL Service	Valid
4.12.3	inhibitAnyPolicy - 2	Baseline FPKI PD-VAL Service	Invalid
4.12.4	Invalid inhibitAnyPolicy	Baseline FPKI PD-VAL Service	Invalid
4.12.5	Invalid inhibitAnyPolicy	Baseline FPKI PD-VAL Service	Invalid
4.12.6	Invalid inhibitAnyPolicy	Baseline FPKI PD-VAL Service	Invalid
4.12.7	Valid Self-Issued inhibitAnyPolicy	Baseline FPKI PD-VAL Service	Valid
4.12.8	Invalid Self-Issued inhibitAnyPolicy	Baseline FPKI PD-VAL Service	Invalid
4.12.9	Valid Self-Issued inhibitAnyPolicy	Baseline FPKI PD-VAL Service	Valid
4.12.10	Invalid Self-Issued inhibitAnyPolicy	Baseline FPKI PD-VAL Service	Invalid
4.13	Name Constraints		
4.13.1	Valid DN nameConstraints	Baseline FPKI PD-VAL Service	Valid
4.13.2	Invalid DN nameConstraints	Baseline FPKI PD-VAL Service	Invalid
4.13.3	Invalid DN nameConstraints	Baseline FPKI PD-VAL Service	Invalid
4.13.4	Valid DN nameConstraints	Baseline FPKI PD-VAL Service	Valid
4.13.5	Valid DN nameConstraints	Baseline FPKI PD-VAL Service	Valid
4.13.6	Valid DN nameConstraints	Baseline FPKI PD-VAL Service	Valid
4.13.7	Invalid DN nameConstraints	Baseline FPKI PD-VAL Service	Invalid
4.13.8	Invalid DN nameConstraints	Baseline FPKI PD-VAL Service	Invalid
4.13.9	Invalid DN nameConstraints	Baseline FPKI PD-VAL Service	Invalid
4.13.10	Invalid DN nameConstraints	Baseline FPKI PD-VAL Service	Invalid
4.13.11	Valid DN nameConstraints	Baseline FPKI PD-VAL Service	Valid
4.13.12	Invalid DN nameConstraints	Baseline FPKI PD-VAL Service	Invalid
4.13.13	Invalid DN nameConstraints	Baseline FPKI PD-VAL Service	Invalid
4.13.14	Valid DN nameConstraints	Baseline FPKI PD-VAL Service	Valid
4.13.15	Invalid DN nameConstraints	Baseline FPKI PD-VAL Service	Invalid
4.13.16	Invalid DN nameConstraints	Baseline FPKI PD-VAL Service	Invalid
4.13.17	Invalid DN nameConstraints	Baseline FPKI PD-VAL Service	Invalid
4.13.18	Valid DN nameConstraints	Baseline FPKI PD-VAL Service	Valid
4.13.19	Valid Self-Issued DN nameConstraints	Baseline FPKI PD-VAL Service	Valid

Path Validation Testing Program			
Test #	Test Case Description	Corresponding FPKI PD-VAL Service	Expected Validation Test Result
4.13.20	Invalid Self-Issued DN nameConstraints	Baseline FPKI PD-VAL Service	Invalid
4.13.21	Valid RFC822 nameConstraints	Baseline FPKI PD-VAL Service	Valid
4.13.22	Invalid RFC822 nameConstraints	Baseline FPKI PD-VAL Service	Invalid
4.13.23	Valid RFC822 nameConstraints	Baseline FPKI PD-VAL Service	Valid
4.13.24	Invalid RFC822 nameConstraints	Baseline FPKI PD-VAL Service	Invalid
4.13.25	Valid RFC822 nameConstraints	Baseline FPKI PD-VAL Service	Valid
4.13.26	Invalid RFC822 nameConstraints	Baseline FPKI PD-VAL Service	Invalid
4.13.27	Valid DN and RFC822 nameConstraints	Baseline FPKI PD-VAL Service	Valid
4.13.28	Invalid DN and RFC822 nameConstraints	Baseline FPKI PD-VAL Service	Invalid
4.13.29	Invalid DN and RFC822 nameConstraints	Baseline FPKI PD-VAL Service	Invalid
4.13.30	Valid DNS nameConstraints	Baseline FPKI PD-VAL Service	Valid
4.13.31	Invalid DNS nameConstraints	Baseline FPKI PD-VAL Service	Invalid
4.13.32	Valid DNS nameConstraints	Baseline FPKI PD-VAL Service	Valid
4.13.33	Invalid DNS nameConstraints	Baseline FPKI PD-VAL Service	Invalid
4.13.34	Valid URI nameConstraints	Baseline FPKI PD-VAL Service	Valid
4.13.35	Invalid URI nameConstraints	Baseline FPKI PD-VAL Service	Invalid
4.13.36	Valid URI nameConstraints	Baseline FPKI PD-VAL Service	Valid
4.13.37	Invalid URI nameConstraints	Baseline FPKI PD-VAL Service	Invalid
4.13.38	Invalid DNS nameConstraints	Baseline FPKI PD-VAL Service	Invalid
4.14	Distribution Points		
4.14.1	Valid distributionPoint	Baseline FPKI PD-VAL Service	Valid
4.14.2	Invalid distributionPoint	Baseline FPKI PD-VAL Service	Invalid
4.14.3	Invalid distributionPoint	Baseline FPKI PD-VAL Service	Invalid
4.14.4	Valid distributionPoint	Baseline FPKI PD-VAL Service	Valid
4.14.5	Valid distributionPoint	Baseline FPKI PD-VAL Service	Valid
4.14.6	Invalid distributionPoint	Optional FPKI PD-VAL Service: Products that can process a nameRelativeToCRLIssuer in the cRLDistributionPoint and/or issuingDistributionPoint	Invalid

Path Validation Testing Program			
Test #	Test Case Description	Corresponding FPKI PD-VAL Service	Expected Validation Test Result
4.14.7	Valid distributionPoint	Optional FPKI PD-VAL Service: Products that can process a nameRelativeToCRLIssuer in the cRLDistributionPoint and/or issuingDistributionPoint	Valid
4.14.8	Invalid distributionPoint	Optional FPKI PD-VAL Service: Products that can process a nameRelativeToCRLIssuer in the cRLDistributionPoint and/or issuingDistributionPoint	Invalid
4.14.9	Invalid distributionPoint	Baseline FPKI PD-VAL Service	Invalid
4.14.10	Valid No issuingDistributionPoint	Baseline FPKI PD-VAL Service	Valid
4.14.11	Invalid onlyContainsUserCerts CRL	Baseline FPKI PD-VAL Service	Invalid
4.14.12	Invalid onlyContainsCACerts CRL	Baseline FPKI PD-VAL Service	Invalid
4.14.13	Valid onlyContainsCACerts CRL	Baseline FPKI PD-VAL Service	Valid
4.14.14	Invalid onlyContainsAttributeCerts	Baseline FPKI PD-VAL Service	Invalid
4.14.15	Invalid onlySomeReasons	Optional FPKI PD-VAL Service: Products that process the onlySomeReasons field of the issuingDistributionPoint extension	Invalid
4.14.16	Invalid onlySomeReasons	Optional FPKI PD-VAL Service: Products that process the onlySomeReasons field of the issuingDistributionPoint extension	Invalid
4.14.17	Invalid onlySomeReasons	Optional FPKI PD-VAL Service: Products that process the onlySomeReasons field of the issuingDistributionPoint extension	Invalid
4.14.18	Valid onlySomeReasons	Baseline FPKI PD-VAL Service	Valid
4.14.19	Valid onlySomeReasons	Optional FPKI PD-VAL Service: Products that process the onlySomeReasons field of the issuingDistributionPoint extension	Valid
4.14.20	Invalid onlySomeReasons	Optional FPKI PD-VAL Service: Products that process the onlySomeReasons field of the issuingDistributionPoint extension	Invalid
4.14.21	Invalid onlySomeReasons	Optional FPKI PD-VAL Service: Products that process the onlySomeReasons field of the issuingDistributionPoint extension	Invalid

Path Validation Testing Program			
Test #	Test Case Description	Corresponding FPKI PD-VAL Service	Expected Validation Test Result
4.14.22	Valid IDP with indirectCRL	Optional FPKI PD-VAL Service: Products that process indirect CRLs	Valid
4.14.23	Invalid IDP with indirectCRL	Optional FPKI PD-VAL Service: Products that process indirect CRLs	Invalid
4.14.24	Valid IDP with indirectCRL	Baseline FPKI PD-VAL Service	Valid
4.14.25	Valid IDP with indirectCRL	Optional FPKI PD-VAL Service: Products that process indirect CRLs	Valid
4.14.26	Invalid IDP with indirectCRL	Optional FPKI PD-VAL Service: Products that process indirect CRLs	Invalid
4.14.27	Invalid cRLIssuer	Optional FPKI PD-VAL Service: Products that process indirect CRLs	Invalid
4.14.28	Valid cRLIssuer	Optional FPKI PD-VAL Service: Products that process indirect CRLs	Valid
4.14.29	Valid cRLIssuer	Optional FPKI PD-VAL Service: Products that process indirect CRLs; Products that can process a nameRelativeToCRLIssuer in the cRLDistributionPoint and/or issuingDistributionPoint	Valid
4.14.30	Valid cRLIssuer	Optional FPKI PD-VAL Service: Products that process indirect CRLs (and properly handle a CRL issuer certificate that's signed with the same key as the key that signs the CRL identified in its own CDP)	Valid
4.14.31	Invalid cRLIssuer	Optional FPKI PD-VAL Service: Products that process indirect CRLs	Invalid
4.14.32	Invalid cRLIssuer	Optional FPKI PD-VAL Service: Products that process indirect CRLs	Invalid
4.14.33	Valid cRLIssuer	Optional FPKI PD-VAL Service: Products that process indirect CRLs	Valid
4.14.34	Invalid cRLIssuer	Optional FPKI PD-VAL Service: Products that process indirect CRLs	Invalid
4.14.35	Invalid cRLIssuer	Optional FPKI PD-VAL Service: Products that process indirect CRLs	Invalid
4.15	Delta-CRLs		
4.15.1	Invalid deltaCRLIndicator No Base	Baseline FPKI PD-VAL Service	Invalid
4.15.2	Valid delta-CRL	Optional FPKI PD-VAL Service: Products that support delta-CRLs	Valid
4.15.3	Invalid delta-CRL	Optional FPKI PD-VAL Service: Products that support delta-CRLs	Invalid

Path Validation Testing Program			
Test #	Test Case Description	Corresponding FPKI PD-VAL Service	Expected Validation Test Result
4.15.4	Invalid delta-CRL	Optional FPKI PD-VAL Service: Products that support delta-CRLs	Invalid
4.15.5	Valid delta-CRL	Optional FPKI PD-VAL Service: Products that support delta-CRLs	Valid
4.15.6	Invalid delta-CRL	Optional FPKI PD-VAL Service: Products that support delta-CRLs	Invalid
4.15.7	Valid delta-CRL	Optional FPKI PD-VAL Service: Products that support delta-CRLs	Valid
4.15.8	Valid delta-CRL	Optional FPKI PD-VAL Service: Products that support delta-CRLs	Valid
4.15.9	Invalid delta-CRL	Optional FPKI PD-VAL Service: Products that support delta-CRLs	Invalid
4.15.10	Invalid delta-CRL	Optional FPKI PD-VAL Service: Products that support delta-CRLs	Invalid
4.16	Private Certificate Extensions		
4.16.1	Valid Unknown Not Critical Cert Extnsn	Baseline FPKI PD-VAL Service	Valid
4.16.2	Invalid Unknown Critical Cert Extnsn	Baseline FPKI PD-VAL Service	Invalid

APPENDIX C: PATH DISCOVERY TESTING PROGRAM – TEST CASE DETAILS

Path Discovery Testing Program			
Test #	Test Case Description	Corresponding FPKI PD-VAL Service	Expected Validation Test Result
4.1	Rudimentary		
4.1.1	Rudimentary Directory-based Path Discovery		
4.1.1.1	Rudimentary Directory Path Discovery	Baseline FPKI PD-VAL Service	Valid
4.1.1.2	Rudimentary Directory Path Discovery	Baseline FPKI PD-VAL Service	Valid
4.1.1.3	Rudimentary Directory Path Discovery	Baseline FPKI PD-VAL Service	Valid
4.1.1.4	Rudimentary Directory Path Discovery	Baseline FPKI PD-VAL Service	Invalid (Revoked EE)
4.1.1.5	Rudimentary Directory Path Discovery	Baseline FPKI PD-VAL Service	Valid
4.1.1.6	Rudimentary Directory Path Discovery	Baseline FPKI PD-VAL Service	Invalid (Revoked EE)
4.1.1.7	Rudimentary Directory Path Discovery	Baseline FPKI PD-VAL Service	Valid
4.1.1.8	Rudimentary Directory Path Discovery	Baseline FPKI PD-VAL Service	Invalid (Revoked EE)
4.1.1.9	Rudimentary Directory Path Discovery	Baseline FPKI PD-VAL Service	Invalid (Revoked CA)
4.1.1.10	Rudimentary Directory Path Discovery	Baseline FPKI PD-VAL Service	Invalid (Revoked EE)
4.1.1.11	Rudimentary Directory Path Discovery	Baseline FPKI PD-VAL Service	Invalid (Revoked CA)
4.1.1.12	Rudimentary Directory Path Discovery Referral	Baseline FPKI PD-VAL Service	Valid
4.1.1.13	Rudimentary Directory Path Discovery Referral	Baseline FPKI PD-VAL Service	Invalid (Revoked EE)
4.1.2	Rudimentary URI based Path Discovery		
4.1.2.1	Rudimentary LDAP Path Discovery	Baseline FPKI PD-VAL Service	Valid
4.1.2.2	Rudimentary HTTP Path Discovery	Baseline FPKI PD-VAL Service	Valid
4.1.2.3	Rudimentary LDAP Path Discovery	Baseline FPKI PD-VAL Service	Valid
4.1.2.4	Rudimentary HTTP Path Discovery	Baseline FPKI PD-VAL Service	Valid
4.1.2.5	Rudimentary LDAP Path Discovery	Baseline FPKI PD-VAL Service	Valid
4.1.2.6	Rudimentary LDAP Path Discovery	Baseline FPKI PD-VAL Service	Invalid (Revoked EE)
4.1.2.7	Rudimentary HTTP Path Discovery	Baseline FPKI PD-VAL Service	Valid
4.1.2.8	Rudimentary HTTP Path Discovery	Baseline FPKI PD-VAL Service	Invalid (Revoked EE)
4.1.2.9	Rudimentary LDAP Path Discovery	Baseline FPKI PD-VAL Service	Valid
4.1.2.10	Rudimentary LDAP Path Discovery	Baseline FPKI PD-VAL Service	Invalid (Revoked EE)

Path Discovery Testing Program			
Test #	Test Case Description	Corresponding FPKI PD-VAL Service	Expected Validation Test Result
4.1.2.11	Rudimentary LDAP Path Discovery	Baseline FPKI PD-VAL Service	Valid
4.1.2.12	Rudimentary LDAP Path Discovery	Baseline FPKI PD-VAL Service	Invalid (Revoked EE)
4.1.2.13	Rudimentary HTTP Path Discovery	Baseline FPKI PD-VAL Service	Valid
4.1.2.14	Rudimentary HTTP Path Discovery	Baseline FPKI PD-VAL Service	Invalid (Revoked EE)
4.1.2.15	Rudimentary HTTP Path Discovery	Baseline FPKI PD-VAL Service	Valid
4.1.2.16	Rudimentary HTTP Path Discovery	Baseline FPKI PD-VAL Service	Invalid (Revoked EE)
4.1.2.17	Rudimentary LDAP Path Discovery	Baseline FPKI PD-VAL Service	Invalid (Revoked CA)
4.1.2.18	Rudimentary LDAP Path Discovery Referral	Baseline FPKI PD-VAL Service	Valid
4.1.2.19	Rudimentary LDAP Path Discovery Referral	Baseline FPKI PD-VAL Service	Invalid (Revoked EE)
4.2	Basic Path Discovery		
4.2.1	Basic Directory-based Path Discovery		
4.2.1.1	Basic Directory Mesh Path Discovery	Baseline FPKI PD-VAL Service	Valid
4.2.1.1	Basic Directory Mesh Path Discovery	Baseline FPKI PD-VAL Service	Valid
4.2.2	Basic URI based Path Discovery		
4.2.2.1	Basic LDAP URI Mesh Path Discovery	Baseline FPKI PD-VAL Service	Valid
4.2.2.2	Basic HTTP URI Mesh Path Discovery	Baseline FPKI PD-VAL Service	Valid
4.2.2.3	Basic LDAP URI Mesh Path Discovery	Baseline FPKI PD-VAL Service	Valid
4.2.2.4	Basic LDAP URI Mesh Path Discovery	Baseline FPKI PD-VAL Service	Valid
4.2.3	Basic Combined Path Discovery		
4.2.3.1	Basic Combined Mesh Path Discovery	Optional FPKI PD-VAL Service: Products that support mesh environments with a mix of URI types in the certificates, including no AIA or SIA in the certificates and CRLs issued by the CAs closest to the trust anchor	Valid