FINAL DRAFT

PATH DISCOVERY & VALIDATION

CRITERIA & METHODOLOGY

JANUARY 30, 2006

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This document describes the process for qualifying proposed solutions that provide government agencies with options to implement path discovery and validation (PD-Val) in various ways.

There are four categories for proposed solutions: toolkits, applications, products, and hosted services.

Toolkits may be used to enable the development of custom applications that require PD-Val capabilities. Applications are COTS products that natively include PD-Val capabilities. Products are considered as plug-ins that add or supplement PD-Val capabilities to applications. The hosting of a qualified validation server in an accredited facility that can provide PD-Val capabilities to clients is defined as services.

This document defines key roles and responsibilities. The process to qualify and engage a proposed solution is also detailed, and is highlighted by the following steps:

- Vendor Submits Questionnaire
- Questionnaire Assessment
- Test Planning
- Conduct Testing
- Determination of Test Outcome
- Add solution to *PD-Val Qualified List*

1.0 INTRODUCTION

The Federal Public Key Infrastructure Policy Authority (FPKIPA) sets policy governing operation of the Federal PKI Architecture (FPKIA), and approves applicants for cross certification with the Federal Bridge Certification Authority (FBCA).

It was created by and operates under authority of the Federal Chief Information Officers Council and is composed of entities who wish to interoperate and exchange digital certificates with the FPKIA.

The FPKIPA efforts primarily focus on providing an infrastructure that facilitates trust through: 1) cross-certifying with the Federal Bridge Certification Authority, 2) providing the Common Policy Certificate Authority as a trust anchor and root certification authority for trusted third party vendors operating under the Shared Service Providers program, 3) cross-certifying with the C4 Certification Authority with commercial and other external PKIs at a trust level separate from those found in the FBCA, and 4) providing secure server certificates from the E-Governance Certificate Authority to credential service providers audited by the E-Authentication Program Management Office, for purposes of mutual authentication during interchanges to validate credentials.

To address policy, technical, and business issues relating to the architecture, the FPKIPA may create or have temporary or permanent subordinate committees or working groups as determined by a vote of the membership, to incorporate comments and support for operation of the FPKIA.

The FPKIPA found it essential that relying parties have path discovery and validation (PD-Val) solutions if they are to use the FPKIA. Agency applications rely on PD-Val solutions to determine certificate status (i.e., whether the certificate can be trusted).

Based on this need, the FPKIPA established the PD-Val Working Group (WG) to test and recommend infrastructure or desktop validation solutions that facilitate certificate validation across the FPKIA. It is comprised of federal representatives, contractors supporting federal agencies, and industry partners offering solutions that are integrated with the end-entity's application, web-server plug-ins, or a hosted service for an organization.

The PD-Val WG has written this document to describe the process for qualifying an infrastructure or desktop validation solution.

The scope of this document is limited to defining how a questionnaire is processed, and the manner in which a solution is tested, specifically for qualification purposes.

2.0 GENERAL APPROACH

Qualification of a proposed solution is based on the ability to successfully demonstrate path discovery and validation capability using the Public Key Interoperability Test Suite (PKITS) and the Path Discovery Test Suite.

A vendor begins the process by completing a questionnaire. The PD-Val WG reviews the information provided by the vendor and determines whether to proceed with testing, which is conducted by the Operational Authority (OA) Team at the direction of the OA Program Manager.

Test results are reviewed by the PD-Val WG and if the product passed the tests satisfactorily, it is posted to the *Qualified Validation List* along with a technical synopsis at http://www.cio.gov/fbca/validation_solutions.htm.

3.0 ROLES AND RESPONSIBILITIES

This section describes the key roles and responsibilities associated with qualifying a solution. Figure 1 shows the end-to-end qualification process, highlighting the roles and responsibilities discussed here.

3.1 Federal PKI Policy Authority

The Federal PKI Policy Authority (FPKIPA) has overall responsibility for coordinating technical addressing the availability of end-to-end solutions for use with the FPKIA. For PD-Val solutions, the FPKIPA has the following responsibilities:

- Oversees the PD-Val WG

3.2 Path Discovery and Validation Working Group

The PD-Val WG is one of the working arms for the FPKIPA. It has the following responsibilities:

- Reviews responses to questionnaire to determine acceptability
- Determines whether a vendor qualifies, per test results
- Approve technical synopses
- Qualify validation solutions based on test results
- Notify webmaster to a post synopsis

3.3 Operational Authority Program Manager

The OA Program Manager has overall responsibility in directing the OA Team, as well as, facilitating interaction between the OA Team and external entities. The OA Program Manager has the following responsibilities:

- Plans tests for all qualification activities
- Plans infrastructure and resources for all FPKI test environment activities

3.4 Operational Authority Team

The OA Team performs technical testing. They provide test results and status updates throughout the testing process. The OA Team has the following responsibilities:

- Have vendor to sign lab agreements
- Prepare test plan
- Prepare written technical synopses for the PD-Val WG
- Document configurations that passed testing

4.0 STANDARD PRACTICE

4.1 Questionnaire Submission

The vendor submits a completed questionnaire to the PD-Val WG, which reviews it for completeness and clarity. If complete and clear, the PD-Val WG determines whether testing is in the best interest of the government. The PD-Val WG notifies the Operational Authority Program Manager and its team to prepare for testing, if the product is feasible. The questionnaire can be found at http://www.cio.gov/fbca/validation_solutions.htm.

4.2 Test Planning

The OA Program Manager determines testing resource needs, and establishes a testing schedule. Inputs from the vendor are obtained as necessary. The OA Team establishes a test plan and shares it with the PD-Val WG and the vendor. The copy to the vendor will include the validation lab agreement for signature.

4.3 Testing

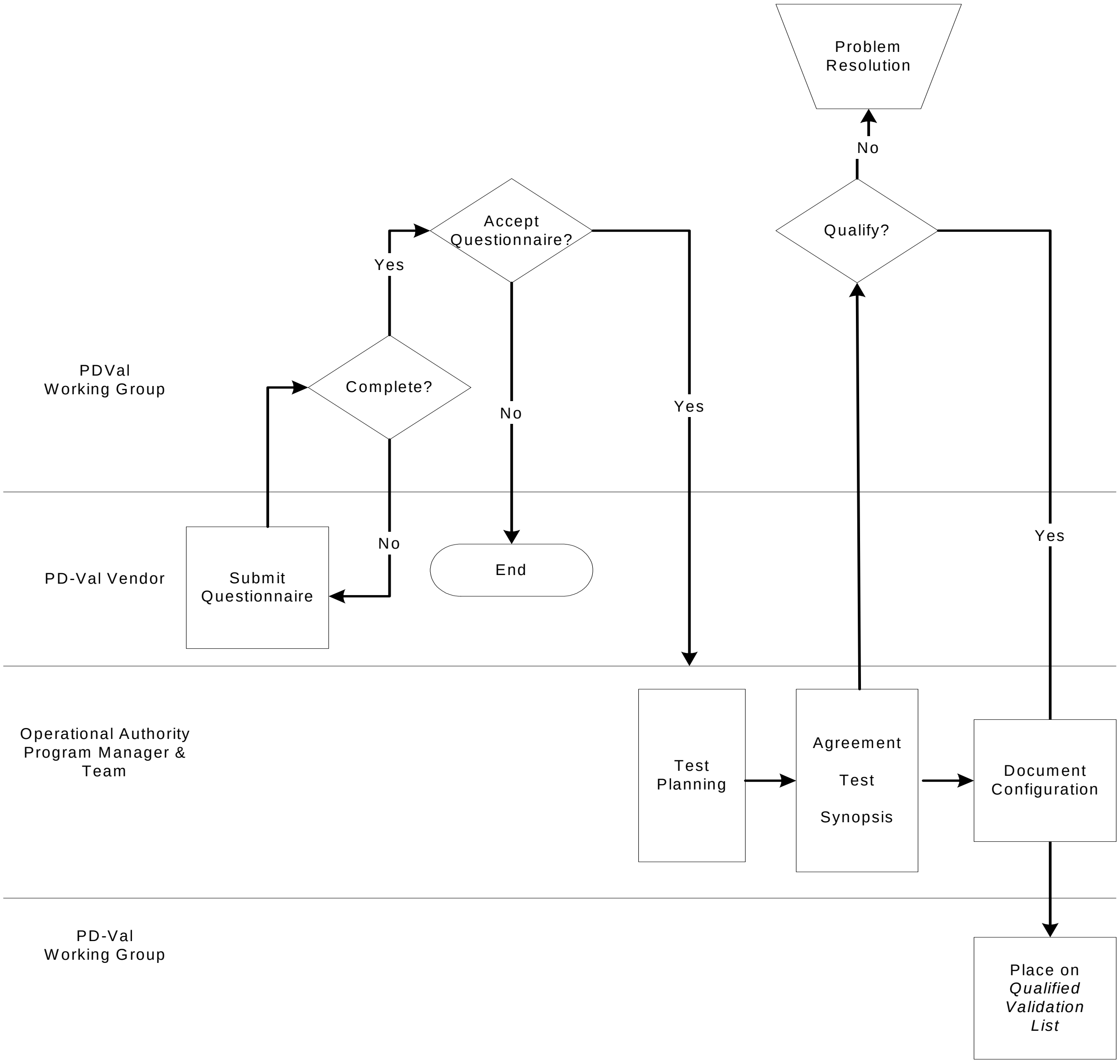
The OA Team conducts testing in accordance with the test plan. If the results are favorable, the team prepares and sends the test result report and synopsis for the PD-Val WG's review. Otherwise, the test result report is forwarded to the PD-Val WG for problem resolution.

4.4 Determination of Test Outcome

The PD-Val WG determines whether the solution is qualified, based on the test results and notifies the vendor of the decision.

4.5 List Validation Solution

The PD-Val WG informs the FPKIPA of the qualified solution and posts the technical synopsis on the PD-Val website.



5.0 HOSTED VALIDATION SERVICES

A Hosted Validation Service (HVS) is an end-to-end service that validates PKI certificates remote from the agency application. The HVS server is hosted by a Validation Service Provider (VSP) at their facility. An agency application, enabled with validation functionality provided by the VSP, requests the remotely hosted HVS to inspect and validate the PKI certificate. If information returned to the agency application indicates that the PKI certificate is valid and its assurance level is appropriate for the agency application (equal to or higher than the assurance level required by the agency application), the agency application can make access control decisions as appropriate for that user.

In conjunction with the standard practice, a HVS has additional requirements to meet, as it is provided on behalf of the federal government.

The VSP must undergo a certification and accreditation (C&A) process, as a requirement of the Federal Information Security Management Act (FISMA) of 2002. The process should be performed in accordance with National Institute of Standards and Technology Special Publication 800-53, for moderate level (minimum) information system.

A previous federal accreditation may be leveraged with the completion of the following requirements:

- Install product into the accredited environment (if applicable)
- Configure product with the OA Team's documented configuration
- Test successfully with a production application
- Have a third-party qualified auditor perform a risk assessment to ensure that the product has been configured properly and poses no new threats or risks to the accredited environment.

Upon completion of these steps, the auditor should provide their Designated Approving Authority and the PD-Val WG with Letter-A stating that the product was already included in VSP's environment and meet the above requirements or Letter-B stating that the product was added to the VSP's environment and meet the above requirements.

6.0 PROBLEM RESOLUTION

In the event a validation solution does not successfully pass the PD-Val test suites, the PD-Val WG will provide the vendor with the test results to discuss the residual issues and to determine the next steps.