FPKI OA:
End-Entity Test Procedures

Last updated: October 28, 2005

TABLE OF CONTENTS

SECTION 1 : INTRODUCTION 3

SECTION 2 : TESTING INFRASTRUCTURE 4

2.1 PROTOTYPE DIRECTORY AND CA INFRASTRUCTURE 4
2.2 VALIDATION ENGINES AND SERVICES 5

SECTION 3 : AGENCY APPLICATION PREREQUISITES AND POLICIES 6

3.1 RISK ASSESSMENT 6
3.2 PRE-OPERATIONAL TESTING 6
3.3 PKI-ENABLING THE APPLICATION 6
3.4 PKI VALIDATION OPERATIONS 7

SECTION 4 : TESTING SCENARIOS AND PROCEDURES 8

4.1 AA OWNERSHIP INFORMATION 8
4.2 PDVAL Product and Configuration Information 8
4.3 Basic Network Connectivity and Directory Chaining Test 9
4.4 PATH DISCOVERY PERFORMANCE TESTS 10
4.4.1 Testing With a Valid Certificate 10
4.4.2 Path Discovery and Validation Timed Performance 10
4.4.3 Testing With a Revoked Certificate 10
4.4.4 Testing With an Expired Certificate 11
4.4.5 Testing With a Suspended Certificate [Optional] 11
4.4.6 Testing With an Unmapped Certificate 11
4.4.7 Testing With an Untrusted Certificate 11
4.5 EE CERTIFICATE ACCEPTABILITY 12

APPENDIX A : ACRONYMS 13

SECTION 1: INTRODUCTION

This document provides testing procedures for agency applications (AAs) wishing to interoperate with the production Federal Public Key Infrastructure Architecture (FPKIA). These tests focus on end-to-end testing from the AA—whether a desktop or server-based application—through an FPKI-approved certificate path discovery and path validation (PDVAL) engine, through the FPKI directory infrastructure, to FPKI-authorized credential service provider (CSP).

Upon approval from the FPKI Policy Authority, agencies should complete and submit the testing results form (found in Section 4 of this document) to the FPKI Operational Authority (OA). Agencies should complete these tests against the Prototype FPKIA before connecting to the Production FPKIA. The submitted test results will serve as evidence of testing and will be kept on file as background for any future debugging sessions.

The FPKI OA is available to provide additional guidance, if necessary.

SECTION 2: TESTING INFRASTRUCTURE

The FPKI OA, in conjunction with all cross-certified CSPs, provides a testing infrastructure—called the Prototype FPKIA—that parallels the Production FPKIA. This section describes components of the prototype infrastructure and the roles of various stakeholders.

2.1 PROTOTYPE DIRECTORY AND CA INFRASTRUCTURE

One purpose of the Production FPKI X.500 directory is to provide a single access point from which all cross-certificates, CA certificates, and CRLs can be retrieved.

Prior to final approval by the FPKI PA for cross-certification, each CSP must demonstrate X.500 or LDAP directory interoperability, including directory chaining. Additionally, each CSP must stand up a test CA that issues cross-certificates to the Prototype FPKIA CA. Even after cross-certification with the Production FPKIA, each CSP is encouraged to continually maintain their test CA and prototype directory infrastructure, mimicking the CSP's production CA hierarchy and border directories, giving detail to the following characteristics:

- The CSP's test CAs and directory products will match those in their production environment, although the patch/revision levels need not match exactly (but should be only a version level or two apart). Specifically, the CSP is encourage to apply software patches to their test CAs and prototype directories to ensure successful interoperability before applying those same patches to their production systems. Similarly, the CSP should test new products in the Prototype FPKIA before deploying in production.
- All cross-certificates, root CA certificates, and subordinate CA certificates appearing in a CSP's production environment have commensurate counterparts in the prototype environment.
- Similarly, all chaining agreements in a CSP's production environment have corresponding counterparts in the prototype environment.
- Similarly for SIA, AIA, and AKI field formats used in all root, subordinate, cross-certificates, and end-entity certificates. Also, there should be an exact correspondence in certificate profile formats between production and test certificates.
- If delta CRLs or partitioned CRLs are used in the production environment, then they are also used in the prototype environment.
- Certificate policy information should match that of their proposed production cross-certificate to and from the FPKIA. There are test certificate policy Object Identifiers (OIDs) on the NIST website http://csrc.nist.gov/csor/pkireg.htm, under the heading, *PKI Pilots and Testing Registered Objects.* Four (4) of these OIDS are used in the FPKIA prototype cross-certificates. The remaining six (6) OIDS may be used by CSPs in their prototype cross-certificate to and from the FPKIA, if necessary.

All participating CSPs will issue end-entity (EE) test certificates from their test environment. Private keys will also be provided by the CSP in those instances where the test user can not or prefers not to generate their own private key. These EE test certificates will be used in the compliance tests of Section 4.

When possible, the public certificates containing the test keys will be stored in the CSP's prototype X.500 directory. It is left to the CSP's discretion as to how they would like to handle the corresponding private keys.

At least one of each of the following statuses of test certificates will be made available from the CSP to the AA testers:

- A valid certificate
- A revoked certificate
- An expired certificate
- Optionally, a suspended certificate

2.2 VALIDATION ENGINES AND SERVICES

AAs may use only those PDVAL validation engine products or hosted validation services that have been previously tested and approved by the Path Discovery and Validation Working Group (PD-VAL). If an agency wishes to use a PDVAL product or service that has not yet been approved, the AA should direct the vendor to contact the PD-VAL Co-Chairs for instructions on how to submit their product for compliance testing. In the interim, the agency or organization is encouraged *not* to proceed with the tests of Section 4 incase PDVAL product enhancements or patches are required.

SECTION 3: AGENCY APPLICATION PREREQUISITES AND POLICIES

This section outlines evaluations and testing which must be completed, and policies which must be in place before an agency application (AA) is permitted to interoperate with the FPKIA infrastructure.

3.1 RISK ASSESSMENT

Each AA must undergo a risk assessment (RA)[1] to determine the minimum level of assurance (LOA) of end-entity certificates acceptable to that application. (Please note that acceptable LOAs are expressed from the viewpoint of the trust anchor, as discussed further in Section 4.2.)

3.2 PRE-OPERATIONAL TESTING

If desired, AAs should first connect to, and test thoroughly with the prototype infrastructure (discussed in Section 2) before connecting with the production FPKIA infrastructure. The required functionality and interoperability tests are detailed in Section 4, and the associated questionnaire and checklist must be completed and transmitted to the FPKI OA.

3.3 PKI-ENABLING THE APPLICATION

Each AA must be PKI-enabled. Depending on the purpose of the application, and whether the application is to be deployed on the end-user's desktop or hosted on a central server as a web-based tool, the PKI integration and enabling steps vary greatly.

Assuming one of the purposes of the PKI component of the AA is for access control, the following is a brief overview of functionality expected in a PKI-enabled AA:

- The AA must prompt for and accept presentation of user's credentials
- The AA must locally verify proof of private key (typically through a signed nonce)
- The AA must pass the user's public certificate to the validation service[2] (VS) which will handle all aspects of certification validation and associate trust configuration and management
- The AA must convey the flavor of validation results to user (e.g., informing the user of why they are being denied access)
- The AA must locally log validation results as part of their system of records

[1] e-Authentication participants can find additional information on that program's Electronic Risk and Requirements Assessment (ERA) at: http://www.cio.gov/eauthentication/era.htm

[2] The validation service may be either a PDVAL product or a hosted service, but it must be a product or service pre-approved by the FPKI OA

- The AA authentication module must then pass a unique representation[3] of the user's identity to the authorization module to determine exact access privileges

3.4 PKI VALIDATION OPERATIONS

Certificate validation consists of two phases: trust path discovery and trust path validation. Trust path discovery is the process of discovery a chain of cross-certificates and CA certificates from the relying party's trust anchor to the end-entity's certificate. A trust path may be discovered dynamically each time as needed, or it may be constructed once manually and stored (or "cached"); PDVAL products may vary in how they choose to implement this operation. Trust path validation is the process of examining each certificate comprising the trust path, and consulting the issuing CA's CRL or OCSP responder to determine the certificate's validity status at that moment. It is expected that even if a trust path is pre-cached, all certificates in the trust path are validated in real-time at the beginning of each transaction.

Each AA must use a PDVAL product (or service) that finds certificate trust paths for only those policy OIDs acceptable to that AA's requirements. (Acceptable policy OIDs can be those directly recognizable by the trust anchor, as will be discussed in Section 4.2.)

[3] The unique representation of the user's identity could take the form of the SHA-256 hash of the concatenation of the following fields extracted directly from the user's public certificate: issuer's DN string; subject's DN string; issuer's public key

SECTION 4: TESTING SCENARIOS AND PROCEDURES

This section focuses on the end-to-end tests to be performed by the agency application (AA) owners. This section also functions as a questionnaire to be completed by the AA owners and returned to the FPKI OA, which will keep the answers on file. The questionnaire answers will provide a good starting point for any necessary debugging sessions.

4.1 AA Ownership Information

Name of AA:

Brief description of AA:

Managing POC (name & email address):

Technical POC (name & email address):

4.2 Validation Product and Configuration Information

- Name of Validation product or service:

A relying party (RP) using path discovery and validation must specify two key items: a trust anchor and a set of acceptable certificate policy OIDs. Technically speaking, a trust anchor is a trusted public key, the public key algorithm, and the trusted issuer name [RFC3280 §6.1.1]. Although a trust anchor is not the entire public key certificate, it is convenient to convey trust anchor information via a certificate. It is assumed that most PDVAL products will read the trusted public key from a certificate, but it is also possible that an isolated trusted public key can be taken as input. If the latter is the case, please also write the word "isolated" after the thumbprint in the following question.

N.B.: You are not permitted use the Federal Bridge Certification Authority (FBCA) root CA public key as your trust anchor. If you are not using a public key from locally issued root CA as your trust anchor and you wish to an FPKI-issue public key instead, it is recommended that you use the Common Policy root CA's public key.

SHA1 thumbprint of DER-encoded certificate containing trusted public key: **N/A**

Expiration date of public certificate containing trust anchor public key: **N/A**

If the relying party wishes to honor the policy mappings in cross-certificates, then acceptable certificate policy OIDs must be also be specified. These policy OIDs are express in the policy space of the trust anchor. For instance, the cross-certificate issued[4] from the Common Policy root CA to the FBCA root CA contains a policy mapping from 2.16.840.1.101.3.2.1.3.7 (id-fpki-common-hardware) in the issuer's domain to 2.16.840.1.101.3.2.1.3.4 (id-fpki-certpcy-highAssurance) in the subject's domain. If your trust anchor is the Common Policy root's public key and you wish to accept only "FBCA High" Level of Assurance credentials, then you would specify the certificate policy OID in the Common Policy's domain, i.e. you would specify 2.16.840.1.101.3.2.1.3.7 (id-fpki-common-hardware) as your acceptable policy OID.

Acceptable policy OIDs: **N/A**

The following questions will determine if you used the correct PDVAL and AA configuration methods, and it will serve as a good reminder for you later on how to change the setting(s). (One type of acceptable answer could be: Entered the address 66.10.x.x into "Edit // Configuration… // Default X.500 Directory [tab] // IP Address [box]")

How did you confirm the PDVAL product/service is using the FPKI infrastructure? **N/A**

How did you confirm the AA is using the PDVAL product/service? **N/A**

4.3 Basic Network Connectivity and Directory Chaining Test

The tests in this section confirm that the underlying operating system's TCP/IP network settings are correct and communications are not being blocked by intervening firewalls. A system administrator is probably the best candidate for perform these tests. (Checking the box indicates the test has been completed successfully.)

From the computer hosting the PDVAL software, confirm the DNS servers have entries for the DNS name found in the CDP field of any production cert: ______________________________ [**N/A**]

From the computer hosting the PDVAL software, use an LDAP browser/client to connect to the prototype FBCA directory and retrieve the EE test certs: _______________________________ [**N/A**]

Using the PDVAL software testing interface, submit a valid public test certificate (no private key required), and confirm a correct validation response: __________________________________ [**N/A**]

[4] We examined the cross-certificated issued from "CN=Common Policy, OU=FBCA, O=U.S. Government, C=US" to "OU=Entrust, OU=FBCA, O=U.S. Government, C=US" on August 22, 2005, and valid through October 6, 2010 with the SHA1 thumbprint ce 07 73 9d 58 e4 25 04 08 5f 20 37 65 e6 e5 3c 48 4f c4 bd.

4.4 Path Discovery Performance Tests

Tests in this section confirm end-to-end behavior of the agency application (AA). A user with both test certificate and its corresponding private key should perform these tests. (Checking the box indicates the test has been completed successfully.)

4.4.1 Testing With a Valid Certificate

Using a valid end-entity (EE) test private key, submit an EE test public certificate to the AA: __ [__]

Ensure user is granted appropriate access: ____ [__]

Ensure access granting is logged properly: ____ [__]

4.4.2 Path Discovery and Validation Timed Performance – N/A

The following test both ensures that AA time-outs are set correctly and manages expectations of performances of your PDVAL system:

Repeat the above test 5 times and calculate the average time to (optionally discover)[5] and validate the certificate path: ____ seconds

Using a valid EE certificate from a 2nd cross-certified CA, repeat the timed tests of Section 4.4.1 and calculate the average time to (optionally discover) and validate the certificate path: ___ seconds

Using a valid EE certificate from a 3rd cross-certified CA, repeat the timed tests of Section 4.4.1 and calculate the average time to (optionally discover) and validate the certificate path: ___ seconds

4.4.3 Testing With a Revoked Certificate

Using a revoked EE test private key, submit an EE test public certificate to the AA: _________ [__]

Ensure user access is denied: ____ [__]

Ensure user is informed why access has been denied: _________________________________ [__]

Ensure access denial is logged properly: ____ [__]

[5] PDVAL products may optionally choose to cache previously discovered paths for a certain amount of time. In that case, these timed tests will reflect only the time needed to validate a certificate path and not the time to discover it.

4.4.4 Testing With an Expired Certificate

Submit an expired EE test certificate to the AA: ________________________________ [__]

Ensure user access is denied: ____ [__]

Ensure user is informed why access has been denied: _____________________________ [__]

Ensure access denial is logged properly: ______________________________________ [__]

4.4.5 Testing With a Suspended Certificate [Optional]

e.g. A CRL check was used for all tests.

Submit a suspended EE test certificate to the AA: _____________________________ [**N/A**]

Ensure user access is denied: ____ [**N/A**]

Ensure user is informed why access has been denied: ___________________________ [**N/A**]

Ensure access denial is logged properly: ____________________________________ **[N/A]**

4.4.6 Testing With an Unmapped Certificate

As stated in Section 4.3, **[Application name]** uses a Trust List model.

Submit to the AA an EE certificate from a cross-certified CA, but containing a policy OID for which no valid path exists: ____ [**N/A**]

Ensure no path is discovered: ____ [**N/A**]

Ensure user access is denied: ____ [**N/A**]

Ensure user is informed why access has been denied: ___________________________ [**N/A**]

Ensure access denial is logged properly: ____________________________________ [**N/A**]

Repeat test 5 times and calculate average time to timeout: ______________________ seconds

4.4.7 Testing With an Untrusted Certificate

As stated in Section 4.3, **[Application name]** uses a Trust List model.

Submit an EE certificate issued from an unknown (i.e., not cross-certified) CA: ___________ [__]

Ensure no path is discovered: ____ [**N/A**]

Ensure user access is denied: ____ [__]

Ensure user is informed why access has been denied: ______________________________ [__]

Ensure access denial is logged properly: ____ [__]

4.5 EE Certificate Acceptability

Determine if the EE certificate profile is acceptable; e.g.: The profile is acceptable. uses the Issuer DN and CerSerialNumber fields only.

Is the user's email address in field expected? ___________________________________ [___]

If a UID identifier is expected, is it in an acceptable field (e.g., as a standalone RDN or imbedded in the CN RDN)? ____ [___]

If the AA expects specific key usage fields (e.g., data encryption usage, but not the "CA" bit), does the EE certificate conform to expectations? ________________________________ [___]

Please email this completed form to Ms. Cheryl Jenkins at cheryl.jenkins@gsa.gov .

APPENDIX A: ACRONYMS

AA	Agency Application
AIA	Authority Information Access
CA	Certificate Authority (or Certification Authority)
CRL	Certificate Revocation List
CSP	Credential Service Provider
DN	Distinguished Name
FBCA	Federal Bridge Certification Authority
FPKI	Federal PKI
FPKIA	Federal PKI Architecture
LOA	Level(s) of Assurance
OA	Operational Authority
OIDs	Object Identifiers
PDVAL	Path Discover and Validation
PKI	Public Key Infrastructure
RP	Relying Party
SIA	Subject Information Access
SKI	Subject Key Identifier