

# Path Discovery and Validation Working Group

David A. Cooper  
NIST

April 6, 2006

# What is the PD-Val WG?

---

- The PD-VAL WG is a working group of the Federal PKI Policy Authority. Its mission is to make recommendations to the Federal PKI (FPKI) community on infrastructure and desktop solutions that will facilitate bridge-enabled certificate validation. Recommendations are based on the applicant's test results received from the FPKI Lab.
- Meetings are open to both agency representatives and vendors.
- Meetings held about once a month.

# Accomplishments

---

- Developed functional requirements for Path Discovery and Validation
- Sent out RFI to invite vendors to share information about their products' path discovery and validation capabilities
- Established testing program to verify products' capabilities
- Established Qualified Validation List

# Path Validation Requirements

- NIST Recommendation for X.509 Path Validation
  - Establishes path validation requirements at multiple levels (e.g., Enterprise, Bridge-enabled)
    - Levels based on set of extensions that can be processed.
  - Specifies how to use the Public Key Interoperability Test Suite (PKITS) to verify a path validation module's capabilities
  - Applications that satisfy all requirements for Bridge-enabled level generally preferred.

# Path Discovery Requirements

---

- Path Discovery test suite (still under development)
- Currently includes tests at two levels of complexity:
  - Rudimentary: Path discovery in a hierarchy
  - Basic: Path discovery in a mesh with one bridge
- Products currently being tested at both levels
- Plans call for development of Intermediate and Advanced Levels

# Path Discovery Requirements

- At each level there are three distinct PKIs.
- PKIs differ in how intermediate certificates and CRLs can be located:
  - Directory: locate certificates and CRLs based on DNs in **issuer** and **subject** fields and **cRLDistributionPoints** extension.
  - LDAP URI: locate certificates and CRLs based on LDAP URIs in **authorityInfoAccess**, **subjectInfoAccess**, and **cRLDistributionPoints** extensions.
  - HTTP URI: locate certificates and CRLs based on HTTP URIs in **authorityInfoAccess**, **subjectInfoAccess**, and **cRLDistributionPoints** extensions.
- Current Federal PKI only supports Directory based location.

# Qualified Validation List

- Vendors submit information about their products' path discovery and validation capabilities
- PD-Val WG (government members only) review submission and decide whether product should be tested
- Government funded lab performs path discovery and validation testing and reports results to PD-Val WG (government members only)
- If results are deemed satisfactory, product is added to Qualified Validation List (QVL).
  - Synopsis of test results is posted for each product on list.

# Qualified Validation List

---

- Five vendors currently listed
  - Three Web server plug-ins
  - One Delegated Path Validation Server/E-mail client plug-in
  - One Delegated Path Discovery Server/client toolkit
- Agencies should carefully review synopses

# Qualified Validation List

- Products are included on QVL solely based on functional testing of path discovery and validation capabilities
- Inclusion on QVL is not based on:
  - Performance or stress testing
  - Products' capabilities other than path discovery and validation
  - Ease of installation or use
  - Vendor support services
  - Cost
  - Etcetera

# Future Directions for PD-Val WG?

---

- Possible future work includes:
  - Add OCSP to test suite
  - Develop a profile of SCVP for DPV/DPD clients and servers