Path Discovery and Validation Requirements

David A. Cooper
NIST

April 10, 2006

Types of Applications

- Path discovery and validation requirements depend on type of application being supported.
- Applications can be separated into three classes:
  - Intra-agency: Application only needs to validate credentials issued on behalf of a single Agency.
  - Inter-agency: Application only needs to validate credentials issued to U.S. Government employees and contractors.
  - Cross-organization: Application needs to validate crendentials issued by external entities.
- NIST has defined (or is defining) path discovery and validation requirements that are appropriate for each of these classes of application.

Path Validation Requirements and Testing

- The Public Key Interoperability Test Suite (PKITS):
  - Successor to *Conformance Testing of Relying Party Client Certificate Path Processing Logic*, version 1.07
  - Includes over 200 certification paths covering most of the features of RFC 3280
  - Several vendors have been using PKITS to test their path validation libraries

NIST Recommendation for X.509 Path Validation

- Specifies a minimal set of functionality for Path Validation Modules (PVMs) used in:
  - *Enterprise PKIs*: PKI that is limited to a single organization
  - *Bridge-enabled PKIs*: PKI that spans multiple organizations
- Additional packages of functionality are defined.

Enterprise PVMs

- Verify RSA with SHA-1 signatures
- Processing of **basicConstraints** and **keyUsage**
- Basic policy processing
- Processing CRLs, including distribution point CRLs

Bridge-enabled PVMs

- Enterprise PVM requirements + 3 packages:
  - *Name Constraints*: **directoryName** and **rfc822Name**
  - *Policy Mapping*: **policyMappings** extension and **inhibitPolicyMapping**
  - *anyPolicy*: **anyPolicy** OID and **inhibitAnyPolicy** extension

Supplementary Packages

- *Indirect CRLs*: processing indirect CRLs, including
  - **cRLIssuer** field of **cRLDistributionPoints**
  - **indirectCRL** flag of **issuingDistributionPoint**
  - **certificateIssuer** CRL entry extension
- *Reasons*: CRLs segmented by reason code
- *Delta-CRLs*: processing delta-CRLs
- *DSA*: verify DSA with SHA-1 signatures

Path Validation Module Naming Scheme

Path Validation Module Name	NameConstraints	Policy Mapping	anyPolicy	Indirect CRLs	Reasons	Delta-CRLs	DSA
Bridge-enabled PVM with Advanced CRLs [, *f*, and *g*]	✔	✔	✔	✔	✔	*f*	*g*
Bridge-enabled PVM [with *d*, *e*, *f*, and *g*]	✔	✔	✔	*d*	*e*	*f*	*g*
Enterprise PVM with Advanced CRLs[, *a*, *b*, *c*, *f*, and *g*]	*a*	*b*	*c*	✔	✔	*f*	*g*
Enterprise PVM [with *a*, *b*, *c*, *d*, *e*, *f*, and *g*]	*a*	*b*	*c*	*d*	*e*	*f*	*g*

✔: required package for this naming scheme

Optional packages:

a: Name Constraints
b: Policy Mapping
c: anyPolicy
d: Indirect CRLs
e: Reasons
f: Delta-CRLs
g: DSA

Current Status

- *PKITS*:
  - version 1.0 is complete
- *NIST Recommendation for X.509 Path Validation*:
  - Initial draft posted on May 3, 2004
  - Available at http://csrc.nist.gov/pki/PKITesting.html
  - No substantive changes need to be made to address comments

Path Discovery Requirements and Testing

- Path Discovery Test Suite
  - Includes multiple levels that differ in complexity of PKI architecture that must be navigated to build certification path.
  - Test Suite is still under development
  - Rudimentary level (almost complete):
    - Path discovery in hierarchical PKI
    - Sufficient for intra-agency applications
  - Basic level (almost complete):
    - Based on current Federal PKI
    - Sufficient for inter-agency applications

Path Discovery Testing

- Path Discovery Test Suite
  - Intermediate level (not yet developed):
    - Mesh architecture with multiple bridges
    - May be sufficient for cross-organzation applications
  - Advanced level (not yet developed):
    - Complex mesh architecture with “added complexities”
    - Sufficient for cross-organization applications

Path Discovery

- Directory based path discovery
  - locate certificates and CRLs based on DNs in **issuer** and **subject** fields and **cRLDistributionPoints** extension.
- LDAP URI based path discovery
  - locate certificates and CRLs based on LDAP URIs in **authorityInfoAccess**, **subjectInfoAccess**, and **cRLDistributionPoints** extensions.
- HTTP URI based path discovery
  - locate certificates and CRLs based on HTTP URIs in **authorityInfoAccess**, **subjectInfoAccess**, and **cRLDistributionPoints** extensions.

Path Discovery

- Current Federal PKI architecture supports Directory based path discovery
- Support for LDAP URI based path discovery increasing

Are there any intra-agency applications?

- Smart card login?
- Authentication to local email server for POP or IMAP access?
- VPN?

One ID per user?

- Can a contractor who works for multiple agencies get by with a single PIV card?
  - Can the path validation modules of all “intra-agency” applications build and validate certificates across the Federal PKI?
  - Do any of the “intra-agency” applications require impose specific requirements on the certificates?
  - Does the contractor have email accounts at multiple agencies?
    - Would the digital signature and key management certificates need to include all of the email address?
  - Does the application require the presence of a name (e.g., UPN) or KRB5PrincipalName) that is particular to each agency?