Path Validation Testing

NIST Recommendation for X.509 Path Validation

David Cooper
May 19, 2004

NIST Recommendation

- 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 (support for RSA with SHA-256 recommended)
- 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

PKITS

- The Public Key Interoperability Test Suite (PKITS):
  - Includes over 200 certification paths covering most of the features of RFC 3280
  - Covers all features required for Enterprise PVMs, Bridge-enabled PVMs, all four supplementary packages, and more
  - The Draft *NIST Recommendation for X.509 Path Validation* indicates how PKITS can be used to test a PVM

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/testing/x509paths.html
  - Comments due by June 1, 2004

Independent Testing?

- Development of a Protection Profile is not a viable option
- It may be possible to develop an independent testing program similar to the current cryptographic algorithm testing program
- Other options may be considered
- Future direction will depend on level of interest