Path Validation Testing

The Path Validation Module Protection Profiles and the Federal Certificate and CRL Profile

David Cooper
June 23, 2003
PKITS

- The Public Key Interoperability Test Suite (PKITS) is available for review:
  - Includes over 200 certification paths covering most of the features of RFC 3280.
  - Will be used as the basis for advancing RFC 3280 to Draft Standard.
  - Will be the basis for the testing requirements of the Path Validation Module Protection Profiles.
Protection Profiles specify a minimal set of functionality plus several optional functionality packages.

Applications that implement the minimal functionality may be used within Enterprise PKIs, but are not suitable for use in PKIs that span multiple domains.

Applications must implement many of the optional packages in order to be considered Bridge Enabled.
The Packages

- The optional packages are: Name Constraints, Policy Mapping, anyPolicy, delta-CRLs, Distribution Points, indirect CRLs, and DSA.

- Applications must implement the Name Constraints, Policy Mapping, and anyPolicy packages in order to claim that they are Bridge Enabled.

- Applications must implement Distribution Points and indirect CRLs to claim Advanced CRL processing.
PVM PP vs. Federal Profile Algorithms

- PKITS includes tests for RSA and DSA
- Only RSA is required for Bridge Enabled.
- Federal Profile allows RSA, DSA, and ECDSA signatures.
- Federal Profile also allows for DH and ECDH public keys.
PVM PP vs. Federal Profile
Name Constraints

- PKITS includes tests for name constraints on directoryName, rfc822Name, dNSName, and uniformresourceIdentifier.

- DirectoryName, rfc822Name, and dNSName required for Bridge Enabled.

- Federal Profile allows directoryName, rfc822Name, and dNSName.
PVM PP vs. Federal Profile
Distribution Point names

- Federal Profile allows for distribution point names as:
  - fullName:
    • directorName
    • uniformResourceId
  - nameRelativeToIssuer (abbreviated directorName)

- PKITS includes tests for directorName only (both fullName and nameRelativeToIssuer)

- Only fullName required for Bridge Enabled.
Federal Profile allows for indirect CRLs (cRLIssuer field in cRLDistributionPoints extension, indirectCRL field in issuingDistributionPoint extension, and certificateIssuer CRL entry extension)

PKITS includes tests for these features

Required for Advanced CRLs (but not Bridge Enabled).
PVM PP vs. Federal Profile
Other Distribution Point fields

● Federal Profile allows use of onlyContainsUserCerts, onlyContainsCACerts, and onlySomeReasons fields of issuingDistributionPoint extension.

● PKITS includes tests for all of these.

● Required for Advanced CRLs (but not Bridge Enabled).
PVM PP vs. Federal Profile
Delta-CRLs

- Federal Profile allows use of delta-CRLs.
- PKITS includes some delta-CRL tests.
- PVM PP includes a delta-CRL package, but not required for either Bridge Enabled or Advanced CRL.
Recommendations

- Remove the following from the Federal Profile:
  - Use of nameRelativeToIssuer in distribution point names
  - Indirect CRLs
  - Use of onlyContainsUserCerts, onlyContainsCACerts, and onlySomeReasons
  - Delta-CRLs