Revisions to the FPKI Certificate Profile

Tim Polk

David Cooper

May 2, 2002

Background

- FPKI Certificate profile
  - First draft January, 1997 (TWG 97-04)
  - Numerous successive drafts
  - Certificate profile stable April, 2000 (TWG 00-18)
- NIST initiated revisions Cycle
  - First draft February, 2002 (TWG 02-04)
  - March TWG presentation & list discussions
  - New draft April 30, 2002

FPKI Profile Contents

- Two Part document
  - Preamble
    - Identifies reference specifications
    - Introduction to Part II
  - Suite of certificate and CRL profiles
    - Excel Worksheets for each class of certificates and CRLs used in the FPKI
    - Describes contents of
      - each base field in certificate and CRL
      - each FPKI recognized extension

Current Status

- Vendors are actively using the profile because:
  - FBCA references the FPKI Certificate and CRL Profile
  - Agency procurements reference this profile
- Current profile is showing its age
  - Vendors have questioned some requirements

NIST Review

- The FPKI Profile needs to be updated
  - Need to update references
  - Need to clarify requirements
- NIST performed a first pass, making modifications in both the preamble and the Excel Worksheets
  - result is TWG 02-04, on TWG website

Preamble Modifications, 1st Revision

- Based on RFC 3280 (a.k.a., Son-Of-2459) rather than RFC 2459
  - Enhanced path validation algorithm
  - Added a new section on encoding DNs
    - PKIX mandates a 2004 conversion to UTF8String
    - FPKI encoding rules encourage consistent processing by legacy implementations

Preamble Modifications, 2nd Revision

- Added a new section on URIs in certificate and CRL extensions
  - URIs appear in four extensions:
    - cRLDistributionPoints, issuingDistributionPoint, authorityInfoAccess, subjectInfoAccess
  - Preamble limits URIs to ldap and http
    - http, https – used for OCSP servers
    - ldap – used for all other purposes
      - The hostname or IP address of server is required
      - The port, entry, and attribute are optional

Additions to Suite of Profiles

- Added a worksheet for certificates whose subject is a CRL issuer
  - Previous specification assumed CAs were CRL issuers and vice versa

Suite of Profiles

- The following profiles are now defined:
  - BCA-issued certificates
  - BCA-issued CRLs
  - CA (cross certificate)
  - CRL issuer certificate (subject only signs CRLs)
  - end entity signature certificate
  - end entity key management certificate
  - self-signed (root certificate)
  - CRLs (issued by subjects other than the BCA)

Global Changes (all Worksheets), 1st Revision

- Marked extensions as required or optional
- Names
  - DirectoryStrings in DNs point to preamble text
  - Added “dc” attribute in DNs, *except issuer field of FBCA*
- Keys and Signatures
  - Added ECDSA signatures and EC public keys
  - Specification of parameter fields for keys and signatures
- Specified key usage for each certificate class

Specific Changes, 1st Revision

- Clarified requirements for SKI extension in Cross Certificate Profile
  - Must match AKI in certificates/CRLs issued by the subject
- Clarified contents of policy mapping extension in CA Certificates

Global Changes (all Worksheets), 2nd Revision

- URIs
  - URIs point to preamble text
- Added AIA and SIA extensions
  - AIA added to all certificate profiles except self-signed
  - SIA added to all CA certificate profiles except self-signed

Proposal

- PKI-TWG review April draft and discuss the document on the list
- Goal: Reach consensus on the list ASAP so NIST can request formal FPKIPA recognition of the new certificate and CRL profile