Updating the FPKI Certificate Profile

Tim Polk

David Cooper

March 14, 2002

Background

- FPKI Certificate profile
  - Perhaps the most enduring PKI-TWG product
    - Dates to at least January, 1997 (TWG 97-04 FPKI Certificate Profile Tables)
    - Numerous successive versions
- Current certificate profile is TWG 00-18
  - Draft from 18 April 2000
  - Based upon RFC 2459

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, I

- Based on “Son-Of-2459” rather than RFC 2459
  - Enhanced path validation algorithm
  - Numerous minor clarifications

Preamble Modifications, II

- Added a new section on encoding DNs
  - Discusses use of UTF8String as mandated by PKIX
  - Rules encourage consistent processing by legacy implementations
  - Affects name chaining, name constraints, CRL and issuing distribution points

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

Added CRL Issuer to Suite of Profiles

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

Global Changes (all Worksheets)

- Clarified whether extensions are required or optional
- Modified all fields of type DirectoryString in DNs to point to preamble text
- Added support for “dc” attribute in DNs
  - *Not required for issuer field of FBCA*
- Added support for ECDSA signatures and EC public keys

Global Changes, II

- Clarified specification of parameter fields for RSA, Diffie-Hellman, DSA, and elliptic curve keys
- Clarified specification of parameter fields for RSA, DSA, and ECDSA signatures

Global Changes, III

- Clarified acceptable values in key usage extensions for each certificate class
  - For example, CA Signature Certificates MUST include keyCertSign and MAY include cRLSign

Specific Changes

- 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 Signature Certificate

Proposal

- PKI-TWG review TWG 02-04 and discuss the document on the list
- Goal: Reach consensus by first week of April so that FPKIPA can formally accept new certificate and CRL profile