5280 Implementation Report

November 10, 2009

Tim Polk for David Cooper

Preamble

- Credit where due
  - David Cooper did all the work
  - Any mistakes on slides are mine
    - just in time slides not available for prior review!

- Implementation Report
  - conforming to RFC 5667 (Part of BCP 9)
- Advance 5280 to Draft Standard
  - Already cycled at PS twice!

Methodology

- Certificate & CRL generation
  - Public data collection
  - Laboratory data generation
- Path validation
  - PKITS test suite
  - Supplemental test development

Certificate & CRL Generation, 1

- Primary source was signed S/MIME messages sent to the PKIX and S/MIME mail lists
    - America Online, Ascertia, Dartmouth College, EdelWeb, Entrust, Izecom, Microsoft, MITRE, TC TrustCenter, Thawte, the U.S. Department of Defense, and VeriSign
    - at least five different CA products were used to issue these certificates: Entrust, Microsoft, Red Hat, RSA, and VeriSign
- This set covered most features
    - Primary omissions were delta CRLs and generalized time (e.g., after 2049)

Certificate & CRL Generation, 2

- Supplemental certificates & CRLs generated to cover remaining features
  - Delta CRLs
    - Used EJCBA and OpenSSL
  - Generalized time
    - Used Network Security Services (NSS) and OpenSSL

Path Validation

- Past work at NIST had already verified most features
  - PKITS Test Suite has over 200 tests
  - Five products were tested by USG back in 2005 and 2006
- New tests generated to cover omissions in PKITS and tests executed against a variety of PKI client implementations
  - For most of these tests, Network Security Services (NSS), via either Mozilla Thunderbird or Mozilla Firefox, and OpenSSL were used. However, for a few tests either Safari or the Certificate Management Library was used as the second implementation of the feature.

Exceptions

- processing rules for internationalized names
- User notice certificate policy qualifiers encoded in VisibleString
  - Conforms with 2459 and 3280, but not 5280

Proposal

- Initiate process to advance 5280 to Draft without a new draft
- After IETF LC, issue a -00 draft that
  - Permits VisibleString in user notice
  - Incorporates errata
- IESG Evaluation