PKI Components to Support HSPD-12: FPKIA Directory Ops and Certificate Publishing

PKI Implementation Workshop
April 10, 2006

James L. Fisher, Ph.D.
Andrew Lins

Overview

- Purpose of FPKIA Directory
- FPKIA Directory Communication Mechanisms
- Prototype Directory
- Miscellaneous

FPKIA Directory Infrastructure

- Purpose:
  - Provide a “one-stop shop” retrieval mechanism for all certificates and CRLs necessary to perform FPKIA path discovery and validation
- Why this capability is needed:
  - Not all certificates have correctly populated Authority Information Access (AIA) and Subject Information Access (SIA) fields
  - Some products utilize DN-only formatted fields
    - Some can query only one directory, rather than “chasing down” the certificate path from multiple directories

FPKIA Directory Infrastructure Communications

- Please use a NTP daemon
- Directory access methods
  - Open access to LDAP service on port 389; anonymous bind
  - Open access to HTTP service on port 80
  - Restricted access to X.500 DAP/DSP service on port 102; anonymous bind
    - Restricted to organizations issued cross-certificates, and also those needing DAP/DSP access
- Information retrieval mechanisms/services
  - X.500 directory chaining
  - LDAP directory “chaining”
  - Both types of chaining normally provide direct retrieval, but will return referrals after connection timeout (of 100 seconds)

FPKIA Directory Infrastructure Communications (Continued)

- Information in directories (required):
  - All `cACertificate` (`;binary` depends on directory)
  - All `crossCertificatePair`
  - All current `certificateRevocationList` and `certificateRevocationList`
- Information in directories (optional at agencies):
  - `userCertificate`
    - End-entity signature certificates
    - End-entity encryption certificates
- Information via HTTP (none required)—for FPKIA dir only:
  - CRLs
  - Bundles of cross-certificates in .p7c format
  - In future, may support HTTPS
- Revocation information via OCSP
  - Mechanism required in HSPD-12 follow-on docs
  - Currently planned for FPKIA future

FPKIA Directory Information

- CRLs
  - RFC3280 §3.3 “Revocation”:
    - “An entry MUST NOT be removed from the CRL until it appears on one regularly scheduled CRL issued beyond the revoked certificate's validity period.”
  - Is everybody archiving? (Probably non-LDAP archives.)
- End-entity certificates
  - FIPS 201-1 §5.4.5.1 “Certificate and CRL Distribution”:
    - “PIV Authentication certificates contain the FASC-N in the subject alternative name extension; hence, these certificates shall **not** be distributed publicly via LDAP or HTTP. Individual departments and agencies can decide whether other user certificates (digital signature and key management) can be distributed via LDAP.”

Prototype Directory Infrastructure

- All cross-certified organizations are required to maintain a mirror of their directory structure for…
- Purpose of prototype directory infrastructure:
  - Ensure correct cross-certificate formats
  - Test all cross-vendor directory interoperability functionality
  - Test directory patches and upgrades before applying to production systems
  - Provide environment for testing new middleware and applications

Certificates on PIV-2 Cards

- OMB M-05-24 states the mandatory digital certificate "and any optional digital certificates on the identity credential" must originate from:
  - "An agency certification authority cross-certified with the Federal Bridge Certification Authority at medium assurance or higher by December 31, 2005; or"
  - "An approved Shared Service Provider." [per M-05-05]
- Therefore:
  - *If* a legacy (and non-SSP) PKI system has already completed cross-certification* with the FBCA
  - *Then* it may issue certificates onto PIV-2 smartcards
  - *Else* it is NOT permitted to issue PIV-2 certificates

  (* = which includes directory interoperability)

Miscellaneous

- Choice of Trust Anchor:
  - Common Policy root is available as the trust anchor
    - FBCA is explicitly forbidden as trust anchor
  - Agency may choose own trust anchor
    - Must also specify acceptable policy OIDs
    - Pay attention to policy mappings and granularity
- FPKIA CA Certificate Topology:
  - Common Policy (CP) root issues subordinate CA certificates to all Shared Service Provider (SSP) CAs
  - FBCA is for cross-certification with non-SSP entities, e.g., other bridges (HEBCA; SAFE; CertiPath), other PKI hierarchies (ACES; legacy agency CAs)
  - FBCA and CP root are cross-certified:
    - CP → FBCA with policy mappings
    - CP → FBCA explicitly prohibiting mappings
    - FBCA → CP with policy mappings

Miscellaneous (Continued)

- If (non-PIV) legacy PKI support is needed:
  - Must cross-certify with FBCA
  - "If you sign it, they will come"
    - …come to your directory to retrieve CRLs
    - DN-only products will need to be able to retrieve legacy PKI's CRL via the FPKIA directory
  - Must make directory infrastructure publicly accessible