Shared Service Providers

Common Policy, Certificate and CRL Profile, and Repository Profile

David Cooper and Nelson Hastings
January 14, 2004

Background

- Supports OMB Mandate to Buy not Build
- Eliminates CP development cycle
- Eliminates policy mapping
- Simplifies PKI architecture

FICC SSP Working Group Members

- Peter Alterman, HHS/NIH
- Bill Altmire, NSF
- Bo Berlas, GSA
- Dallas Bishoff, VA
- Donna Canode, Treasury
- Tin Cao, DOS
- Fred Catoe, VA
- David Cooper, NIST
- John Cornell, GSA
- Bob Donelson, BLM
- Mike Dunham, Treasury
- Dave Hanko, DOD
- Nelson Hastings, NIST
- Dan Maloney, VA
- Gene C. McDowell, NOAA
- Michelle Moldenhauer, Treasury
- Brant G. Petrick, GSA/FICC
- Tim Polk, NIST
- Judy Spencer, GSA/FICC
- Ted Wentz, DHS TSA-CPO

http://www.cio.gov/ficc/pki.htm

Common Policy Framework: Overview

- Applies to Federal Employees, Affiliates (e.g., guest researchers), & Devices (e.g., servers)
- Three policies at a single level of assurance
  - Two user policies
    - FIPS 140 Level 2 Hardware Cryptomodule (GSC-IS)
    - FIPS 140 Level 1 Software Cryptomodule
  - One device policy (Level 1 Cryptomodule)
- Assurance comparable to FBCA Medium
  - More detailed Identity Proofing requirements
  - Transition strategy to 2048 bit RSA, SHA-256

Identity Proofing of Applicants

- A priori request from management required
- Employees' employment verified through use of "official agency records"
- In-person identity proofing
  - Credentials verified for legitimacy
  - Biometric recorded for non-repudiation
- Trusted Agent may perform proofing
  - RA still verifies credentials

Policy Management

- Common Policy was developed and will be maintained by the FPKI CPWG
- Policy Mapping performed by the CPWG and approved by the FPKI Policy Authority
- Independent compliance audit still required:
  1. Evaluate CPS compliance to Common Policy using CPWG provided *Analysis Matrix*
  2. Evaluate PKI operations compliance to CPS

Algorithms

- RSA
  - 1024 bit acceptable now
  - 2048 bit required for certificates that expire on or after December 31, 2008
- SHA-1 or SHA-256
  - SHA-1 only until 2007
  - SHA-256 only beginning 2009
- Current Federal Profile requires RSA, DSA, or ECDSA with SHA-1
  - Will need to incorporate transition other hash algorithms (SHA-256, SHA-384, SHA-512)

Directory strings

- Common Policy mandates PrintableString. Allows UTF8String for common name of human subscribers.
- Federal Profile currently requires UTF8String for all new CAs (based on RFC 3280).
  - Will need to allow for use of PrintableString in more circumstances.

CRLs

- CRLs may be complete or segmented based on:
  - Distribution point name
  - onlyContainsCACerts
  - onlyContainsUserCerts
- No segmentation based on reason code or indirect CRLs
- Delta-CRLs and OCSP are optional, but may not be used to meet issuance requirements.

Distribution Points

- All certificates include CDP extension with:
  - LDAP URI
  - HTTP URI
- CDP may include directoryString as well.
- LDAP URIs must include DNS name, directory entry, attribute(s), and “;binary” (if necessary)

AIA and SIA

- All certificates (except self-signed) include AIA
- All CA certificates include SIA
- AIA extensions include both LDAP and HTTP URIs for id-ad-caIssuers access method.
- SIA extensions include both LDAP and HTTP URIs for id-ad-caRepository access method
- AIA should include id-ad-ocsp access method if OCSP supported.

Other restrictions

- Name constraints only on directoryStrings
  - Federal Profile also allows rfc822Name and dNSName
- No policy qualifiers in certificatePolicies
  - Federal Profile allows user notice and CPS pointer
- No policy constraints

General Repository Requirements

- The repository service shall
  - contain all the provider's Certificate Authority (CA) certificates except for self-signed certificates
  - contain all Certificate Revocation Lists (CRLs) issued by all the provider's CA(s)
- Requirements specified in the Common Policy

Repository Access Requirements

- The repository service shall provide at minimum
  - a Lightweight Directory Access Protocol (LDAP) interface at the port 389, supporting both LDAP versions 2 and 3
  - a Hyper Text Transmission Protocol (HTTP) version 1.1 interface at the port 80
- The repository service shall allow unauthenticated access by the public to the information (CA certificates and CRLs)

Repository LDAP Requirements

- The following requirements are drawn from the Federal Directory Profile, RFC 2587, and X.509
- Distinguished Names for directory entries shall use either
  - Geopolitical Names (c=, o=,ou=,...); or
  - Domain Components (dc=,dc=,...)
- CA entries shall include the *pkiCA* object class with a base object class of least one of the following: *person*, *organizationalPerson*, *inetOrgPerson*, or *organizationalUnit*

Repository LDAP Requirements

- *cACertificate* Attributes
  - Shall include all certificates issued to the provider's CA; including self-issued certificates
- *authorityRevocationList* Attributes
  - Shall include all CRLs issued by the provider's CA containing the Issuing Distribution Point (IDP) extension with *onlyContainsCACerts* set to TRUE
- *certificateRevocationList* Attributes
  - Shall include all CRLs issued by the provider's CA that are not required to be in the *authorityRevocationList* attribute

LDAP Repository Requirements

- *crossCertificatePair* Attributes
  - The issuedToThisCA (forward) elements of the *crossCertificatePair* attribute of a CA's directory entry shall be used to store all, except self-issued certificates issued to the provider's CA.
  - The issuedByThisCA (reverse) elements of the *crossCertificatePair* attribute, of a CA's directory entry shall contain all certificates issued by the provider's CA to other CAs.
  - When both elements are present in a single attribute value,
    - Issuer name in one certificate shall match the subject name in the other and vice versa, and
    - The subject public key in one certificate shall be capable of verifying the digital signature on the other certificate and vice versa.

Repository HTTP Requirements

- The following requirements are drawn from RFC 2633
- CRLs issued by the provider's CA shall be DER encoded and stored in files with .crl extensions
- The provider's CA certificates shall be stored as degenerate *signedData* "certs-only" messages in files with .p7c extensions

Repository Performance Requirements

- The following requirements are drawn from the DoD’s Global Directory Service Requirements
- The scheduled downtime for the repository service shall not exceed .05%
- The repository shall provide an average three second response time from the time the repository receives the request until it delivers the response to the network