Certificate Profiles for FIPS 201

David A. Cooper
NIST

April 10, 2006

Overview

- Certificate profiles for PIV specific certificates are included in:
  - *X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program*
- Profiles in this document are based on:
  - *Federal Public Key Infrastructure (PKI) X.509 Certificate and CRL Extensions Profile*
  - FIPS 201: *Personal Identity Verification (PIV) of Federal Employees and Contractors*
  - SP 800-78: *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*
  - *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework*
  - *Shared Service Provider Repository Service Requirements*

Certificate Profiles

- Profile document includes 9 worksheets (or profiles):
  - 3 CA certificate profiles (self-signed, self-issued, and cross-certificate)
  - 1 CRL profile
  - 1 device certificate profile
  - 4 profiles for human subscribers:
    - Digital signature
    - Key management
    - PIV authentication
    - Card authentication

Common Elements

- All profiles share common requirements for:
  - Signature algorithms
  - Public key algorithm
  - Encoding of distinguished names
  - authorityInfoAccess extension
  - subjectInfoAccess extension
  - cRLDistributionPoints extension

Public Key Algorithms

- Requirements from NIST Special Publication 800-78.
- Public keys may be either RSA or elliptic curve.
- Elliptic curve limited to the six curves specified in 800-78.
- 1024 bit RSA keys are allowed, but only 2048 bit keys will be allowed in the near future. 2048 bit RSA required for:
  - CA keys distributed as trust anchors
  - Digital signature and key management keys issued to human subscribers that expire on or after December 31, 2008.
  - Subject public keys in device certificates, Card Authentication certificates, and PIV Authentication certificates that expire on or after December 31, 2010.

Signature Algorithms

- Requirements from NIST Special Publication 800-78.
- Acceptable algorithms include:
  - RSA - PKCS #1 Version 1.5
  - RSA Probabilistic Signature Scheme (RSASSA-PSS)
  - Elliptic Curve Digital Signature Algorithm (ECDSA)
- Hash Algorithms:
  - SHA-1 (only for RSA PKCS #1 v1.5 signatures on certificates and CRLs that expire before December 31, 2010)
  - SHA-224 (ECDSA only)
  - SHA-256

Encoding of distinguished names

- Requirements for subject names specified in Common Certificate Policy
- Many attributes used in distinguished names are of type DirectoryString: organization (o), organizational unit (ou), common name (cn).
- Profile mandates the use of PrintableString encoding for all attributes that use DirectoryString except common name.
- Common Names may be encoded in UTF8String instead of PrintableString only if subject's name cannot be represented in PrintableString.

AIA, SIA, and CDP extensions

- authorityInfoAccess (id-ad-caIssuers) and cRLDistributionPoints must be included in all certificates except self-signed certificates.
- subjectInfoAccess (id-ad-caRepository) must be included in all CA certificates.
- Must include both HTTP and LDAP URIs

PIV Specific Requirements

- Both PIV Authentication and Card Authentication certificates:
  - Certificate status must be provided via OCSP in addition to CRLs.
    - AIA extension must point to OCSP server via HTTP URI.
  - Must include FASC-N in the subjectAltName extension.
  - Must not set the nonRepudiation bit (only digitalSignature).
  - Must include a piv-interim extension that indicates whether certificate subject's NACI was complete at time of certificate issuance.

Card Authentication Certificates

- Must include critical extended key usage that asserts id-PIV-cardAuth.
- Must not include any names other than the FASC-N (but FASC-N may appear in subject field in addition to subjectAltName).

CHUID and Biometric Signer's Certificate

- Must include extended key usage extension with id-PIV-content-signing.
- May be either digital signature (human subscriber) or device certificate.

Other Certificate Requirements

- Some applications impose requirements on certificate profiles:
  - Microsoft Smart Card Logon:
    - subjectAltName must include user principal name (UPN)
    - Extended key usage must specify Microsoft Smart Card Logon OID
  - A Kerberos Key Distribution Center (KDC) using public key cryptography for initial authentication may require the certificate to include:
    - KRB5PrincipalName in subjectAltName
    - id-pkinit-KPClientAuth in extended key usage
  - Subject field is optional in PIV Authentication Certificates, but many applications require it to be present.

Other Certificate Requirements

- S/MIME
  - Digital Signature and Key Management certificates should include email address in subjectAltName extension to support signing and encrypting email.