Certificates and FIPS 201

Tim Polk

March 3, 2006

X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program **[February 6, 2006]**

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

Common Certificate & CRL Profile

- Updated February 2006
  - Added FIPS 201 specific certificate profiles
    - PIV Authentication certificate
    - Card Authentication certificate
  - Enhanced Signature Certificate profile to identify PIV Content Signers

What's different?

- Departs from current best practice to meet new requirements
  - Different public keys
  - New signature options
  - Larger certificates
  - FASC-N
  - Extended key usage extension
  - Multiple status mechanisms
  - PIV interim extension

Different public keys

- Bigger RSA keys
  - 2048 and 3072 bit keys
- ECC keys for 224 - 283 bit curves

New signature options

- ECDSA signatures
- SHA-224 and SHA-256
- PSS padding

Larger Certificates

- Certificate size is dominated by the public key and the signature
  - 3072 bit keys means a larger maximum certificate size
- Multiple URLs for status mechanisms can add size if URLs are too long

FASC-N

- The FASC-N is encoded as an additional name in the certificate to link the physical and logical credentials

Extended key usage

- This extension is required to differentiate the card authentication key from the PIV authentication key

Status Mechanisms

- Certificates include http and ldap pointers to CRLs
- PIV and card authentication certificates include pointer to OCSP server

PIV Interim Extension

- New, private extension required to indicate investigation status
  - Noncritcal extension
  - Specifies whether a NACI is completed at the time of certificate issuance

X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program **[February 6, 2006]**

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