FIPS 201 Cryptography and PKI

Tim Polk

May 26, 2005

Cryptographic Requirements Overview

- FIPS 201 relies on cryptography
  - To protect objects stored on the PIV card
  - To authenticate the PIV card or cardholder
  - To authenticate the source and integrity of status information
- The details are in SP 800-78

Cryptographic Strength Requirements

- SP 800-78 mandates a transition from 80 bit strength to 112 bits of strength by 1/1/2011
  - Cryptographic keys that provide long term data protection transition by 1/1/2009 to provide two years “forward security”
- Elliptic Curve Cryptography is specified with a minimum of 112 bits of strength (224 bit keys)
  - Avoid transition issues

NIST
National Institute of Standards and Technology

Cryptographic Objects Stored on the PIV Card

- FIPS 201 specified
  - Cryptographic keys
  - Digitally signed objects
    - CHUID
    - Biometrics
    - X.509 Certificates
- SP 800-073 specified
  - Authentication/Integrity Object

Cryptographic keys

- Asymmetric private keys
  - PIV Authentication key (Mandatory)
  - Digital Signature key (Optional)
  - Key Management key (Optional)
    - May support key transport or key agreement
- Card Management Key (Optional)
  - Symmetric key
- PIV Card Authentication Key (Optional)
  - May be symmetric or asymmetric

Asymmetric Algorithms for Cryptographic Keys

- SP 800-78 limits asymmetric keys to RSA and ECC
  - RSA must be 1024/2048/3072
    - 1024 bit keys phased out by 1/1/2011
    - Digital signature and key management keys transition by 1/1/2008 to provide for forward security
    - Authentication keys transition by 1/1/2011 since forward security is not an issue
  - ECC must use a recommended curve from FIPS 186-2
    - 224 through 283 bit keys
    - No phase out specified

X.509 Certificates for Asymmetric Keys, I

- PIV Authentication and Card Authentication certificates
  - Subject name is omitted
  - OtherName contains FASC-N
  - May not be stored in public directories!
  - OCSP and CRL based status distribution mandatory

X.509 Certificates for Asymmetric Keys, I

- PIV Authentication and Card Authentication certificates
  - Assert *CommonAuth* certificate policy
  - KeyUsage asserts digitalSignature but not nonRepudiation
- Card Authentication certificates
  - Mandatory extended key usage signals cryptographic operations performed without cardholder authentication

X.509 Certificates for Asymmetric Keys, III

- PIV Signature and Key Mgmt certificates
  - Assert the *commonHW* certificate policy
  - Subject name is present
  - FASC-N is omitted
  - Optionally stored in public directories
  - CRL based status information mandatory
- PIV Signature Certificate
  - KeyUsage asserts both digitalSignature and nonRepudiation

Symmetric Algorithms for Cryptographic Keys

- SP 800-78 limits symmetric keys to Triple DES (TDEA) and AES
  - TDEA must be two key or three key
    - Two key TDEA phased out by 1/1/2011
  - AES may be 128, 192, or 256 bit keys
    - No phase out specified

NIST
National Institute of Standards and Technology

Digitally Signed Objects

- Signatures may be generated using RSA or ECDSA
  - RSA may use PKCS #1 or PSS padding schemes
  - SHA-1, SHA-224, and SHA-256 hash algorithms
    - SHA-1 phased out by 1/1/2011
- Phase out depends on card *expiration*, not signature generation date

NIST
National Institute of Standards and Technology

SP 800-73 Security Object

- ICAO Authentication/Integrity Object
- Digitally signed hash table
  - The table includes a message digest for each of the objects (CHUID, keys, etc.) stored on the card
  - Message digests are generated using SHA-1, SHA-224, or SHA-256
    - SHA-1 phased out by 1/1/2011
  - Signature requirements from previous slide

NIST
National Institute of Standards and Technology

Status Information

- FIPS 201 relies upon digitally signed X.509 CRLs and OCSP responses to distribute status information
- Signatures may be generated using RSA or ECDSA
  - RSA may use PKCS #1 or PSS padding schemes
  - SHA-1, SHA-224, and SHA-256 hash algorithms
    - SHA-1 phased out by 1/1/2011
- Phase out depends on signature *generation* date

NIST
National Institute of Standards and Technology

OCSP and FIPS 201

- OCSP
  - mandatory for status of PIV Authentication Key and Card Authentication Key (if present)
  - Optional for Signature and Key Management Key
- Outstanding comment
  - OCSP service requirements are underspecified
    - Are nonces required?

NIST National Institute of Standards and Technology

Summary: Certificates

- X.509 certificates to support FIPS 201 conform to standard FPKI profiles but
  - Use of the otherName field in the subject alternative name extension to specify the FASC-N
  - Use the extended key usage extension to differentiate the Card Authentication key
  - Rely on the AIA and SIA extension for path building and to locate status information

Summary: Algorithms

- RSA and SHA transition strategies from Common Policy are specified in SP 800-78
  - Move to 2048 bits RSA (or comparable) and SHA-256 is mandated
  - PSS padding for RSA signatures specified
- ECC is a transition strategy, but limited to six of the NIST Approved curves from FIPS 186-3
- 2 key TDEA phased out in 2010

Summary: Architecture

- OCSP is required to distribute status for authentication keys
- CRLs are required to distribute status for all certificates
- LDAP and HTTP are required to distribute CA certificates and CRLs