Cryptography and FIPS 201

Donna F Dodson

donna.dodson@nist.gov

301 975 3669

NIST
National Institute of Standards and Technology

FIPS 201 Cryptographic Specifications

- Cryptographic key(s)
  - One **mandatory** PIV asymmetric authentication key
    - May be used to sign an externally generated hash
  - Optional symmetric and asymmetric keys
    - Symmetric key for challenge response protocols
    - Asymmetric keys for digital signatures and key management
    - Symmetric key for card management
- Digital signatures on logical credentials
  - CHUID, X.509 certificates, biometrics, the SP800-73 Security object

Cryptographic Keys

- On-card key generation for PIV authentication keys and optional digital signature keys
  - *RSA or elliptic curve key pairs*
- Import symmetric authentication and card management keys
  - *Triple DES or AES*
- Import or generate asymmetric key management keys
  - *RSA or elliptic curve key pairs*
- All private/secret key computations on-card
- Message hashing off-card

PIV Key Type	Time Period for Use	Algorithms and Key Sizes
PIV Authentication key	Through 12/31/2010	RSA (1024, 2048, or 3072 bits) ECDSA (Recommended Curves, 224 – 283 bits)
	After 12/31/2010	RSA (2048 or 3072 bits) ECDSA (Recommended Curves, 224 – 283 bits)
Card Authentication key	Through 12/31/2010	2TDEA 3TDEA AES-128, AES-192, and AES-256 RSA (1024, 2048, or 3072 bits) ECDSA (Recommended Curves, 224 – 283 bits)
	After 12/31/2010	3TDEA AES-128, AES-192, and AES-256 RSA (2048 or 3072 bits) ECDSA (Recommended Curves, 224 – 283 bits)
Digital Signature key	Through 12/31/2008	RSA (1024, 2048, or 3072 bits) ECDSA (Recommended Curves, 244 – 283 bits)
	After 12/31/2008	RSA (2048 or 3072 bits) ECDSA (Recommended Curves, 224 – 283 bits)
Key Management key	Through 12/31/2008	RSA key transport (1024, 2048, or 3072 bits) ECDH or ECC MQV (Recommended Curves, 224 – 283 bits)
	After 12/31/2008	RSA key transport (2048 or 3072 bits); ECDH or ECC MQV (Recommended Curves, 224 – 283 bits)

Digitally Signed Credentials

- CHUID and biometrics employ CMS external detached signature
- X.509 Certificate signature formats as specified in RFC 3279

Card or Certificate Expiration Date	Public Key Algorithms and Key Sizes	Hash Algorithms	Padding Scheme
Through 12/31/2010	RSA (1024, 2048, or 3072 bits)	SHA-1 or SHA-256	PKCS #1 v1.5, PSS
	ECDSA (Recommended Curves, 224 – 283 bits)	SHA-1, SHA-224 or SHA-256	N/A
After 12/31/2010	RSA (2048 or 3072 bits)	SHA-256	PKCS #1 v1.5, PSS
	ECDSA (Recommended Curves, 224 – 283 bits)	SHA-1, SHA-224 or SHA-256	N/A

NIST
National Institute of Standards and Technology

X.509 Certificates

- PIV Authentication Certificate
  - keyUsage asserts digitalSignature but NOT nonrepudiation
  - Certificate includes FASC-N from CHUID in altSubjectName and PIV NACI indicator
- Digital Signature and Key Management certificates

Hash Algorithm Requirements for the 800-73 Security Object

- SHA-1, SHA-224 or SHA-256 through 12/31/2010
- SHA-224 or SHA-256 after 12/31/2010

Moving Forward: A Migration Strategy

- Algorithm changes after 2010
- Need CAs to support multiple algorithms and different key sizes
- Need to consider computational power of smart card
  - Crypto co-processor?
  - JAVA implementation
- Infrastructure support for multiple algorithms

Selecting solutions

- Flexibility
- Scalability
- Interoperability

Infrastructure

- Middleware
- Operating Systems
- Security Protocols
- Applications