Cryptography in FIPS 201

• Digital signatures on logical credentials
  o CHUID, X.509 certificates, biometrics

• Cryptographic key(s)
  o One mandatory PIV asymmetric authentication key
    • May be used to sign an externally provided hash
  o Optional symmetric and asymmetric keys
    • Symmetric or asymmetric key for challenge response protocols
    • Asymmetric keys for digital signatures and key management
    • Symmetric key for card management
Digitally Signed Credentials

- CHUID and biometrics employ CMS external detached signature
- X.509 Certificate signature formats as specified in RFC 3279
  - 1024 or 2048-bit RSA/160 or 224-bit elliptic curves
  - For RSA: SHA-1 or SHA-256 hash
  - For ECDSA: SHA-1 or SHA-224 hash
X.509 Certificates

• PIV Authentication Certificate
  o keyUsage asserts digitalSignature but NOT nonrepudiation
  o Certificate includes FASC-N from CHUID in altSubjectName

• Digital signature and Key management certificates

• Asymmetric challenge-response key
Cryptographic Keys

- On-card key generation for PIV authentication keys and optional digital signature key pair
  - 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
## Key Sizes

- Key sizes transition in 2008 and 2010

<table>
<thead>
<tr>
<th>Initial Key Sizes</th>
<th>Key Sizes after 2008/2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two and Three Key Triple DES</td>
<td>Three Key Triple DES</td>
</tr>
<tr>
<td>AES-128, AES-192, and AES-256</td>
<td>AES-128, AES-192, and AES-256</td>
</tr>
<tr>
<td>1024 and 2048 bit RSA</td>
<td>2048 bit RSA</td>
</tr>
<tr>
<td>160 and 224 bit elliptic curve</td>
<td>224 bit elliptic curve</td>
</tr>
<tr>
<td>SHA-1, SHA-224 and SHA-256 hash</td>
<td>SHA-224 and SHA-256 hash</td>
</tr>
</tbody>
</table>
Cryptographic Operations

- Initially permits 80-bit or stronger cryptography
  - On card
    - Two and Three Key Triple DES
    - AES-128, AES-192, and AES-256
    - 1024 and 2048 bit RSA
    - 160 and 224 bit elliptic curve
  - Off card
    - SHA-1, SHA-224 and SHA-256 hash
FIPS 140 validation required for all cryptographic operations

- Level 3 Physical Security
- Level 3 Operator Authentication
- Level 2 Overall
Open Issues

- Contactless asymmetric cryptography
- Primes Testing for RSA
- Random Number Generation
Contactless Cryptography

• Efficiency
  o Will the electrical power available to the card be sufficient to implement a cryptographic challenge-response protocol?
  o Will the time required at the gate exceed human patience?
Primes Testing for RSA

- Tests for prime numbers are specified in FIPS 186-2, X9.31, X9.80
- Is X9.31 primes testing practical for PIV cards?
  - What performance numbers can be achieved for generation of 2048 bit keys?
Random Number Generation

- NIST is developing new standards for random number generation within ANSI
  - Target delivery late 2005
  - Will impact CMVP validation requirements
- Sources of randomness for PIV cards?
  - On-card hardware RNG
  - Vendor installed seed with PRNG
- Vendor installed seed precludes non-repudiation!