PIV Test Cards: Project Goals and Design

Tim Polk
NIST/ITL/CSD
August 25, 2010

Disclaimer

- This project is in its infancy
  - Lots of decisions are yet to be made
  - Decisions made to date are subject to change

That is Why I'm Here!

- To alert agencies and industry to our plans
- To obtain feedback on whether our plans meet the needs of application developers, and
- To get this information before it is too late to be useful

Project Goals

- Accelerate integration and development of PIV-based PKI applications
- Permit testing of revoked/expired/etc. cards
- Promote cryptographic agility
- Support testing of corner cases
- Accelerate support for PIV features
- Ensure independence of any manufacturer-specific features

Consequences

- Demands a “live” infrastructure to support status checking
- Requires a small stack of cards representing all the approved PIV vendors
- Cards include CHUID, fingerprints, and facial image for completeness
  - One card omits fingerprints
  - Note that testing of fingerprints and facial image equipment is out of scope

High level Design

- Set of about 20 test cards
  - A set of “plain vanilla” cards representing the set of approved manufacturers that are valid and don’t push the envelope in features
  - Approximately fifteen additional cards that include all approved cryptographic algorithms, PKI-relevant optional features (e.g., key history), and the various card and certificate status cases

Card Set: Cryptographic Algorithms

- Cryptographic algorithms
  - RSA Signatures generated with
    - 2048 and 3072 bit keys
    - PKCS #1 and PSS padding
    - SHA-1 and SHA-256 hash algorithms
  - ECDSA Signatures with {P-256 and SHA-256} and {P-384 and SHA-384}
  - PIV User keys
    - 1024 and 2048 bit RSA keys
    - P-256 and P-384 ECC keys

Card Set: Optional Features

- Key History
  - Consistent and mixed algorithms
  - With and without certificates on card
- Discovery Object
  - Absent
  - Present with {no Global PIN, Global is primary; Global is secondary}

Card Set: Status Checking and Corner Cases

- PIV Certificates and Card expired
- PIV Certificates expired, card unexpired
- PIV Certificates revoked
- PIV Content Signer revoked
- FASC-N mismatch (CHUID vs. PIV auth)
- Forged card (Invalid signature on certificates and CHUID)

Infrastructure, I

- All card sets share the same issuers and serial numbers
  - Only differences are in authentication and digital signature public keys and the signatures on the corresponding certificates
- Status information is static
  - No matter how many card sets are generated, the CRL contents do not change

Infrastructure, II

- PKI hierarchy
- LDAP and HTTP for retrieval of CA certificates, and CRLs
  - May need multiple DNS names and perhaps multiple IP addresses
- OCSP server
  - Status information for all end entity certificates
- HTTP retrieval of retired user keys

Status

- NIST contractor is currently reviewing our tool set for completeness
  - ECC, key history, and discovery object are known shortfalls
  - Current tools perform live capture for biometrics
- Beta test card sets without key history, etc. for internal testing early FY11

Many Unknowns, Many Dependencies

- Initial availability date for official test card set?
- Cost for Test Card Set?
- Source for white stock? ECC white stock?
- Is on card key gen enforced by the PIV card or the card management system?
- Contract vehicle to create and verify test sets?
- Vehicle to distribute test sets?
  - NIST Standard Reference Material Program?
- Assignment of operational responsibilities for infrastructure?
  - NIST CSD?
  - OCSP services?
- Is a Support Desk required?

Questions?