Overview/Case Study

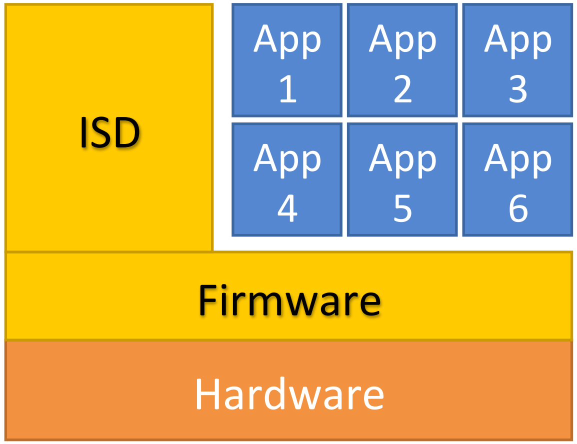
Validating FIPS 140-2 Security in PIV Credential Cryptographic Modules

PIV – Personal Identity Verification

- A means to establish a "Trusted Identity"
  - issued based on sound criteria for verifying an individual employee's identity
  - strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation
  - rapidly authenticated electronically
- Common Federal Identity badging and proofing
- Credentials issued on Smart Cards

Smart card 101

- Plastic card with one or more chips
- For RF communications an antenna is included
- Contact based connections through a standard pad layout
- Printable surface for badging
- Internal logical design of Hardware, Firmware and Software



ISD

App 1

App 2

App 3

App 4

App 5

App 6

Firmware

Hardware

Certification Types

- CAVP - Cryptographic Algorithm Validation Program
  - Cryptographic algorithm testing
- CMVP - Cryptographic Module Validation Program
  - FIPS 140 module testing
- NPIVP - NIST's Personal identity verification program
  - Conforms to FIPS 201 card edge
- GSA - General Services Administration
  - Total card conforms to FIPS 201 specifications

FIPS 140 certification areas

- Hardware
  - Protection from attacks
  - Tamper resistance
- Firmware
  - Integrity
  - Provides secure services
  - Self tests
- Software
  - Integrity checked
  - Secure and conforms to standard practices

Our differences

- SP800-73-3 compliant with all algorithms
- Dual chip
- One of the first to offer Biometric Match on Card
- Designed to be a true Multiple Application card
  - Multiple Security Domains
  - Applets that provide their own secure channels in Java
- ISO-14443-B RF interface for performance and increased capabilities

Time to allocate to the process

- CAVP – About 2 weeks to a month
  - Create test harness
  - Run vectors – May take multiple cards and a significant amount of time
  - Approval process
- CMVP – 3 – 6 months (can vary greatly)
- NPIVP – a couple weeks over all working with the Lab
- GSA – Depends on many factors – 2 months or more for all levels

Lessons Learned

- Read the specifications
    - I say again, read the specifications
- The boundary matters
- Dual Chip issues
- Smart card OS vendor support
- Standards – Must be followed by all
- PIV stopped a little short – Management functions missing
- POST tests are painful
- The Testing Lab MATTERS

Lessons Learned…

- Issues when implementing more than the minimum
    - POST self tests in applet startup
    - Larger set of algorithms
        - POST testing performance impact
        - More CAVP tests to perform
    - More to document and to review
- Exact wording in the Security Policy and supporting docs matters