

2007: Deployment

- The FIPS 201 Standard Suite is complete
- The Approved Products List is growing
- Issuance has begun

Agencies: how do you plan to benefit from PIV Card deployment?

Companies: what applications will you PIV-enable next?

NIST PIV Strategy in 2007

1. Respond to critical urgencies as they arise.
2. Provide application examples & advice.
3. Complete revisions already committed.
 - SP800-76-1 editorial improvements
 - SP800-78-1 and SP800-73-2 changes
 - SP800-104 (color coding)—it's *optional*
4. Technology transfer beyond HSPD-12.
5. Begin work towards PIV step-up.

Application Examples

- Card and Middleware Reference Implementation
 - Updated now to SP800-73-1; will track SP800-73-2
- Windows Logon
 - Demo CSP source code
- Linux Login, SSL/TLS, and S/MIME
 - Demo PKCS #11 module source code
- PACS examples next?
- Whole disk encryption?

Revisions Already Committed

- SP800-78-1 (crypto) publication imminent.
- SP800-73-2 (card technology) goals:
 - Implement -78-1 requirements
 - Add crypto discovery mechanism.
 - Repackage -73-1 in four modules (editorial)
 - Data Model, End-point, Transition, Middleware
 - Incorporate all errata.

Technology Transfer

- Modularize SP800-73-2 to promote reuse.
- With TSA & TWIC, develop “biometric authentication over contactless”
- With NCR & FRAC, develop “skills & qualifications representation”
- Note: new card-applications, coexisting with PIV card-application, are likely (i.e., no PIV standard changes soon).

Card Personalization Product

Testing – On going support to GSA

- Already Provided:
 - A new Test Results Report based on GSA's Approval Criteria (in addition to test assertions)
 - Challenge-Response tests based on RSA 2048
 - Additional internal consistency tests for Digital Signature Block
- In the pipe-line:
 - Testing of ECC algorithms on the Card
 - More diagnostic messages for non-conformance scenarios.

Data Model Tester – (SP 800-85B Tool Availability

- Made available based on Agency Request
 - One installation done at FAA
- Going to be made available to the public
 - Password protected Zip file to be posted on NIST website this week.
 - Will also contain installation and configuration instructions.
 - Agencies, Vendors and System Integrators can obtain the password by sending an email request to NIST contact.