Public Key Infrastructure (PKI) Deployment & HSPD-12 Compliance

Sally Caldwell
PKI Program Manager

Deployment Status

- State Department stands a good chance of meeting HSPD-12 requirements
  - This is possible—worldwide—because:
    - State was an early adopter of three key technologies
    - Benefited from early buy-in by senior management and a coordinated effort by Diplomatic Security (DS) and IT

Going In…

- State's PKI has always been associated with a smart ID card for both physical and logical access control
  - DS Bureau recognized that legacy security badge system needed replacing
  - IRM Bureau was looking for a FIPS 140-compliant smart card as a PKI token
  - Bureaus formed a working group recognized by the Under Secretary for Management

Background

- Settled on one smart card in 2002 based on business case, operating environment, and worldwide security concerns using best available information at that time
  - Smart card/PKI/biometric vendors cooperative and supportive
  - Able to leverage current smart card layout as the logical access container on PIV card
  - PKI issuance collocated with badging offices
- Current smart card used for both physical access control (PIN at turnstile) – and logical access control (biometric/PKI) – where implemented
- Fielding for physical access control domestically, domestic and overseas logical access control still in-progress

Smart Card Deployment

- DS Bureau targeting HSPD-12 physical access
  - DS and IRM Bureaus cooperated on domestic Smart ID Card
  - Badging stations in place overseas for Global ID card
  - DS was already doing required identity proofing and security checks on most personnel
  - Planning for PIV transition on-going since September 2004; only tweaks required to the process

Our Progress

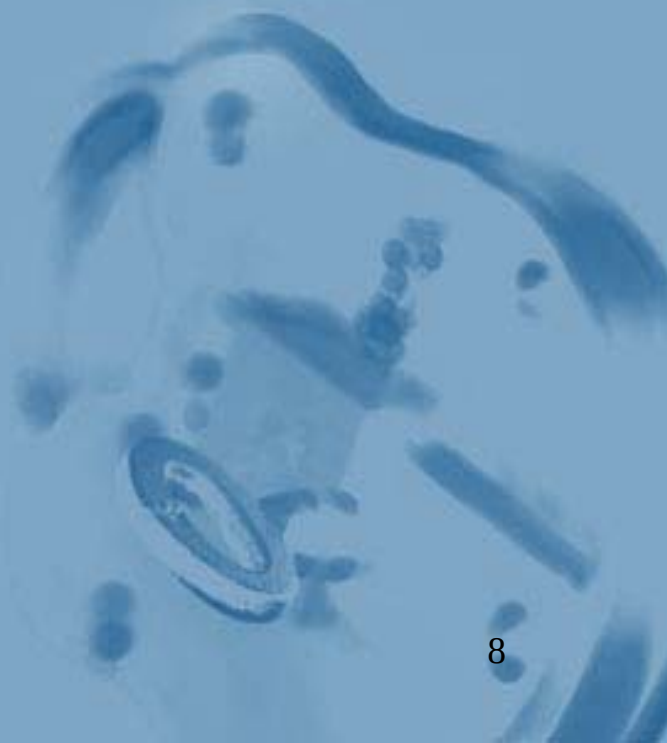
- An operational PKI for nearly five years
- Cross-certified with Federal Bridge at High Assurance level since early 2004
- Internal PKI Projects, beginning in 2002, include:
  - Digital signature/privacy encryption for e-mail, forms and other applications
  - Secure authentication leading to single sign-on
  - Secure Web application and applet code signing
  - Logon using smart card PKI/Biometric token replacing User ID/password

Additional Projects

- Additional PKI Projects in operation:
  - Machine Readable Travel Document (MRTD), a.k.a. ePassport in conjunction with CA Bureau to digitally sign identity information on passport
  - eAuthentication initiatives
  - Remote access/teleworking
  - Support for joint applications with other agencies (e.g., IVAMS, IPCA, ATS)

Overall Deployment

- Extensive deployment domestically
- About half of overseas diplomatic posts



BLADE

- Initiated Biometric Logical Access control pilot with PKI in mid-2003
  - Selected match-on-card vice client-server solution
    - Met business case and operating environment requirements for speed, privacy, and security
  - Chose fingerprint as biometric based on internal DoS testing and security requirements

More BLADE

- Selected hybrid minutiae points-pattern matching template rather than image for security and privacy concerns
  - NIST SP 800-76 calls for minutiae template with interoperable header information
  - State will incorporate such templates for physical access
  - Current BLADE program will be retained for logical access control
  - Will add interoperable header data (vice proprietary header) in near future

What BLADE Gets Us

- PKI/BLADE features interaction of PKI and biometrics, in a match-on-card solution, for mutual security
- Provides minimum two-factor authentication and will support three-factor as needed
- Increased user acceptance

Status

- Early adoption has provided experience and time to comply with federal mandates
- Benefited from senior management buy-in and reasonably steady, funding since beginning
- Joint effort by Bureau responsible for physical & personnel security and Bureau responsible for IT
- Both bureaus have assembled very good policy and technical teams; leading the Department effort that now includes HR, Administration (privacy), and other Bureaus
- Have procured PKI hardware/software to establish PIV Certificate Authority; awaiting FPKIPA policy updates to finalize decisions on how to architect

Problems and Risks

- Risks are the same as everyone's:
  - Will validated products (smart cards) be available?
  - Will we have enough time for procurement?
  - Will the PIV card standard enable transition of existing capabilities—representing 4-5 years effort and millions of dollars invested?
  - Time required for internal C&A
  - Unfunded mandate requires leveraging in-house resources

Overseas Deployment Challenges

- Will use “overseas security provisions” of FIPS 201
- Will not issue PIV cards to local employees
- Varying local environments
- Very expensive
- 260 overseas missions with logistical obstacles

Point of Contact

Sally Caldwell
PKI Program
(202) 203-7808
CaldwellSX@state.gov