PIV Life Cycle Management: *Maintaining Assurance and Enhancing Utility*

Tim Polk

October 6, 2005

Security is More Than Technology

- Policies and procedures play a key role in a secure PIV token – just like any other security system
- Things change – the system has to keep pace
  - People retire, change jobs, get fired
  - The environment changes – can the token change with it?

Policies and Procedures

- Policies and procedures must include
  - Token and certificate issuance
  - Token and certificate revocation
  - Notification and changes to token holder attributes
  - Re-authentication and Re-issuance

Implementing Policies and Procedures

- Personnel
  - Personnel in trusted roles must be trustworthy
  - Training
  - Auditing
- Verifying Policies and Procedures
  - Compliance audits
    - Common PKI tool for Policy compliance
    - Approved by FPKI Policy Authority
  - Certification and Accreditation
    - Agency DAA signs off on system

Emergency Notification

- Emergency notification procedures must be established for each agency
- Triggers:
  - Employee or contractor separation
  - Assurance decreased
  - Token lost or compromised

When are emergencies noticed?

- Separation
  - Usually known to government or the employer, but who tells the token issuer and certificate issuer?
- Loss or compromise
  - Do token holders know their responsibilities?

Emergency Response

- Token Revocation
- Token Status Registry Updates
- Certificate Management Issues

Directory Management

- Directory architecture reflects local versus global data
  - If all data is global
    - Then a single publicly accessible directory is sufficient
  - If some data is local, two solutions:
    - Internal and border directories
    - Authenticated access to controlled attributes

OCSP Responder

- Essentially, two configurations:
  - CRL driven
  - CA database driven
- For CRL driven responders, updating the LDAP directory is a complete solution
- Where the CA database drives the OCSP responder, secure connections between CA and OCSP responder are required

So, FIPS 201 Will Establish…

- Policy and procedural requirements to ensure token management and personnel management are tightly coupled
- Policy and mechanism requirements to ensure token status information is accurate and available
- C&A and training requirements to ensure procedures are implemented correctly

Adapting to Environment

- The PIV token needs to be adaptable to reflect changes in environment
  - Every agency is different
  - Every agency evolves
- FIPS 201 will specify a minimum set of functionality
  - Additional functions may be added to meet agency requirements