CYGNACOM
SOLUTIONS

PKI Implementation Workshop 2006

Charles Horowitz
CygnaCom Solutions, Inc – an Entrust company
chorowitz@cygnacom.com

CYGNACOM SOLUTIONS

Agenda

- What is a PKI deployment?
- What makes a deployment successful?
- What complicates a deployment?
- How does HSPD-12 impact deployments?

CYGNACOM SOLUTIONS

What is a PKI deployment?

- PKI infrastructure implementations are well known
  - Security controls, policy and practices
  - High availability and DR
  - Operations and management
- Some areas continue to offer challenges
  - Integration with directory services
  - Snapshot interoperability
- Deployment is
  - Distribution and maintenance of PKI h/w and s/w
  - Implementation of registration and lifecycle model for people and devices/applications
  - Training and help desk for administrators and end users
  - Application enablement?

CYGNACOM SOLUTIONS

Keys to success - Deployment

- Lifecycle management must be user-lite and tech-heavy
- Understand and line up with enterprise refresh and maintenance for software and hardware
  - Automated software distribution is coming into reality
- Manage releases conservatively
- Understand the integration with provisioning systems
  - This may only be the directory, but even that presents challenges
    - Tradeoffs between simplified PKI implementation and deployment and data synchronization demands
- Lots of real-environment testing
- Organizational support for PKI
  - Enterprise help desks
  - ISSOs and systems administrators
  - LRA/TA network

CYGNACOM SOLUTIONS

Keys to success - Applications

- Executive buy-in
  - Not necessary to operate an infrastructure
  - Eases deployment by delivering vision to end users
  - Eases application enablement by establishing policy
- Enterprise planning and architecture
  - Aligning system, integration, and capability with EA planning will result in easier implementation and deployment
  - Get PKI on the radar as an item that application owners will budget and shop for
- Understand your organization's information needs
  - PKI boils down to authentication, data security, or BPR (dig sig)
  - Find applications whose needs are clearly aligned with those offerings
- BPR stakeholders must get involved early
  - Legal, policy, records management, etc have a long ramp-up for PKI
  - Many BPR stakeholders are used to the pace of paper
  - New challenges introduced by PKI that have no paper analogy

CYGNACOM SOLUTIONS

More Keys to Success - Applications

- Deploy, deploy, deploy!
  - Applications don't exist for infrastructures with no customers
  - And customers don't exist for infrastructures with no applications
  - Getting cards, certs, readers, and software in the hands of the user community, whether they want it or not, helps defuse this issue
- Ownerless applications
  - Some applications have no or minimal governance and are prime targets for "grass roots" enablement
  - Don't forget about stakeholders
- Applications already enabled or using PKI
  - COTS products
  - SSL, VPNs, etc
- Proofs of concept and prototypes
  - Seeing is believing and gains thought time
- Applications with external interactions
  - Often higher visibility
  - Often higher drain

CYGNACOM SOLUTIONS

Deployment challenges

- Moving capabilities, environment, and objective targets
- COTS shortcomings for enablement
- Metrics for use
- Card reader funding
- Major applications may be “untouchable”
- New applications or system integrations may or may not have considered PKI
- Legacy systems may or may not have a solution at all
- Fringe cases can be high-visibility and/or high cost
- Users

CYGNACOM SOLUTIONS

HSPD-12 Impacts to Deployment

- ∞

CYGNACOM SOLUTIONS

HSPD-12 Impacts to Deployment

- Issuance and management model has to be aligned with badge issuance
  - This includes provisioning in systems like Active Directory, e-mail systems, NACI checks
  - Can be beneficial for functions like revocation
  - Can be complicated with respect to governance
- Registration model can be streamlined
  - PIV enrollment can take the place of existing PKI registration forms and processes
- Support profile discrepancies
  - Software updates to the desktop (support for PIV)
  - Potential reader changes
- Increased lifecycle costs and lifecycle
- Policy support has arrived
  - "Where practicable…"
  - Use the governance model to get the message to application and system owners
  - Double-edged sword
- Remote access policy and implementation
- Choose your SSP wisely
  - Governance and oversight
  - Lock-in
  - Flexibility in process, product, and support