HSMs and the Evolving PKI Ecosystem

Mark B. Cooper
President & Founder
PKI Solutions Inc.

October 2014

THALES

- **About PKI Solutions Inc.**
  - 10 years as Microsoft Senior Engineer for PKI
  - Numerous books and whitepapers
  - Services include:
    - ADCS Architecture, Deployment and Consulting
    - Assessment and Remediation Services
    - In-Depth PKI Training
    - Retainer and Support Services

HSMs and the Evolving PKI Ecosystem

- PKI ecosystem changes
- BYOD and Internet of Things
- Security threats
- Leveraging HSMs
- Deployment challenges

PKI ecosystem changes

HSMs and the Evolving PKI Ecosystem

- **PKI adoption rates are quickly increasing**
- **Evolving usage scenarios**
  - **Traditional uses**
  - **Greater product integration and dependencies**
- **Scaling and availability**
  - **Fault tolerance**
  - **OCSP**
- **Integration into continuity plans**

HSMs and the Evolving PKI Ecosystem

- **Evolving to meet the new enterprise**
  - **Disconnected**
  - **Unmanaged**
  - **Diverse**
  - **Computers AND devices**

BYOD and IoT impact

HSMs and the Evolving PKI Ecosystem

- **BYOD and corporate security policies**
  - 180 degree change from traditional models
  - Primarily user driven demand
- **Accessibility**
  - What's the cost?
  - Risk versus reward
- **Affects security postures**
  - BYOD S/Mime & Smart cards
  - Weaknesses will be exploited

HSMs and the Evolving PKI Ecosystem

- **IoT evolving**
  - Tighter interaction with corporate networks
  - De-evolution of PSTN and side-band communications
- **IoT challenges everything**
  - Integrated OS
    - Management
    - Security
    - Identity
- **Shell Bash**
  - Weaknesses will be exploited

Security threats

HSMs and the Evolving PKI Ecosystem

- **Data theft no longer theoretical exercises**
  - **Valuable information will be sought by others**
  - **Internal, domestic and foreign interests and gain**
- **Outright compromises**
  - **Target**
  - **Michael's**
- **Vulnerabilities**
  - **Heartbleed**
  - **Shell Bash**

Leveraging HSMs

HSMs and the Evolving PKI Ecosystem

- **Disconnects keys and access**
  - **OS and devices have limited access to keys**
  - **Compromises and vulnerabilities reduced**
- **Implements Role Separation**
  - **Internal attacks and social engineering**

HSMs and the Evolving PKI Ecosystem

- **HSM and CA Signing Keys**
  - **Traditional use of HSM and CA**
  - **Most valuable keys, but not the only ones**
- **OCSP Responder**
  - **Signs revocation queries on-behalf of CA**
  - **Revocation is key to trust of PKI – keys are valuable**

HSMs and the Evolving PKI Ecosystem

- **Network Device Enrollment Service**
  - **Microsoft's SCEP implementation**
  - **Enrolls and renews devices**
  - **Designed for segmented authentication & enrollment**
  - **New whitepaper from Microsoft**
    - **NDES Keys secured on HSM (Explicitly tested with Thales)**
    - **Firewall and hardening recommendations**
    - **"Securing and Hardening Microsoft Network Device Enrollment Service"**

HSMs and the Evolving PKI Ecosystem

- **Manufacturers**
  - **Leveraging PKI for device identities**
  - **IoT maturity demands**
- **HSMs role in manufacturing**
  - **Integrated for CA key protection**
    - **Combined with TPM for end-to-end protection**
  - **Thales nCipher**

Deployment challenges

HSMs and the Evolving PKI Ecosystem

- **Old Habits**
  - **Theoretical threats hard to quantify**
  - **Software doesn't require HSM**
  - **"It wont happen to us"**
- **Challenges rarely in the technology**
  - **People resources**
  - **Policies**
  - **Budgets**

HSMs and the Evolving PKI Ecosystem

- **InfoSec groups are still the exception**
- **Difficulty to define quorums and role owners**
  - **Separation of duties and collusion requirements**
  - **Still compromising and right-sizing to environments**
- **PKI depends on clear policies**
  - **Defines security risks, policies and rules**
  - **Highly dependent on controls to enforce**

HSMs and the Evolving PKI Ecosystem

- **Enterprises strive for secure – default to easy**
- **Hard to enforce security policies**
  - **#1 vulnerability to secure data centers**
- **PKI depends on clear policies**
  - **Defines security risks, policies and rules**
  - **Highly dependent on controls to enforce**

HSMs and the Evolving PKI Ecosystem

- **Budget Challenge – "We'll do it in the future"**
  - **Must be part of initial deployment**
  - **Integration later is possible, but integrity is questionable**
  - **"A moment alone can never be undone"**
- **Response**
  - **Value of protected keys is diminished in the future**
  - **Additional expense to migrate and integrate**
  - **If worth protecting with PKI, why not do it properly?**
  - **PKI without protections is a false sense of security**

HSMs and the Evolving PKI Ecosystem

- **Budget Challenge – "It's too expensive"**
  - **Cost of acquiring and integrating HSMs**
  - **Perceived value of protecting "our lowly keys"**
  - **"We're not a target"**
- **Response**
  - **Cost of acquisition is considerably cheaper than a compromise**
    - **Think about this challenge after a compromise**

Questions?

ADCS Hotfix Digest:

http://pkisolutions.com/adcs-hotfixes

mark@pkisolutions.com || pkisolutions.com || @pkisolutions

Available Training

4 Day ADCS In-Depth Server 2012 R2

Washington, DC: November 4-7, 2014

San Francisco, CA: January 27-30, 2015

New York City, NY: February 2015 (TBA)

mark@pkisolutions.com || pkisolutions.com || @pkisolutions