Upgrading and Improving the Trust of Microsoft Windows Certificate Authorities

Mark B. Cooper
President & Founder
PKI Solutions Inc.

PKI Solutions

THALES

About PKI Solutions

10 years as Microsoft Senior Engineer for PKI

Numerous books and whitepapers

Services include:

- **ADCS Architecture, Deployment and Consulting**
- **PKI Assessment and Remediation Services**
- **In-Depth PKI Training**
- **Retainer and Support Services**

“A poorly designed, executed or managed PKI can introduce more security issues than it solves.”

Agenda

- Your self-managed public key infrastructure
- Vulnerabilities of an aging infrastructure
- Mitigating risks

Self-Managed PKIs

and

The Vulnerabilities of an Aging Infrastructure

Self-Managed Public Key Infrastructures (PKIs)

Characteristics

- Establish framework for secure exchange of information
- Form core of an organization's critical security posture
- Now support more and more critical business applications

Microsoft Active Directory Certificate Services (AD CS)

- Part of the operating system
- Lower barrier for adoption
- Over a decade of proven history

Legacy Windows Server 2003 Operating System

Product Lifecycle

- Legacy – 10 year old features
- End of service next year

Practical Considerations

- Threat and vulnerabilities – old security process
- Maintainability – expanding PKI uses

Digital Certificates Are Everywhere

PKI is the Root of Trust for expanding uses

- Identity and access control
  - System Center, Exchange, DirectAccess, Link
  - Certificates for Web Servers, access points, communications
- Device credentialing
  - “Electronic asset” tag
  - “Bring your own device”
- Content integrity
  - Code signing (Authenticode)
  - Document signing

PKI Solutions

THALES

Impact of a Deprecated Operating System

- **Lacks features of the newer OSs**
  - Crypto next generation (CNG) and Suite B
  - Encrypted certificate enrollment
- **Will become target for hackers**
  - No formal security patches available
  - No fixes to combat new threats
- **Restricts agility**
  - Older features can’t respond to new use cases
  - Older architecture limits scalability

Mitigating Risks

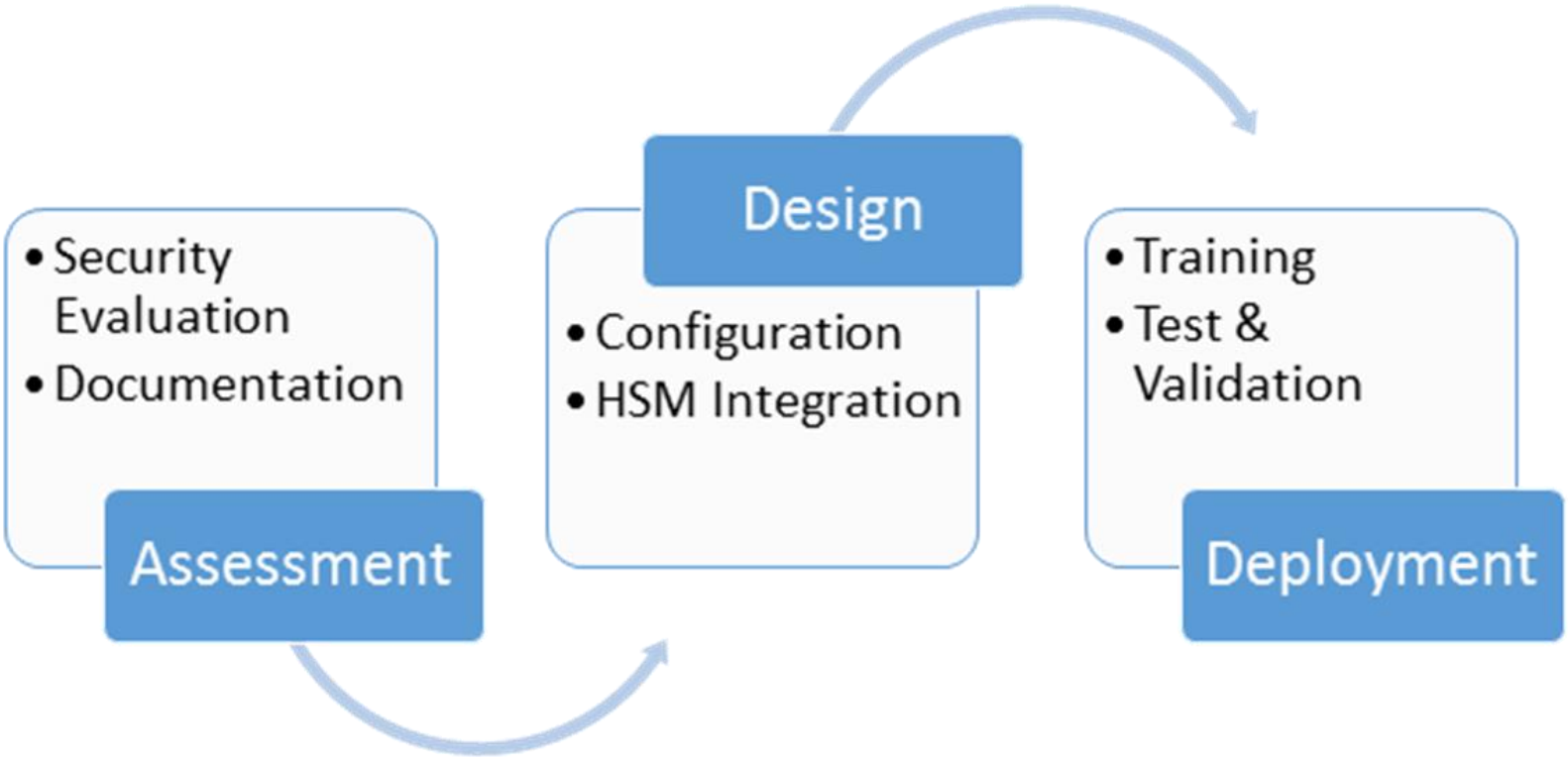
Major Changes to the Core Crypto

- Support for CAPI Next Generation
- Support for Suite B algorithms
- Process isolation for long term keys
- Improved Role Description and Enrollment

Hardware Security Modules (HSMs)

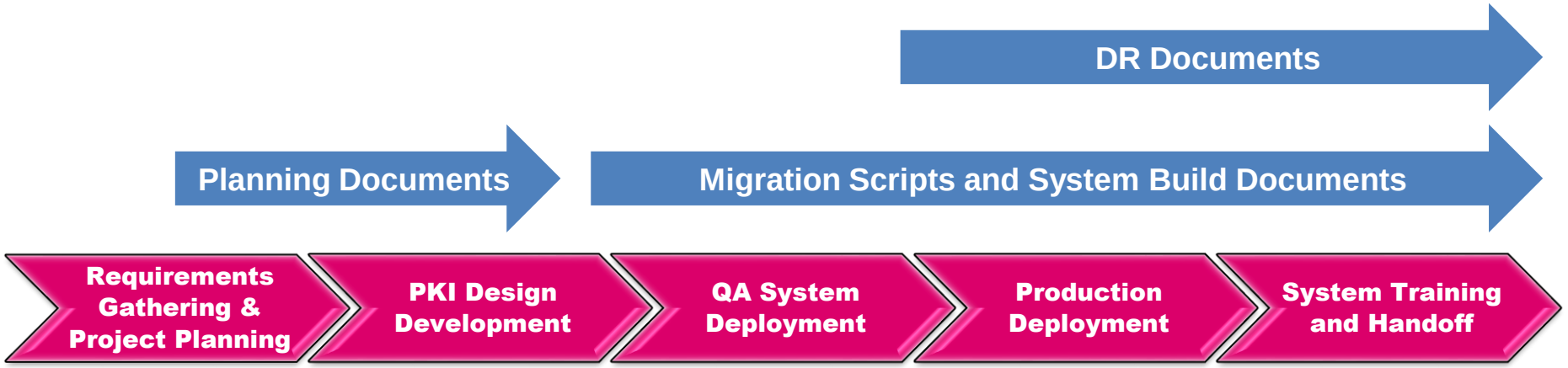
- Hardened key protection
- Auditable lifecycle key management

PKI Project Methodology



***PKI Projects are 80% process and documentation and 20% technology**

A Typical Migration in More Detail



- Document Certificate Use cases
- Create detailed project plan
- Evaluate existing documentation
- Report on extent of documentation task set

- Develop trust model
- Create system design document
- Begin Business Continuity Plan document (DR plan)
- Begin CP/CPS document development
- Create documentation roles and responsibilities

- Install and configure CA servers in lab
- Install and configure HSMs in lab
- Begin system build document
- Finalize BCP
- System stability testing

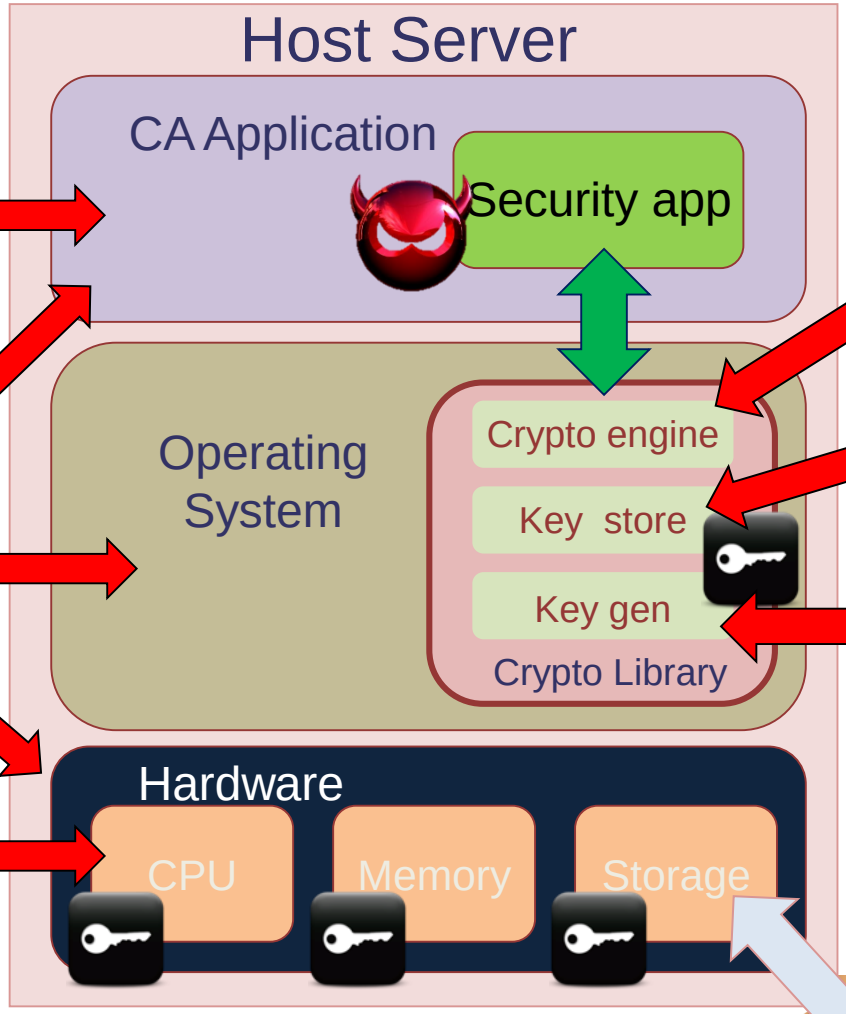
- Install and configure CA servers at Production sites
- Install and configure HSMs at Production sites
- Finalize system build documents
- Migrate Security World
- Migrate ADCS DB

- System architecture overview
- Process review (DR, Root signing, etc.)
- nCSE course
- Review and deliver final documentation
- Delivery final CP/CPS draft
- Project Signoff

Protecting Critical Keys

- Keys stored in software are at risk
- Exploit illustrated by Heartbleed
- Potential threat exists in any OS

Threats to Software Keys



Malware corrupts application

Malicious admin and privileged users

Physical attack, side channel analysis, “snap shotting”

Weak algorithm choice or implementation

Short keys are easy to guess

Poor random number generators

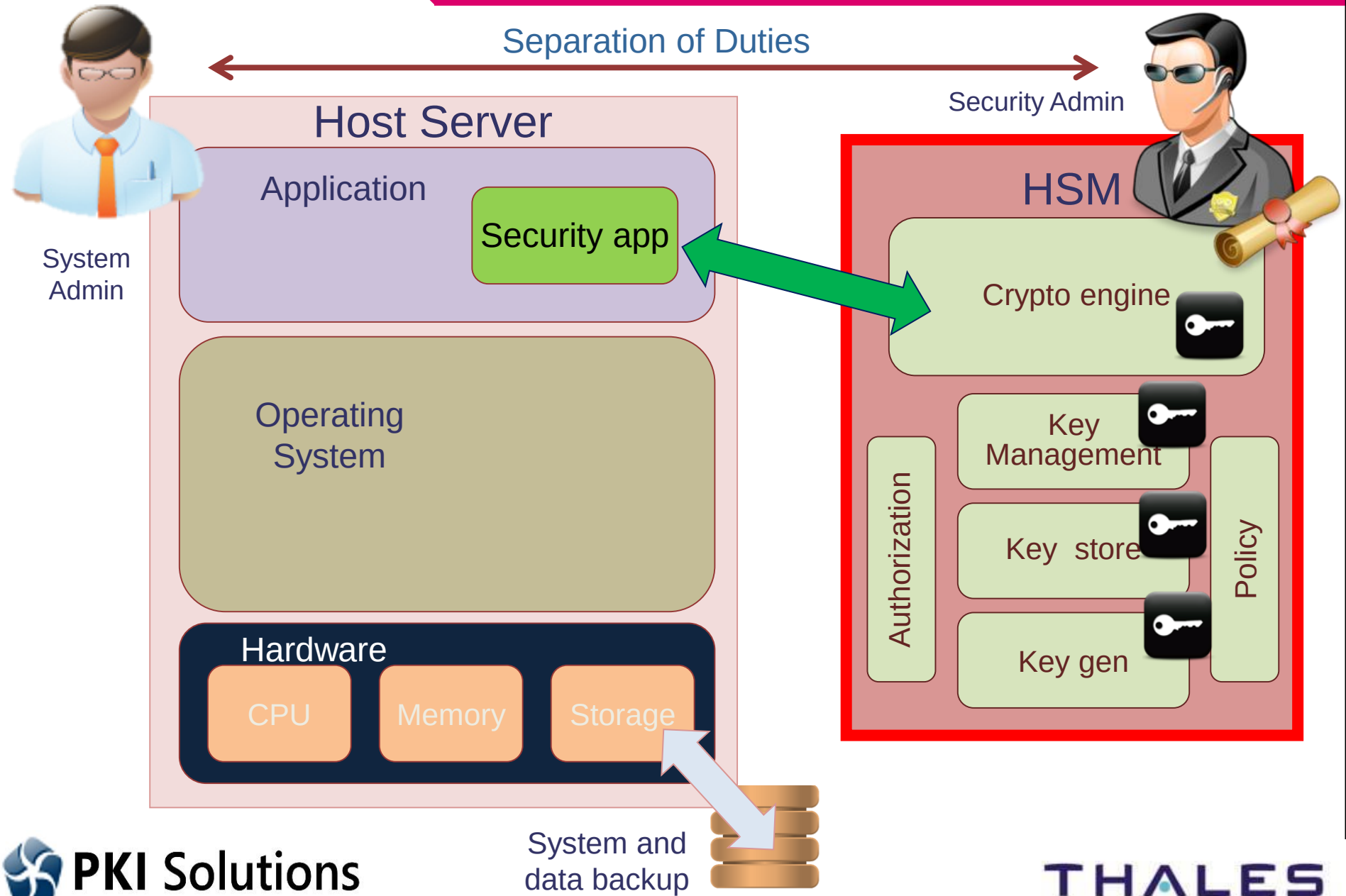
Stolen backup media

System and data backup

PKI Solutions

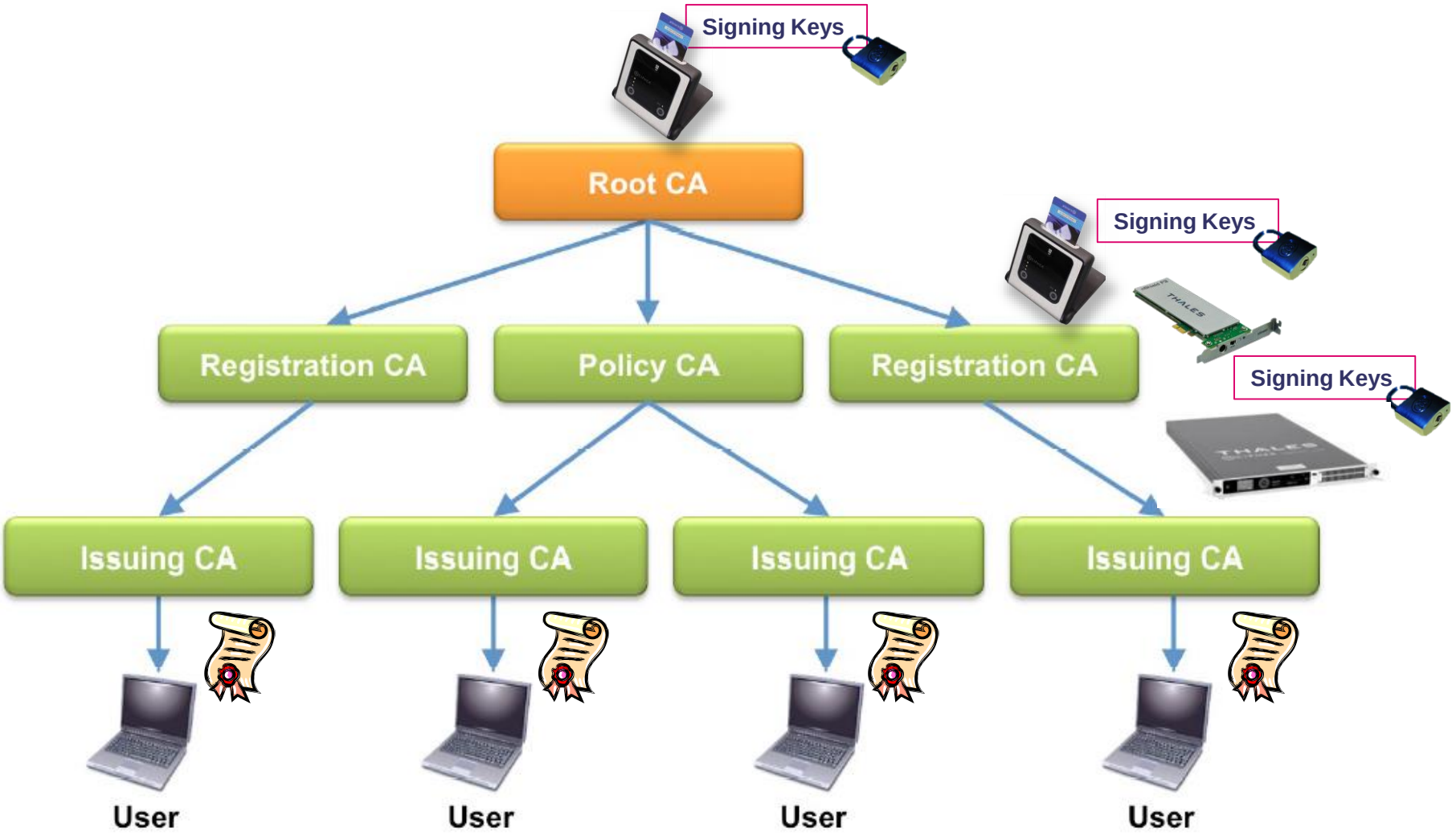
THALES

How HSMs Help Reduce Risk



Protecting Your Critical Certificate Authority Keys

Securing the Root of Trust



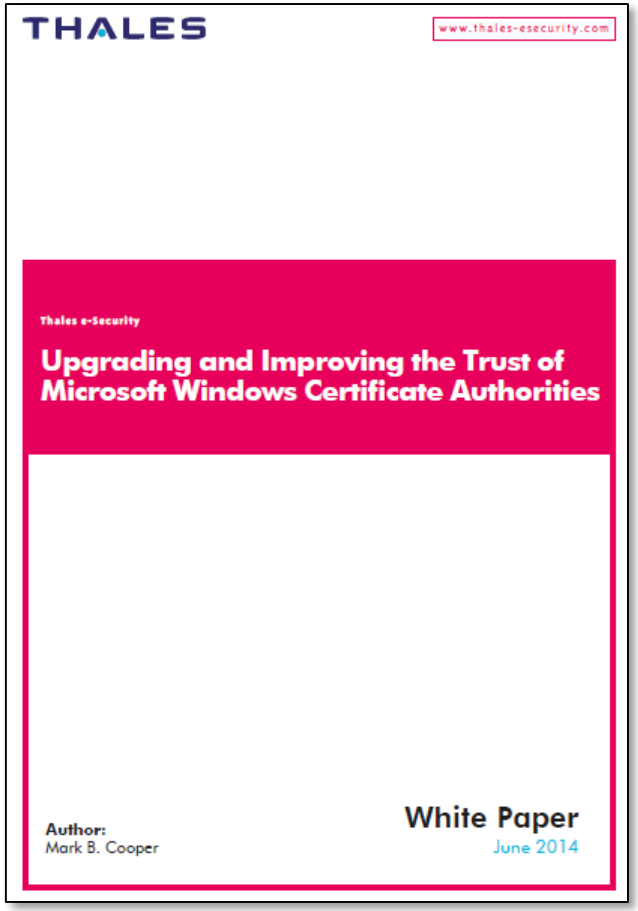
New White Paper

Learn how to mitigate risks and protect CA root keys

Download white paper from Thales e-Security website

Upgrading and Improving the Trust of Microsoft Windows Certificate Authorities

https://www.thales-esecurity.com/cpn/pki-trust



In Summary...

- Wide-scale reliance on Microsoft self-managed PKIs
- Significant numbers built on OS going end of service
- Security updates must happen now before its too late
- Thales and PKI Solutions can help you in the process

PKI Solutions

THALES

White Paper: https://www.thales-esecurity.com/cpn/pki-trust

Stay Connected:

www.pkisolutions.com
www.pkisolutions.com/adcs-hotfixes
@pkisolutions

PKI Solutions

THALES