2017 PKI GLOBAL TRENDS STUDY

November 2017

PKI at the Crossroads: the Impact of the IoT and more!

Amogh Ranade

About this research

- **1,510 global respondents**

- **Covers US, Germany, India, UK, Brazil, Japan, Mexico, France, Arabia, Russian Federation, and Australia**

- **Part of Global Encryption Trends Study published in April 2017**
  - Third year with PKI trends

THALES

Ponemon INSTITUTE

2017 PKI GLOBAL TRENDS STUDY

October 2017

THALES Ponemon INSTITUTE

Agenda

- Ongoing PKI challenges

- Increasing security maturity of enterprise PKIs

- Increasing influence of the IoT in PKI planning

- Takeaways

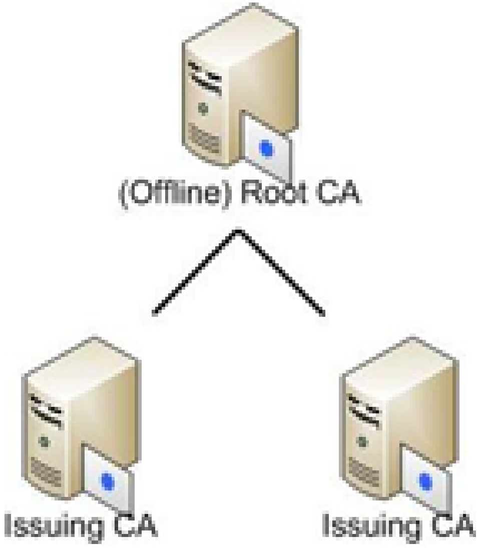
PKI state of the state

Public Key Infrastructure

- Issues and manages digital certificates for applications
- Technology, policies, and procedures

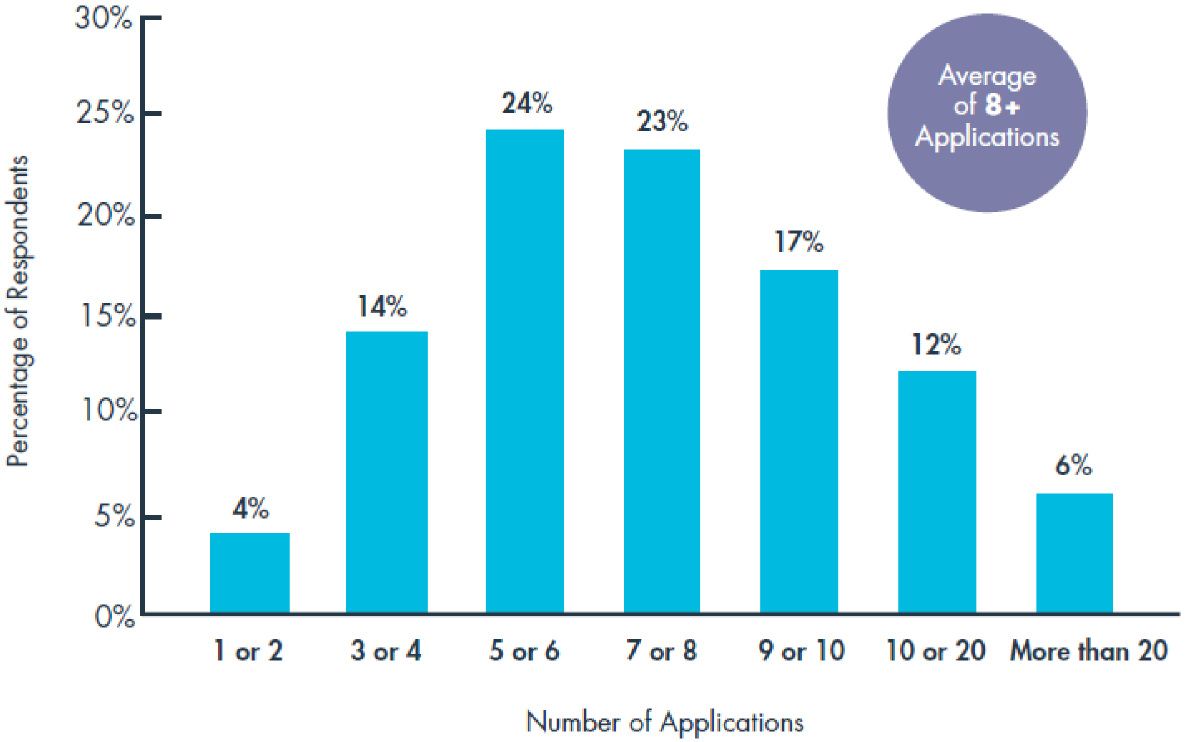
Standards and products stable but infrastructure implementation evolving

- Updated key lengths, algorithms
- Demands of new applications



How many applications does your PKI support?

- Continues to rise
- Complicates management
- Are initial conditions still true?



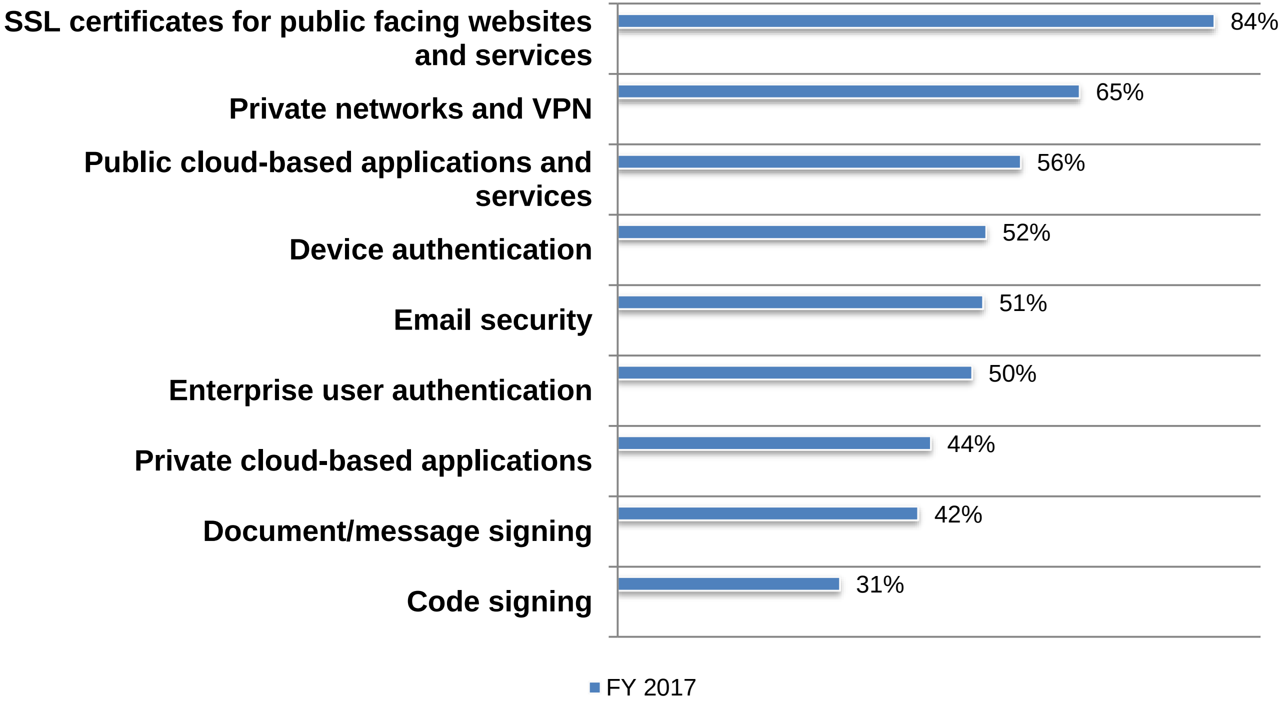
THALES Ponemon INSTITUTE

Applications that use PKI credentials

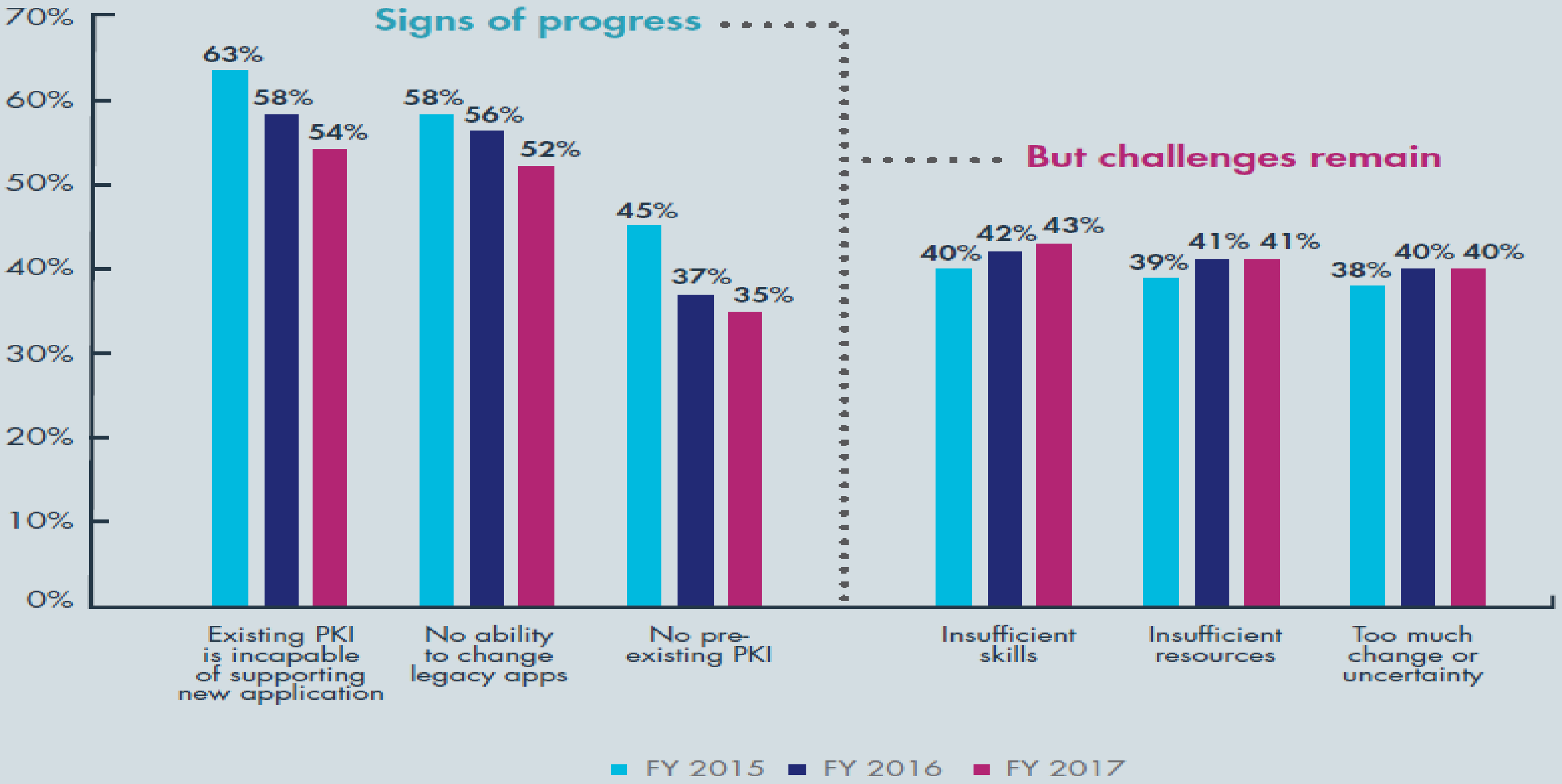
Cloud applications on the rise

These are core enterprise applications

- Downtime or loss of trust would have severe impact



Mixed bag for “challenges to enable applications to use PKI”



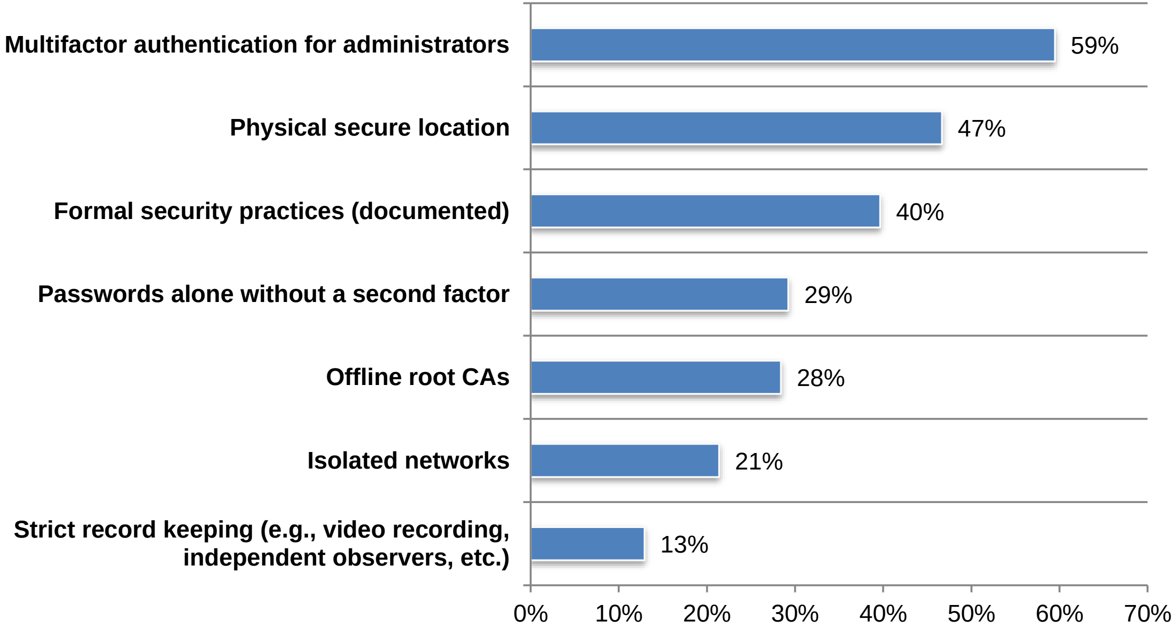
THALES

Ponemon INSTITUTE

Increasing PKI security maturity

Practices to secure PKI and Certificate Authorities

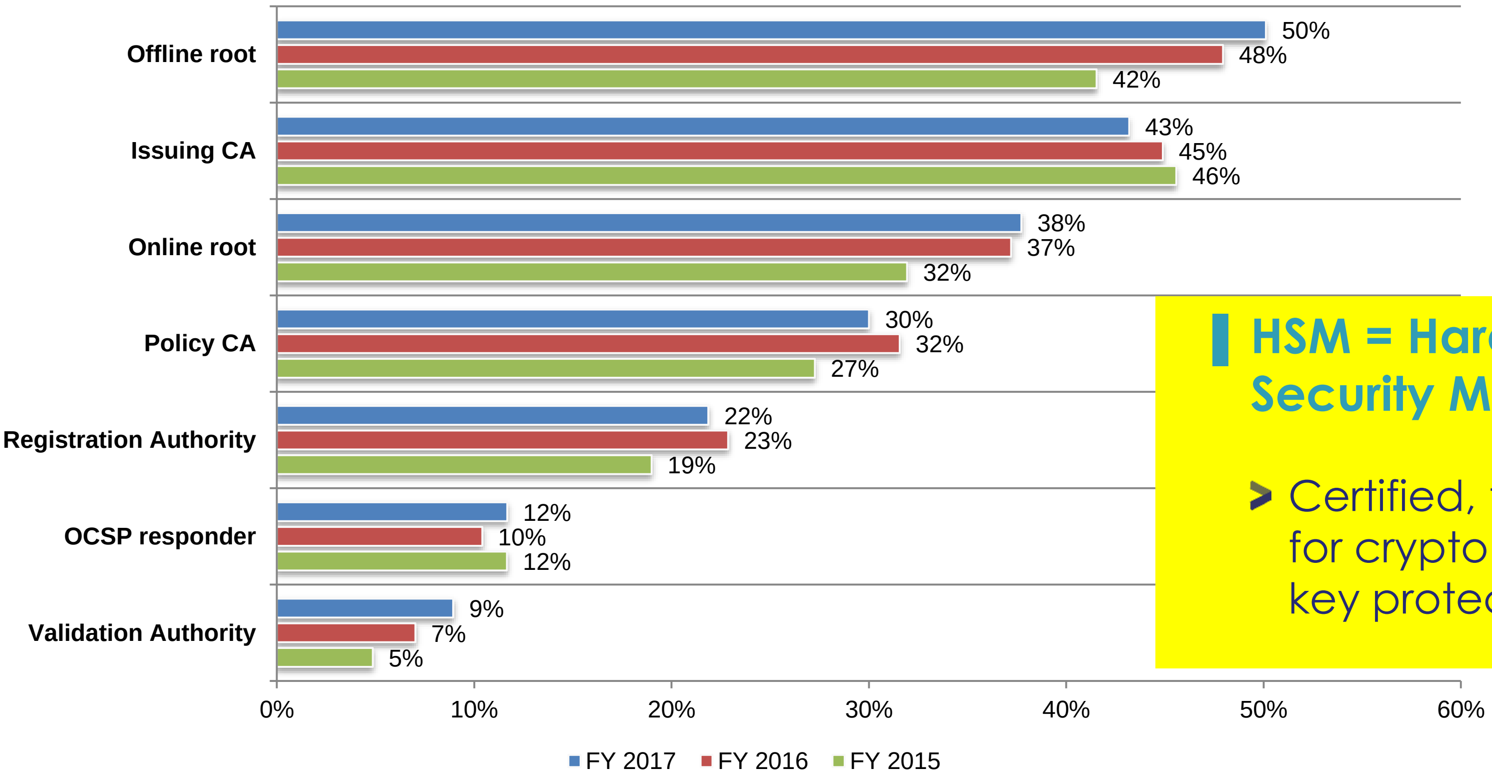
- Shows increasing adoption of best practices
- Less out-of-the-box CA software use, more rigor
- HSM use eclipsed password-only use for the first time!

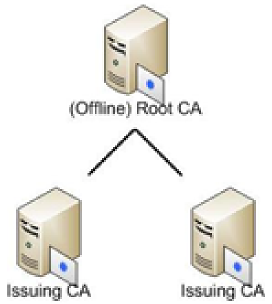


THALES

Ponemon INSTITUTE

Where HSMs are used

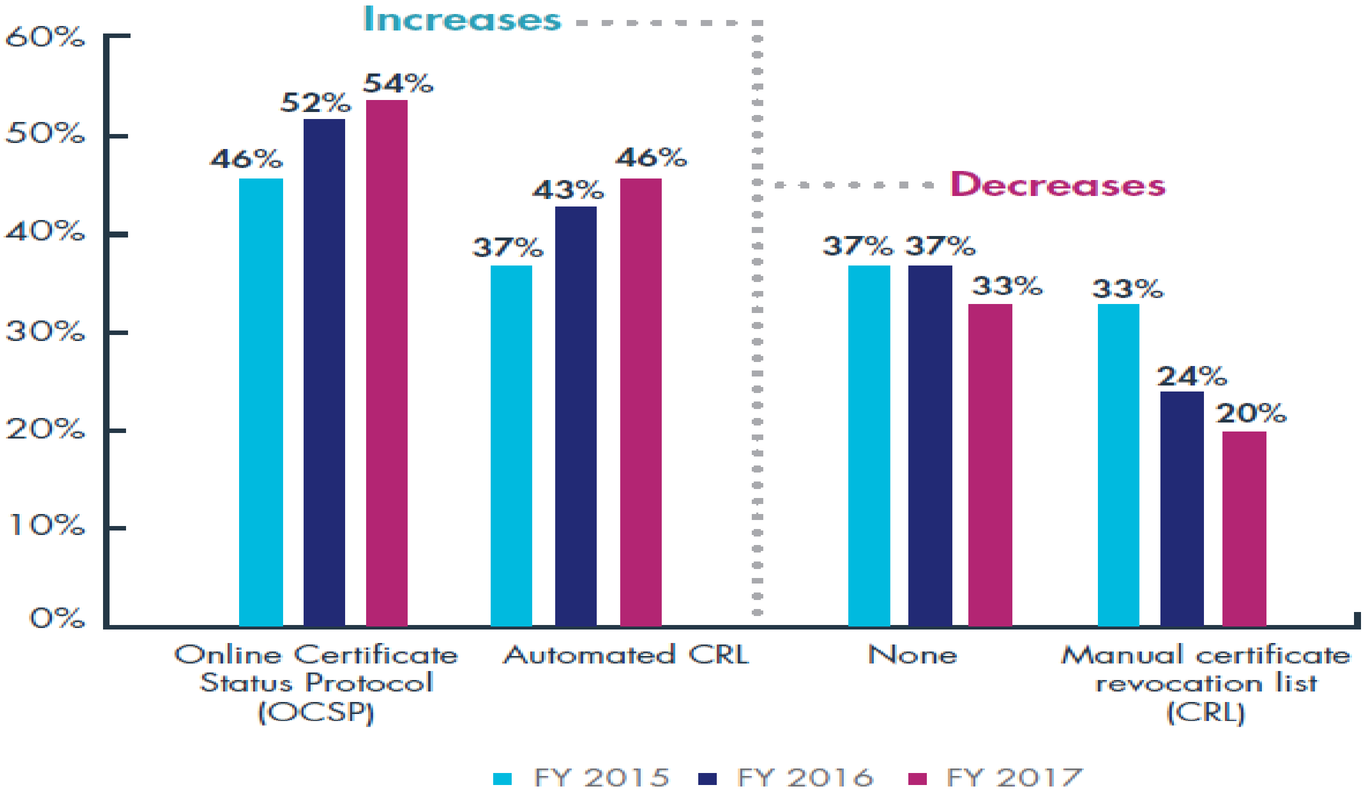




HSM = Hardware Security Module

- Certified, trusted platform for crypto operations and key protection

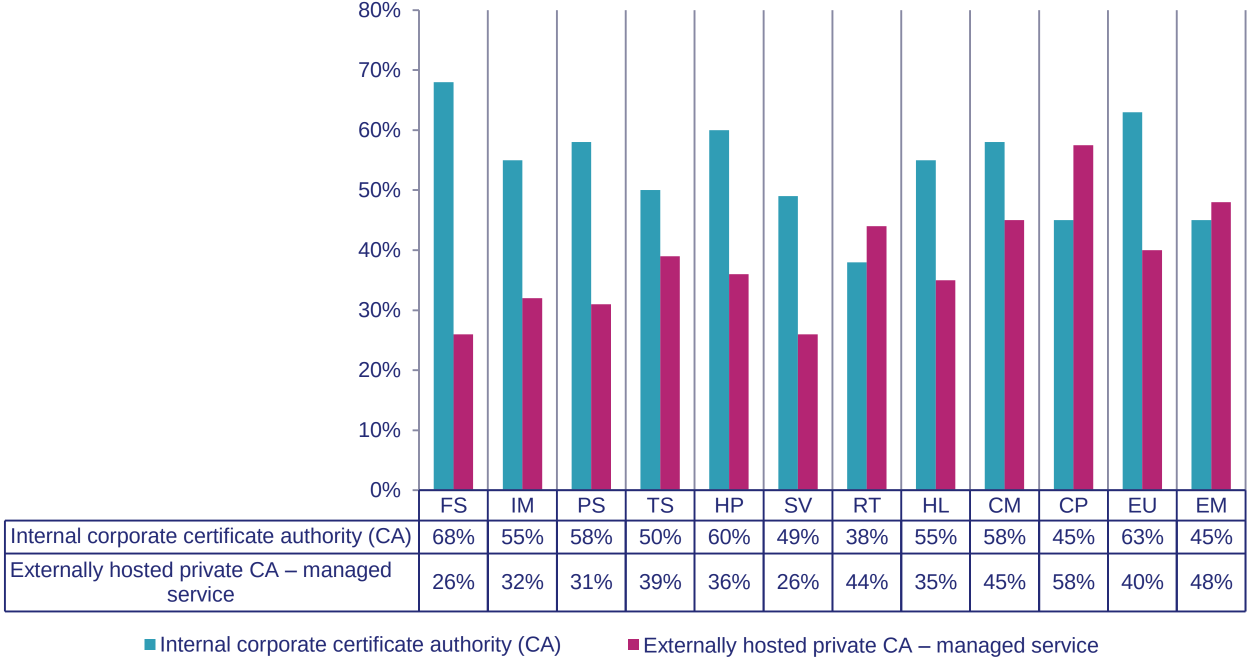
Approaches to certificate revocation



PKI deployment by industry sector

- Internal CA choice correlates with security maturity and heavier regulation

- Similar results from regional analysis



	FS	IM	PS	TS	HP	SV	RT	HL	CM	CP	EU	EM
Internal corporate certificate authority (CA)	68%	55%	58%	50%	60%	49%	38%	55%	58%	45%	63%	45%
Externally hosted private CA – managed service	26%	32%	31%	39%	36%	26%	44%	35%	45%	58%	40%	48%

FS = Financial services
IM = Industrial/manufacturing
PS = Public sector
TS = Technology & software

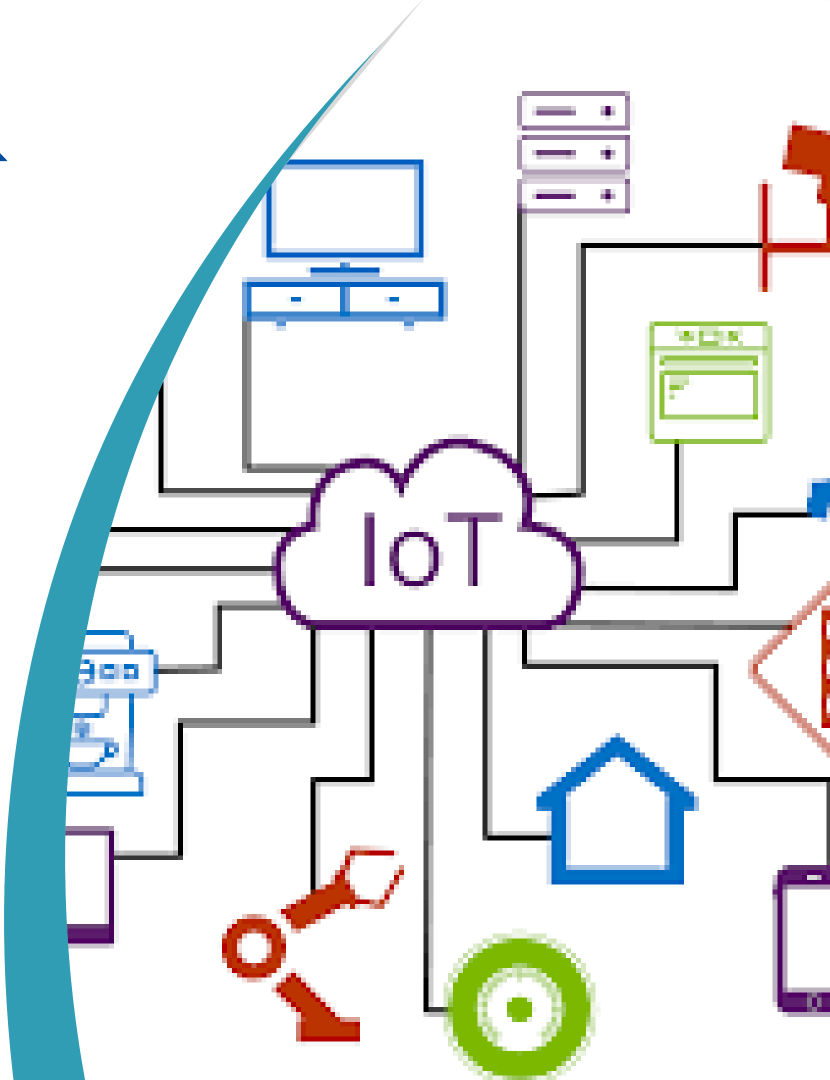
HP = Healthcare & pharma
SV = Services
RT = Retail
HL = Hospitality & leisure

CM = Communications
CP = Consumer products
EU = Energy & utilities
EM = Entertainment & media

THALES

Ponemon INSTITUTE

Increasing influence of the Internet of Things (IoT) in PKI planning

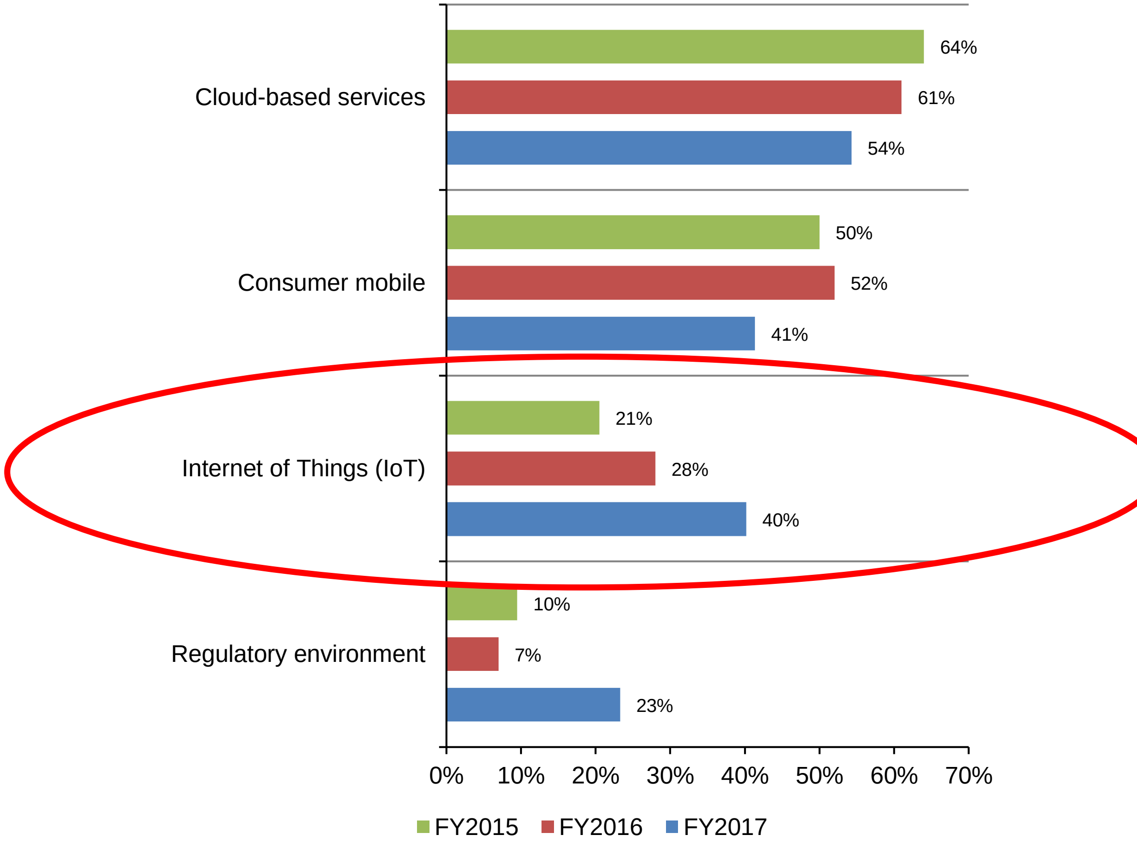


Most important trends driving PKI deployment

- IoT is mirroring the rapid rise of cloud services

- Logical given increased enterprise PKI leverage and security investment

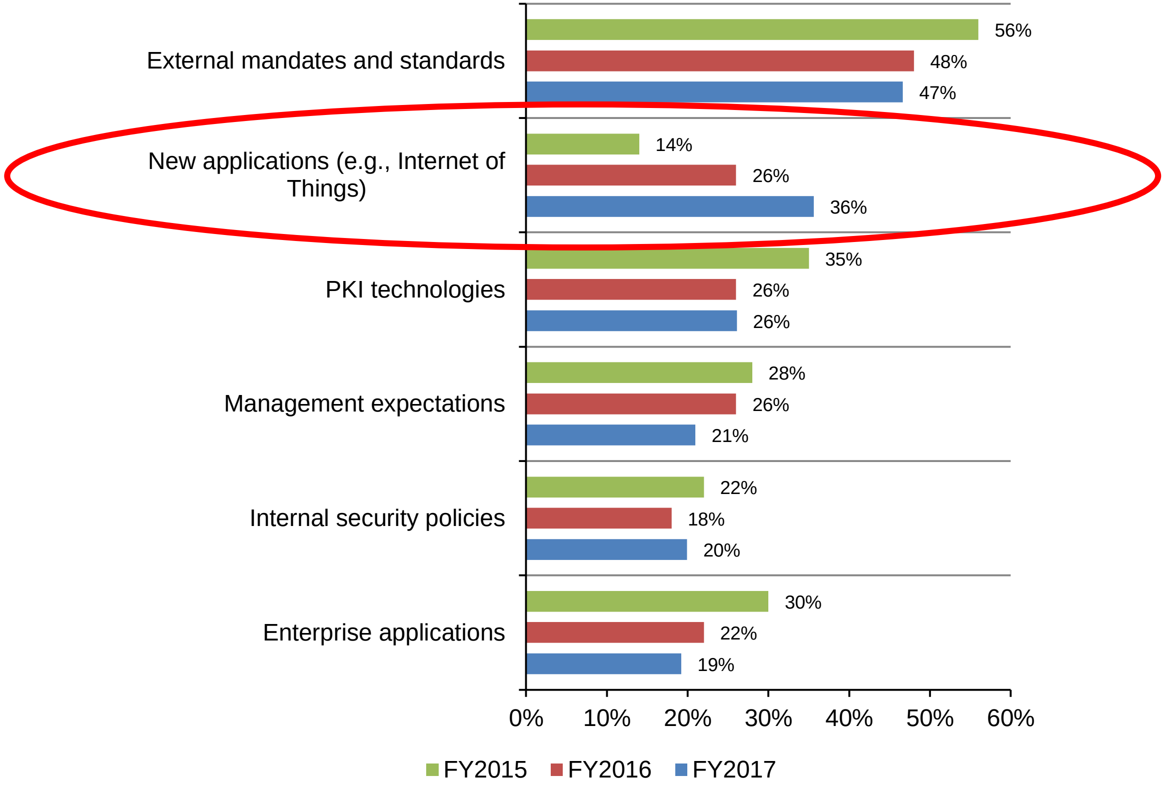
- Expect adaptations to fit IoT environments



Greatest areas of change for PKI planning/evolution

- **43% of IoT devices in use will use will use digital certificates in the next two years**

- **PKI deployment will evolve to a combination of enterprise-based and cloud-based**



THALES Ponemon INSTITUTE

PKI/IoT customer example

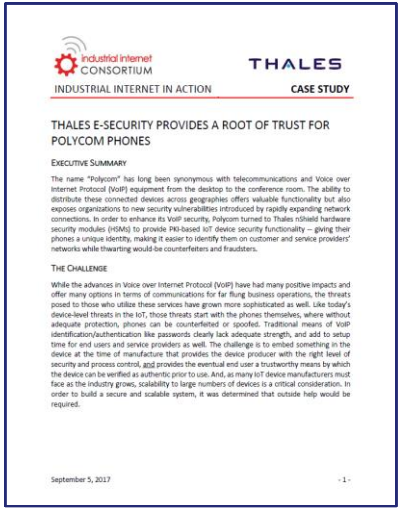
Problem

- Prevent counterfeiting
- Enable secure device authentication

Solution

- Embed keys and certificates at the time of manufacture
- nShield HSMs with CodeSafe working with Microsoft PKI
- Professional Services

Similar customers include set-top-box manufacturers



industrial internet CONSORTIUM

THALES

INDUSTRIAL INTERNET IN ACTION

CASE STUDY

THALES E-SECURITY PROVIDES A ROOT OF TRUST FOR POLYCOM PHONES

Executive Summary

The name "Polycom" has long been synonymous with telecommunications and Voice over Internet Protocol (VoIP) equipment from the desktop to the conference room. The ability to distribute these connected devices across geographies offers valuable functionality but also exposes organizations to new security vulnerabilities introduced by rapidly expanding network connections. In order to enhance its VoIP security, Polycom turned to Thales nShield hardware security modules (HSMs) to provide PKI-based IoT device security functionality -- giving their phones a unique identity, making it easier to identify them on customer and service providers' networks while thwarting would-be counterfeiters and fraudsters.

The Challenge

While the advances in Voice over Internet Protocol (VoIP) have had many positive impacts and offer many options in terms of communications for far flung business operations, the threats posed to those who utilize these services have grown more sophisticated as well. Like today's device-level threats in the IoT, those threats start with the phones themselves, where without adequate protection, phones can be counterfeited or spoofed. Traditional means of VoIP identification/authentication like passwords clearly lack adequate strength, and add to setup time for end users and service providers as well. The challenge is to embed something in the device at the time of manufacture that provides the device producer with the right level of security and process control, and provides the eventual end user a trustworthy means by which the device can be verified as authentic prior to use. And, as many IoT device manufacturers must face as the industry grows, scalability to large numbers of devices is a critical consideration. In order to build a secure and scalable system, it was determined that outside help would be required.

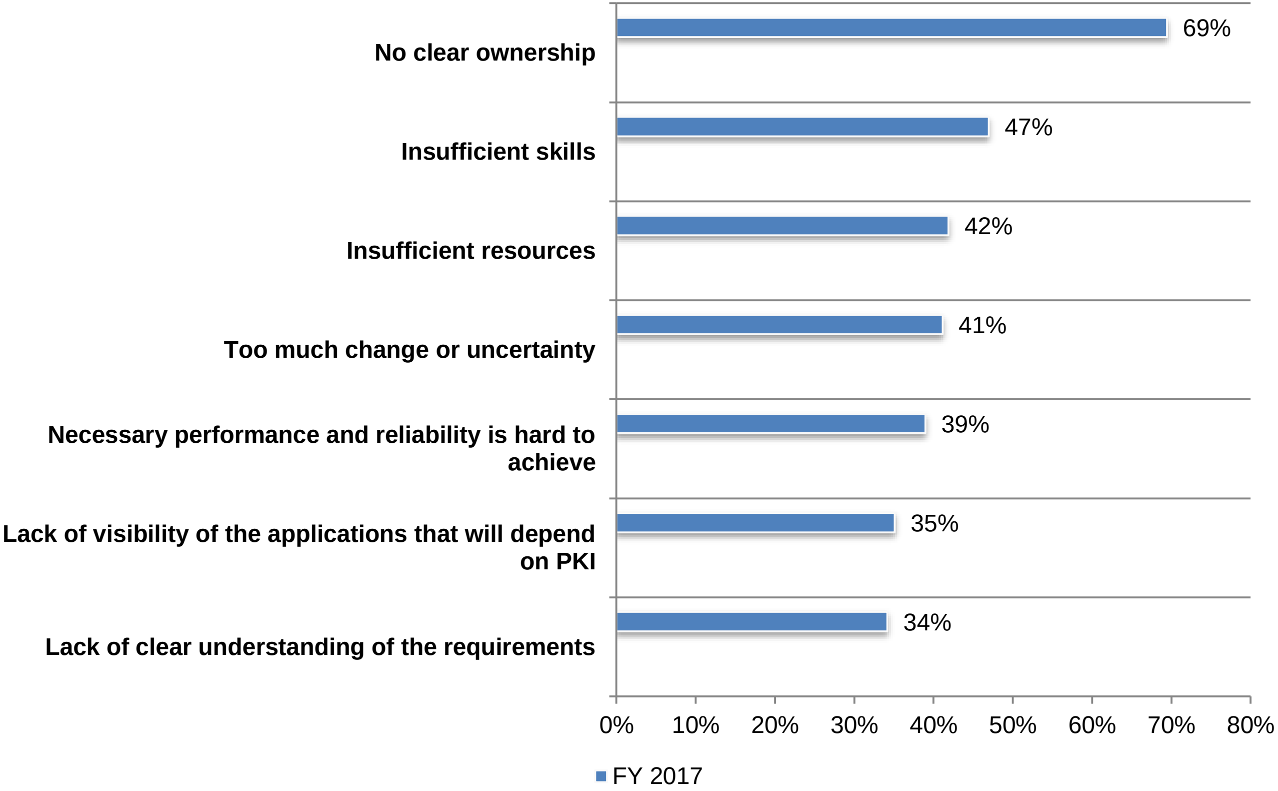
September 5, 2017

- 1 -

PKI deployment/management challenges

- Ownership clashes and skill/resource issues have plagued PKIs for years

- All signs are that IoT projects are revealing very similar challenges



THALES

Ponemon INSTITUTE

Takeaways

PKI is a critical investment – today and tomorrow

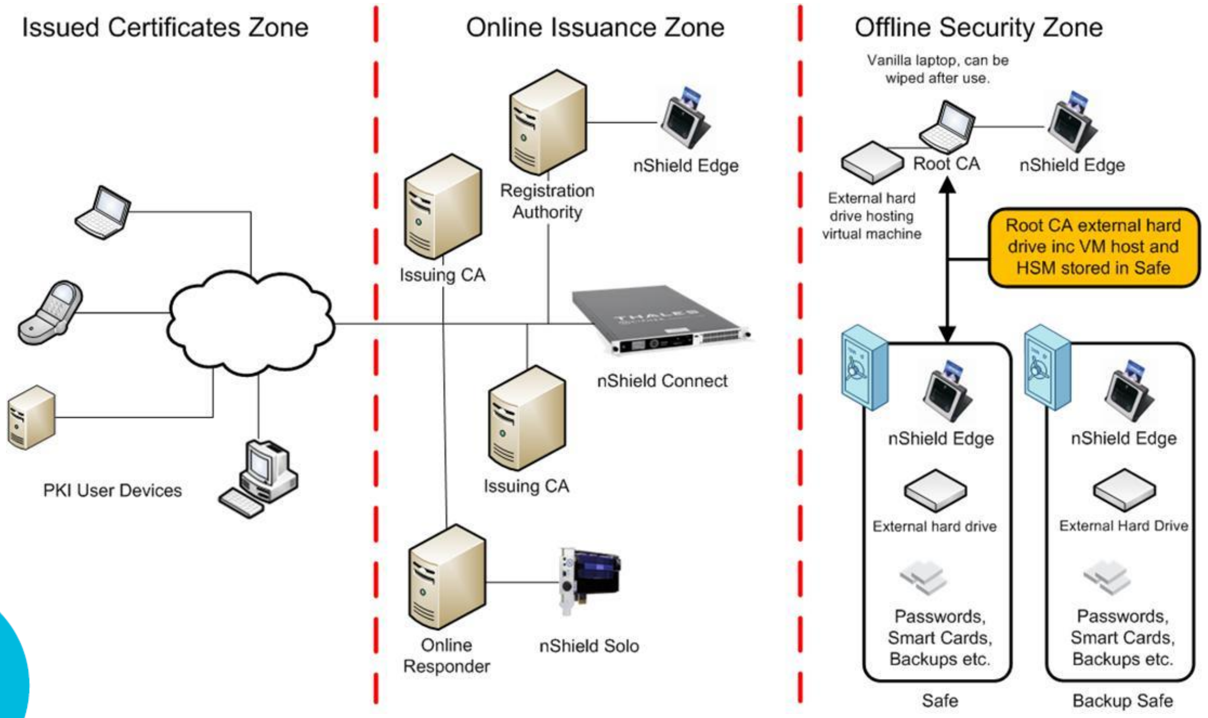
Increased adoption of best practices

- Multi-factor auth
- HSMs
- Certifications

Planning and skills/resources important

65% rate **FIPS 140-2 Level 3** as important for PKI

64% rate **Common Criteria EAL Level 4+** as important for PKI



https://www.thalesesecurity.com/products/general-purpose-hsms

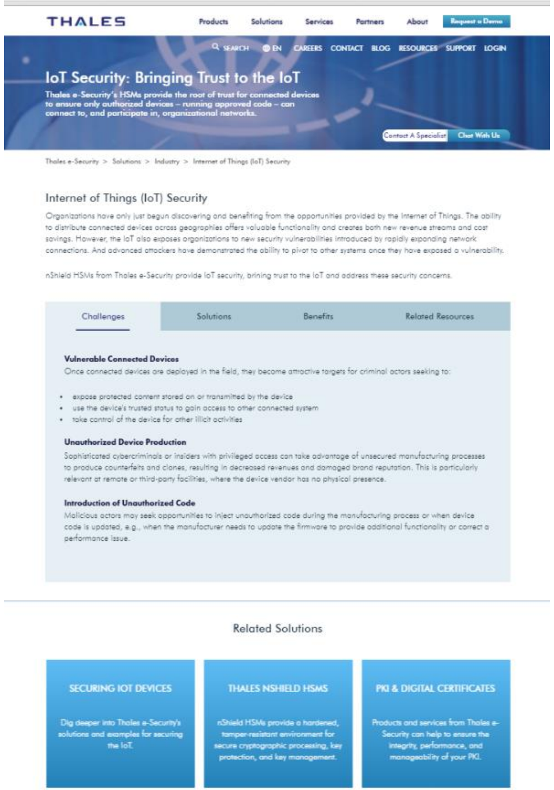
THALES

Ponemon INSTITUTE

PKI provides an important component of Trust for the IoT

If you can’t trust the data, there’s no point in collecting it, analyzing it, or making business decisions based on it

- Trust starts at the device with authentication
- Code signing and encryption/key management address device integrity and data protection through an IoT ecosystem



IoT Security: Bringing Trust to the IoT

Thales e-Security’s HSMs provide the root of trust for connected devices to ensure only authorized devices – running approved code – can connect to, and participate in, organizational networks.

Internet of Things (IoT) Security

Organizations have only just begun discovering and benefiting from the opportunities provided by the Internet of Things. The ability to distribute connected devices across geographies offers valuable functionality and creates both new revenue streams and cost savings. However, the IoT also exposes organizations to new security vulnerabilities introduced by rapidly expanding network connections. And advanced attackers have demonstrated the ability to pivot to other systems once they have exposed a vulnerability.

nShield HSMs from Thales e-Security provide IoT security, brining trust to the IoT and address these security concerns.

Vulnerable Connected Devices

Once connected devices are deployed in the field, they become attractive targets for criminal actors seeking to:

- expose protected content stored on or transmitted by the device
- use the device’s trusted status to gain access to other connected system
- take control of the device for other illicit activities

Unauthorized Device Production

Sophisticated cybercriminals or insiders with privileged access can take advantage of unsecured manufacturing processes to produce counterfeits and clones, resulting in decreased revenues and damaged brand reputation. This is particularly relevant at remote or third-party facilities, where the device vendor has no physical presence.

Introduction of Unauthorized Code

Malicious actors may seek opportunities to inject unauthorized code during the manufacturing process or when device code is updated, e.g., when the manufacturer needs to update the firmware to provide additional functionality or correct a performance issue.

Related Solutions

SECURING IOT DEVICES

Dig deeper into Thales e-Security’s solutions and examples for securing the IoT.

THALES NSHIELD HSMS

nShield HSMs provide a hardened, tamper-resistant environment for secure cryptographic processing, key protection, and key management.

PKI & DIGITAL CERTIFICATES

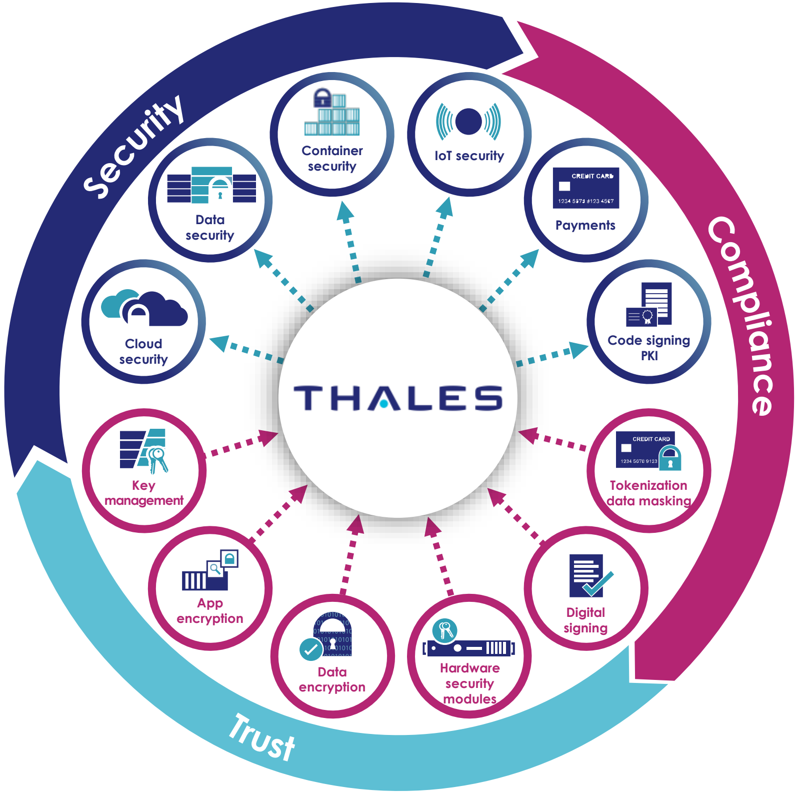
Products and services from Thales e-Security can help to ensure the integrity, performance, and manageability of your PKI.

https://www.thalesesecurity.com/iot

Q&A

Ponemon Institute
Toll Free: 800.887.3118
Michigan HQ: 2308 US 31 N.
Traverse City, MI 49686 USA
research@ponemon.org

Thales eSecurity
+1 954 888 6200
Americas: sales@thalesesec.com
EMEA: emea.sales@thales-esecurity.com
APAC: asia.sales@thales-esecurity.com
www.thalesesecurity.com



THALES Ponemon INSTITUTE