



Role of PKI Today, Tomorrow, and How It Enables Secure Use of New Technology

Bernd Stamp
**Solutions Consultant – Technical
Lead**



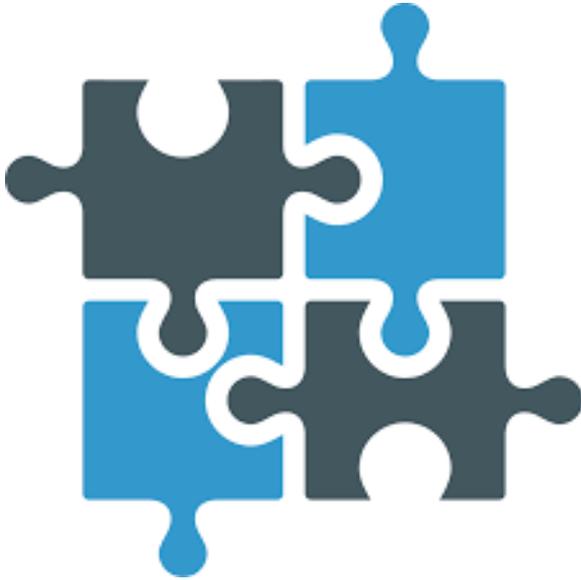
Agenda

- Public Key Infrastructure Explained
- Uses and Traditional Applications
- Evolving Demand and Importance
- Enabler for Use of New Technology
- Critical Importance of Root of Trust

2



PKI – Introduction



○ Foundational Building Block

- Hardware
- Software
- Procedures
- Processes

○ Secure Mechanism

- Issue / manage digital identities
- Identify people / devices (things)
- Validate and authenticate

3

How does it Work?



Can be an individual user or a device (machine)

○ Use Asymmetric Cryptography

- Public key (Issued with certificate)
- Private key (Used for initial signing)

○ Enable Scalable Credentialing System for Validating Identities

- Certificate establish the identity
- Signature provide the validation

○ Private Key Delivers Root of Trust

4

Credentialing and Identity

Identities Forms the Basis of Trust



5



Legacy:

**PKIs have Enabled the Large-Scale Use
of Digital Signatures for e-Commerce**

6



Evolving Demand and Importance

○ Internet of Things (IoT)

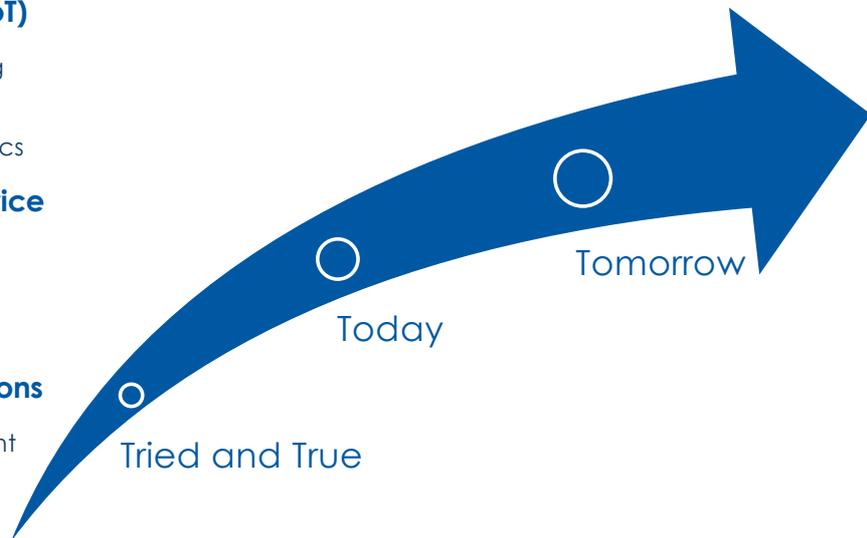
- Device credentialing
- Code signing
- Big data and analytics

○ Bring Your Own Device

- Device identification
- User access controls
- Asset management

○ Enterprise Applications

- Identity management
- Access control
- Web applications
- Digital signing



7

N CIPHER

Changing Role of PKIs

○ Smart Devices Deploying at Rapid Pace

- Projected to reach 20.4 billion by 2020*
- Industrial/manufacturing sector leading

○ IoT - Top Trends Driving PKI Deployment**



42%

of IoT devices in use will use digital certificates for identification/authentication in the next two years.



*Gartner <https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016>

**Ponemon Institute 2019 Global PKI Trends Study

8

N CIPHER

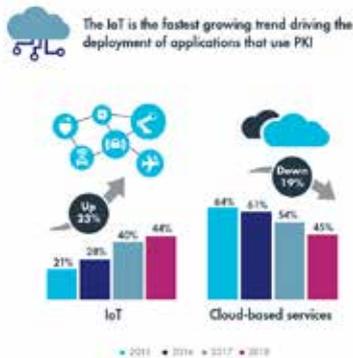
Growing Demand for Certificates

○ Ponemon Institute PKI Trends Study

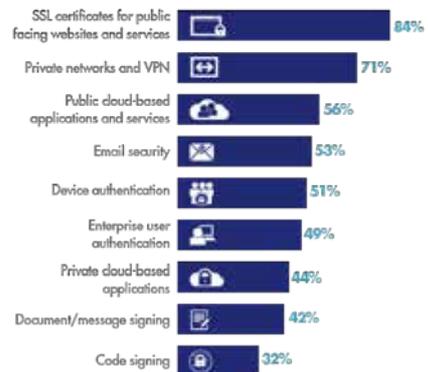
- Reveals growing demand for digital certificates

Survey results from 1,688 respondents in 42 countries

The Rise of the IoT



APPLICATIONS THAT MOST COMMONLY USE DIGITAL CERTIFICATES



9

Device Identities are Everywhere



Mobile Phone Apps



Autonomous Cars



WiFi and VPN Access



Remote Sysadmin Access



Industrial/Agricultural IoT



Medical Records and Devices



Transportation



Home Internet of Things



Wearables



10

IoT Dependence on PKI

○ What Does IoT Need from a PKI?

1. Production control
 - Ensure legitimacy of mass-produced devices
2. Certificate injection
 - Authenticate identity of deployed devices
3. Code signing
 - Validate integrity of device software
4. Data protection
 - Safeguard confidentiality and integrity



11

Step 1: Production Control

○ Ensure Legitimacy of Mass-Produced Devices

- Meters certificate issuance
- Controls production runs
- Eliminate rogue devices
- Prevents counterfeiting (genuineness)



0 1 2 3 4 5 6 7 8 9

12

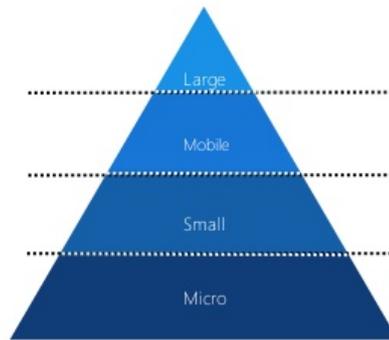
Step 2: Certificate Injection

○ Authenticate Identity of Manufactured Devices

- Establish root of trust and maintain secure configuration

Authentication Methods

PKI/RSA
 PKI/ECC
 Lightweight/Symmetric
 Password/None



IoT Device Type

POS terminal, ATM, MRI
 x86, PC-like, apps

Industry handheld, POS tablet
 ARM and x86, shell experience, apps

Gateways, wearables, panels, cars
 ARM and x86, diverse hardware, no shell

Controllers, fixed-use, sensors, actuators
 ARM, constrained hardware, headless

13



Step 3: Code Signing

○ Validate Integrity of Devices' Software/Firmware

- Verifies identity of software/firmware publishers
- Detects alteration or insertion of malicious code
- Protects end-user devices and their applications
- Safeguards bigger systems these are connected

○ Analogous to Tamper-Seals Used in Medications



14



Threat

- **More Software and Firmware Updated on a Regular Basis**
 - Typically happens in background
 - Automatic – middle of the night
- **These are ways for Attacks**
 - Provenance
 - Authenticity
 - Integrity
- **Biggest Consumer of Digital Certs.**
 - High tech manufacturing
 - Software development



Ponemon Institute 2019 Global PKI Trends Study



17

Step 4: Data Protection

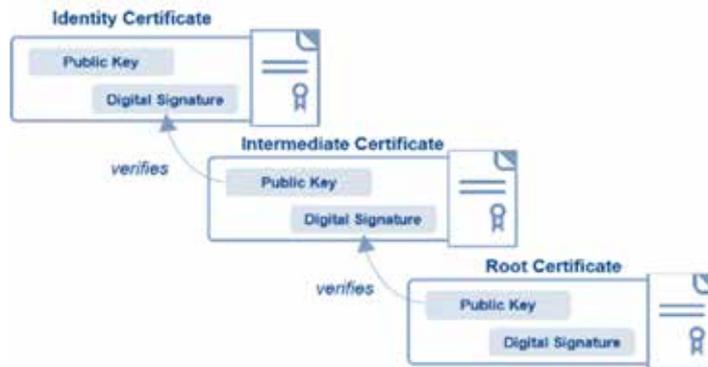
- **Safeguard Confidentiality/Integrity of Collected Data and Analytics**



18

Importance of a Root of Trust

- PKI Certificates are Based on Chain of Trust



If One Cannot Trust the Devices, It is Pointless to Analyze Data Collected

19



IoT Model and Why Trust is Critical

- Data collection



- If You can't Trust Devices



- Data Analytics



- It's Useless to Analyze Data



- Insight and Action



- Insight can be Questionable and your Action Misguided



20



The More Device Identifies you have...

○ The More Cryptographic Keys you have to Store and Manage

- Where are the keys located?
- Who controls the keys?
- Are the keys trusted?
- Would your process pass an audit?



21

Empowering Safe Use of New Technology

○ Authentication

Certificates as access tokens enables only approved devices to connect to your networks
 Only authorized users, messages, or servers have access to your device and their services
 PKI allows revocation which instantly blocks access in case of compromise or emergency

○ Integrity and Privacy

Devices use digitally signed messages to prove the origin of the data they collect
 Enable the detection of unauthorized device or data manipulation or interception
 Signed software/firmware enable secure downloads of ongoing software updates

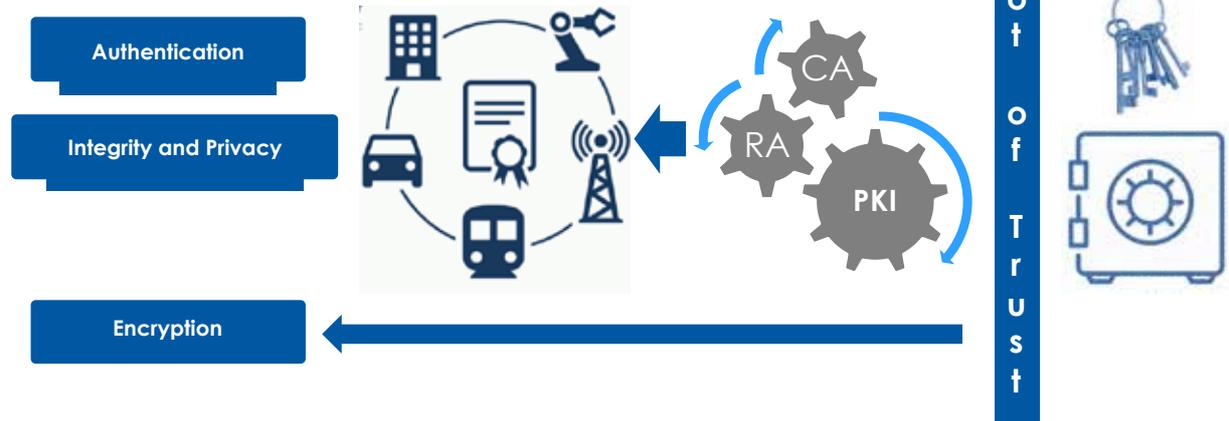
○ Encryption

Certificates enable protection of links between devices and services for secure transmission of data over TLS

22

Root of Trust

Establishing Trust and Reliable Security for IoT Devices



23

Value of Hardware Security

- Protect Enterprise PKI Root/Issuing CA Keys
- Secure Issuance and Validation of Identities
- Establish a Root of Trust for the Entire System
- Facilitate Compliance with Security Regulations

24

Hardware Security Modules

○ HSMs

- Specialized tamper-resistant equipment with cryptographic processing
- Lets you safeguard/manage your cryptographic keys and sensitive data

○ Serve as Root of Trust in Security Stack

- Generate encryption/signing keys
- Encrypt and decrypt data
- Store and protect keys
- Interface with/support applications

Over half (56%) of survey respondents* now rate the use of HSMs as very important

Ponemon Institute 2019 Global Encryption Trends Report

- Final sample of 4,802 practitioners from around the globe with bona fide credentials in IT/security fields

25

 CIPHER

In Summary...

- IoT Data-Centric Model Fueling Growth in PKIs
- Devices Must be Authentic and Software Valid
- Data Confidentiality/Integrity Must be Ensured
- Root of Trust Required to Protect Entire Systems
- PKIs Enable the Secure Use of New Technology



26

 CIPHER

nCipher Security



20+ Years of delivering trusted threat protection and enabling compliance



Deep expertise and track record in applied cryptography



HSM market leader with a long history of industry certifications and validation



**Trust
Integrity
Control**

**Cloud
IoT
Blockchain
Payments**

Solutions delivering trust for business critical applications and information



1000+

Organizations rely on nCipher to secure and globally support their applications and information

- 5 of the top 10 Fortune 100
- 10 of the top 20 FTSE 100

27

nCipher – securing the industry’s leading solution providers

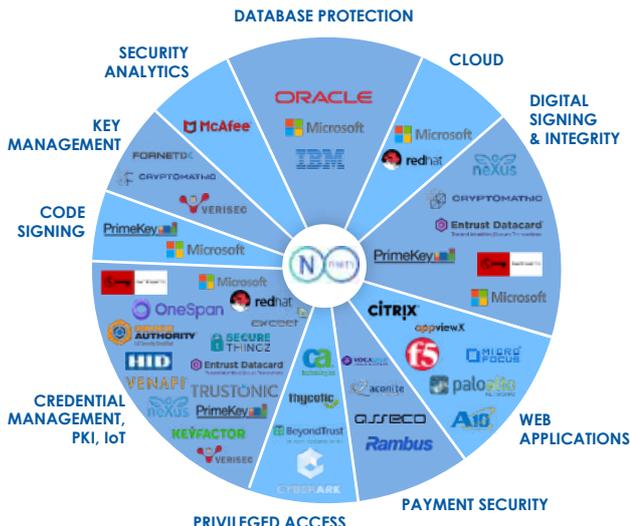


Strategic technology partner program

Integrations with growing ecosystem of over 100 security solution providers

Delivers value and enhanced security to end customers by hardening partner solutions with certified, hardware-based cryptography

Mature, proven processes backed by technology expertise and global coverage ensure the strongest customer support



The diagram is a circular hub-and-spoke model. At the center is the nCipher logo. Surrounding it are ten security categories, each with a list of partner logos:

- SECURITY ANALYTICS:** McAfee, Microsoft, IBM
- DATABASE PROTECTION:** Oracle, Microsoft, IBM
- CLOUD:** Microsoft, redhat, nexus
- DIGITAL SIGNING & INTEGRITY:** Cryptomathic, Entrust Datacard, PrimeKey, Red Hat
- KEY MANAGEMENT:** ForNED, Cryptomathic, Verisec, PrimeKey, Microsoft
- CODE SIGNING:** Microsoft, OneSpan, redhat, citrix, appviewX, Microsoft
- WEB APPLICATIONS:** Citrix, appviewX, Microsoft, Palo Alto, AIO
- PAYMENT SECURITY:** Citrix, appviewX, Microsoft, Rambus
- PRIVILEGED ACCESS:** Citrix, appviewX, Microsoft, BeyondTrust
- CREDENTIAL MANAGEMENT, PKI, IoT:** Venafi, Trustonic, PrimeKey, Microsoft, Verisec, Entrust Datacard, SecureTrinize, HID, OneSpan, redhat, citrix, appviewX, Microsoft

28

Questions?

THANK YOU

Bernd Stamp, CISSP
Technical Lead DACH – Solutions Consultant
Bernd.Stamp@ncipher.com

29

