nCIPHER

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

Bernd Stamp
Solutions Consultant – Technical Lead
June 2019

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

PKI – Introduction

Foundational Building Block

- Hardware
- Software
- Procedures
- Processes

Secure Mechanism

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

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**

nCIPHER

Credentialing and Identity

Identities Forms the Basis of Trust

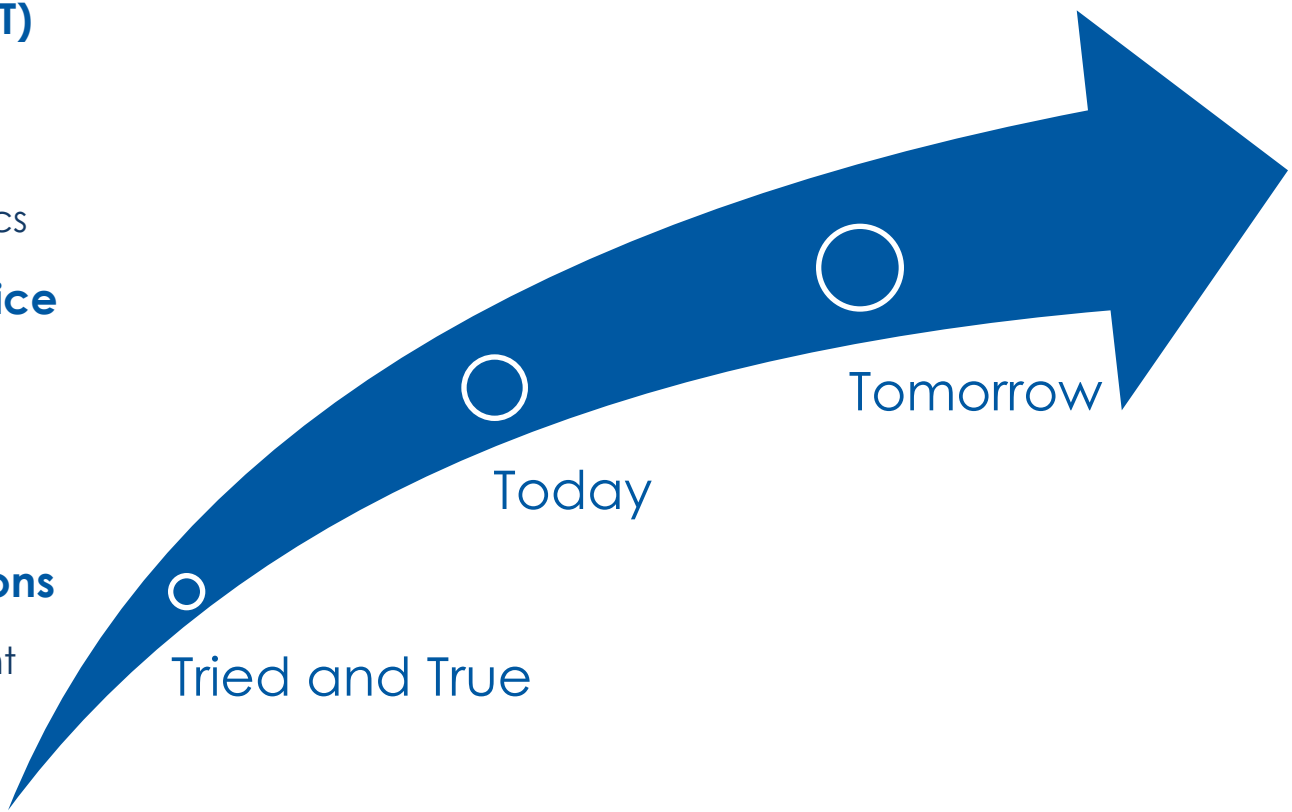
nCIPHER

Legacy:

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

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



nCIPHER

Growing Demand for Certificates

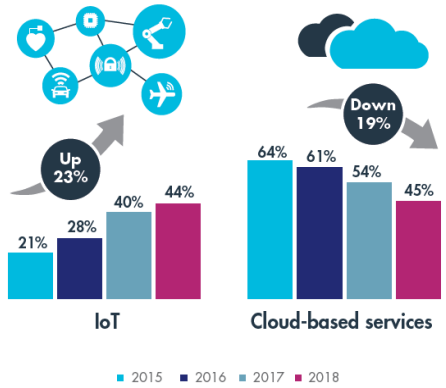
Ponemon Institute PKI Trends Study

- Reveals growing demand for digital certificates

Survey results from 1,688 respondents in 12 countries

The Rise of the IoT

The IoT is the fastest growing trend driving the deployment of applications that use PKI



APPLICATIONS THAT MOST COMMONLY USE DIGITAL CERTIFICATES

nCIPHER

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 2018 Global PKI Trends Study

CIPHER

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

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

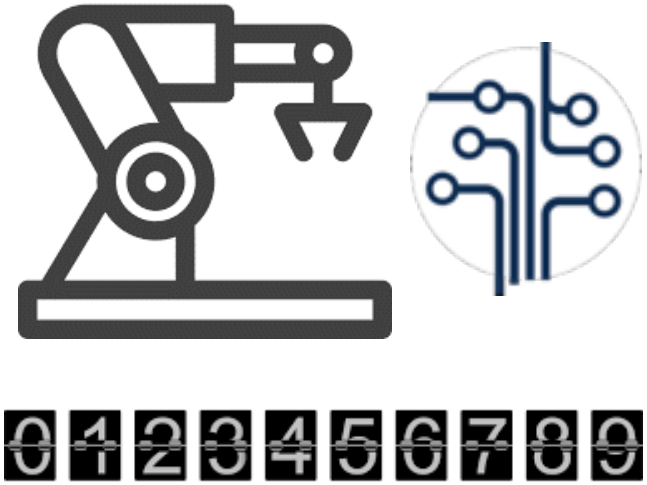
   Safeguard confidentiality and integrity

nCIPHER

Step 1: Production Control

O Ensure Legitimacy of Mass-Produced Devices

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



Step 2: Certificate Injection

Authenticate Identity of Manufactured Devices

- Establish root of trust and maintain secure configuration

Authentication Methods

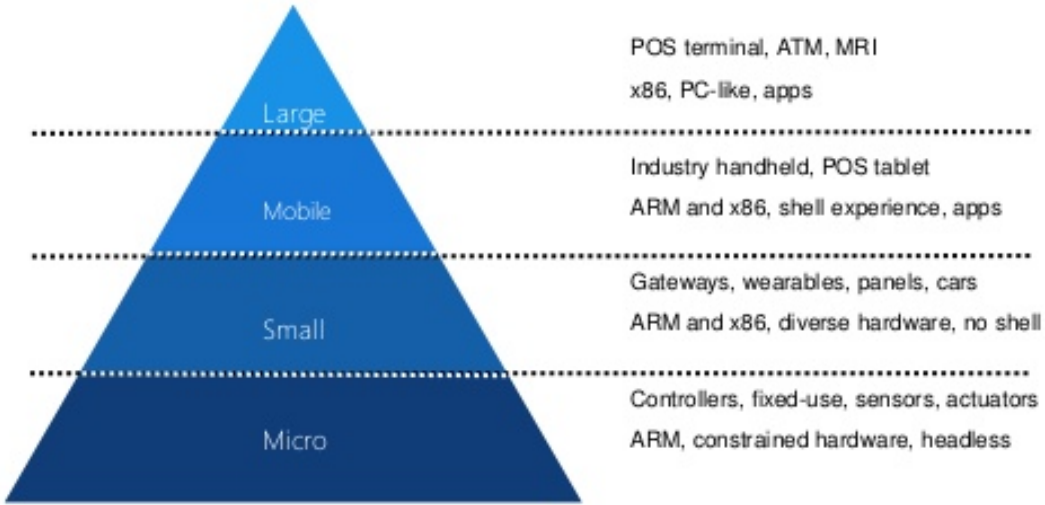
PKI/RSA

PKI/ECC

Lightweight/Symmetric

Password/None

IoT Device Type



nCIPHER

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

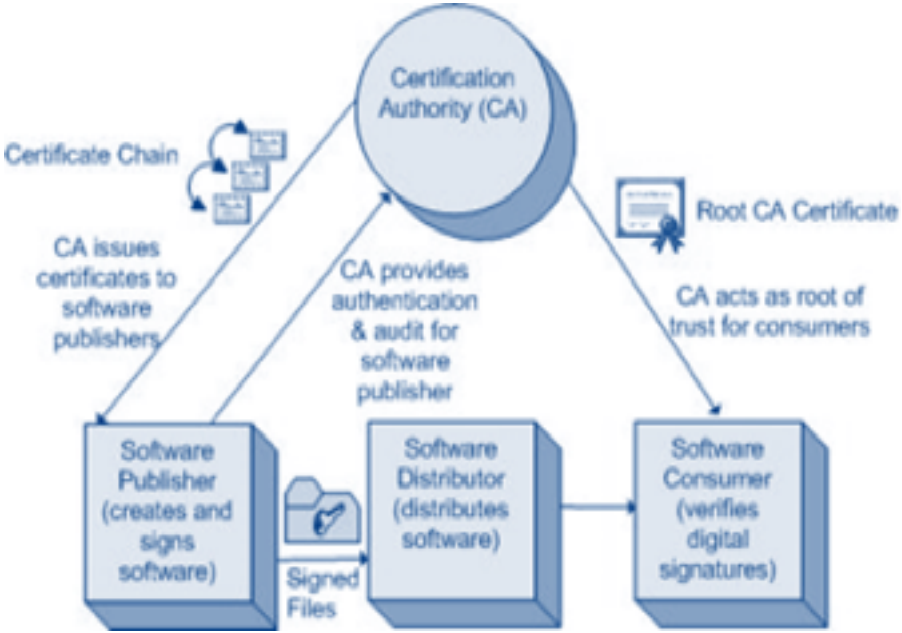
Analogous to Tamper-Seals Used in Medications

nCIPHER

Code Signing (continued)

How it works?

- Public/private key pair created (PKI)
- Certificate, including public key and associated identification, obtained from Certification Authority (CA)
- Private key used to "hash" software



nCIPHER

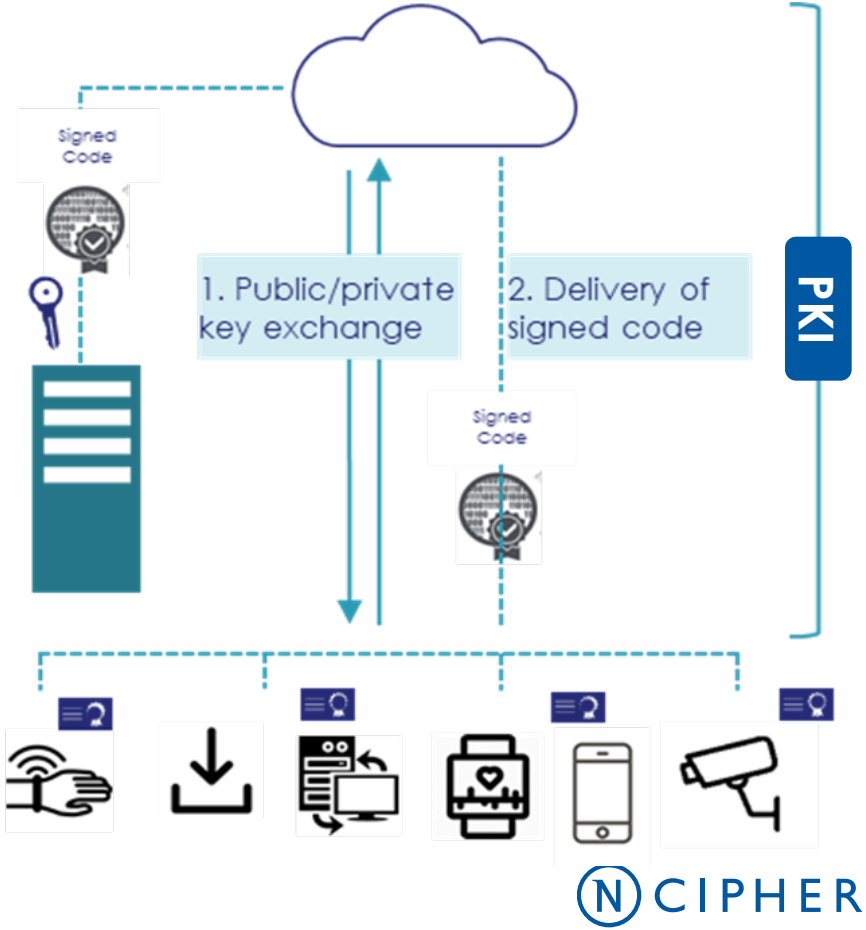
Code Signing (continued)

How it works?

- Public/private key pair created (PKI)
- Certificate, including public key and associated identification, obtained from Certification Authority (CA)
- Private key used to "hash" software

Security of Private Key is Critical

- Private keys sign all certificates
- Must never be revealed/shared
- If compromised, trust system fails



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 2018 *Global PKI Trends Study*

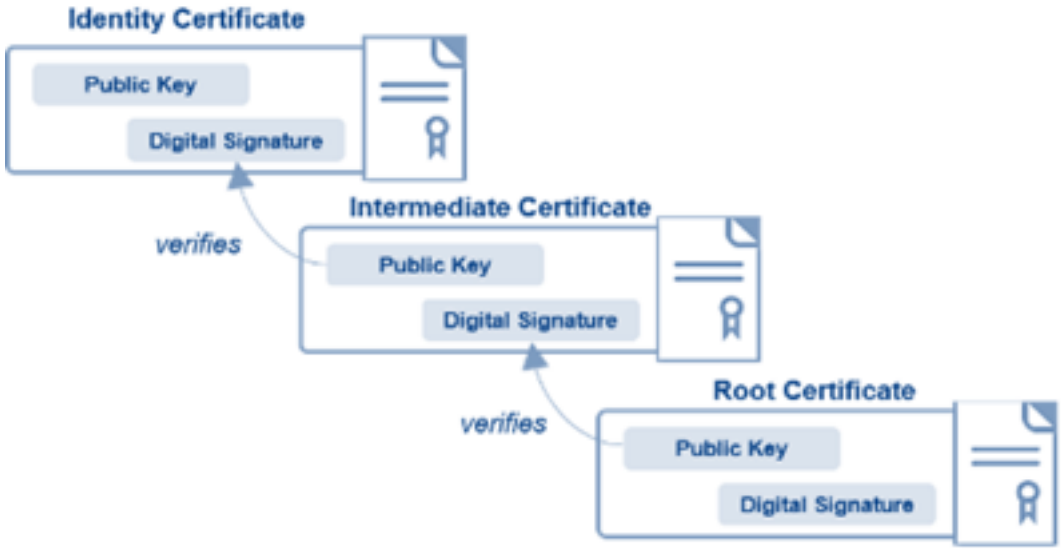
Step 4: Data Protection

- Safeguard Confidentiality/Integrity of Collected Data and Analytics

Devices **IoT Hubs** **Big Data Algorithms** **Outcomes**

Importance of a Root of Trust

O PKI Certificates are Based on Chain of Trust



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

nCIPHER

IoT Model and Why Trust is Critical

- Data collection

- Data Analytics

- Insight and Action

- If You can't Trust Devices

- It's Useless to Analyze Data

- Insight can be Questionable and your Action Misguided

The More Device Identities 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?

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

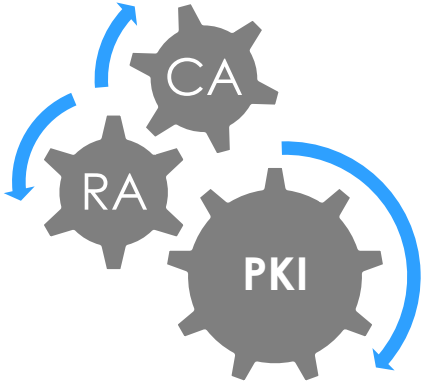
Certificates enable protection of links between devices and services for secure transmission of data over TLS

Root of Trust

Establishing Trust and Reliable Security for IoT Devices

Authentication

Integrity and Privacy



Encryption

Root of Trust

NCIPHER

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

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 2018 *Global Encryption Trends Report*

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

nCIPHER

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

nCIPHER

Questions?

THANK YOU

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

nCIPHER