



Can This Code Be Trusted? Why Code Signing is Essential for IoT

Stephen Helm
Senior Product Marketing Manager

PCI Bridge/pci-ata@1/CRD...
Driver/IOATABLockStorageDevice/IOBlockStorageDevice/...

Gemalto's Purpose

We enable our clients to deliver a vast range of **trusted digital services** for billions of individuals and things across the globe



We are the world leader in digital security



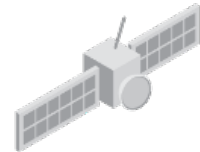
WE'RE UNIQUE. WE'RE GLOBAL. WE'RE INNOVATIVE

- ✦ Internet of Things 101
- ✦ What Makes IoT Different?
- ✦ History of Relevant Cyber Attacks
- ✦ Code Signing Basics
- ✦ Why is Code Signing Important in IoT?
- ✦ The importance of key security
- ✦ Questions!

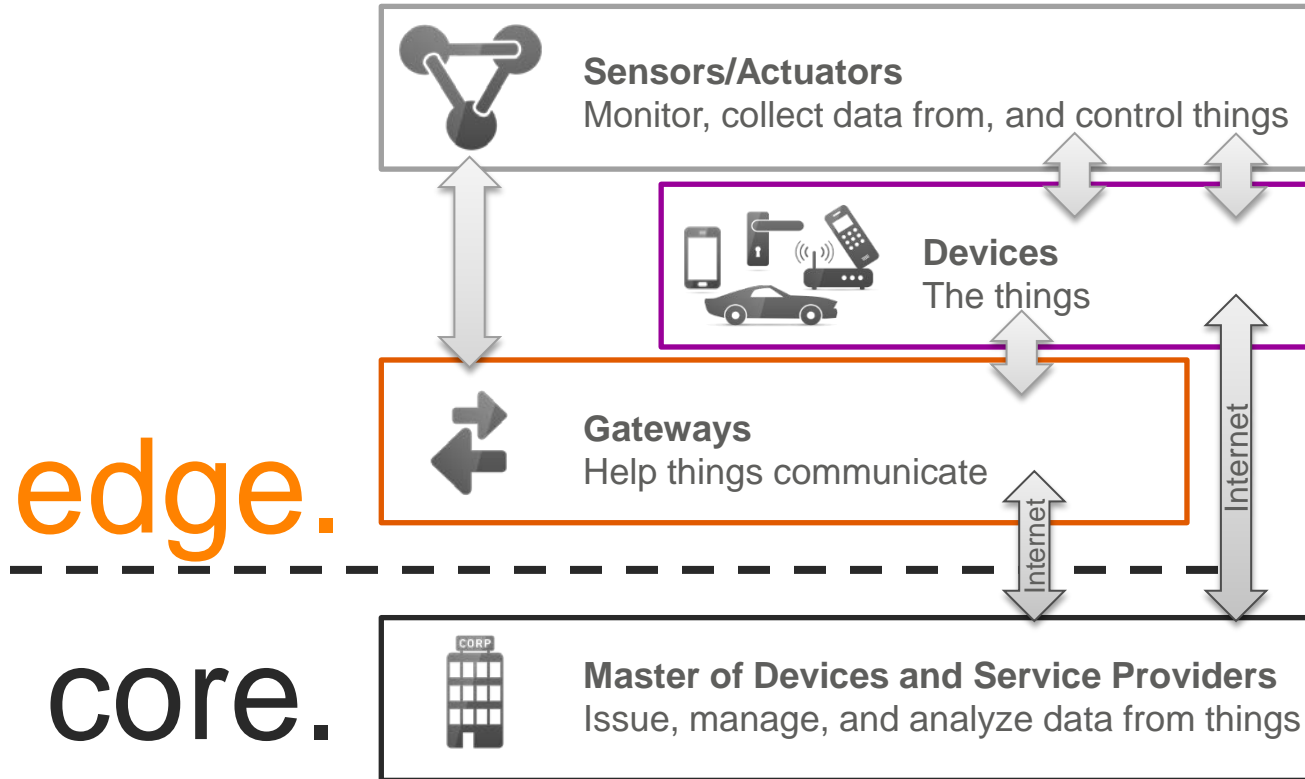
A woman with dark hair, wearing a grey blazer over a white collared shirt, is standing in an office environment. She is looking towards the camera with a slight smile. The background shows office windows and ceiling lights.

Agenda










- The **Internet of Things (IoT)** is the interconnection of **uniquely identifiable** embedded computing devices within the **existing Internet infrastructure**.
- **Machine to Machine (M2M)** refers to technologies that allow both wireless and wired systems to **communicate with other devices of the same type**. M2M is considered **an integral part of the Internet of Things**.



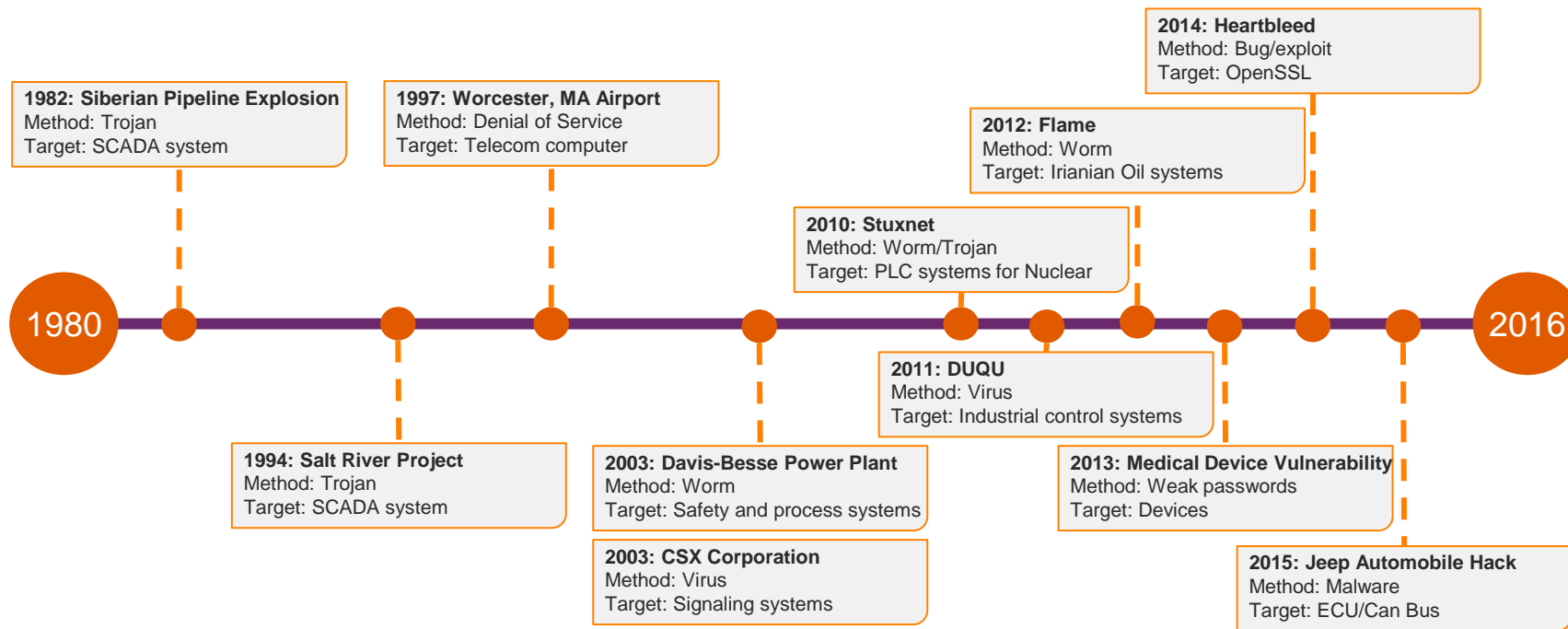
Elements of the Internet of Things



What Makes IoT Different?

| | | |
|------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <p>It's everywhere...</p>  | <p>...so is the data..</p>  | <p>...and so are the threats.</p>  |
| <p>It's built on the cloud...</p>  | <p>...is thin by design...</p>  | <p>...and uses new communication tech.</p>  |
| <p>It's collects sensitive personal data...</p>  | <p>...that must be encrypted...</p>  | <p>...with smaller, more efficient keys/certs.</p>  |

Brief History of Relevant Attacks



Top Cyber Security Myths about the Smart Grid

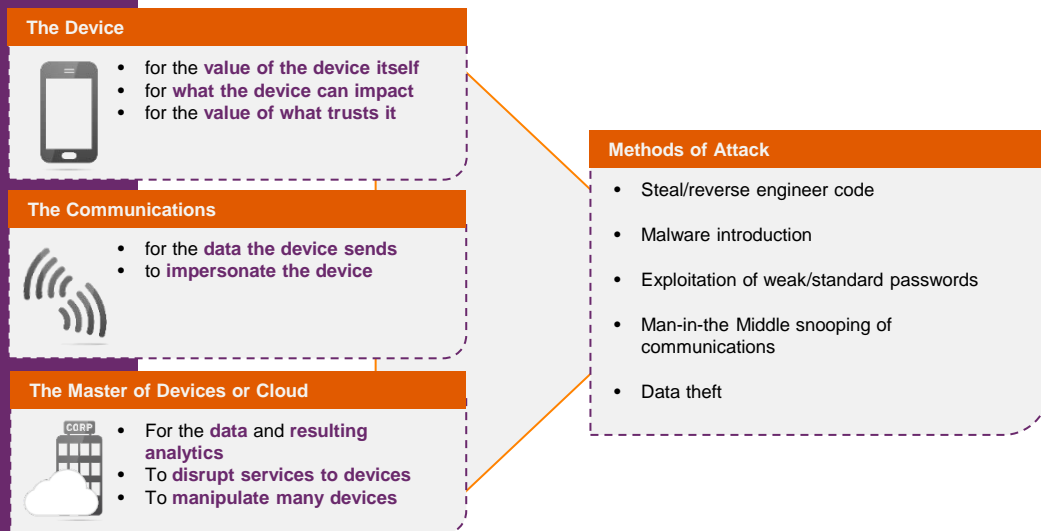
1. “Industrial Control Systems are isolated.”
2. “Nobody will want to attack us.”
3. “Utilities only use obscure protocols/systems.”
4. “Social engineering is not an issue.”
5. “It’s Encrypted: It’s Protected”

Source: IEEE TRANSACTIONS ON POWER DELIVERY, VOL. 26, NO. 1, JANUARY 2011

“One utility reported that it was the **target of approximately 10,000 attempted cyberattacks each month.**”

“More than one public power provider reported being **under a “constant state of ‘attack’ from malware and entities seeking to gain access to internal systems.”**”

Source: Electric Grid Vulnerability: Industry Responses Reveal Security Gaps.



Code Signing **protects the devices we use every day.** From games to airplanes, fridges to bridges, satellites to street lights, **code signing is everywhere.**

What is Code Signing?

Code Signing **uses digital certificates and Public Key Infrastructure** to associate code with a publisher, and provide assurances that the **code has not been modified or tampered** after the signing process.

Code Signing ensures:

- Code comes from an authentic source
- Code hasn't been altered

The Role of Keys in Code Signing



- Used a means of attaching a publishers identity to code.
- Must be kept secret!



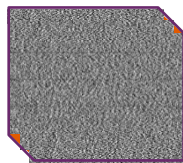
- Used to verify the identity/source of code.
- Security not an issue.

```
Original Code (Source Code)
```

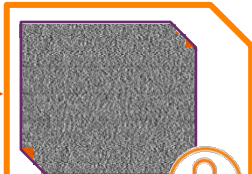
Hash Function

```
Hash (Hexadecimal String)
```

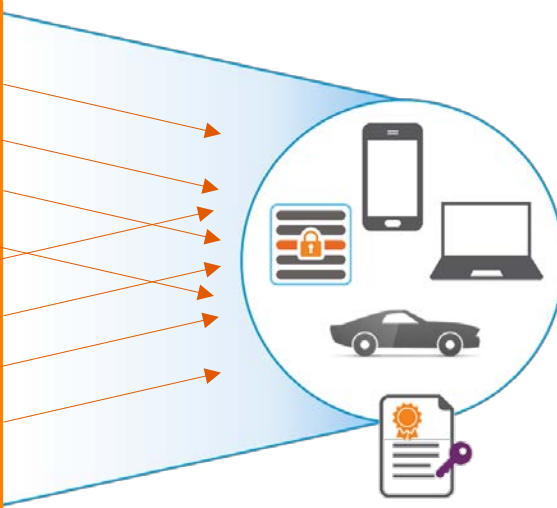
Encrypt Hash with Private Key

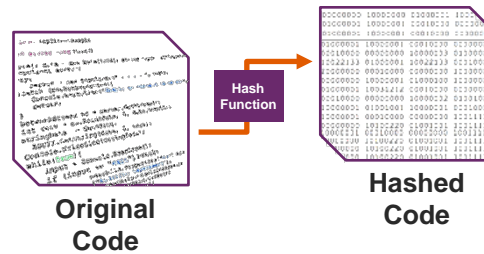
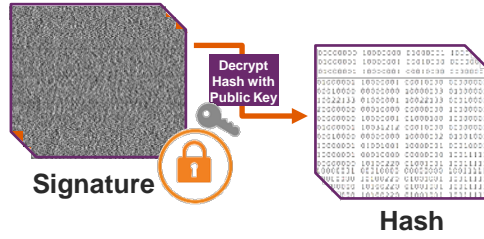


Time Stamp



Original Code (Source Code)





hashes match = code origin verified

What Code Signing Isn't...

Code Signing...

- Doesn't ensure code is free from bugs
- Doesn't ensure code is up-to-date or supported.
- Doesn't guarantee that code is safe to use.

Why is Code Signing Important in IoT?

A look at the connected car

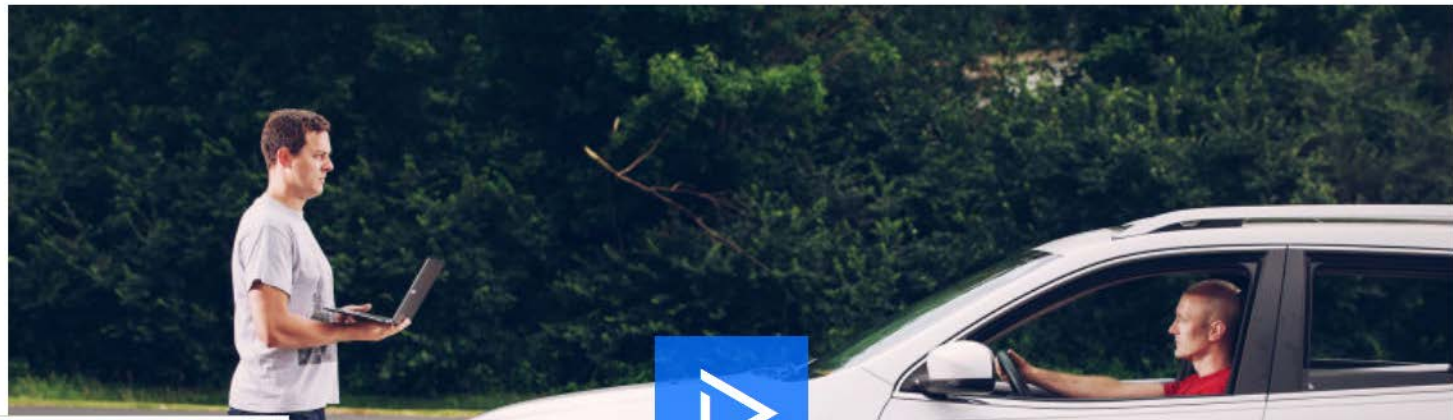
“Where once cars could be defined as a collection of mechanical and electrical parts, **the modern automobile relies on more code than the Space Shuttle**. Hundreds of millions of lines of code facilitate **everything from environmental controls and infotainment, to lane detection and safety features.**”

Dangers of Allowing Unsigned Code

“There's no *code signing*; you can update the chip, no questions asked...”

ANDY GREENBERG SECURITY 07.21.15 6:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT



The Threat of Signed Malware

RISK ASSESSMENT / SECURITY & HACKTIVIS







To bypass code-signing checks, malware gang steals lots of certificates

Legitimate code-signing certificates provide secret cover for attack groups.

by Dan Goodin | Mar 16, 2015 8:44am PDT

Sony Left Passwords, Code-Signing Keys Virtually Unprotected

By Robert Lemos | Posted 2014-12-10 

 Tweet  LinkedIn 47  Like 31  Share 5  Share 78  Email

Researchers reportedly find hundreds of code-signing keys

Symbian Signing Key Reportedly Stolen From Nokia Could have Enabled Powerful Malware

Someone blackmailed Nokia in 2007 by threatening to leak a digital key the company used to sign Symbian applications, a news report says

    MORE 

By Lucian Constantin | Follow
IDG News Service | Jun 18, 2014 8:00 AM PT

D-LINK ACCIDENTALLY LEAKS PRIVATE CODE-SIGNING KEYS

by Michael Mimoso 

September 18, 2015, 10:21

A simple mistake by networking gear manufacturer D-Link could have opened the door for costly damage.

DAILY TECH NEWS SHOW

The Risk to Apple's Code-Signing Key

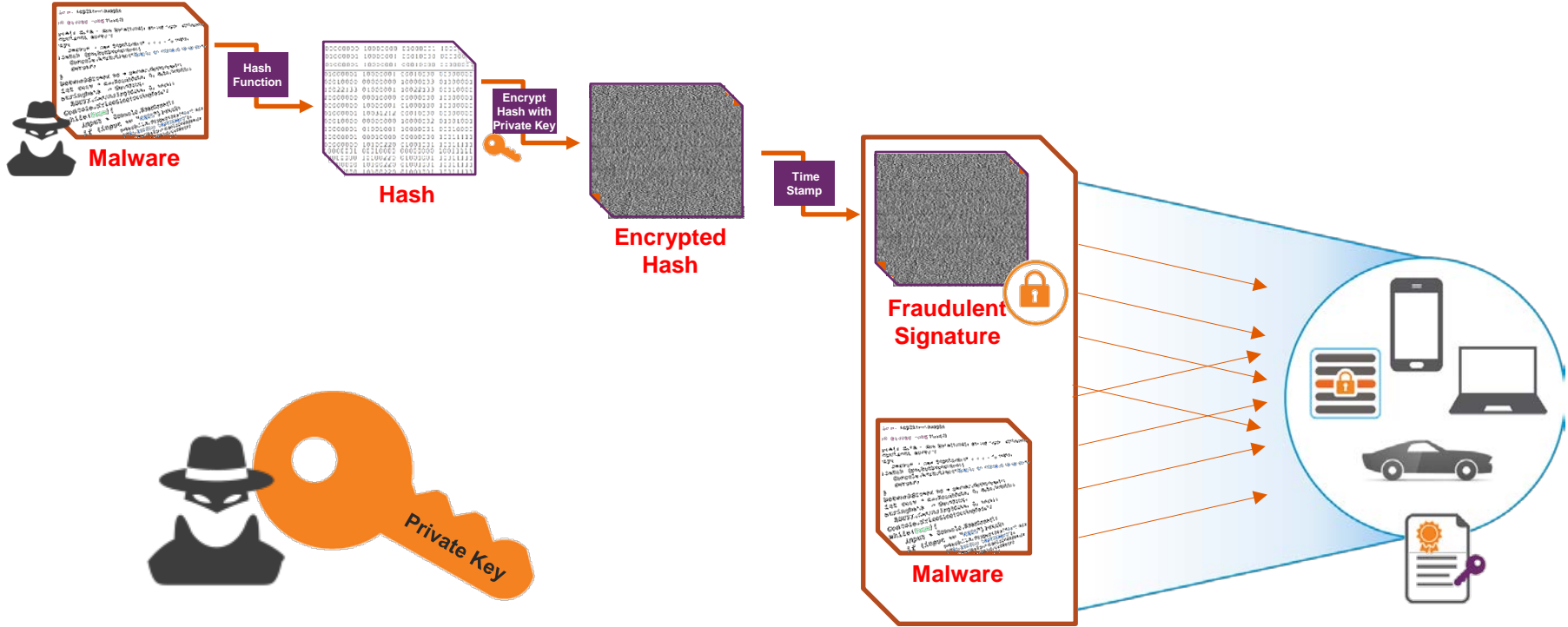
by Tom on March 2, 2016 • 0 Comments

One Security can is it

Stuxnet-style code signing of malware becomes darknet cottage industry

Even reports of crims offering signing-as-a-service





“With today’s signature verification tools, and with hardware support for secure boot improving, the next **challenge for many companies is “managing the keys,” and “controlling access to the keys” for code signing** and protection of embedded software.”

Key Statistics



86%

of CIOs believe keys and certificates are the next big hacker marketplace.

Source: 2016 CIO STUDY RESULTS – VansonBourne and Venafi



23k

average # of keys and certificates in an enterprise

Source: 2016 CIO STUDY RESULTS – VansonBourne and Venafi



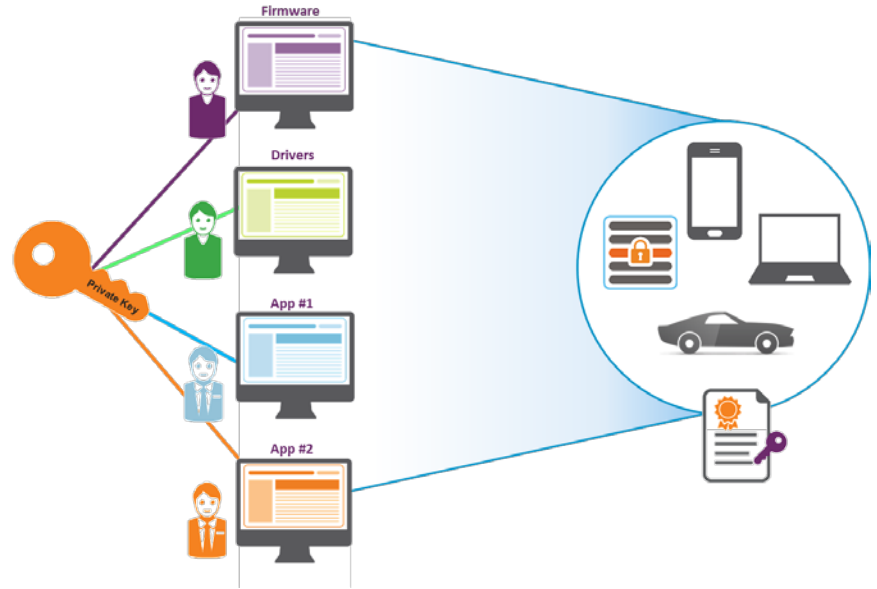
85%

of CIOs expect criminal misuse of keys and certificates to get worse

Source: 2016 CIO STUDY RESULTS – VansonBourne and Venafi

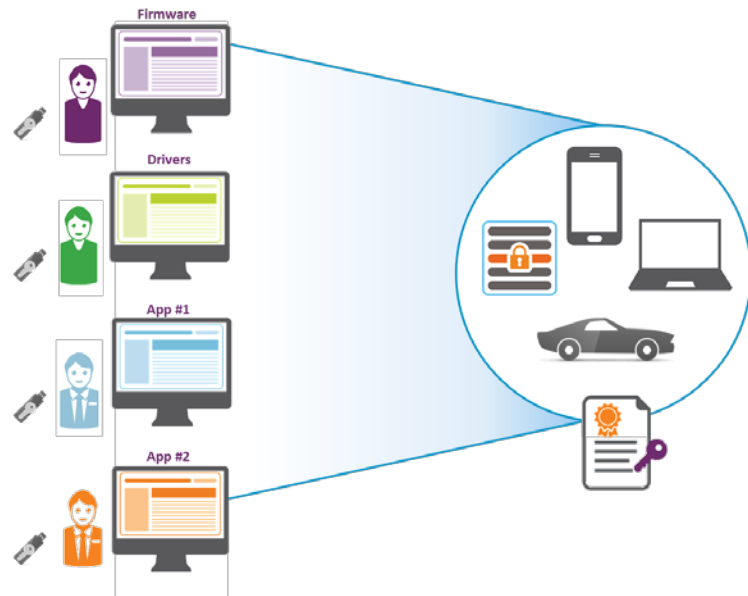
Private Keys Stored on Workstations

- ✓ Simple and easy!
- ✗ Single key for multiple/many signing needs.
- ✗ Storing private keys on workstations isn't secure.
- ✗ No way to audit the use of keys. Who signed what/when/where?



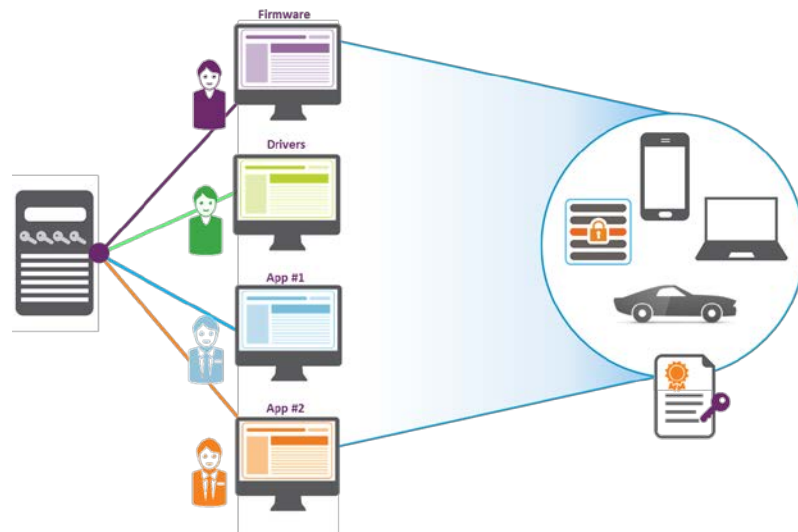
Private Keys Stored on Tokens/Smart Cards

- ✓ Still fairly simple and easy.
- ✓ One or more keys for multiple/many signing needs.
- ✓ Storage of private keys on a Token enhances security.
- ✗ Limited ability to audit key usage and who signed what/when/where.



Private Keys Stored on Signing Server

- ✓ Signings must be requested/submitted to a signing server/authority.
- ✓ One or more keys for multiple/many signing needs stored centrally.
- ✗ Controlling signing operations through centralization enhances security, but keys are left insecure.
- ✗ Able audit who requested to sign what/when/where, but insecure keys mean you don't know when fraudulent signings occur.



What is a Hardware Security Module?

dedicated processor

for cryptographic operations

source of random numbers

with a high level of entropy

root of trust

designed for the protection of the crypto key lifecycle

flexible crypto solution

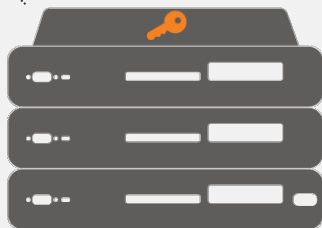
that implements the algorithms you want to use

key vault

for holding sensitive cryptographic keys

validated for security

by third-parties



Who Uses HSMs?



Large Enterprise



Government



Financial and Payments



Utilities



Telecom



Retail



Transportation



Healthcare



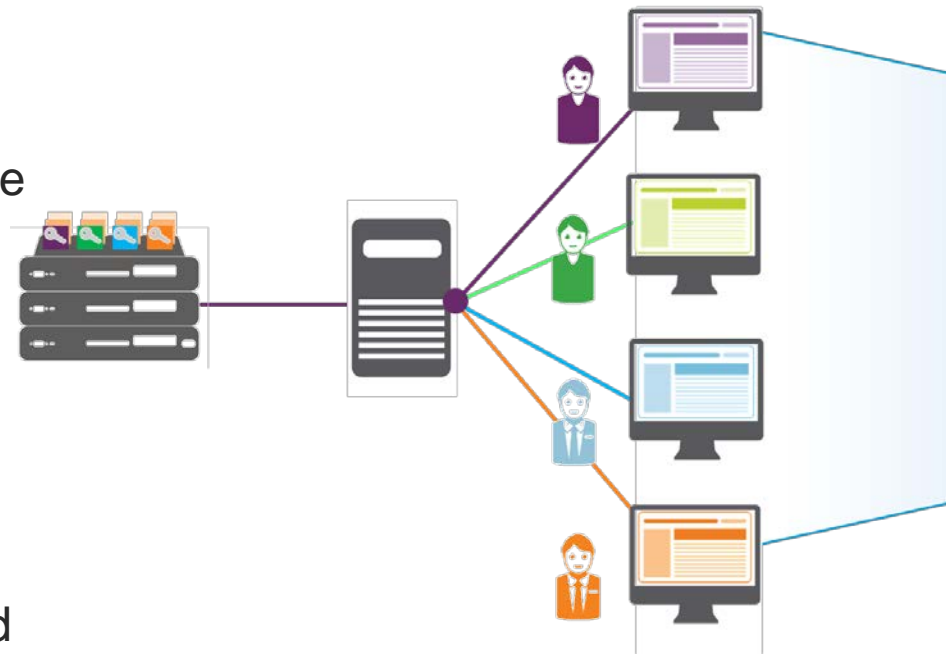
Cloud/App. Providers

And Many More!

gemalto

Private Keys Stored on HSM

- ✓ Signings must be requested/submitted to a signing server/authority.
- ✓ One to many thousands of keys are stored in an high-assurance Hardware Security Module.
- ✓ Keys stored securely --and all signing operations occur --within the physical and logical boundary of the FIPS 140-2 validated HSM
- ✓ Trusted audit, including signed and time stamped logs of key usage and who signed what/when/where.



Code Signing Best Practices

- **Use Hardware.** Hardware is best way to ensure access to the keys is reduced. Keys for code signing should be generated within a hardware device and have policy which denies exportation or misuse.
- **Centralize.** This keeps the ownership of the keys in one central geographic region for ease of management and compliance. Also gives an easy way of authenticating the request to sign code and log all signing operations for auditing purposes.
- **Timestamp.** Timestamping is the process of attaching a signed timestamp to a code signing signature. This ensures that the certificate was valid at the time the signing operation took place.

Thank you! Questions?