RSAConference2015
Abu Dhabi | 4–5 November | Emirates Palace

CHANGE
Challenge today's security thinking

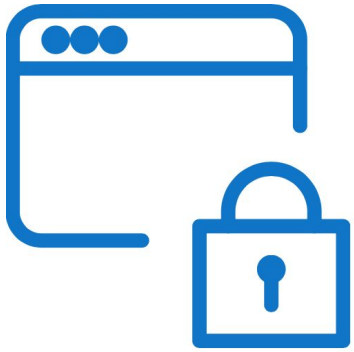
SESSION ID: **SSC-R05**

Maximum Overdrive: Death by Your Microwave

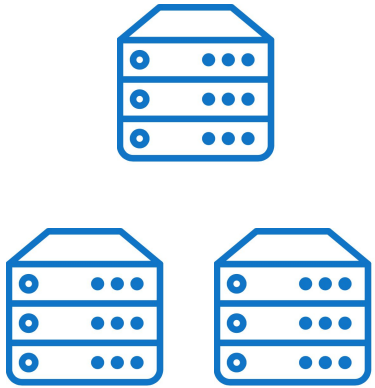
(How to Solve the Insecurity in the Internet of Things)

Dan Timpson

Chief Technology Officer
DigiCert, Inc.
@danno_t | @digicert



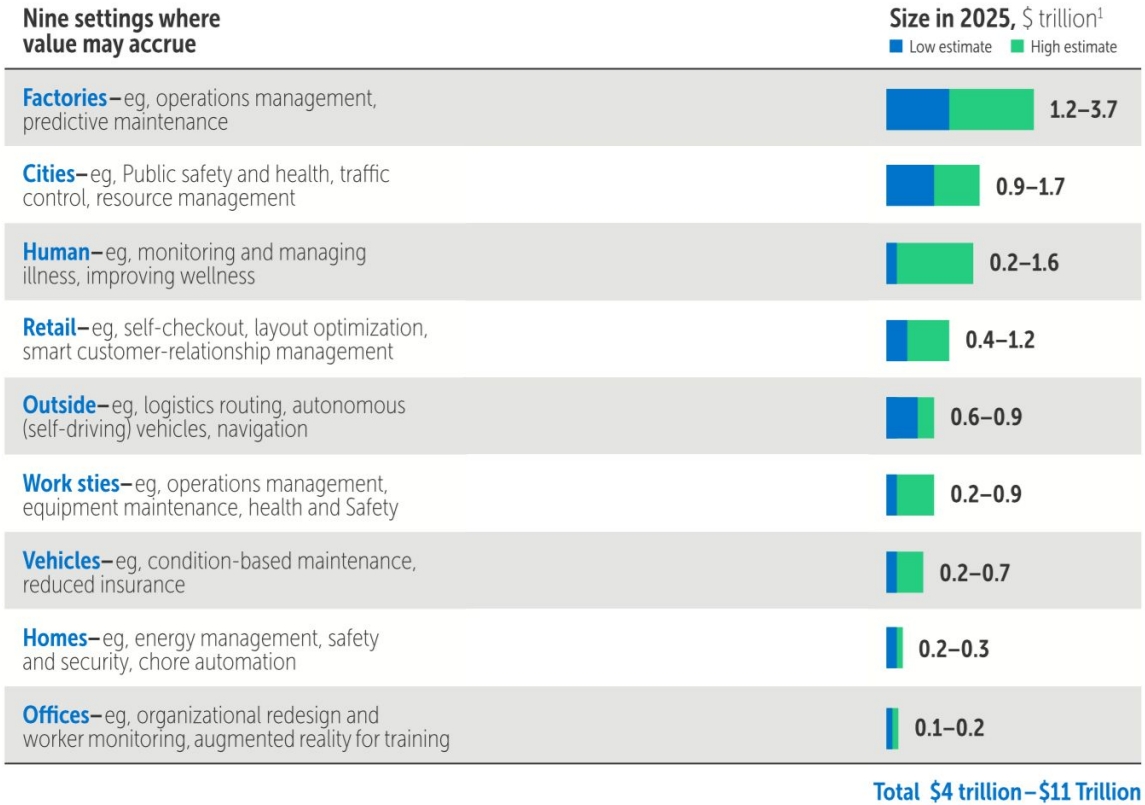
2000



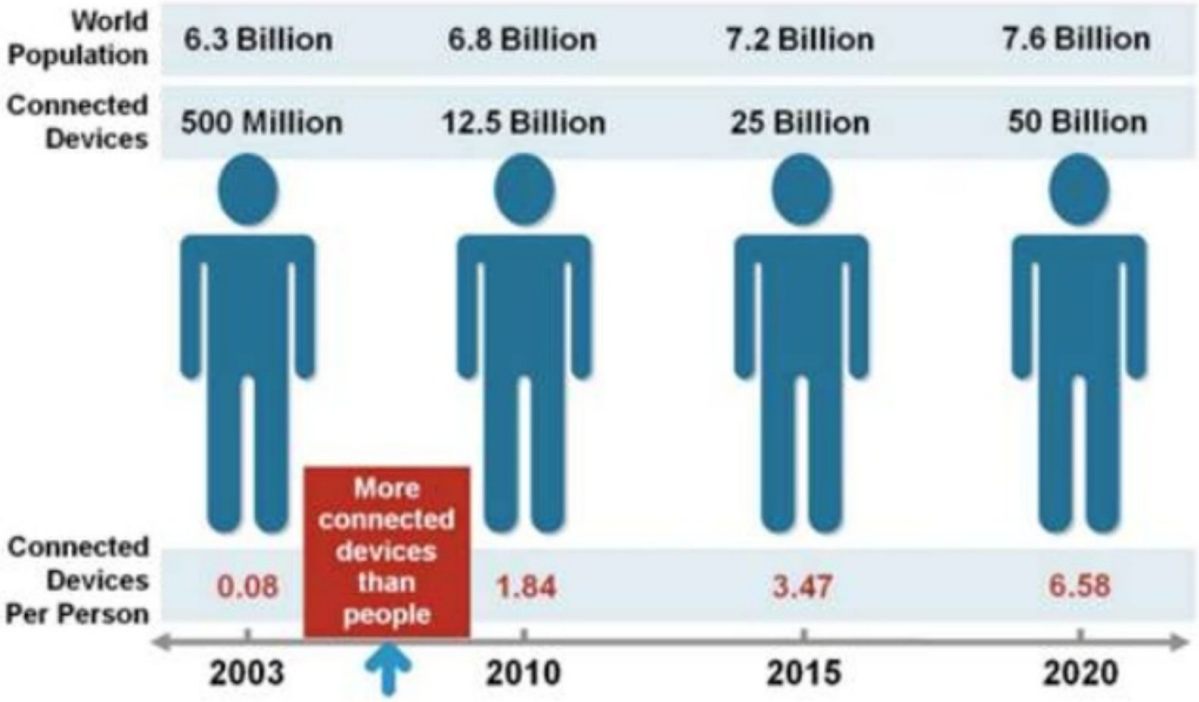
2007

2015

$11 Trillion Economic Impact by 2025

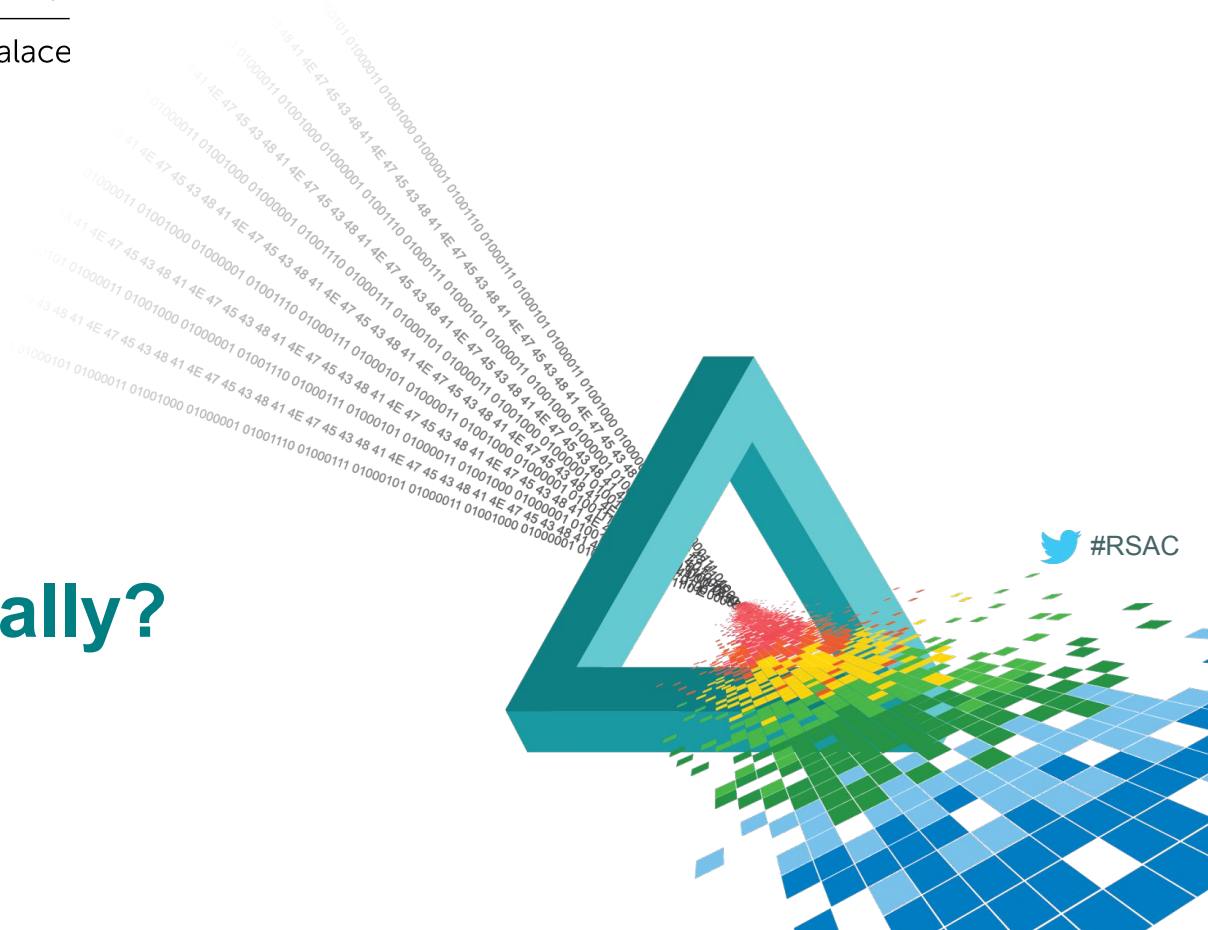


More Devices Than People



Source: Cisco IBSG, April 2011

A Microwave? Really?



Software Vulnerabilities = #FAIL

- Hackers gain access by exploiting weaknesses in Internet-connected systems
- All software is a **target**!
- **Threat** - May be able to harm tens of thousands of people at once depending on the platform

1982 Trans-Siberian Pipeline Explosion

- …in 1982 tampered pump/turbine control software caused a 3 kiloton explosion in the Trans-Siberian pipeline;
- …and that was before we had billions of microcontrollers. I'm not sure we'll ever have a 35 kiloton "nuclear" event like the picture

2008 Pipeline Disruption in Turkey

- The hacker's point of entry was an unexpected one: the surveillance cameras themselves.
- Hackers had shut down alarms, cut off communications and super-pressurized the crude oil in the line.

2014 German Steel Mill - Blast Furnace Attack

- **A blast furnace at a German steel mill suffered "massive damage" following a cyber attack on the plant's network**
- …that went through a gateway from “IT” networks to plant/production floor “operational” systems.
- It said attackers used booby-trapped emails to steal logins that gave them access to the mill's control systems.

2015 Hospital Medical Devices Hacked

- Earlier this month a security firm disclosed that Three hospitals had been
- …breached through vulnerabilities in their medical devices.
- …These devices ranged from MRI machines to Blood Gas Analyzers.
- Another security professional saw an MRI machine crash from a simple port-scan.
- …an MRI machine accessible from Guest Wifi, where anyone could've crashed the machine.

2015 Wireless Carjackers

- “They disabled my brakes, honked the horn, jerked the seat belt, and commandeered the steering wheel.”
- [Hacked] into the vehicles’ onboard diagnostic port, a feature that normally gives repair technicians access to information about the car’s electronically controlled systems

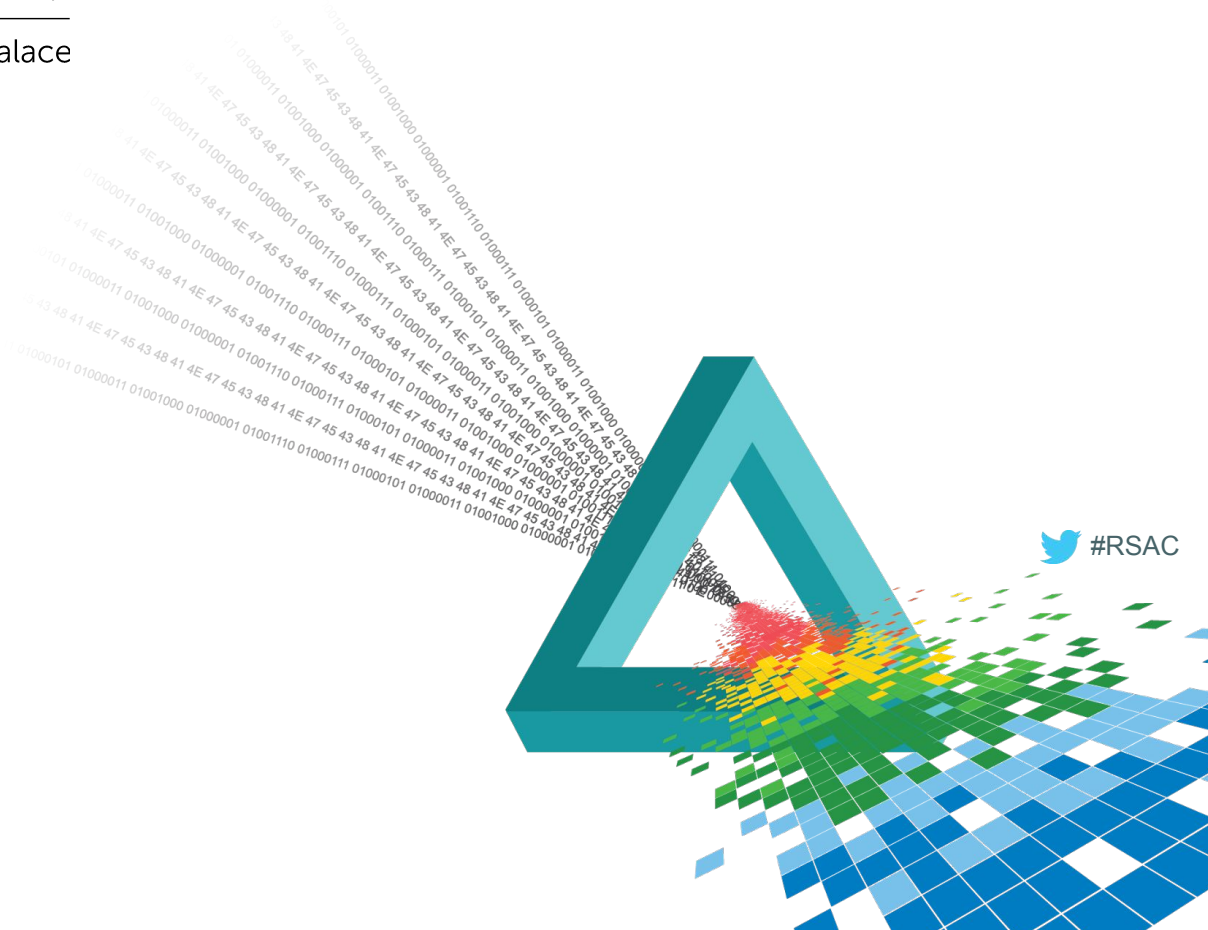
2015 Hackers Change Rifle Target Remotely

- Security researchers Runa Sandvik and Michael Auger hack a $13,000 TrackingPoint self-aiming rifle.
- Vulnerabilities enable changes of variables in the scope's calculations that make the rifle inexplicably miss its target, permanently disable the scope's computer, or even prevent the gun from firing.

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

Building Trust



#RSAC

The security vs. usability continuum

- Maximum usability and zero security

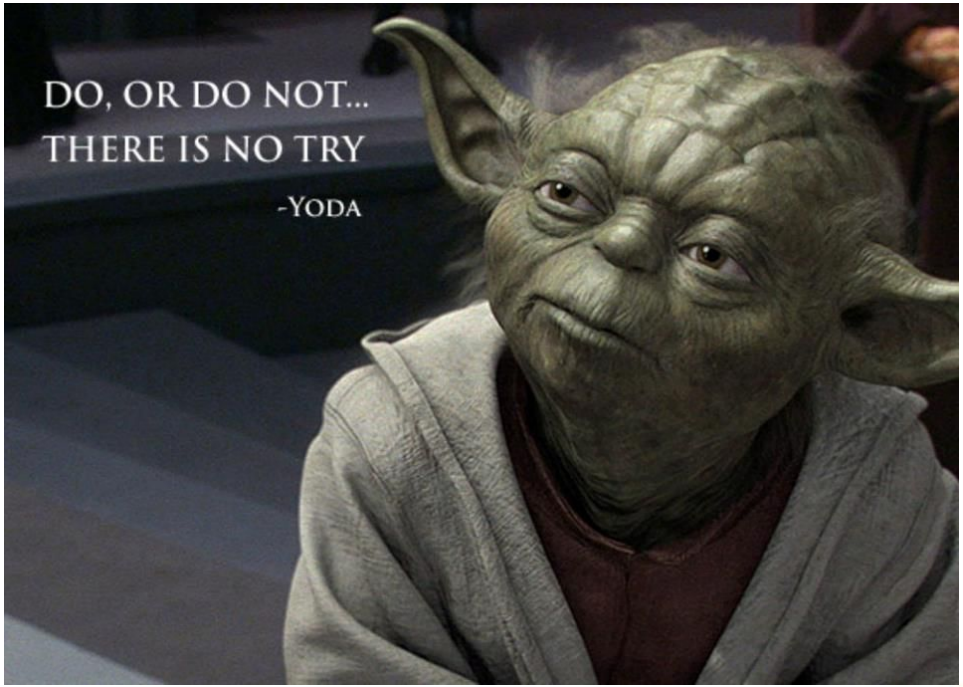
vs.

- Maximum security and zero usability

- **Key:** Find the balance between functionality and security

De-Fragmenting Security in IoT

- Connectivity Standards
- Operating Systems
- Network Topologies
- Security Frameworks



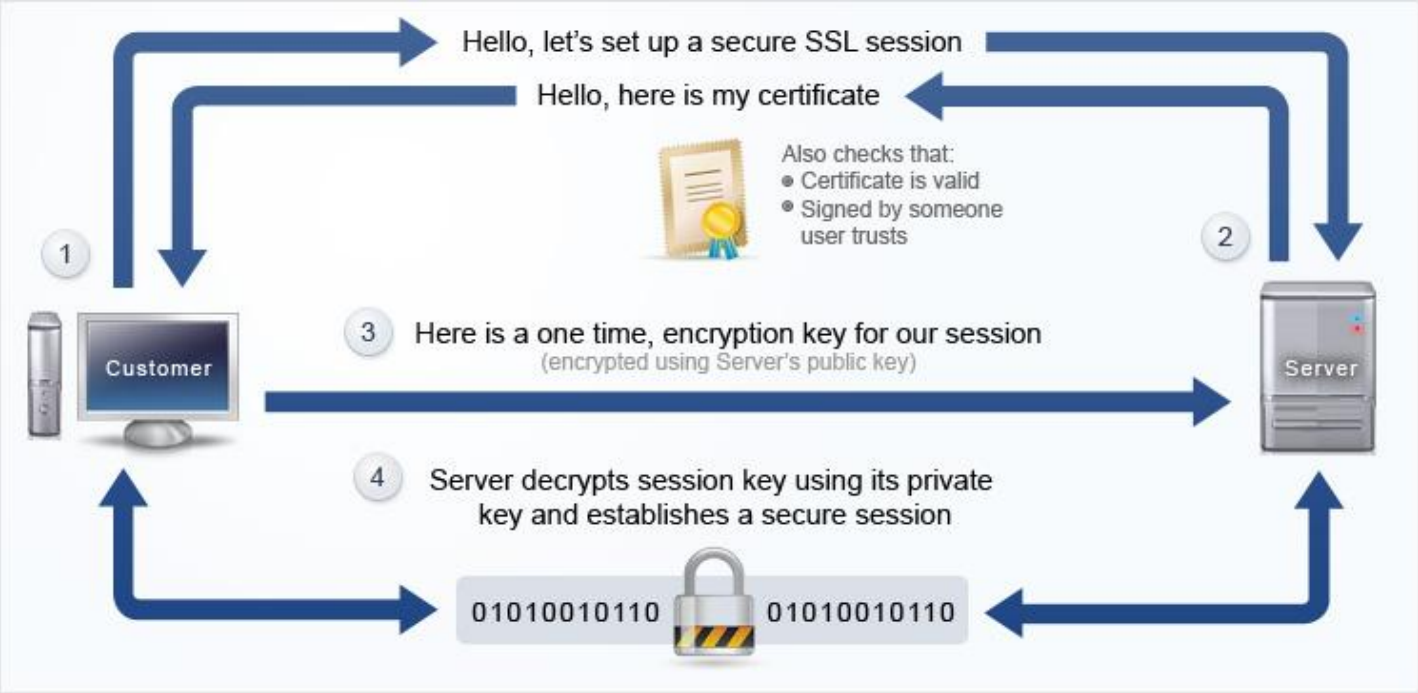
In Technology We Trust?

- **Technology does not trust by default**
  - Framework - 3 leg Stool
    - Software/Tech.
    - Policy & Procedures
    - Relationships & Liability

IoT Frameworks We Can Trust

- **What is Trust?** - Confidence or assurance that a person, system, thing will behave exactly as you expect, or alternatively, in your best interests
- **Trust cannot be established by technology alone**
  - PKI is a good example. *"I" stands for infrastructure*
- **Communities to watch**
  - OTA IoT Trust Framework
  - AllSeen Alliance (AllJoyn)
  - Securemedicine.org

Traditional PKI Implementation



PKI for IoT?

Proven past:

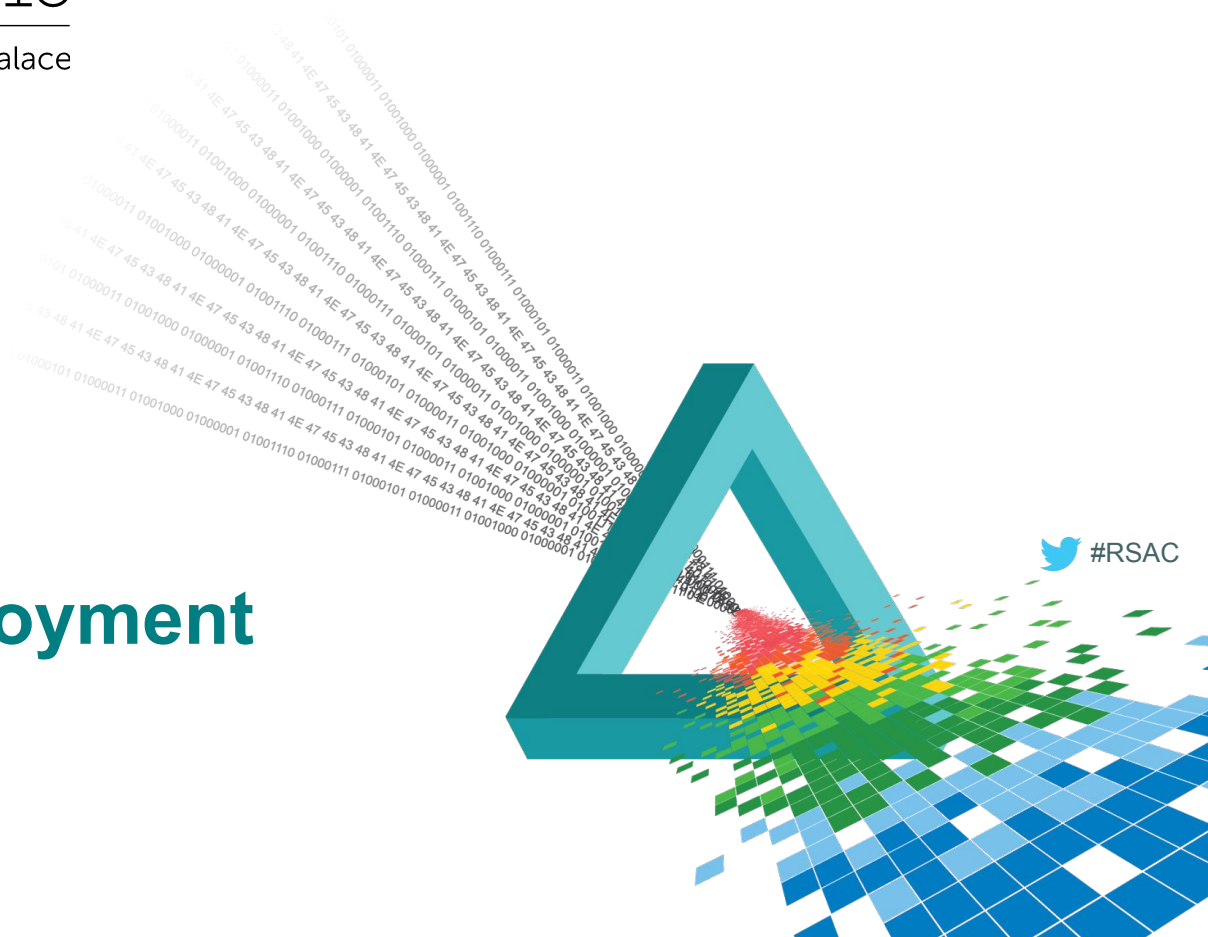
- Scalable
- Cost of deployment is well-defined
- Well tested in the real world

Transform to IoT:

- Binds a device identity to a key
- Crypto engine - built-in CIA (Confidentiality, Integrity, Authentication & Access Control)

RSAConference2015

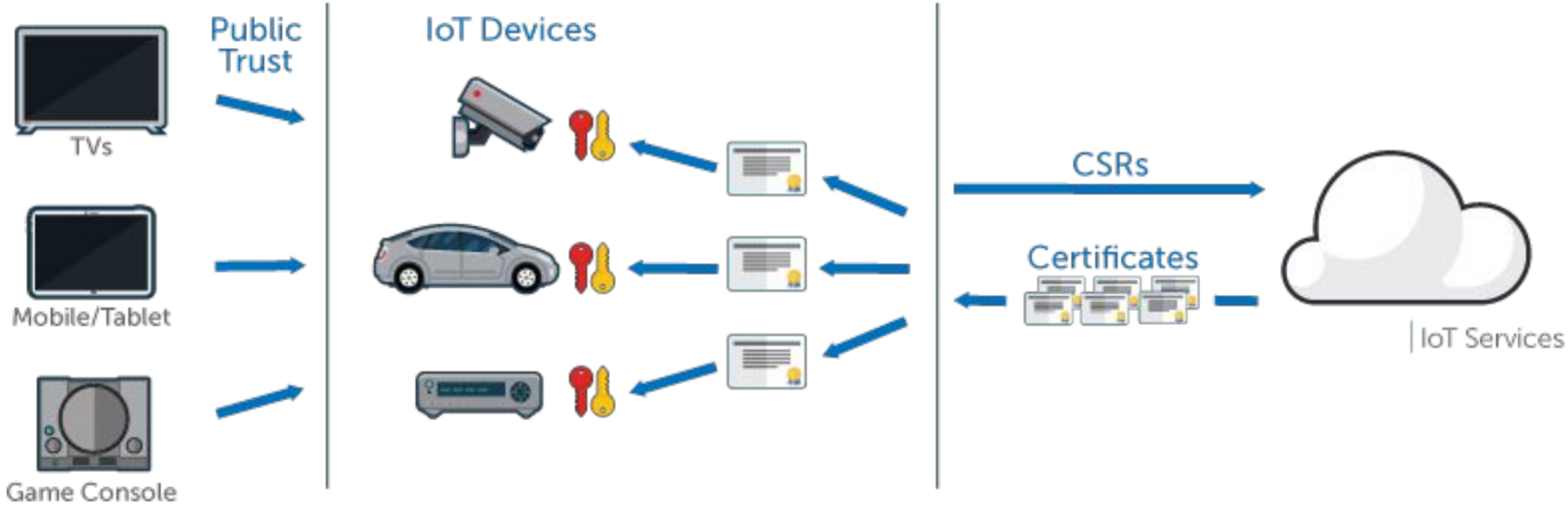
Abu Dhabi | 4–5 November | Emirates Palace



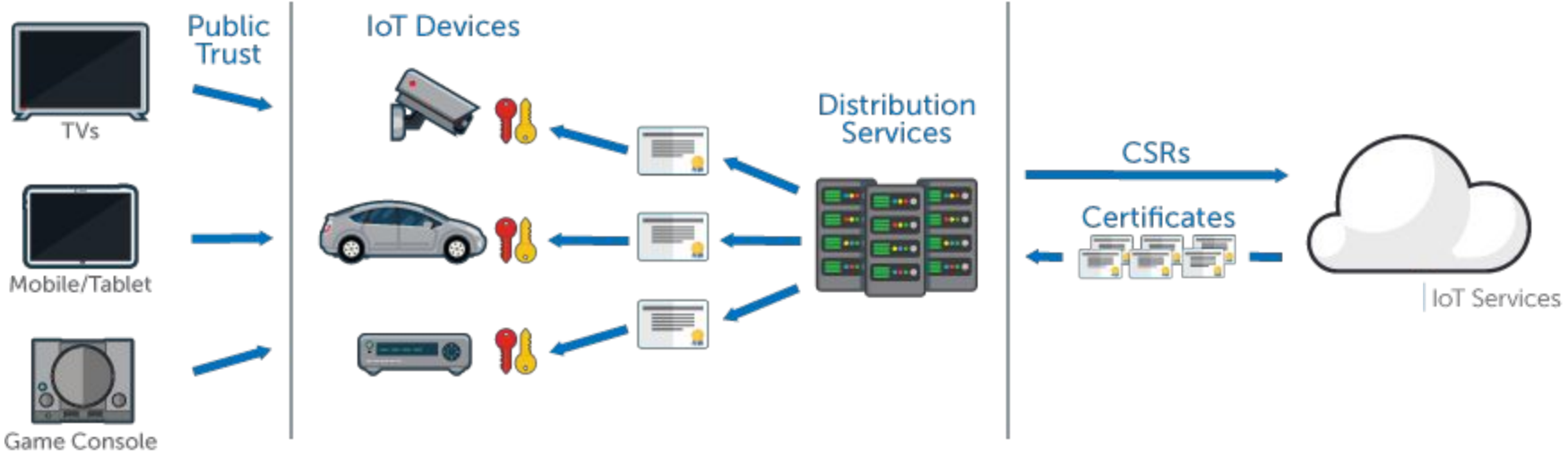
#RSAC

IoT Security Deployment

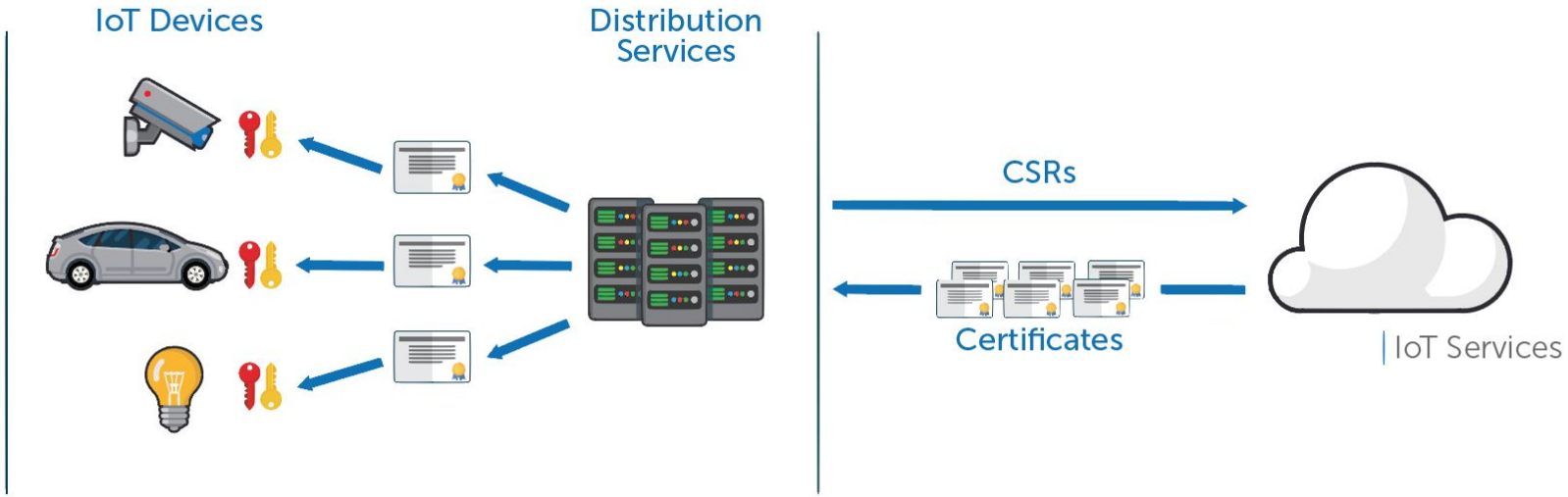
IoT Security Deployment - Interoperability



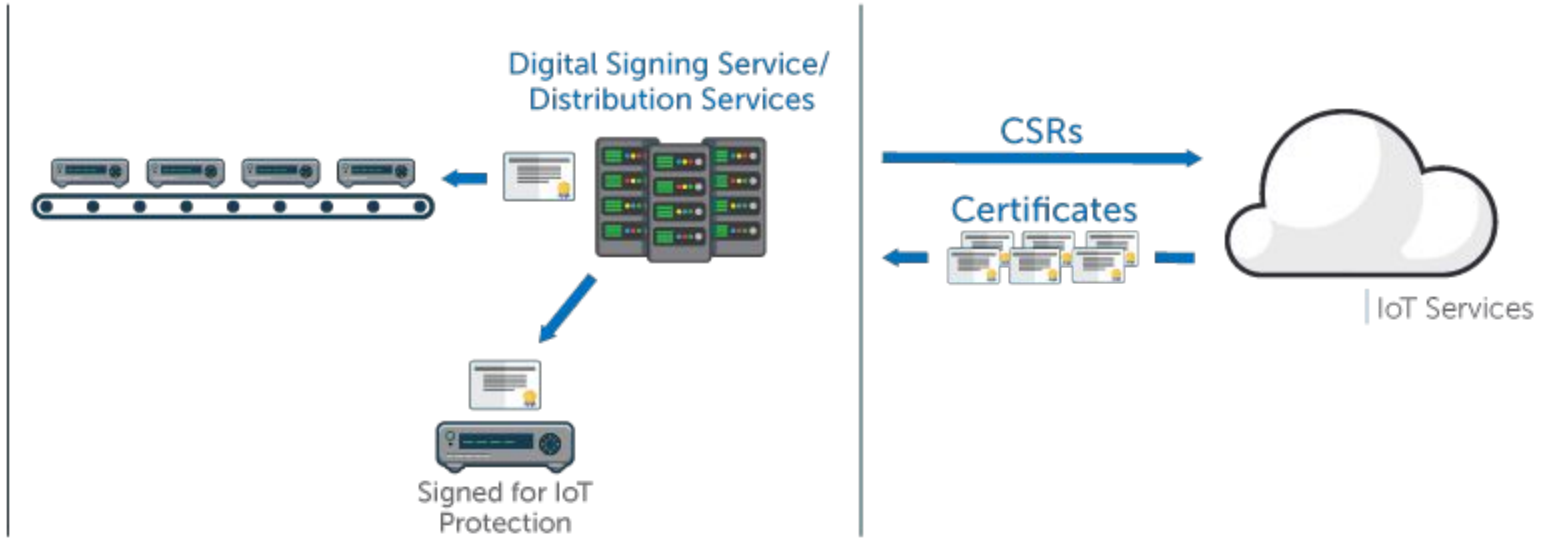
IoT Security Deployment + Distribution



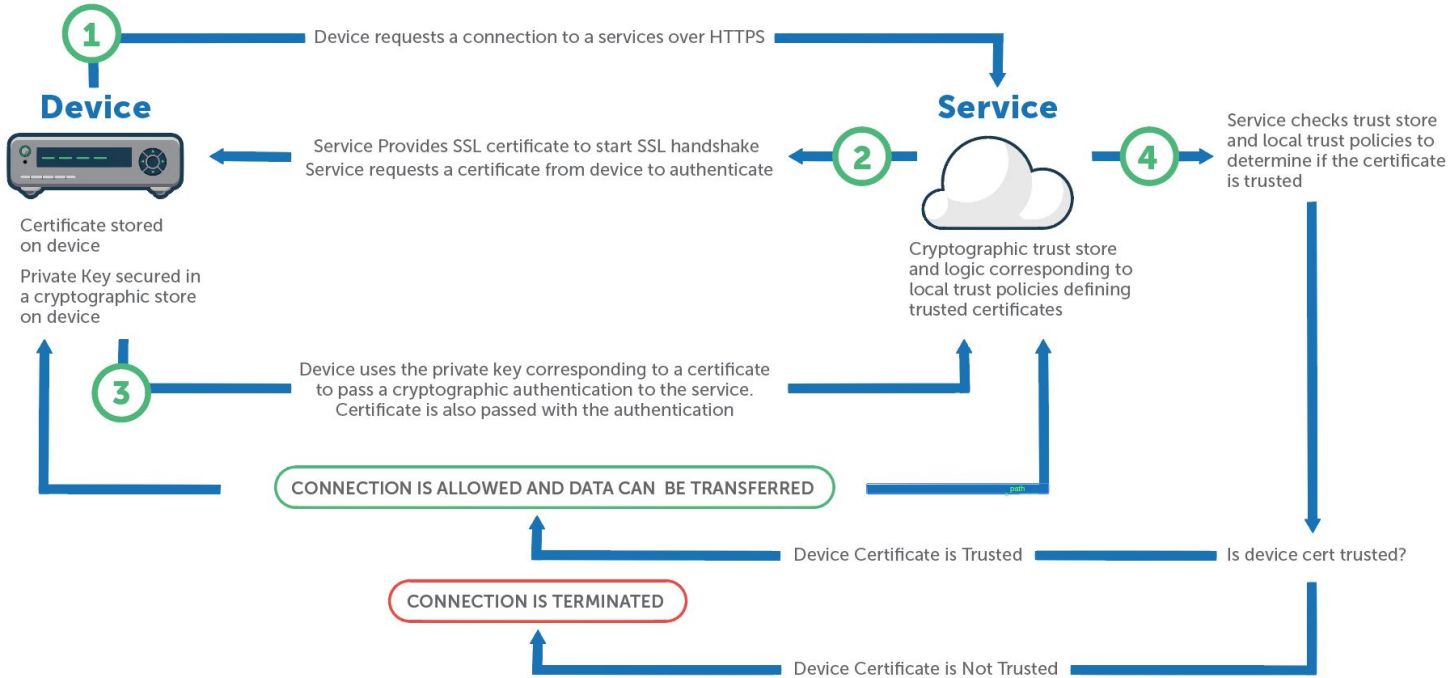
IoT Security Deployment - Private PKI



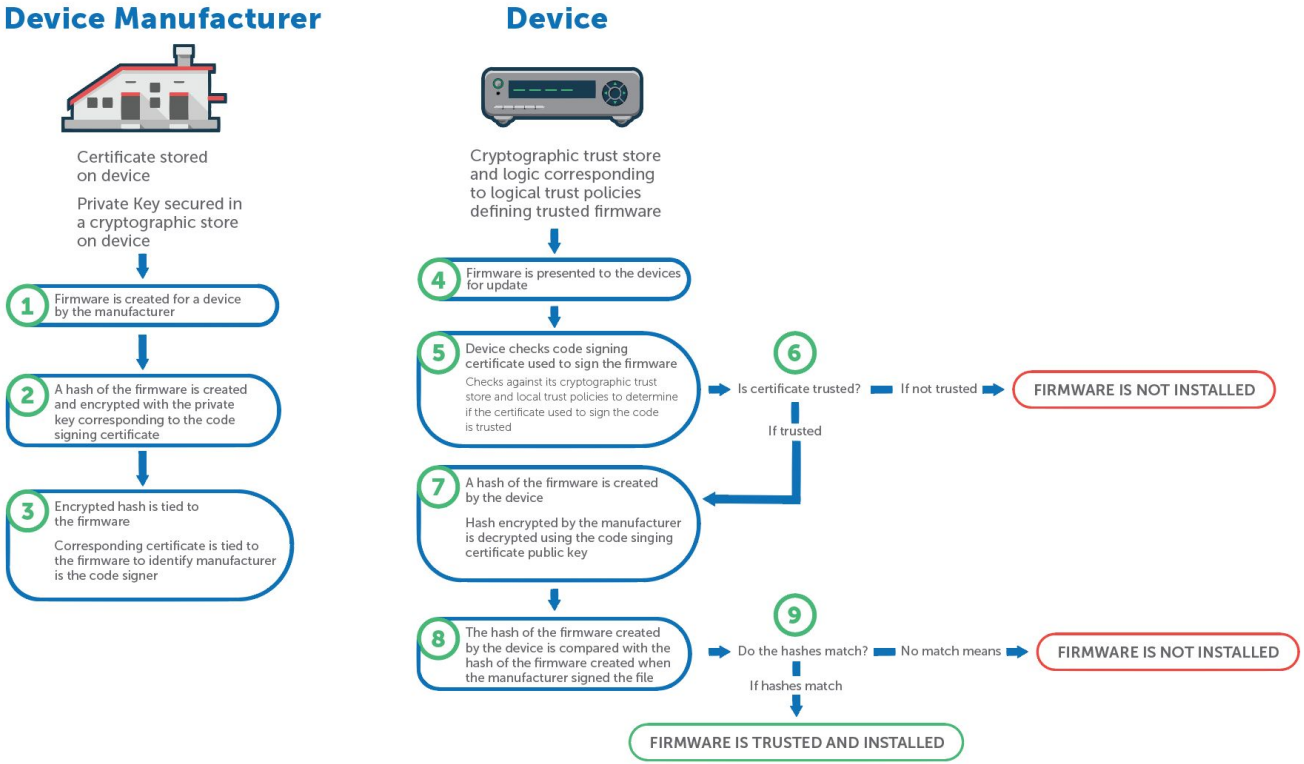
IoT Security Deployment - Integrity + Auth



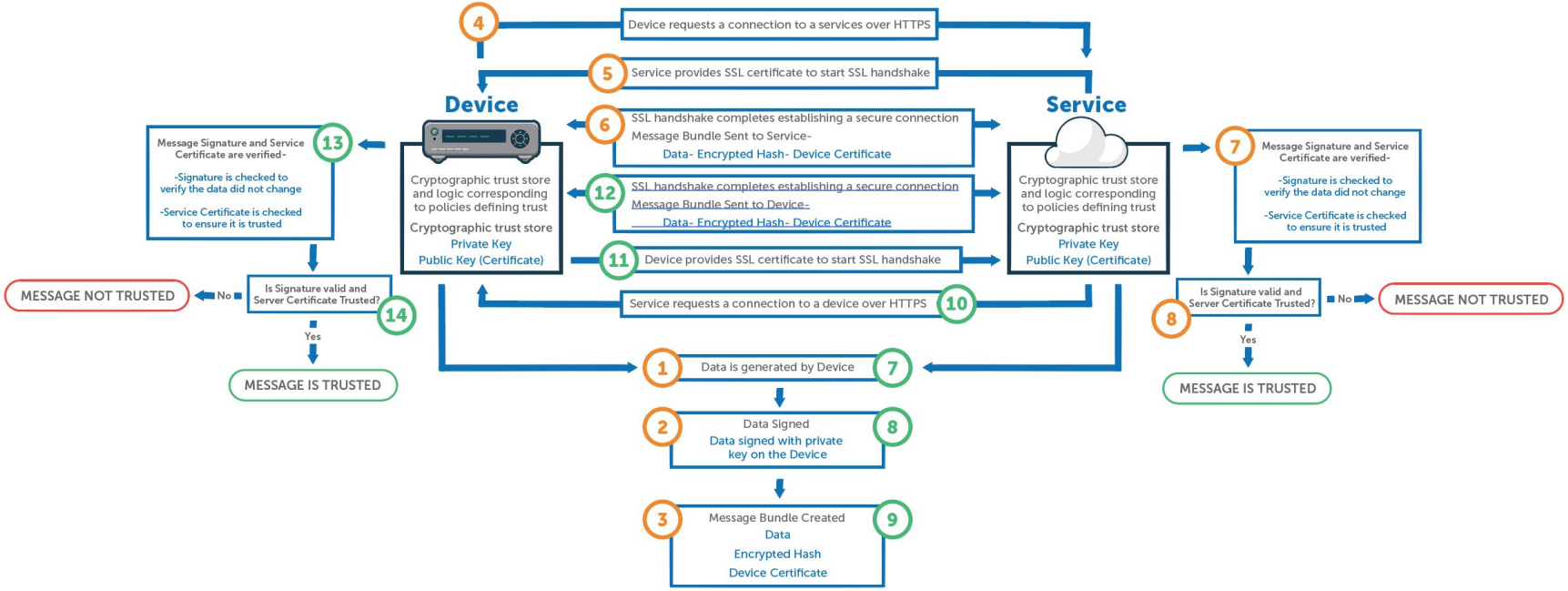
IoT PKI Implementation



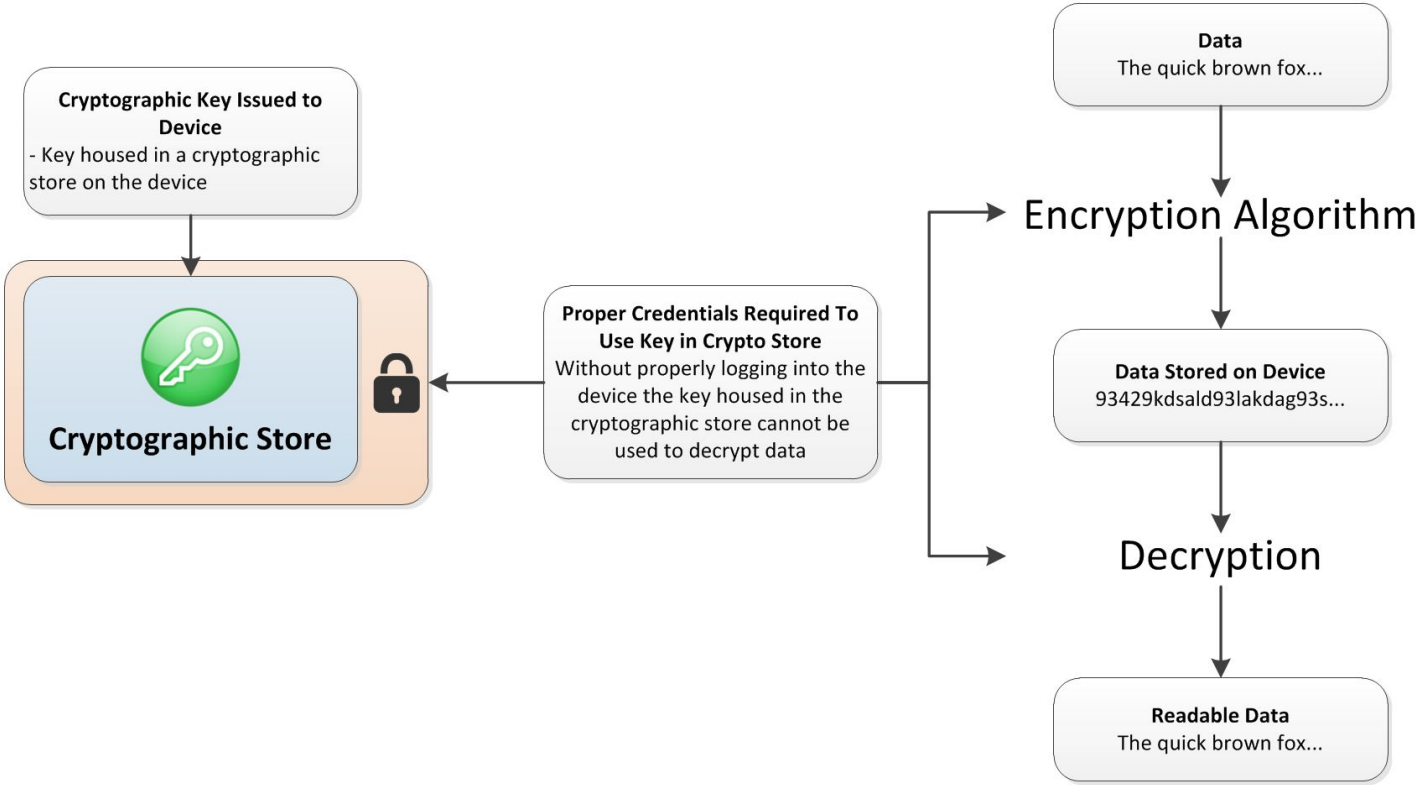
IoT PKI Device Management - Codesigning



IoT PKI Secure Device Messaging



IoT PKI Device - Protect Data at Rest



What Should IoT Architects Do?

- **Utilize PKI – it the best technology we have for securing messages, data, and identities across open networks**
- **PKI > PKT - "I" is for infrastructure**
  - PKI is not just about the technology and establishing trust means defining the processes and procedures for each actor in the PKI and clearly communicating the responsibilities
  - Acknowledgement of liabilities of each actor in the system
  - Build abuse cases

What Should IoT Architects Do?

- **Determine what problem you're solving:**
  - Encryption of communication
  - Identity and Authentication of devices
  - Signing of executables or binaries
  - Data or Message signing
  - Encrypting data at rest

What Should IoT Architects Do?

- **Implement a Trusted IoT Security Framework**
  - **Local CA or Commercial CA**
    - Choose a partner who knows how to scale
    - Ensure partner is trusted and audited across broadest scale
    - Collaborate with partner to reduce your implementation effort
  - **Don’t rely on established technology alone**
    - Integrate Technology & Tokens
    - Adopt Policy & Procedures
    - Review Relationships & Responsibilities
  - **Embed Identity in device during OEM rollout process**

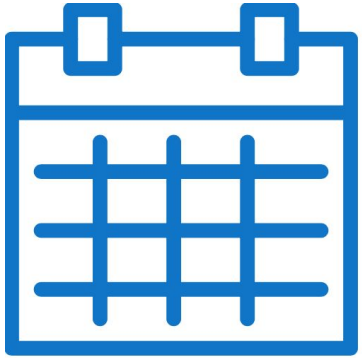
Summary

IoT security concerns are legit

- **Attacks now cross physical boundaries**
  - Watch out for the microwave ;-)
- **Build Trust - Prescription for Implementations:**
  - SDLC is now a requirement (built-in NOT bolted-on)
  - Incorporate PKI based trust principles
  - Participate in active communities and industry groups
- **Secure your deployments**
  - Choose models that incorporate CIA elements***(confidentiality, integrity, authentication and access control)***

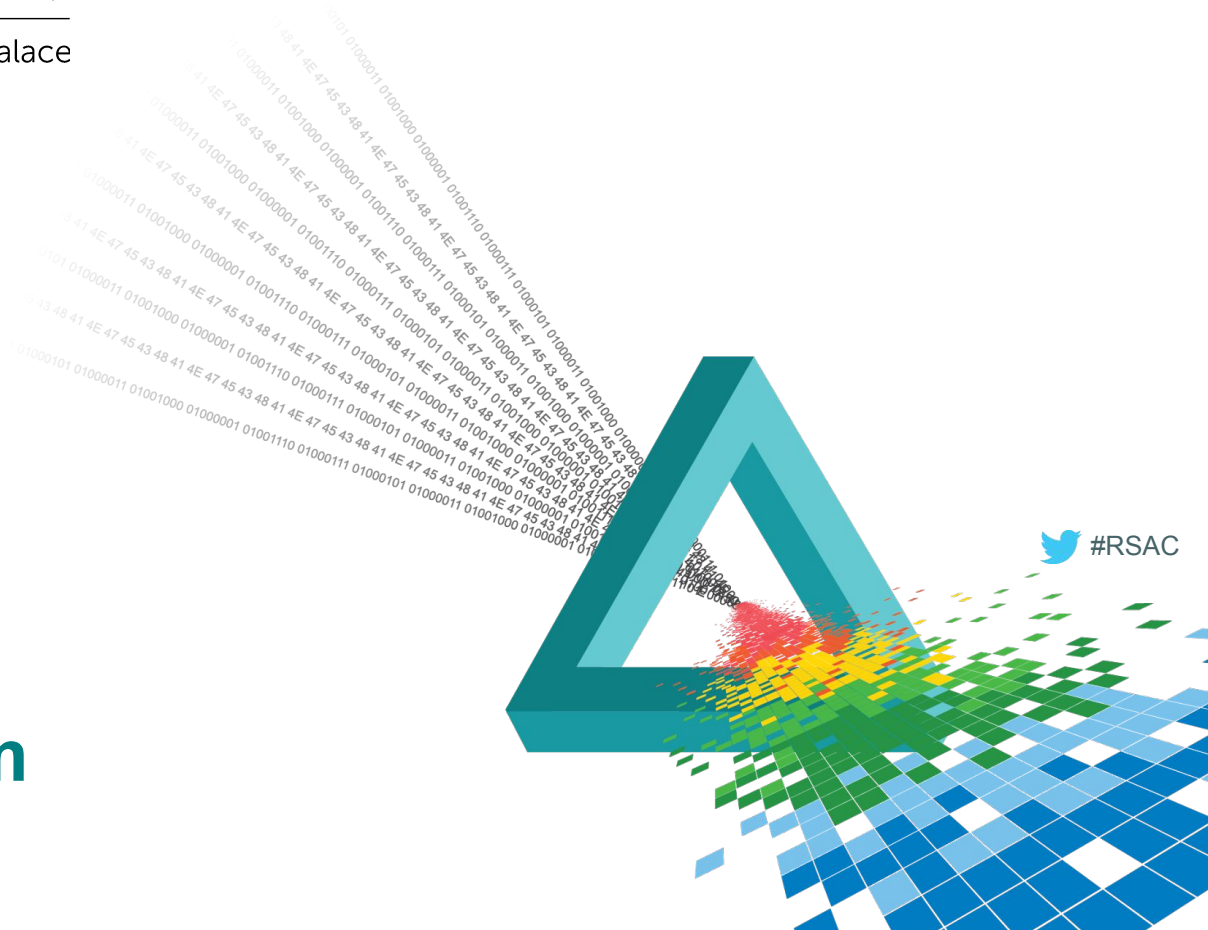
Next Steps…

- **Next week you should:**
  - Identify key stakeholders in your IoT ecosystem
  - Evaluate security mechanisms and insider threats
- **Next month from today you should:**
  - Determine weaknesses, build threat models
  - Start creating “Abuse cases”
  - Build a secure deployment strategy
- **Within six months you should:**
  - Create a roadmap for implementing IoT SDLC
  - Find and partner with trusted 3rd parties



RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace



Q&A

dan@digicert.com