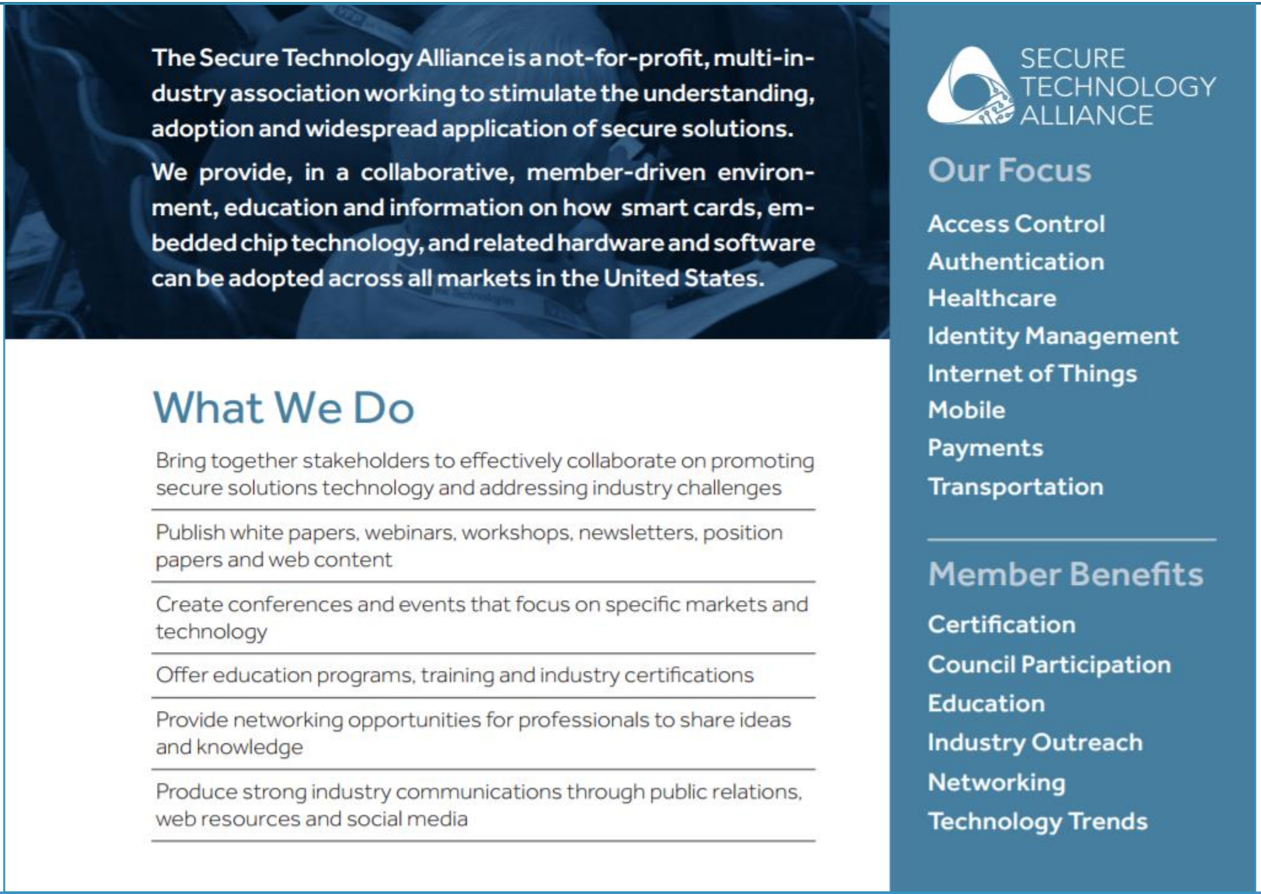
SECURE TECHNOLOGY ALLIANCE

Security in the IoT Ecosystem: The Role of PKI in IoT

IoT Security Council Webinar

May 16, 2019

Who We Are



The Secure Technology Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption and widespread application of secure solutions.

We provide, in a collaborative, member-driven environment, education and information on how smart cards, embedded chip technology, and related hardware and software can be adopted across all markets in the United States.

What We Do

- Bring together stakeholders to effectively collaborate on promoting secure solutions technology and addressing industry challenges
- Publish white papers, webinars, workshops, newsletters, position papers and web content
- Create conferences and events that focus on specific markets and technology
- Offer education programs, training and industry certifications
- Provide networking opportunities for professionals to share ideas and knowledge
- Produce strong industry communications through public relations, web resources and social media

SECURE TECHNOLOGY ALLIANCE

Our Focus

Access Control
Authentication
Healthcare
Identity Management
Internet of Things
Mobile
Payments
Transportation

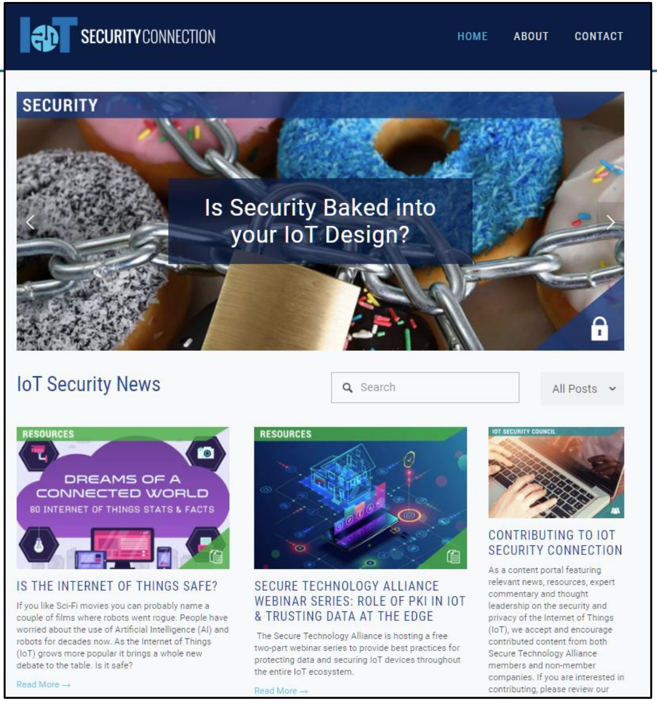
Member Benefits

Certification
Council Participation
Education
Industry Outreach
Networking
Technology Trends

IoT Security Council

IoT SECURITY COUNCIL PRIORITIES

- Accelerate market adoption of secure IoT architectures that incorporate embedded security and privacy
- Provide a forum for intra-industry and cross-industry collaboration on secure IoT architectures
- Provide a business-focused organization to discuss best practices and implementation of IoT architectures using embedded security and privacy
- Provide a single organization where all industry stakeholders can network, share implementation experiences, and discuss applications and security approaches
- Identify and collaborate with other industry organizations to define and promote standards for secure IoT architectures using technologies that provide embedded security and privacy



IoT SECURITY CONNECTION

HOME ABOUT CONTACT

SECURITY

Is Security Baked into your IoT Design?

IoT Security News

Search

All Posts

RESOURCES
DREAMS OF A CONNECTED WORLD
80 INTERNET OF THINGS STATS & FACTS
RESOURCES
IOT SECURITY COUNCIL

IS THE INTERNET OF THINGS SAFE?

If you like Sci-Fi movies you can probably name a couple of films where robots went rogue. People have worried about the use of Artificial Intelligence (AI) and robots for decades now. As the Internet of Things (IoT) grows more popular it brings a whole new debate to the table. Is it safe?

Read More →

SECURE TECHNOLOGY ALLIANCE WEBINAR SERIES: ROLE OF PKI IN IOT & TRUSTING DATA AT THE EDGE

The Secure Technology Alliance is hosting a free two-part webinar series to provide best practices for protecting data and securing IoT devices throughout the entire IoT ecosystem.

Read More →

CONTRIBUTING TO IOT SECURITY CONNECTION

As a content portal featuring relevant news, resources, expert commentary and thought leadership on the security and privacy of the Internet of Things (IoT), we accept and encourage contributed content from both Secure Technology Alliance members and non-member companies. If you are interested in contributing, please review our

Publications – IoT

- Blockchain and Smart Card Technology
- Embedded Hardware Security for IoT Applications
- Implementation Considerations for Contactless Payment-Enabled Wearables
- IoT and Payments: Current Market Landscape

Security in the IoT Ecosystem Webinar Series

- **#1 – The Role of PKI in IoT – May 16th**
  Review of how public key infrastructure (PKI) can play a role in securing the IoT ecosystem
- **#2 – Trusting Data at the Edge – May 22nd**
  Review of the security requirements for trusting and managing data collected and/or stored at the edge of the IoT network and approaches for ensuring data integrity, privacy and authenticated access control

Introductions

- Randy Vanderhoof, Secure Technology Alliance

- Josh Jabs, Entrust Datacard

SECURE TECHNOLOGY ALLIANCE

The Role of PKI in IoT

May 16, 2019

The largest IoT opportunities require the digital transformation of our most critical environments

What is driving digitization in industry?

CONNECTIVITY

- Smart connected devices
- Standards-driven connectivity
- Lower cost of measurement

CLOUD

- Massive data aggregation
- Data access by specialists
- Industrial application developer ecosystem

MOBILITY

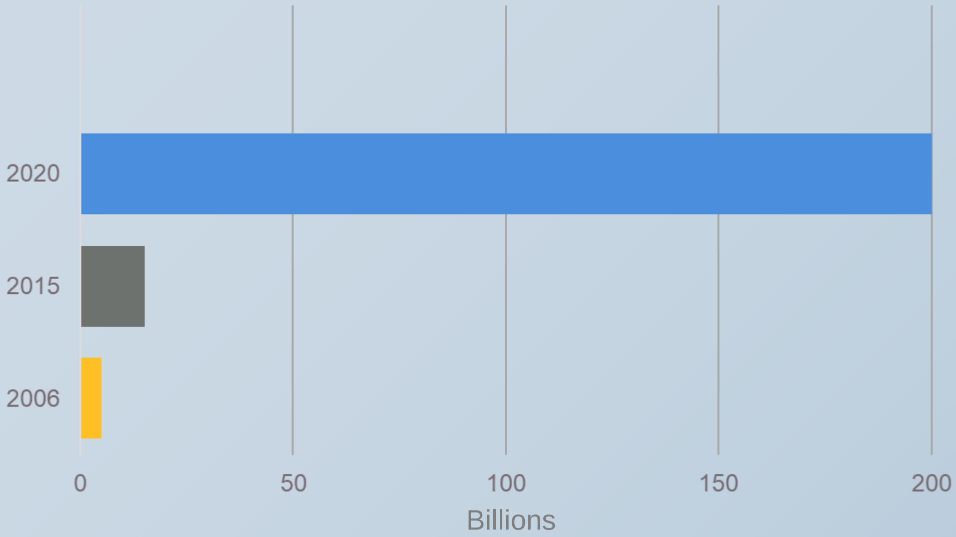
- Pervasive, affordable communication
- Remote access
- User-driven interfaces

ANALYTICS

- Cognitive applications
- AI optimizing performance
- Actionable information

Entrust Datacard™

Growth of connected IoT devices



A guide to the internet of things infographic – Source: Intel report
https://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html

40.2% Industry

30.3% Healthcare

8.3% Retail

7.7% Security

4.1% Transportation

Entrust Datacard™

Growth in IoT connected devices creates opportunity – and risk.

Companies must address the challenge on multiple levels.

By 2020, 60% of digital businesses will suffer **major service failures** due to the inability of IT security teams to **manage digital risk**

Special Report: Cybersecurity at the Speed of Digital Business, Gartner, G00315580

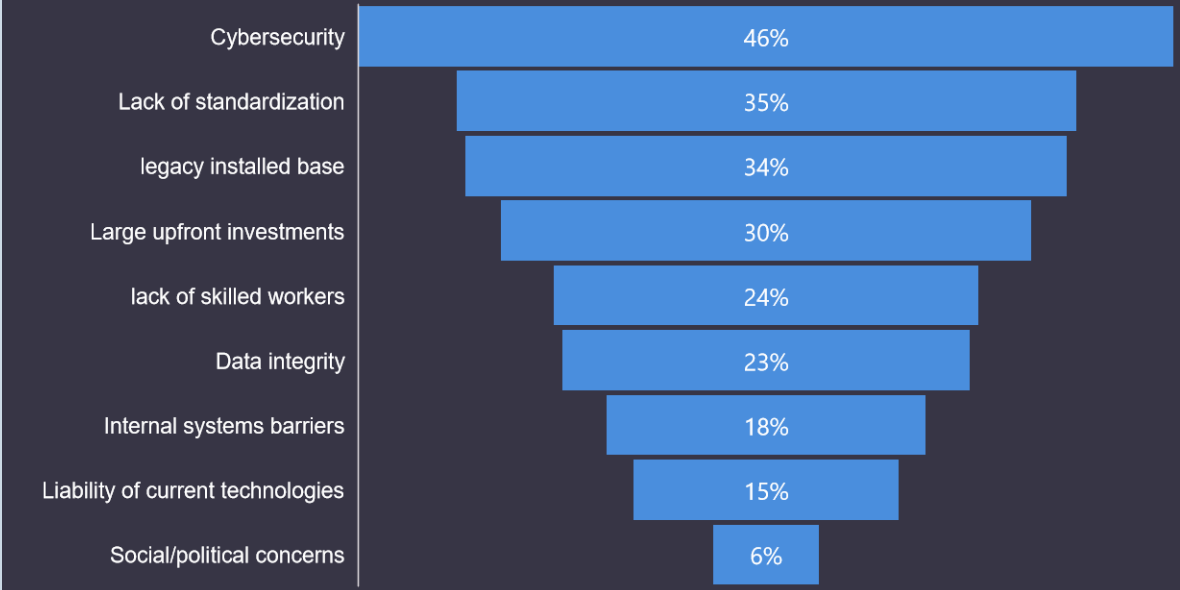
Entrust Datacard™

Polling Question

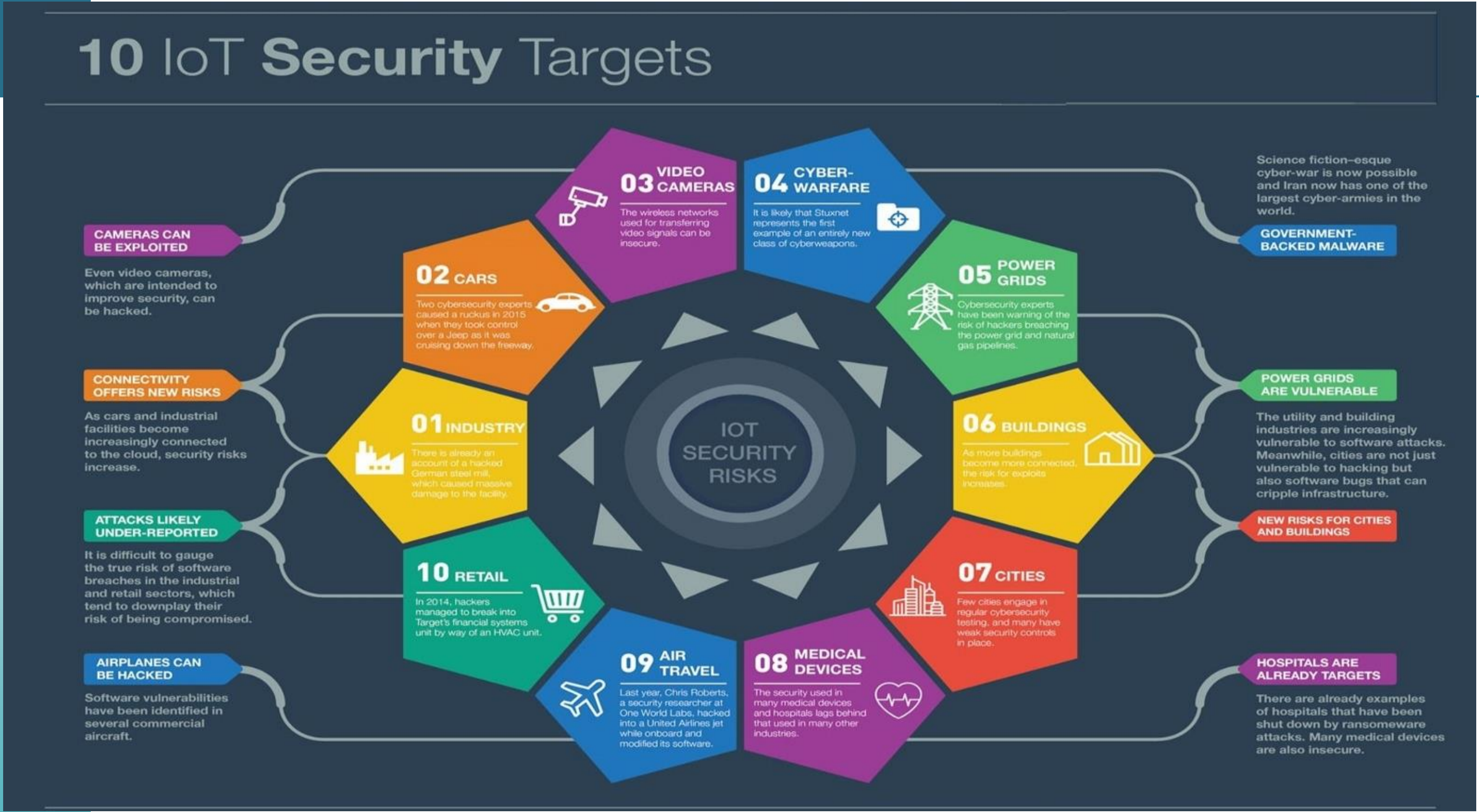
What’s the status of your organization’s plans for IOT deployment?

- No identified projects or not applicable
- Investigating, but no firm plans
- New project in next 12 months, but figuring out security approach
- New project in next 12 months, with aligned security approach
- Project already deployed, looking at improving security posture

Challenges to IoT adoption



10 IoT Security Targets



IOT SECURITY RISKS

01 INDUSTRY

There is already an account of a hacked German steel mill, which caused massive damage to the facility.

02 CARS

Two cybersecurity experts caused a ruckus in 2015 when they took control over a Jeep as it was cruising down the freeway.

03 VIDEO CAMERAS

The wireless networks used for transferring video signals can be insecure.

04 CYBER-WARFARE

It is likely that Stuxnet represents the first example of an entirely new class of cyberweapons.

05 POWER GRIDS

Cybersecurity experts have been warning of the risk of hackers breaching the power grid and natural gas pipelines.

06 BUILDINGS

As more buildings become more connected, the risk for exploits increases.

07 CITIES

Few cities engage in regular cybersecurity testing, and many have weak security controls in place.

08 MEDICAL DEVICES

The security used in many medical devices and hospitals lags behind that used in many other industries.

09 AIR TRAVEL

Last year, Chris Roberts, a security researcher at One World Labs, hacked into a United Airlines jet while onboard and modified its software.

10 RETAIL

In 2014, hackers managed to break into Target's financial systems unit by way of an HVAC unit.

CAMERAS CAN BE EXPLOITED

Even video cameras, which are intended to improve security, can be hacked.

CONNECTIVITY OFFERS NEW RISKS

As cars and industrial facilities become increasingly connected to the cloud, security risks increase.

ATTACKS LIKELY UNDER-REPORTED

It is difficult to gauge the true risk of software breaches in the industrial and retail sectors, which tend to downplay their risk of being compromised.

AIRPLANES CAN BE HACKED

Software vulnerabilities have been identified in several commercial aircraft.

Science fiction–esque cyber-war is now possible and Iran now has one of the largest cyber-armies in the world.

GOVERNMENT-BACKED MALWARE

POWER GRIDS ARE VULNERABLE

The utility and building industries are increasingly vulnerable to software attacks. Meanwhile, cities are not just vulnerable to hacking but also software bugs that can cripple infrastructure.

NEW RISKS FOR CITIES AND BUILDINGS

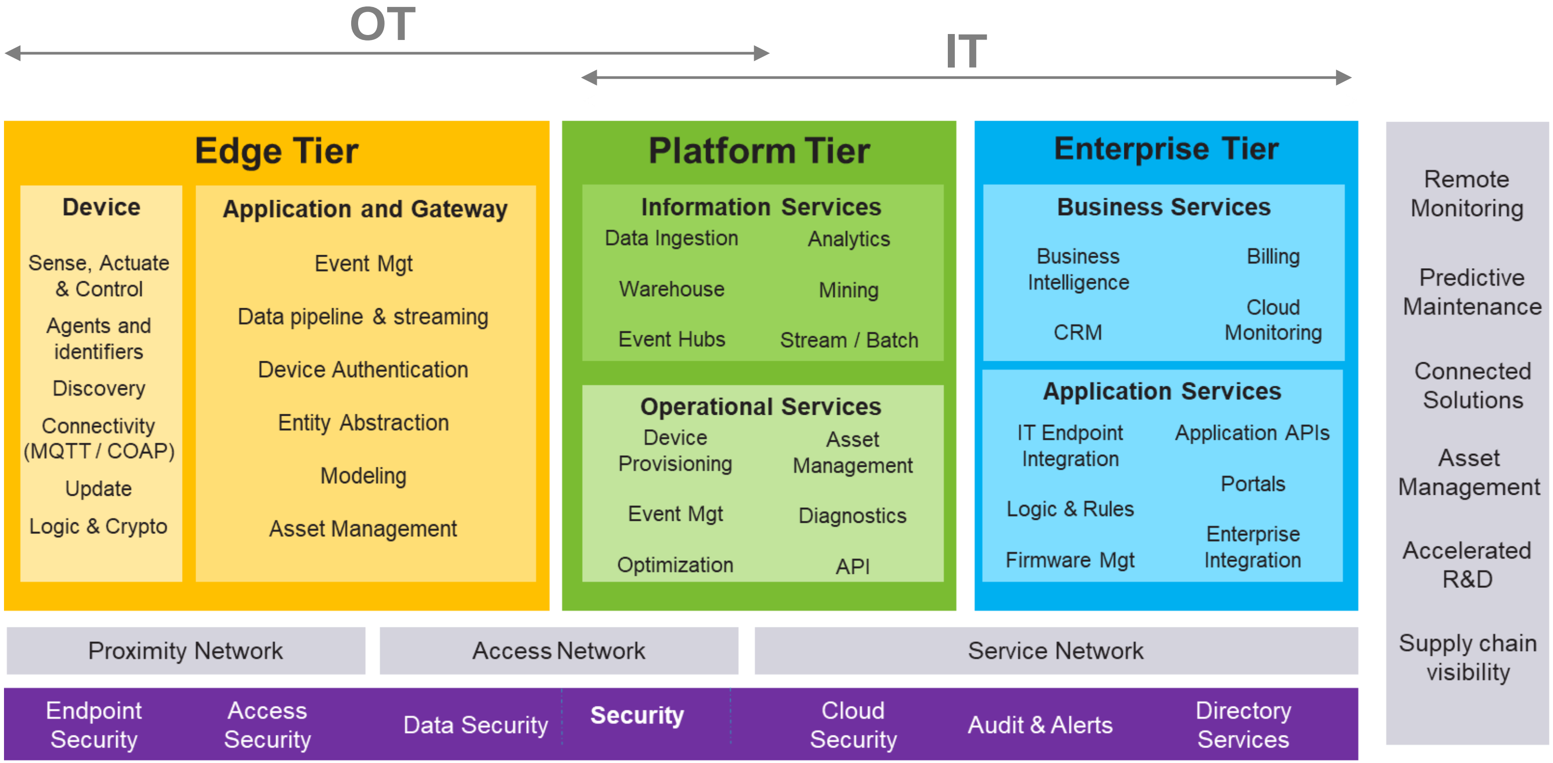
HOSPITALS ARE ALREADY TARGETS

There are already examples of hospitals that have been shut down by ransomware attacks. Many medical devices are also insecure.

IoT Presents New Security Challenges

- Device Disparity & High Volumes
- IoT and OT Convergence
- Immature Security Standards
- Gap in Technology Sophistication
- Operational Challenges
- Data Integrity
- Common Security Framework
- Privacy Issues
- Automation Challenges
- Encryption Capabilities

When the Worlds of IT and OT collide



OT

IT

Edge Tier

Device

Sense, Actuate & Control

Agents and identifiers

Discovery

Connectivity (MQTT / COAP)

Update

Logic & Crypto

Application and Gateway

Event Mgt

Data pipeline & streaming

Device Authentication

Entity Abstraction

Modeling

Asset Management

Platform Tier

Information Services

Data Ingestion

Analytics

Warehouse

Mining

Event Hubs

Stream / Batch

Operational Services

Device Provisioning

Asset Management

Event Mgt

Diagnostics

Optimization

API

Enterprise Tier

Business Services

Business Intelligence

Billing

Cloud Monitoring

CRM

Application Services

IT Endpoint Integration

Application APIs

Portals

Logic & Rules

Enterprise Integration

Firmware Mgt

Remote Monitoring

Predictive Maintenance

Connected Solutions

Asset Management

Accelerated R&D

Supply chain visibility

Proximity Network

Access Network

Service Network

Endpoint Security

Access Security

Data Security

Security

Cloud Security

Audit & Alerts

Directory Services

Polling Question

Which part of your organization do you report into?

- IT
- CTO
- Security or Risk
- Line of Business or Product Team
- Other

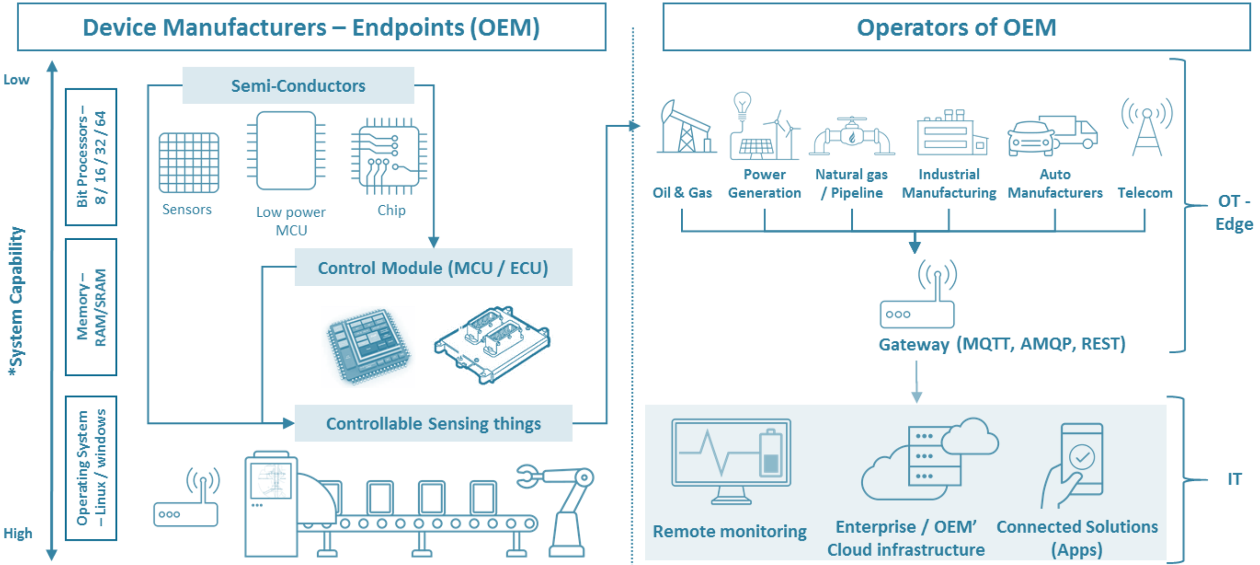
SECURE
TECHNOLOGY
ALLIANCE

Establishing Trust in the IoT

Trust is having the confidence or assurance that a person, system, or thing will behave as you expect or as intended

Entrust Datacard™

Device Lifecycle in IoT



Device Manufacturers – Endpoints (OEM)
Operators of OEM
Low
High
*System Capability
Bit Processors – 8 / 16 / 32 / 64
Memory – RAM/SRAM
Operating System – Linux / windows
Semi-Conductors
Sensors
Low power MCU
Chip
Control Module (MCU / ECU)
Controllable Sensing things
Oil & Gas
Power Generation
Natural gas / Pipeline
Industrial Manufacturing
Auto Manufacturers
Telecom
OT - Edge
Gateway (MQTT, AMQP, REST)
Remote monitoring
Enterprise / OEM' Cloud infrastructure
Connected Solutions (Apps)
IT

Module / Sensor Manufacturing **Security** **Securing Sensor / Module + Data**

Identity Set up

- Installation of Device Agent
- Addition of Device attributes & bootstrap certificate / token
- Key & Certificate generation

Secure Identity

- HSM, TPM, E-Sim, SE (Secure Element), software keystore
- TEE

Provisioning

- Discovery
- Device Authentication
- Provisioning & Authorization

Lifecycle Mgt

- Secure Data & Identity
- Policy Updates
- Activate / Suspend / Terminate
- Device Update – Firmware, Cert
- User Access

Identity Lifecycle Management for Devices

Manufacture

- Identity Issuance
- Scalable Device trust and Identity
- All classes of devices

Provision

- Whitelisting the device
- Register the device
- On-Demand / Bulk

Deploy

- Enrollment of device
- Authenticate the device
- Part of Trusted Ecosystem
- Enterprise Integration

Monitor

- Access control
- Audit
- Block unauthorized connections
- Data extraction
- Secure Data Transmission

Service

- Suspend device
- Activate / Re-Activate device
- Prevent unauthorized command and control

Update

- Code Signing
- Secure Bootstrapping
- Secure Firmware update
- Secure Software Update

Decommission

- Terminate the Device
- Blocked from the Trust zone / network

IDENTITY

AUTHENTICATION & AUTHORIZATION

CREDENTIAL LIFECYCLE MANAGEMENT

DATA SECURITY

SUPPLY CHAIN INTEGRITY

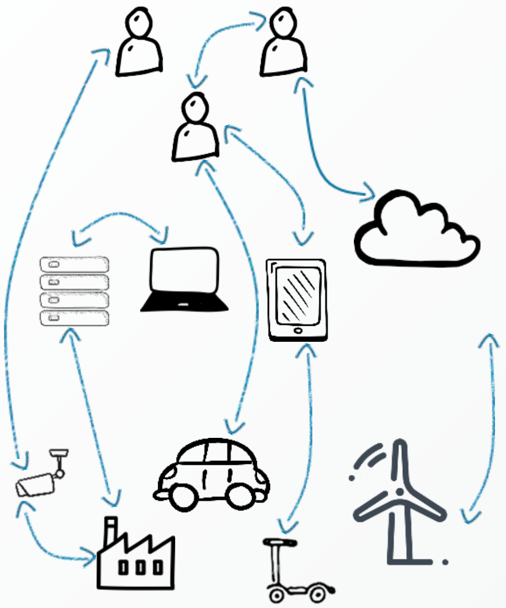
Entrust Datacard™

Polling Question

What’s your familiarity with Public Key Infrastructure

- Expert
- Operate it, but not an expert
- I know about it, but don’t have hands on experience
- I think I’ve heard about certificates before
- Unfamiliar

Why PKI? What does it do?



Trustworthy Interactions

1) How do I know who I'm talking to?
2) Are these parties allowed to communicate?
3) How do I prevent others from listening in?
4) How do I make sure what was sent was received?
5) How do I prove what was said later?

Authentication
Authorization

Encryption

Integrity (signing)

Entrust Datacard™

Important Concepts (especially with scale)

It's digital, so keys and crypto make it work and you need to protect them accordingly

It starts with registration

It's a system and will evolve (there's a lifecycle)

Validation is required and the concepts impact performance (when, how)

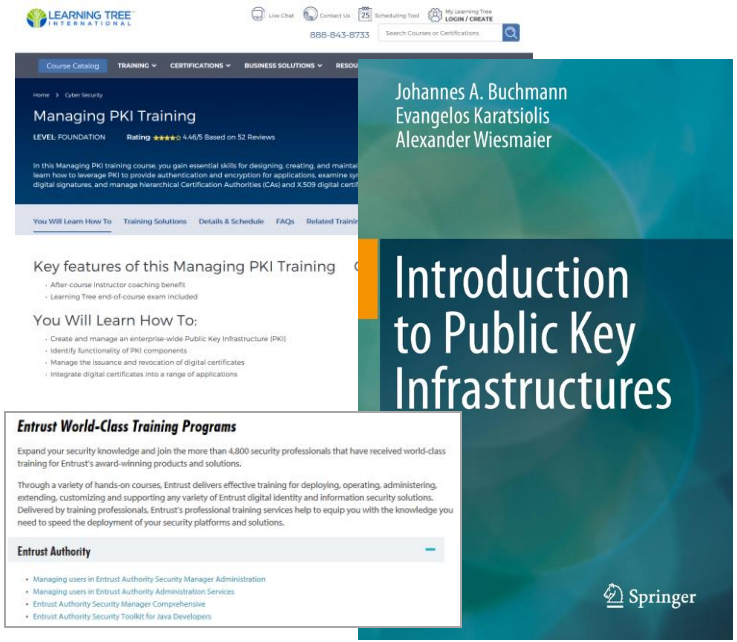
What is PKI?

What is a public-key infrastructure (PKI)?

The comprehensive set of roles, policies, and procedures required to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption. Every authorized person, device and app gets a digital certificate that proves their identity

What does PKI do?

A PKI enables an organization to establish and maintain a trustworthy digital ecosystem (people, systems, and things) by managing keys and certificates.



LEARNING TREE INTERNATIONAL

Live Chat · Contact Us · Scheduling Tool · My Learning Tree LOGIN / CREATE

888-843-8733 · Search Courses or Certifications

Course Catalog · TRAINING · CERTIFICATIONS · BUSINESS SOLUTIONS · RESOU

Home > Cyber Security

Managing PKI Training

LEVEL: FOUNDATION   Rating ★★★★☆ 4.46/5 Based on 52 Reviews

In this Managing PKI training course, you gain essential skills for designing, creating, and maintai
learn how to leverage PKI to provide authentication and encryption for applications, examine sy
digital signatures, and manage hierarchical Certification Authorities (CAs) and X.509 digital certi

You Will Learn How To · Training Solutions · Details & Schedule · FAQs · Related Trainin

Key features of this Managing PKI Training

- After-course instructor coaching benefit
- Learning Tree end-of-course exam included

You Will Learn How To:

- Create and manage an enterprise-wide Public Key Infrastructure (PKI)
- Identify functionality of PKI components
- Manage the issuance and revocation of digital certificates
- Integrate digital certificates into a range of applications

Johannes A. Buchmann
Evangelos Karatsiolis
Alexander Wiesmaier

Introduction to Public Key Infrastructures

Springer

Entrust World-Class Training Programs

Expand your security knowledge and join the more than 4,800 security professionals that have received world-class training for Entrust's award-winning products and solutions.

Through a variety of hands-on courses, Entrust delivers effective training for deploying, operating, administering, extending, customizing and supporting any variety of Entrust digital identity and information security solutions. Delivered by training professionals, Entrust's professional training services help to equip you with the knowledge you need to speed the deployment of your security platforms and solutions.

Entrust Authority

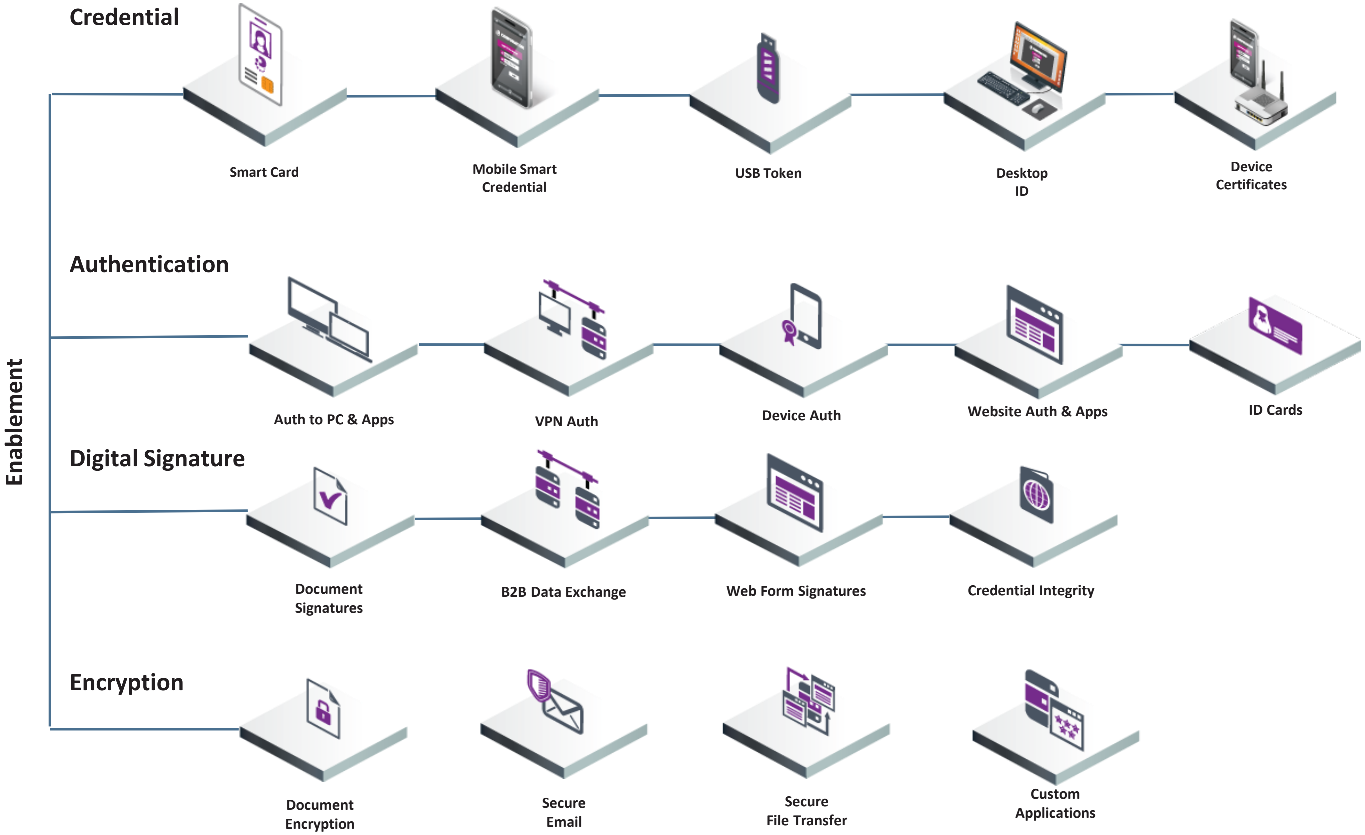
- Managing users in Entrust Authority Security Manager Administration
- Managing users in Entrust Authority Administration Services
- Entrust Authority Security Manager Comprehensive
- Entrust Authority Security Toolkit for Java Developers

For more on PKI, these sound like fun =)

SECURE TECHNOLOGY ALLIANCE

Entrust Datacard™

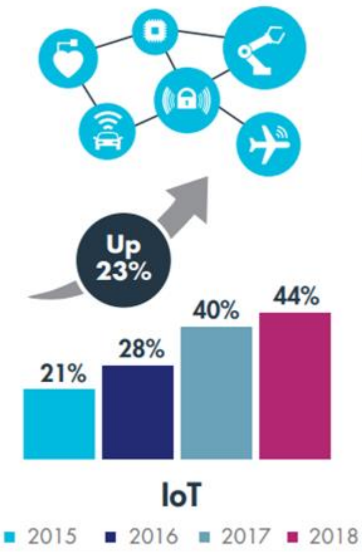
PKI – A history of providing security at scale



Entrust Datacard™

PKI – Continues to gain traction in the IoT security community

IoT is becoming a major driver for the use of PKI

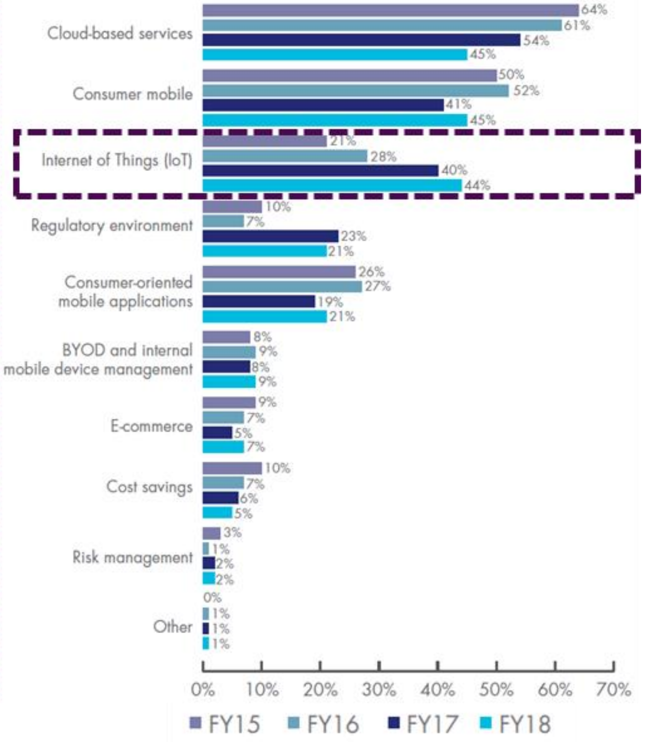


42%

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

IoT is the most important trend driving the deployment of applications using PKI has increased significantly from 21 percent to 44 percent

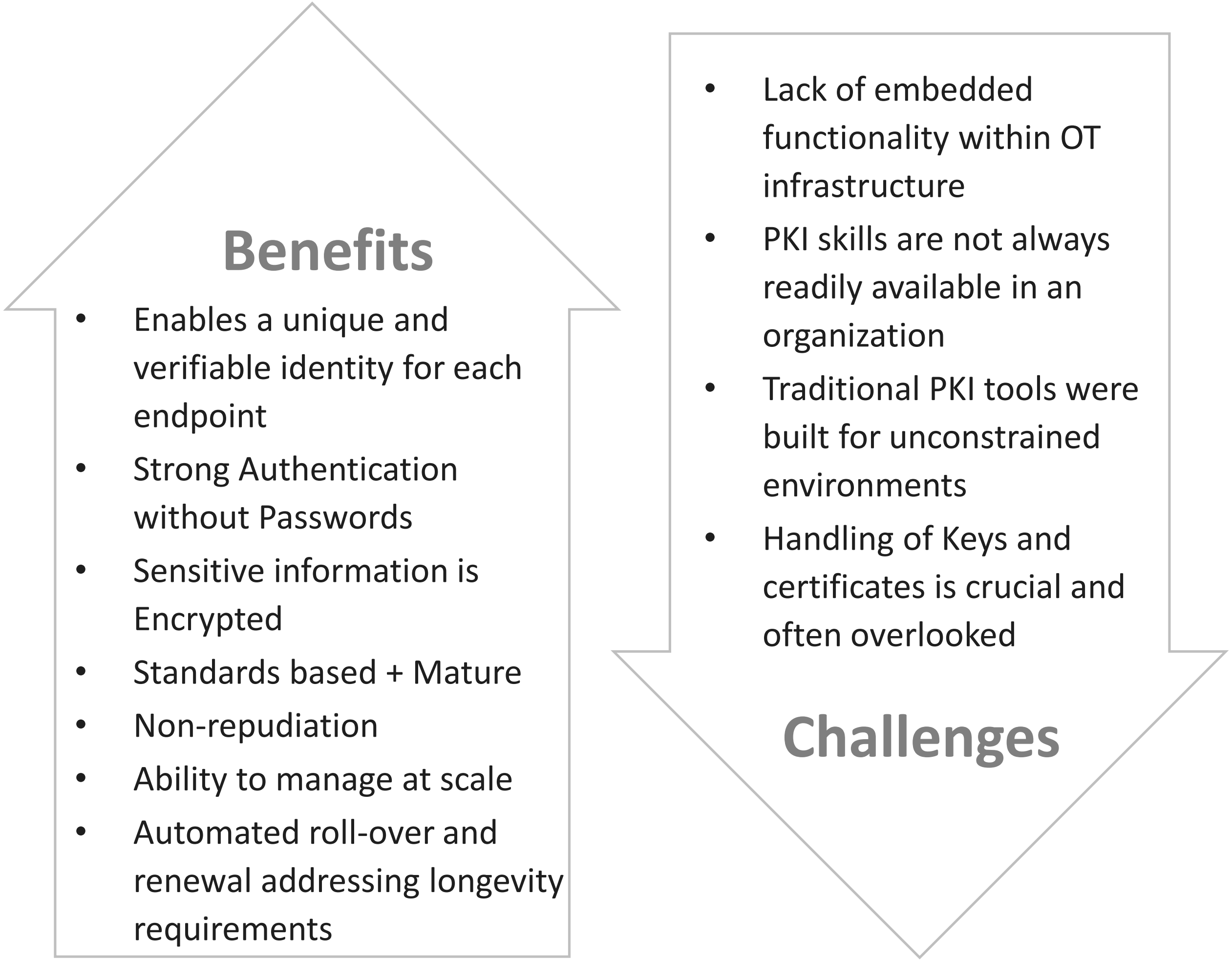
Important trends driving PKI deployment



Entrust Datacard™

Weighing PKI for IOT

Entrust Datacard™



Benefits

- Enables a unique and verifiable identity for each endpoint
- Strong Authentication without Passwords
- Sensitive information is Encrypted
- Standards based + Mature
- Non-repudiation
- Ability to manage at scale
- Automated roll-over and renewal addressing longevity requirements

Challenges

- Lack of embedded functionality within OT infrastructure
- PKI skills are not always readily available in an organization
- Traditional PKI tools were built for unconstrained environments
- Handling of Keys and certificates is crucial and often overlooked

PKI for IOT Considerations

- Supply chain considerations
- Brownfield vs Greenfield devices
- Two tier (device to cloud) vs three tier (operations) environments
- Skill-sets and organizational structure
- Device provisioning and scale (manual or automated)
- Device and service lifecycles
- Deployment preferences (on-premises, cloud, hybrid)
- Compliance requirements
- Protocol requirements
- Key generation and storage

The value of cybersecurity in IoT Ecosystems

Protect your IoT Investment

- Support Safety for Staff and Environment
- Protect Corporate Image and Reputation
- Ensure Business Continuity
- Avoid Regulatory & SLA Penalties
- Protect Critical Digital Assets (IP)
- Improve Cyber Defensible Position to Threats

SECURE TECHNOLOGY ALLIANCE

Entrust Datacard™

> **“There's no silver bullet solution with cybersecurity, a layered defense that is adequately monitored, is the only viable defense.”**
>
> \- James Scott, Senior Fellow, Institute for Critical Infrastructure Technology

Entrust Datacard™

SECURE TECHNOLOGY ALLIANCE

Q&A

IoT Security Webinar Series Assessment

- Online assessment quizzes available for both webinars in the series
- Participate in the two webinars and pass both assessments to receive a Secure Technology Alliance certificate of participation
- Assessment link: https://www.surveymonkey.com/r/PKIinIOT

Selected Secure Technology Alliance Resources

- **IoT Security Council Resources**
  - https://www.securetechalliance.org/activities-councils-internet-of-things-security/

- **Secure Technology Alliance Knowledge Center** https://www.securetechalliance.org/knowledge-center/
  - Embedded Hardware Security for IoT Applications
  - IoT and Payments: Current Market Landscape
  - IoT Security: Mitigating Security Risks in Secure Connected Environments Webinar
  - IoTSecurityConnection.com
  - Secure Technology Alliance Response: NIST "IoT Security and Privacy Risk Considerations" Questions

SECURE
TECHNOLOGY
ALLIANCE

Randy Vanderhoof, rvanderhoof@securetechalliance.org

Josh Jabs, Josh.Jabs@entrustdatacard.com