intertrust®

BUYER'S GUIDE

PKI for IoT buyer's guide

Building trust for a connected world.

Contents

Introduction 2

Gotchas IoT devices face 3

PKI protections and considerations 4

Weighing PKI approaches 5

How Intertrust can help 7

Introduction

Today, more than 16.7 billion IoT devices have been deployed–and their number continues to expand at a dizzying 16% compound annual growth rate.[1]

From crop sensors and connected cars to more efficient manufacturing and smart grids, IoT devices are performing wonders in automation and efficiency, delivering unprecedented insights through real-time data. Yet, with this huge footprint of devices and incredible number of endpoints they encompass, the attack surface is vast and it creates a playground for hackers that we've never experienced before.

Given the expanded capabilities of IoT devices and networks, protecting them is paramount, yet, it can be daunting to even get started.

What should you consider in your PKI approach for protecting these assets? The end result can amount to protecting your IP, your reputation in the market, and even your ability to do business in the future.

Use this quick guide to navigate through the task of picking the right protection methodology and approach. First we will look at some of the issues IoT devices face, next we will discuss essential cybersecurity standards for protection.

Then we will review different approaches to PKI for IoT, and finally we will look at PKI must-haves for your business.

Gotchas IoT devices face

The year-over-year increase in IoT malware incidents rose by 87%.[2] So, why are there so many successful attacks and what security challenges lie ahead?

Insecure protocols

The number one threat IoT devices face is insecure protocols. Many field area networks, especially mesh networks have insecure protocols that are either not up to date or the protocols themselves are not well designed.

Man-in-the-middle attacks

These attacks can have significant implications because that man in the middle, the hacker, can intercept traffic, change traffic, and create advanced persistent threats. And since most IoT device traffic is insufficiently secured, this challenge is not going away anytime soon.

Device hijacking

Hijacking happens when your ecosystem is accessed and devices are compromised. The rise of botnets shows the damage hijacked devices can do and the serious security risk they represent. A majority of today's internet attacks are bot-based and the Mirai botnet today has hundreds of thousands of devices that are at the command and control of the botnet manager.

Weak encryption

Often weak encryption creates significant security risks and breaches. Insufficient key links, insufficient key types, compromised encryption key storage are a few of the culprits. Encryption can be fine on the server side, but it's only as good as how well the device is protected.

Poor IT/OT connection

One of the main themes that continues to persist within the Internet of Things is the intersection between information technology and operational technology, or IT and OT. Both systems need to function in concert or a ready attack surface will present itself to hackers. A key problem that prevents IT and OT from working properly and leads to attacks is bad or missing authentication and secure communications. This is where public key infrastructure (PKI) comes in and is uniquely positioned to help.

What should you take into consideration when deploying your public key infrastructure? Let's look at what things PKI can and should do to protect IoT devices and functionality.

PKI protections and considerations

First of all, you need to examine the scope and the threat models you're considering. What are the use cases of the devices and the types of devices? Ask these questions upfront to set your initial parameters. They will dictate the specifics, such as the types of keys, key links, and protocols.

You need a really good understanding of the risk so that you can create the appropriate countermeasures to thwart that risk. So, knowing the probability of an attack, and the impact. What happens if a device or collection of devices gets attacked and compromised? And what is the inherent risk that comes from this event? That answer should inform how you build your portfolio of controlling mitigations and protections.

This leads to how you are going to operate your public key infrastructure, its policies, and procedures, and how you document it all within a certificate practice statement.

How will you protect keys and keep some keys offline, some online, how will you securely access them?

Key creation and management involve things like building the route CA, the route signing ceremony to create the initial root key, and putting these into a high-security module disconnected from the internet in a secure room, with high assurance.

Having sufficient availability of your systems is critical in the face of denial of service attacks as well as a full chain of custody for your keys and how they interact with other trusted systems as well. And then you need to build and configure all the infrastructure behind the scenes. This includes management systems, infrastructure systems to support business continuity and, of course, disaster recovery. It is extremely important to build a repeatable security process to continually review and continually test. You need to be vigilant and audit on a regular basis to provide adequate protection. And this where IoT security standards come in and the current IoT device cybersecurity capability core baseline. Developed by the National Institute of Standards Technology, their NIST cybersecurity framework is an effective way of analyzing and understanding risk. Device configuration is another key element. This is one of the reasons why the Mirai botnet has been so successful because many default configurations within IoT are very weak, with insufficient protocols or weak requirements for passwords. This is an outdated approach to authentication in the first place, versus more robust certificate-based authentication.

Data protection is another consideration. Device data can give attackers deep insight into how a manufacturing plant operates or a smart grid operates so that they can further compound an attack. Since IoT devices are increasingly used to automate operations with machine learning and AI capabilities, the risk is even greater. In the hands of an attacker, the very command and control of mission critical operations are now at risk.

Finally, another important factor is how software updates are handled. All software has to be signed. PKI should check the authenticity of the software, where it came from, and its integrity–so the contents and meaning haven't changed and they are cleared for the device software update.

Weighing PKI approaches

There are two sides to running enterprise-grade PKI, the management and the infrastructure. Some organizations will try to manage and support PKI in-house or go with a no-frills provider with basic device protections.

Scale and management

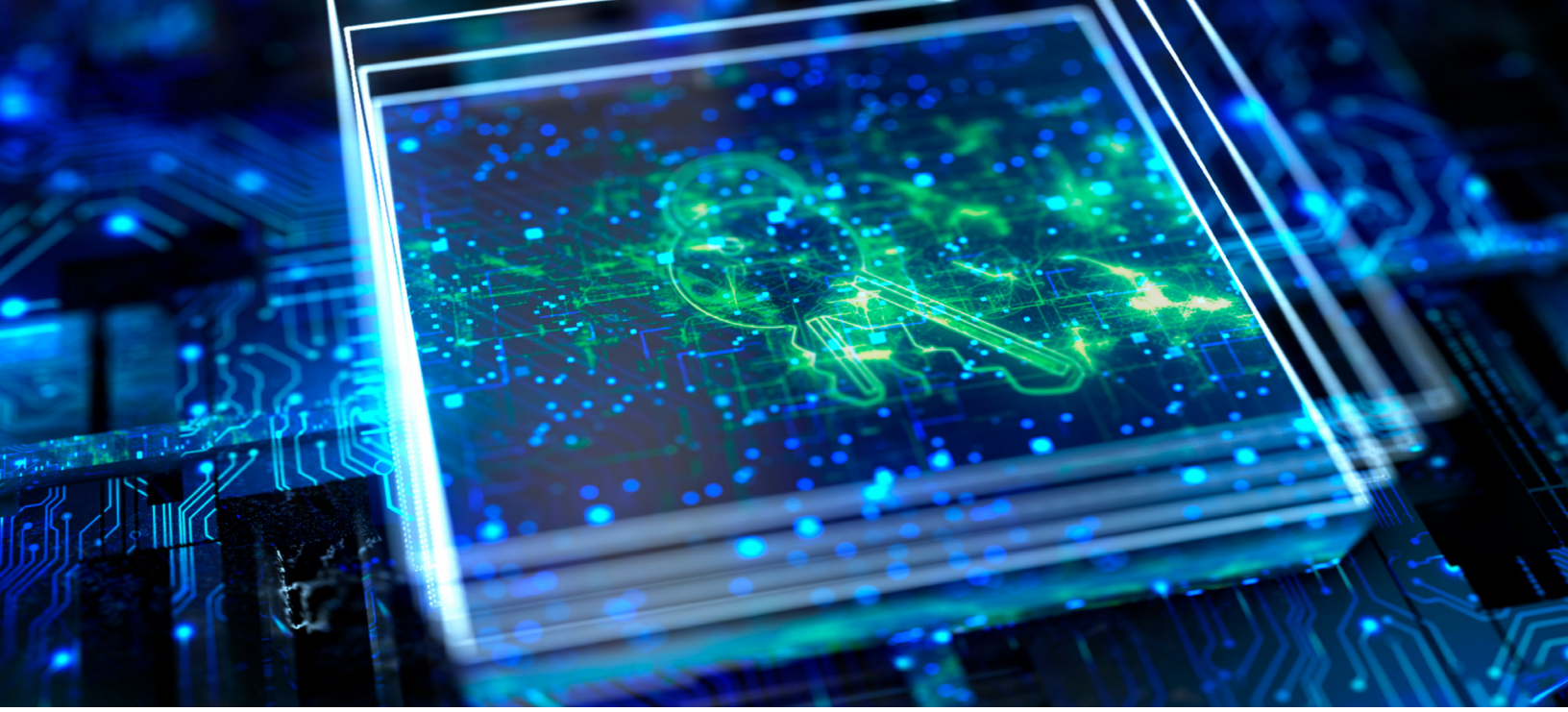
The management part of the PKI involves how you operate a key infrastructure. One of the main elements is a registration authority. So the first thing is to know what devices need to be onboarded and brought into your trusted universe.

That trust actually extends beyond devices, when you are thinking about managing a PKI system. You must trust the people behind the system and have demonstrated due diligence with deep background checks and other ways to audit PKI administration and custody protocols, especially within in-house or offshore operations settings.

One difficulty in deploying PKI is securely embedding the key material into the IoT device.

A second challenge is that chipsets are often very different. The wide variety of different chipsets is accompanied by an equally large number of security architectures. As a result, being able to handle embedded crypto development is critical.

WebTrust certification should be maintained by any proper PKI implementation. It ensures that what you write in your certificate practice statement is your actual operation. Yearly audits will scrutinize your process line by line and ensure everything is in order. So if you're looking at an outsourced PKI solution, you need to ensure that it's WebTrust certified so you can trust it. Given the vast number of IoT devices and how a given IoT infrastructure must scale, auto-renewal of short-lived certificates is another important feature to have within a robust PKI solution.



Infrastructure and expense

WIth any PKI infrastructure, You need to have 24/7/365 operations because attackers don't sleep.

High availability is essential so you need multi-region disaster recovery for business continuity against disasters, man-made or otherwise.

Controlling system access is also essential, where you securely identify people with badges, secure cards, and biometric authentication. The sensitive operations need to be run in an air gap and tempera-shielded secure room. And of course, there must be proper ventilation and air conditioning. Regular data operations are critical as well.

These infrastructure features all add up to extensive capital or operational expenses. Additionally, you will need SDKs for embedded developers for chipset targets. Other requirements include data monitoring and analytics for detecting potential threats, as well as high security modules that protect keys when they are not connected to the internet. A trusted time server and automatic renewal of short-lived certificates are also necessary for scalable protection.

Fortunately, for a provider and expert in offering managed PKI services, the cost of all of these elements are amortized across each certificate. So it scales with your business on a per-device basis.

IoT PKI checklist

What to look for in a robust managed service provider:

- Comprehensive professional services
- Full infrastructure design assistance
- Complete integration with your offering
- Rich X.509 certificates including SAML assertions for authorized operation
- Integration with security architectures of embedded systems
- WebTrust certified: the gold standard for PKI systems ensures security operations and principles are adhered to
- Hyper scale and track record of serving millions and billions of devices
- Protection options for brownfield devices with no built-in hardware security

How Intertrust can help

Intertrust has managed enterprise-grade PKI for more than 12 years with some of the biggest chipset providers in the world. We've issued well over 20 billion keys to 2 billion devices and issued tens of millions of keys every month.

Our PKI service has never had a security breach or concern, and we offer a deep bench of capabilities and flexible provisioning, whether on the factory floor or as is more common today with IoT devices being deployed at scale, in the field.

Our solution is WebTrust-certified with device protection that extends to secure highly vulnerable legacy devices using app shielding and secure key box technologies.

1 https://iot-analytics.com/number-connected-iot-devices

2 https://www.statista.com/statistics/1377569/worldwide-annual-internet-of-things-attacks

Learn more: intertrust.com/pki-for-iot
Contact us: iot@intertrust.com

intertrust®

Building trust for a connected world.