How to Secure IoT Devices with PKI-as-a-Service

EBOOK

Contents

Executive Summary

The term Internet of Things (IoT) was coined by Kevin Ashton in 1999, but didn't become mainstream until early 2014. Security has always been an afterthought of technological advancement, and IoT was no exception. The security industry has been trying to narrow down the best approach to IoT security for years now. These devices have become an easy target for attackers with cyberattacks against IoT devices now very common and sophisticated. The cyberattack surface is rapidly expanding as more and more devices are enabled with internet connectivity. One of the most disruptive events, the Mirai botnet denial of service (DDoS) attack, was orchestrated by leveraging IoT devices and left much of the internet inaccessible for the U.S.

Despite the lack of strong security practices, the number of IoT devices continues to grow. IoT security is top of mind for many organizations, especially those who manage networks with critical devices like power grids, nuclear reactors, patient pacemakers or connected cars. Implementing proven security technologies, such as public key infrastructure (PKI) solutions, can help address these mounting security concerns. PKI has been around for decades and used by enterprises to control access based on the identity of employees or devices on the network. In very basic terms, PKI provides public cryptographic keys that are used for encrypting data and authenticating the identity of communicating parties or devices. The same concept applies to IoT devices, since they should be verified before gaining access to any network resources or cloud services. If properly designed, implemented and managed, PKI can be a very powerful solution for securing IoT devices.

Cloud-based private PKI-as-a-Service (PKIaaS) solutions enable organizations to quickly create and deploy their own private PKI trust hierarchies to secure their networks, IT systems and IoT devices. They eliminate operational complexity and dramatically reduce costs related to operating and deploying an organizational private PKI. Designed to scale for IoT, they also offer complete policy controls, delegated administration, on-demand auditing and reporting.

The Role of PKI in IoT Security

IN THE WORLD OF IOT DEVICES, PKI PRESENTS VARIOUS BENEFITS, INCLUDING:

- A unique, verifiable identity for each device within the ecosystem
- Passwordless authentication between devices and systems
- Strong encryption for data in transit and at rest
- Scalable, proven technology that's been used for decades to secure networks, devices and users
- Automation of certificate provisioning and renewal to support millions or billions of IoT devices

WHAT IS PUBLIC KEY INFRASTRUCTURE (PKI)?

Public key infrastructure (PKI) is a 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. It establishes digital trust and creates a secure communication channel between communicating parties, whether they're users or devices. It uses public-private key pairs to create a trusted ecosystem. When devices communicate with each other, one can authenticate the other and encrypt the communication by using a key pair. It also allows for the validation of data integrity when the transaction is signed.

Using a technology for extended use cases does present some challenges, and PKI is no exception. Let's review some of the challenges you may face when using PKI for IoT use cases, and how to overcome them.

The Challenges

PKI INFRASTRUCTURE COMPLEXITY

PKI has been around for many decades and enterprises use it in various ways, but the set up and operation of PKI is still very complex. A PKI deployment is often unique from other network security applications in an organization because it involves hardware (HSMs), software, policies, operating procedures and stringent security controls for successful operation. When planning for PKI deployment, ensure that the policy, procedures and technical implementation meet the needs of your business now, and in the future, as technology and business needs evolve. Keep in mind that IoT will add another layer of scalability and performance, so if not planned carefully, you may end up needing to redeploy the infrastructure later, which is expensive and time consuming.

In addition, prepare for compliance and regulatory audits. A PKI system holds the keys to the kingdom, so it needs to be protected with stringent security controls. PKI is not a static system and requires strong governance and audits for successful operation.

COMPLEX IOT DEVICE MANUFACTURING ENVIRONMENTS

Deploying PKI for an enterprise network is different than deploying PKI for IoT devices, as most enterprises own their network devices. IoT devices are manufactured and shipped to the consumer through various channels, so security should be considered a must-have feature. Any manufacturing facility, whether it's for small IoT devices or complex ATMs, relies on automation and streamlined processes to operate at full capacity. There are various factors to keep in mind while designing a successful PKI system within an IoT device manufacturing environment:

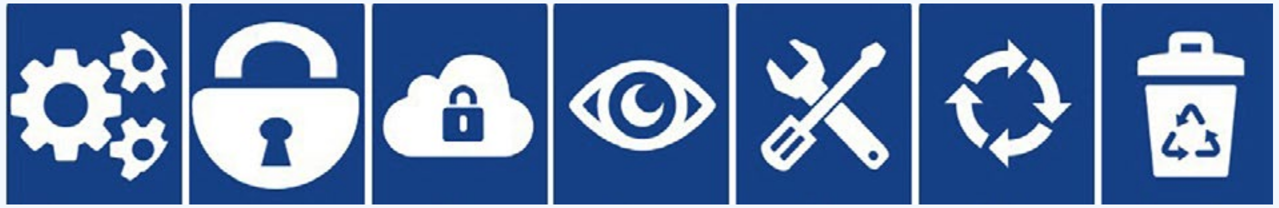
- PKI hierarchy should be defined based on how the IoT device is going to reach the end consumer—if it's going through OEM partners, consideration must be given to how trust will be established with the end device
- Generating a certificate can take a few seconds as it requires complex mathematical calculations, so enough time must be factored into the manufacturing process to allow for this
- Internet connectivity is a risk factor that needs to be considered while designing the PKI system—plan for the effects of the loss of internet connectivity to the manufacturing plant
- Nowadays, large corporations have multiple manufacturing facilities, so consider how to design a PKI system that works for global deployment

PRIVATE KEY STORAGE AND SECURITY

The digital certificate contains a public key and private key pair. The public key is available for anyone to use, and it's associated with the private key. It's extremely important to protect the private key as it allows authentication and data encryption between devices. The best way to generate private keys is within the secure storage of the device, but often IoT devices do not contain a secure chip or storage on the device. In those cases, consider how to store and protect the private keys of the devices.

CERTIFICATE LIFECYCLE MANAGEMENT

The first piece of the PKI puzzle is inserting the certificate into the device during the manufacturing process, but the device also needs to be provisioned, deployed, monitored, updated and eventually decommissioned. The digital certificate does expire and will need to be replaced. The worst-case scenario is that the private key gets compromised and the certificate needs to be reissued or revoked for millions of devices out in the field. Automation is the key for certificate lifecycle management for IoT devices.



Manufacture Provision Deploy Monitor Service Update Decommission

The Solution

HID Global provides a managed cloud-based PKI-as-a-Service (PKIaaS) solution specifically designed to support IoT use cases with completely automated certificate lifecycle management and scale. Our Private Root PKI offers a completely customizable service that provides organizations the flexibility to secure a large, complex network, inclusive of an IoT ecosystem. The Private Root PKI service model includes a dedicated customer management process and security model to ensure your root key material is kept safe.

It allows you to simplify PKI operations by outsourcing the complexity of running a best-in-class PKI without losing control of trusted assets. You get the best-in-class PKI (Trust) infrastructure that aligns with industry best practices and leverages highly secure and audited technical facilities with the expertise to deliver it all. As your business evolves, HID PKIaaS can adapt and scale to your changing needs with complete flexibility to add new services at any time.

KEY BENEFITS

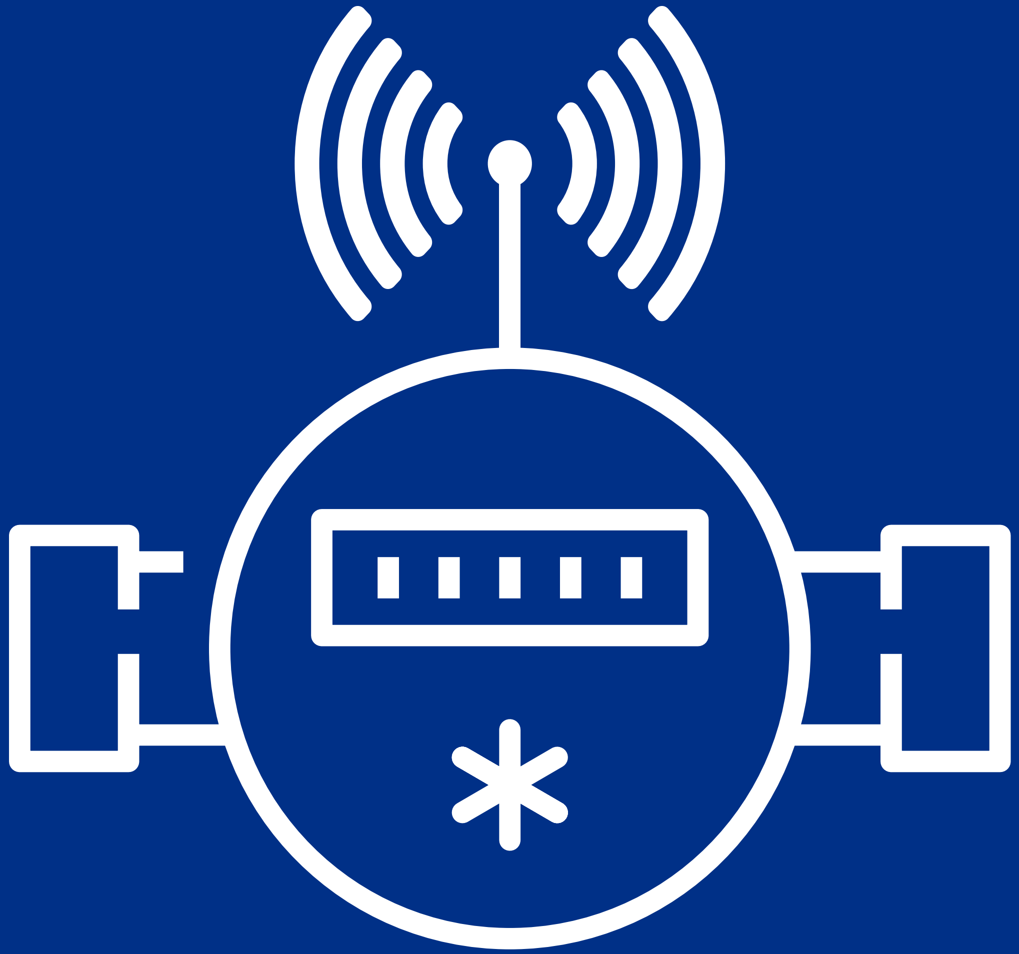
- Design of private trust hierarchy architecture(s) and implementation
- Turn-key root key generation ceremony processes and documentation
- Off-line root key custody management
- Management of on-line issuing CA(s) signing, operations, documentation and security processes
- M of N security control model of off-line assets
- Off-line and on-line key material BCP and disaster recovery process
- Management of all certificate validation processes including HA implementation and highly scalable OSCP and CRL processes
- HSM operations and HA model for continuous operations
- Web-based certificate management portal to support both private and trusted certificate services
- Automation support for MS autoenrollment and other standards-based certificate management protocols such as SCEP, EST and ACME as well as RESTful API
- Guidance and support for current PKI migrations to HID PKIaaS, as well as guidance and recommendations for migration of CA key material obtained in acquisitions

To learn more about this solution, read our **executive brief**.

IOT DEVICE IDENTITY LIFECYCLE MANAGEMENT SOLUTION

HID Global offers an integrated solution in partnership with Device Authority that establishes digital trust, automates device provisioning and manages certificate lifecycle at IoT scale. The Device Authority KeyScaler platform provides trust for IoT devices and the IoT ecosystem to address the challenges of securing the Internet of Things.

To learn more about our combined solution, please visit the **IoT Device Identity Lifecycle Management page.**



Customer Use Case:
Smart Meter Manufacturer

PROFILE:

A large company based in the U.S. that helps a wide range of public service providers (from utilities to cities to industrial complexes and campuses) do more with their infrastructure to improve quality of life in their communities. It enables customers to reach farther through the application of technology and data-driven insights that deliver efficiency and responsiveness.

NEEDS:

The organization was using symmetric key cryptography to protect smart meters but the inherent problem of transmitting the keys used for encrypting and decrypting data was a big challenge. When these keys are shared over the internet, they are vulnerable to cyber-attack. To solve that problem, they needed asymmetric encryption, or in other words public key infrastructure (PKI), to replace symmetric key implementation. The service would be used to generate signed keys from a two-tier certificate authority hierarchy that would then be embedded in smart meters during the manufacturing process.

The service would also be used to generate certificates for use in head-end command-and-control and firmware authentication to the smart meter. Being a large smart meter provider, they had a requirement to support around four million certificate issuances per year to meet customer demand.

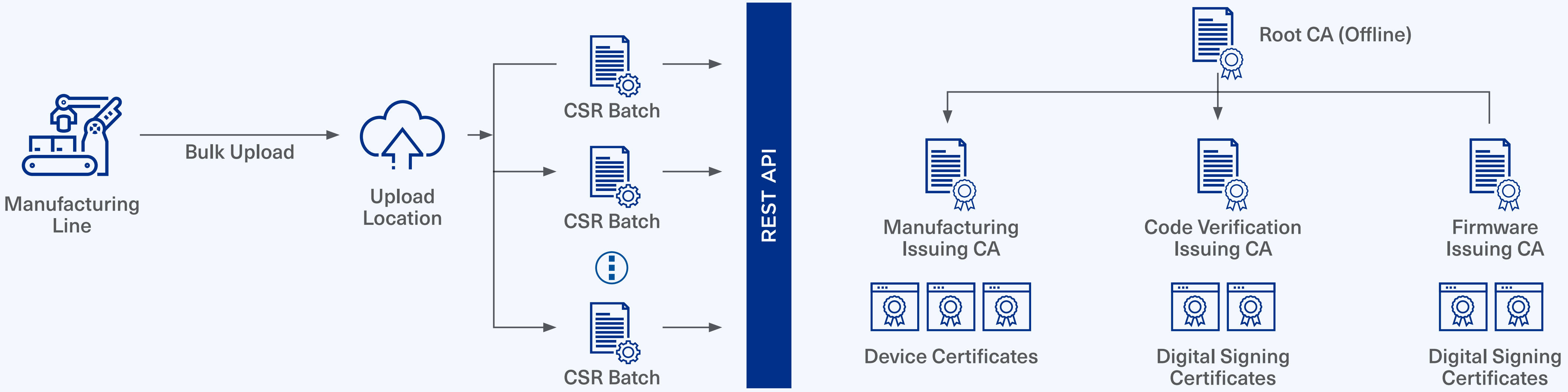
SOLUTION

After evaluating many options, the company chose to implement HID PKIaaS to provide a managed, private solution that encompassed offline root certificate authority and three online issuing certificate authorities.

1. Manufacturing Certificate Authority
   This certificate authority is used for signing endpoint keys. The customer has developed a server that can generate suitable endpoint unique public and private keypairs and submit batches of CSR's to HID PKIaaS for signing. Those batches of signed endpoint certs will be returned and from there distributed to device manufacturers to inject during device manufacturing.

2. Firmware Signing Certificate Authority
   This certificate authority is used for creating the certificate for firmware signing. It is another element in the trust hierarchy but located in the secure cloud and only accessed very infrequently by authorized personnel.

3. Code Verification Issuing Certificate Authority
   This certificate authority is used for issuing certificates for Regional Network Interface (RNI) devices. These devices potentially communicate with millions of endpoints. The unique key pair is generated for each RNI device, the public key is put in a CSR and sent to the CA for signing. The returned certificate is loaded into the RNI, and dynamically distributed to the endpoints for use in verifying signed critical commands from that RNI.



About HID PKIaaS

HID PKIaaS helps enterprises leverage the power of PKI to better protect their networks. It secures every device that accesses your network to create your own Internet of Trusted Things—even within a complex ecosystem. Certificate-based security easily integrates with core business applications and with management functions accessible in the cloud. Plus, robust automation features across use cases take the burden of enrolling devices and updating certificates away from your IT resources. With the shift to short-lived certificates, not automating is not an option.

For one low subscription fee, it's possible to obtain centralized, managed PKI for your organization—without any billing surprises or lengthy on-prem deployments. And because PKI is foundational technology that's seen decades of use in every major OS and online, you don't have to worry about compatibility issues.

KEY BENEFITS

Eliminates the need to run complex CA services

Supports private/public trust model designed for IoT

Automates the issuance of millions of certificates through API or a web-based interface

Enables tracking of a single certificate across a product line

Want to learn more about HID PKIaaS?

SCHEDULE A TIME TO TALK WITH A PKI EXPERT HERE.

hidglobal.com

North America: +1 512 776 9000
Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +44 1440 714 850
Asia Pacific: +852 3160 9800
Latin America: +52 (55) 9171-1108

For more global phone numbers click here

2021-11-23-iams-how-to-secure-iot-devices-eb-en
PLT-05385

Part of ASSA ABLOY