Enterprise Certificate Authority for IoT Device Manufacturing

With widespread market success and a desire to provide its customers with the highest possible levels of security, speed, and technology, a global leader in manufactured electronic devices and the Internet of Things (IoT) worked with Futurex over multiple project phases to deploy a next-generation digital signature infrastructure from the ground up.

The use of smart devices in modern society is growing rapidly, with many consumers owning multiple pieces of sophisticated technology for personal use and even more for business. In the manufacturing industry, an enterprise certificate authority is essential to securing these devices that make up the Internet of Things. Certificate authority and digital signature technology have proven themselves vital components of modern IT ecosystems. They can provide the technology foundation to authenticate firmware, enable secure outsourcing to contract manufacturers, allow sales and technical applications to remotely enable and disable device features, and much more.

A Public Key Infrastructure (PKI) provides the framework for secure communication across systems and is often used in manufacturing environments. Using a PKI, asymmetric public and private key pairs are used to secure and authenticate sensitive data objects. Public keys, which can be widely distributed, encrypt or validate the data. Only the private key, which must be protected, can decrypt or sign the data.

These asymmetric keys are issued by a certificate authority, which is capable of managing entire trees from trusted roots all the way down to unique certificates per device, file, or other object.

The Business Case

An integral player in Internet of Things device manufacturing came to Futurex in need of an enterprise certificate authority to sign firmware files on its devices. Establishing this would meet international compliance standards, enable advanced features to offer their customers, and ensure consistency across their multiple global locations.

With an aggressive timeline to fulfill strong market demands, they approached Futurex for a customized, scalable, high availability-ready solution designed to meet their current and anticipated future needs.

Company Profile: Electronics Manufacturer

With a long history in the technology industry, this publicly traded company in consumer and corporate electronics manufacturing now boasts an enterprise cryptographic infrastructure with the robust scalability to meet its global size and volume. The company maintains numerous manufacturing facilities around the world, with yearly output numbering in the hundreds of millions.

Project Requirements

Requirement: Digitally sign hundreds of millions of manufactured IoT devices per year

The manufacturer needed to digitally sign hundreds of millions of their devices per year during the manufacturing process, in a number of worldwide locations. To achieve the compliance certification they desired, the devices had to be signed by a FIPS 140-2 Level 3 validated cryptographic module.

Requirement: High availability infrastructure, delivering 99.999% or greater uptime

Devices needed to be signed in batches of 10,000+ at a time, so reliability and system uptime was paramount. To fulfill this requirement, a 24x7x365 high availability configuration was required.

Requirement: Rapid design and deployment timeline, with zero-downtime implementation

With a timeline of under three months from initial design to full production implementation, the manufacturer needed to work with a trusted vendor with a proven track record of delivering complex, global projects on time and under budget. Additionally, the production deployment had to be completed without downtime and could not introduce any delays to the manufacturing process.

Requirement: N^{th} degree throughput scalability

The manufacturer required both vertical and horizontal scalability to accommodate future growth without affecting production capabilities.

Requirement: Automatic synchronization of information between manufacturing sites

With frequent certificate updates, hardware at all manufacturing sites needed to be automatically synchronized to ensure timely and consistent production can occur regardless of location.

Requirement: Initial signing by a unique key per device group, with the ability to seamlessly transition to a unique key per device

The manufacturer initially wanted to sign all devices with a unique certificate per device group. Following this initial deployment, they needed the ability to substantially increase capabilities to support a unique certificate per device.

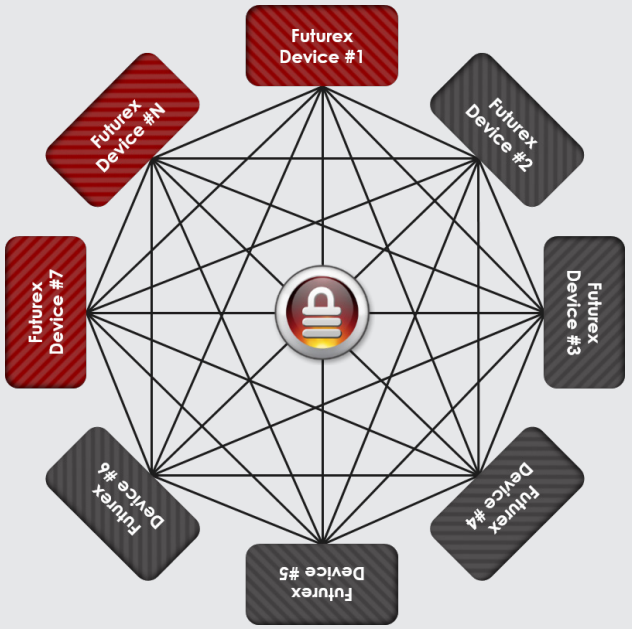
Requirement: Design, development, and deployment guidance from experienced cryptographic solutions experts

Providing compliant, scalable hardware is only one part of building a robust infrastructure. To guide them on best practices, implementation, and future enhancements, the manufacturer needed support from a team of proven industry experts.

Technology Profile: Masterless Peering

Because this manufacturer has geographically dispersed production sites, their device signing solution incorporated several Guardian9000s. This built a centralized management platform, incorporating Masterless Peering technology to ensure keys, certificates, and configuration details are replicated seamlessly between all manufacturing locations.

- Active-Active redundancy between all managed Futurex devices, creating a high availability-enabled environment
- Equal distribution of cryptographic resources to multiple host applications across multiple sites
- Automatic replication of keys, certificates, and configuration details between all devices in the environment
- Seamless scalability when adding new devices



Enterprise Cryptographic Infrastructure: a Multi-Phase Approach

PHASE ONE

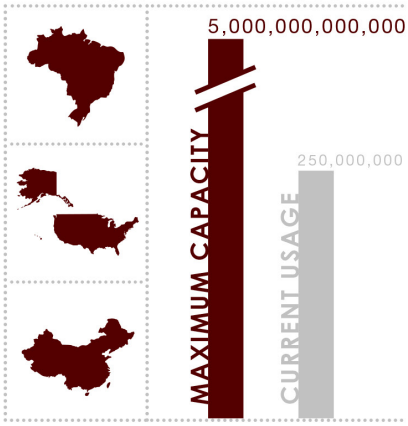
UNITED STATES
manufacturing facility
Corporate headquarters and Network Opperations Center.
01

BRAZIL
manufacturing facility
Enterprise device manufacturing facility
02

CHINA
manufacturing facility
Enterprise device manufacturing facility
03

6 WEEKS

ANNUAL SIGNATURE THROUGHPUT



PHASE TWO

INDIA ADDED
manufacturing facility
Consumer and Enterprise device manufacturing facility.
04

SAS9000 ADDED
secure attached storage
Large-scale storage of PKI key pairs for scalability.
05

SCALABILITY
infinite
Nth degree scalability ensures demand will never outpace capacity.
06

1 WEEK

PHASE THREE

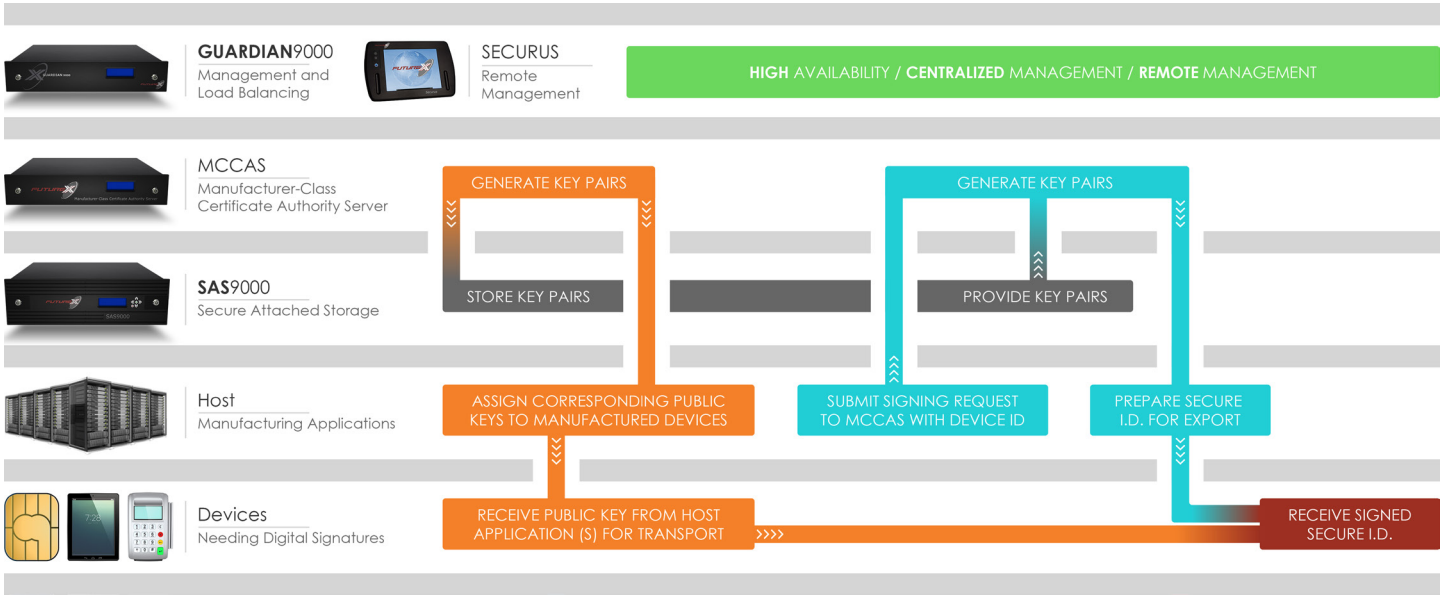
VIRTUCRYPT
virtucrypt VIP
Cloud-based environment for scalability and testing.
07

SOFTWARE
analytics
Support for new algorithms, protocols, and device types.
08

INFRASTRUCTURE
optimal
Future-proof design ensures emerging needs can be met.

3 WEEKS

Case Study: Enterprise Certificate Authority for High Volume Manufacturing



The Solution

To fulfill the manufacturer's requirements, the Futurex Hardened Enterprise Security Platform, was implemented, including the Manufacturer-Class Certificate Authority Server for PKI management; the Guardian9000 for centralized configuration, monitoring, alerting, and load balancing; and the Securus for remote management. Following a successful deployment, they expanded in later phases to include the SAS9000 for large-scale certificate storage and VirtuCrypt's cloud-based services for testing and on-demand scalability.

All Futurex devices are digitally signed by the Futurex-Signed Certificates service, creating a trusted domain for the entire environment. With this, Futurex devices on the manufacturing floor can securely communicate across sites, with full assurance of firmware and device authenticity.

In their environment, increases in processing throughput can easily be accommodated, along with expansion to new manufacturing sites. Additional Futurex solutions may be easily implemented, allowing their manufacturing environment to be scaled in a cost-effective, turnkey manner. Together this platform meets the needs of the device manufacturer in a convenient, secure manner capable of continued growth.

The Results

Since implementing their enterprise certificate authority, the manufacturer's requirements have been met or exceeded, and their devices have been FIPS 140-2 validated. The digital signing process is integrated directly into the production line, all while the manufacturing floor maintains 100% uptime.

After two years of successful production, Futurex helped them expand device signing functionality to an additional manufacturing facility in Brazil, adding consumer-grade devices to their already-robust enterprise line. They accomplished this by adding the SAS9000, a scalable, hardware-based solution for high-volume data encryption and storage to store generated key pairs.

Following that, the company continued to expand scalability efforts by working with VirtuCrypt, a Futurex company and the provider of the industry's first and only Hardened Enterprise Security Cloud.

Following a successful deployment in all manufacturing sites assisted by Futurex's Solutions Architect team, this manufacturer has seen additional operational and cost efficiencies for its worldwide locations, elevated its devices to FIPS 140-2 validation, secured firmware releases, and built assurance that its data protection infrastructure is poised to grow alongside the organization.

Engineering Campus 864 Old Boerne Road, Bulverde, Texas 78163 USA
TF 800.251.5112 P +1 830.980.9782 info@futurex.com
WWW.FUTUREX.COM