WHITE PAPER

Zero Trust Manufacturing

How to navigate complex supply chains to build trusted IoT devices

KEYFACTOR

Table of Contents

Introduction

The rapid adoption of cloud computing and the Internet of Things (IoT) is ushering in billions of connected devices that, left unsecured, represent a significant risk to businesses and consumers. Connected things include a variety of IoT endpoint devices across several critical infrastructure segments, including utilities, automotive, healthcare, retail, and building automation.

Complex manufacturing supply chains make it difficult to build electronic devices that can be trusted by both the manufacturer and device owner. A dizzying ecosystem of contract manufacturers, component suppliers, software developers, logistics companies, and systems integrators makes for an environment in which multiple security vulnerabilities can mushroom.

Manufacturers need to take a Zero Trust approach.

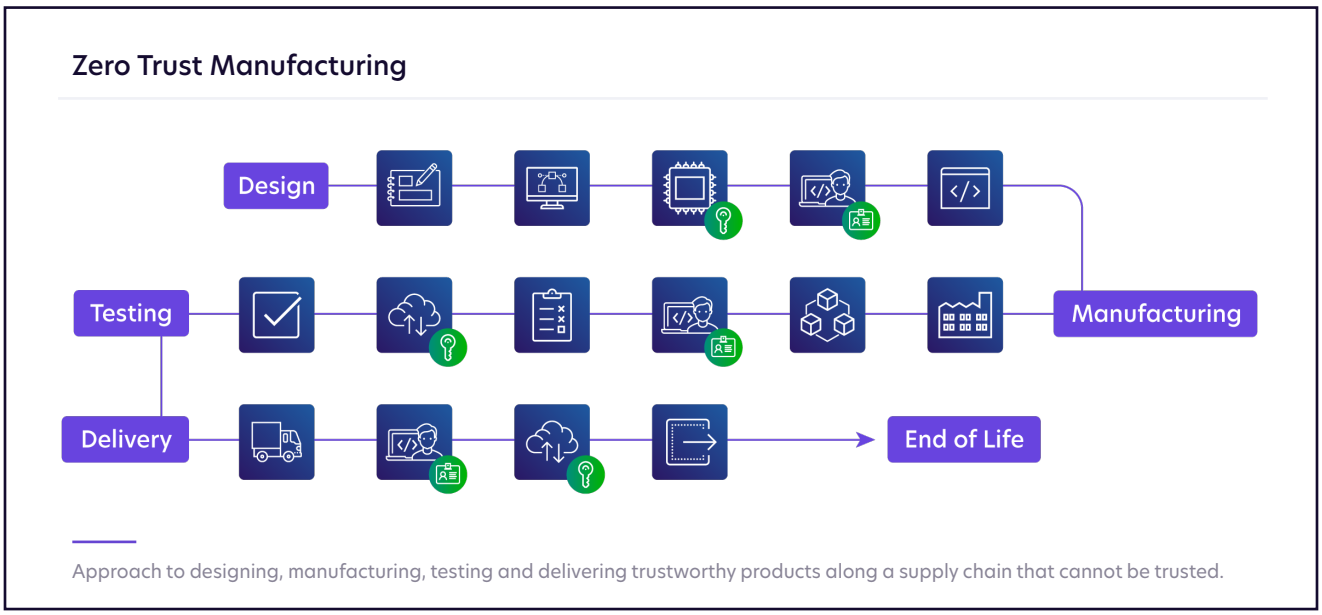
This complex ecosystem means that attackers have many avenues to compromise a device's security as it is being designed, manufactured, tested, and delivered. The original equipment manufacturer (OEM), the company usually responsible for bringing the product to market, is often focused on building products that meet its customers' specifications while minimizing manufacturing and delivery costs. Frequently an afterthought, security is too often bolted on as a feature rather than being a critical element designed at the start of a product's lifecycle.

With many supply chain partners, the reality is that you cannot trust the manufacturing process's security to ensure that the hardware, firmware, or credentials of the device have not been altered. To ensure the trustworthiness and safety of devices, manufacturers need to take a "zero trust" approach and design security into the devices while maintaining effective security controls throughout the manufacturing process and product lifecycle. A zero trust manufacturing approach gives manufacturers flexibility when moving production to a different location with little downtime.

What is Zero Trust Manufacturing?

IoT devices are manufactured and deployed along a supply chain that inherently can't be trusted.

Zero trust manufacturing is an approach to manufacturing trustworthy electronic, industrial control, and IoT devices along a supply chain that inherently can't be trusted. Zero trust manufacturing is not achieved by any single technology. Instead, it is an approach to designing, manufacturing, testing, and delivering products that can be trusted by the owner or operator. Manufacturers can use this zero trust approach on products as simple as electronic components or as complex as medical devices, smart meters, automotive control systems, telematics devices, or building automation controllers.



Approach to designing, manufacturing, testing and delivering trustworthy products along a supply chain that cannot be trusted.

Traditional manufacturing supply chains involve dozens or even hundreds of companies that perform various tasks to bring a product to market. An electronics manufacturing supply chain includes design houses, OEMs, contract manufacturers, component suppliers, contract software and systems developers, logistics companies, and systems integrators.

OEMs often contract with a supply chain of global partners to minimize costs, which can inadvertently vastly expand the potential for IP theft and nation-state attacks. Analysts estimate that intellectual property (IP) theft costs the U.S. economy as much as $600 billion per year.1 Global manufacturers use contract manufacturers and suppliers with operations in China, Thailand, and the Czech Republic—countries known to be involved in IP theft.

Zero trust manufacturing architecture contains many concepts, including hardware-based security, embedded security, public key infrastructure (PKI), key and certificate lifecycle management, device trustworthiness, code signing, and authentication. When implemented holistically, a zero trust manufacturing architecture will ensure that a product's firmware, data, and digital credentials can be trusted at each step of the manufacturing supply chain and beyond.

Security vulnerabilities are bolted on rather than designed in.

Beyond Zero Trust Networking

Forrester Research Inc. originated zero trust networking in 2010. Google adopted the approach a few years later, followed by broader adoption by the tech industry. Zero trust networking is an IT security concept that requires strict identity verification for every person and device accessing a private network, regardless of whether they are within or outside a network perimeter.

[1] IP Commission report (2017)

Given that network communications may transit multiple networks that cannot always be trusted and that many attacks start from within the network, zero trust networking leverages several controls to ensure that only trusted parties are able to access the network. Central to the zero trust networking approach are the concepts of least-privilege access, multi-factor authentication (MFA), micro-segmentation, and access controls.

Zero trust networking strives to ensure that users and devices can be verified before they access the network. The problem is that oftentimes device identities cannot be trusted, fundamentally undermining the zero trust networking architecture. In fact, unless a zero trust manufacturing model is followed, device credentials can be more easily stolen, enabling attackers to impersonate devices and users to gain unauthorized access to a network, thus limiting the benefits of zero trust networking. Implemented together effectively, zero trust manufacturing and zero trust networking ensure that devices, applications, data, and communications can be trusted.

Why Zero Trust Manufacturing Matters

According to Global Market Insights, the market for electronic manufacturing services (EMS) is expected to grow from $500 billion in 2019 to $650 billion by 2026[2], a five percent compound annual growth rate (CAGR). The EMS market comprises global companies that design, manufacture, test, distribute, and provide return/repair services for electronic components and assemblies for OEMs.

As OEMs bring products to market faster and more cost-effectively, they rely heavily on EMS companies as partners. According to the report, the EMS industry is being driven by:

- Growing need to accelerate time-to-market.
- Growing penetration of smartphones and smart devices.
- Production shifts to Asia Pacific (APAC) countries with low labor costs.
- Growing opportunities in medical device manufacturing in North America and Europe.
- An increasing trend toward outsourcing by OEMs to enhance productivity.
- Increasing electrification of vehicles and an increasing shift toward electric/autonomous vehicles.
- Proliferation of smart home devices in developing nations.

The fastest-growing EMS market region, the APAC, is expected to achieve an eight percent CAGR from 2020 to 2026. The ongoing China–US trade war is shifting production from China to Southeast Asian countries as OEMs seek to minimize supply chain risks and avoid tariffs.

In addition to enabling the production of secure and trustworthy devices, zero trust manufacturing enables OEMs to more rapidly shift contract manufacturing to different original design manufacturers (ODMs) and countries. This provides a meaningful competitive advantage that enables manufacturers to leverage their full supply chains to accelerate time-to-market, minimize production risks, and maintain cost competitiveness.

[2] Electronics Manufacturing Services Market Forecasts 2020–2026, Global Market Insights, July 2020

Challenges

Cyber-Attacks and Breaches

Manufacturers and device owners are subject to a range of debilitating cyber-attacks. A breach of manufacturing processes leads to device vulnerabilities against which owners must defend, whether they have identified the vulnerability or not. Increasingly, actors with malicious intent use sophisticated means to steal credentials and attack systems. According to the Verizon 2021 Data Breach Investigation Report, over 40 percent of breaches involved hacking, and of those breaches, 89 percent involved some sort of credential abuse (use of stolen credentials or brute force).[3]

Stolen user and device credentials are typically the basis for attacks designed to steal assets, compromise web applications, and abuse privileges. The report also found that 80 percent of breaches were by external actors.

Stolen credentials, including private keys and digital certificates, directly affect businesses. In a study by the Ponemon Institute, sponsored by Keyfactor, 98% of organizations experienced at least one incident involving key misuse or theft in the past 24 months and 61% say these incidents are very serious.[4]

Ensuring that private keys and digital certificates are protected, kept private, and managed securely is critical to protecting devices and applications against sophisticated cyber-attacks across the supply chain.

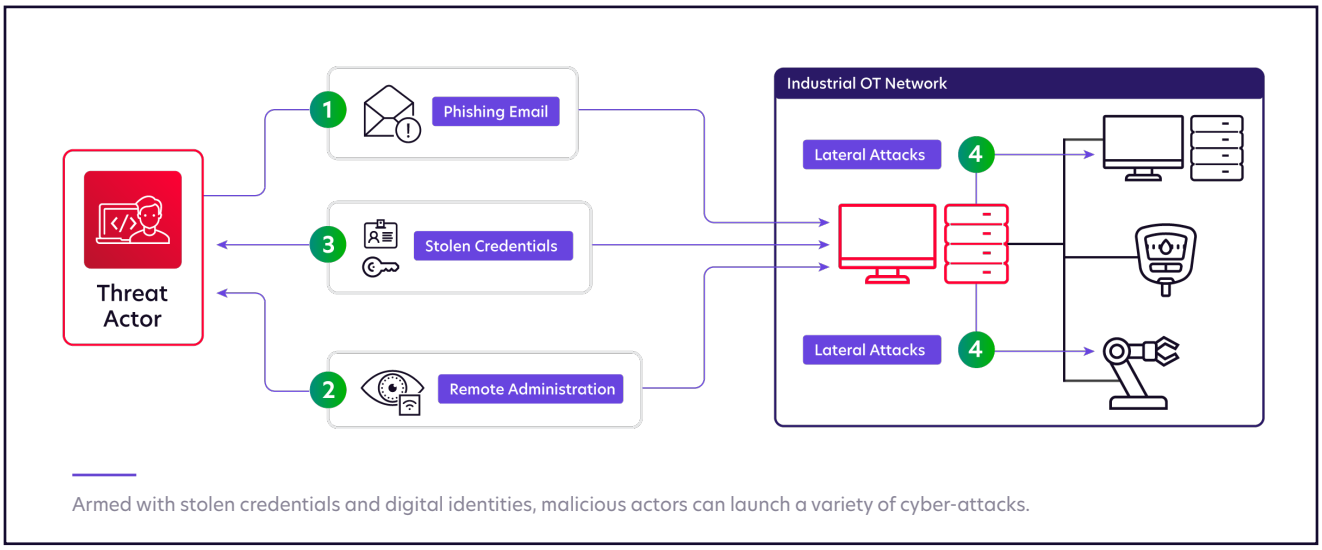
98%

of organizations experienced incidents of key misuse or theft in the past 24 months.

[3] The Verizon 2021 Data Breach Investigations Report, Verizon, 2021

[4] State of Machine Identity Management Report, Ponemon Institute + Keyfactor, 2022

IoT Threats and Vulnerabilities



Armed with stolen credentials and digital identities, malicious actors can launch a variety of cyber-attacks.

Man-in-the-Middle

Using stolen credentials, an attacker can impersonate a user, decrypt traffic destined for that user, and modify responses. These man-in-the-middle attacks are relatively easy to carry out if the traffic between endpoints is not authenticated and encrypted. This can be avoided entirely by using PKI-based digital certificates, as is done today with web browsers.

Root CA Impersonation

Compromising a root CA enables the attacker to authenticate rogue devices and users on the network. This type of attack is a bit more challenging to carry out, but it is quite devastating once it succeeds. If an attacker can get ahold of the root key to a CA, they can set up their own root CA, which will be recognized as legitimate. This is why the root CA is arguably the most important thing to protect. Root certificates should be stored only in FIPS 140-2 level 3 or Common Criteria EAL 4 on security compliant hardware.

Unauthorized Firmware Updates

Compromised credentials used to sign code can enable modification of the firmware and the uploading of unauthorized, modified firmware. When code is signed, it is first hashed, and when it is installed, the authorized installation instance must include a way to check the hash against a known good copy. All this can easily be accomplished using PKI-based authentication.

IP Theft and Counterfeiting

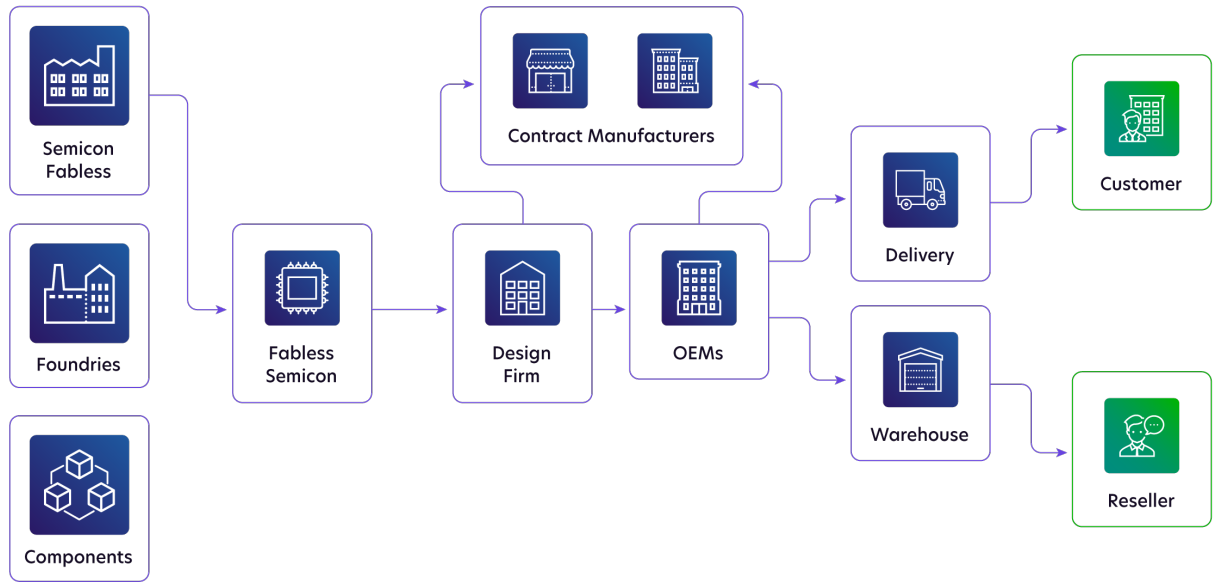
Compromised credentials enable companies to steal intellectual property and bring counterfeit products to market. This can be avoided by including a strong identity with authentic devices. One of the most effective ways to do this is to embed a digital certificate with a unique identifier in the device, preferably in a secure hardware-based chip, for example, a secure microcontroller conforming to the requirements of FIPS 140-2 level 3 or Common Criteria EAL 4 or higher for secure certificate and key storage. In addition, it is important to make sure that workers in manufacturing facilities do not have access to root keys so that they cannot make duplicates of the secure provisioning system.

IoT Manufacturing Supply Chain Complexity

Manufacturers have their own sets of suppliers, subcontractors, and downstream electronic contract manufacturers (ECMs). In some cases, supply chains for creating just one product may include dozens or more than 100 partners. For instance, building an aircraft might require a supply chain of more than 1,000 companies.

When buyers have a well-defined set of design and product specifications, they will contract with an OEM that specializes in manufacturing products that fit their specifications. OEMs typically do not have in-house design services to provide customized equipment. However, they will provide development and prototyping before manufacturing the product. OEMs often manufacture products in house, but if it is more cost effective, they will outsource production to an ECM that can manufacture products to their specifications.

When buyers have a general idea of their product requirements but lack complete specifications, or when they are looking for products to resell as part of a solution, they contract with an ODM. ODMs have full design, development, and manufacturing capabilities. Oftentimes, an ODM will have a catalog of products that have been designed to meet common usage requirements. ODMs own the IP of the products they provide while allowing customers to sell them under their own brands. ODMs either manufacture the product in-house or subcontract the work to an ECM.



Supply Chains include dozens to hundreds of Contractors and Vendors, presenting many opportunities for compromise.

Apple, ABB, BMW, Dell, HP, IBM, and Schneider Electric are examples of OEMs. Some OEMs also operate as ODMs, including DellEMC, which allows its OEM partners to resell Dell products under the OEM's brand. Other ODMs, including Lanner Inc. and Supermicro, specialize in manufacturing networking and server equipment that other OEMs rebrand and resell, often loading their own operating systems and firmware onto the devices.

Both OEMs and ODMs often subcontract manufacturing outside of their region to ECMs. ECMs typically specialize in certain types of products and provide scalable manufacturing costs effectively.

Building an IoT device requires integrating electronic components, embedded software, cryptographic libraries, hardware, and other material or enclosures. Without a strong PKI management system and process to protect digital identities and credentials, it is nearly impossible to ensure the integrity of an IoT device.

Public Key Infrastructure (PKI) Management Complexity

PKI consists of a set of hardware, software, and policies for managing, distributing, and using digital certificates for public key encryption. PKI facilitates the authentication of users and devices when passwords are inadequate. In cryptography, PKI refers to the binding of a public key associated with an identity (person, organization, or device) to a digital certificate. The binding is established through a process of registration and issuance of certificates with a CA. The X.509 standard defines the most commonly used format for public key certificates.

We all use PKI every day. It is used to validate the identity of a website and to authenticate access to email or a company's IT systems. PKI is a well-established model for handling authentication in enterprise IT environments where users (clients) must authenticate the server, and vice versa.

Implementing and managing PKI in manufacturing processes to enable manufactured devices to support PKI is more complicated. Many components are required to establish a robust PKI capability in the manufacturing process, including:

Root of Trust (RoT)

A RoT is the foundation upon which all secure computing operations are based. Installed on a device, a RoT contains the keys used for cryptographic functions and enables a secure boot process. RoTs can be implemented in hardware, making it immune to malware attacks. A RoT can also be implemented as a security module within processors or a system on a chip (SoC).

Root CA

A root CA provides further trustworthiness along the chain of trust of digital certificates.

Certificate Authority (CA)

Implementing an on-premises CA or integrating with a third-party CA enables the validation of digital certificates.

On-device key generation and storage

Generating keys on a device enables a private key to be known only by the device itself. Stored securely on the device, the private key enables the device to attest to its own identity.

Device management

PKI lifecycle-management tools should be integrated into the device-management system so that generating key pairs and updating the PKI is a seamless process.

Mutual authentication

The best way to establish trust between IoT endpoints is to use mutual authentication, in which both the client and server are authenticated. Implementing client-side certificate authentication, whereby the IoT device itself owns the private key and only the public key is shared with the other party, is critical to ensuring the integrity and trustworthiness of the device.

Code signing

The process of digitally signing executables and scripts to confirm the author of software.

Cryptographic software libraries

Using strong crypto-libraries like WolfSSL to handle certain crypto-operations, including encryption, trusted platform module (TPM) operations, and authentication, is critical to protecting a device.

PKI lifecycle management

Managing the PKI lifecycle is the most complicated part of implementing PKI, and also the most important. Doing so enables the secure transfer of devices between supply chain partners. The lifecycle includes:

- The root signing ceremony.
- Key and certificate management updates.
- Revocation.
- Transfer of ownership.
- End-of-life.

PUTTING THEORY INTO PRACTICE

Best Practices for Zero Trust Manufacturing

To implement zero trust manufacturing and ensure that devices are trustworthy, manufacturers should embrace the following best practices.

Hardware-based security

Leverage device-based, tamper-resistant hardware secure elements, TPMs, or hardware secure modules (HSMs) to create a trustworthy RoT.

On-device key generation

Private keys should be generated and stored securely on the device so that it can attest to its own identity.

PKI management

Implement and automate PKI and key/certificate lifecycle management.

Secure communication with end-to-end encryption

Implement encrypted SSL/TLS or IP VPN communications to ensure data privacy.

Secure bootstrap certificate

Replace the initial bootstrap certificate with an updated certificate to ensure that the device boots up with the intended firmware.

Enable mutual M2M authentication

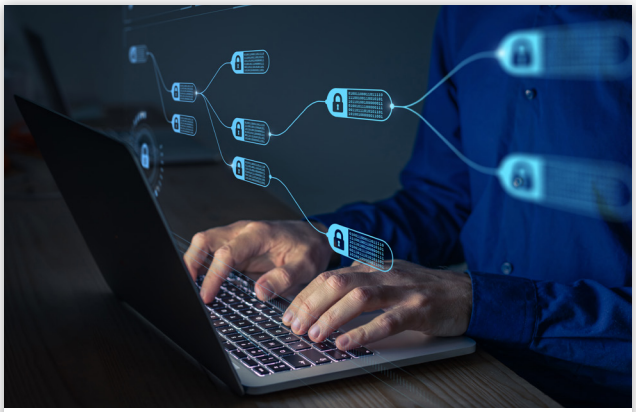
Implement strong user access controls and machine-to-machine (M2M) mutual authentication.

Centralized code signing

Ensure that firmware updates are signed by the developer and authenticated by the device before being installed.

Keyfactor EJBCA

EJBCA Enterprise is a full PKI solution with all the necessary components to set up a complete deployment for industrial grade manufacturing supply chains or IoT product design and delivery.



PKI for Product Security

Secure connected products and IoT devices by design with unique certificate-based identities.

PKI for Manufacturing

Ensure trust in the manufacturing supply chain and industrial IoT (IIoT) environments

Deploy your way

EJBCA can be deployed as a turnkey SaaS PKI, in your AWS or Azure environment, or as a turnkey software or hardware appliance. It can also be deployed alongside Identity Authority Manager (IdAM) an industrial-grade registration authority.

Scale without limits

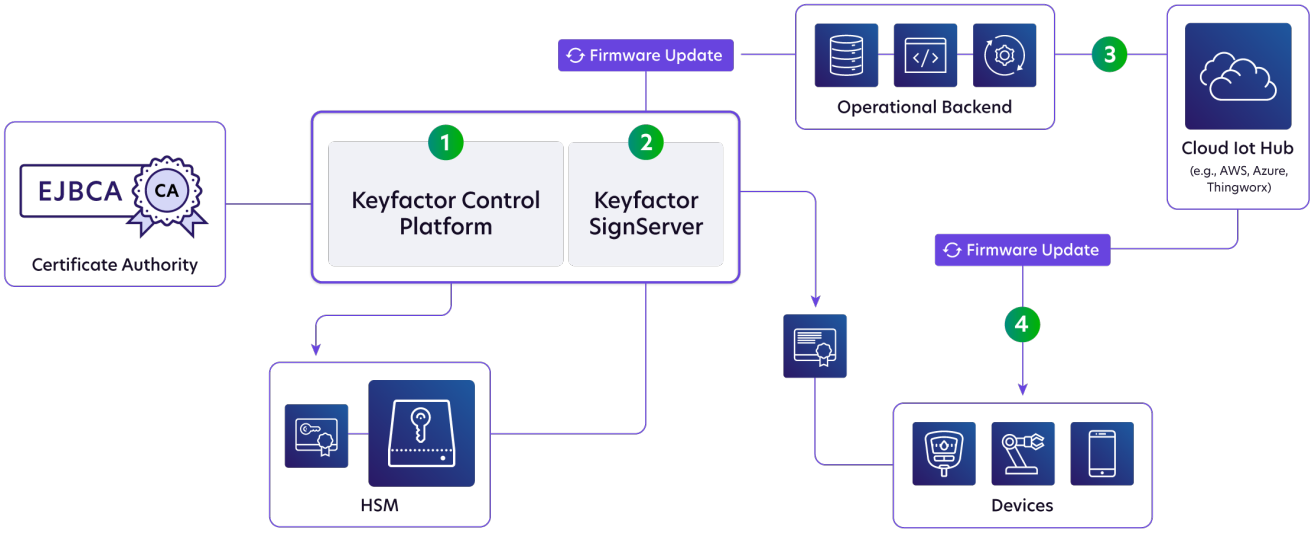
EJBCA can be scaled to handle billions of certificates. Spin up new certificate authorities, registration authorities, and validation authorities as needed to scale as your manufacturing environment grows.

Comply with cyber-security requirements

EJBCA Enterprise also offers detailed, signed audit and transaction logs, role-based authorization and extensive support for HSMs.

Keyfactor Control

Keyfactor Control is an end-to-end, identity security platform for connected devices that makes it easy and affordable to ensure the trustworthiness of devices and software during manufacturing and the device lifecycle. Keyfactor enables the management of PKI processes from design to end-of-life, enabling manufacturers to secure devices across a complex, untrusted supply chain.



Security by Design Simplified

By embedding Keyfactor's software-based agent and PKI orchestrator within the device or device firmware, OEMs are able to streamline and scale the management of the lifecycle of keys, trust anchors, and signed code. Keyfactor's agent is designed for Windows and Linux-based operating systems and can leverage embedded hardware-secure elements, including TPMs and on-device key generation functionality and cryptographic operations.

On-Prem and Hosted PKI

Keyfactor Control provides a state-of-the-art PKI technology delivered as a standalone system or on-demand from the cloud with a highly secure, customer-dedicated root CA and no shared infrastructure. Keyfactor's cloud-hosted platform scales to support millions of devices and is designed to keep PKI operating at peak performance. Keyfactor Control issues unique digital identities for IoT devices, establishes RoT for IoT systems, and enables secure firmware signing.

Centralized Code Signing

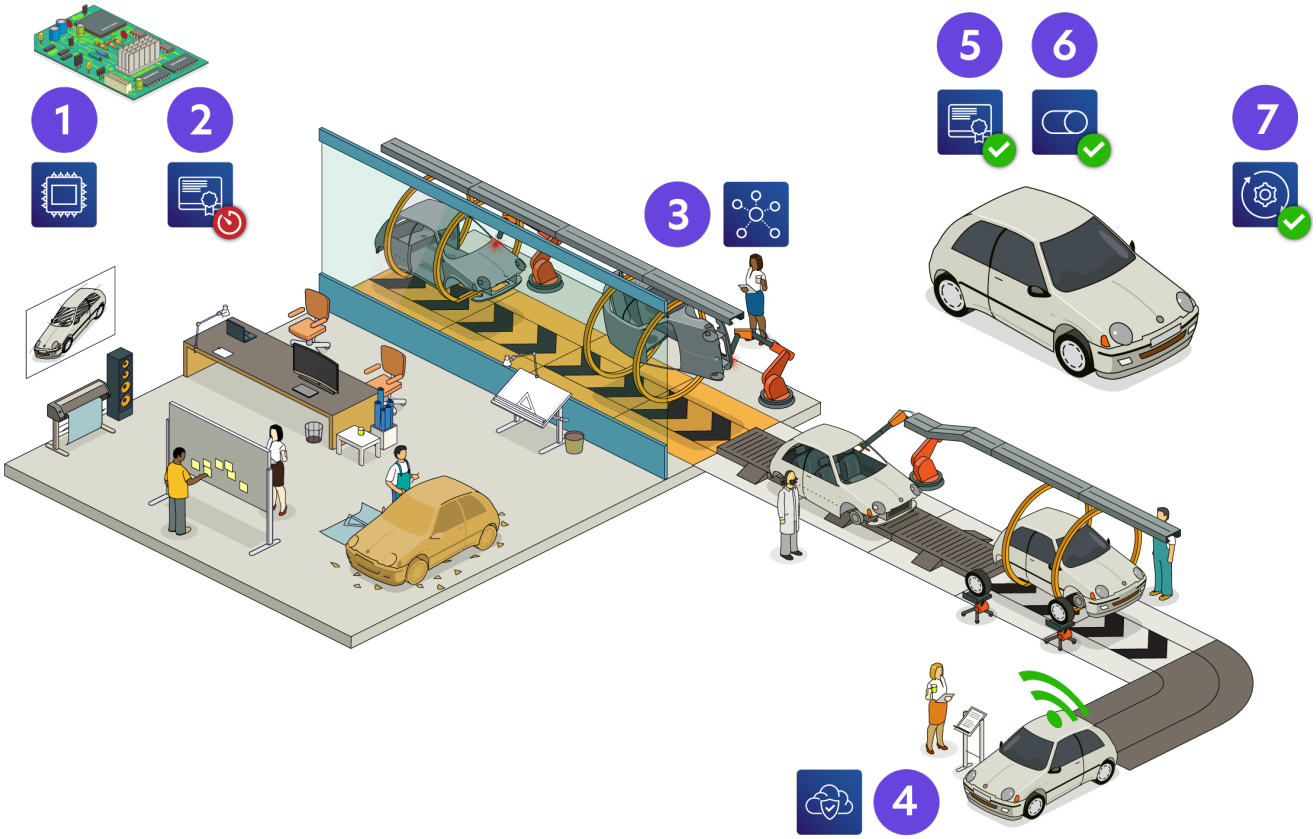
Keyfactor SignServer is a highly scalable and versatile digital signing platform, including support for timestamping services. SignServer allows development teams and manufacturers to digitally sign firmware or software before it is deployed on the manufacturing floor or to connected devices in the field. This ensures maximum integrity and security for over the air (OTA) software or firmware updates.

Visibility and Compliance

Keyfactor's available, fully redundant infrastructure is hosted in a SOC 2 Type II documented environment, including root key protection with multi-part authentication and FIPS 140-2 level 3 validated HSMs.

Bootstrap Certificate Implementation Example

The following describes the bootstrap certificate and registration handling vetting process.



Step 1

An initial certificate is generated on each device using on device key generation (ODKG).

Step 2

A bootstrap certificate can be a self-signed certificate that is not chained to a RoT and requires no CA.

Step 3

When the device is created on the manufacturing line, sufficient information/metadata is collected about the device to be used for the vetting process.

Step 4

After the vehicle is turned on for the first time or during QA/ testing, a registration request is processed and presented along with specific manufacturing information.

Step 5

The bootstrap certificate in each device is replaced with a real certificate only after the registration handling process has been completed successfully.

Step 6

The device is fully provisioned, and the official certificate is activated.

Step 7

The Keyfactor platform and certificate automation will be used to re-enroll/ replace/revoke certificates over the lifetime of the device and replace credentials as needed.

Use Cases and Applications

Healthcare

The ever-expanding world of network-connected medical devices has led to a need for stronger authentication. Medical devices are often counterfeited due to their high cost and value, and this can lead to challenging issues, not the least of which is patient harm. Unless the manufacturer has a way to positively identify that their devices are authentic, there is a high risk that rogue devices will enter the marketplace. A device manufacturer must have the ability to positively identify those who can access, manage, and operate the manufacturing line. Regardless of who the manufacturing system operator is, the device owner must be able to ensure that the operator cannot compromise the integrity of the device or access any secret keys that would enable counterfeiters to manufacture devices that appear to be authentic. As the device moves through the supply chain from the manufacturer to the end user, it is important to ensure that device integrity remains in place and that everyone handling the device at every stage is authenticated and authorized to do so.

After the device has made its way to the end user, a different set of challenges arises. In some cases, the end user is a healthcare delivery organization where the device is used in a controlled environment, such as a hospital room. In other cases, the device may be used in a home care environment or be implanted within a patient. Each of these scenarios leads to different approaches to how security needs to be managed.

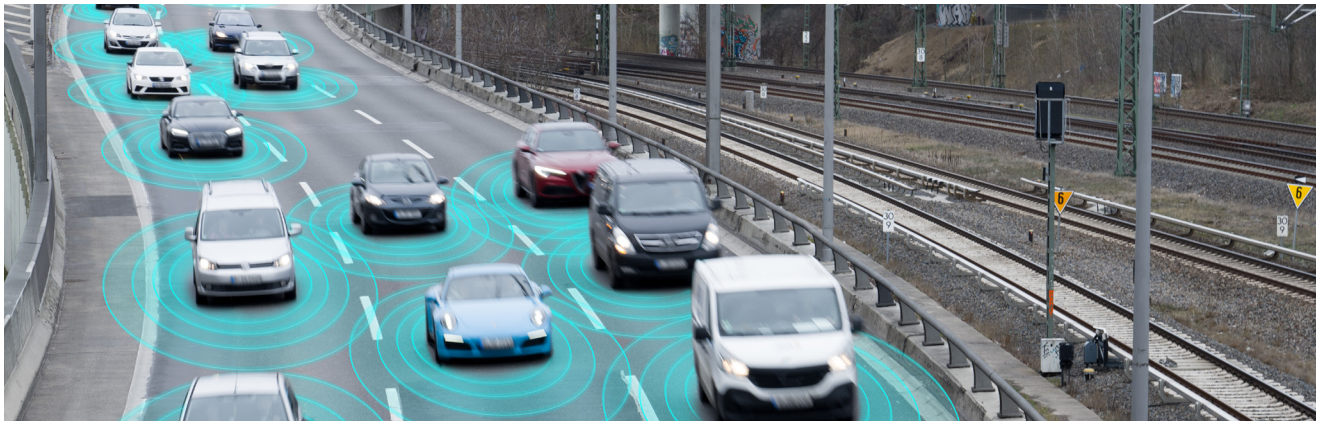
In the case of a device that never leaves a hospital (e.g., fixed MRI machine), it may be possible to store secret keys in something like an HSM and rely on available resources to provide strong authentication and cryptography operations. Here, network connectivity must be readily available in case any changes to the system related to security are needed, or if it becomes necessary to revoke and replace compromised identities. This scenario becomes more complicated when devices are placed in private homes, where consistent connectivity may be a problem, and even more complicated when the device (e.g., a pacemaker) is implanted in a patient. A provider of secure identities and provisioning must take these multiple, complex scenarios into account when designing the system.

Utilities

The utilities industry has a long history of operating highly reliable power generation, distribution, and transmission networks. These systems have been managed both within the power-generation environment and through substations and the use of Operational Technology (OT) control systems, including Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCSs), among others. Until about the turn of the century, utility networks were walled off from the outside world, and their control-system networks operated using protocols that were not compatible with modern IT-based networks. Today, power utility networks are being forced to merge their OT and IT networks in order to more effectively communicate and enable remote access to the OT environment. This enables system operators to manage and monitor far more locations and applications with far fewer resources. It has also led to the need to uniquely identify and authenticate both users and devices on the network, especially because many of the systems and devices used in utility networks are mission critical, and their misuse can lead to massive economic effects or even death.

Transportation

The transportation industry has lately shown great interest in essentially turning vehicles into connected, electronic devices. The most interesting application is seen in autonomous vehicles, which operate by communicating with an extended network of sensors as well as directly with humans. As the popularity of self-driving vehicles continues to grow, so does the need to positively authenticate them to the electronic charging network, which must have the ability to authenticate both the vehicle and the user, as well as the payment method used for purchasing electric charges.



Industrial Control Systems (ICS)

Like power utilities, the OT environments used in manufacturing have long relied on ICS networks. Thus, to remain competitive, ICS manufacturers have had to become more connected to IT. The world of industrial manufacturing includes everything from food and pharmaceuticals to military equipment, weaponry, and of course oil and gas—everything needed to keep today's world running as we are accustomed to. As manufacturing environments increasingly move into the connected network world, the failure to properly secure them and authenticate users and devices can result in attacks that can wreak havoc on our critical infrastructure.

PKI + Certificate Automation

With billions of IoT endpoints slated to be manufactured over the next five years, it is imperative that manufacturers design stronger security into connected devices to make them trustworthy. For many manufacturers, building security into devices is a daunting task, given the growing number of attack surfaces in today's increasingly complex and distributed manufacturing supply chain. Manufacturers also need the flexibility to seamlessly change contract partners in order to manage costs and shorten time to market without compromising the security, intellectual property, and safety of their products.

GET IN TOUCH

To learn more about your readiness to build secure IoT devices and manage PKI securely, contact Keyfactor today to learn about EJBCA and Control.

REQUEST A DEMO

To build trustworthy electronic, industrial control, and IoT devices, it is critical for manufacturers to adopt a zero trust manufacturing approach. Supply chains need to move beyond implementing zero trust networking to ensure that the identity of every device can be trusted. Without trusted identities and credentials, the network authentication, data, and firmware of systems simply cannot be trusted.

Keyfactor EJBCA along with Keyfactor Control provides a robust, cost-effective solution for managing PKI that is easy to implement. The solution ensures secure identities across the IoT device lifecycle, including design, manufacturing, commissioning, and end-of-life. OEMs, ODMs, and electronics contract manufacturers should follow the best practices outlined here to adopt a zero trust manufacturing approach.

KEYFACTOR

Keyfactor is the machine and IoT identity platform for modern enterprises. The company helps security teams manage cryptography as critical infrastructure by simplifying PKI, automating certificate lifecycle management, and enabling crypto-agility at scale.

For more information, visit www.keyfactor.com or follow us on LinkedIn, Twitter, and Facebook.

Built on a foundation of trust and security, Keyfactor is a proud equal opportunity employer, supporter and advocate of growing a trusted, secure, diverse and inclusive workplace.

Contact Us

- www.keyfactor.com
- +1.216.785.2990