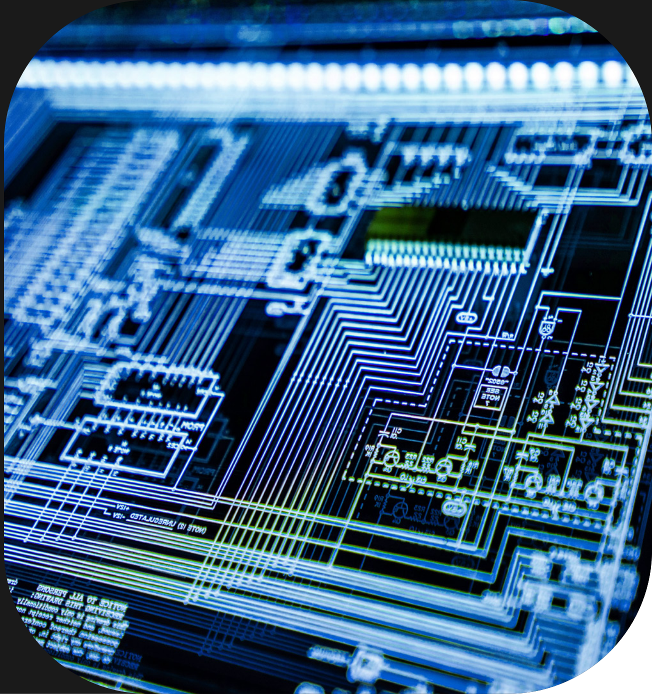
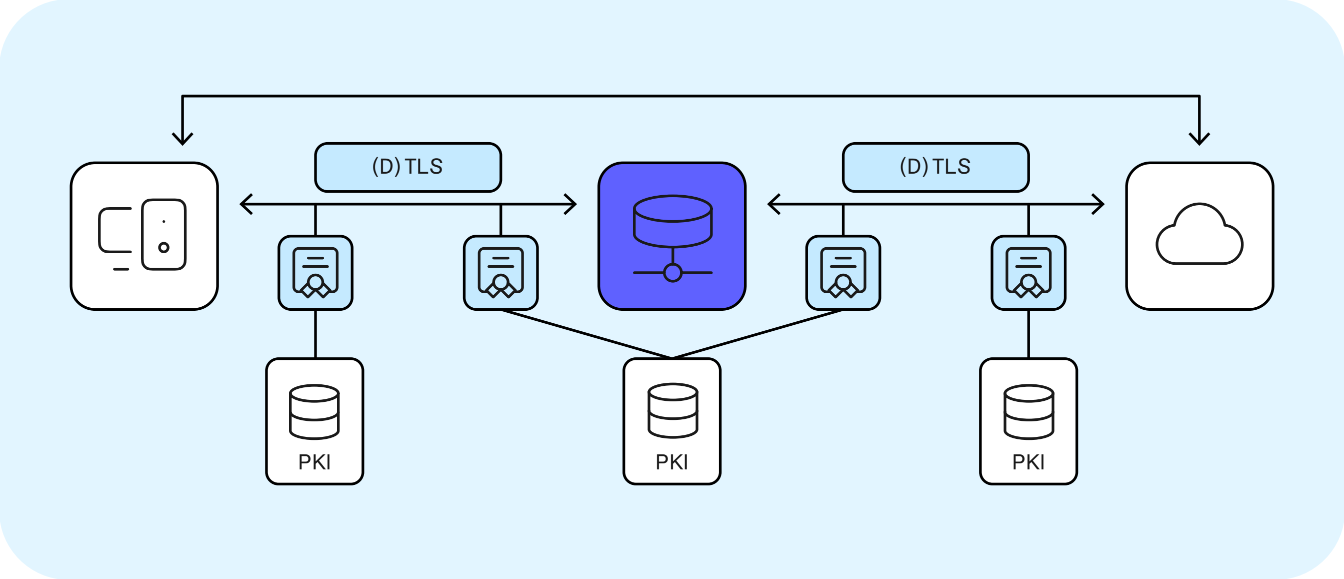
Injecting Initial Device Certificates in the factory: the foundation of security



The world is more connected than ever with smart devices sending information on everything from water bills, to thermostats controlling HVAC, to containers that optimize logistics.

Connected devices typically enable hardware products to provide “smart” network-reliant services to end users. These services are often dispatched by servers that connect to both the service customer as well as a number of connected devices installed and operating in the field. These connections all need to be secured by the same state-of-the-art technologies that secure everything else on the Internet: (D)TLS, PKI, and short-lived operational certificates.



A service provider operating their own PKI should draw a circle of trust around their assets—IoT devices, servers, smartphone apps, infrastructure, databases—so that each connection can be mutually authenticated and protected, end-to-end.

Just like in the IT world, where renewing user passwords and machine certificates is best practice, operational certificates within IoT appliances should be short-lived and renewed regularly to prevent compromise.

There are a variety of standard PKI (re-)enrollment protocols, such as EST, EST over CoAP, SCEP, and CMP, as well as certificate lifecycle management platforms, such as Keyfactor Command, which can be used to manage certificate renewal. However, these protocols and systems rely on there being a pre-existing certificate on the IoT device from a trusted PKI. This seed identity—an initial device certificate such as the IDevID in the IEEE802.1AR framework—needs to be injected by the OEM during device manufacturing.

tops plug&go

When it comes to initial identity provisioning, multiple challenges can arise.

- The factory may not be trusted to provision in a secure manner.
- The PKI may reside off-site and need to rely on cloud solutions.
- Device constrictions limiting the ability to:
  - Generate a random number with enough entropy for strong private keys.
  - Assemble a certificate signing request (CSR) to get a certificate.
  - Contact the PKI at all by itself.

To help solve these challenges, Trusted Object’s **tops plug&go** acts as a fully configurable secure hub and sequencer to bridge between the device or chip programmer and external systems including:

- The OEM PKI, like EJBCA
- Firmware delivery server
- Key Management System (KMS)
- OEM databases and production logging systems to push/pull production data and generate secure production reporting

Since **tops plug&go** understands the memory map of the target MCU it is helping to program, it can pre-assemble memory blocks before feeding the programmer. This drastically reduces programming time and cost.

The product is based on an industrial computer with an on-board FIPS 140-2 Level 2 and CC EAL4+ certified TPM (hardware security module) which secures all connections to peripheral systems—PKI, device FW repositories, production databases, industrial programmers— then generates device key material, and random numbers with strong entropy.

Protects all sensitive data (application firmware, secrets) during transit and manufacturing operations

Enables secure key and certificate material injection as well as in the component and secure provisioning of the application server

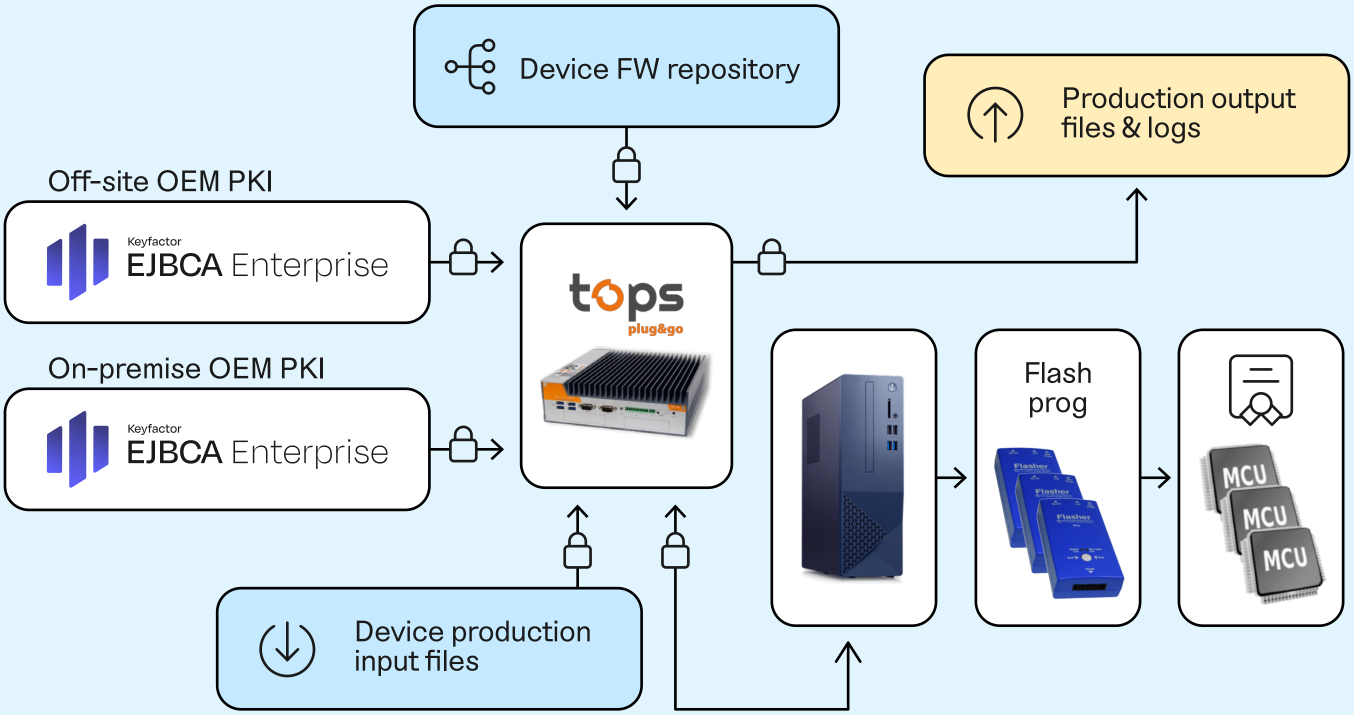
Generates unique device symmetric keys, device private keys, assembles CSRs, and securely connects to the OEM EJBCA PKI to collect device certificates

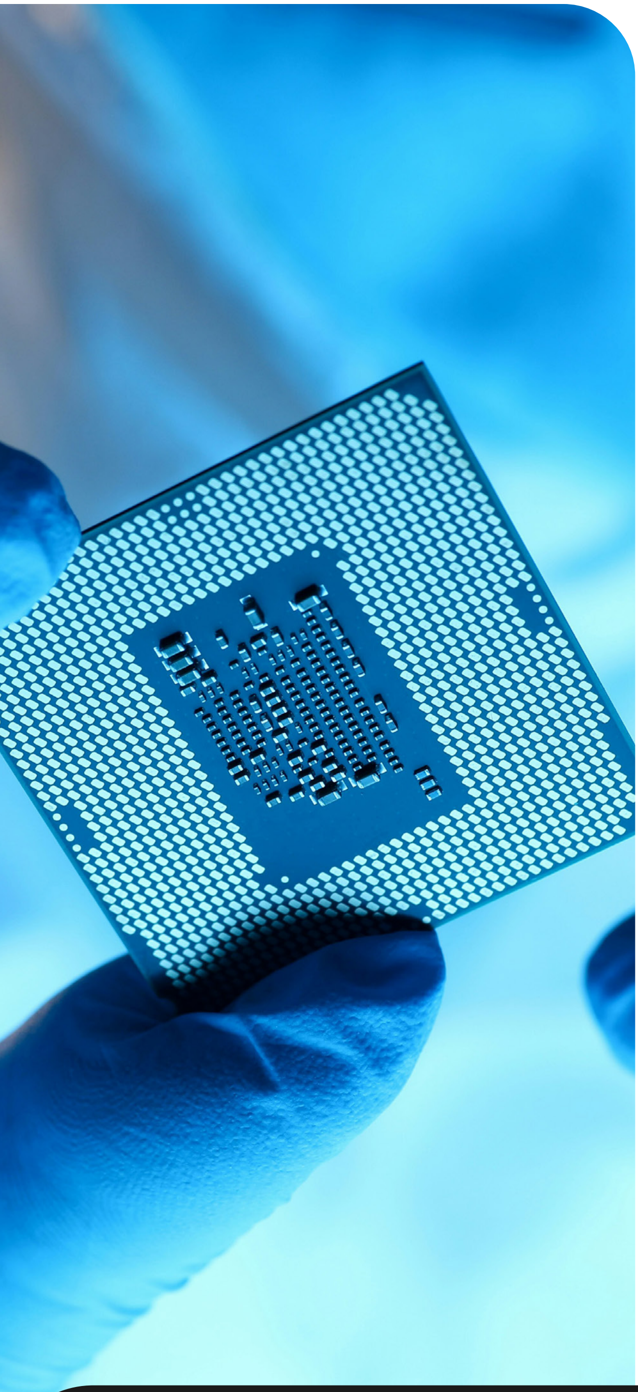
Production control with signed report, whitelist, and blacklist at the end of the production batch to counter overproduction

Compatible with most microcontrollers and most programming equipment

Collects all data to be programmed, unique per device or common, from all other systems

tops plug&go integrates seamlessly with popular industrial programmers such as those from System General, with a local client to interface with any production test bench. It can also be configured as a server for multiple programming machines.





EJBCA for IoT

EJBCA for IoT simplifies PKI operations for OEMs, service providers, and IoT users, providing an easy way to issue, manage and maintain digital certificates, even at massive scale. Built on open-source standards and an open-source platform, EJBCA is the most widely used and trusted CA software on the planet.

The platform comes pre-packaged with all the components required to run a robust PKI, deploys wherever and however you need it, and scales on demand, making it easy for teams to:

- **Simplify and consolidate PKI:** run multiple PKI hierarchies on a single instance, centrally configure and govern certificate policies, and view detailed (and optionally signed) audit and transaction logs all in one place, with templates for easy configuration.
- **Deploy fast – run anywhere:** choose or combine any PKI deployment model, from a turnkey software appliance or hardware appliance with a built-in HSM, to a self-managed or SaaS-delivered PKI deployed directly from the AWS or Azure marketplace.
- **Meet the standard:** use customizable certificate formats and templates to meet the requirements for most international and consortium standards including Matter, multiple RFC standards, C-ITS, and many more.

About Keyfactor

Keyfactor brings digital trust to the hyper-connected world with identity-first security for every machine and human. By simplifying PKI, automating certificate lifecycle management, and securing every device, workload, and thing, Keyfactor helps organizations move fast to establish digital trust at scale — and then maintain it. In a zero-trust world, every machine needs an identity and every identity must be managed. For more, visit keyfactor.com or follow @keyfactor.

About Trusted Objects

Trusted Objects is a leading player in cybersecurity technologies for embedded systems. Trusted Objects products and services for constrained devices are positioned to create trust all along the value chain including edge devices, networks, clouds and manufacturing.