Keyfactor

Bring Your Own Root of Trust (BYORoT) by Keyfactor

The hardware Root-of-Trust

A crucial decision an OEM must consider when designing a connected device is where all the device's most important secrets will be stored and processed: the Root of Trust (RoT). Important secrets include artifacts such as:

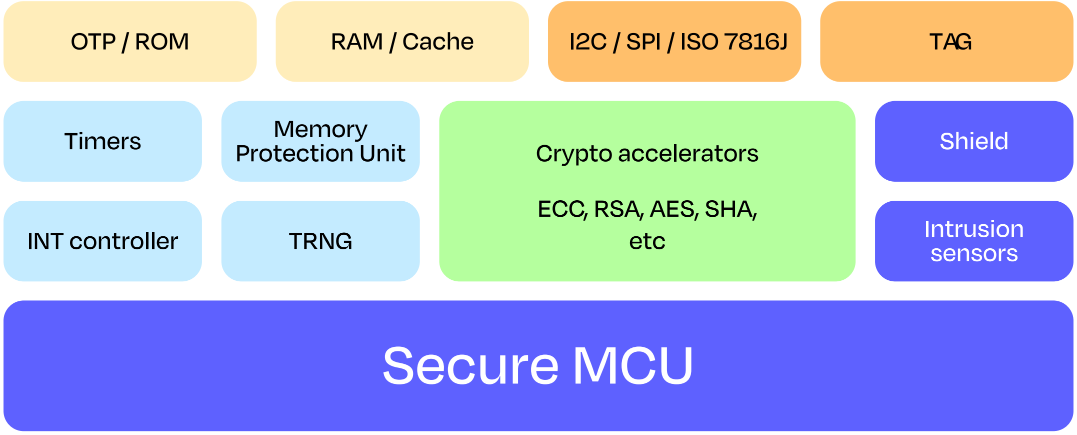
- Unique, device-specific private keys and Initial Device Certificate pairs attesting the genuineness of the device
- OEM software/firmware signature verification keys and/or certificates
- Symmetric session keys derived from TLS or equivalent security protocols
- Certificates that the device should trust when interacting with other machines
- Other unique private key and Operational Certificate pairs that the device will use during regular operations to secure end-to-end connections with other devices or servers

In addition to securely hosting secrets, the OEM might consider protecting the execution of cryptographic primitive functions or algorithms on the RoT. These can inadvertently leak secrets from improper software implementation, mismanagement of memory, instantaneous power consumption glitches, or electromagnetic emissions.

Given the importance of all data stored and executed on it, the RoT must be kept out of reach of unauthorized users and potential malware.

Silicon vendors offer many options to provide the required security:

- Secure elements, which may come with strong certifications such as Common Criteria
- Secure microcontroller units (MCUs) used in sensitive applications such as point-of-sale terminals used for payments or other financial transactions
- Ordinary MCUs with a Trusted Execution Environment that provides isolation between stacks, processes, and memory
- Secure software stacks running on ordinary MCUs, which can obfuscate secrets and prevent leaks



Example drawing of the architecture of a secure element

Bring Your Own Root-of-Trust (BYORoT)

BYORoT by Keyfactor is designed to allow any OEM or Service Provider to use Keyfactor EJBCA's PKI to issue Initial Device Certificates and Operational Certificates then store them into the RoT of their choice. The RoT can be a secure element or an MCU from a wide selection of silicon vendors, either hardware or software.

Keyfactor EJBCA supports:

- Microchip ECC608A, ECC608B, and TA100
- NXP EdgeLock® SE050
- STSAFE A100
- Silicon Labs Secure Vault MCUs
- Infineon Optiga Trust M
- Renesas RX MCUs
- Trusted Objects TO-Protect
- Many more...

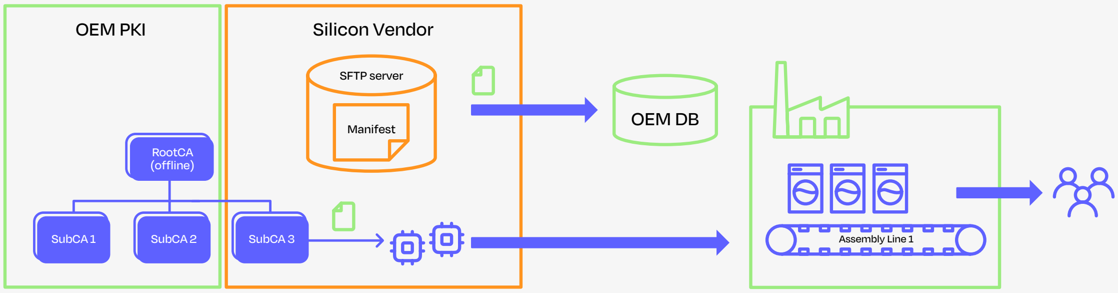
Initial Device Certificate Injection Options

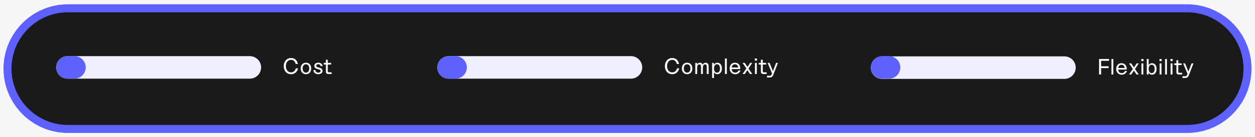
There are multiple avenues available when generating the first private key and injecting the Initial Device Certificate. Keyfactor offers many different options to perform this task in the factory during manufacturing, possibly including a Local Registration Authority (LRA), or over-the-air later in the deployment process. Alternatively, some customers prefer to leverage personalization services offered by some silicon vendors to receive the chips pre-provisioned with a unique private key and an Initial Device Certificate.

With pre-provisioned chips, a dedicated issuing Certificate Authority (CA) must be located at the silicon vendor chip factory, which creates a challenge in establishing a connection with the OEM PKI. If this is the desired option, Keyfactor EJBCA BYORoT also offers one-off processes allowing the OEM to set up their own PKI then sign Issuing CAs hosted by the silicon vendor before production starts.

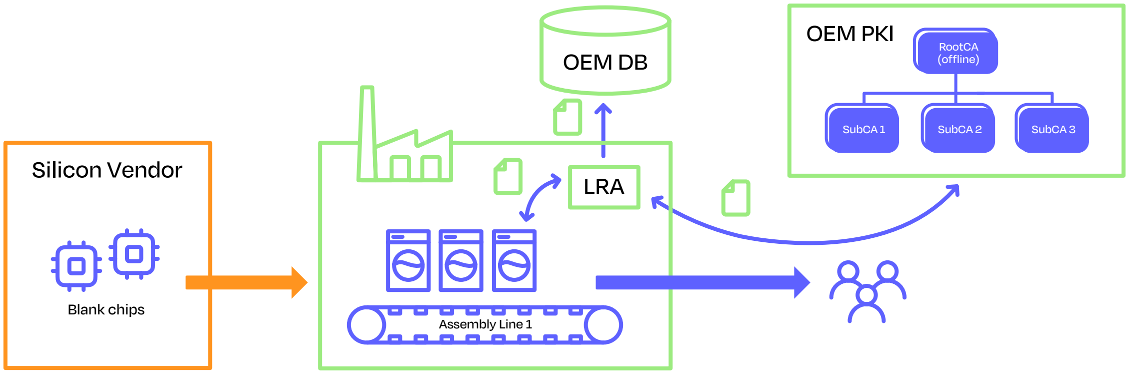
IoT identity provisioning happens at the silicon vendor factory

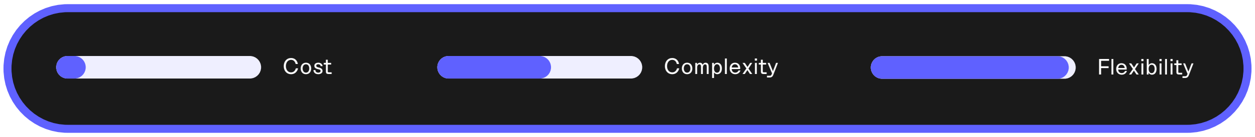
Before device manufacturing in the OEM factory





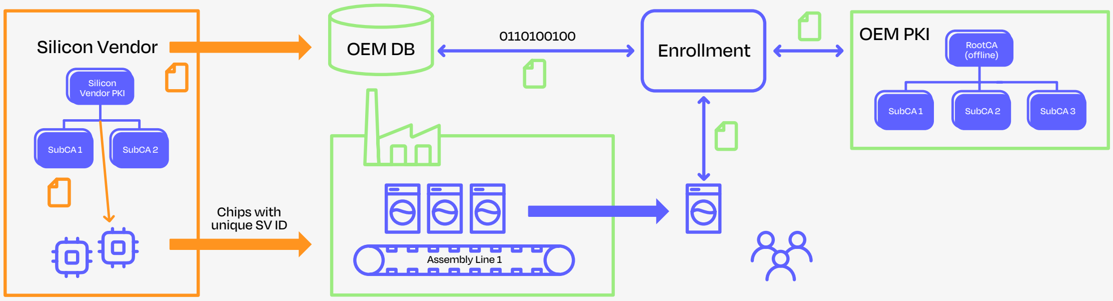
IoT identity provisioning happens at the OEM factory

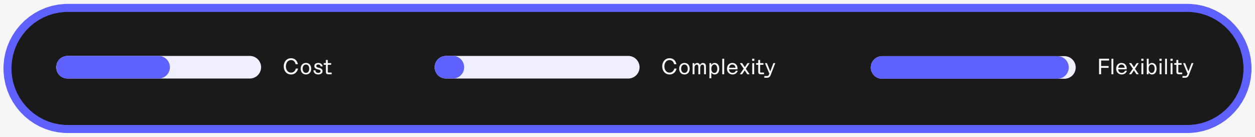




IoT identity provisioning happens Over-the-Air

After device manufacturing, before shipping to customer or in the field





Conclusion

With the IoT boom, more and more devices are being designed and launched every day. Given the size of the market, security must be at the forefront of every OEM's mind, but it must fit as seamlessly into their current processes as possible.

BYORoT supported by Keyfactor EJBCA allows manufacturers to provide unique identities to all of their devices, on a RoT of their choosing, with a PKI architecture that fits their business.

Get started

With support for a wide variety of protocols including ACME, EST, and CMPv2, EJBCA Enterprise is a highly scalable and extensible PKI platform for certificate-based identity issuance. 5G network providers and users can issue device identity and SSH certificates at a massive scale, whether during manufacturing, as an update in the field, or short lifespan-session certificates as a replacement for tokens. EJBCA PKI has a flexible architecture and can be deployed within a data center, in the cloud, or as a managed service.

Keyfactor EJBCA

For a complete list of supported technologies visit: https://www.keyfactor.com/products/ejbca-enterprise/

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.

Contact us

- www.keyfactor.com
- +1 216 785 2946
  (North America)
- +46 8 735 61 01
  (Europe)