Device Certificates

Secure connectivity has never been more important.

Cryptera's Device Certificate solution enables seamless, secure cloud connectivity for your devices.

OVERVIEW

Data fuels the digital economy, and connected devices deliver lots of it. To deliver data you can trust, and to avoid leaking sensitive data when sending it from a connected device to the cloud, you need encryption, integrity and authentication.

All of this can be achieved by using digital certificates. Introducing the use of certificates in connected devices can be hard and requires expertise across multiple domains if you want to gain the full benefits of scaling your device fleet.

Cryptera gets you all the way from manufacturing to the cloud when integrating device certificates for cloud communication.
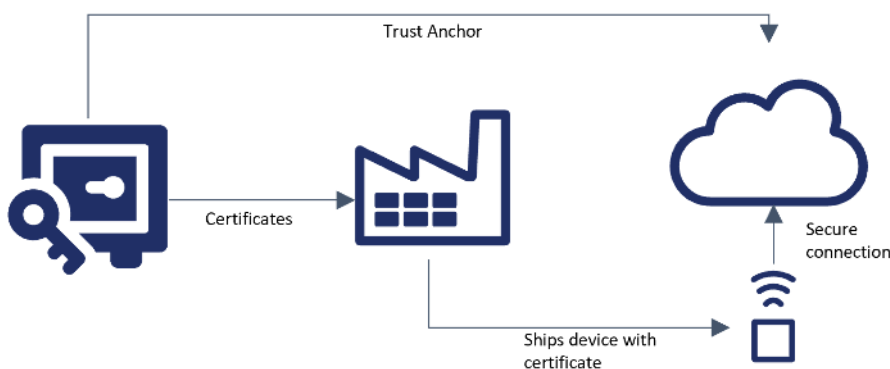
Cryptera's Device Certificate solution provides device certificates as a service and secure key storage using Cryptera's KeyServer.

This integrates easily with device onboarding solutions for cloud IoT services such as Azure IoT hub and AWS IoT with the use of Azure DPS or Just-in-time provisioning using AWS.

Additionally, we help you integrate this into a manufacturing setup, enabling you to add certificates to your devices in a secure and scalable way.
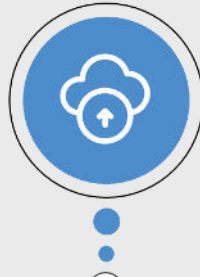
KeyServer
(Key Management)

Robust centralized key management and backup for managing cryptographic keys.
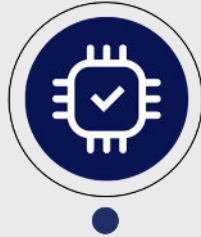
Firmware Signing
(Code Signing)

Automates the critical tasks of code signing and key management. Facilitates compliance with leading standards such as IEC 62443 and EU CRA and NIS2. It integrates with your existing tools and processes.

Device Certificates

Avoid the risk of unauthorized access. Cryptera Device Certificates gets you all the way from manufacturing to the cloud by adding certificates to your devices in a secure and scalable way.
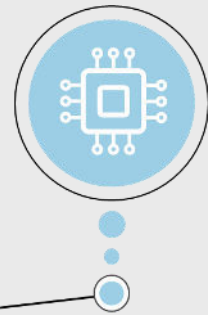
Feature Licensing

Leverage differentiated functionality levels and monetize additional features in your system.
Cryptera's secure feature licensing solution safeguards your functionalities and activates only the features that customers have purchased.

SUPERIOR KEY STORAGE

The KeyServer Device Certificate solution provides you with a private certificate authority (CA) and protected API access for issuing digital (x.509) certificates, leveraging secure key storage while providing ease of access for you.

Prevents key abuse

→   API access is protected with authentication and access control

Protects against key leakage

→   Keys are stored in FIPS 140-2 Level 2 approved HSMs in a secure and audited key storage facility in the nordics

Prevents loss of critical keys

→   Encrypted back-up is performed continuously

KeyServer also provides advanced access control concepts that anchor authentication within the hardware security module. This means that even Cryptera does not have access to your keys stored in the hardware security module.

About Cryptera

For more than 30 years, Cryptera has supported customers across virtually every sector and continent with over two million world class security solutions installed worldwide. We are experts in the fields of encryption, certification and secure provisioning. We offer a full span of solutions comprising of hardware, software and services to protect sensitive information using cryptographic methods and secure processes.

With in-house manufacturing, R&D and support functions, Cryptera has a vast experience to ensure that solutions meet various regulatory compliances and standards. Our team of engineers and experts can help you to create robust device security with the highest security measures, to safeguard your connected devices.

Scan the code with your smartphone and get more information about Cryptera

APRIL 2024 - Device Certificates

CRYPTERA®