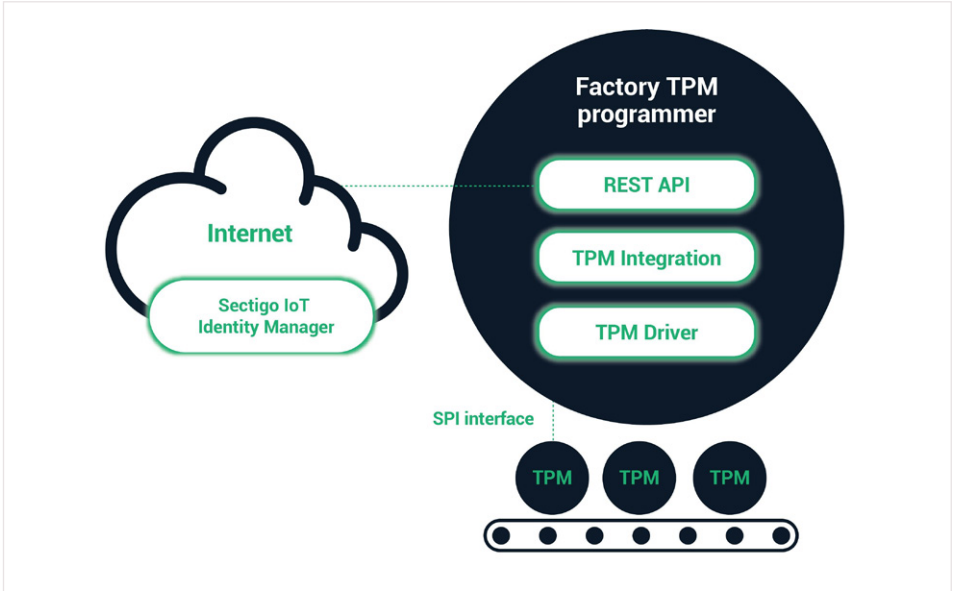
Security Partner
Preferred

Partner Use Case

PKI services, including automated certificate programming for OPTIGA™ TPM

Automated PKI solutions for certificate issuance and lifecycle management for IoT devices using the OPTIGA™ TPM secure key storage, including initial certificate creation using the TPM.



Products

OPTIGA™ TPM

Infineon Security Partner Preferred

SECTIGO

Use case

Application context and security requirement

Sectigo provides a complete certificate management solution starting with secure certificate creation & insertion in the factory using the OPTIGA™ TPM for private key storage. The Sectigo IoT Manager enables key management and certificate signing during manufacturing. The Sectigo Public Key Infrastructure (PKI) client provides device-side software enable creation of a Certificate Signing Request (CSR) and CSR signing while using the Trusted Platform Module (TPM) for secure key storage. The Sectigo IoT Manager allows management of PKI certificates after the device is deployed.

Challenge

OPTIGA™ TPM provides robust, secure hardware elements that create a foundation for building secure products. Implementing a PKI solution using the TPM, however, is a complex challenge for most Original Equipment Manufacturers (OEMs). Sectigo's IoT Manager and PKI Client enables OEMs to implement a PKI solution and automate certificate issuance to secure embedded connected devices with ease and at scale. Cloud issuance of certificates via a Web User Interface (UI) or programmatically via a Representational State Transfer Application Programming Interface (REST API) enables full PKI implementations, including root hosting, Hardware Security Module (HSM) provisioning, and the creation and ongoing management of private trust ecosystems.

Implementation

Creating a signed certificate during manufacturing requires several steps. First, the PKI client requests the OPTIGA™ TPM to generate a new public-private key pair. The PKI client uses the public key to create a CSR while the private key never leaves the TPM, ensuring maximum security. The Sectigo PKI client sends the CSR to the IoT Manager, which signs the request and returns a signed certificate to the PKI client. This certificate can then be used to authenticate the device when the device is provisioned in the field.

User benefits

- Certificate Authority (CA) services including cloud-based certificate issuance, CA hosting services and CA ecosystem setup
- Supports key generation by the OPTIGA™ TPM and enrollment with a Certificate Authority
- Provides Certificate Signing Requests using Enrollment over Secure Transport (EST), and REST APIs
- Full integration with Sectigo IoT Manager for Certificate issuance and renewal

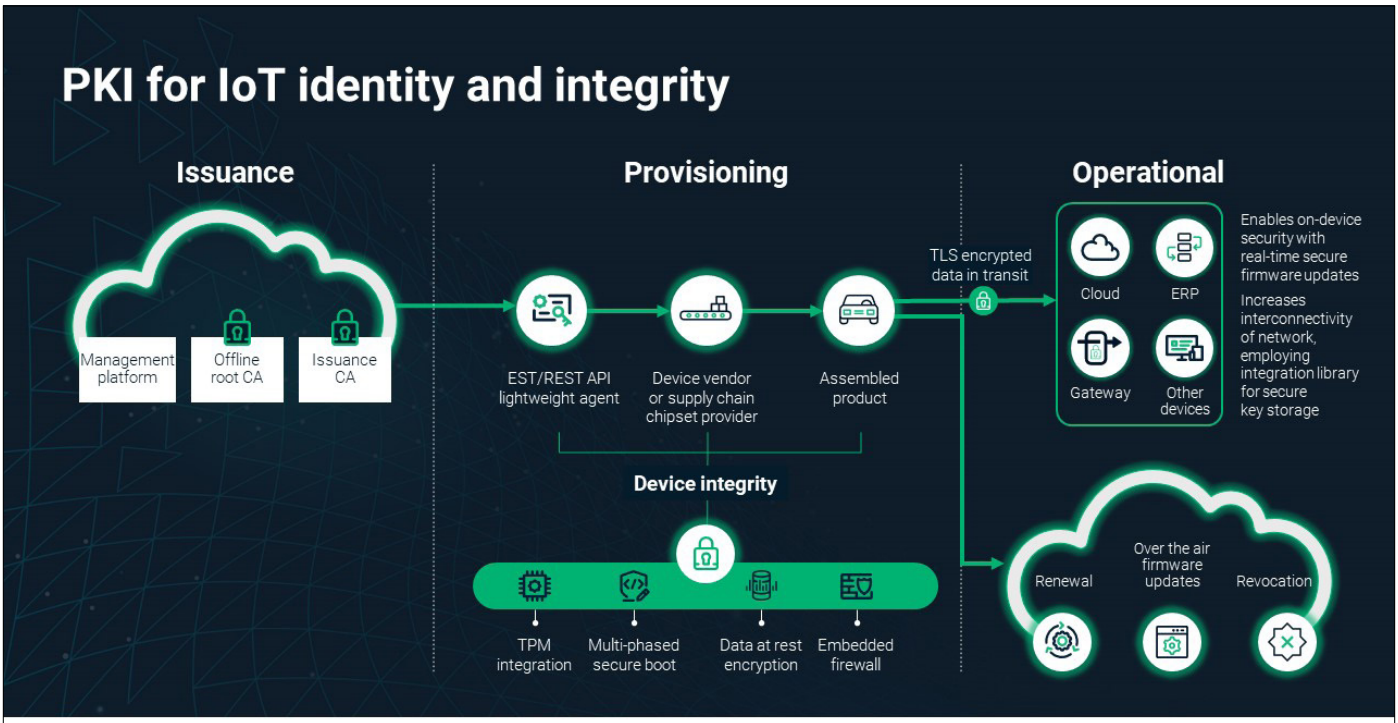
> "More connected devices mean more attack vectors and more possibilities for hackers to target us. IoT security, previously ignored, has now become an issue of high concern."
>
> Ben Dickson, Crunch Network

Solution

Sectigo's IoT identity platform and REST API client automates certificate provisioning for Infineon TPM based devices. The solution is modular in design and incorporates both device and server elements to allow a robust, secure PKI solution for end-to-end security implementation. OPTIGA™ TPM generates and securely stores the key, the REST client extracts the public key from the TPM and enables communication with the Sectigo IoT Identity Manager to create the certificate and store it on the TPM-based device. This solution enables certificate program either during manufacturing or when the device is provisioned to create a device identity to enable secure machine-to-machine communications, using the keys stored security in the TPM.

Main benefits of the Infineon product

The Infineon OPTIGA™ TPM is essential to the Strong Device Identity solution since the crypto co-processor can securely store the private key of the device and help in proving aforementioned identity akin to a device hardware fingerprint.



Security Partner Preferred

Partner

SECTIGO

Partners from the Infineon Security Partner Network help you secure your devices and applications: understand which threats can undermine your business, propose solutions that will protect your business, build and implement such security solutions and, when relevant manage their operation. They have been selected by Infineon on the basis of their system security competence and ability to design and deliver strong and trustworthy security solutions. Their activities are diverse and include security consulting, security solution provision, electronic design, systems integration and trust services management. For some, offers are off-the-shelf; while for others, offers are custom-built.

Sectigo

Sectigo provides award-winning purpose-built and automated PKI management solutions to secure websites, connected devices, applications, and digital identities. As the largest commercial Certificate Authority, trusted by enterprises globally for more than 20 years, Sectigo has the proven performance and experience to meet the growing needs of securing today's digital landscape. In 2019, Sectigo acquired the company Icon Labs, which is focused on addressing the security needs of connected devices. From the acquisition, Sectigo gained capabilities such as device embedded firewall, secure boot, and TPM integration. These capabilities allow customers to rapidly provision certificates and ensure the integrity of kernel-level and firmware level information.

Sectigo's contribution to the Infineon Security Partner Network

Businesses now rely more than ever on smart devices that link to one another and to the public internet for a wide variety of use cases and industries, ranging from automotive and aerospace, to manufacturing, industrial controls, and healthcare, just to name a few. While connecting devices can enable innovative revenue models, improve device functionality, and enhance visibility and control, they also introduce significant business, legal, and compliance risk. The Sectigo IoT Identity Platform is the first end-to-end platform offering embedded device identity and integrity technologies, as well as purpose-built certificate issuance and management. It removes the complexity associated with securing and authenticating connected devices, so customers can protect their infrastructure in a way that is scalable, cost-effective, and easy to manage. It allows them to ensure the integrity and identity of their devices and maintain that security via over-the-air updates. By removing security and authentication as barriers, customers can maximize the value of their IoT solutions and enjoy the peace of mind that comes from knowing their connected devices are protected in a shifting threat environment, not just today but for years to come.

Published by
Infineon Technologies AG
81726 Munich, Germany

Date: 03 / 2020

Additional information
For further information on technologies, our products, the application of our products, delivery terms and conditions and/or prices please contact your nearest Infineon Technologies office (www.infineon.com).

Please note!
This Document is for information purposes only and any information given herein shall in no event be regarded as a warranty, guarantee or description of any functionality, conditions and/or quality of our products or any suitability for a particular purpose. With regard to the technical specifications of our products, we kindly ask you to refer to the relevant product data sheets provided by us. Our customers and their technical departments are required to evaluate the suitability of our products for the intended application.

We reserve the right to change this document and/or the information given herein at any time.

Warnings
Due to technical requirements, our products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by us in a written document signed by authorized representatives of Infineon Technologies, our products may not be used in any life endangering applications, including but not limited to medical, nuclear, military, life critical or any other applications where a failure of the product or any consequences of the use thereof can result in personal injury.