Security Partner

Partner Use Case

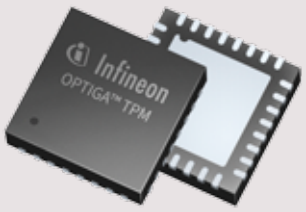
Automated certificate insertion for OPTIGA™ TPM

ICON LABS

Manage PKI certificates from the point of insertion at the factory with the OPTIGA™ TPM, and throughout the life of the product, using either a private or public certificate authority (CA).

Products

OPTIGA™ TPM



Security Partner

Use case

Application context and security requirement

Icon Labs provides a complete certificate management solution starting with secured certificate creation & insertion in the factory using the OPTIGA™ Trusted Platform Module (TPM) for private key storage. The Floodgate Factory CA (Certificate Authority) Server enables key management and certificate signing during manufacturing. The Floodgate TPM library provides the device-side software to streamline TPM usage and key storage, while the Floodgate CA Server allows management of Public Key Infrastructure (PKI) certificates after the device is deployed.

Challenge

OPTIGA™ TPM provides robust secure elements in hardware that create a foundation for building security products. Implementing a complete security solution using the TPM, however, is a complex challenge for original equipment manufacturers (OEMs). Floodgate TPM Library and the Floodgate PKI Client enable OEMs to develop and deploy secured embedded connected devices with relative ease.

Implementation

Creating a signed certificate during manufacturing requires several steps. First, the TPM library requests the OPTIGA™ TPM to generate a new public-private key pair. The TPM library uses the public key to create a certificate signing request (CSR); in this procedure the private key does not leave the TPM. The Floodgate PKI Client sends the CSR to the Factory CA Server, 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 first provisioned in the field.

User benefits

- Provides the APIs, libraries, and code running on the device to enable integration with the OPTIGA™ TPM
- Supports key generation by the OPTIGA™ TPM and enrollment with a Certificate Authority
- Provides Certificate Signing Requests using Simple Certificate Enrollment Protocol (SCEP), Enrollment over Secured Transport (EST), and Online Certificate Status Protocol (OCSP)
- Full integration with public and private Certificate Authorities

> “More connected devices means 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**

Security Partner

Solution

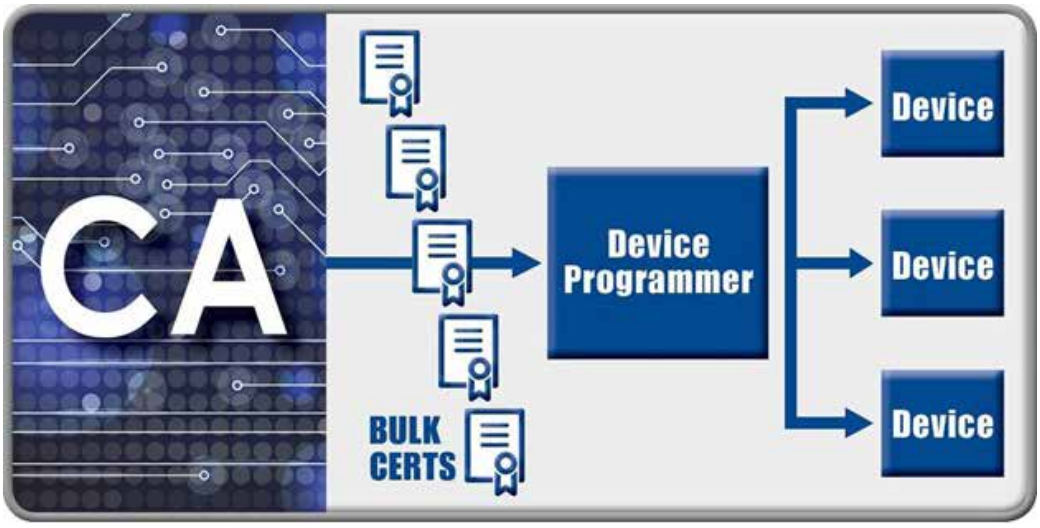
ICON LABS

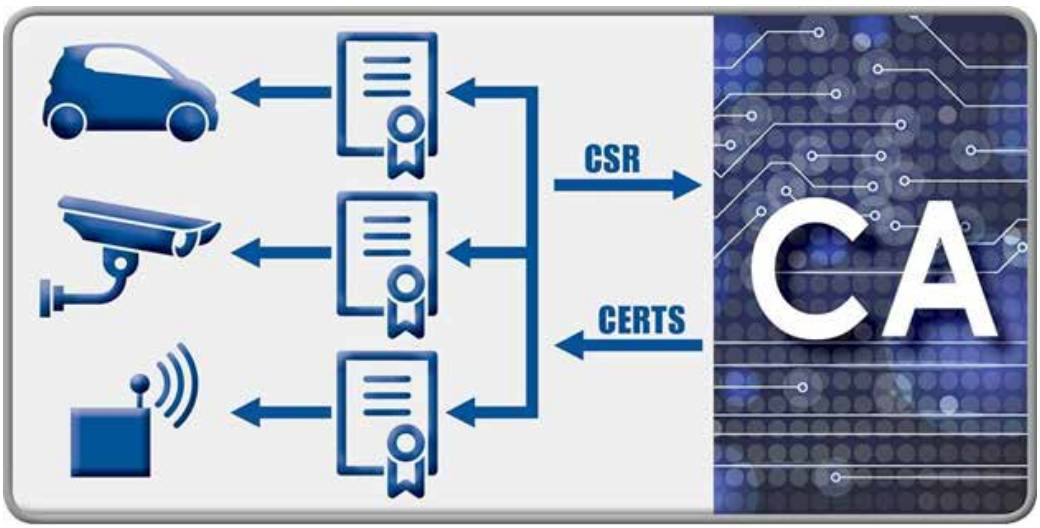
Floodgate TPM library is embeddable software providing a simple, robust API for the OPTIGA™ TPM. This solution provides integration with either a public or private CA for certificate creation during factory programming or when the device is provisioned. OPTIGA™ TPM 1.2 is currently supported, with TPM 2.0 support planned. Integration with a CA is implemented using SCEP or EST for certificate enrollment and CRLs or OCSP for certificate revocation.

The solution is modular in design and incorporates both device and server elements to allow a robust, secured PKI solution for end-to-end security implementation. The OPTIGA™ TPM securely stores the keys, the Floodgate Factory CA Server injects the keys, and the Floodgate PKI Client enables a connection in the field to either a public CA or a private CA. The Root of Trust implementation allows machine-to-machine communications, using secure keys for authentication and/or encryption, without human intervention.

Main benefits of the Infineon product

Icon Labs' solution solves two main security problems for the IoT. The solution makes it easy for OEMs to add security to their devices and, by automating the process, provides the scalability required as the number of IoT devices grows into the billions.





Security Partner

Partner

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.

Icon Labs

Icon Labs, a 2014 Gartner “Cool Vendor” and 2015 Gartner “Select Vendor”, is a leading provider of embedded software for device security, device protection, and networking management. They are known for their award-winning Floodgate Defender and Floodgate Security Framework products. The recently announced Floodgate Certificate Authority (CA) and Public Key Infrastructure (PKI) Client offer manufacturers easy and efficient integration of certificate-based machine-to-machine authentication. Founded in 1992, Icon Labs is headquartered in West Des Moines, Iowa, USA.

Icon Labs contribution to the Infineon Security Partner Network

The Floodgate CA and Floodgate PKI Client, when integrated with the OPTIGA™ TPM, allow manufacturers to incorporate certificate-based authentication. This includes a wide range of potential use cases including key management, generating public key infrastructure certificates, and injecting pre-generated keys during the manufacturing process. The PKI security solution provides both the client- and server-sides required to automate secure provisioning and enrollment. The Floodgate PKI Client is compatible with public or private CA’s, giving installed clients the flexibility to run in a private environment without dependence on the Internet or public CA.

Published by
Infineon Technologies AG
81726 Munich, Germany

Date: 04 / 2017

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.