Infineon Security Partner Network

Security Partner

Partner Use Case

Build Strong Device Identity with TPMs and PKI

Leveraging best in class hardware and software based security technologies combined with the benefits of cloud-based infrastructure to secure your IoT solutions from manufacturing through provisioning.

Products

OPTIGA™ TPM

Use case

Application context and security requirement

With the increase of internet-enabled instrumentation in industrial endpoints and machines, the need for securing and strongly identifying these devices is of utmost importance from a cybersecurity standpoint. This is challenging for traditional Operational Technology teams to accomplish.

Challenge

Device manufactures often have difficulty finding simple yet strong security solutions for establishing robust trust mechanisms. This is often because of either constrained or limited feature environments but also attributable to a lack of trust and control in the manufacturing environment. To compound the problem, information security is often a newer organizational competancy for Original Equipment Manufacturers (OEM) in the context of their products and these organizations are evolving their understanding of protection against cyberattacks.

Implementation

By combining hardware based TPM and software based Public Key Infrastructure (PKI), OEMs are able to fold in robust device integrity attestation and verification into a limited trust manufacturing environment, with devices leaving the factory with strong and trusted device identities. Using proven PKI technology and a hardware-based root of trust approach, GlobalSign's Identity and Security solutions can effectively establish a trusted ecosystem of devices that can communicate with each other reliably.

User benefits

- Users can verify that a device, which is claiming to be one of their products, has indeed been manufactured by them or their partners
- Users can prevent counterfeit products from connecting to their system - reducing the number of black or gray market devices
- Users can leverage the device identity determined by this solution to selectively control the feature set available to their customers based on the corresponding subscription/agreement level

Solution

The security solution is used to provision the manufactured device with a GlobalSign certificate. This step may be towards the end of the production cycle, preferably during the Quality Assessment or firmware initialization phase, or potentially can be done during initial onboarding of the device in the field.

The production line infrastructure should be able to connect to, and integrate with, the GlobalSign cloud or on-premise hosted service to enable the solution.

Infineon OPTIGA™ TPMs need to be physically installed and integrated into the manufacturing device design.

Architecturally, a sub-component of the system will act as the provisioning device. This will run software that will integrate with 2 components: upstream, the aforementioned GlobalSign Certificate provisioning service; downstream the TPM installed on the manufactured device.

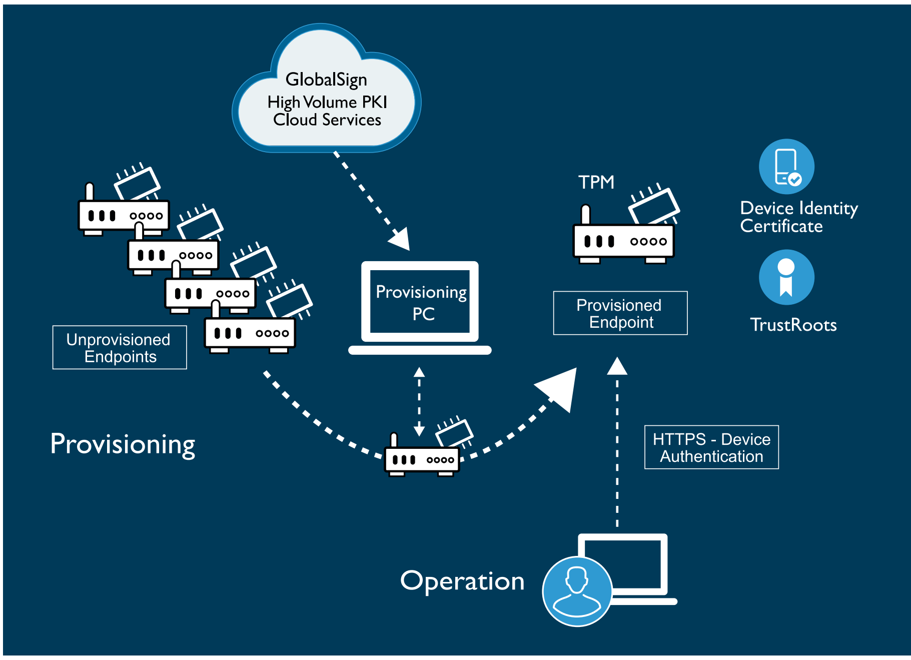
The solution will consist of a Representational State Transfer Application Programming Interface (REST API) that the provisioning software can make calls against and which will perform validation of trusted hardware components prior to identity credential issuance. The exact architecture of the provisioning device will be case-dependent and determined and developed by the OEM.

Physical security of on-premise appliances, if any, will need to be ensured by the OEM.

For further information on the solution please watch the youtube video under: http://youtu.be/j8scQ_atQBg

Main benefit 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.



What Does the POC Show?

Automated device provisioning

- Analogous to units coming through a manufacturing line or being enrolled in an environment
- Secure identity generation
- Illustration of support for massive identity velocity

Operation with cryptographic device identity

- Strong Authentication
- Encrypted Communications

Partner Use Case

Infineon Security Partner

Partner

GlobalSign GMO INTERNET GROUP

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.

GlobalSign

GlobalSign is the leading provider of trusted identity and security solutions enabling businesses, large enterprises, cloud service providers, and IoT innovators around the world to secure online communications, manage millions of verified identities and automate authentication and encryption. Its high-scale PKI and identity and access management (IAM) solutions support the billions of services, devices, people and things comprising of the Internet of Everything (IoE). The company has offices in the Americas, Europe and Asia with over 300 employees world-wide and 5.000 global partners.

GlobalSign's contribution to the Infineon Security Partner Network

GlobalSign will provide device identity and security solutions that leverage Infineon products such as the OPTIGA™ TPMs. These security solutions will be targeted towards various 'Internet of Things' verticals, including but not limited to – smart manufacturing, automotive and industrial automation.

The joint technology partnership will help IoT developers leverage PKI and secure hardware to implement strong authentication, encryption and privacy in communications in a scalable method.

GlobalSign brings experience and expertise in using PKI and Secure Sockets Layer (SSL) technologies and applying them towards solving cybersecurity problems in various small and large business contexts through our comprehensive product portfolio.

Published by
Infineon Technologies AG
81726 Munich, Germany

Date: 05/2016

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.