Infineon Security Partner Network

infineon

Security Partner

Preferred

Partner Use Case

EBV Personalization Services for Secure Devices – Update

EBV Elektronik

An Avnet Company

Securely generate and store personalized OEM certificates in the OPTIGA™ TPM to reduce the risk of counterfeiting and tampering without facing high expenses or risks.

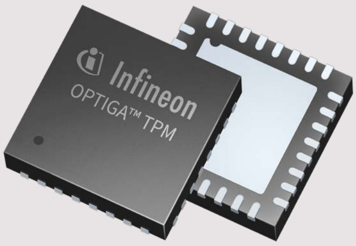
CUSTOM PROGRAMMED CRYPTO-HARDWARE ENABLES

- **Precise identification and authentication of devices**
- **High-levels of security**
- **Excellent anti-counterfeiting & brand protection**

The advantages of customized security elements are only accessible for companies capable of handling the related high costs of equipment, required security and programming expertise as well as high product volumes to make the implementation feasible.

Products

OPTIGA™ TPM



Security
Partner
Preferred

Use case

Application context and security requirement

Connectivity has spread to almost every market segment and is now part of diverse devices and applications. Consequently more and more original equipment manufacturers (OEMs) need to rethink their product security strategy. One fundamental part of security is hardware-based security. Personalized security solutions based on hardware-based security like the OPTIGA™ TPM provide excellent protection for a large variety of application scenarios but also require custom certificates and programming.

Challenge

In order to defend devices against counterfeiting, data theft and attacks, smaller and medium sized enterprises now face the challenge of implementing advanced security mechanisms. The ideal solution would be based on personalized hardware-based security. However the customization of hardware-based security solutions is bound to high investments in programming hardware/machines and extensive security expertise –smaller and medium sized enterprises often can't afford this. In addition these companies have only limited flexibility within their supply chain and depend on partners that are able to reliably deliver solutions in order to prevent down time and delivery issues.

Implementation

EBV, as a semiconductor specialist, has now developed a unique security hardware service that covers this gap and enables small and medium size companies to get access to OEM level hardware-based security solutions. The solution consists of a programming service for security chips paired with extensive design and security strategy support as well as additional hardware support and delivery services. The system works as follows: A customer defines the parameters for his own personalized OEM security certificate together with EBV. EBV programs the "blank" Infineon OPTIGA™ TPM solution using a Data I/O machine. The components are then shipped to the customer ready to be deployed in the final product.

User benefits:

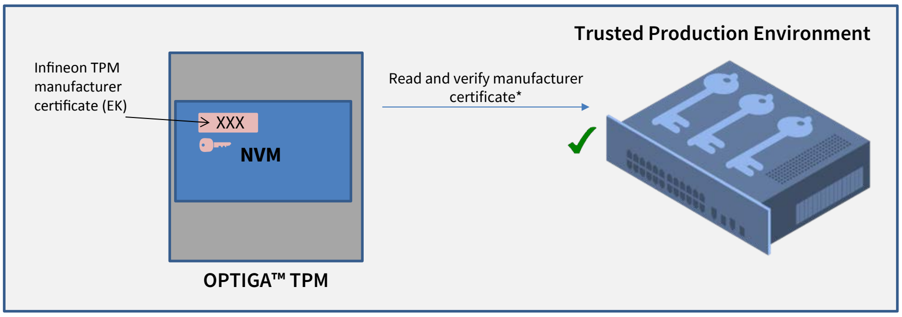
- › Costs for the programming of the security solutions and definition of the OEM certificate are significantly reduced
- › Small and medium size companies that could usually not afford personalized hardware-based security solutions can now easily design-in such solutions with EBV's support
- › End-consumer enjoys a high level of security at reasonable cost creating a strong level of trust and contributing to the reputation of the OEM
- › Supply chain is based on EBV's Avnet Logistic backbone and is therefore promising ultra-high reliability

Solution

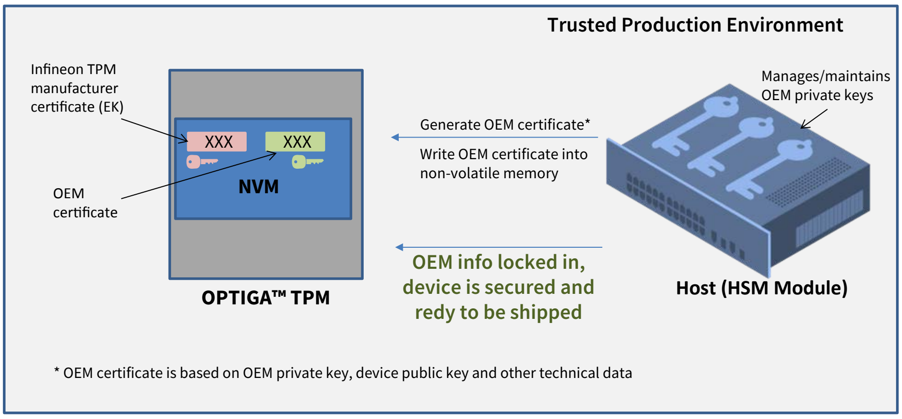
In order to protect products, identities and intellectual property against common threats like counterfeiting, strong and well-secured hardware-based security solutions are required. This can be easily achieved with the inclusion of hardware-based security solutions like Infineon's OPTIGA TPM. The design-in of such hardware-based security solutions can be achieved with comparably lower effort. In order to further minimize this effort the security strategy should be considered early in the design process.

The production and programming of a personalized, genuine hardware-based security solutions however requires extensive security expertise as well as highly-specialized production hardware. The process which is used to create the necessary security certificate and to program the security solutions is outlined in the graphic below.

Step 1: Verify that it is a genuine TPM


Trusted Production Environment
Infineon TPM manufacturer certificate (EK)
XXX
NVM
OPTIGA™ TPM
Read and verify manufacturer certificate*
✓

Step 2: Provision TPM with OEM's credentials


Trusted Production Environment
Infineon TPM manufacturer certificate (EK)
OEM certificate
XXX
XXX
NVM
OPTIGA™ TPM
Generate OEM certificate*
Write OEM certificate into non-volatile memory
OEM info locked in, device is secured and redy to be shipped
Manages/maintains OEM private keys
Host (HSM Module)

* OEM certificate is based on OEM private key, device public key and other technical data

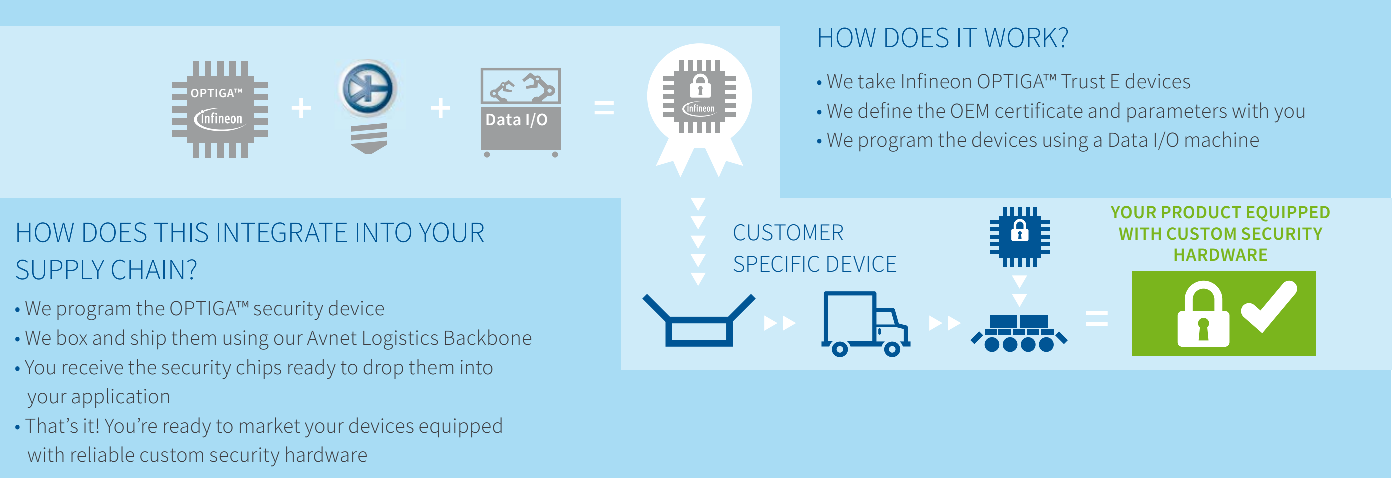
Core to this approach is a Hardware Security Module (HSM) attached to a computer or a programming machine (in production environments). A HSM is a physical computing module that can generate OEM certificates, securely manage/store keys and provide tamper-detect alerts.

EBV has installed such a setup consisting out of a HSM and a Data I/O programming machine in its Avnet Logistics warehouse in Poing, Germany. In these facilities EBV is defining the personalized security certificates together with customers and is executing the programming of the security devices. In addition, EBV takes over the storage of the private OEM keys in the secured Trusted Production Environment.

The whole supply chain process is outlined in the graphic below

Solution

The OPTIGA™ TPM is a turnkey security solution based on hardware security to reduce the risk of counterfeiting and tampering. Targeted at industrial automation, healthcare consumer electronics, smart home and PKI network applications, the reduced design-in and integration effort of the OPTIGA™ TPM offers OEMs an attainable peace of mind that their products are secured. EBV, with their personalization services, makes this even further achievable by enabling customers to integrate embedded custom security into their products independent of their security experience or volumes.



HOW DOES IT WORK?

- We take Infineon OPTIGA™ Trust E devices
- We define the OEM certificate and parameters with you
- We program the devices using a Data I/O machine

HOW DOES THIS INTEGRATE INTO YOUR SUPPLY CHAIN?

- We program the OPTIGA™ security device
- We box and ship them using our Avnet Logistics Backbone
- You receive the security chips ready to drop them into your application
- That's it! You're ready to market your devices equipped with reliable custom security hardware

Partner Use Case

Security Partner
Preferred

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.

EBV Elektronik
EBV Elektronik, an Avnet Company, was founded in 1969 and is one of the leading specialists in European semiconductor distribution.

EBV covers a broad range of market areas with its vertical technology and market segments that include Security & Identification, Analog & Power, High-End Processing, Smart Sensing & Connectivity, RF & Wireless, Industrial, Automotive, Healthcare & Wearables, High-Rel, LightSpeed, Smart Consumer & Buildings, and Smart Grid.

The company's successful strategy of personal commitment and excellent services enables its customers to develop and design some of the most innovative products available today.

The special focus on embedded security and services, like the personalization of security hardware and crypto components, help EBV to offer sophisticated solutions in order to prevent hacking, counterfeiting and other attacks.

240 Technical Sales Specialists and 105 continuously trained Application Specialists offer extensive application know-how and design expertise. EBV operates from 62 offices in 28 countries throughout Europe as well as in Israel and South Africa.

EBV Elektronik's contribution to the Infineon Security Partner Network
EBV Elektronik offers personalization services for embedded security devices and extensive security hardware design support in the context of ISPN. The company is the first semiconductor distributor able to program secure devices like the OPTIGA™ Trust E from Infineon for customers. The generation of OEM certificates and the secured programming of the security components can be fully managed and executed by EBV Elektronik, enabling customers with low production volumes or without security expertise to take advantage of the high protection levels of customized security hardware. In addition to these unique services, EBV Elektronik offers comprehensive hardware design support and security hardware consultancy including guidance during the selection process of the appropriate security hardware. The security know-how of the company spans across the complete IoT market enabling outstanding support for customers in areas like smart consumer devices, home automation, connected car and industrial automation.

Published by
Infineon Technologies AG
81726 Munich, Germany

Date: 01/2018

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.