Security Partner

escrypt
Embedded Security by ETAS

Partner Use Case

# Enabling secure industrial automation

Protecting industrial systems and PLCs against attackers from the inside and the outside.

## Product

OPTIGA™ TPM

Infineon Security Partner

escrypt Embedded Security by ETAS

# Use case

**Application context and security requirement**

As the application drives production lines, the integrity and authenticity of the software is critical and has to be ensured. Furthermore, every interruption or limitation of the throughput of the production line will cause a direct loss of money. As a result, the industrial control system in general and the Process Logic Controllers (PLC) in particular need to be protected against attacks.

**Challenge**

With the advent of the Stuxnet Worm, Industrial Control Systems are gaining increased interests from attackers. PLCs are the most important building blocks to realize complex industrial control systems. To provide the necessary security against attacks from outside and inside the plant, a secure hardware platform including cryptographic software is needed.

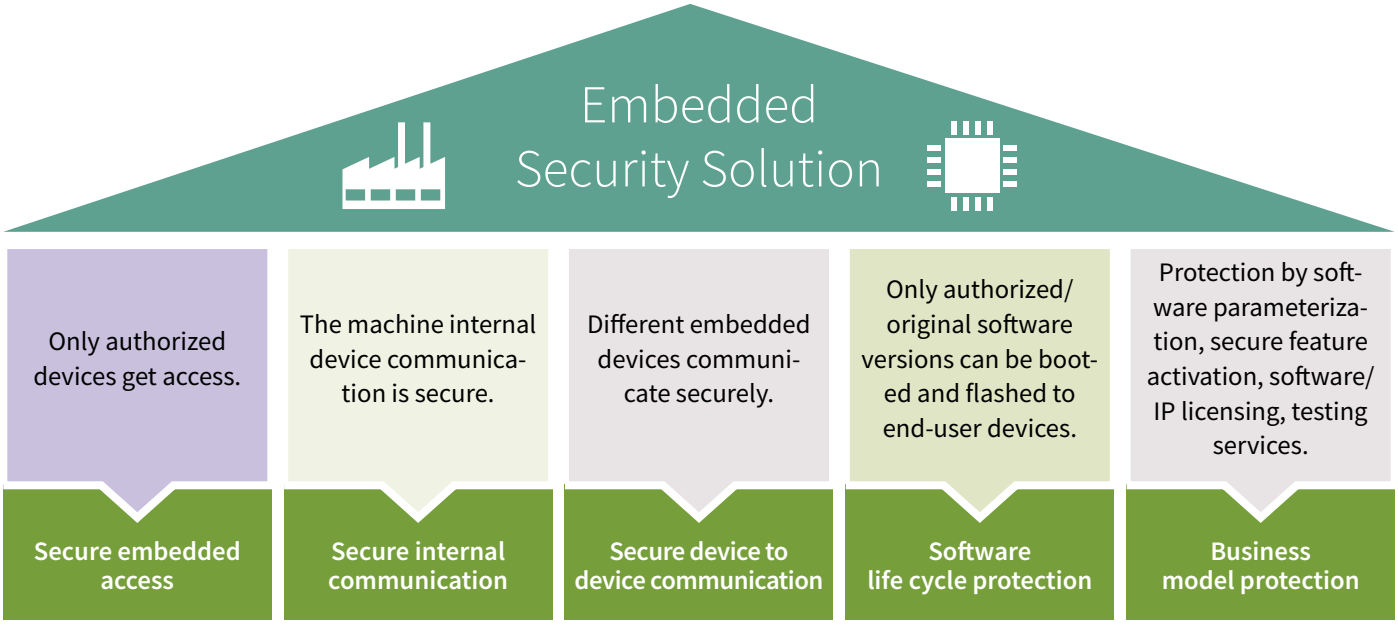
While Infineon provides respective security controllers e.g. OPTIGA™ TPM (Trusted Platform Modules ), ESCRYPT GmbH is specialized in embedded security system consulting and software, including central key management as backend component. In combination, complete embedded security solutions can be designed and implemented by the partners.

In the industrial field, a concrete use cases is securing the integrity of the PLC software, enabling secure update processes so that new software will only be flashed if it has been approved to be original.

**Concrete benefits of an integrated hardware / software security solution**

PLCs with enhanced hardware security modules, offer the following key benefits to its users:

- Providing integrity and authenticity of the software executed on the PLC
- Secured and strong identities for machine-to-machine communication
- Enhanced PLC administrator/user authentication
- Intellectual property protection of critical software on the PLC
- Complex rights management of software including updating and licensing of software on the PLCs



Security Partner

# Solution

The system will be used in a challenging environment: it has to fulfill strong requirements for the availability of the system, the integrity of its functionality, while also having a very long lifetime.

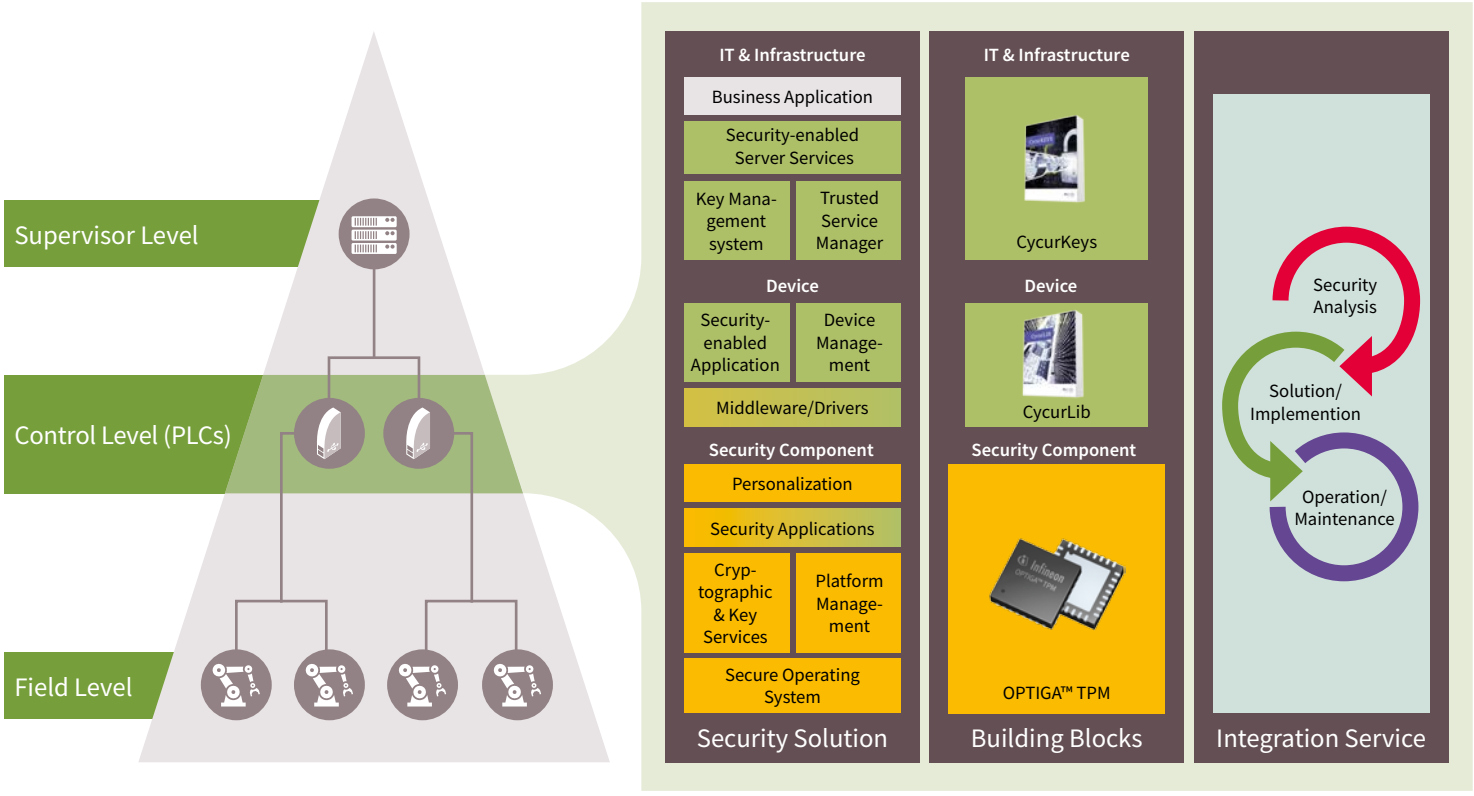
Thus, all security measures and the used cryptography have to be future-proof and there should be the possibility to update the system if the employed security measures are broken.

TPM technology, based on the Trusted Computing Group (TCG) international standard provides a full security ecosystem that includes application software to facilitate the hardware security module and ensure application programming interfaces (APIs) and processes are standardized and documented. Key management processes defined by the TCG allow for keys to be updated inside the OPTIGA™ TPM with dedicated API calls and standard processes; thus the industrial control system in general and the PLC system in particular can be protected over the lifetime.

Additionally, the used hardware components need to be designed for the desired lifetime of the product and they should be specified for a high temperature environment and also have to be tolerant to vibrations and dirt.

**Main benefits of the Infineon product**

› Infineon and ESCRYPT GmbH are security experts in various industries in need of embedded security.
› Infineon OPTIGA™ TPM meets the security requirements of a suitable hardware security module in the industrial applications.



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.

**ESCRYPT**

ESCRYPT - Embedded Security is a leading system provider for embedded security solutions world-wide. With international locations including Germany, Sweden, the USA, China, Korea, and Japan Escrypt has over one hundred security specialists available to help with current security topics such as secure M2M-communication, IT-security in the Internet of Things, protection of e-business models and automotive security.

**ESCRYPT's contribution to the Infineon Security Partner Network**

ESCRYPT defines and builds end-to-end security solutions relying on Infineon security products and provides a back-end technology and frame to manage the security along the secured application's lifecycle.

ESCRYPT provides a cryptographic Key Management Solution for embedded systems security based on Infineon's automotive microcontroller AURIX™, industrial controller XMC and secure elements OPTIGA™ Trust and OPTIGA™ TPM. In particular, ESCRYPT proposes a secure software updates solution that assures secure transmission of the code into the device, ensuring code integrity and authenticity. ESCRYPT offers key management solutions both as a commercial product named CycurKEYS (software license) and as a hosted and managed service. ESCRYPT's services include security strategy, security assessment, customized software, PKI & key management, certification support, application & code testing, training and awareness.

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.