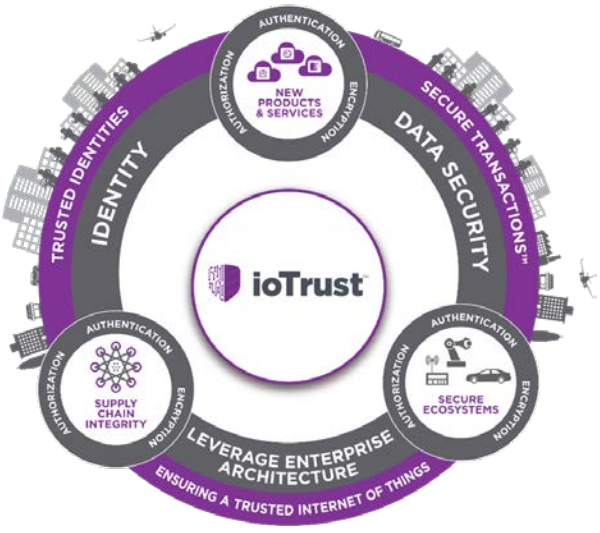
Security Partner
Preferred

Partner Use Case

ioTrust™ Security Solutions

Entrust Datacard™ ioTrust™ Security Solutions allow customers to establish secured IoT infrastructures from sensor to cloud, and throughout the device lifecycle - from manufacturing to operations.

Entrust Datacard™



Products

OPTIGA™ TPM

Security Partner Preferred

Use case

Application context and security requirement

Modern IoT ecosystems are complex combinations of powerful general-purpose compute nodes to constrained purpose built sensors. Integrating these systems into a solution that addresses a business need requires operators to authoritatively identify equipment that is intended for their operational use case. The secured establishment and usage of digital identities and cryptography throughout the lifecycle of a device or system therefore is the first essential building block of any secured IoT implementation. The ioTrust™ Security Solutions enable services and software allowing manufacturers and operators to establish a secured supply chain and device operations with security that starts on the manufacturing floor.

Challenge

The technology provided by the Infineon OPTIGA™ TPM (Trusted Platform Module) provides a secured and trusted building block for application and device security when present. However, implementing a solution that operationally leverages TPM features requires a robust infrastructure capable of complete Identity Lifecycle Management. The ioTrust™ software on TPM-equipped devices provides a secured wrapper, protecting interactions with the TPM and usage of its keys. Through administrator defined policy, ioTrust will securely enroll devices into a PKI anchored management system featuring secured data routing, data encryption and data acquisition features.

Implementation

ioTrust provides a secured End Point Agent which interfaces with the Infineon OPTIGA™ TPM to secure software elements such as key stores and application binaries. This Agent enables customers to access secured identities so that all device/sensor/application interactions are cryptographically authenticated and authorized. Working in conjunction with the ioTrust Service & Edge Gateway's End Point Agents enables that devices are monitored and receive key and certificate management based on policy defined by the ioTrust Identity Authority.

Benefits for the user:

- Allows customers application portability across TPM equipped and non TPM environments
- Enables secured device enrollment into managed identity ecosystem anchored by PKI
- Cryptographic agility and flexibility (ECC & RSA) is made possible through the provisioning of secured software key stores backed by TPM Hardware security
- Enables secured data flow management including data routing, payload and transport security

Solution

Entrust Datacard™ ioTrust™ Security Solution is based on enterprise-grade encryption technologies and offers an end-to-end solution that establishes a connected ecosystem which is secured by design from device manufacturing through the entire IoT lifecycle. It accelerates IoT deployments and time-to-value by enabling a secured and trusted network of people, applications and things for the industrial and manufacturing sectors.

The software platform is technology agnostic allowing for easy integration into both brownfield and greenfield IT/OT infrastructures. ioTrust is a tiered solution which provides flexibility to scale IoT deployments while offering end-to-end supply chain integrity.

The security solution provides embeddable libraries and services for IoT sensors/devices and gateways in addition to server-side device policy management and health reporting the infrastructure provided carries out critical certificate and key management tasks. Both server side and embedded device components of ioTrust enable to support key storage and generation features of the OPTIGA™ TPM using TPM 1.2 or 2.0 protocols.

The joint solution from Infineon and Entrust Datacard, using ioTrust Security Solutions, secures cryptographic material in Endpoints and Security Appliance with TPM protocols.

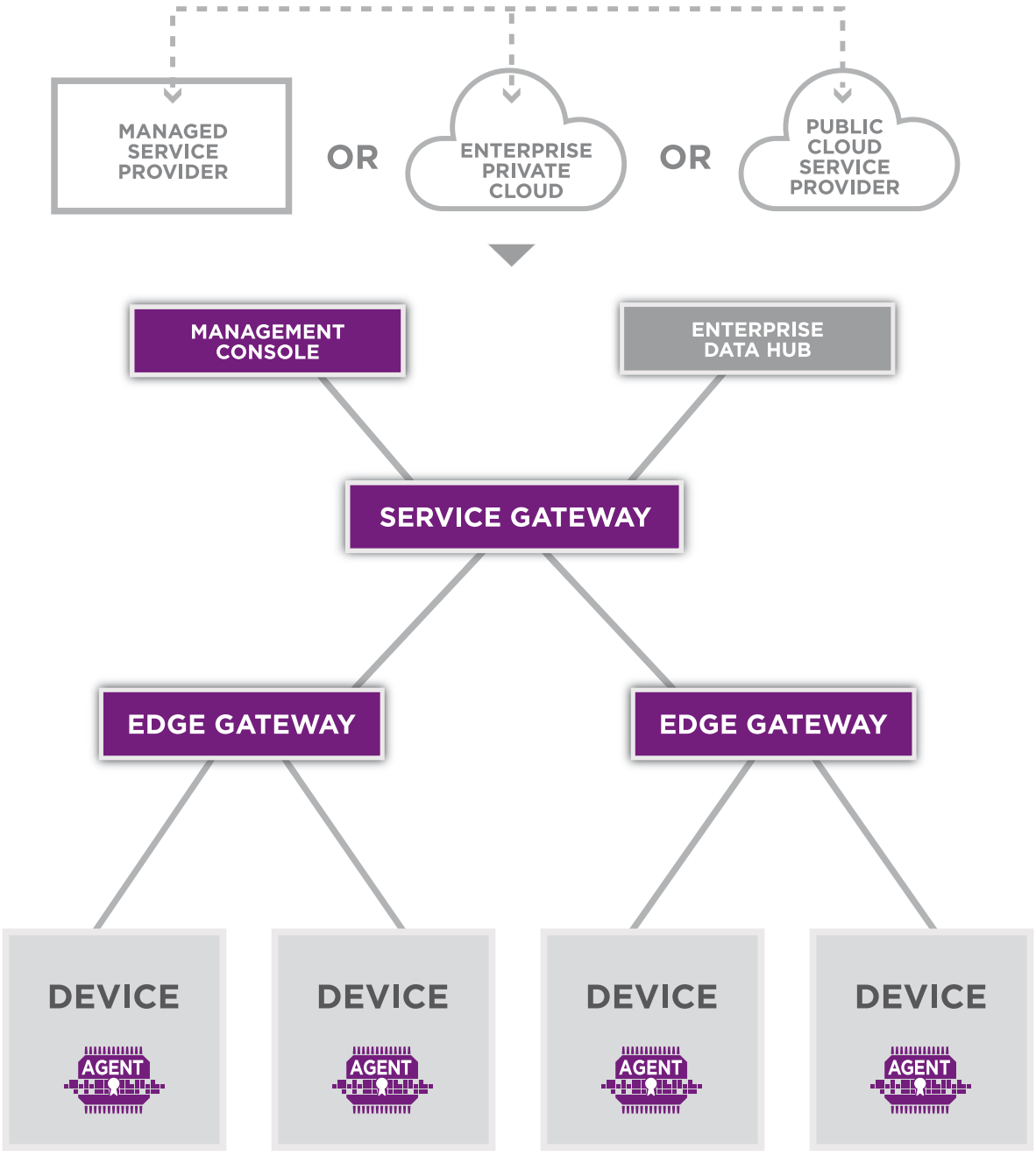
The Infineon OPTIGA™ TPM provides:

› robust and secured identity seed for ioTrust Endpoint agent
› crypto acceleration when enabled by solution
› secured key storage for ioTrust components

Infineon Security Partner Preferred

Entrust Datacard™

Solution



Security Partner Preferred

Partner

Entrust Datacard™

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.

Entrust Datacard

Consumers, citizens and employees increasingly expect anywhere-anytime experiences — whether they are making purchases, crossing borders, accessing e-gov services or logging onto corporate networks. Entrust Datacard offers the trusted identity and secure transaction technologies that make those experiences reliable and secure. Solutions range from the physical world of financial cards, passports and ID cards to the digital realm of authentication, certificates and secure communications. With more than 2,000 Entrust Datacard colleagues around the world, and a network of strong global partners, the company serves customers in 150 countries worldwide. For more information, visit www.entrustdatacard.com.

Entrust's contribution to the Infineon Security Partner Network

The technology provided by the Infineon OPTIGA™ TPM (Trusted Platform Module) provides a secured and trusted building block for application and device security when present. However, implementing a solution that operationally leverages TPM features requires a robust infrastructure capable of complete Identity Lifecycle Management. The ioTrust™ software on TPM-equipped devices provides a secured wrapper, protecting interactions with the TPM and usage of its keys.

Published by
Infineon Technologies AG
81726 Munich, Germany

Date: 11 / 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.