Security Partner

MOCANA

Partner Use Case

Easy Incorporation of OPTIGA™ TPMs to Support Mission-Critical Applications

Providing Infineon customers with an easy path to integrating TPM support into their products and systems via a common Application Programming Interface (API) architecture, independent of the operating environment.

Products

OPTIGA™ TPM

Security Partner

Use case

Application context and security requirement

Many Original Equipment Manufacturers (OEMs) and vendors, especially those who provide solutions for mission-critical applications, are required to meet stringent infrastructure security standards such as IEC 62443. Implementing these standards requires the use of dedicated security co-processors to check the integrity of keys and cryptographic operations. Integrating these chips into products can be challenging, even for developers with security expertise.

The Trusted Computing Group's (TCG) Trusted Platform Module (TPM) standard specifies the means for implementing trusted devices that can be cryptographically verified with respect to their identity, operational state and trustworthiness for secured data exchange over a network. These capabilities are viewed as being essential for network-connected devices that are used in manufacturing, utilities, healthcare, transportation, defense and other mission-critical applications.

Challenge

Successfully integrating TPM chips into device designs requires meticulous software design and implementation. The challenge is compounded by the continuing evolution and enhancement of the TPM standard. OEM's need to provide support for both the latest and the prior versions of the TPM specification (2.0 & 1.2) in order to maintain compatibility while taking full advantage of improvements in the standard. This can be completed through the inclusion of keys for Elliptic Curve Cryptography (ECC) in addition to the RSA-Keys. Additionally, mission-critical systems incorporate a wide range of devices; from simple sensors to controllers, gateways and general purpose computing platforms. Developing and supporting the interface to the TPM across multiple product lines with different processors and operating systems poses additional development challenges and costs.

Implementation

The TPM enables OEMs to include a highly secured, hardware-based "trust anchor" within their devices. This root of trust then becomes the basis for establishing the authenticity and integrity of a device, its operating software, its operational state and the information that it transmits. For example, when a device is powered on or reset, the TPM can be used to execute and cryptographically sign a series of measurements that fingerprint the device's BIOS and firmware. Using cryptographic keys that are generated within the TPM, not leaving the chip, provides a high level of assurance. When the device connects to the network, it can be interrogated and allowed to communicate only if the measurements are as expected. If validation fails, which could indicate that the device has been tampered with, it can be prevented from communicating with other devices or upstream services and the appropriate monitoring systems can be notified.

The Mocana NanoTAP module, which is part of the Mocana Security of Things Platform™ (SoTP), provides a high-level interface to the Infineon TPM that greatly simplifies the development effort required to utilize the TPM's capabilities in OEM products. The NanoTAP module provides a high-level abstraction of the TPM that is accessed via a common Application Programming Interface (API); this hides much of the underlying complexity and simplifies device code. The NanoTAP API is platform agnostic, making device software more portable across different products with different underlying CPU/OS combinations. The NanoTAP module is also pre-integrated with the Mocana NanoCrypto module; a comprehensive cryptographic library available with FIPS 140-2 certification. Using an efficient, pre-tested, high-level interface to the TPM and associated cryptographic functions makes product designs simpler, more consistent, easier to maintain and ultimately more secure.

Security Partner

Use case

User benefits

When devices and systems incorporate TPM in their design they are able to meet substantially higher standards of trust than devices which rely solely on software-based security mechanisms. Benefits of integrating the TPM using Mocana's SoTP software include:

- Increased market potential: TPM-based devices can be deployed in mission-critical applications that require the highest levels of trust such as utilities, manufacturing, transportation, healthcare and defense.
- Faster time to market: Creating device software using pre-tested, pre-integrated modules dramatically cuts development time.
- Greater design flexibility: Coding to a high-level API (versus lower-level device drivers) results in software that is more portable and re-usable across different CPU/OS combinations.
- Reduced software testing and maintenance: With a common code base across device designs it's much easier to develop and deliver software updates that add new capabilites and respond to technical evolution, such as the introduction of TPM 2.0.

Security Partner

Solution

MOCANA

In order for a device to be deemed trustworthy it should meet a number of functional requirements and capabilities, including:

› Verification that its operating code is valid, supplied by the device manufacturer or trusted 3rd party and has not been substituted with an attacker's code;
› Verification that the device hardware has not been tampered with;
› Proof of its identity via standardized cryptographic algorithms;
› Use of encrypted communications via standard protocols and strong encryption algorithms for all interactions with management and control systems, applications and other devices.
› The Infineon OPTIGA™ TPM enables products to meet these requirements with a high degree of assurance by performing critical security functions in a dedicated chip, including:
› Non-volatile storage of unique device identity information;
› Execution and storage of measurements used to verify integrity of the device hardware and software;
› Generation and storage of secret keys;
› Encryption for secure local storage and secure communcations;
› Acceleration of cyptographic operations.

Integrating TPMs into device designs has an impact on many core elements of the device's operating software. The Mocana NanoTAP module abstracts the complexity of the underlying security hardware and delivers numerous benefits for device and application developers, including:

› A consistent API that simplifies critical operations required to generate and utilize keys securely;
› Re-use of code across designs regardless of the underlying OS and CPU;
› A significantly smaller code footprint than is possible with open source alternatives, which reduces coding errors and vulnerabilities and also reduces memory requirements and power usage.
› Pre-integration with Mocana's cryptographic libraries, which abstracts and delivers cryptographic operations seamlessly using the TPM and further simplifies development.

The NanoTAP module is a core element of the Mocana Security of Things Platform™ (SoTP), which provides a full suite of embedded security functions including certificate management, authentication, and secured communications, all of which can leverage the TPM. The Platform also supports policy-based logging and alerting. Thereby, potential issues detected by the TPM can be delivered securely to industry standard Security Information and Event Management (SIEM) and logging systems.

Security Partner

Solution

MOCANA

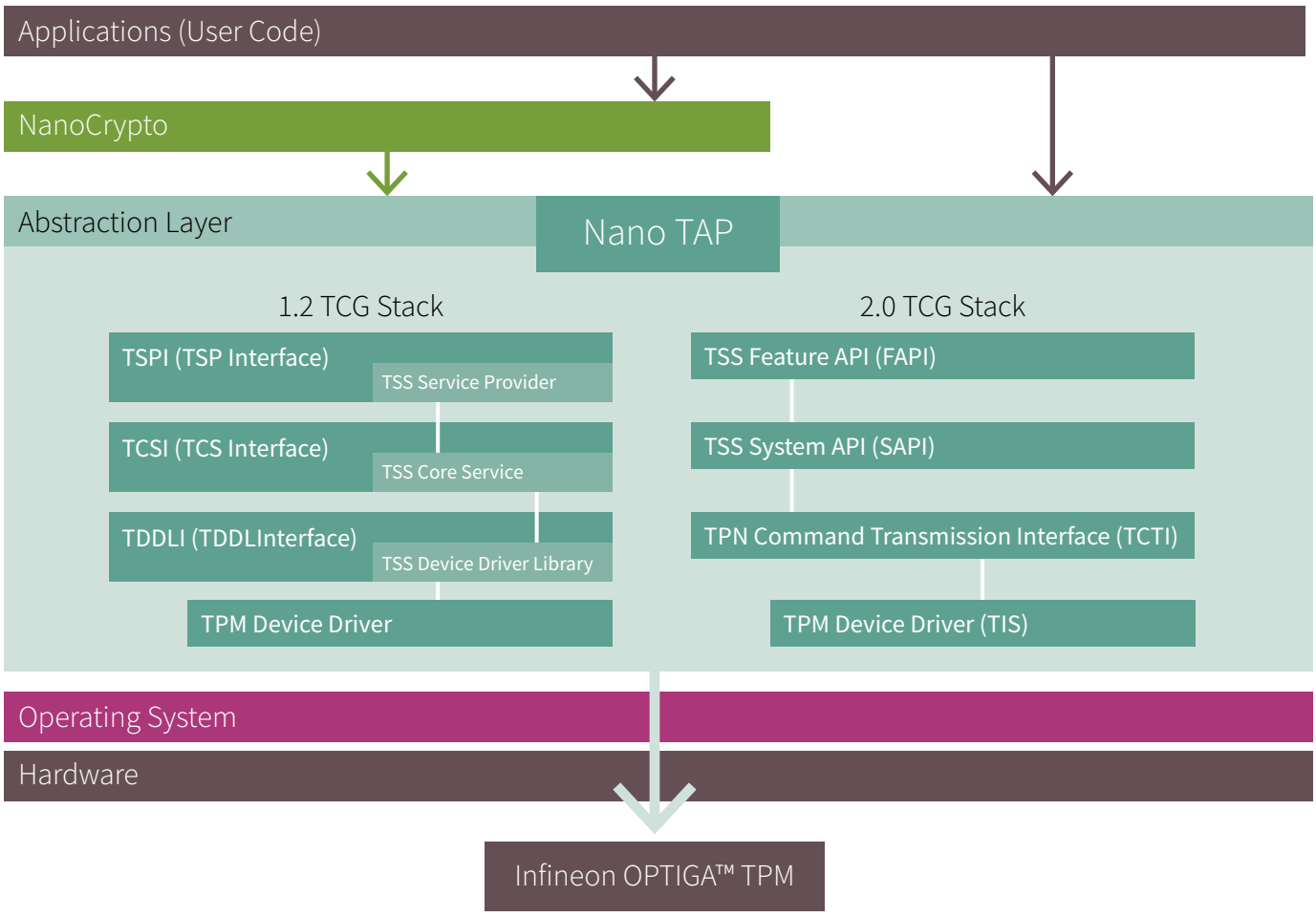
Main benefit of the Infineon product

The Mocana & Infineon Solution comes with out-of-the box support for the Infineon TPM and an integrated cryptographic library. It significantly reduces the time and cost required to develop and deliver products and services, providing a high level of hardware-based security.

Customers using OPTIGA™ TPM 1.2 or 2.0 with the Mocana NanoTAP module can benefit from having only one development track. Device and system OEMs can upgrade their products to the latest TPM standard with minimal code changes.

For OEMs who are already using the Mocana Security of Things Platform key functions, the transition to TPM is much easier than with custom software or open source solutions. The NanoTAP module is fully supported by Mocana with regular releases to deliver updates and enhancements. This eliminates the need for OEMs to continue investing in software support to access and utilize the TPM.

The Mocana / Infineon solution supports commercial IoT, Industrial IoT and traditional client-server security operations. This supports a device-to-cloud security architecture and delivers interoperable security across product lines, divisions and ecosystems.



Security Partner

Partner

MOCANA

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.

Mocana Corporation

Mocana provides the Mocana Security of Things Platform—a high-performance, ultra-optimized, OS-independent, high-assurance security solution for any device class. The Platform is being rapidly adopted by next-gen IoT device designers who demand architectural freedom, and who understand the complexity and risk exposure inherent in in-house and other solutions. Mocana's award-winning cryptographic solutions are used in the most stringently-constrained and life-critical systems by Fortune 500 companies, world-leading smart device manufacturers, and government agencies.

Mocana Corporation's contribution to the Infineon Security Partner Network

Mocana works with Infineon on their OPTIGA™ TPM 1.2 and 2.0 chips to tie root of trust down to the hardware level. Mocana's TPM support provides the tools to increase security surrounding sensitive information on devices containing a TPM. Our software licensing is subscription based, and can be implemented to interface with the TPM chip to generate hardware or software keys that can only be decrypted by the TPM. Mocana's security solutions are generally used by large industrial firms, automakers and device manufactures. Especially when it comes to Industrial Control Systems (ICS), it is hard to manage the Operation Technologies (OT) security systems that are in place. Mocana software was developed and tested to give companies architectural and safety benefits, having unified API- and General Public License (GPL)-free code.

Published by
Infineon Technologies AG
81726 Munich, Germany

Date: 09 / 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.