Security Partner

Partner Use Case

Accelerating the implementation of trusted computing

Building Confidence in Our Connected World with TPM middleware

Products

OPTIGA™ TPM

Security Partner

Use case

Application context and security requirement
IoT companies understand that having a Hardware Root of Trust, like the Infineon Trusted Platform Module (TPM), is an essential part of a secured application.

Challenge
The OPTIGA™ TPM provides a more secured way of assuring the integrity, authentication, and booting of IoT systems. However, using a TPM properly in a trusted computing environment can be tricky for IoT developers who are unfamiliar with the complex details of TPM architecture, and just want to focus on their application instead of learning the intricacies of the hardware to secure their system. OnBoard Security's TrustSentinel TSS 2.0 can solve all of those problems with an easy-to-use middleware solution.

Implementation
Instead of writing their own interfaces to the OPTIGA™ TPM, hardware, software developers can use the Trusted Computing Group Software Stack (TSS), which is middleware that provides the core interface and security services framework for any application relying on the TPM. OnBoard Security's TrustSentinel TSS 2.0 provides a direct interface to the OPTIGA™ TPM chip, IoT developers merely interface their applications with one of TrustSentinel's three Application Programming Interfaces (APIs) for the TPM, allowing applications to continue to function.

Benefits for the user:
- Using Infineon's OPTIGA™ TPM helps assure the integrity, authentication, and booting of IoT systems
- OnBoard Security's TrustSentinel TSS 2.0 enables applications to work across different operating systems with an easy-to-use middleware solution
- IoT developers only have to concentrate on the interface instead of having to code directly to the TPM

Security Partner

Solution

OnBoard Security gives Infineon customers the easiest way to realize the inherent value of Infineon's TPM within their platforms and systems through the strict adherence to the standardized Trusted Computing Group (TCG) APIs that are increasingly required by corporations and government agencies. OnBoard Security leads the TSS working group within the TCG, and therefore has a unique understanding of TSS standards, ensuring that TrustSentinel TSS 2.0 operates efficiently and effectively.

TrustSentinel TSS 2.0 provides three easy-to-use APIs, with varying levels of TPM abstraction depending on end application requirements.

1. The System API (SAPI) is especially designed for deeply embedded applications and has the smallest footprint.
2. The Enhanced System API (ESAPI) is a customized security solution, which can access to all TPM functions and offers the most flexibility.
3. A Higher-level Feature API (FAPI), which combines the most commonly, used TPM functions into easy-to-use features.

TrustSentinel is written in highly portable C99, simplifying the creation of language bindings to other programming languages (Java, Python, C++, etc.). It has a maximum portability across different Operating Systems and rich context management allows applications to share a TPM without worrying about resource collisions. ESAPI offers encrypted channels to the TPM, preventing side channel attacks and FAPI provides a new level of abstraction that allows programmers to use TPMs without having to be TPM experts.

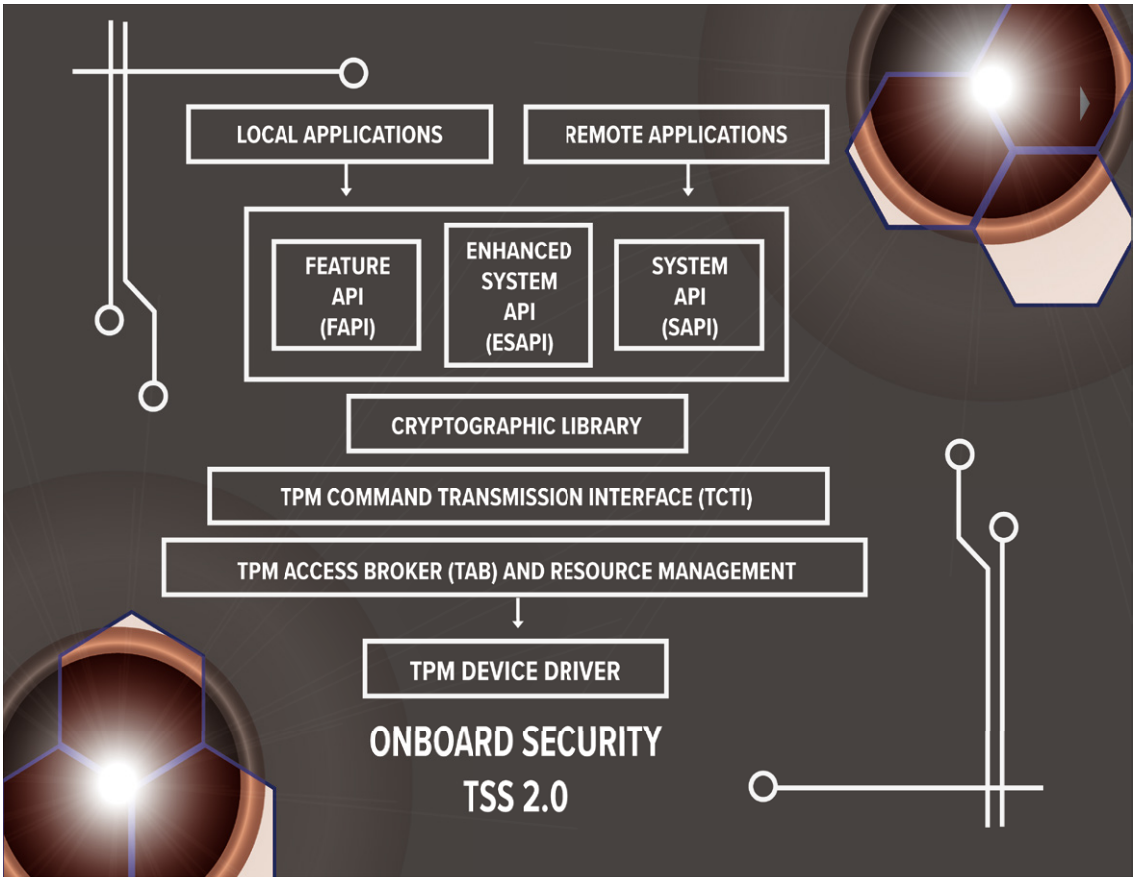
Key features:

› OnBoard Security's TrustSentinel 2.0 supports TCG Specifications
› Comprehensive testing ensures correct, secured TSS 2.0 behavior regardless of the vendor
› Versions for Linux, Windows and other operating systems
› World-class support to properly implement the transitive trust chain
› All code security and safety vulnerabilities addressed
› Leading provider of Industrial-Strength TSS 1.2

Security Partner

Solution

The Infineon TPM provides a hardware root of trust that your IoT system can rely on, thereby conferring significantly more security than a software-only solution. The TPM provides for the secured generation of cryptographic keys through a local random number generator and includes capabilities for remote attestation and secured boot. For remote attestation, the TPM creates a hash key summary of the hardware and software configuration allowing verification that the software has not been modified. The TPM also provides binding and sealing functions, which encrypts data and can specify the required TPM state before the data can be decrypted.



Security Partner

Partner

OnBoardSecurity
STAY AHEAD OF THE CURVE

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.

OnBoard Security
OnBoard Security was created to help automotive and IoT organizations stay ahead of the curve through superior cybersecurity.

For over 10 years, the world-renowned experts at OnBoard Security have been pioneering technologies that protect the Internet of Things, now and for the future. We address three significant challenges: ensuring the security and privacy of connected vehicles, making hardware roots of trust easy to use, and avoiding the existential threat from quantum computers to the integrity of the internet.

We are best known for the award-winning Aerolink® V2X libraries that are the de facto standard for connected vehicle security and privacy; our NTRU algorithm which is the most tested and trusted quantum-resistant cryptosystem; and our TrustSentinel TSS 2.0 middleware that simplifies implementation of Trusted Platform Modules. Headquartered in Wilmington, MA, OnBoard Security is a subsidiary of Security Innovation, with 25 employees.

OnBoard Security's contribution to the Infineon Security Partner Network
We can help you secure your IoT application. Our TrustSentinel TSS 2.0 makes using Trusted Platform Modules simple, creating a strong trusted computing environment for attestation and integrity. Our pqNTRUsign digital signing algorithm secures code updates and documents and will withstand the quantum computing assault on cryptography. Our Aerolink® Vehicle-to-Everything communications security software protects cars or any IoT device that needs a low bandwidth communication security solution. Finally, if you know you need a secured trusted computing environment, with secured communications and code updates but don't know how to achieve it, then our expert consultants can help you design a secured system.

Published by
Infineon Technologies AG
81726 Munich, Germany

Date: 10 / 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).