TrustSentinel 2.0

TCG SOFTWARE STACK (TSS) FOR TPM 2.0

Trusted Platform Modules (TPMs) are powerful, low-cost hardware security modules as specified by the Trusted Computing Group (TCG). The TCG Software Stack (TSS) is security "middleware" that allows applications and platforms to conveniently share and integrate TPMs into their secure applications. The OnBoard Security TrustSentinel 2.0 is a fully-supported, industrial-strength TSS 2.0 solution for platforms and applications using TPM 2.0.

TSS 2.0 is comprised of 3 discrete API layers, each offering different levels of abstraction and feature support. TrustSentinel 2.0 offers all 3 APIs.

KEY FEATURES

OnBoard Security TrustSentinel 2.0

Three layers allow scaling (memory, CPU, etc.) from the simplest IoT device to large servers

- SAPI (System Application Interface)
- ESAPI (Enhanced System Application Interface)
- FAPI (Feature Application Interface)

Written in highly portable C99, simplifying the creation of language bindings to other programming languages (Java, Python, C++, etc.)

Maximum portability across different Operating Systems

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

FAPI provides a new level of abstraction that allows programmers to use TPMs without having to be TPM experts

TrustSentinel 2.0 provides a simple, consistent API for application developers, allowing them to use the strong security features of the TPM 2.0 without having to learn the intricacies of the hardware.

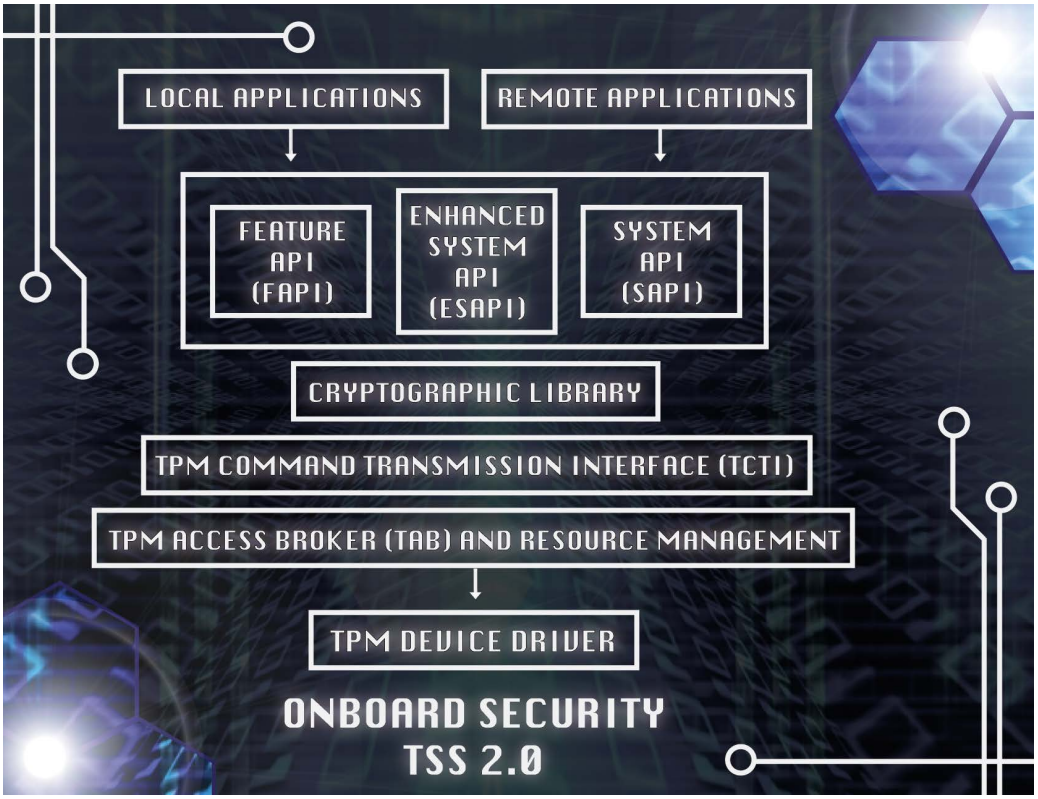
1.978.905.6796 ■ onboardsecurity.com

OnBoardSecurity

TSS 2.0 is a standard specified by the Trusted Computing Group. But even though it is a standard, not all TSS 2.0 solutions are alike.

WHY ONBOARD SECURITY'S TRUSTSENTINEL 2.0?

- OnBoard Security's TrustSentinel 2.0 supports TCG Specifications
- Comprehensive testing ensures correct, secure 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



TRUSTED COMPUTING GROUP

1.978.905.6796 ■ onboardsecurity.com

ONBOARDSECURITY