SECURITY INNOVATION

TSS

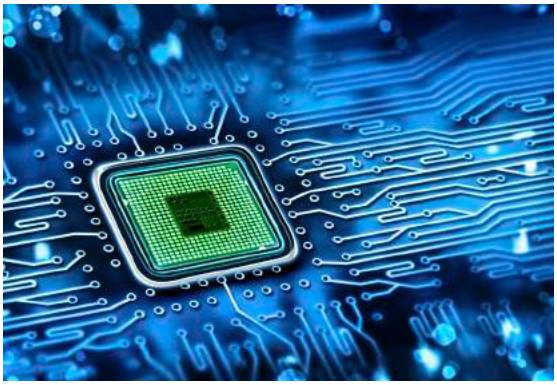
ROBUST, LOW-COST, HIGH SECURITY SOLUTION

Trusted Platform Modules (TPM) are powerful, low-cost hardware security modules (HSMs). The TPM Software Stack (TSS) is security "middleware" that allows applications and platforms to conveniently share and integrate TPMs into their security solutions. Today's TPM 1.2 and TSS 1.2 are mature and widely-deployed security solutions. The Security Innovation TSS is a well-supported, industrial-strength solution for platforms and applications using TPM 1.2.

FEATURES

The TSS provides a set of software components that allows platforms and applications to take advantage of a platform's TPM in a coordinated, consistent, and portable manner.

- Strong, standards compliant cryptographic services built-in
- Modular design enables addition of custom functionality
- Protects authorization data within the local process
- Thread-safe design
- Supports local and remote TPMs
- Design and implementation techniques in accordance with industry best practices for protecting against security vulnerabilities
- Ability to leverage TPM custom features



Designed in Strict Compliance with TCG TSS Specifications

- By leveraging SI's extensive TCG expertise and involvement, application developers can focus on their core competencies without worrying about the security and reliability of their underlying TPM and TSS infrastructure.

Application Defined Security Policies

- Security policies defined to meet the needs of the end user

Posed for Tomorrow

- Security Innovation's TSS 2.0 will continue to provide all the benefits of our current TSS while introducing new and more powerful features to address our customer's evolving security needs.

INDUSTRY STANDARD CYRPTOGRAPHIC SERVICES

- RSA encrypt/decrypt OAEP
- RSA encrypt/decrypt RSAES-PKCSv15
- RSA sign/verify RSASSA PKCS1-V1_5
- HMAC-SHA1 RFC2202
- AES

SUPPORTED PLATFORMS

- Windows 10, 8, 7, Vista, XP
- Linux Kernels 2.6 and higher

www.securityinnovation.com/contact | 978.694.1008 | @SecInnovation