TSP

Tyrone Secure Platform

Add-on-Module TCG 1.2 / 2.0 -FIPS

The Tyrone Trusted Platform Module (TCG 2.0) is a hardware-based security device that can be added to a system motherboard to hold computer generated keys for encryption. This outstanding solution ensures that information keys, passwords and digital certificates will be more secure from external software attacks and physical theft, by performing all cryptographic functions on the device. Tyrone TPM (TCG 2.0) is an ideal tool for customers who are looking for an additional layer of security to their Tyrone Servers.

Specifications

Physical Dimensions

26.13mm x 14.64mm x 9.93mm

Security Features

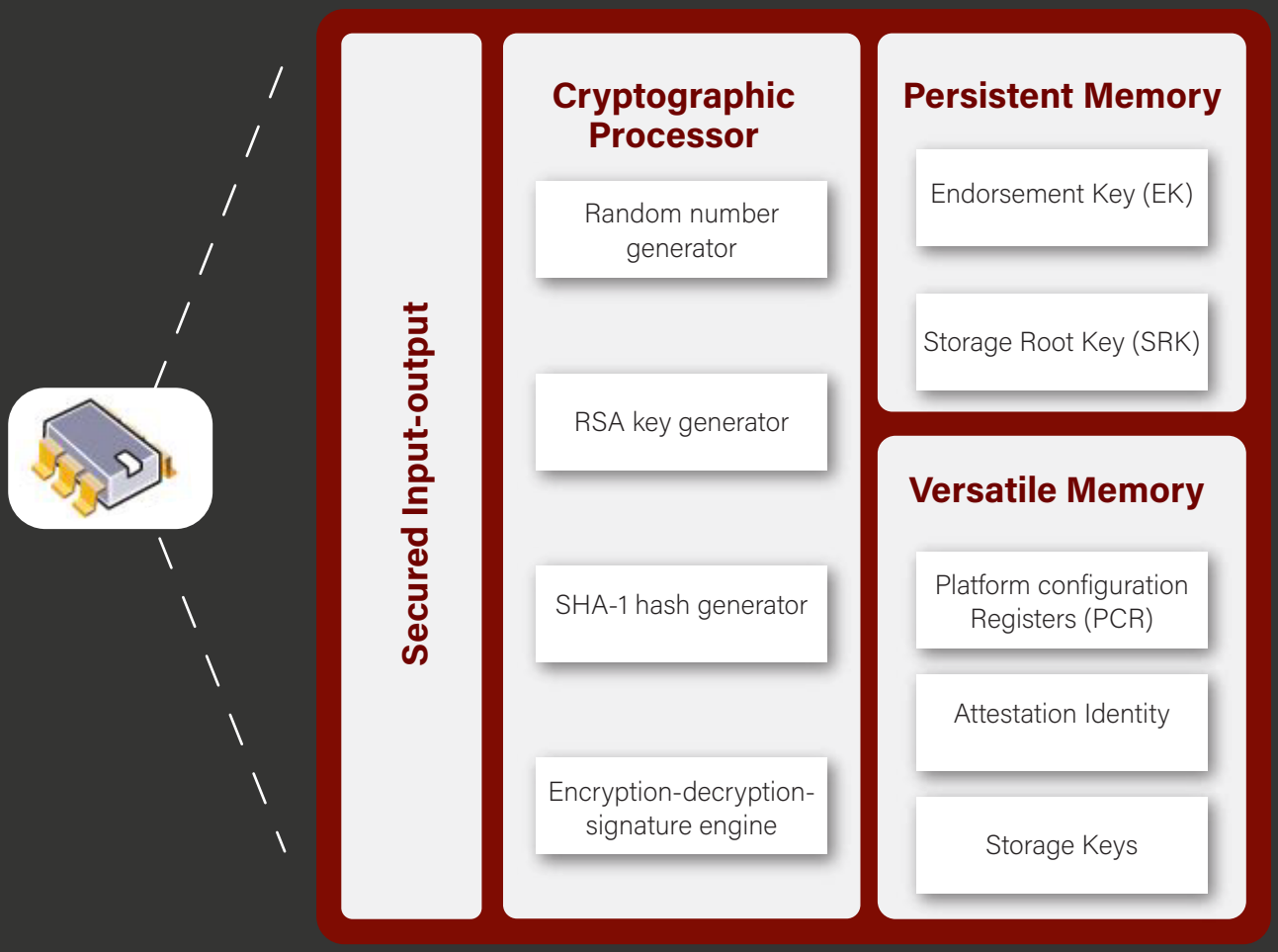
Over/Under voltage Detection
Low frequency sensor
High frequency filter
Reset filter
Memory Encryption/Decryption (MED)

System Lockdown

System Lockdown is a security feature that prevents all system configuration changes including firmware updates.

Application Supports

Microsoft Tools
Mozilla Firefox™
Mozilla Thunderbird™
Netscape Communicator
Google Chromebook
Google Chromebox
Microsoft Encrypted File System
RSA Secure ID
Check Point r▪ SecuRemote/SecureClient
Check Point™ VPN-1/FireWall-1 NG
Entrust™ Desktop Manager Solutions
Adobe™ Acrobat 6.0 Professional
GemSafe for TPM / Smart Card



Key Features

TCG 2.0 compliant trusted platform module (TPM)
Compliant embedded software
EEPROM for TCG firmware enhancements and for user data and keys
Hardware accelerator for SHA-1 and SHA-256
Random Number Generator (RNG)
Meeting Intel TXT, Microsoft Windows and Google Chromebook certification criteria Protection against Dictionary Attack
SPI interface
Intel Trusted Execution Technology Support
AMO Secure Virtual Machine Architecture Support
Protection and Secrecy of the cryptographic system both for reading out and manipulation of the material.
Pre-Generation of RSA Keys
Power saving sleep mode
3.3 V power supply
Built-in support by Linux Kernel
Operating temperature range: -20"C to +B0"C
Root-of-Trust

Compliance

RoHS	RoHS Compliant 6/6 (2011/65/EU), Pb Free

Tyrone

facebook.com/tyronesystems
twitter.com/tyronesystems
linkedin.com/company/tyrone-systems

Let's Talk

Press Inquiries
Email: info@tyronesystems.com

Support Inquiries
Email: tyronecare@tyronesystems.com

Partner Inquiries
Email: info@tyronesystems.com