Trusted Platform Module with TCG 2.0

Introduction

Supermicro's Trusted Platform Module **AOM-TPM-9665V/H** with TCG 2.0, stores information such as keys; password and digital certificates, and provides additional security against external software attacks and from physical theft to systems.

TPM implements Root-of-Trust, which initiates during system boot process to establish trust level; gathering measurements about the running environment, OS, for trusted reporting. Security of the whole system is based on the protection and secrecy of the cryptographic system, especially against reading out or manipulation of the key material.

Supermicro's **AOM-TPM-9665V/H** provides a computing system the ability to run applications more securely, run a more secured remote access environment, as well as perform electronic transactions and digital communications more safely and security.

TCG 2.0	Model #	Form Factor	TXT* (provisioning)	MB Support	Supported CPUs
	AOM-TPM-9665V	Vertical	N/A	Intel®	Any MBs with TPM support
	AOM-TPM-9665V-S	Vertical	Server	Intel®	Xeon® E5/7 processors
	AOM-TPM-9665V-C	Vertical	Client	Intel®	Intel® Core i5/ i7 & Xeon E3 processors
	AOM-TPM-9665H	Horizontal	N/A	Intel®	Any MBs with TPM support
	AOM-TPM-9665H-S	Horizontal	Server	Intel®	Xeon® E5/7 processors
	AOM-TPM-9665H-C	Horizontal	Client	Intel®	Intel® Core i5/ i7 & Xeon® E3 processors

** TPM provisioning is required for TXT function, selecting server or client provisioning depends on the CPU and MB that is going to be used.*

Key Features:

- TCG 2.0 compliant Trusted Platform Module (TPM)
- Microcontroller in 0.22/0.09 µm CMOS technology
- Compliant embedded software
- EEPROM for TCG firmware enhancements and for user data and keys
- Hardware accelerator for SHA-1 and SHA-256 hash algorithm
- True Random Number Generator (TRNG)
- Tick counter with tamper detection
- Protection against Dictionary Attack
- General Purpose Input/output
- Intel® Trusted Execution Technology (TXT) Support
- Full personalization with Endorsement Key (EK) and EK certificate
- Power saving sleep mode
- 3.3 V power supply
- Form Factor:
  Vertical: AOM-TPM-9665V (8mm x 26mm x 25mm) (W x L x H)
  Horizontal: AOM-TPM-9665H (26mm x15.6mm x13.10mm) (W x L x H)

Security Features:

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

TPM 2.0 improvements

- Improved encryption capability
- Improved TPM to application integration
- Enhanced authorization mechanisms
- Simplified TPM management with additional capabilities to enhance platform security
- Provides specific-use algorithms to meet geographies based or market specific requirement

Trusted Execution Technology (TXT)

Supermicro **AOM-TPM-9665V/H** leverages Intel's Trusted Execution Technology (Intel® TXT) to strengthen platforms from the emerging threats of hypervisor attacks, BIOS, or other firmware attacks, malicious root kit installations, or other software based attacks. It increases protection by allowing greater control of the launch stack through a Measured Launch Environment (MLE) and enabling isolation in the boot process. More specifically, it extends the Virtual Machine Extensions (VMX) environment of Intel® Virtualization Technology (Intel® VT), permitting a verifiably secure installation, launch, and use of a hypervisor or operating system (OS).

Supermicro **AOM-TPM-9665V/H**, with Intel® TXT, gives IT and security organizations critical enhancements to help ensure more secure platforms.

It also provides greater application, data, or virtual machine (VM) isolation; and improved security or compliance audit capabilities. Not only can it help reduce support and remediation costs, it can also provide a foundation for more advanced solutions as security needs change to support increasingly virtualized or "multi-tenant" shared data center resources.

Key Features:

- **Strong authentication**: Uses hardware module, TPM and Software TXT to provide two-factor authentication
- **Low risk**: Two Authentication methods utilizing TPM & TXT ensuring interoperability by authentication, platform Integrity check, RSA key creation management and storing the encrypted key with in the TPM chipset.
- **Low TCO**: 50% or more reduction in total cost of ownership (TCO) by leveraging existing hardware and lowering ongoing costs, providing a highest security at lowest cost per TB
- **Easy to manage**: Integrates with existing X10/B10 MB Platform
- **Flexibility**: Supports any Supermicro Systems/Motherboards with multiple RAID controllers & HDDs