Add-on-Module AOM-TPM-9665H(-S/C)

Specifications

Add-on-Module

Supermicro's Trusted Platform Module **AOM-TPM-9665H(-S/-C)** 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-9665H(-S/-C)** 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.



To order, contact your distributor. This product is only available through Supermicro.

Key Features

- TCG 2.0 compliant trusted platform module (TPM)
- Microcontroller in 0.22/0.09 m 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

Compliance

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

Specification

- **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

- **Application Supports**
  - Microsoft Outlook® and Outlook Express®
  - Microsoft Office 2010, Office 2000, Office XP and Office 2003
  - Microsoft Internet Explorer®
  - Mozilla Firefox™
  - Mozilla Thunderbird™
  - Netscape Communicator®
  - Microsoft Encrypted File System
  - RSA Secure ID®
  - Check Point™ SecuRemote/SecureClient
  - Check Point™ VPN-1®/FireWall-1 NG®
  - Entrust™ Desktop Manager Solutions
  - Adobe™ Acrobat 6.0 Professional

- **Operating Conditions**
  - Operating temperature range:
    -20°C to 80°C (-4°F to 176°F)
    -40°C to 85°C (-40°F to 185°F)

- **Physical Dimensions (W x L x H)**
  - Horizontal Design / 26mm x15.6mm x13.10mm

Supported Platforms

Motherboards	X10 motherboards with 20-pin TPM header

Downloads

Datasheet	[Download]
User's Guide	[Download] (2MB)

Trusted Execution Technology (TXT) 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

Parts List

Parts List

Part Number	Form Factor	TXT*	MB Platform	Supported CPUs
AOM-TPM-9665H	Horizontal	N/A	Intel	Any MBs with TPM support
AOM-TPM-9665H-S	Horizontal	Server	Intel	Xeon® E5/E7 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.

Copyright © 2019 Super Micro Computer, Inc.

Information in this document is subject to change without notice.
Other products and companies referred to herein are trademarks or registered trademarks of their respective companies or mark holders.