AOM-TPM-9655H

SUPERMICRO®

The Supermicro AOM-TPM-9655H is a security hardware device on the system board that will hold computer generated keys for encryption. Supermicro's outstanding hardware base solution ensures that the information like keys, password and digital certificates stored within is made more secure from external software attacks and physical theft. With the handful of keys it stores, all cryptographic functions are performed on the chip. AOM-TPM-9655H is an ideal tool for customers who are looking for additional layer of security to their superservers.

Key Features

- **TCG 1.2/2.0 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**
- **Infineon's TPM 1.2 is Common Criteria certified at Evaluation Assurance Level (EAL) 4 Moderate**
- **General Purpose Input/Output**
- **Intel® Trusted Execution Technology Support**
- **AMD® Secure Virtual Machine Architecture Support**
- **Full personalization with Endorsement Key (EK) and EK certificate**
- **Power saving sleep mode**
- **3.3 V power supply**
- **WHQL dual mode 1.1b + 1.2 TPM Windows Kernel Mode Driver**
- **Operating temperature range: -20°C to +80°C and -40°C to +85°C**

Specifications

Security Features

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

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
- GemSafe for TPM / Smart Card

Mechanical specifications for the module (Horizontal)

- Dimension: (26mm x15.6mm x13.10mm) (W x L x H)

Compliance/Environmental

- RoHS Compliant 6/6, Pb Free RoHS

Supported Platforms

- Supermicro motherboards with 20-pin TPM connectors

Please note that this product is only available as an integrated solution with Supermicro server systems