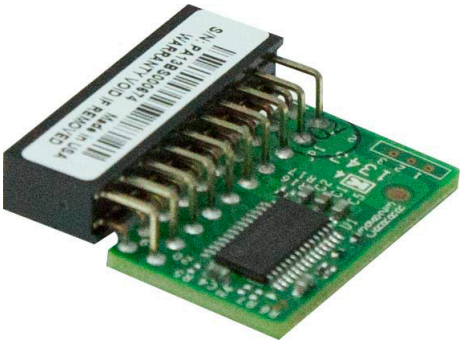
Add-on-Module AOM-TPM-9655V

The Supermicro Add-on-Module AOM-TPM-9655V is a specialized security device that stores RSA encryption keys specific to the host system for hardware authentication. The Supermicro AOM is implemented using Infineon's Trusted Platform Module (TPM), and is fully standards compliant with the specifications published by Trusted Computing Group (TCG) certification process. The Trusted Platform Module (TPM) has a protected and encapsulated microcontroller security chip to defend the internal data structures against real intelligent attacks. The cryptographic function ensures that the information like keys, password and digital certificates stored on the chip are protected from external software attacks and physical theft. The TPM module is typically paired to the motherboard of the computing system. The TPM function is integrated into the boot process to establish trust level and gather measurement about the runtime environment for trusted reporting.
AOC-TPM-9566V is ideal for customer looking for additional layer of security for their systems. It provides the ability for a computing system to run applications more securely, while allowing remote access and to perform online transactions and communications more safely.

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 (TXT) 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**

Specifications

Security Features

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

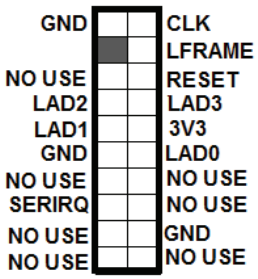
Application Support (including, but not limited to)

- 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

Mechanical specifications for the module (Vertical Design)

- Dimensions (8mm x 26mm x 25mm) (W x L x H)

Pin out of the module



Compliance/Environmental

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

Supported Platforms

- Supermicro systems/motherboards with 20-pin TPM headers