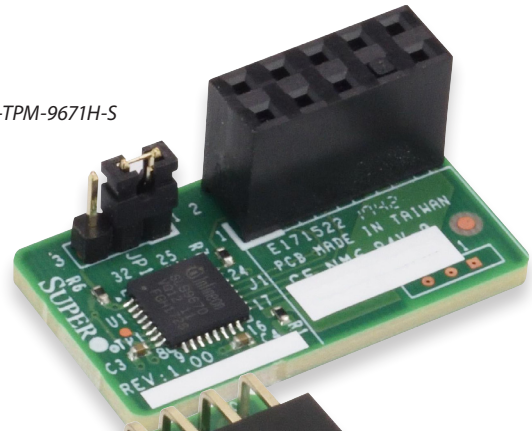
AOM-TPM-9671V-S / AOM-TPM-9671H-S

The Supermicro AOM-TPM-9671V/H-S 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. AOM-TPM-9671V/H-S is an ideal tool for customers who are looking for an additional layer of security to their Supermicro Superservers.

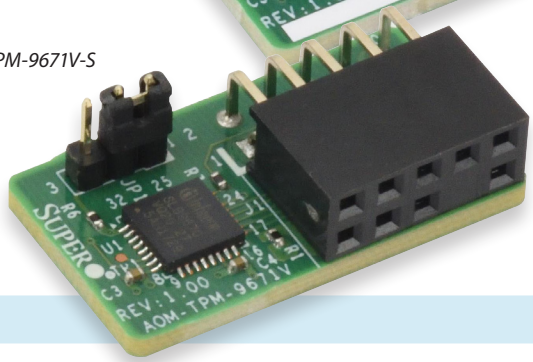
Key Features:

- **TCG 1.2 compliant trusted platform module (TPM)**
- **Compliant embedded software**
- **EEPROM for TCG firmware enhancements and for user data and keys**
- **Hardware accelerator for SHA-1**
- **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**
- **AMD Secure Virtual Machine Architecture Support**
- **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 +80°C**

AOM-TPM-9671H-S



AOM-TPM-9671V-S



Specifications & Features

- **Physical Dimensions**
  - AOM-TPM-9671V-S (WxLxH): 26.13mm x14.64mm x9.93mm
  - AOM-TPM-9671H-S (WxLxH): 26.13mm x14.64mm x13.10mm
- **Security Features**
  - Over/Under voltage Detection
  - Low frequency sensor
  - High frequency filter
  - Reset filter
  - Memory Encryption/Decryption (MED)
- **Application Supports**
  - Microsoft Tools
  - Mozilla Firefox™
  - Mozilla Thunderbird™
  - Netscape Communicator
  - Google Chromebook
  - Google Chromebox
  - 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
- **Supported Platforms**
  - Supermicro motherboards with 10-pin TPM connectors.

MKT-0023-3/2018- 1.4