ASHATA ASHATAo1a3ygruec

ASHATA TPM 2.0 Module Instruction Manual

Model: ASHATAo1a3ygruec

Brand: ASHATA

1. Introduction

This manual provides instructions for the installation and operation of the ASHATA TPM 2.0 Module, model ASHATAo1a3ygruec. This module is designed to enhance system security by providing cryptographic functions and secure storage for sensitive data, compliant with TCG 2.0 standards.
The TPM (Trusted Platform Module) is a dedicated microcontroller designed to secure hardware by integrating cryptographic keys into devices. It is essential for features like Windows BitLocker, secure boot, and other security-sensitive applications.

2. Key Features

- **SuperMicro Compatibility:** Specifically designed for 10Pin SPI TMP2.0 trusted platforms, compatible with SuperMicro AOM TPM 9670V S.
- **TCG 2.0 Compliant:** Adheres to Trusted Computing Group (TCG) 2.0 specifications for enhanced security.
- **Advanced Security:** Supports embedded software for TCG firmware enhancement and hardware accelerators for user data and keys, including EEPROM SHA 1 and SHA 256, and a random number generator (RNG).
- **Standard Support:** Meets Intel TXT, Windows, and Chromebook authentication standards to prevent dictionary attacks.
- **Stable Performance:** Constructed with a premium printed circuit board material for reliable and efficient operation.

- **Power Saving:** Supports power-saving sleep mode and Intel trusted technology.
- **RSA Key Pre-generation:** Facilitates RSA key pre-generation for cryptographic operations.
- **Linux Core Support:** Includes built-in support for Linux core environments.

3. Technical Specifications

Item Type	TPM 2.0 Module
Material	Printed Circuit Board
Color	Green
Chipset	For INFINEON 9670
Interface	SPI
TPM Version	TPM 2.0
Pin Definition	10Pin (10-1Pin)
Application	Designed for SuperMicro AOM TPM 9670V S
Power Supply	3.3V
Model Number	ASHATAo1a3ygruec
Item Weight	0.528 ounces
Package Dimensions	8.94 x 3.78 x 0.63 inches

4. Compatibility

This TPM 2.0 module is specifically designed for SuperMicro AOM TPM 9670V S motherboards that support a 10-pin SPI TPM 2.0 interface. It is crucial to verify your motherboard's compatibility before installation.
The module is compatible with embedded software for TCG firmware enhancement and hardware accelerators for cryptographic operations, including SHA 1 and SHA 256, and a random number generator (RNG).
It supports Intel TXT, Windows, and Chromebook authentication standards.

5. Setup and Installation

Before proceeding with installation, please review the following important notices:

- **Motherboard Manual Check:** Always consult your motherboard's manual to confirm that it supports TPM 2.0 technology and has the correct 10-pin SPI header.
- **BIOS Update:** Some motherboards may require a BIOS update to the latest version to enable the TPM option in the BIOS settings.
- **Security Technologies:** It is recommended to remove or disable any other existing security technologies (e.g., older TPM modules, specific software-based security features) from your computer before installing this module to prevent conflicts.

Installation Steps:

1. **Power Off System:** Ensure your computer is completely powered off and disconnected from the power source.
2. **Open Computer Case:** Carefully open your computer case to access the motherboard.
3. **Locate TPM Header:** Identify the 10-pin SPI TPM header on your motherboard. Refer to your motherboard manual for its exact location.
4. **Insert TPM Module:** Align the ASHATA TPM 2.0 module with the 10-pin header. Gently press the module into the header until it is securely seated. Ensure the orientation is correct to avoid damage.
5. **Close Case:** Once the module is installed, close your computer case.
6. **Power On System:** Reconnect the power and turn on your computer.

Image 1: Top view of the ASHATA TPM 2.0 Module, showing the main chip and the 10-pin connector. This is the module you will be installing.

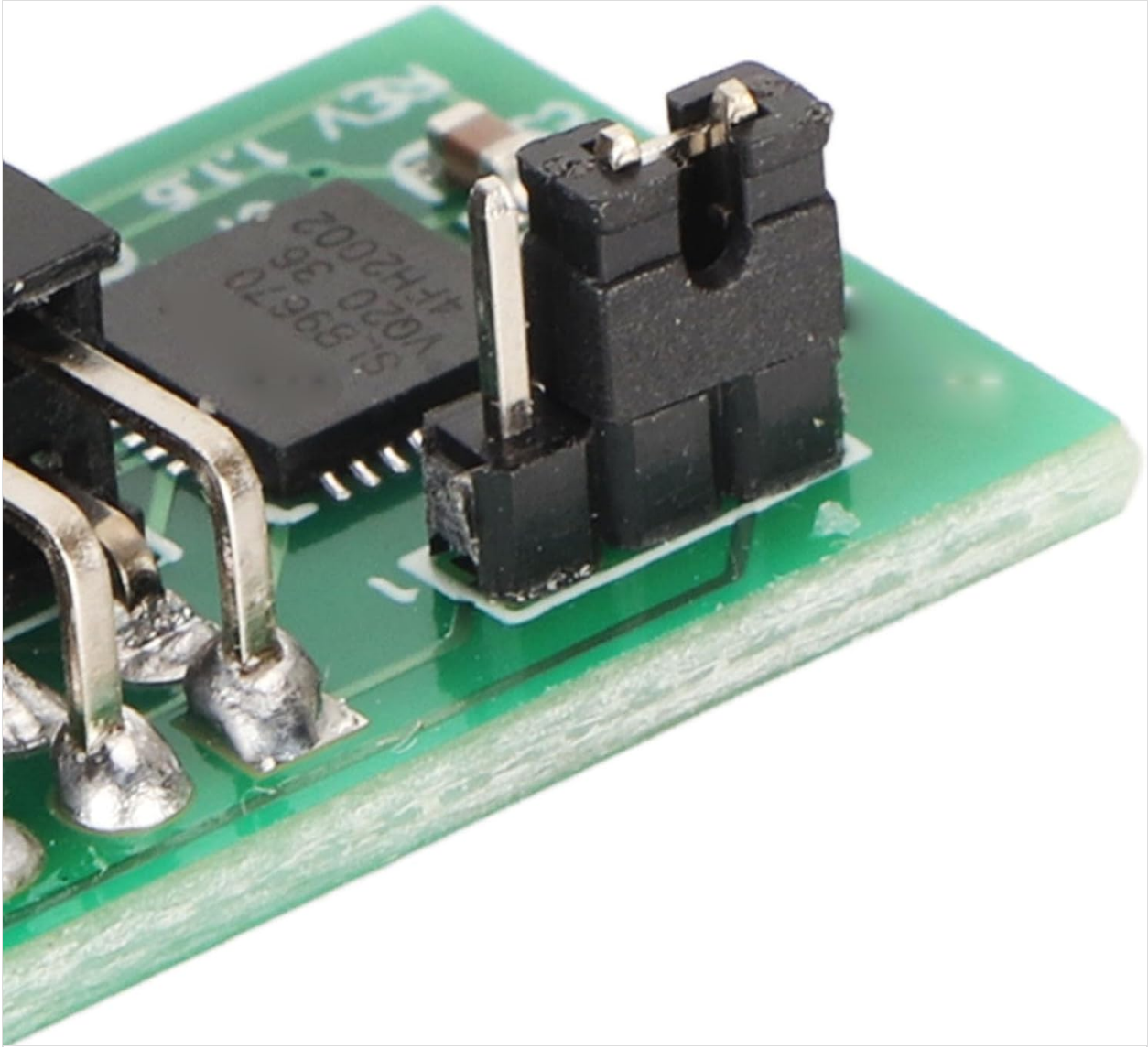

Image 2: A close-up view of the 10-pin connector on the TPM module, which connects to the motherboard header. Ensure proper alignment during installation.

6. Operating Instructions

After physical installation, the TPM module typically needs to be enabled and configured within your system's BIOS/UEFI settings.

1. **Access BIOS/UEFI:** During system startup, repeatedly press the designated key (commonlyDel, F2, F10, or F12) to enter the BIOS/UEFI setup utility. The specific key varies by motherboard manufacturer.
2. **Locate TPM Settings:** Navigate through the BIOS/UEFI menus to find settings related to "Security," "Trusted Computing," or "Advanced." Look for options like "TPM State," "Intel Platform Trust Technology (PTT)," or "AMD fTPM."
3. **Enable TPM:** Set the TPM state to "Enabled" or "Active." You may also need to enable "Secure Boot" or other related security features depending on your system's requirements.
4. **Save and Exit:** Save the changes to the BIOS/UEFI settings and exit. Your system will restart.
5. **Verify in Operating System:** Once the operating system loads, you can verify the TPM status.
    - **Windows:** Press Win + R, type `tpm.msc`, and press Enter. The TPM Management console will display the status of the TPM.
    - **Linux:** Use commands like `dmesg | grep -i tpm` or check the `/dev/tpm0` device.

Once enabled, the TPM module will function automatically with compatible operating system features and applications that utilize trusted computing capabilities.

7. Maintenance

The ASHATA TPM 2.0 Module is a passive component and requires minimal maintenance. Follow these guidelines for optimal performance and longevity:

- **Physical Care:** Keep the module free from dust and moisture. Ensure it is securely seated in its header.
- **Firmware Updates:** TPM firmware updates are typically handled through motherboard BIOS/UEFI updates. Always refer to your motherboard manufacturer's website for the latest BIOS versions and instructions.
- **System Environment:** Operate your computer in a clean, dry, and temperature-controlled environment to prevent damage to internal components, including the TPM module.

8. Troubleshooting

If you encounter issues with your ASHATA TPM 2.0 Module, consider the following troubleshooting steps:

- **TPM Not Detected:**
  - Ensure the module is correctly and firmly seated in the motherboard's TPM header.
  - Verify that your motherboard supports TPM 2.0 and has the correct 10-pin SPI header.
  - Check your motherboard's BIOS/UEFI settings to ensure TPM is enabled.
  - Update your motherboard's BIOS/UEFI to the latest version.
- **TPM Errors in OS:**
  - Ensure all necessary drivers (usually part of OS or chipset drivers) are installed.
  - If migrating from an older TPM, ensure the old TPM was cleared or disabled before installing the new one.
  - Check for conflicting security software or settings.
- **System Instability After Installation:**
  - Remove the TPM module and check if the system stabilizes. If it does, re-verify compatibility and installation steps.
  - Ensure the module is not damaged.

For persistent issues, consult your motherboard's support documentation or contact ASHATA customer support.

9. Important Notices

- This TPM module is designed for specific motherboard compatibility. Incorrect installation or use with unsupported motherboards may lead to system instability or damage.
- Always handle electronic components with care, observing anti-static precautions.
- Modifying the module or using it in ways not specified in this manual may void any applicable warranty.

For support, please visit the ASHATA official website or contact your retailer.