Asrock-TPM

TPM2.0 Module Asrock-TPM 18-1Pin 2.0mm Security Module User Manual

Model: Asrock-TPM | Brand: Generic

1. Introduction

This manual provides comprehensive instructions for the installation, operation, and troubleshooting of the Generic Asrock-TPM 18-1Pin 2.0mm Security Module. This Trusted Platform Module (TPM) is designed to enhance system security by providing hardware-based cryptographic functions, essential for modern operating systems like Windows 11.

Figure 1.1: Generic Asrock-TPM 18-1Pin 2.0mm Security Module (Top View)

This image displays the top side of the TPM2.0 module, highlighting its compact form factor and the 18-1Pin connector. The module features the Infineon security chip, visible on the board.

2. Compatibility Notes

Before proceeding with installation, please review the following critical compatibility information:

- This TPM module is **not compatible** with motherboards that utilize 3rd generation DDR3 memory.
- This module is **compatible** with DDR4 RAM motherboards.
- Laptops are **not supported**. This module is intended for desktop motherboards.
- Motherboards manufactured before the X99 chipset generation generally **do not support** TPM2.0.
- Ensure your motherboard has the necessary hardware interface support for an 18-1Pin TPM module. Verify the pin sequence and pin spacing match the module.
- The TPM function must be enabled in your motherboard's BIOS/UEFI settings. Some motherboards may require a BIOS update to enable this option.

3. Installation Guide

3.1 Pre-installation Checks

Before installing the TPM module, perform the following checks:

1. **Verify Motherboard Support:** Confirm your motherboard has a dedicated TPM header and supports TPM2.0. Consult your motherboard's manual or manufacturer's website if unsure.
2. **Check Pin Configuration:** Ensure the pin sequence and spacing of your motherboard's TPM header match the 18-1Pin configuration of this module.
3. **BIOS/UEFI Readiness:** Check if your BIOS/UEFI has the option to enable TPM. If not, you may need to update your BIOS to the latest version.
4. **Power Off System:** Completely shut down your computer and disconnect it from the power source before proceeding with physical installation.

3.2 Physical Installation

Follow these steps to physically install the TPM module onto your motherboard:

1. **Locate TPM Header:** Identify the TPM header on your motherboard. It is typically labeled "TPM" or "JTPM". Refer to your motherboard's manual for the exact location.
2. **Align Module:** Carefully align the TPM module with the header pins. Ensure the missing pin on the module aligns with the corresponding blocked pin on the motherboard header.
3. **Insert Module:** Gently but firmly press the TPM module into the header until it is fully seated. Do not force the module, as this can damage the pins.

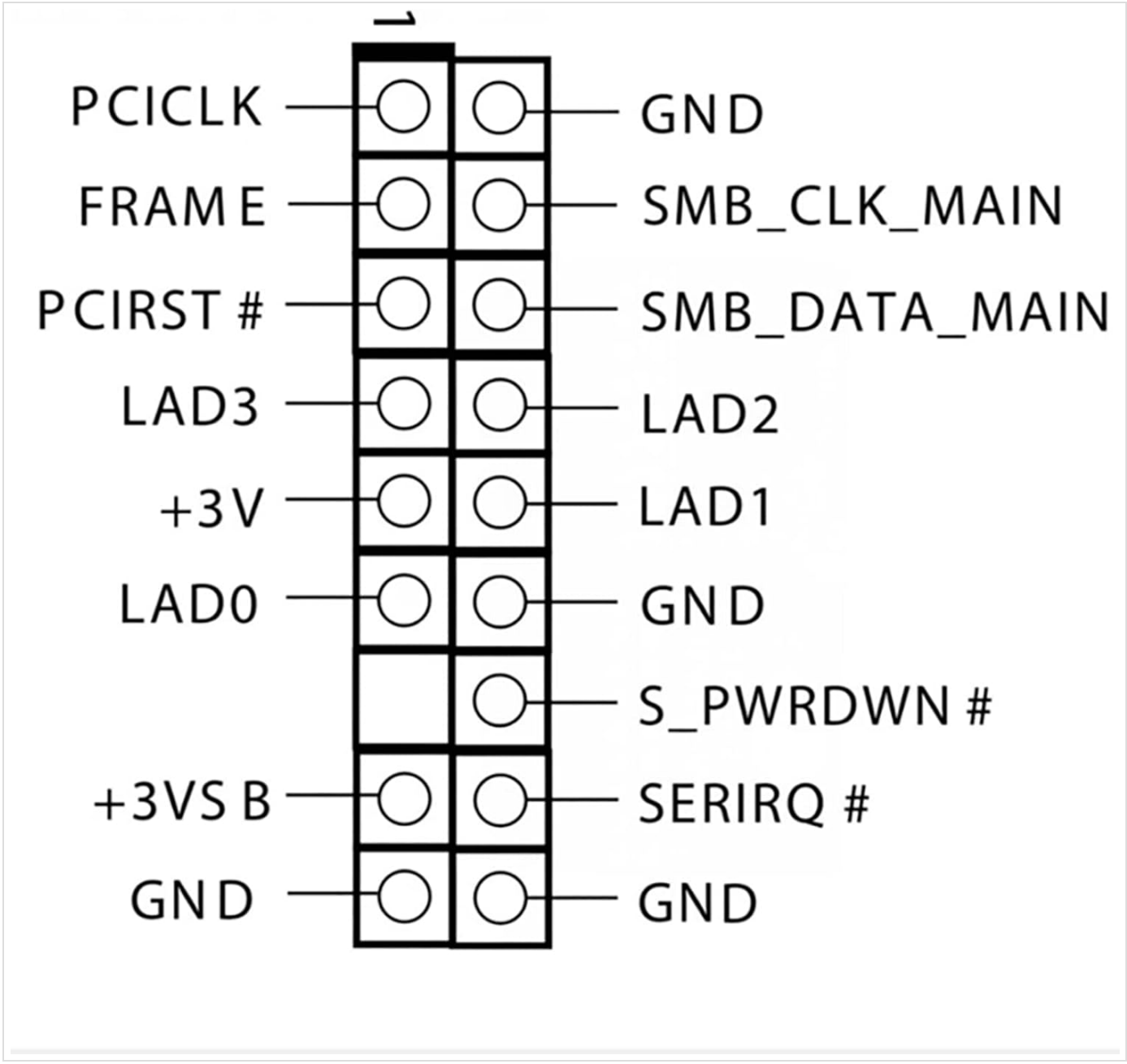

Figure 3.1: Typical TPM Header Pinout Diagram

This diagram illustrates a common pinout configuration for a TPM header, showing pin labels such as PCICLK, FRAME, PCIRST#, LAD0-3, +3V, GND, SMB_CLK_MAIN, SMB_DATA_MAIN, S_PWRDWN#, and SERIRQ#. Pin 1 is typically indicated for correct orientation.

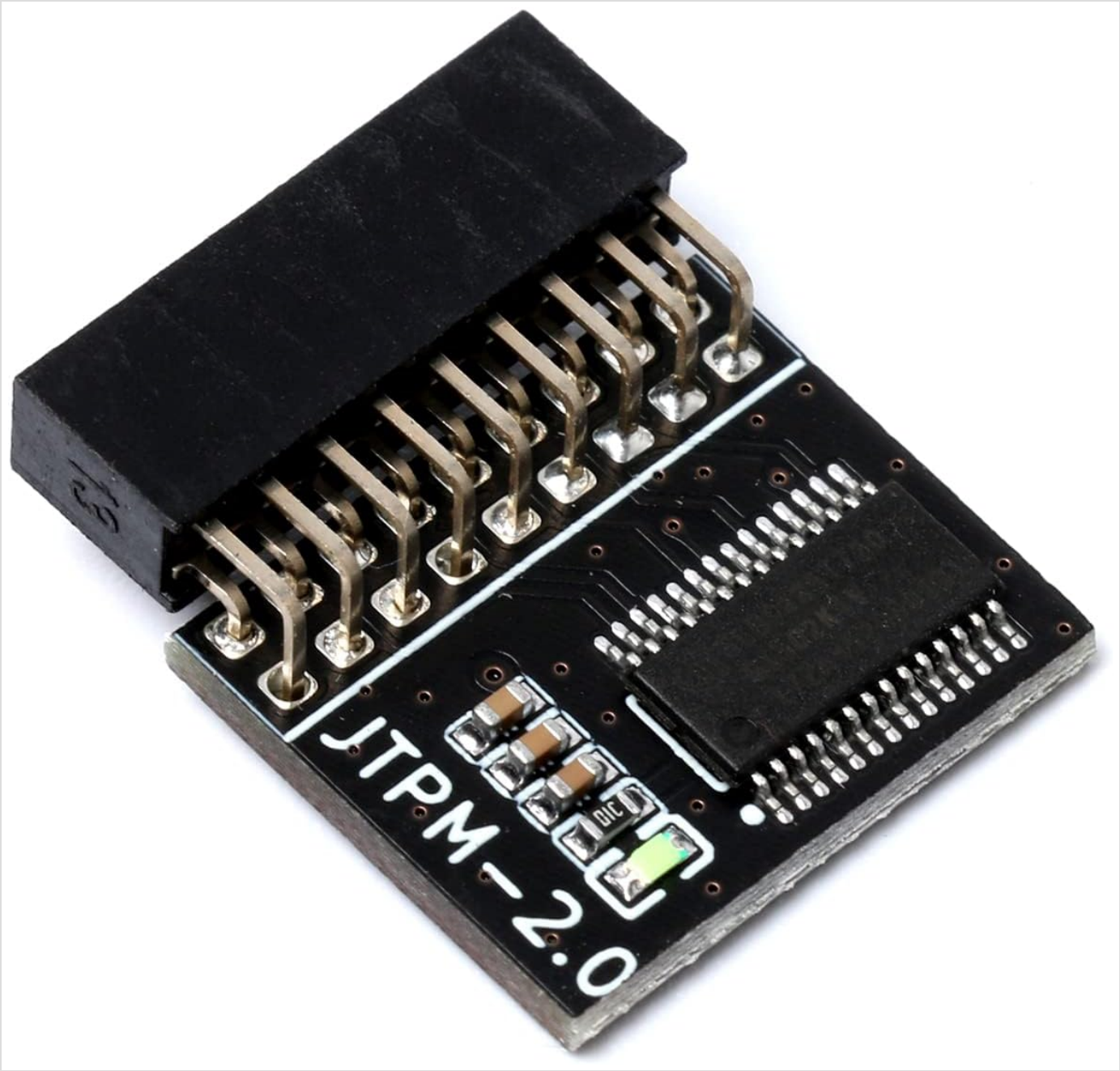

Figure 3.2: TPM Module Pin Connector

This image provides an angled view of the TPM module, clearly showing the 18-1Pin connector designed to interface with the motherboard's TPM header. Proper alignment is crucial for installation.

3.3 BIOS/UEFI Configuration

After physical installation, you must enable the TPM function in your system's BIOS/UEFI:

1. **Enter BIOS/UEFI:** Power on your computer and repeatedly press the designated key (e.g., Del, F2, F10, F12) during startup to enter the BIOS/UEFI setup utility.
2. **Locate TPM Setting:** Navigate to the security, boot, or advanced settings section. Look for an option related to "TPM," "Trusted Platform Module," "Intel Platform Trust Technology (PTT)," or "AMD fTPM."
3. **Enable TPM:** Change the setting from "Disabled" to "Enabled."
4. **Save and Exit:** Save your changes and exit the BIOS/UEFI. Your system will restart.

Note: The exact menu names and locations may vary depending on your motherboard manufacturer and BIOS version. If you encounter difficulties, consult your motherboard's user manual or manufacturer's support resources.

4. Operation

Once the TPM module is installed and enabled in the BIOS/UEFI, your operating system, such as Windows 11, will automatically detect and utilize it for enhanced security features. These features include BitLocker drive encryption, secure boot, and other integrity checks.

To verify TPM status in Windows:

1. Press `Windows Key` + `R` to open the Run dialog.
2. Type `tpm.msc` and press `Enter`.
3. The "TPM Management on Local Computer" window will display the status of your TPM module.

5. Maintenance

The TPM module is a hardware component that generally requires no ongoing maintenance once installed and configured. However, consider the following:

- **Firmware Updates:** In rare cases, your motherboard manufacturer might release BIOS/UEFI updates that include TPM firmware updates. Always follow the manufacturer's instructions carefully when performing such updates.
- **Physical Handling:** Avoid touching the gold contacts or chip directly. If you need to remove or re-install the module, handle it by its edges.
- **Dust Accumulation:** Ensure your computer case is kept clean to prevent excessive dust buildup, which can affect any internal component.

6. Troubleshooting

If you encounter issues with your TPM module, consider the following troubleshooting steps:

Problem	Possible Cause / Solution
TPM not detected in BIOS/OS.	Ensure the module is correctly seated in the TPM header. Verify TPM is enabled in BIOS/UEFI settings. Check motherboard compatibility (DDR3, X99 chipset limitations). Update motherboard BIOS to the latest version.
Windows 11 upgrade fails due to TPM.	Confirm TPM2.0 is enabled and detected (use `tpm.msc`). Ensure Secure Boot is also enabled in BIOS/UEFI.
System instability after installation.	Re-check module seating. Ensure motherboard compatibility. If issues persist, remove the module and test system stability without it.

7. Specifications

Feature	Detail
Model Name	Asrock-TPM
TPM Version	2.0
Pin Configuration	18-1Pin, 2.0mm spacing

Feature	Detail
Compatible RAM Type	DDR4 Motherboards (Not compatible with DDR3 3rd Gen)
Operating System Support	Windows 11 and other modern operating systems supporting TPM2.0
Chip Manufacturer	Infineon
Item Weight	Approximately 15.2 ounces (package weight)
Package Dimensions	5.31 x 5.28 x 5 inches

8. Support

For any questions regarding your Generic Asrock-TPM module, including installation, compatibility, or troubleshooting, please do not hesitate to contact our customer support team.

We aim to respond to all inquiries within 24 hours.

Contact Information: Please refer to your purchase documentation or the seller's contact details on the platform where you purchased the product.

9. Warranty Information

This Generic Asrock-TPM module is covered by a standard manufacturer's warranty against defects in materials and workmanship. The warranty period typically begins from the date of purchase.

For specific warranty terms, conditions, and claim procedures, please retain your proof of purchase and refer to the warranty information provided at the time of purchase or contact the seller directly.

Note: Damage resulting from improper installation, misuse, unauthorized modification, or natural disasters is not covered under warranty.