E22019 / First Edition / May 2023

TPM-SPI-A (14-1 pin)

Quick Start Guide

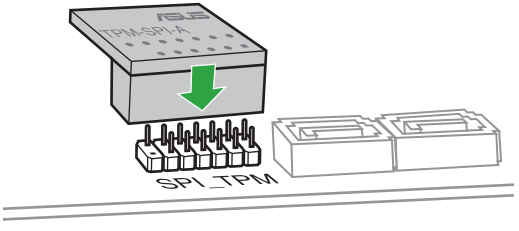
Using the TPM-SPI-A card

The TPM-SPI-A card securely stores keys, digital certificates, passwords, and data. It helps enhance the network security, protects digital identities, and ensures platform integrity.

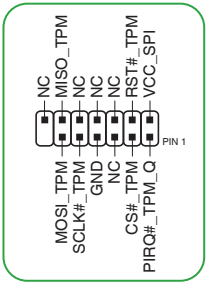
The TPM-SPI-A card supports 64-bit Windows® 10 UEFI OS only.

To use the TPM-SPI-A card:

1. Insert the TPM-SPI-A card to the SPI_TPM connector on your motherboard.



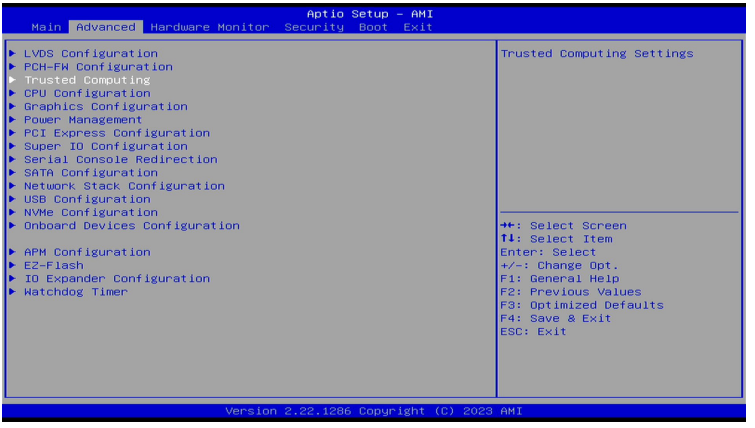
Pin definition:



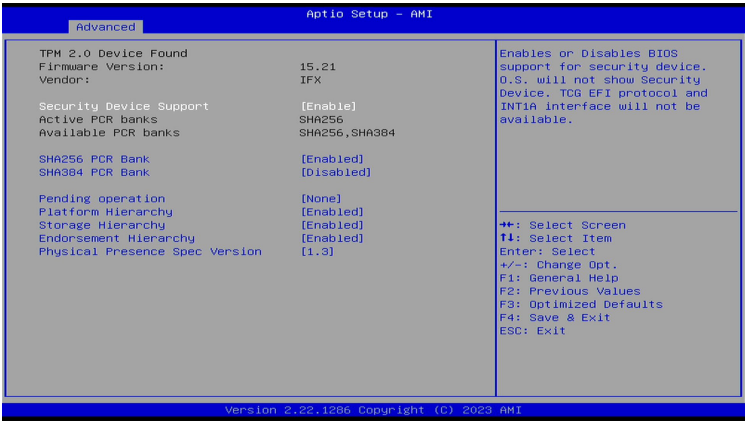
NOTE: The TPM module and BIOS share the same pin layout. The NC signal is used for the TPM-SPI-A, while the BIOS signal is used for the motherboard.

2. Press <**Delete**> or <**F2**> to enter the BIOS Setup program at the system startup.
3. From the Advanced menu, do any of the following:

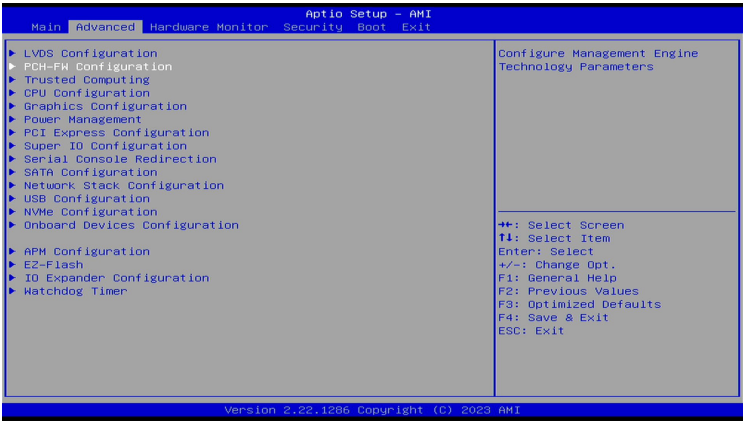
- a) Click **Trusted Computing**.



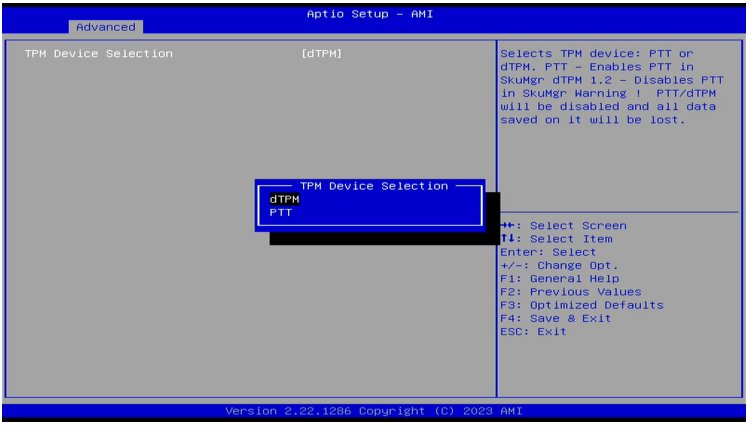
b) Set the **Security Device Support** item to [Enabled].



- a) Click **PCH-FW Configuration**.



b) Set the **TPM Device Selection** item to [**dTPM**].



4. Press <**F10**> to save the changes, exit the BIOS Setup program and boot into the OS.

Now you can start using the TPM-SPI-A card with Windows® BitLocker.

Clearing the TPM security hardware

You can clear the TPM security hardware either from the BIOS or the OS.

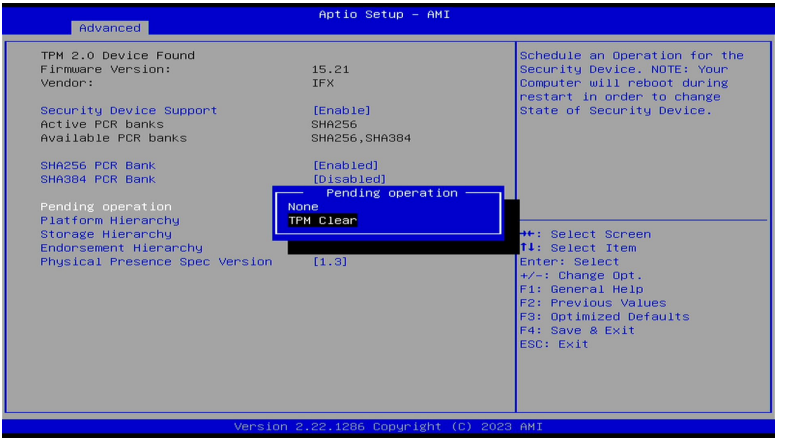
Clearing from the BIOS

To clear from the BIOS:

1. Launch the **Trusted Computing** BIOS screen.

> **NOTE**: For details, refer to steps 2-3 of the section **Using the TPM-SPI-A card**.

2. Set the **Pending operation** item to [**TPM Clear**].

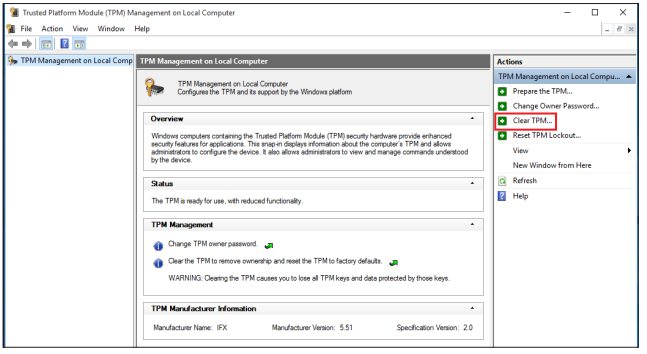


3. Press <**F10**> to save the changes and exit the BIOS Setup program.

Clearing from the OS

To clear from the OS:

1. In the Windows® Search box, key in **tpm.msc** and press <Enter>. The TPM Management screen appears.



2. Under **Actions**, click **Clear TPM...**

3. Click **Restart** to restart your computer.