

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.



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.

Pin definition:

- 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.

Main Advanced Hardware Monitor	Aptio Setup – AMI curity Boot Exit			
 LVDS Configuration PCH-FR Configuration PCU Configuration Graphics Configuration Fouser Management PCI Express Configuration Serial Console Redirection SATA Configuration Network Stack Configuration NVME Configuration Onboard Devices Configuration APM Configuration E2-Flash IO Expander Configuration Watchdog Timer 	Trusted Computing Settings ++: Select Screen T4: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit			
Version 2.22.1286 Copyright (C) 2023 AMI				

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



• a) Click PCH-FW Configuration.



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

Advanced	Aptio Setup – AMI				
TPM Device Selection	(dTPM)	Selects TPM device: PTT or dTPM. PTT - Enables PTT in Skuuggr dTPM 1.2 - Disables PTT in Skuuggr Harning ! PTT/dTPM will be disabled and all data saved on it will be lost.			
	dTPM PTT	++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit			
	Version 2.22.1286 Copyright (C) 2023 AMI				

 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.

Trusted Platform Module (TPM) N	fanagement on Local Computer	- 🗆 ×
🖀 File Action View Window	Help	- 0 ×
🔶 🔿 🔯 🔯		
(中 中) 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日	TPM Management on local Computer Term Term Chilges the TPM and its accord by the Windows platform Overvie Working compares on training the Total of TerMan Modes (TPM) security involves provide wheread security framework applications. The same is designed romanic about the compare / TPM and also applications. The same is designed romanic about the compare / TPM and also applications. The same is designed romanic about the compare / TPM and also applications. The same is designed romanic about the compare / TPM and also applications. The major designed romanic acceleration with the same is a distribution of the compare / TPM and also applications. The major designed romanic acceleration with the same is a distribution of the compare / TPM and also applications. The TPM rest for the same is a distribution of the compare / TPM rest for the same is a distribution of the compare / TPM rest for the same is a distribution of the compare / TPM rest for the same / the TPM is for the same / the top is same / term / ter	Actions TPM Management on Local Comput. Progree the TPM Change Owner Passend Change Owner Passend Change Owner Passend Reat TPM Locked Yew New Window from Hee R dartsM Heig
	TPM Manufacturer Information Manufacturer Version: 551 Specification Version: 2.0	

- 2. Under Actions, click Clear TPM...
- 3. Click **Restart** to restart your computer.

Trusted Platform Module (TPM) M	anagement on Local Computer	- 🗆 X
🖀 File Action View Window	Help	- 8 ×
(+ +) 📅 🖬 📷		
See TPM Management on Local Comp	TPM Management on Local Computer	Actions
		TPM Management on Loca A
	TPM Management on Local Computer Configures the TPM and its support by the Windows platform	Prepare the TPM
	•• • • • • •	Clear TPM
	Overview -	View >
	Windows computers containing a Trusted Platform Module (TPM) provide enhanced security features. This snap-in	New Window from Here
displays information about the computer's TPM and allows administrators to manage the device.		Q Refresh
	Status	🖉 Help
	The TPM is ready for use	
	×	
	A Manage the TDM require backupe	
	Interage the term security network	
	Class the TDM	
	n Clear the TPNT	
	y You must restart your computer to apply necessary configuration changes to the TPM	
	Click the Restart button below.	
	Log on to Windows to continue the wizard automatically.	
	WARNING: Clearing your TPM causes you to lose all TPM Keys. You should only perform this operation if instructed to by your System Administrator.	
< >		
	Restart Cancel	1