

Questo manuale d'istruzione è fornito da trovaprezzi.it. Scopri tutte le offerte per Asus TPM-SPI o cerca il tuo prodotto tra le migliori offerte di Altre Schede



E15028 / First Edition / November 2018

# **TPM-SPI (14-1 pin)** Quick Start Guide

## Using the TPM-SPI card

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

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

#### To use the TPM-SPI card:

1. Insert the TPM-SPI 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, 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, click Trusted Computing.



4. Set the Security Device Support and TPM State items to [Enabled].

TPM20 Device FoundSecurity Device Support[Enable]Active PCR banksSHA-1, SHA256Available PCR banksSHA-1, SHA256SHA-1 PCR Bank[Enabled]SHA256 PCR Bank[Enabled]Pending operation[None]Platform Hierarchy[Enabled]Endorsement Hierarchy[Enabled]FTM2.0 UEFI Spec Version[TCG_2]Fhysical Presence Spec Version[1.3]	Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc. Main Ai Tweaker <mark>Advanced</mark> Monitor Boot Tool Exit				
SHA-1 PCR Bank       [Enabled]         SRA256 FCR Bank       [Enabled]         Pending operation       [None]         Platform Hierarchy       [Enabled]         Storage Hierarchy       [Enabled]         Endorsement Hierarchy       [Enabled]         TPM2.0 UEFI Spec Version       [TCG_2]         Physical Presence Spec Version       [1.3]	TFM20 Device Found Security Device Support Active PCR banks Available PCR banks	[Enable] SHA-1,SHA256 SHA-1,SHA256	Enables or Disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INTIA interface will not be available.		
ShA256 FOR Bank       [Enabled]         Pending operation       [None]         Platform Hierarchy       [Enabled]         Storage Hierarchy       [Enabled]         Endorsement Hierarchy       [Enabled]         TPM2.0 UEFI Spec Version       [TCG_2]         Physical Presence Spec Version       [1.3]	SHA-1 PCR Bank	[Enabled]			
	SHA255 PCK Bank Pending operation Platform Hierarchy Storage Hierarchy Endorsement Hierarchy TPM2.0 UEFI Spec Version Physical Presence Spec Version	[Enabled] [Enabled] [Enabled] [Enabled] [TCG_2] [1.3]	<ul> <li>→-: Select Screen</li> <li>11: Select Item</li> <li>Enter: Select</li> <li>+/-: Change Opt.</li> <li>F1: General Help</li> <li>F2: Previous Values</li> <li>F5: Optimized Defaults</li> <li>F10: Save &amp; Exit</li> <li>ESC: Exit</li> </ul>		

 Press <F10> to save the changes, exit the BIOS Setup program and boot into the OS. Now you can start using the TPM-SPI card with Windows<sup>®</sup> 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 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<sup>®</sup> Search box, key in **tpm.msc** and press <Enter>. The TPM Management screen appears.

Trusted Platform Module (TPM) M	anagement on Local Computer	- 🗆 ×
🖀 File Action View Window	Help	- 0 ×
(+ +) 🔯 🖬 📷		
4a ab 100 E 00	TMM Management on Local Computer         Image: Configure that TMM and its apport by the Windows platform         Overvier         Working compares on contempt the Total of Platform Nodule (TMM) security hardwares provide whereased explorations that the applications. The same is designed formation about the compare of TMM and a submitted in to the and manage command underwood by the device.         Sature       •         TM TMR substitution of functional to the saturation of the compare of TMM and a submitted in to the and manage command underwood by the device.         Sature       •         TM TMR substitution of the compare of TMM and the submitted in to the and manage command underwood by the device.         Image: TMM substitution of the compare of the compare of TMM and the submitted in to the and manage command underwood by the device.         Image: TMM substitution of the compare of the	Actions           TPM Management on Local Comput. •           Progree the TPM           Chang Owner Passed           Chang Owner Passed           Beat TPM Locked           Werk Window from Here           Refer TPM Locked           Help
	TPM Manufacturer Information  Manufacturer Vanion: 5.51 Specification Version: 2.0	

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

Trusted Platform Module (TPM) N	Aanagement on Local Computer	- 🗆 X
File Action View Window	Help	- # ×
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
		<ul> <li>Clear TPM</li> </ul>
	Overview -	View 🕨
	Windows computers containing a Trusted Platform Module (TPM) provide enhanced security features. This snap-in	New Window from Here
	uspays internation about the computers in the and allows durinistrations to manage the device.	Refresh
	Status *	🛛 Help
	The TPM is ready for use.	
0	Manage the TPM security hardware     Clear the TPM     Council retart you compute to apply measure y configuration dampes to the TPM     Security damped and the apply measure y configuration dampes to the TPM     Council retart you computer to apply measure y configuration dampes to the TPM     Council retart you computer to apply measure you have a TPM request, the damped and provide the security and the damped and t	
< >>	Restart Cancel	1