How to program TPM FW on HP Personal Systems

Version: 6

Release Date: 19 October 2017

The instructions below describe how to update the firmware for the TPM (Trusted Platform Module) on selected HP systems. For reference on the SoftPaqs listed below and the HP products supported by these Softpaqs, please see the HP Security Bulletin at the link below:
https://support.hp.com/us-en/document/c05792935

WARNING! HP strongly recommends backing up all data before performing this procedure. Errors or mistakes during the process can render the hard drive inaccessible and can result in loss of data stored on the hard drive. HP is not responsible for loss of data that might occur during the procedure.

Preparing your system

- If BitLocker Drive Encryption is used on your system, make sure before performing the update, that you know the BitLocker recovery password or you have the recovery key on a USB flash drive
- Verify admin privileges
- Verify that the TPM is visible and not hidden by F10 BIOS Setup (BIOS Admin password may be needed to make the TPM visible if it has been hidden)
- Verify that the TPM is enabled and the TPM owner is set
- Verify that you have an Infineon TPM
- Verify that you are vulnerable by checking that you do not have the fixed FW versions as listed in the security bulletin: https://support.hp.com/us-en/document/c05792935
- Verify the following F1 BIOS Setup features are turned off (if enabled this may require BIOS Admin Password to disable as well as a reboot to complete the disablement)
    - TXT
    - VT-x
    - SGX
- Verify that Bitlocker or other drive encryption software that depends on the TPM is disabled (i.e., drive is decrypted) or suspended, depending on the SW vendor's recommendations.
- Backup any data on the drive and ensure that the TPM keys are backed up
- Verify that TPM FW Update is not prohibited by group policy settings
- Verify that AC power is present (i.e., avoid any accidental power loss or suspend/hibernate in the middle of the update)
- Determine the appropriate Softpaq for your platform and install it

Updating the FW

For HP TPM Configuration Tool:

Create a folder and put the TPMConfig64.exe and the **desired** firmware into the folder. Launch executable. There is a PPI (Physical Presence Interface) key press required after reboot.

For further instructions and details, please see the pdf file that is downloaded with the Softpaq.

For Infineon TPM FW update tool:

The firmware upgrade for older TPM (SLB9665, SLB9660) uses a tool from Infineon. You should verify the TPM is active and run the executable. It will respond with:

1. Run TPM Upgrade after accepting warning.
2. Say TPM has already upgraded.
3. Say TPM is not supported.

For further instructions and details, please see the HTML readme file that is downloaded with the SoftPaq.

FAQs

Physical Presence

1. Is physical presence required for FW update? Can this change be accomplished via SCCM?
    - For most systems, there needs to be a physical presence for the Infineon firmware update. This may be run as an SCCM task / scripted task, but it still requires a physical presence. HP User tool and Infineon user tool are both capable of silent install.
    - The physical presence consists of pressing a key to acknowledge the Infineon TPM firmware change.

2. Does secure boot need to be disabled prior to patching?
    - Please reference Microsoft's Security Advisory, which does not specify additional steps to disable Secure Boot.

Deployment

1. Does the Bitlocker drive need to be decrypted prior to applying the patch? Or can Bitlocker just be suspended?
    - The firmware update tool requires Bitlocker to be either decrypted or suspended.

2. Does both the MS patch and the Infineon softpaq need to be installed?
    - Please reference Microsoft's Security Advisory. Microsoft recommends installing the MS patch first, so that TPM.MSC can identify the security level of the current TPM firmware. After applying the patch, TPM.MSC can inform the user if the TPM firmware is vulnerable and requires an update.

3. What is the best way to verify that users are secure once the patch has been applied? Where and which version numbers should be verified?
    - Please reference Microsoft's Security Advisory. Microsoft recommends installing the MS patch first, so that TPM.MSC can identify the security level of the current TPM

firmware. After applying the patch, TPM.MSC can inform the user that they are secure, based on the Infineon TPM firmware revision.
- Please also reference HP's Security Bulletin for the updated TPM firmware versions for each HP platform.

4. Will this patch follow a WSUS procedure or need to be distributed as a package?
    - WSUS will not be supported. The Softpaqs are not SSM compliant.

5. Will this be integrated with the MIK TPM firmware upgrade/downgrade tool?
    - This will work as any other upgrade.

6. Can this be run as SCCM task? Or a scripted task?
    - This can be run as either an SCCM task or a scripted task. Please see documentation on relevant Softpaq.

General

1. Is this a f/w update to the TPM? If not, what changes?
    - Please reference the Infineon site. This is an Infineon TPM firmware update.