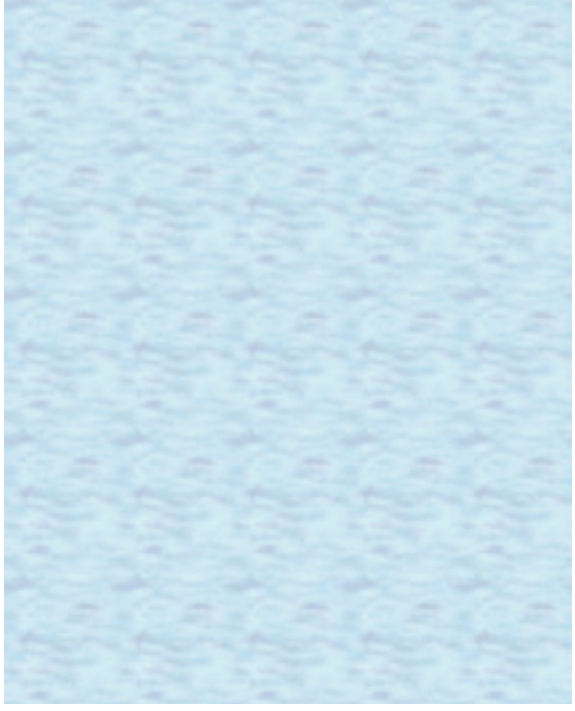
Panasonic®

Installation Manual

Trusted Platform Module (TPM)



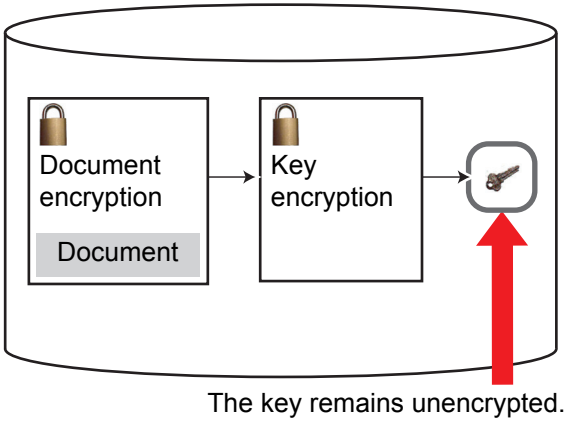
We recommend that this Installation Manual be printed.

TPM's Outline

The conventional security measures such as file encryption and public key encryption save the encryption keys in the computer's hard disk drive. Therefore the keys and passwords as well as the encrypted data are exposed to the risk of unauthorized copying and hacking.
The TPM method saves the encryption keys in the TPM chip that is separated from the hard disk drive and CPU. To access the encryption keys, you need to input the password registered in the Security Platform (➔ page 8). You can apply a different security setting to each user account in the Security Platform.

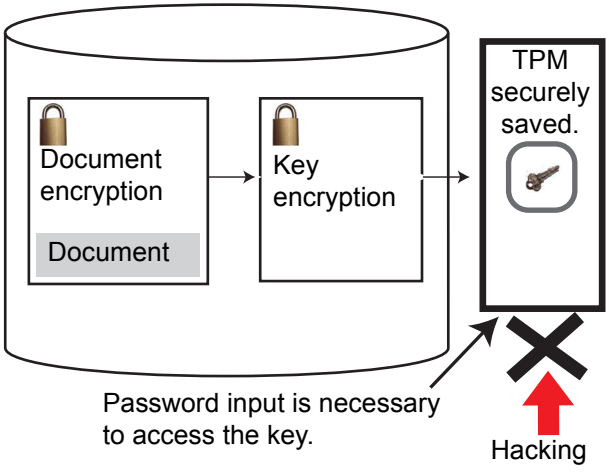
Conventional encryption

The encryption key is saved as a file in the hard disk drive.



TPM encryption

The encryption key is saved in the TPM chip.



Security Functions

- The TPM method does not guarantee data protection under all conditions.
- The TPM method uses multiple encryption keys, certificates and passwords. You cannot decrypt the encrypted data if you lose them. Safely keep the keys, certificates and passwords. (See “Backup” below.)
- We shall not be liable for any loss or damage whatsoever resulting from your TPM use or your neglect of TPM use, or any data loss resulting from such developments as TPM malfunctioning.
- Personal Secure Drive function is not supported with Fast User Switching function enabled environment. Disable Fast User Switching function when you use the Personal Secure Drive function.

Backup

The files described below are necessary for recovering the Security Platform function. Back them up periodically in a safe location such as removable disk to avoid data loss resulting from TPM malfunctioning or other accidents. We recommend you to store the files in removable disk or network drive because the benefit of TPM security can be reduced if you keep the files in the internal hard disk drive.

NOTE

- In the default setting, the “System Backup Archive”, “System Backup Folder”, “Emergency Recovery Token”, “Password Reset Token”, and “Personal Secret File for Password Reset” are stored in “C:\Documents and Settings\(user account)\My Documents\Security Platform”. If a removable disk is connected, the files excluding the System Backup Archive and the System Backup Folder are automatically stored in the removable disk by priority.

- Files and folder used by the Computer Administrator
  - **System Backup Archive**
    (Default name: SPSystemBackup.xml)
    System Backup Folder
    (Default name: SPSystemBackup)
    You need the file and folder when you replace the embedded TPM chip or the hard disk drive, or reinstall Windows. The file and folder contain the backup of the emergency recovery data, and the keys, certificates and settings of all users.
    If you make the setting of routine backup, the backup of each user setting will be automatically saved at the scheduled interval. To ensure the latest backup, manually backup every time you create or change the user setting.
    For further information, refer to “How to Backup and Restore”-“How to configure automatic backups (“System Backup”)” in the Infineon Security Platform Help menu. (Click [start] - [All Programs] - [Infineon Security Platform Solution] - [Help on Security Platform] - [Welcome to the Infineon Security Platform Solution] - [Advanced Security Platform Operation] - [Backup and Restore Security Platform Data])

- **Emergency Recovery Token**
  (Default name: SPEmRecToken.xml)
  You need this file when you replace the embedded TPM chip.
  Use the file for recovery using the emergency recovery data. (The emergency recovery data is contained in the System Backup Archive and System Backup Folder, and protected by this file.)
- **Password Reset Token**
  (Default name: SPPwdResetToken.xml)
  You need this file to create the Reset Authorization Code that is required to reset a specific user's password.
  You cannot reset the password without this token.

- File used by each User
  - **Personal Secret File for Password Reset**
    (Default name: SPPwdResetSecret.xml)
    You use this file in combination with the Password Reset Token to reset the Basic User Password.

Cautions for Encryption

- Do not encrypt the files described in "Backup" (➔ page 3). If you encrypt them, you will not be able to restore the Security Platform settings. In the default setting, these files are stored in "C:\Documents and Settings". Do not encrypt "C:\Documents and Settings".
- Do not encrypt the files in "C:\Program Files" because they contain a lot of application software. If you encrypt them, other users cannot access the software, and the software may not start up or other malfunction may occur.
  Note that encrypting other files such as "C:\" may also cause similar problems.
- Do not encrypt the "Security Platform" folder as well as any file/folder contained in it. This folder is created under the drive (default setting: "C:\") which you specified while setting up the Personal Secure Drive. Because the Security Platform refers to this folder, encrypting it may disable the Personal Secure Drive.

Installing TPM

Performed by the Computer Administrator

Step 1	Step 2	Step 3
Changing the Setup Utility Settings ● Supervisor Password ● Setting the Embedded Security (TPM)	**Installing the Security Platform**	**Initializing the Security Platform** ● Owner's Data • Owner Password • System Backup Archive • System Backup Folder • Password Reset Token • Password Reset Token Password ● Data for emergency use • Emergency Recovery Token • Emergency Recovery Token Password

Performed by each user

Step 4
Initializing the user ● User's Data • Basic User Password • Personal Secret

This manual describes about Steps 1, 2 and the initial part of Step 3.
For further steps, refer to (➔ page 8 "Step 3 Initializing the Security Platform") and the Infineon Security Platform Help menu.
(Click [start] - [All Programs] - [Infineon Security Platform Solution] - [Help on Security Platform].)

Step 1 Changing the Setup Utility Settings

Performed by the Computer Administrator.

1 Register the Supervisor Password.

You have to register the Supervisor Password to proceed to the next step.

① Turn on or restart the computer.

② Press **F2** while [Panasonic] boot screen is displayed soon after the computer starts the startup procedure.
The Setup Utility starts up.

③ Select the [Security] menu.

④ Select [Set Supervisor Password] and press **Enter**.

⑤ Enter your password in the [Enter New Password] and press **Enter**.

- The password will not be displayed on the screen.
- You can use up to 32 alphanumeric characters (including spaces).
- The case (upper/lower) is ignored.
- To input numbers for the password, use the numbered keys on the keyboard.
- You cannot use **Shift** and **Ctrl** to input a password.

⑥ Enter your password again in [Confirm New Password] and press **Enter**.

⑦ In [Setup Notice], press **Enter**.

2 Enable the Embedded Security (TPM).

① Select [Embedded Security (TPM) Sub-Menu] and press **Enter**.

② Select [Embedded Security Chip (TPM)], and set to [Enable].
At the confirmation message, press **Enter**.

③ Press **Esc** to close the sub-menu.

④ Press **F10**, select [Yes] and press **Enter** to exit the Setup Utility.

NOTE

- The default setting of [Sub-Menu Protection] is [Protected]. If you select [No Protection], an user with only an User Password can enter [Embedded Security (TPM) Sub-Menu] and change the settings including [Clear Owner settings] (➔ page 9). Take special care when you change the default setting.

Step 2 Installing the Security Platform

Performed by the Computer and Windows Administrator.

1. **Log on to Windows as an Administrator.**
2. **Close all programs.**
3. **Click [start] - [Run], enter [C:\util\drivers\tpm\infineon\setup.exe], and click [OK].**
   The [InstallShield Wizard] screen appears.
4. **Click [Next].**
5. **Carefully read the License Agreement. Select “I accept the terms of the license agreement”, and click [Next].**
   Installation starts. Follow the on-screen instructions.
6. **When the message [InstallShield Wizard completed] appears, click [Finish].**
   When readme is displayed, read carefully and close it.
   The computer restarts.
7. **Log on to Windows as an Administrator.**

   The “Security Platform Indicator Icon”  appears in the notification area.

Step 3 Initializing the Security Platform

The “Security Platform is not initialized.” message is displayed by the “Security Platform Indicator Icon”  in the notification area.

1 Click on “Security Platform is not initialized.” message to start the “Infineon Security Platform Initialization Wizard”.

Follow the on-screen instructions.

- For further information, refer to the Infineon Security Platform Help menu. (Click [start] - [All Programs] - [Infineon Security Platform Solution] - [Help on Security Platform] - [Welcome to the Infineon Security Platform Solution] - [The Security Platform Solution Tools] - [Security Platform Initialization Wizard].)

CAUTION

- Do not forget or delete any of the passwords and files. If you lose them, administration or recovery of the Security Platform becomes impossible. Keep the passwords and files safe.

After completing the above procedure, initialize each user.

NOTE

- Creating the Personal Secure Drive will take 1-2 minutes in the capacity of 1GB. Wait until the process is completed.

Initializing Owner's Data

When you dispose the computer or transfer the ownership, initialize the owner's data to avoid the TPM-encrypted data from being decrypted by unauthorized person.

1. **Start the Setup Utility (➔ page 6).**
2. **Select the [Security] menu, and select [Embedded Security (TPM) Sub-Menu] and press Enter.**
   - When you cannot enter [Embedded Security (TPM) Sub-Menu] using the User Password, ask the administrator for the Supervisor Password.
   - You cannot enter [Embedded Security (TPM) Sub-Menu] if the Supervisor Password has not been registered.
3. **Select [Embedded Security Chip (TPM)] and set to [Disable].**
   - At the confirmation message, press **Enter**.
4. **Select [Clear Owner settings] and press Enter.**
   - Carefully read the setup confirmation.
5. **Select [Execute] and press Enter.**
6. **Select [Execute] and press Enter.**
   The computer restarts automatically.

You will not be able to use the TPM-encrypted data after this procedure, but it will still remain on the hard disk drive. Erase this data and all internal data using the Hard Disk Data Erase Utility.
For further information, refer to the Operating Instructions of this computer.

Can I Uninstall the Security Platform?

- Yes, you can.
  Click [start] - [Control Panel] - [Add or Remove Programs] and delete the [Infineon TPM Professional Package]. Before uninstalling the Security Platform, back up or decrypt the files encrypted in the Security Platform. If you do not back up or decrypt the files, you will not be able to access them after uninstallation.
  Note that even after uninstallation, a part of the data will remain in the computer.
  For further information, click [start] - [All Programs] - [Infineon Security Platform Solution] - [Help on Security Platform] - [Welcome to the Infineon Security Platform Solution] - [Frequently Asked Questions and Troubleshooting] - [Frequently Asked Questions (FAQ)].

I Cannot Encrypt Files. What Should I Do?

- The hard disk drive should be formatted in the NTFS volume. If [NTFS] is displayed in [File system], you can encrypt the files. To check the status, click [start] - [My Computer], right-click [Local Disk (C:)] and click [Properties].

The [C:\Documents and Settings] Folder Was Encrypted by Mistake. Can I Decrypt It?

- You can decrypt the folder, but the data may not be restored completely. To decrypt the folder, you must log on as the user who encrypted it. Logging on as other user may cause such troubles as hang-ups during Windows logon and irregular displays of file icon.
  ① Log on as the user who encrypted the folder. (If may take some time to start up the computer.)
  If the Basic User Password is requested, enter the password.
  ② Click [start] - [My Computer] - [Local Disk (C:)], right-click the [Documents and Settings] and click [Decrypt].
  ③ Click [Confirm Attribute Changes] - [Apply changes to this folder, subfolders and files] - [OK].
    - If an error message appears, click [Ignore] or [Ignore all].
    - If the Basic User Password is requested, enter the password.

What Should I Do When I Received the Repaired Computer?

- Perform “Step 1 Changing the Setup Utility Settings” (➔ page 6), and follow the Security Platform Help menu to restore the Security Platform settings.

PCE0181H_XP