TOSHIBA

TPM

(Trusted Platform Module)

Installation Guide V2.1

Table of contents

Copyright

Trademarks

1 Introduction

Your computer has an integrated Trusted Platform Module (TPM). To activate TPM, you will need to either enable it or install the Infineon Security Platform Tools software. This installation guide describes how to install and configure TPM. Before using TPM, please read this Installation Guide carefully.

1.1 Convention

This guide uses the following formats to describe, identify, and highlight terms and operating procedures.

Safety Icons

This guide contains safety instructions that must be observed in order to avoid potential hazards that could result in personal injuries, damage to your equipment, or loss of data. These safety cautions have been classified according to the seriousness of the risk, and the icons highlight these instructions as follows:

⚠ DANGER	*Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.*
⚠ WARNING	*Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.*
⚠ CAUTION	*Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.*
CAUTION	*Indicates a potentially hazardous situation which, if not avoided, may result in property damage.*
NOTE	*Provides important information.*

1.2 TPM - An Overview

The built-in security controller TPM based on the Trusted Computing Group specifications. TPM offers data protection by using secret encryption keys instead of secret encryption formulae (Algorithms). In encryption based solely on software, there is a danger that the encryption key saved in the file or read into the PC's memory could be read and deciphered. By storing the encryption key in TPM instead, the data is more securely protected.

As TPM uses public and standardized specifications, a more secure PC environment can be built by utilizing the corresponding security solution.

For additional TCG specification information visit their website at http://www.trustedcomputinggroup.org/

CAUTION

Encryption, Certificates and Passwords

- *TPM offers a feature to create and set multiple encryption keys, certificates and passwords. Once set, make sure the passwords are carefully stored and encryption key files are backed up. If these settings are lost or forgotten, files encrypted using this TPM cannot be decrypted and the encrypted data cannot be accessed.*

TPM

- *Though TPM offers the latest security features, it does not guarantee complete data and hardware protection. Please note that Toshiba is not responsible for any failure or damage that might be caused due to the use of this feature.*

NOTE

If multiple users have been registered in Microsoft® Windows® and if these users are to use TPM, each user must log into Windows® and register individually.

2 Using TPM for the first time

This manual contains only the general guidelines. Please refer to and read the TPM HELP after installing the TPM Professional Package.

When using TPM for the first time, you will need to configure it as follows. (The settings 1 - 3 can be done by logging in as *Windows*® administrator.)

1. Enable TPM.
2. Install the **Infineon TPM Professional Package**.
3. Register the owner and users in TPM.

2.1 Enabling TPM

To enable TPM, perform the following BIOS settings:

1. Switch on your computer while pressing the **Esc** key.
2. A message is displayed. Press the **F1** key.
3. The BIOS Setup screen is displayed.
4. Press **Page Down** to see the next screen.
5. Set the **TPM** in **SECURITY CONTROLLER** to **Enabled**.

NOTE

Some models may have **Hide TPM** *as an option on the BIOS setup screen. If your system shows* **Hide TPM**, *it should be set to* **No** *before you set* **TPM** *to* **Enabled**. *Otherwise, you will not be able to change* **TPM**.

6. Press the **End** key, save the changes to the BIOS settings and press **Y** key.

CAUTION

Internal data consistency in TPM is not guaranteed when the computer is sent for repair or maintenance. Before sending the computer for repair or maintenance, please make a backup of not only the files in the HDD (Hard Disk Drive), but also the TPM data by using the backup feature. (Refer to Chapter 8 - Recovery for TPM*.) The security functions that use TPM can no longer work properly if the data in TPM is lost. (Example: Files that were encrypted using TPM can no longer be opened.) Failure to do so may result in possible data loss.*

NOTE

- **TPM** *is shipped with the* **Disabled** *setting by default Also, there might be cases where the* **TPM** *is set to* **Disabled** *after the computer has been sent for repair or maintenance. Please enable TPM by reconfiguring it again.*
- *To prevent anybody other than the administrator and users of this computer from changing the BIOS settings, it is strongly recommended that you set a BIOS password and a BIOS supervisor password. Please refer to the Computer User's guide on how to set these passwords.*

2.2 Installing the Infineon TPM Professional Package

Install the **Infineon TPM Professional Package** from the TOSHIBA Application Installer. Please refer to the User's Manual on details about the TOSHIBA Application Installer.

The **Infineon TPM Professional Package** includes the following software and features:

- Security Platform Getting Help
- Security Platform Settings Tool
- Security Platform Initialization Wizard
- Security Platform User Initialization Wizard
- Security Platform Migration Wizard
- Security Platform Backup Wizard
- Security Platform Password Reset Wizard
- Security Platform PKCS #12 Import Wizard
- Security Platform Certificate viewer and Certificate Selection
- Security Platform Status Indicator Applet
- Security Platform Integration Services
  - Microsoft© Outlook© Integration
  - Netscape© Integration
  - Encrypted File System Integration
  - Personal Secure Drive
  - Policy Administration
- Security Platform Services
  - TSS (TCG Software Stack) Service Provider
  - TSS Core Service
  - TSS Device Driver Library

2.3 Registering Owners and Users in TPM

1. Click the **Security Platform** icon in the task tray and select **Security Platform Initialization**.

2. TPM starts up and its screen is displayed. Click the **Next** button.
3. In the **Initialization** screen, select Initialize a new Security Platform. And click the **Next** button.

4. In the **Create Security Platform Owner** screen for owner authentication, enter the password in the **Password** and **Confirm Password** text boxes and click the **Next** button.
5. The **Features** screen will be displayed. Select the Security Platform function to set and click the **Next** button. Refer to Help for more details on the Security Platform functions.

CAUTION

Setting **Automatic Backup** *is strongly recommended. If it is not set, encrypted user data might be lost if it is abnormal.*

6. In the **Backup** screen, specify the location for creating and saving the backup file. Click the **Next** button.
7. In the **Emergency Recovery** screen, select the **Create a new Recovery Token** and specify the location for creating and saving the **Emergency Recovery Token**.
8. In the **Emergency Recovery** screen for **Emergency Recovery Token** authentication, enter the password in the Password and Confirm Password text boxes and click the **Next** button.

CAUTION

It is strongly recommended that you create an emergency recovery token is created so that information in TPM and user data related to TPM is safe in the event that severe system troubles occur. Failure to follow this recommendation could possibly result in data loss.

9. In the **Password Reset** screen, select the **Create a new Token** and specify the location for creating and saving the **Password Reset Token**.
10. In the **Password Reset** screen for **Password Reset Token** authentication, enter the password in the Password and Confirm Password text boxes and click the **Next** button.

NOTE

It is strongly recommended that you create and save the **Password Reset Token** *on a storage medium such as a floppy disk that is accessible even in the event of a computer failure. Be sure to store the disk in a safe location for possible future use.*

- If there are multiple computers with TPM, the token for each computer is different and should be stored separately.
- The recovery token for the registered TPM owner* cannot be recreated. In order to prevent loss, multiple copies of the token should be created and stored, as recommended in the note above.

  *The same TPM owner name can be created by initializing TPM at the BIOS menu and registering a new owner, however, as the owner is actually different from the previously registered owner in this case, previously encrypted files cannot be decrypted.
- If the token is leaked to or stolen by third parties together with the password, they would be able to access the encrypted data. Therefore, it is strongly advised that the tokens and passwords are stored carefully.

11. The **Summary** is displayed. Check the summary and click the **Next** button.
12. It may take a few minutes before the **Wizard completed successfully** message is displayed. Next, click the **Start Security Platform User Initialization Wizard** checkbox and then click the **Finish** button.
13. In the **User Initialization Wizard** screen, click the **Next** button.
14. In the **Basic User Key Password** screen for user authentication, enter the password in the **Password** and **Confirm Password** text boxes and click the **Next** button.
15. In the **Basic User Password Reset** screen, ensure that **Enable the resetting of my Basic User Password in case of an emergency** has been selected. Specify the location for creating and saving the **Personal Secret** file.

NOTE *Please store this file in a safe location. In times of need, it would be required to reset the Basic User Password.*

16. The **Password and Authentication** screen will be displayed. Confirm the displayed content and click the **Next** button.

NOTE *It might take several minutes for the Security Platform Features screen to be displayed.*

17. Ensure that the desired features are selected in the **Security Platform Features** screen and click the **Next** button.

NOTE

- *To use* **Secure E-mail**, *it is necessary to set the configuration in the* **Mail Software**. *Refer to Chapter 4 -* Secure E-Mail *for details on Secure E-mail.*
- *The* **File and Folder encryption (EFS)** *feature is not available in the Windows® XP Home edition.*
- *The HDD (Hard Disk Drive) must be formatted in NTFS format to use the* **File and Folder encryption (EFS)** *feature.*

The configurations set in this section can also be modified after configuration.

18. If **Secure E-mail** is selected in the **Security Platform Features** screen, the following screen is displayed. Click the **Next** button.

NOTE *If any of the* **Outlook**, **Outlook Express** *or* **Netscape** *buttons are clicked on the screen, the help for the* **Secure E-mail** *settings for the respective* **Mail Software** *is displayed. (It is possible to see this help even after the wizard is closed.)*

19. The **Encryption Certificate** issuance message would be displayed in the Security Platform Features screen. Select the certificate to issue and click the **Next** button. Normally, click on the **Create** button to create and select the certificate.

20. If **Personal Secure Drive (PSD)** is selected in the **Security Platform Features** screen, the following screen is displayed. On this screen, select the drive you wish to allocate to PSD, then enter the label name of that drive and click the **Next** button. Refer to Chapter 3 - *Personal Secure Drive* for details on Personal Secure Drive (PSD).
21. In the **Security Platform Features** screen, enter the volume of storage space you wish to allocate for PSD, then select the drive and click the **Next** button.
22. The Confirm setting is displayed, click the **Next** button.

NOTE

- *It is strongly recommended that you specify a built-in HDD (Hard Disk Drive) (normally C drive) in the* **My Personal Secure Drive will be saved on this drive** *pull-down menu.*
- *The space available in the drive specified above should be more than the space specified in* **My Personal Secure Drive will have [XX] MB of storage space***.*

23. After some time, the **Wizard completed** message will be displayed. Click the **Finish** Button.

NOTE

If multiple users have been registered in Windows® and if these users are to use TPM, each user must log into Windows® and register individually. After logging into Windows® to perform user registration, click the **Security Platform** *icon in the task tray and select* **Security Platform User initialization***.*

When modifying the configuration, click on the **Security Platform Setting Tool** icon in the task tray and do the modifications in the configuration screen.

3 Personal Secure Drive

The **Personal Secure Drive** creates data storage for storing the information (files) and data files can be encrypted and saved in the virtual drive. The files are not simply encrypted and stored in the HDD. As they are protected by TPM, the level of safety is higher than existing software-based encryption. The PSD size can't be specified less than 10MB.

3.1 Advantages of Personal Secure Drive

- Encryption of the virtual drive using the safe and secure AES (Advanced Encryption Standard) key.
- RSA algorithm for encrypted key generation.
- Automatic encryption and decryption of transparent security data.
- Files can be easily protected.
- Simple Operation: Personal Secure Drive functions in the same way as a standard *Windows*® drive.
- Easy management and setup procedure using Wizards.

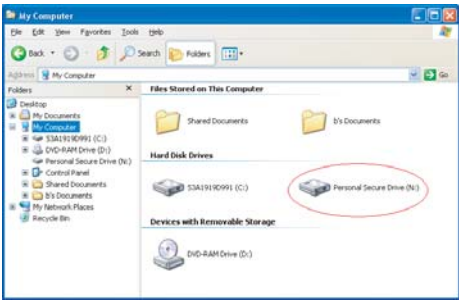
3.2 Personal Secure Drive (PSD) - Basic Operation

1. If PSD is selected in **Security Platform Futures**, click on the **Security Platform** icon in the task tray after logging in to Windows and select **[Personal Secure Drive]** - **[Load]**.

NOTE *Clicking on the **Security Platform** icon in the task tray allows selection of* **[Personal Secure Drive]** - **[Load]**, **[Unload]** *or* **[Load at Logon]**.

2. Infineon Security Platform User Authentication would be displayed. Enter the TPM password. The PSD virtual drive will be recognized once the correct password is entered.

3. The following is a sample screen showing the PSD detected in *Windows®* explorer.



In this screen, although the Personal Secure Drive has been detected as Drive **[N:]** with a drive name of **Personal Secure Drive**, it is possible to change this setting in the **User Settings** of the **Infineon Security Platform Settings Tool**.

CAUTION

- *As files in the PSD are not backed up using the* **Backup** feature of the **Infineon Security Platform Settings** *Tool, general backup methods such as copying the files in the PSD to an external, removable medium in the explorer should be used to avoid possible data loss.*
- *The data for the system restore point* set by the Windows® System Restore function is deleted after the TPM password is entered during Windows startup, the PSD is mounted and the virtual drive is assigned. It is strongly recommended to use either of the following methods to save the system restore point data.*
  - *Do not use the PSD function and use only the file encryption function via the EFS.*
  - *Temporarily disable the PSD function just before modifying the Windows environment.*

  Disable the PSD function -> Set the Restore Point -> Modify the system -> Check that Windows starts up properly -> Set the PSD function back to its previous state.

  ** Please refer to Windows® Help for details on the restore point.*

NOTE

The PSD needs to be set for each TPM user. For example, if there are two registered TPM users 'A' and 'B', B cannot see the PSD contents of A.

4 Secure E-Mail

In this security platform, the Digital IDs used for E-mail are protected by TPM, securing them from loss or theft.

Compatible E-mail software includes Outlook*, Outlook Express* and Netscape*.

* Note that this function may not be usable depending on the version of the software.

Configuration

1. Acquire a Digital ID for use in Secure E-Mail from the Commercial Certificate Authority (CA). Refer to TPM Help for details on CA.
2. Install the Digital ID to the computer based on the usage and installation methods specified by CA. At this stage, ensure that the Digital ID is linked to TPM as a Cryptographic Service Provider (CSP).
3. Set the configuration for Secure E-Mail in the E-mail software. Refer to the manual for each E-mail software and the help for the Infineon Security Platform for details.

NOTE

Set the **Secure E-mail** *setting in the Security Platform Features when carrying out user registration to TPM (Step 2.3) if it was not assigned (*1, *2).*

*1 Using Help to look up information related to E-mail and TPM

1. Double-click the **TPM** icon in the task tray.
2. Select the **Info** tab.
3. Click the **Help** button.
4. Search using keywords under the **Search** tab for items you wish to find out more about. (Example: **E-Mail**)

*2 Enabling the E-mail function in User Settings

1. Double-click the **TPM** icon in the task tray.
2. Select the **User Settings** tab.
3. Click the **Configure** button.
4. Check the **Secure E-mail** option and click the **Next** button.

5 EFS (Encrypting File System) Extension

If the File and Folder **encryption** option is checked in Step 2.3, the EFS function of the OS is extended and the system is made more secure as the encrypted key for the file encrypted by EFS is protected by TPM.

The operations required for encrypting/decrypting the files are very similar.

The difference in operation is that when files encrypted by EFS are initially accessed after logging on to *Windows*®, the TPM password of the current logon user must be entered.

CAUTION

- *Please do not specify C:\Documents and Settings and use EFS to encrypt all the folders and files under it.*
- *Do not use EFS to encrypt if the token file or backup file created during owner or user registration is stored in "C:". If encrypted, the decryption process might not work.*
- *When using file encryption by EFS, it is strongly recommended that the user become familiar with the EFS-related information in Windows® Help. This will help prevent files from not being able to be decrypted due to unknowingly changing the encryption key used in EFS or due to the loss of the key.*

6 TOSHIBA Password Utility

By using the TOSHIBA Password Utility, the configuration can be set to prevent users without Supervisor authority from changing TPM-related settings in the BIOS setup.

Once this configuration is set, users without Supervisor authority will not be able to change TPM-related settings in the BIOS setup (items in the **Security Controller** box).

1. Run the following file to start TOSHIBA Password Utility.

   C:\Program Files\Toshiba\Windows Utilites\SvpwTool\TOSPU.exe

2. Register the Supervisor Password in the **Supervisor Password** tab.
3. Open the User Policy setup screen from the **Supervisor Password** tab.
4. In the **TPM** box, uncheck the items that you do not want users without Supervisor authority to access and modify.
5. Press the **Set** button, and after carrying out Supervisor authentication, save the modified User Policy.
6. Exit TOSHIBA Password Utility.

7 Migration of the TPM Environment and Disposal

7.1 Migration

Click the **Security Platform** icon in the task tray and select **Manage Security Platform**. In the **Infineon Security Platform Settings Tool** window, click the **Migration** tab. In the **Migration** tab, clicking the **Learn more...** button displays the details of the migration operation. (The operation must be performed for both the source platform and the destination platform.) Please perform the operation as per the instructions on the screen.

CAUTION

Only the TPM data is migrated during this process, so perform the migration of the data inside the Personal Security Drive and the files encrypted with EFS using the usual file operations.

NOTE

- *Remember, it is necessary to also install the* **Infineon TPM Professional Package** *in the destination platform.*
- *Migration between the PCs via a network cannot be done when using Windows® Firewall under the Windows® XP-SP2 environment. Please use a FD or other external removable media for migration.*

7.2 PC Disposal

When discarding the PC, please perform the following two processes in order to prevent any leak in confidential information. Please do the same when changing the PC owner too.

1. Uninstall the **Infineon TPM Professional Package** and delete the recovery archive and the **Emergency Recovery Archive Token**. Furthermore, please delete all the data in the HDD (Hard Disk Drive).
2. Step:1 Display the **BIOS Setup** screen.
   (Refer to Chapter 2 - *Using TPM for the first time*.)

   Step:2 Move the cursor to the **Clear TPM Owner** option in the **SECURITY CONTROLLER** setting and press the spacebar or backspace key. With this operation, all the data inside TPM is destroyed and TPM is disabled thereafter.

   Step:3 A message is displayed. Press **Y**, **E**, **S** keys followed by the **Enter** key.

NOTE

As the internal TPM data is deleted, the files can no longer be read.

8 Recovery for TPM

8.1 Emergency Recovery Process - An Overview

The Emergency Recovery Process is used:

- when changing TPM due to TPM problems.
- when the motherboard with the onboard TPM has a defect and the motherboard was changed.
- when TPM was cleared either accidentally or due to some other reasons.

Refer to *Restore Emergency Recovery Data Step by Step* in Help for details.

NOTE

- *Printing out a hardcopy of Restore Emergency Recovery Data Step by Step in Help beforehand is recommended.*
- *The explanations stated here are for the recovery of TPM content and not for the recovery of TPM-related data such as EFS encrypted files or files in the PSD. For files in the built-in HDD, it is strongly recommended that backups are separately created and safely stored.*

8.2 Resetting the User Password

This function can be used if the Infineon Security Platform user forgets the basic User Password or if there is a problem with the user's authentication device. If the password cannot be reset, the user cannot use the functions in the Security Platform. This might result in loss of secret data.

Refer to *Basic User Password Reset* in Help for details.

8.3 PSD restore

PSD data can be recovered if the PSD certificate is lost using Personal Secure Drive Recovery.

Refer to *Personal Secure Drive Recovery* for details.

Index

R

S

T

U

W

Memo

Please ensure that the passwords or keywords used are stored carefully (in case the passwords are forgotten) where third parties cannot access (to prevent leakage of secret information). Do not store in locations which are accessible by unauthorized personnel (Example: pasted onto tabletops).

Owner Password:

Basic User Password:

Storage Location of the Emergency Recovery Token:

Emergency Recovery Token Password:

Storage Location of the Backup file:

Storage Location of the Password Reset Token:

Password Reset Token Password:

Storage Location of the Personal Secret file:

TPM User Password

Windows® User Name:

TPM User Password:

Windows® User Name:

TPM User Password:

Windows® User Name:

TPM User Password: