Smart TPM

User's Manual

Rev. 1001
12MD-STPM-1001R

- We recommend that you download the latest version of the Smart TPM utility from GIGABYTE's website.
- If you have installed Ultra TPM earlier, you can install the Smart TPM utility directly without uninstalling Ultra TPM first. The original settings in Ultra TPM will be kept.

Table of Contents

TPM Configuration Procedure

To enable the TPM, follow the steps below in sequence:

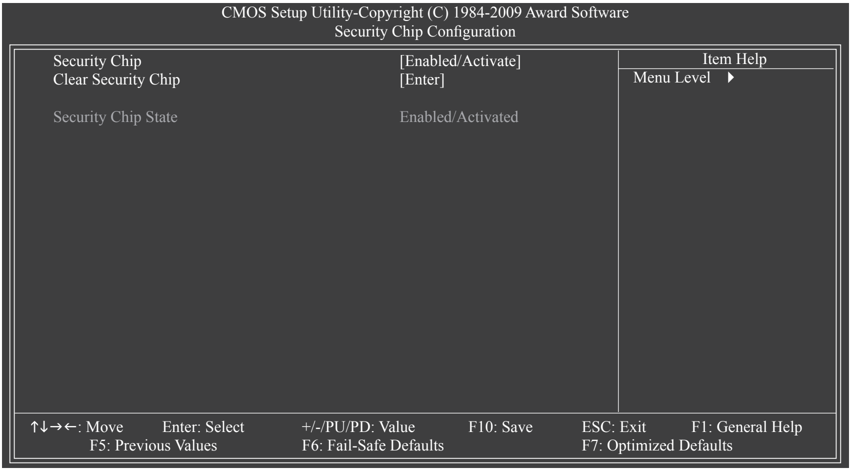
1. Configuring the system BIOS
2. Installing the Infineon TPM driver and the Smart TPM utility
3. Initializing the TPM chip
4. Configuring the Smart TPM utility

1. Configuring the System BIOS

To use the TPM functionality, first enter the system BIOS Setup to activate the TPM chip.

Step 1:
As the computer starts, enter the BIOS Setup program. Go to the **Security Chip Configuration** menu and the following screen will appear. To activate the TPM chip, set **Security Chip** to **Enabled/Activate**. It's recommended that you use the **Clear Security Chip** setting (press <Ctrl> + <F1> in the BIOS main menu to display this setting) to clear the TPM chip.

Previously encrypted files will become inaccessible after the TPM chip is cleared. Be sure to back up the encrypted files first.



```
          CMOS Setup Utility-Copyright (C) 1984-2009 Award Software
                        Security Chip Configuration

  Security Chip                      [Enabled/Activate]        Item Help
  Clear Security Chip                [Enter]               Menu Level  ▶

  Security Chip State                Enabled/Activated

↑↓→←: Move    Enter: Select    +/-/PU/PD: Value    F10: Save    ESC: Exit    F1: General Help
       F5: Previous Values     F6: Fail-Safe Defaults           F7: Optimized Defaults
```

Step 2:
After completing the settings, press <F10> to save changes and then exit the BIOS Setup program.

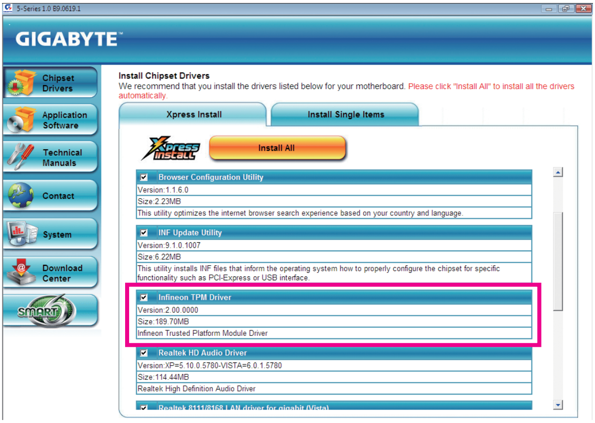
To prevent the TPM settings being cleared by other users, we recommend that you set the User Password in the BIOS Setup program.

2. Installing the Infineon TPM Driver and the Smart TPM Utility

Before you use the Smart TPM utility, ensure that the Infineon TPM driver and the Smart TPM utility have been installed.

2.1. Installing the Infineon TPM Driver

Insert the GIGABYTE motherboard driver disk. "Xpress Install" will automatically scan your system and list all of the drivers that are recommended to install. Click the **Install All** button and "Xpress Install" will install all of the selected drivers, including the Infineon TPM driver.



Install Chipset Drivers

We recommend that you install the drivers listed below for your motherboard. Please click "Install All" to install all the drivers automatically.

☑ Browser Configuration Utility
Version:1.1.6.0
Size:2.23MB
This utility optimizes the internet browser search experience based on your country and language.

☑ INF Update Utility
Version:9.1.0.1007
Size:6.22MB
This utility installs INF files that inform the operating system how to properly configure the chipset for specific functionality such as PCI-Express or USB interface.

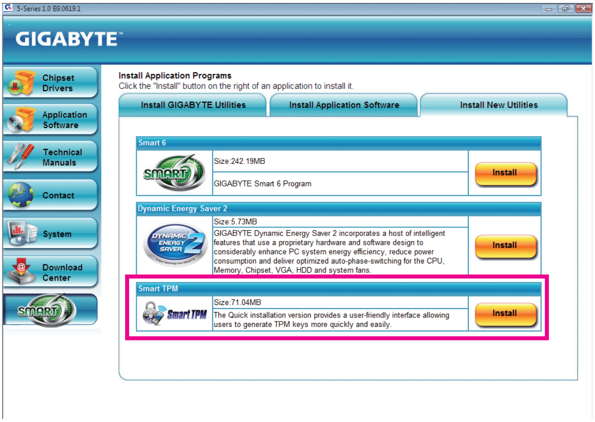
☑ Infineon TPM Driver
Version:2.00.0000
Size:189.70MB
Infineon Trusted Platform Module Driver

☑ Realtek HD Audio Driver
Version:XP=5.10.0.5780-VISTA=6.0.1.5780
Size:114.44MB
Realtek High Definition Audio Driver

☑ Realtek 8111/8168 LAN driver for gigabit (Vista)

2.2. Installing the Smart TPM Utility

Click the tab at the bottom of the left pane of the autorun screen and you'll be directed to the **Install New Utilities** menu. Click the **Install** button on the right of Smart TPM to install it.



Install Application Programs

Click the "Install" button on the right of an application to install it.

Smart 6
Size:242.19MB
GIGABYTE Smart 6 Program

Dynamic Energy Saver 2
Size:5.73MB
GIGABYTE Dynamic Energy Saver 2 incorporates a host of intelligent features that use a proprietary hardware and software design to considerably enhance PC system energy efficiency, reduce power consumption and deliver optimized auto-phase-switching for the CPU, Memory, Chipset, VGA, HDD and system fans.

Smart TPM
Size:71.04MB
The Quick installation version provides a user-friendly interface allowing users to generate TPM keys more quickly and easily.

Some motherboard driver disks include the Smart TPM utility in "Xpress Install." Click the "Install All" button on the "Xpress Install" main menu to install the Infineon TPM driver and the Smart TPM utility altogether.

3. Initializing the TPM chip

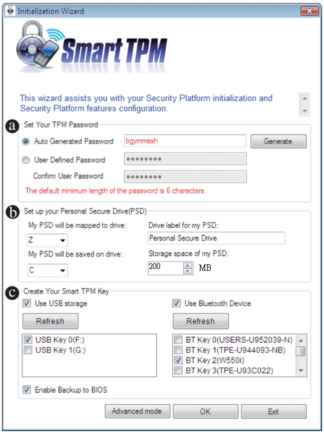
After configuring the system BIOS and installing the driver software, the Infineon Security Platform icon, which indicates that the Infineon Security Platform is not yet initialized, will appear in the notification area. Double-click the icon or right-click the Smart TPM icon and select **Initialization Wizard** to access Smart TPM. With the Smart TPM utility, you can initialize the TPM chip, set up a TPM User Password, configure a Personal Secure Drive (PSD), and create a portable user key (refer to the instructions in Section 3.1). Or you can select **Advanced mode** (refer to the instructions in Section 3.2) to launch the Infineon Security Platform Initialization Wizard to configure advanced settings in the Infineon Security Platform.

3.1. Initializing the TPM Chip with the Smart TPM Utility

The easy-to-use Smart TPM interface allows you to easily initialize the TPM chip, set up a TPM User Password, and configure a Personal Secure Drive.

- **Smart TPM simplifies the configuration procedure of the Infineon Security Platform initialization and its functions. To make further settings, please select "Advanced mode."**
- **Smart TPM provides the "File and folder encryption - Personal Secure Drive (PSD)" settings only. To use the "Secure e-mail" or "File and folder encryption - Encrypting File System (EFS)" functions, please select "Advanced mode."**

3.1.1. The Smart TPM Interface



This wizard assists you with your Security Platform initialization and Security Platform features configuration.

ⓐ Set Your TPM Password

● Auto Generated Password: bgymmexh

○ User Defined Password: ••••••••

Confirm User Password: ••••••••

The default minimum length of the password is 6 characters.

ⓑ Set up your Personal Secure Drive(PSD)

My PSD will be mapped to drive: Z

Drive label for my PSD: Personal Secure Drive

My PSD will be saved on drive: C

Storage space of my PSD: 200 MB

ⓒ Create Your Smart TPM Key

☑ Use USB storage

☑ USB Key 0(F:)
□ USB Key 1(G:)

☑ Use Bluetooth Device

□ BT Key 0(USERS-U952039-N)
□ BT Key 1(TPE-U944093-NB)
☑ BT Key 2(W550i)
□ BT Key 3(TPE-U93C022)

☑ Enable Backup to BIOS

ⓐ **Set Your TPM Password**

A password is automatically provided. You can change it to your own password. Be sure to memorize this password because it allows you to create a portable user key using your Bluetooth cell phone or USB flash drive.

ⓑ **Set up your Personal Secure Drive(PSD)**

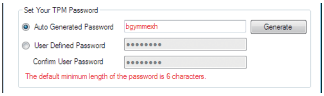
Configure a Personal Secure Drive (PSD) here. Specify the PSD drive letter, drive label, size, and a local drive on which your PSD will be saved.

ⓒ **Create Your Smart TPM Key**

Set your Bluetooth cell phone/USB flash drive as the Smart TPM user key. You will be able to access/close your PSD data when connecting to the Bluetooth cell phone or when plugging in the USB flash drive that is configured as the Smart TPM user key.

3.1.2. Initialization Procedure of Smart TPM

Step 1: Set Your TPM User Password



Set Your TPM Password

● Auto Generated Password: bgymmexh [Generate]

○ User Defined Password: ••••••••

Confirm User Password: ••••••••

The default minimum length of the password is 6 characters.

1. Auto Generated Password

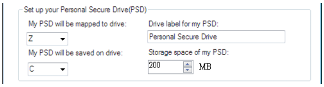
A password will be automatically provided after Smart TPM is launched. To generate a new password, click **Generate**.

2. User Defined Password/Confirm User Password

You can define your own password in the **User Defined Password** box (the maximum length is 16 characters). Enter the password in the **Confirm User Password** box again to confirm.

- **To prevent the TPM settings being cleared by other users, we recommend that you set the User Password in the BIOS Setup program.**
- **This password incorporates the functionalities of the "Owner Password," "User Password," "Emergency Recovery Token Password," and "Password Reset Token Password" of the Infineon Security Platform. Be sure to memorize this password to administrate and use the Security Platform in the future. For details on the rules of the Infineon Security Platform passwords and their usage, please refer to the Infineon Security Platform accompanying documentation.**

Step 2: Set up Your Personal Secure Drive (PSD)



Set up your Personal Secure Drive(PSD)

My PSD will be mapped to drive: Z

Drive label for my PSD: Personal Secure Drive

My PSD will be saved on drive: C

Storage space of my PSD: 200 MB

1. Specify a drive letter and label for your Personal Secure Drive

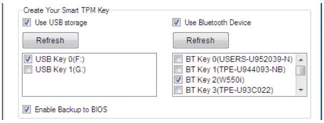
To specify the drive letter for your Personal Secure Drive, select an unused letter from the **My PSD will be mapped to drive** drop-down list of available letters. To specify the drive label, enter the label in the **Drive label for my PSD** box. The label should be no more than 32 characters in length.

2. Specify your Personal Secure Drive size and a local drive on which your Personal Secure Drive will be saved

Select a local drive from the **My PSD will be saved on drive** drop-down list for saving your Personal Secure Drive and enter the Personal Secure Drive size in the **Storage space of my PSD** box.

Your Personal Secure Drive size cannot be changed after setup, so please ensure that the size you specify is large enough to meet your needs. Please note that you cannot use the full drive size, since the file system allocates some space. This depends on the operating system and may be significant for small drive sizes. Please also note that the maximum PSD drive size is limited:
The maximum PSD drive size on FAT16 volumes is 2 GB.
The maximum PSD drive size on FAT32 volumes is 4 GB.

Step 3: Create Your Smart TPM Key



Create Your Smart TPM Key

☑ Use USB storage

☑ Use Bluetooth Device

☑ USB Key 0(F:)
□ USB Key 1(G:)

□ BT Key 0(USERS-U952039-N)
□ BT Key 1(TPE-U944093-NB)
☑ BT Key 2(W550i)
□ BT Key 3(TPE-U93C022)

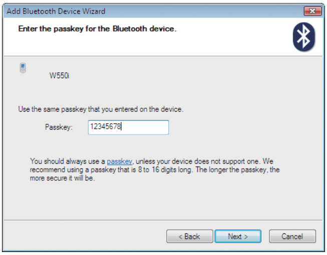
☑ Enable Backup to BIOS

1. Create a USB key:

Select the **Use USB storage** check box and click **Refresh** to search for the USB flash drive(s) that you plug in. Then select the USB flash drive that you want to use as the portable Smart TPM user key. You can select more than one USB flash drive at the same time. Selecting the **Enable Backup to BIOS** check box will store the encrypted TPM User Password in the system BIOS.

⚠ **If more than one user stores their encrypted TPM User Passwords in the BIOS, the latter will overwrite the former.**

2. Create a Bluetooth cell phone key:



Add Bluetooth Device Wizard

Enter the passkey for the Bluetooth device.

W550i

Use the same passkey that you entered on the device.

Passkey: 12345678

You should always use a passkey, unless your device does not support one. We recommend using a passkey that is 8 to 16 digits long. The longer the passkey, the more secure it will be.

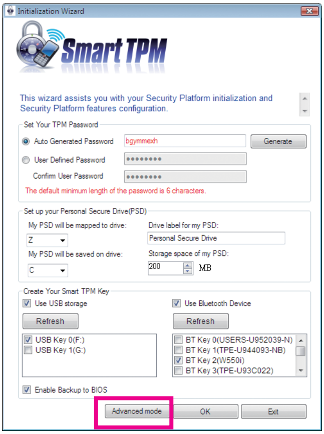
Select the **Use Bluetooth Device** check box and click **Refresh** to search for the Bluetooth enabled cell phone(s). Then select the cell phone that you want to use as the portable Smart TPM user key and a screen similar to that on the left will appear. Enter a passkey (8~16 digits recommended) in **Passkey** which will be used for pairing with your cell phone. Then enter the same passkey on your cell phone for pairing.

Before creating a Bluetooth cell phone key, make sure your motherboard includes a Bluetooth receiver and turn on the search and Bluetooth functions on your phone.

Upon completing the steps above, click **OK** to begin the initialization of the TPM chip and the setups of the TPM User Password, your PSD, and the Smart TPM user key(s).

3.2. Advanced Mode

On the Smart TPM main screen, click **Advanced mode** to access the Infineon Security Platform Initialization Wizard.



Initialization Wizard

This wizard assists you with your Security Platform initialization and Security Platform features configuration.

Set Your TPM Password

● Auto Generated Password bgymmexh

○ User Defined Password ••••••••

Confirm User Password ••••••••

The default minimum length of the password is 6 characters.

Set up your Personal Secure Drive(PSD)

My PSD will be mapped to drive: Z

Drive label for my PSD: Personal Secure Drive

My PSD will be saved on drive: C

Storage space of my PSD: 200 MB

Create Your Smart TPM Key

☑ Use USB storage

☑ USB Key 0(F:)
□ USB Key 1(G:)

☑ Use Bluetooth Device

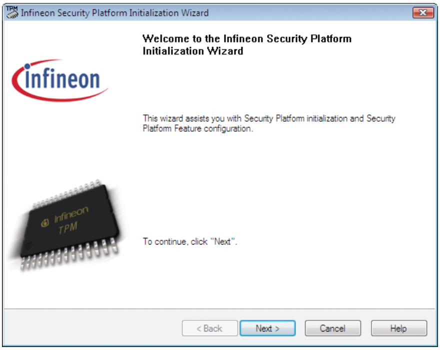
□ BT Key 0(USERS-U952039-N)
□ BT Key 1(TPE-U944093-NB)
☑ BT Key 2(W550i)
□ BT Key 3(TPE-U93C022)

☑ Enable Backup to BIOS

A. Infineon Security Platform Initialization Wizard - Owner

Click **Advanced mode** to launch the Infineon Security Platform Initialization Wizard. Follow the on-screen instructions to initialize the Security Platform Owner and to configure Security Platform Features (backup including Emergency Recovery, Password Reset, Enhanced Authentication, BitLocker). This wizard provides the basis for all further activities on the Infineon Security Platform.

A-1. When the Infineon Security Platform Initialization Wizard appears, click **Next** to continue.



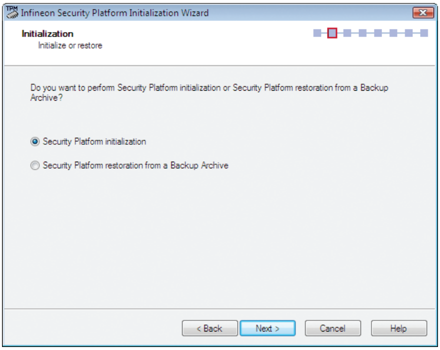
Infineon Security Platform Initialization Wizard

Welcome to the Infineon Security Platform Initialization Wizard

This wizard assists you with Security Platform initialization and Security Platform Feature configuration.

To continue, click "Next".

A-2. Select **Security Platform initialization** and click **Next** to create the Security Platform Owner Password.



Infineon Security Platform Initialization Wizard

Initialization
Initialize or restore

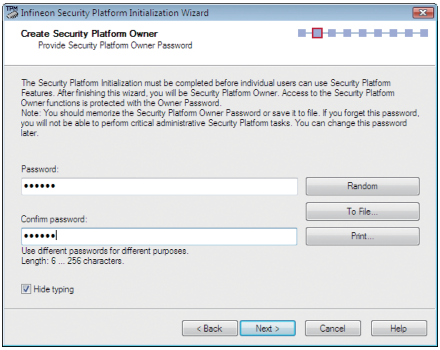
Do you want to perform Security Platform initialization or Security Platform restoration from a Backup Archive?

● Security Platform initialization

○ Security Platform restoration from a Backup Archive

Explanations on setting the Owner Password

1. Enter the Owner Password in the **Password** box or click **Random** to randomly generate a password.
2. Enter the password again to confirm (not necessary if you use a random password).
3. You must uncheck the **Hide typing** check box if you decide to use the random password. Save this password or print it to prevent the loss of the password.



Infineon Security Platform Initialization Wizard

Create Security Platform Owner
Provide Security Platform Owner Password

The Security Platform Initialization must be completed before individual users can use Security Platform Features. After finishing this wizard, you will be Security Platform Owner. Access to the Security Platform Owner functions is protected with the Owner Password.
Note: You should memorize the Security Platform Owner Password or save it to file. If you forget this password, you will not be able to perform critical administrative Security Platform tasks. You can change this password later.

Password: ••••••

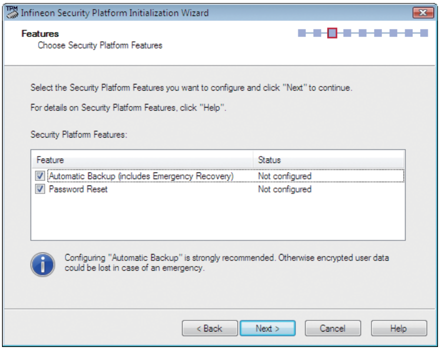
Confirm password: ••••••

Use different passwords for different purposes.
Length: 6 ... 256 characters.

☑ Hide typing

The Infineon Security Platform Owner key is created and stored in the Infineon Trusted Platform Module together with the Infineon Security Platform Owner secret. This key is protected by the Owner Password that must be defined here. You must memorize this password in order to administrate the Security Platform.

A-3. Select Security Platform Features, which comprises **Automatic Backup** (includes Emergency Recovery) and **Password Reset**. Click **Next**.



Infineon Security Platform Initialization Wizard

Features

Choose Security Platform Features

Select the Security Platform Features you want to configure and click "Next" to continue.

For details on Security Platform Features, click "Help".

Security Platform Features:

Feature	Status
☑ Automatic Backup (includes Emergency Recovery)	Not configured
☑ Password Reset	Not configured

Configuring "Automatic Backup" is strongly recommended. Otherwise encrypted user data could be lost in case of an emergency.

Details on Features

Automatic Backup (includes Emergency Recovery)

Check this feature, if you want to configure automatic Security Platform backups. Configuring Backup is strongly recommended. Otherwise all user data will be lost in case of emergency.

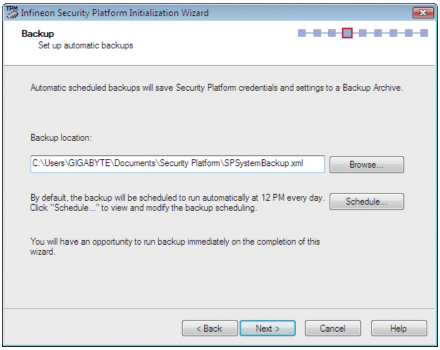
⚠ **You cannot uncheck this feature, if the policy Enforce configuration of Backup including Emergency Recovery is enabled.**

Password Reset

Check this feature, if you want to create a Password Reset Token for all users. Configuring Password Reset is strongly recommended. Otherwise Basic User Passwords can not be reset.

⚠ **You cannot uncheck this feature, if the policy Enforce configuration of Password Reset is enabled. This feature can be configured only once. The selection is disabled, if Password Reset has already been configured.**

A-4. With this page you can configure automatic Security Platform backups. The Security Platform backups comprise the Security Platform Credentials and Settings and the PSD encrypted data, etc. This can prevent if a hardware or storage media failure occur, the backups could restore for the certain users settings. Click **Next**.



Infineon Security Platform Initialization Wizard

Backup

Set up automatic backups

Automatic scheduled backups will save Security Platform credentials and settings to a Backup Archive.

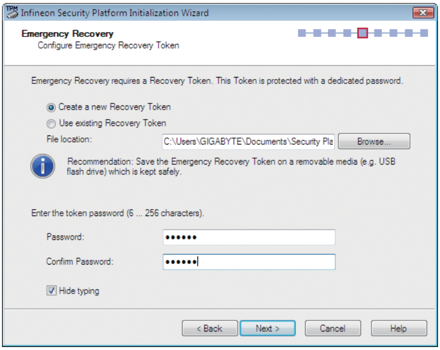
Backup location:

C:\Users\GIGABYTE\Documents\Security Platform\SPSystemBackup.xml

By default, the backup will be scheduled to run automatically at 12 PM every day. Click "Schedule..." to view and modify the backup scheduling.

You will have an opportunity to run backup immediately on the completion of this wizard.

A-5. Select **Create a new Recovery Token**. Then enter a new token password to be used for Emergency Recovery.



Emergency Recovery
Configure Emergency Recovery Token

Emergency Recovery requires a Recovery Token. This Token is protected with a dedicated password.

● Create a new Recovery Token
○ Use existing Recovery Token

File location: C:\Users\GIGABYTE\Documents\Security Pla Browse...

Recommendation: Save the Emergency Recovery Token on a removable media (e.g. USB flash drive) which is kept safely.

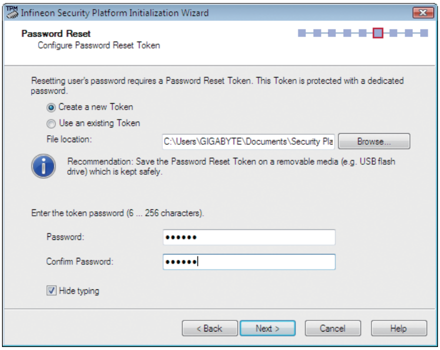
Enter the token password (6 ... 256 characters).

Password: ••••••

Confirm Password: ••••••

☑ Hide typing

A-6. Select **Create a new Token** to create a Password Reset Token. Then enter a new token password.



Password Reset
Configure Password Reset Token

Resetting user's password requires a Password Reset Token. This Token is protected with a dedicated password.

● Create a new Token
○ Use an existing Token

File location: C:\Users\GIGABYTE\Documents\Security Pla Browse...

Recommendation: Save the Password Reset Token on a removable media (e.g. USB flash drive) which is kept safely.

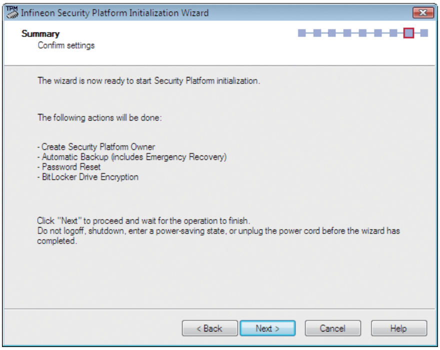
Enter the token password (6 ... 256 characters).

Password: ••••••

Confirm Password: ••••••

☑ Hide typing

A-7. Make sure you have selected all the functions you want to perform. Click **Next** to continue.



Summary
Confirm settings

The wizard is now ready to start Security Platform initialization.

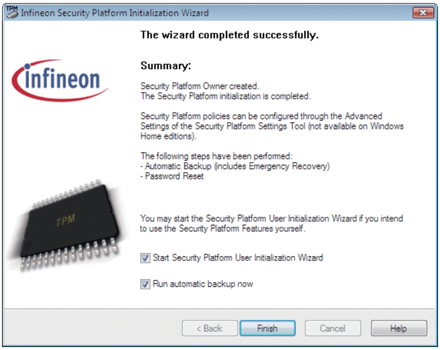
The following actions will be done:

- Create Security Platform Owner
- Automatic Backup (includes Emergency Recovery)
- Password Reset
- BitLocker Drive Encryption

Click "Next" to proceed and wait for the operation to finish.
Do not logoff, shutdown, enter a power-saving state, or unplug the power cord before the wizard has completed.

Do not log off, shutdown, enter a power-saving state, or unplug the power cord before the wizard has completed.

A-8. Click **Finish** to complete the initialization and configuration of the Infineon Security Platform. Then access the Infineon Security Platform User Initialization Wizard (select the **Start Security Platform User Initialization Wizard** check box).



The wizard completed successfully.

Summary:

Security Platform Owner created.
The Security Platform initialization is completed.

Security Platform policies can be configured through the Advanced Settings of the Security Platform Settings Tool (not available on Windows Home editions).

The following steps have been performed:
- Automatic Backup (includes Emergency Recovery)
- Password Reset

You may start the Security Platform User Initialization Wizard if you intend to use the Security Platform Features yourself.

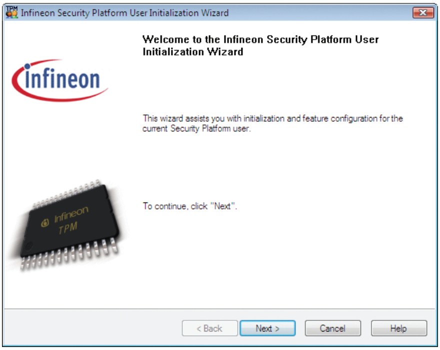
☑ Start Security Platform User Initialization Wizard

☑ Run automatic backup now

B. Infineon Security Platform Initialization Wizard - User

The Infineon Security Platform User Initialization Wizard is used to initialize the Security Platform Users and to configure the user-specific features (secure e-mail, file and folder encryption with EFS and PSD, Enhanced Authentication). This wizard has to be started for each computer user, who is intended to use the personalized Infineon Security Platform Features (i.e., who will be Infineon Security Platform User).

B-1. Launch the Infineon Security Platform User Initialization Wizard. Click **Next** to continue.

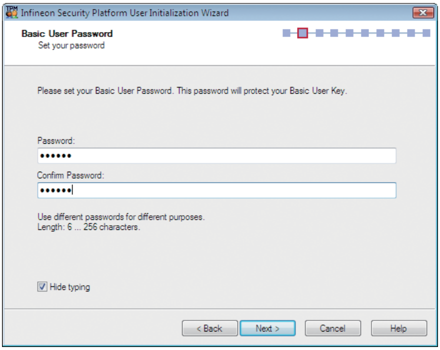


Welcome to the Infineon Security Platform User Initialization Wizard

This wizard assists you with initialization and feature configuration for the current Security Platform user.

To continue, click "Next".

B-2. Set a Basic User Password and click **Next**.



Infineon Security Platform User Initialization Wizard

Basic User Password

Set your password

Please set your Basic User Password. This password will protect your Basic User Key.

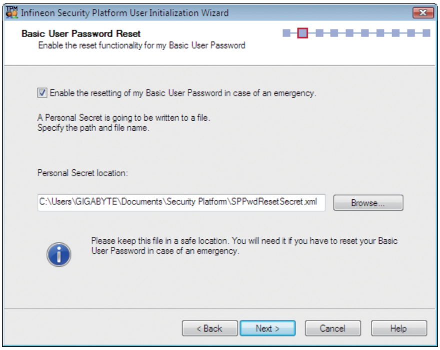
Password: ••••••

Confirm Password: ••••••

Use different passwords for different purposes.
Length: 6 ... 256 characters.

☑ Hide typing

B-3. Enable the reset functionality for the Basic User Password. Select the location that you wish to save the file and then click **Next**.



Infineon Security Platform User Initialization Wizard

Basic User Password Reset

Enable the reset functionality for my Basic User Password

☑ Enable the resetting of my Basic User Password in case of an emergency.

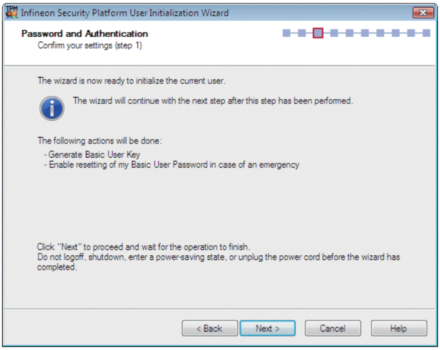
A Personal Secret is going to be written to a file.
Specify the path and file name.

Personal Secret location:

C:\Users\GIGABYTE\Documents\Security Platform\SPPwdResetSecret.xml

Please keep this file in a safe location. You will need it if you have to reset your Basic User Password in case of an emergency.

B-4. Click **Next** to continue the initialization.



Infineon Security Platform User Initialization Wizard

Password and Authentication

Confirm your settings (step 1)

The wizard is now ready to initialize the current user.

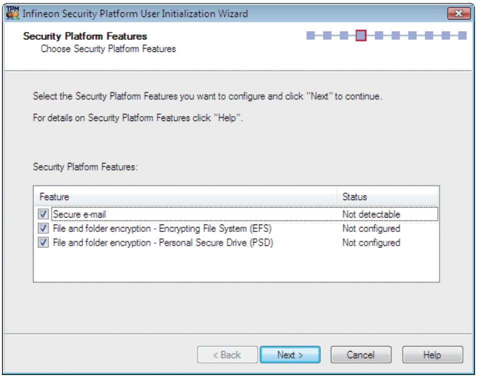
The wizard will continue with the next step after this step has been performed.

The following actions will be done:
- Generate Basic User Key
- Enable resetting of my Basic User Password in case of an emergency

Click "Next" to proceed and wait for the operation to finish.
Do not logoff, shutdown, enter a power-saving state, or unplug the power cord before the wizard has completed.

Do not log off, shutdown, enter a power-saving state, or unplug the power cord before the wizard has completed.

B-5. Select the Security Platform Features you want to configure and click **Next** to continue.



Infineon Security Platform User Initialization Wizard

Security Platform Features

Choose Security Platform Features

Select the Security Platform Features you want to configure and click "Next" to continue.

For details on Security Platform Features click "Help".

Security Platform Features:

Feature	Status
☑ Secure e-mail	Not detectable
☑ File and folder encryption - Encrypting File System (EFS)	Not configured
☑ File and folder encryption - Personal Secure Drive (PSD)	Not configured

Details on Features

Secure e-mail

User-specific e-mail encryption and/or signing to prevent unauthorized persons from reading or changing your e-mails. Using this feature guarantees that only the e-mail creator and the specified recipients will be able to decrypt and read the message or validate the identity of the sender.

If you chose to configure this feature, you can request a certificate for secure e-mail (if a certificate request web address is set in your policy settings). The wizard will provide information how to configure secure e-mail. The configuration of your mail client is not part of this wizard. Thus the status cannot be displayed here.

File and folder encryption - Encrypting File System (EFS)

The operating system incorporates the functionality to perform user-specific encryption of the content of folders and files on the local computer using the Microsoft Encrypting File System (EFS). Only the user who created a file in these folders can access the content of this file. Other users have to be granted access rights to an EFS folder in an explicit administrative operation to enable them to use files in it.

If you chose to configure this feature, you can select a certificate for EFS. You can also request or create a new certificate.

EFS is not supported in Windows Vista Home Basic, Vista Home Premium and XP Home Editions.

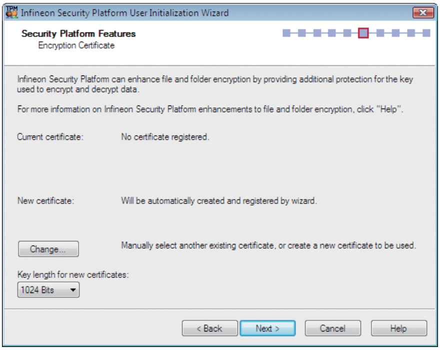
File and folder encryption - Personal Secure Drive (PSD)

Personal Secure Drive features file and folder encryption similar to EFS. Unlike EFS, PSD is supported in Windows Vista Home Basic, Vista Home Premium and XP Home Editions.

A logical drive is provided to permitted users. This drive offers access protection and encryption for all content in it. The encryption is performed automatically. A PSD cannot be accessed via its UNC identifier to get readable data and can be installed only on the local computer. Network access is not possible. If you chose to configure this feature, you can set up, modify or delete your PSD. Like EFS configuration, you can select a certificate for PSD. You can also request or create a new certificate.

B-5-1. Use the **File and folder encryption - Personal Secure Drive (PSD)** as the example:

You can configure a Encryption Certificate with this page. If no valid certificate is registered currently, the wizard offers to create a new certificate and select it automatically. Click **Next** to create the certificate automatically, or click **Change** to create an encryption certificate manually.


Infineon Security Platform User Initialization Wizard

Security Platform Features
Encryption Certificate

Infineon Security Platform can enhance file and folder encryption by providing additional protection for the key used to encrypt and decrypt data.

For more information on Infineon Security Platform enhancements to file and folder encryption, click "Help".

Current certificate: No certificate registered.

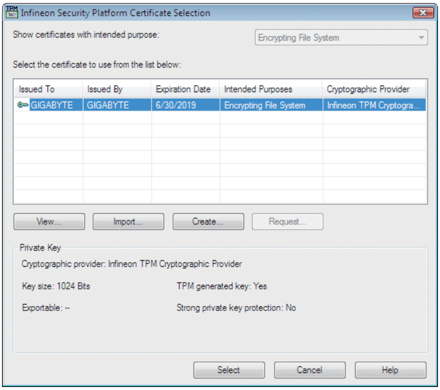
New certificate: Will be automatically created and registered by wizard.

Manually select another existing certificate, or create a new certificate to be used.

Key length for new certificates: 1024 Bits

Key length for new certificates:
Here you can select default key length for newly created encryption certificates, e.g. 1024 bits or 2048 bits.

B-5-2. Click **Create** to create the certificate. After the certificate appears, click the certificate and click **Select**.


Infineon Security Platform Certificate Selection

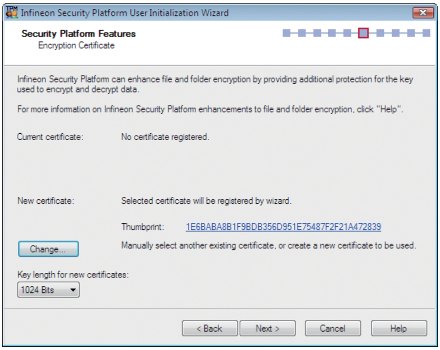
Show certificates with intended purpose: Encrypting File System

Select the certificate to use from the list below:

Issued To	Issued By	Expiration Date	Intended Purposes	Cryptographic Provider
GIGABYTE	GIGABYTE	6/30/2019	Encrypting File System	Infineon TPM Cryptogra...

Private Key
Cryptographic provider: Infineon TPM Cryptographic Provider
Key size: 1024 Bits TPM generated key: Yes
Exportable: -- Strong private key protection: No

B-5-3. The certificate has been selected. Click **Next**.


Infineon Security Platform User Initialization Wizard

Security Platform Features
Encryption Certificate

Infineon Security Platform can enhance file and folder encryption by providing additional protection for the key used to encrypt and decrypt data.

For more information on Infineon Security Platform enhancements to file and folder encryption, click "Help".

Current certificate: No certificate registered.

New certificate: Selected certificate will be registered by wizard.

Thumbprint: 1E6BABA8B1F9BDB356D951E75487F2F21A472839

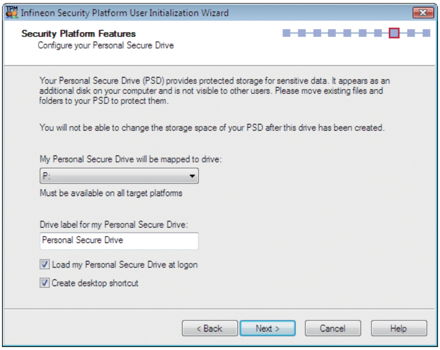
Manually select another existing certificate, or create a new certificate to be used.

Key length for new certificates: 1024 Bits

B-6. Set up a Personal Secure Drive (PSD)

B-6-1. Specify a drive letter and label for your Personal Secure Drive

To specify the drive letter for your Personal Secure Drive, select an unused letter from the drop-down list of available letters. To specify the drive label, enter the label in the field provided. The label should be no more than 32 characters in length. Select the **Load my Personal Secure Drive at logon** check box, if you want to load your PSD at logon. Click **Next**.



Infineon Security Platform User Initialization Wizard

Security Platform Features

Configure your Personal Secure Drive

Your Personal Secure Drive (PSD) provides protected storage for sensitive data. It appears as an additional disk on your computer and is not visible to other users. Please move existing files and folders to your PSD to protect them.

You will not be able to change the storage space of your PSD after this drive has been created.

My Personal Secure Drive will be mapped to drive: P:

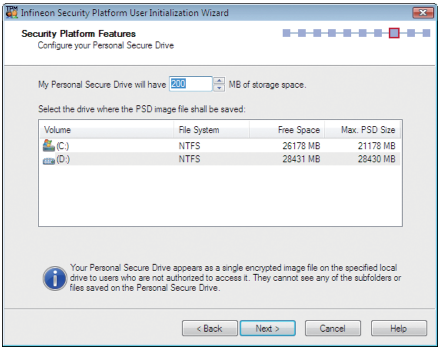
Must be available on all target platforms

Drive label for my Personal Secure Drive: Personal Secure Drive

☑ Load my Personal Secure Drive at logon

☑ Create desktop shortcut

B-6-2. Specify your Personal Secure Drive size and a local drive on which your Personal Secure Drive will be saved. Click **Next**.



Infineon Security Platform User Initialization Wizard

Security Platform Features

Configure your Personal Secure Drive

My Personal Secure Drive will have 200 MB of storage space.

Select the drive where the PSD image file shall be saved:

Volume	File System	Free Space	Max. PSD Size
(C:)	NTFS	26178 MB	21178 MB
(D:)	NTFS	28431 MB	28430 MB

Your Personal Secure Drive appears as a single encrypted image file on the specified local drive to users who are not authorized to access it. They cannot see any of the subfolders or files saved on the Personal Secure Drive.

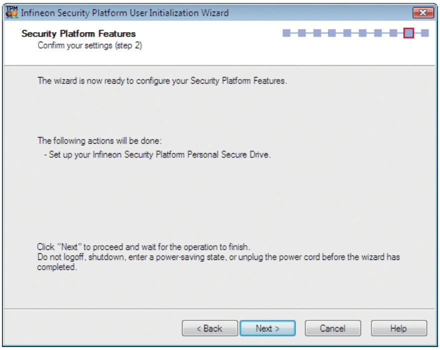
Your Personal Secure Drive size cannot be changed after setup, so please ensure that the size you specify is large enough to meet your needs. Please note that you cannot use the full drive size, since the file system allocates some space. This depends on the operating system and may be significant for small drive sizes.

Please also note that the maximum PSD drive size is limited:

The maximum PSD drive size on FAT16 volumes is 2 GB.

The maximum PSD drive size on FAT32 volumes is 4 GB.

B-7. Click **Next** to continue.



Security Platform Features
Confirm your settings (step 2)

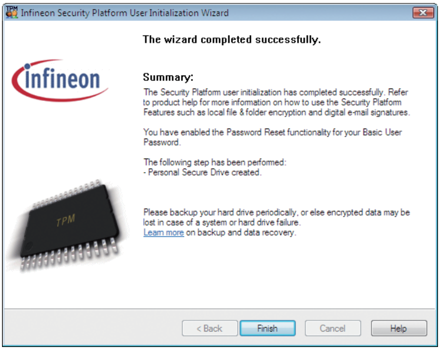
The wizard is now ready to configure your Security Platform Features.

The following actions will be done:
- Set up your Infineon Security Platform Personal Secure Drive.

Click "Next" to proceed and wait for the operation to finish.
Do not logoff, shutdown, enter a power-saving state, or unplug the power cord before the wizard has completed.

⚠ **Do not log off, shutdown, enter a power-saving state, or unplug the power cord before the wizard has completed.**

B-8. Click **Finish** to finish the user initialization and features configuration of the Infineon Security Platform.



The wizard completed successfully.

Summary:
The Security Platform user initialization has completed successfully. Refer to product help for more information on how to use the Security Platform Features such as local file & folder encryption and digital e-mail signatures.

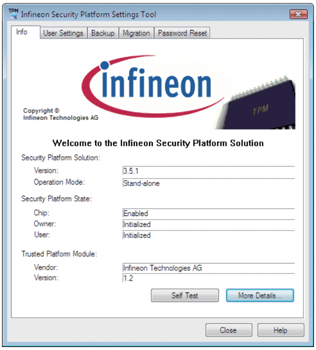
You have enabled the Password Reset functionality for your Basic User Password.

The following step has been performed:
- Personal Secure Drive created.

Please backup your hard drive periodically, or else encrypted data may be lost in case of a system or hard drive failure.
Learn more on backup and data recovery.

C. Infineon Security Platform Settings Tool

With the Security Platform Settings Tool you can get various information about the Trusted Platform Module of your system. Also, you are able to carry out several administrative tasks, such as to change Basic User Password, perform backups, export/import Security Platform User keys and certificates, etc.



Copyright ©
Infineon Technologies AG

Welcome to the Infineon Security Platform Solution

Security Platform Solution:
Version: 3.5.1
Operation Mode: Stand-alone

Security Platform State:
Chip: Enabled
Owner: Initialized
User: Initialized

Trusted Platform Module:
Vendor: Infineon Technologies AG
Version: 1.2

4. Configuring the Smart TPM Utility

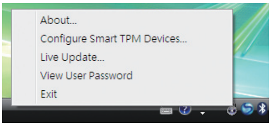
GIGABYTE's unique Smart TPM (Trusted Platform Module) supports the industry's most advanced hardware-based data encryption. Smart TPM provides users with an easy-to-use software interface to create a portable user key using a Bluetooth cell phone or USB flash drive. Users can access/close their PSD data by simply connecting to the Bluetooth cell phone or plugging in the USB flash drive, without the hassles of complicated configurations. In addition, users can create more than one Bluetooth cell phone/USB flash drive key, so when they lost a key they still can access data.

- **After creating the password(s) and key(s) associated with the TPM, be sure to store them in a secure location and back them up. Loss of the password(s) or the key(s) will render the files encrypted via the TPM unable to be cracked or read.**
- **Though the TPM delivers the latest data security technology, it does not guarantee data integrity or provide hardware protection. GIGABYTE is not liable for loss of encrypted data as a result of hardware damage.**

4.1. Creating a USB Key

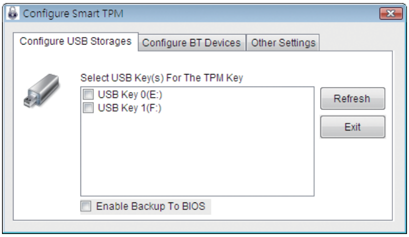
Step 1:

After initializing the TPM chip and setting up the TPM User Password and your PSD, right-click the Smart TPM icon in the notification area to display the menu as shown below.



Step 2:

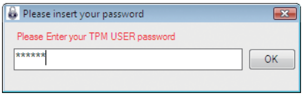
Click **Configure Smart TPM Devices** to launch the Smart TPM utility. To create a portable USB key, select **Configure USB Storages** and then select the USB flash drive that you want to use as the portable user key. (If the screen doesn't display the USB flash drive inserted, click **Refresh** to let Smart TPM re-detect the device.)



If more than one user uses the "Enable Bacup to BIOS" function to store their encrypted TPM User Passwords in the BIOS, the latter will overwrite the former.

Step 3:

Enter the TPM User Password that you set earlier and click **OK** to complete creating the USB key. You are able to access/close your PSD by plugging in or unplugging the USB flash drive.



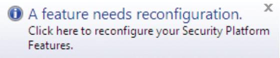
Please insert your password

Please Enter your TPM USER password

******

Do not turn off or reset your computer when a USB key is being created.

- **If you enter the TPM User Password incorrectly three times, Smart TPM will be locked. To be able to enter the password again, go to the "Security Chip Configuration" menu in BIOS Setup and then set "Security Chip" to "Enabled/Activate."**
- **When you unplug the USB key, the Infineon Security Platform Settings Tool will give the following warning message, which is normal.**

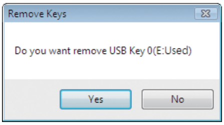


A feature needs reconfiguration.

Click here to reconfigure your Security Platform Features.

To cancel a USB key:

To cancel a USB key, uncheck the USB flash drive that has been configured as the Smart TPM user key on the **Configure USB Storages** tab. When prompted to confirm, click **Yes**. Then the USB key is cancelled.



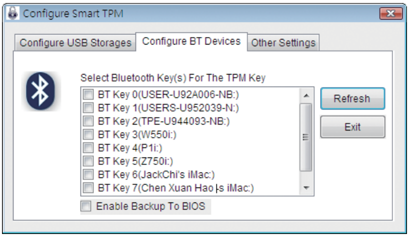
Remove Keys

Do you want remove USB Key 0(E:Used)

4.2. Creating a Bluetooth Cell Phone Key

Step 1:

To create a portable Bluetooth cell phone key, select **Configure BT Devices** and then select the Bluetooth cell phone that you want to use as the portable user key. (If the screen doesn't display your Bluetooth-enabled cell phone, click **Refresh** to let Smart TPM re-detect the device.)



Configure Smart TPM

Select Bluetooth Key(s) For The TPM Key

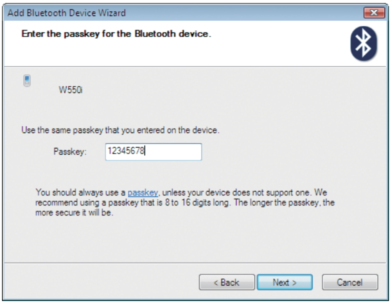
☐ BT Key 0(USER-U92A006-NB:)
☐ BT Key 1(USERS-U952039-N:)
☐ BT Key 2(TPE-U944093-NB:)
☐ BT Key 3(W550i:)
☐ BT Key 4(P1i:)
☐ BT Key 5(Z750i:)
☐ BT Key 6(JackChi's iMac:)
☐ BT Key 7(Chen Xuan Hao ¦s iMac:)

☐ Enable Backup To BIOS

Before creating a Bluetooth cell phone key, make sure your motherboard includes a Bluetooth receiver and turn on the search and Bluetooth functions on your phone.

Step 2:

When the **Add Bluetooth Device Wizard** appears, enter a passkey (8~16 digits recommended) which will be used for pairing with your cell phone.



Enter the passkey for the Bluetooth device.

W550i

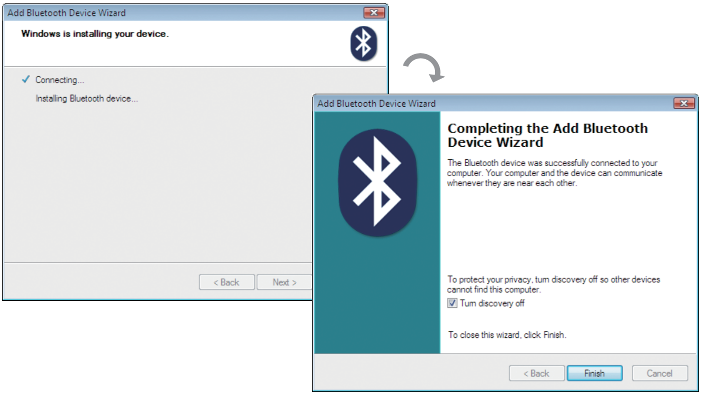
Use the same passkey that you entered on the device.

Passkey: 12345678

You should always use a passkey, unless your device does not support one. We recommend using a passkey that is 8 to 16 digits long. The longer the passkey, the more secure it will be.

Step 3:

Enter the same passkey on your cell phone for pairing. After confirming the passkey, click **Finish** to complete creating the Bluetooth cell phone key. You are able to access/close your PSD when turning on/off Bluetooth on your cell phone or when your cell phone gets close to or away from the computer.



Windows is installing your device.

✓ Connecting...

Installing Bluetooth device...

Completing the Add Bluetooth Device Wizard

The Bluetooth device was successfully connected to your computer. Your computer and the device can communicate whenever they are near each other.

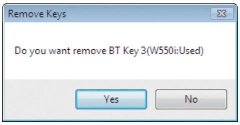
To protect your privacy, turn discovery off so other devices cannot find this computer.

☑ Turn discovery off

To close this wizard, click Finish.

To cancel a Bluetooth cell phone key:

To cancel a Bluetooth cell phone key, uncheck the Bluetooth cell phone that has been configured as the Smart TPM key on the **Configure BT Devices** tab. When prompted to confirm, click **Yes**. Then the Bluetooth cell phone key is cancelled.

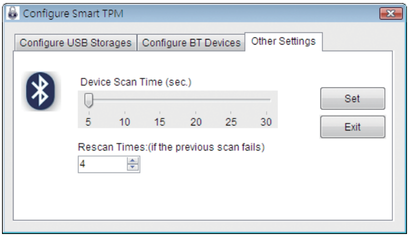


Do you want remove BT Key 3(W550i:Used)

4.3. Other Bluetooth Settings

On the **Other Settings** tab, you can configure how much time it takes to scan your Bluetooth cell phone key and how many times to rescan the key to make sure it is in range of your computer.

- Device Scan Time (sec.):
  Set the length of time Smart TPM scans your Bluetooth cell phone key, ranging from 5 seconds to 30 seconds in 5-second increment. Smart TPM searches for the key based on the length of time you set.
- Rescan Times:
  Set how many times Smart TPM will rescan your Bluetooth cell phone key if it does not detect it, ranging from 1 time to 10 times. Smart TPM will keep rescanning according to the times you set. When the times limit is reached and Smart TPM still doesn't detect your Bluetooth cell phone key, Smart TPM will turn off the TPM function.



Configure Smart TPM

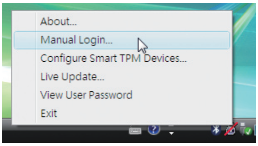
Device Scan Time (sec.): 5

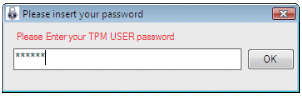
Rescan Times:(if the previous scan fails) 4

4.4. Other Features

A. Manual Login/Logout

You can enable the TPM even if your portable user key is not handy. Right-click the Smart TPM icon in the notification area and select **Manual Login**. When prompted, enter the TPM User Password to enable the TPM.



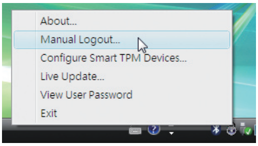


Please insert your password

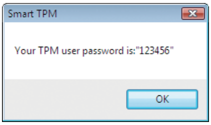
Please Enter your TPM USER password

******

To disable the TPM, select **Manual Logout**.



B. View User Password



Smart TPM

Your TPM user password is:"123456"

Select **View User Password** to display the TPM User Password.

This function requires that you plug in your USB key or enable Bluetooth on your Bluetooth cell phone key.