Table of Contents

TPM Configuration Procedure

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

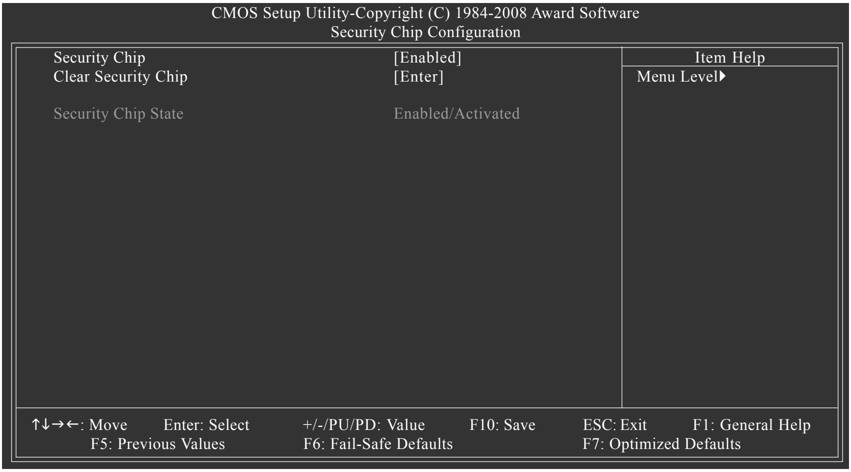
1. Configuring the system BIOS
2. Installing the Infineon TPM driver and the GIGABYTE Ultra TPM utility
3. Initializing the TPM chip
4. Configuring the GIGABYTE Ultra TPM utility

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 BIOS Setup and go to the **Security Chip Configuration** menu. The following screen will appear. To activate the TPM chip, set **Security Chip** to **Enabled**. It's recommended that you use the **Clear Security Chip** item to clear the TPM chip as well.

CAUTION **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) 1984-2008 Award Software
Security Chip Configuration

Security Chip                     [Enabled]              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
```

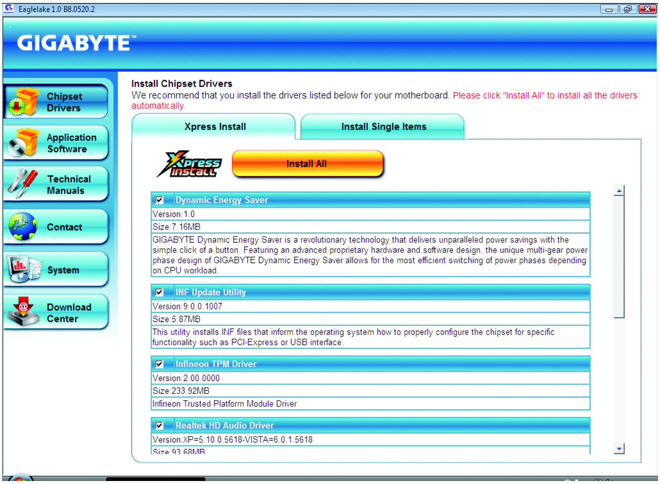
Step 2:
After finishing the settings, press <F10> to save changes and then exit the BIOS Setup program.

2. Installing the Infineon TPM Driver and the GIGABYTE Ultra TPM Utility

To use GIGABYTE's Ultra TPM, ensure that the Infineon TPM driver and the GIGABYTE Ultra TPM utility have been installed in your system.

Method 1:

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



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.

☑ Dynamic Energy Saver
Version:1.0
Size:7.16MB
GIGABYTE Dynamic Energy Saver is a revolutionary technology that delivers unparalleled power savings with the simple click of a button. Featuring an advanced proprietary hardware and software design, the unique multi-gear power phase design of GIGABYTE Dynamic Energy Saver allows for the most efficient switching of power phases depending on CPU workload.

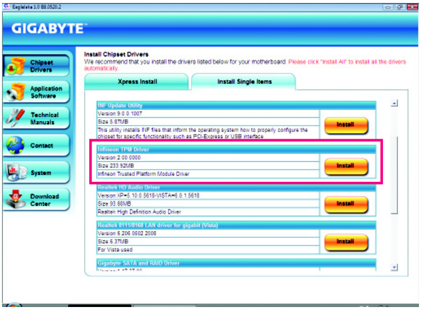
☑ INF Update Utility
Version:9.0.0.1007
Size:5.87MB
This utility installs INF files that inform the operating system how to properly configure the chipset for specific functionality such as PCI-Express or USB interface.

☑ Infineon TPM Driver
Version:2.00.0000
Size:233.92MB
Infineon Trusted Platform Module Driver

☑ Realtek HD Audio Driver
Version:XP=5.10.0.5618-VISTA=6.0.1.5618
Size:93.68MB

Method 2:

To individually install the Infineon TPM driver and the GIGABYTE Ultra TPM utility, go to the **Install Single Items** menu and click the **Install** buttons on the right of the Infineon TPM Driver and GIGABYTE Ultra TPM items.



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.

INF Update Utility
Version:9.0.0.1007
Size:5.87MB
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.

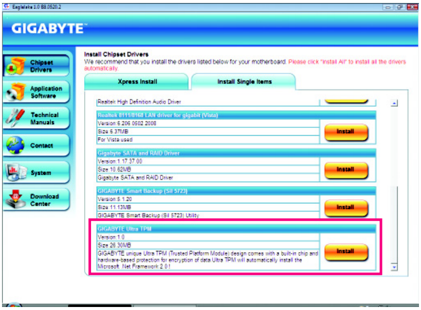
Infineon TPM Driver
Version:2.00.0000
Size:233.92MB
Infineon Trusted Platform Module Driver

Realtek HD Audio Driver
Version:XP=5.10.0.5618-VISTA=6.0.1.5618
Size:93.68MB
Realtek High Definition Audio Driver

Realtek 8111/8168 LAN driver for gigabit (Vista)
Version:6.206.0502.2008
Size:6.37MB
For Vista used

Gigabyte SATA and RAID Driver

Install 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.

Realtek High Definition Audio Driver

Realtek 8111/8168 LAN driver for gigabit (Vista)
Version:6.206.0502.2008
Size:6.37MB
For Vista used

Gigabyte SATA and RAID Driver
Version:1.17.37.00
Size:10.62MB
Gigabyte SATA and RAID Driver

GIGABYTE Smart Backup (SiI 5723)
Version:5.1.20
Size:11.13MB
GIGABYTE Smart Backup (SiI 5723) Utility

GIGABYTE Ultra TPM
Version:1.0
Size:26.30MB
GIGABYTE unique Ultra TPM (Trusted Platform Module) design comes with a built-in chip and hardware-based protection for encryption of data.Ultra TPM will automatically install the Microsoft .Net Framework 2.0 !

Install the GIGABYTE Ultra TPM utility.

3. Initializing the TPM Chip

After configuring the system BIOS and installing the driver software, a small Infineon Security Platform icon (This icon indicates that the Infineon Security Platform is not yet initialized.) will appear in your system tray. Double-click the icon to enter "Easy Mode" (refer to the instructions in Section 3.1) or select "Advanced Mode" (refer to the instructions in Chapter 3.2) and then begin to initialize and configure the Infineon Security Platform.

3.1. Easy Mode

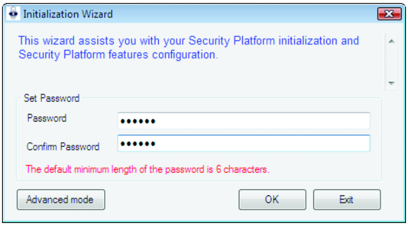
Double-click the Infineon Security Platform icon in the system tray to launch the GIGABYTE Initialization Wizard, which is the "Easy Mode" of the Security Platform. "Easy Mode" is an easy-to-use user interface of the Security Platform that allows users to quickly initialize the TPM chip and set up a Personal Secure Drive (PSD).

NOTE

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

Step 1: Set up a Password

Launch the GIGABYTE Initialization Wizard. This wizard will request you to set up a password. After entering the password, click **OK** to begin the initialization of the Infineon Security Platform.



Initialization Wizard

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

Set Password

Password: ••••••

Confirm Password: ••••••

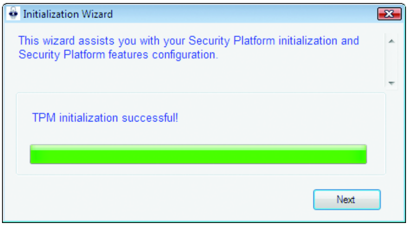
The default minimum length of the password is 6 characters.

CAUTION

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: Infineon Security Platform Initialization

Begin the initialization of the Infineon Security Platform. The "TPM initialization successful!" message appears upon completion of the initialization. Click **Next** to proceed with setting up a Personal Secure Drive (PSD).



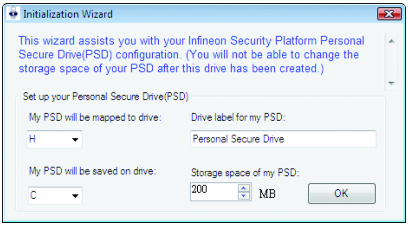
Initialization Wizard

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

TPM initialization successful!

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

Step 3: Set up a Personal Secure Drive (PSD)



Initialization Wizard

This wizard assists you with your Infineon Security Platform Personal Secure Drive(PSD) configuration. (You will not be able to change the storage space of your PSD after this drive has been created.)

Set up your Personal Secure Drive(PSD)

My PSD will be mapped to drive: H

Drive label for my PSD: Personal Secure Drive

My PSD will be saved on drive: C

Storage space of my PSD: 200 MB

3-1. 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.

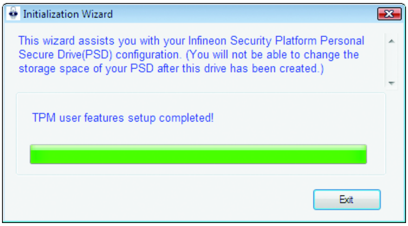
3-2. Specify your Personal Secure Drive size and a local drive on which your Personal Secure Drive will be saved

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 4: Complete the Settings

Click **Exit** to complete the initialization of the TPM chip and setup of the Personal Secure Drive (PSD). You can then access the GIGABYTE Ultra TPM utility to set up a Portable User Key.



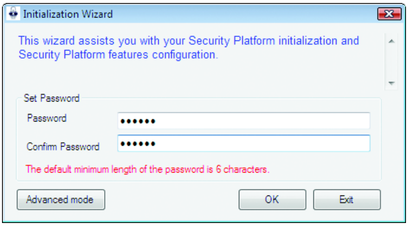
Initialization Wizard

This wizard assists you with your Infineon Security Platform Personal Secure Drive(PSD) configuration. (You will not be able to change the storage space of your PSD after this drive has been created.)

TPM user features setup completed!

3.2. Advanced Mode

When the GIGABYTE Initialization Wizard is launched (by double-clicking the Infineon Security Platform icon in the system tray), if you wish to configure further settings, 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 Password

Password: ••••••

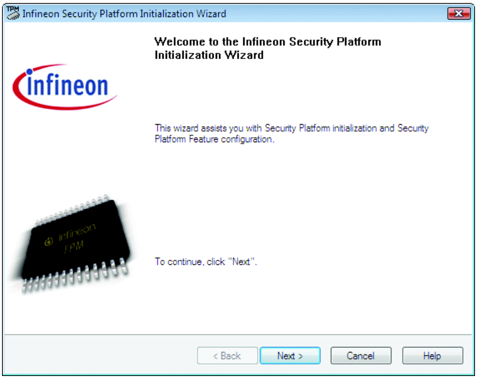
Confirm Password: ••••••

The default minimum length of the password is 6 characters.

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.



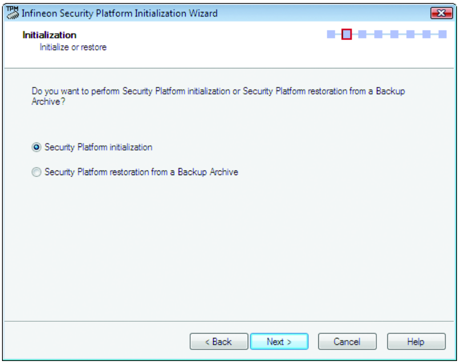
Infineon Security Platform Initialization Wizard

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.



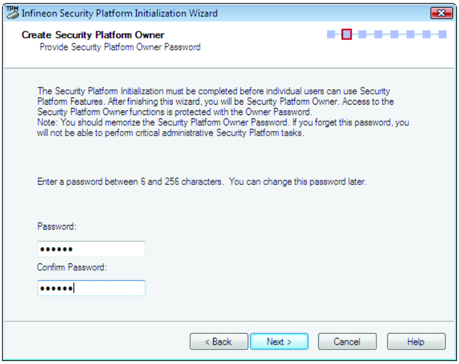
Infineon Security Platform Initialization Wizard

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



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. If you forget this password, you will not be able to perform critical administrative Security Platform tasks.

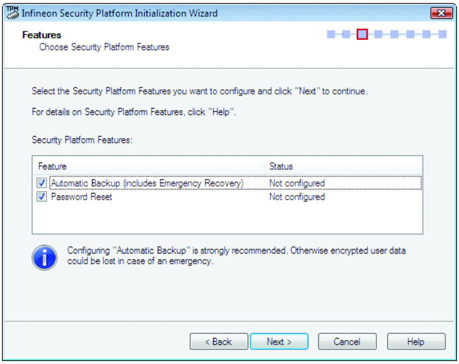
Enter a password between 6 and 256 characters. You can change this password later.

Password:
••••••

Confirm Password:
••••••

NOTE **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.

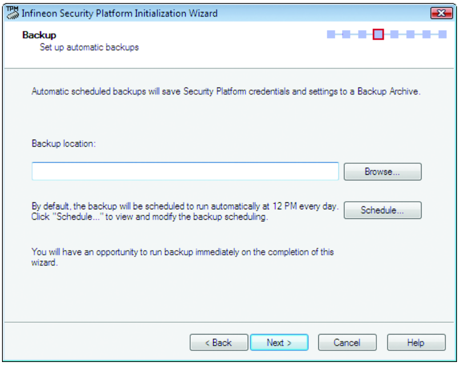
⚠ CAUTION **You cannot uncheck this feature, if the policy Enforce configuration of Backup including Emergency Recovery is enabled.**

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.

⚠ CAUTION **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

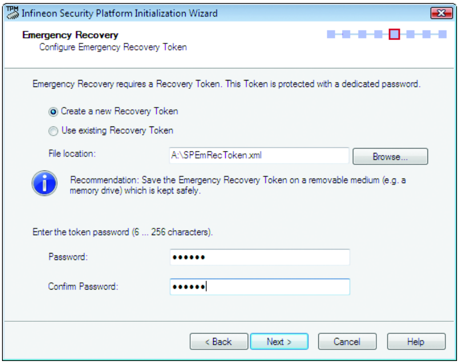
Automatic scheduled backups will save Security Platform credentials and settings to a Backup Archive.

Backup location:

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: A:\SPEmRecToken.xml [Browse...]

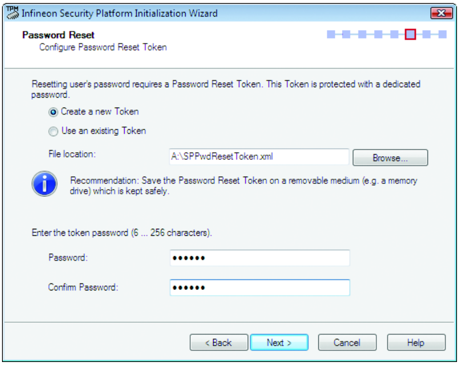
Recommendation: Save the Emergency Recovery Token on a removable medium (e.g. a memory drive) which is kept safely.

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

Password: ••••••

Confirm Password: ••••••

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: A:\SPPwdResetToken.xml [Browse...]

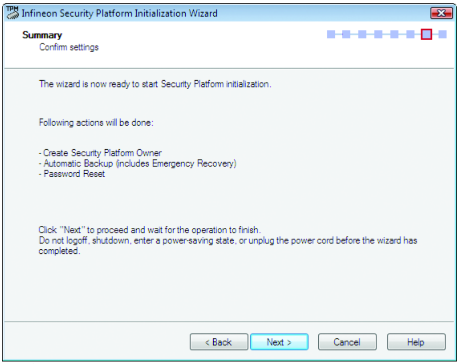
Recommendation: Save the Password Reset Token on a removable medium (e.g. a memory drive) which is kept safely.

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

Password: ••••••

Confirm Password: ••••••

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.

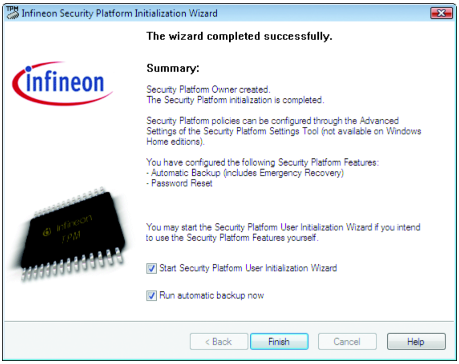
Following actions will be done:

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

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.

CAUTION **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).

You have configured the following Security Platform Features:
- 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.

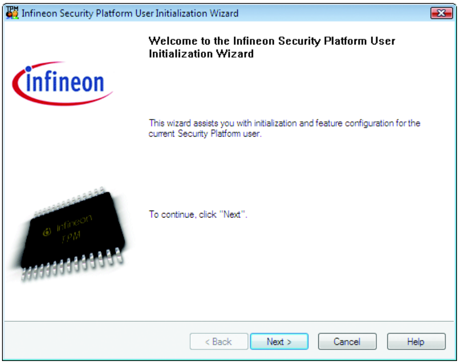
☑ Start Security Platform User Initialization Wizard

☑ 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.

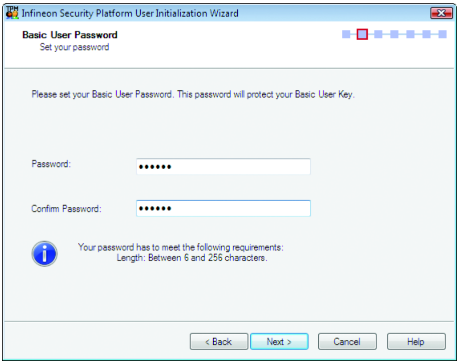


Welcome to the Infineon Security Platform User Initialization Wizard

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**.



Basic User Password
Set your password

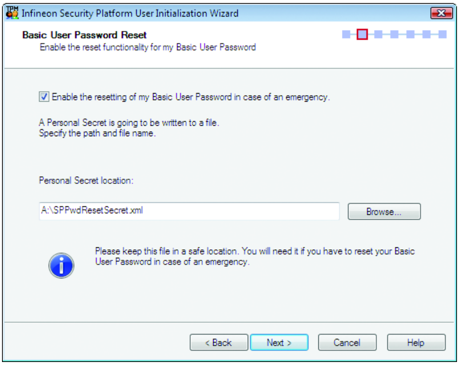
Please set your Basic User Password. This password will protect your Basic User Key.

Password: ••••••

Confirm Password: ••••••

Your password has to meet the following requirements:
Length: Between 6 and 256 characters.

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**.



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.

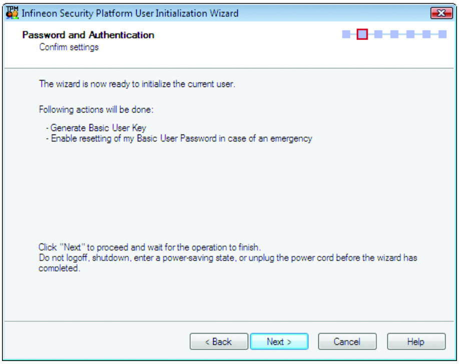
A Personal Secret is going to be written to a file.
Specify the path and file name.

Personal Secret location:

A:\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.



Password and Authentication
Confirm settings

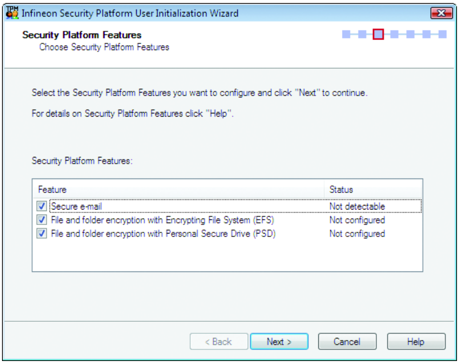
The wizard is now ready to initialize the current user.

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.

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



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 with Encrypting File System (EFS)	Not configured
☑ File and folder encryption with 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 with 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.

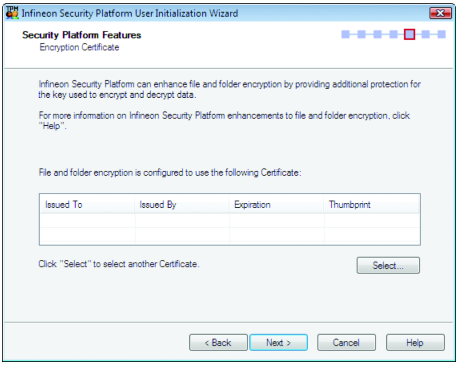
NOTE **EFS is not supported in Windows Vista Home Basic, Vista Home Premium and XP Home Editions.**

File and folder encryption with 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 with Personal Secure Drive (PSD)** as the example:
To configure "Encryption Certificate", click **Select**.



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.

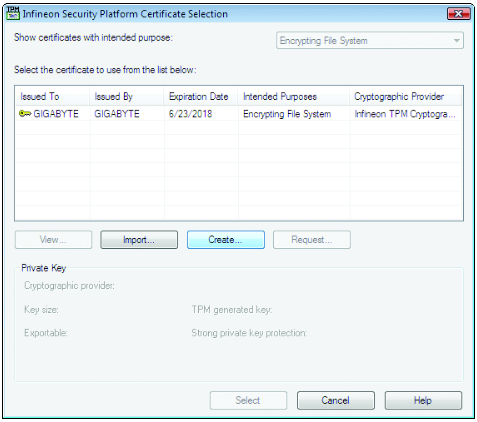
For more information on Infineon Security Platform enhancements to file and folder encryption, click "Help".

File and folder encryption is configured to use the following Certificate:

Issued To	Issued By	Expiration	Thumbprint

Click "Select" to select another Certificate.

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



Infineon Security Platform Certificate Selection

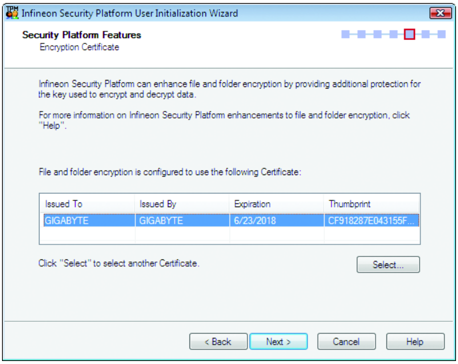
Show certificates with intended purpose: Encrypting File System

Select the certificate to use from the list below:

Issued To	Issued By	Expiration Date	Intended Purposes	Cryptographic Provider
GIGABYTE	GIGABYTE	6/23/2018	Encrypting File System	Infineon TPM Cryptogra...

Private Key
Cryptographic provider:
Key size:
TPM generated key:
Exportable:
Strong private key protection:

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".

File and folder encryption is configured to use the following Certificate:

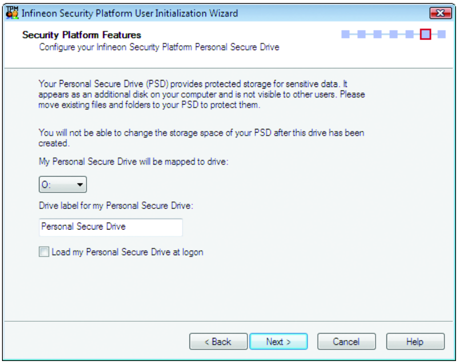
Issued To	Issued By	Expiration	Thumbprint
GIGABYTE	GIGABYTE	6/23/2018	CF918287E043155F...

Click "Select" to select another Certificate.

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**.



Security Platform Features

Configure your Infineon Security Platform 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.

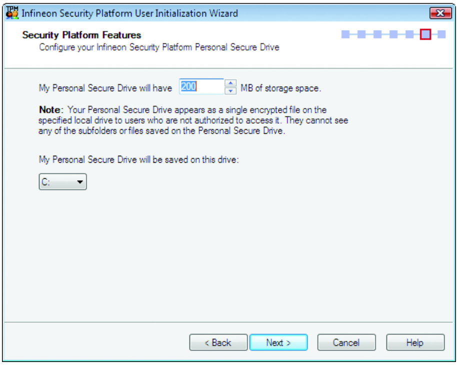
You will not be able to change the storage space of your PSD after this drive has been created.

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

Drive label for my Personal Secure Drive: Personal Secure Drive

□ Load my Personal Secure Drive at logon

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



Security Platform Features

Configure your Infineon Security Platform Personal Secure Drive

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

Note: Your Personal Secure Drive appears as a single encrypted 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.

My Personal Secure Drive will be saved on this drive: C:

NOTE

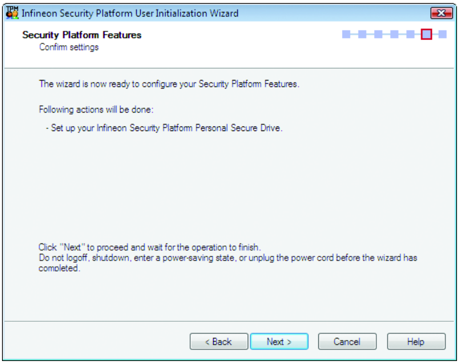
Your Personal Secure Drive size cannot be changed after setup, so please ensure that the size you specify is large enough to meet your needs. Please note that you cannot use the full drive size, since the file system allocates some space. This depends on the operating system and may be significant for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



Infineon Security Platform User Initialization Wizard

Security Platform Features
Confirm settings

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

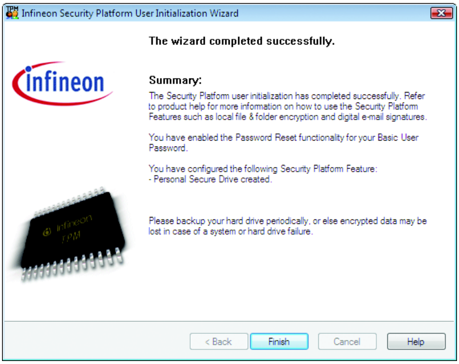
Following actions will be done:

- 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.

CAUTION **Do not logoff, 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.



Infineon Security Platform User Initialization Wizard

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.

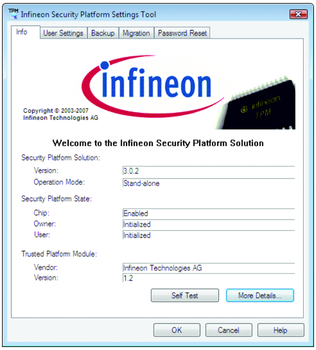
You have enabled the Password Reset functionality for your Basic User Password.

You have configured the following Security Platform Feature:
- 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.

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.



Infineon Security Platform Settings Tool

Copyright © 2003-2007
Infineon Technologies AG

Welcome to the Infineon Security Platform Solution

Security Platform Solution:
Version: 3.0.2
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 GIGABYTE Ultra TPM Utility

GIGABYTE's unique Ultra TPM (Trusted Platform Module) supports the industry's most advanced TPM hardware-based encryption. With the easy-to-use Ultra TPM user interface, users can store/back up their digital signature keys on a USB flash drive or in the system BIOS. The key(s) will be erased from the computer after being stored on a USB flash drive (or in the system BIOS), preventing unauthorized access to the computer. By simply plugging or unplugging the USB flash drive, users are able to access their PSD files without the hassles of complicated configurations. In addition, Ultra TPM's key backup function allows users to still have a way to access their data in case the keys are lost.

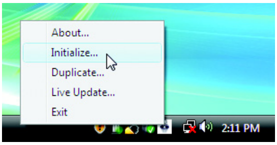
- **After creating the password(s) and key(s) associated the TPM, be sure to store them in a secure location and back them up. Loss of the password(s) or the key(s) will render the files encrypted via the TPM unable to be cracked or read.**
- **Though the TPM delivers the latest data security technology,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

4.1. Instructions for Using Ultra TPM

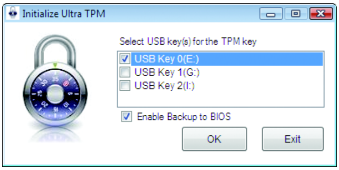
Before launching the Ultra TPM utility, make sure the TPM chip has been initialized and you have encrypted the files you want. (You have to at least set up a Personal Secure Drive (PSD). Refer to **3. Initializing the TPM Chip** to see how to set up a PSD.)

A. Initialize...

Step 1:
After installing the Ultra TPM utility, the Ultra TPM icon will appear in your system tray.
To create a Portable User Key, right-click on the icon and select **Initialize**.



Step 2:
When the **Initialize Ultra TPM** dialog box appears, select a USB flash drive and click the **Enable Backup to BIOS** check box, or select at least two USB flash drives. Click **OK** to continue.


Initialize Ultra TPM

Select USB key(s) for the TPM key

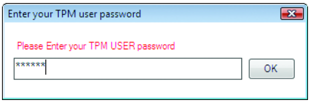
☑ USB Key 0(E:)
□ USB Key 1(G:)
□ USB Key 2(I:)

☑ Enable Backup to BIOS

When more than one user stores their keys in the BIOS, the latter key will overwrite the former key.

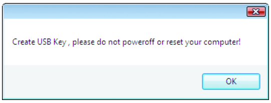
Step 3:

Enter the User Password created in "Easy Mode" or "Advanced Mode." Click **OK** to continue.


Enter your TPM user password

Please Enter your TPM USER password

******

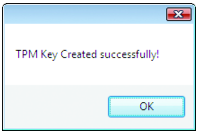

Create USB Key , please do not poweroff or reset your computer!

If you incorrectly enter the password three times, Ultra 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."

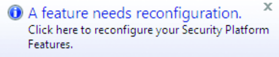
DO NOT turn off or restart the computer when a user key is being generated.

Step 4:

Click **OK** to exit and complete the creation of the Portable User Key. You are able to load or unload your PSD by simply plugging or unplugging the USB flash drive.


TPM Key Created successfully!

After completing the settings and when removing the USB flash drive(s), the Infineon Security Platform Settings Tool will give the following warning message, which is normal.

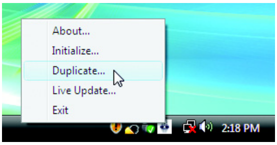

A feature needs reconfiguration.

Click here to reconfigure your Security Platform Features.

B. Duplicate...

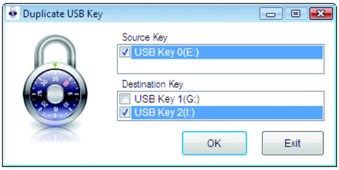
Step 1:

To duplicate the key to another USB flash drive, right-click on the Ultra TPM icon and select **Duplicate**.



Step 2:

When the **Duplicate USB Key** dialog box appears, select the drive letter of the source USB flash drive and then select the drive letter of the destination USB flash drive. Click **OK** to continue.


Duplicate USB Key

Source Key

☑ USB Key 0(E:)

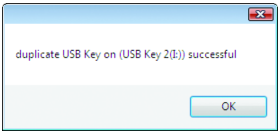
Destination Key

□ USB Key 1(G:)

☑ USB Key 2(I:)

Step 3:

Click **OK** to complete the duplication of the key.


duplicate USB Key on (USB Key 2(I:)) successful

If you want to uninstall the Ultra TPM software, be sure to insert the USB flash drive containing the Portable User Key into your computer before the uninstallation.