# Ultra TPM

GIGABYTE's unique Ultra TPM (Trusted Platform Module) design comes with a built-in chip and hardware-based protection for encryption of data. The thoughtful Ultra TPM user interface allows users to create a portable user key that can secure data's confidentiality in a PC. Users can also store the key in the BIOS to avoid data decryption failure resulting from the loss of the key. Besides, BIOS featuring the patented GIGABYTE DualBIOS™ design gives double security to protect your system against virus attack and physical damage.

## A. Before installing Ultra TPM, follow the steps below in sequence:

Step 1:
Turn on your computer and enter the BIOS Setup program. Go to **Security Chip Configuration** and set **Security Chip** to **Enabled**. Then enter **Clear Security Chip** to clear all settings in the security chip. Refer to Chapter 2, "BIOS Setup," for instructions on configuring the security chip. Save changes and then restart your computer.

Step 2:
Install the Infineon TPM driver from the motherboard driver disk.

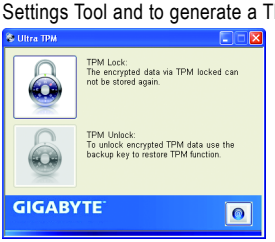
Step 3:
For Windows XP operating system, you need to install Microsoft .NET Framework (2.0 or later version) first.

Step 4:
Install the Ultra TPM utility from the motherboard driver disk.

## B. Instructions for using the Ultra TPM:

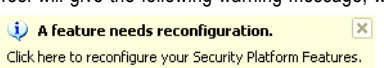
1. Before launching the Ultra TPM, go to the Infineon Security Platform Settings Tool to initialize the TPM chip and then encrypt the files you want. (You have to at least set up a Personal Secure Drive (PSD). Refer to the Infineon Security Platform Help file to see how to set up the PSD.)

2. The following screen appears when launching the Ultra TPM. Click the **TPM Lock** button . Follow the on-screen instructions to protect the files encrypted by the Infineon Security Platform Settings Tool and to generate a TPM key. You can save the key in a USB flash drive or in the BIOS.




NOTE

After completing the settings, the Infineon Security Platform Settings Tool will give the following warning message, which is normal.




3. To release the protected files, click the **TPM Unlock** button after launching the Ultra TPM. Then follow the on-screen instructions to complete the settings.