TRUSTED PLATFORM MODULE (TPM)

WHAT IS TPM?

The Trusted Platform Module (TPM) is a secure storage chip. It is used to store unique Public Key Infrastructure (PKI) key pairs and credentials. PKI is a commonly used method of data encryption in technological security. The TPM ensures a higher level of security by acting as a "safety box" to store the confidential data.

HOW DO I KNOW IF MY TOSHIBA NOTEBOOK HAS TPM?

TPM is a built-to-order specification (available on selected Tecra and Portégé models) that must be indicated when ordering a notebook. If you are not certain whether your machine has TPM, please consult your dealer or sales representative.

HOW DO I ENABLE TPM?

TPM is enabled through the BIOS setup screen. Set the TPM setting in the "Security Controller" section to "Enable".

HOW DO I SET UP A PERSONAL SECURE DRIVE?

The Personal Secure Drive (PSD) can be set up by using wizards. It is similar to a regular Windows drive, but it has a higher level of safety since it is protected by the TPM. To set up the PSD:

• Launch the "Start Security Platform User Initialization Wizard". This will display the "Infineon Security Platform Personal Secure Drive".
• Provide the TPM user password and click OK. This will display the Personal Security Drive.

BEST PRACTICES

SETTING A BIOS PASSWORD AND SUPERVISOR PASSWORD

Setting two passwords (BIOS and Supervisor) enhances the security of the Toshiba notebook. The BIOS password can be set up from either the BIOS screen or the Toshiba Password Utility. It prevents unauthorised access to the Toshiba notebook system before the system boots. The Supervisor password needs to be set up from the Toshiba Supervisor Password Utility. This password is used to protect TPM-related and other settings in the BIOS setup. Users without a Supervisor password cannot change these settings. This two-tier level of password protection results in a more secure Toshiba notebook.

EMERGENCY RECOVERY ARCHIVE AND TOKEN

Using the Emergency Recovery Archive and token is a good way to prevent data loss in the event of a computer failure. This process will recover TPM content but not TPM-related data (files in the built-in Hard-Disk Drive). These files should be backed up separately.

The Emergency Recovery Archive File stores all user security keys. This file should be backed up periodically to an external storage device in case the HDD ever becomes inaccessible. The Emergency Recovery Token is a key that is required to access the Emergency Recovery Archive file. This token file prevents unauthorised individuals from using the Emergency Recovery Archive file (which you have backed up) to restore the system.

Administrators should store the emergency recovery token file on an external storage device. If copies of the token file exist on the Hard Disk Drive, they should be deleted. This practice prevents data theft and unauthorised usage of files.

PSD BACKUP
The recovery agent should be enabled (set to "On") when using the PSD. This will protect the files in the PSD from data loss. For example, if the recovery agent is enabled and a computer failure occurs, the user files that were stored in the PSD can be extracted and recovered after the computer has been restored to normal service.

BACKUP OF TPM-RELATED DATA FOR EMERGENCY RECOVERY
TPM-related data refers to
• Files protected by the Encrypting File System (EFS)
• Files stored in the Hard Disk Drive (HDD)

These files cannot be recovered by the Emergency Recovery Process. This process will only recover TPM content, not TPM-related data. Therefore all TPM-related data should be backed up to an external storage device.

HELPFUL LINKS:
Toshiba EasyGuard mini-site
www.easyguard-info.com/