

Toshiba EasyGuard Carefree Mobile Computing



Toshiba EasyGuard is the better way to enhanced data security, advanced system protection and easy

connectivity. This next-generation computing experience incorporates technologies enabling optimal connectivity and security, Toshiba anti-accident innovations and advanced software utilities for carefree mobile computing.

Three core elements for carefree mobile computing

In addressing the need for enhanced data security, advanced system protection and easy connectivity, Toshiba EasyGuard features can be divided into three core elements:

- Secure** Features that deliver enhanced system and data security
- Protect & Fix** Protective design features and diagnostics utilities for maximum uptime
- Connect** Features and software utility that ensure easy and reliable wired and wireless connectivity



What is Trusted Platform Module?

Trusted Platform Module (TPM) is a secure storage chip for unique Public Key Infrastructure (PKI) key pairs and credentials. In other words, it is the ideal “safety box” where keys of encrypted data can be kept. A small security controller, TPM was developed to conform to industry standard specifications issued by the Trusted Computing Group (TCG) and it provides the standard for Computing Platform Security.



How it works

The majority of current security solutions are software based. Consequently, they do not provide sufficient security protection and are vulnerable to physical and/or logical attacks. TPM, on the other hand, is both a hardware and software-based security solution. It is a part of the notebook's booting process and is also integrated with the operating system. Physically separated from the main CPU, TPM is nevertheless bound to the main board of the notebook.

The hardware-based secure storage lies at the root of this solution. Upon generation of a key or certificate for encrypted data by system software, those keys and certificates are sealed in TPM. These stored information bits authenticate and provide information on the integrity of the platform when needed and inform the user and communication partners (e.g. content provider) of the status of the hardware and software environment. The status is provided based on the uniqueness of the platform, which, in turn, is based on the unique keys stored in the TPM.

Each TPM chip has a unique number, but the system authenticates a user by keys or IDs stored in TPM rather than by the unique number. As a result, TPM is capable of withstanding logical and physical attacks in order to protect the stored keys and credentials.



TPM solution from Infineon includes a security circuit and software that provides computing platforms with a safer subsystem.

The highest security level can be achieved by means of a 2-way authentication using a TPM chip for platform identification as well as a USB key or an SD token for user authentication. This 2-way authentication can only work separately as, for example, the SD token cannot be stored in TPM.

What are the applications that can be used with TPM?

- ▶ File and Folder Encryption
 - Windows EFS (Encrypting File System)
 - Virtual Encrypted Drive (Personal Secure Drive)
- ▶ Secure E-mail
 - Versions of Outlook, Outlook Express and Netscape Communicator that support Digital Signature and Mail Encryption/Decryption features.
- ▶ Secure WWW
 - Internet Explorer and Netscape Communicator that support Secure Protocols (SSL)
- ▶ Others
 - Virtual Private Network (VPN)
 - One Time Password (e.g. RSA SecurID)
 - Client Authentication

Summary of features and benefits

- ▶ TPM (Trusted Platform Module)
 - Protection of sensitive data, encryption and digital signatures to protect users content and privacy.
- ▶ Hardware and software-based solution
 - Ability to withstand logical and physical attacks to protect stored keys and credentials.
- ▶ Industry standard feature (e.g. TCG)
 - Usability across multiple platforms.