







**Tech Insight:**  
**Trusted Platform Module (TPM)**

**EasyGuard**  
Go *Mobile* With Confidence

Toshiba EasyGuard™ technology is a series of hardware and software enhancements to business-class notebooks that greatly improve mobile computing. By providing users with increased data security, system protection, simple connectivity and ease of use, EasyGuard™ technology is continued evidence of Toshiba’s vast experience in mobile computing and our ongoing commitment to providing users with a better, more reliable notebook experience.

Toshiba EasyGuard technology comprises a number of features some of which may or may not be available on a particular Toshiba notebook depending on the model selected. See [www.easyguard.toshiba.com](http://www.easyguard.toshiba.com) for detailed information.

**Toshiba EasyGuard™**  
Four core elements for more confident computing

-  **Protect & Fix**  
Fortifies vital information and vulnerable components against the stress and hazards mobile computers are exposed to every day.
-  **Secure**  
Helps defend your data and your notebook against loss, theft or viral attack.
-  **Connect**  
Helps you locate and establish a wired or wireless connection effortlessly and quickly.
-  **Optimize**  
Allows you to customize the notebook’s system performance so you can be more productive.

**What is the Trusted Platform Module?**

As business becomes increasingly mobile, it is more important than ever that mobile computer users protect their sensitive data from theft and misuse. The Trusted Platform Module (TPM) sets the new standard for computing platform security by safely holding passwords and keys, providing an extra layer of protection for notebook users on the go.

**How it works**

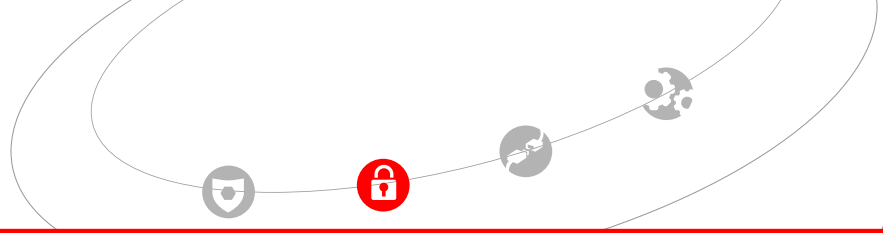
The TPM is an embedded security chip that stores login information and passwords on the motherboard instead of in the PC memory, so data cannot be accessed or seen by anyone but an authorized user. So not only does it encrypt sensitive data, it essentially hides the key to the vault storing the information. Integrated into the booting process, as well as in the operating system, the TPM can withstand virtual and physical attacks to protect critical information.



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

Based on an industry-standard specification issued by the Trusted Computing Group (TCG), the TPM seals keys and certificates within hardware-based secure storage. The TPM uses two-factor authentication, the first factor being the credentials stored inside the TPM and the second factor, the user password. Essentially, the TPM acts as the gatekeeper between the user/application and the data, providing extra protection by requiring a password to confirm that the user/application is authorized to access data, secure email and more.

Users and IT managers can achieve a higher level of security with two-factor authentication by utilizing an SD or USB-based token in lieu of a password, which enables a more complex credential protection scheme.



## 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 Email
  - 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<sup>1</sup>
  - Virtual Private Network (VPN)
  - One-Time Password (e.g., RSA SecurID)
  - Client Authentication

## Summary of features and benefits

### Embedded security

- The TPM is an embedded security chip that acts as a secure vault for encryption keys, passwords and user credentials
- A Personal Secure Drive provides an encrypted location for storage of critical and sensitive data or documents
- Transparent encryption and decryption of documents helps ensure minimal impact on system performance

### Ease of use

- Easy user setup and management via intuitive application wizards
- Easy file protection with the Personal Secure Drive, which functions like a Microsoft® Windows® drive

For additional information, visit [www.trustedcomputinggroup.org](http://www.trustedcomputinggroup.org)

<sup>1</sup>. Requires additional third-party applications and/or devices.