

Toshiba EasyGuard
L'informatique **mobile** sans soucis



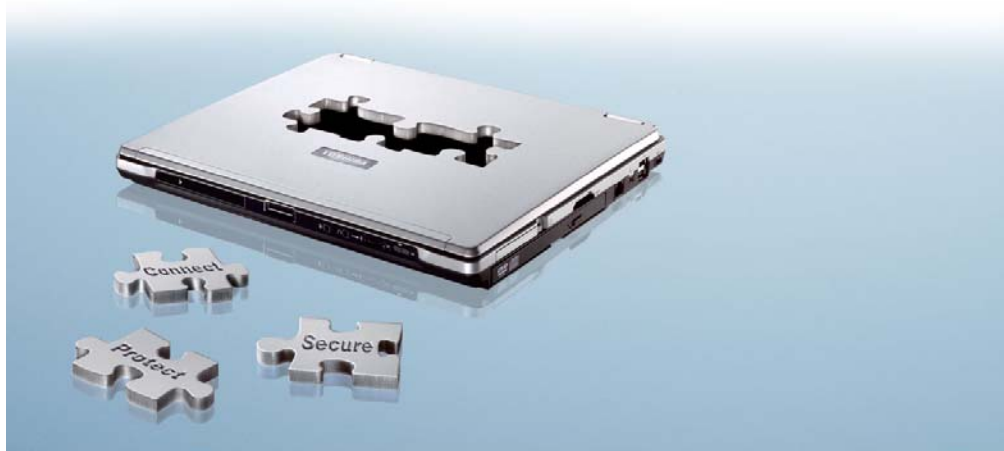
Toshiba EasyGuard est la meilleure solution en matière de

sécurité des données, de protection avancée des systèmes et de connectivité simplifiée. Cette solution informatique nouvelle génération inclut des technologies d'optimisation de la connectivité et de la sécurité : des dispositifs anti-accidents et des utilitaires logiciels avancés destinés à l'informatique mobile.

Trois éléments fondamentaux de l'informatique mobile sans soucis

En matière de sécurisation accrue des données, de protection des systèmes et de simplification de la connectivité, on peut répartir les fonctions de Toshiba EasyGuard en trois groupes principaux :

Sécurité Des fonctions fournissant une sécurité des systèmes et des données accrue.



Protection Des utilitaires de diagnostic et des fonctions de protection optimisant la durée de disponibilité des équipements.

Connectivité Des fonctions et des utilitaires logiciels offrant une connectivité avec ou sans fil, fiable et simplifiée.

Qu'est ce que le TPM (Trusted Platform Module, module de plate-forme sécurisée) ?

Le TPM est une puce de stockage sécurisé pour les identifiants et les clés doubles d'infrastructure à clé publique. En d'autres termes, il s'agit d'un « coffre-fort » idéal dans lequel les clés et données chiffrées peuvent être sauvegardées. Le TPM, petit contrôleur de sécurité, a été conçu pour rendre les systèmes conformes aux normes industrielles éditées par le TCG (Trusted Computing Group) et respecte la norme pour la sécurité des plates-formes informatiques (Computing Platform Security).



Fonctionnement

La majorité des solutions de sécurité actuelles se basent sur une application logicielle. Par conséquent, ces solutions n'offrent pas de protection suffisante face aux attaques logiques et/ou physiques. Le TPM, lui, propose une solution sécurité à la fois logicielle et matérielle. Il fait partie du processus d'amorçage de l'ordinateur portable et est intégré au système d'exploitation. Bien qu'il soit physiquement séparé de l'unité centrale principale, le TPM est néanmoins relié à la carte mère de l'ordinateur.

Le stockage sécurisé basé sur le matériel est au cœur de cette solution. Contrairement aux applications logicielles qui nécessitent la génération de clés et de certificats pour les données chiffrées, le TPM, lui, intègre totalement ces clés et certificats. Ces informations enregistrées authentifient et fournissent des informations relatives à l'intégrité de la plate-forme lorsque cela est nécessaire et informent l'utilisateur et les partenaires communication (fournisseurs d'informations) de l'état de l'environnement matériel et logiciel. Cet état est fourni en fonction de l'unicité de chaque plate-forme, qui, à son tour se base sur les clés uniques enregistrées dans le TPM.

Chaque puce du module possède son propre numéro, mais le système authentifie un utilisateur à l'aide des clés ou des ID enregistrés dans le TPM et non d'après ce numéro unique. De cette façon, le TPM est capable de résister aux attaques physiques et logiques afin de protéger les clés et identifiants enregistrés.

Le niveau de sécurité le plus important est atteint grâce à un double moyen d'identification : une puce TPM pour l'identification de la plate-forme et une clé USB ou une carte SD pour l'authentification de l'utilisateur. Ces deux moyens d'authentification fonctionnent indépendamment étant donné que la carte SD ne peut pas être enregistré sur le TPM.



Le module de sécurité conçu par Infineon comprend un circuit de sécurité et une application logicielle offrant un sous-système plus sûr à votre plate-forme informatique.

Quelles applications peuvent être utilisées avec le TPM ?

- ▶ **Cryptage de fichiers et dossiers** Windows EFS (Encrypting File System, système de cryptage de fichiers)
Lecteur virtuel crypté (lecteur personnel sécurisé)
- ▶ **Courrier électronique sécurisé** Versions de Outlook, Outlook Express et Netscape Communicator prenant en charge les fonctions de signature numérique et de cryptage du courrier électronique.
- ▶ **Web sécurisé** Internet Explorer et Netscape Communicator prenant en charge les protocoles SSL
- ▶ **Autres** Virtual Private Network (VPN)
One Time Password, mot de passe unique (RSA SecurID)
Authentification client

Résumé des fonctions et de leurs avantages

- ▶ **TPM (Trusted Platform Module, module de plate-forme sécurisée)** Protection des données sensibles, cryptage et signatures numériques afin de protéger le contenu des informations personnelles de l'utilisateur.
- ▶ **Solution matérielle et logicielle** Capacité à résister aux attaques logiques et physiques pour protéger les clés et références enregistrées.
- ▶ **Fonction de mise aux normes industrielles (TCG)** Possibilité d'utilisation sur plusieurs plates-formes.