ToshibaEasyGuard
Movilidad sin problemas

Toshiba EasyGuard es la mejor opción para disfrutar de una mayor seguridad de los datos, una protección avanzada del sistema y una conectividad sencilla. Esta avanzada experiencia informática incorpora tecnologías que ofrecen una conectividad y seguridad óptimas, novedades de Toshiba que previenen los accidentes y herramientas de software avanzadas para sistemas portátiles desatendidos.

Tres elementos clave para sistemas portátiles desatendidos

En lo que respecta a su respuesta a la demanda de una mayor seguridad de los datos, protección avanzada del sistema y conectividad sencilla, las características de Toshiba EasyGuard se pueden dividir en tres elementos principales:

Seguridad — Características que proporcionan una mayor seguridad del sistema y los datos

Protección y reparación — Características diseñadas para la protección y herramientas de diagnóstico que ofrecen el máximo tiempo de actividad

Conexión — Características y herramientas de software que garantizan una conectividad cableada e inalámbrica sencillas y fiables

¿Qué es Trusted Platform Module?

Trusted Platform Module (TPM) es un chip de almacenamiento seguro de pares de claves y credenciales PKI (Infraestructura de claves públicas) únicos. En otras palabras, es la "caja fuerte" ideal donde se pueden guardar las claves de datos cifrados.
El pequeño controlador de seguridad TMP se desarrolló para cumplir las especificaciones del estándar del sector publicadas por Trusted Computing Group (TCG), que proporciona el estándar de seguridad de plataformas para equipos informáticos.

Así funciona

La mayoría de las soluciones de seguridad actuales se basan en software. En consecuencia, no proporcionan una protección de seguridad suficiente y son vulnerables a los ataques físicos o lógicos. Sin embargo, TPM es una solución de seguridad basada en hardware y software. Forma parte del proceso de inicio del equipo portátil y también se integra con el sistema operativo. A pesar de estar físicamente separado de la CPU principal, el TPM va unido al circuito principal del portátil.

La raíz de esta solución se encuentra en el almacenamiento seguro basado en hardware. Cuando el software del sistema genera una clave o un certificado para datos cifrados, esas claves y certificados se sellan en el TPM. Los bits de información almacenada autentican y proporcionan información sobre la integridad de la plataforma cuando es necesario, e informan al usuario y a los socios de comunicación (por ejemplo, al proveedor de contenido) del estado del entorno de hardware y software. El estado se proporciona sobre la base de la exclusividad de la plataforma que, a su vez, se basa en las claves únicas almacenadas en el TPM.

La solución TPM de Infineon incluye un circuito y software de seguridad que ofrece a las plataformas de sistemas informáticos un subsistema más seguro.

Cada chip TPM tiene un número único, pero el sistema autentica al usuario mediante las claves o los identificadores (ID) almacenados en el TPM, no por el número único.

Como resultado, el TPM puede soportar los ataques lógicos y físicos para proteger las claves y credenciales almacenadas.

El nivel de seguridad más alto se puede obtener por medio de una autenticación bidireccional que consiste en utilizar un chip TPM para la identificación de la plataforma y una autenticación del usuario en forma de clave USB o testigo (token) SD. Esta autenticación bidireccional sólo funciona por separado, ya que, por ejemplo, el testigo SD no se puede almacenar en el TPM.

¿Qué aplicaciones se pueden utilizar con TPM?

▶ Cifrado de archivos y carpetas	• Windows EFS (Sistema de archivos de cifrado) • Unidad cifrada virtual (unidad segura personal)
▶ Correo electrónico seguro	Versiones de Outlook, Outlook Express y Netscape Communicator que admiten las características de firma digital y cifrado/descifrado de correo.
▶ WWW seguro	Versiones de Internet Explorer y Netscape Communicator que admiten protocolos de seguridad (SSL)
▶ Otros	• Red privada virtual (VPN) • Contraseña de utilización única (por ejemplo, RSA SecurID) • Autenticación de clientes

Resumen de características y ventajas

▶ TPM (Trusted Platform Module)	Protección de datos críticos, cifrado y firmas digitales para proteger el contenido y la privacidad de los usuarios
▶ Solución basada en hardware y software	Capacidad de soportar ataques lógicos y físicos para proteger las claves y credenciales almacenadas
▶ Característica estándar del sector (por ejemplo, TCG)	Se puede utilizar en varias plataformas