ToshibaEasyGuard
CarefreeMobileComputing

Toshiba EasyGuard is dé oplossing voor uitgebreide gegevensbeveiliging, geavanceerde systeembescherming en gebruiksvriendelijke verbindingsmogelijkheden. Deze hypermoderne computerervaring bevat technologie voor optimale verbindingsmogelijkheden en beveiliging, alsmede innovaties van Toshiba om fysieke schade aan de notebook te beperken en bevat bovendien geavanceerde software voor probleemloos mobiel computergebruik.

Drie kernsegmenten voor probleemloos mobiel computergebruik

De oplossing die Toshiba EasyGuard biedt ten behoeve van uitgebreide gegevensbeveiliging, geavanceerde systeembescherming en gebruiksvriendelijke verbindingsmogelijkheden kunnen in drie kernsegmenten worden ingedeeld:

Beveiligen Features voor uitgebreide beveiliging van het systeem en de gegevens

Beschermen & repareren Ingebouwde features en diagnostische hulpprogramma's voor bescherming tegen systeemstoringen

Verbinden Features en software voor gebruiksvriendelijke en betrouwbare draadloze en bedrade verbindingsmogelijkheden

Wat is Trusted Platform Module?

Trusted Platform Module, oftewel TPM, is een chip voor het veilig opslaan van unieke Public Key Infrastructure (PKI) sleutelparen en legitimatiegegevens. In andere woorden: het is de ideale "kluis" voor het bewaren van de sleutels van gecodeerde gegevens. TPM is een kleine beveiligingscontroller die is ontwikkeld om te voldoen aan de gespecificeerde industriestandaarden zoals gepubliceerd door de Trusted Computing Group (TCG) en biedt de basis voor Computing Platform Security.

Hoe het werkt

Het merendeel van de huidige beveiligingsoplossingen is gebaseerd op een softwarematige aanpak. Hierdoor blijven ze kwetsbaar voor fysieke en/of logische aanvallen. TPM daarentegen is zowel een hardware- als softwarematige beveiligingsoplossing. TPM maakt deel uit van het opstartproces van de notebook en is tevens geïntegreerd met het besturingssysteem. Hoewel TPM geen deel uitmaakt van de processor, is het wel een onderdeel van het moederbord van de notebook.

TPM-oplossing van Infineon bestaat uit een beveiligingshardware en -software waardoor onderdelen van het computerplatform beter zijn beveiligd.

Een hardwarematige, veilige opslag is de basis van deze oplossing. Zodra de systeemsoftware een sleutel of certificaat aanmaakt voor gecodeerde gegevens, wordt de sleutel of het certificaat veilig opgesloten in de TPM. Deze opgeslagen informatiebits authenticeren en geven informatie over de integriteit van het platform wanneer dat nodig is en informeren de gebruiker en de communicatiepartners (bijvoorbeeld de content provider) over de status van de hardware- en softwareomgeving. De status wordt bepaald op basis van de unieke kenmerken van het platform, die op hun beurt weer zijn gebaseerd op de unieke sleutels opgeslagen in de TPM.

Elke TPM-chip heeft een uniek nummer, maar het systeem identificeert een gebruiker door sleutels of ID's opgeslagen in het TPM en niet door het unieke nummer. Dit heeft het voordeel dat de TPM niet gevoelig is voor logische en fysieke aanvallen op de opgeslagen sleutels en legitimatiegegevens.

Het hoogste beveiligingsniveau wordt gerealiseerd door middel van een tweeweg authenticatie waarbij het platform door een TPM-chip wordt geïdentificeerd en de gebruiker door gegevens op een USB-stick of SD-kaart. Deze tweeweg authenticatie kan alleen los van elkaar werken omdat bijvoorbeeld de identificatiegegevens van de SD-kaart niet in de TPM kunnen worden opgeslagen.

Welke toepassingen kunnen worden gebruikt met TPM?

▶ Versleuteling van bestand en folder	• Windows EFS (Encrypting File System) • Virtual Encrypted Drive (Personal Secure Drive)
▶ Veilige e-mail	Versies van Outlook, Outlook Express en Netscape Communicator die digitale handtekeningen en versleuteling van mail ondersteunen.
▶ Veilig WWW	Internet Explorer en Netscape Communicator die SSL ondersteunen (Secure Protocols)
▶ Overige	• Virtual Private Network (VPN) • Eenmalig wachtwoord (bijvoorbeeld RSA SecurID) • Authenticatie van clientcomputer

Samenvatting van kenmerken en voordelen

▶ TPM (Trusted Platform Module)	Bescherming van vertrouwelijke gegevens, versleuteling en digitale handtekeningen ter bescherming van de privacy en de gegevens van gebruikers
▶ Hardware- en softwarematige oplossing	Het kunnen weerstaan van logische en fysieke aanvallen op beveiligd opgeslagen sleutels en legitimatiegegevens
▶ Industriestandaard (bijv. TCG)	Te gebruiken op meerdere platformen