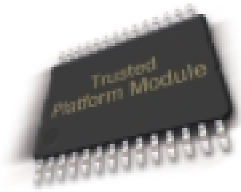
Protecting Your Vital Business Data with the Trusted Platform Module

Connected businesses deliver a universe of new capabilities and convenience to customers, employees, and IT. But connectivity also exposes your data assets to hackers or malicious insiders. To protect networked systems and data, most businesses opt for a security software deployment, because of its low cost and configuration flexibility. But the unfortunate fact is that relying on software alone puts your network at significant risk of successful attack or unauthorized penetration. Enhancing software solutions with security that is rooted in hardware can significantly improve your defenses and increase your peace of mind.



The Trusted Platform Module: Hardware-Based Protection for Business

The Trusted Platform Module (TPM) is a component on the PC motherboard that is specifically designed to enhance platform security above-and-beyond the capabilities of today's software. Defined by the Trusted Computing Group's public specification, the TPM provides hardware-based protection for the encryption and digital signature keys that secure your data's confidentiality. The TPM also provides a hardware-based authentication mechanism that strengthens existing network-access controls.

The Trusted Platform Module **provides a protected space for key operations and other security critical tasks that are not protected today. Using specifically designed hardware and software, the TPM secures encryption and signature keys at their most vulnerable stages—operations when the keys are being used unencrypted in plain-text form. The TPM is specifically designed to shield unencrypted keys and platform authentication information from software-based attacks.**

TPM Security Usages

Secure Operation	Software Vulnerability	Business Risk	Additional Protection Delivered by TPM Hardware
Encrypted e-mail	When decrypting a message using software, your private key is exposed unprotected in system memory, leaving it vulnerable to theft.	A hacker could use your private decryption key to access encrypted messages and data.	During decryption operations, your private key is protected inside the TPM hardware and is not exposed in system memory, reducing the risk of theft or attack.
Digital signature	When signing a document, your private signature key is stored unprotected in system memory.	A hacker with your private signature key could create legally binding forgeries with your digital signature.	During signing operations, your private signature key is protected inside the TPM hardware and is not exposed in system memory, reducing the risk of theft and digital forgeries.
File or folder encryption	Strong file encryption keys depend on a good source of random numbers. Software-generated random number algorithms are relatively weak.	Hackers could use an everyday PC to derive or "crack" an encryption key generated with a weak random-number mechanism and access the protected data.	The TPM contains a strong random number generator that meets the U.S. FIPS 140-1 standard to help create strong encryption keys. A brute-force attack on a TPM-generated key is computationally infeasible.
Platform authentication	The collection and computation of a platform's authentication is done entirely with application software, and is vulnerable to being intercepted and faked by a hacker.	A faked authentication could let a hacker gain access rights to restricted networks or sensitive data.	The TPM logs the platform's authentication information prior to operating system boot and secures it in hardware, making it computationally infeasible for a hacker to "impersonate" your platform.

The TPM and Business Software

Many of today's most popular business applications will benefit from the hardware-hardened protection offered by the TPM, without modification or upgrades. The TPM strengthens existing security mechanisms for Microsoft Office*, Outlook*, Internet Explorer*, Lotus Notes*, and Checkpoint* virtual private network, as well as any application using the industry-adopted cryptographic interfaces such as Microsoft's CAPI and RSA's PKCS#11. In addition, many vendors offer bundled security utilities and management tools to make using the TPM even more simple and convenient. Check with your system and software vendors for specific information about their TPM-enabled applications.

Specify TPM in Your Next PC

TPMs are available today in business desktop and mobile PCs from major system OEMs, as well as select motherboards in the reseller channel. Protect the confidentiality and integrity of your business by specifying that your next PC must include the TPM.

For more information:

http://www.intel.com/design/mobile/platform/downloads/Trusted_Platform_Module_White_Paper.pdf

Frequently Asked Questions

What is the Trusted Computing Group (TCG)?
The Trusted Computing Group is an industry standard body, formed to develop and support public industry specifications that enable secure computing across multiple platform types. The TCG incorporated in 2003 with members from 15 major system and application companies including Intel, IBM, Hewlett-Packard, AMD, and Microsoft. More information is available at www.trustedcomputinggroup.org.

Is my privacy protected when using a TPM?
Yes. TPM security is designed to be "opt-in" and under the owner's control at all times. The TPM specification dictates that the TPM not use any personal user identifiers and does not expose private information without the express permission of the owner.

Is the TPM designed as a Digital Rights Management (DRM) tool?
No. The TPM specification is designed to protect the owner's secrets and data from external software-based attacks and theft. The TPM architecture has no provision to enforce DRM of third-party content on the PC.

Who manufactures the TPM?
TPMs built to the TCG specification are offered by industry-leading semiconductor companies—including Atmel, Infineon, and National Semiconductor—and sold to system and motherboard OEMs. Although Intel does not make them, Intel supports the use of specification-compliant TPMs to help improve data security on PCs in today's connected businesses.

0903/TB/AY/HOP/15K
Part number: 253269-002