



How to Use the TPM: A Guide to Hardware-Based Endpoint Security

Taking advantage of the inherent security provided by the Trusted Platform Module (TPM)

Can you really feel sorry for a person whose car is stolen when the keys are left in it? Surprisingly, in a quite similar manner, many IT administrators are doing just that by not using a security feature they have. The Trusted Computing Group's root of trust, the Trusted Platform Module (TPM), is an integral part of virtually every enterprise level computer sold today.

The TPM, a secure cryptographic integrated circuit (IC), provides a hardware-based approach to manage user authentication, network access, data protection and more that takes security to higher level than software-based security. Perhaps surprisingly to many IT and operations staff, the TPM can be combined with widely used enterprise hardware such as network policy enforcement points, including [Checkpoint firewalls](#), Cisco switchers and routers, and other 802.1x-compatible devices.

For those wondering about standards, the International Standard Organization's (ISO) JTC1 (ISO/IEC Joint Committee 1) has approved the transposition of TCG's TPM 1.2 specification to an ISO/IEC standard. With the completion of the comments resolution process currently underway, publication of ISO/IEC 11889, Parts 1-4 is expected in the first half of 2009. This will make the TPM an even more well-established standard security tool, and yet, strangely, many organizations have not taken advantage of its capability.

Why Not?

Potential added cost and complexity are two of the most frequently cited reasons for not using the TPM. Since the TPM comes as standard equipment at very little or no additional cost on enterprise-level computers and there are over 100 million computers with a TPM, the potential for its presence within an organization is quite high. So the real issue must be complexity, or, as it turns out, perceived complexity. An example is the best way to disprove the complexity myth. It requires only four simple steps to enable and use the TPM.

Four steps to enable and use the TPM

- 1) Turn on the TPM from the BIOS.
- 2) Load available TPM utility software. Dell, HP, Lenovo and others include software applications for using the TPM in their business desktop and notebook products.
- 3) Enable the TPM and take ownership. This is the password that is used for permission to other functions including generate keys.
- 4) Use the TPM to generate Keys for a specific need such as fetching a virtual private network (VPN) Certificate using the Microsoft CA (Certificate Authority). To leverage the TPM, the Microsoft CA needs to be told which Cryptographic Service Provider (CSP) to use. Selecting advanced and then the CSP of choice will cause the Key pair to be generated using the TPM.

This is the first step to leverage the TPM's capabilities. Some vendors now offer applications that remotely provision the TPM and manage it, eliminating the need to "touch" each system. In this way, thousands of systems quickly can be made more secure.

Once the TPM is activated, users can easily encrypt files, folders and email as well as more securely manage passwords. To meet multi-factor authentication requirements, the TPM complements fingerprint readers and stores the keys associated with them securely, and the TPM can be used with a smart card reader.

Computer manufacturers and Microsoft provide detailed how-to instructions to enable and use the TPM more extensively including:

[HP-UX Trusted Computing Services Administrator's Guide HP-UX 11i v2](#) from Hewlett Packard and [A Step-by-Step Guide to Enable Windows BitLocker Drive Encryption](#) from Microsoft.

Acer, [Dell](#), Fujitsu Ltd., [Gateway](#), Lenovo (IBM), Toshiba and other computer suppliers that ship computers with TPMs have similar how-to information. The sidebar below, “**Things to Do with the TPM**” shows the minimum effort that should be made to implement the TPM’s capability. However, this is just the beginning. Other suppliers provide software and applications tools to simplify taking advantage of enhanced security that the TPM provides. A small sample of other tools available from key manufacturers for the TPM includes:

- [Core TCG Software Stack](#) from NTRU Cryptosystems
- [Embassy Trust Suites](#) and [EMBASSY Remote Administration Server \(ERAS\)](#) from Wave Systems
- [Additional Developer Resource tools](#) from TCG Members

With the TPM as an integral part of existing computers and support from other enterprise hardware such as Cisco routers, concentrators and switches as well as Checkpoint firewalls that natively support public key infrastructure (PKI) authentication, this software can take enterprise security to a much higher level.

IT administrators can take the certificate authentication (CA) that is native in their networking gear and move those certificate authentication software components down to hardware. When users log on to the domain or network, the authentication is performed based on the user providing a credential to the hardware on the machine. This provides hardware-based authentication to wireless networks and virtual private networks (VPNs), while removing the potential of users sharing keys.

Once the TPM is enabled, the Systems Management Server (SMS) and traditional enterprise tools can push certificates down using SMS and the active directory and harden the certificates down to the platform minimizing subsequent user interaction. Instead of enabling the TPM machine by machine, infrastructure tools can help enterprises enhance network and data security.

With a renewed thrust to make potential users aware of the TPM, its capabilities and ease of use, TCG is enlisting the use of tools such as the [TCG Blog](#), blogs at other sites such as [Intel vPro Expert Center](#), its members’ sites including online videos such as the Intel [Manageability Engine](#) that uses the TPM, University support such as the [Massachusetts Institute of Technology](#), [University of Birmingham](#), and many others, as well as third parties to provide how-to examples.

Things to Do with the TPM

- Set password
- Store digital credentials such as passwords in a hardware-based vault
- Manage keys with the TPM
- Augment smart cards, fingerprint readers and fobs for multi-factor authentication
- Encrypt files and folders to control access
- Establish state information to enable endpoint integrity
- Hash state information prior to hard drive shutdown for endpoint integrity
- Enable more secure VPN, remote and wireless access
- Use in conjunction with Full Disk Encryption to restrict access to sensitive data