



The Trusted Platform Module (TPM) and Implementation 2005

What is a TPM?

The TPM is a microcontroller that stores keys, passwords and digital certificates. It typically is affixed to the motherboard of a PC. It potentially can be used in any computing device that requires these functions. The nature of this silicon ensures that the information stored there is made more secure from external software attack and physical theft. Security processes, such as digital signature and key exchange, are protected through the secure TCG subsystem. Access to data and secrets in a platform could be denied if the boot sequence is not as expected. Critical applications and capabilities such as secure email, secure web access and local protection of data are thereby made much more secure.

Who provides these TPMs?

TPMs currently are provided by Atmel, Broadcom, Infineon, Sinosun, STMicroelectronics, and Winbond in discrete and integrated forms.

What about smaller devices that might not have the real estate or cost structure to support a separate piece of silicon for TPM functions?

TCG and its work groups are evaluating this issue and may end up offering vendors options in providing the functionality of the TPM for various devices. Vendors also can package the TPM or provide I/O suitable for systems other than PCs – the TCG specification is flexible in this regard. For example, some vendors already offer TPM functionality integrated into other chips.

What applications and services will benefit from systems with TPMs?

Systems with TPMs offer improved, hardware-based security in numerous applications, such as file and folder encryption, local password management, S-MIME e-mail, VPN and PKI authentication and wireless authentication for 802.1x and LEAP.

Are systems with TPMs available?

Desktop, notebook and tablet PCs with TPMs are available from Dell, Fujitsu, HP, Intel, Lenovo, Toshiba and others.

What are the plans for TCG conformance?

A certification and compliance program is in review. TCG will define programs that best fit market needs and specifications.

Do the TPM specifications require a certain cryptographic algorithm (DES, AES, etc.)?

Yes. They require RSA SHA-1 and HMAC. AES is not required in v1.1 of the specification, but may be required in future versions. The use of symmetric encryption is not required in the TPM. TCG will continue to evaluate developments in cryptographics.

How do TPMs compare with smart cards or biometrics?

They are complementary to the TPM, which is considered a fixed token that can be used to enhance user authentication, data, communications, and/or platform security. A smart card is a portable token traditionally used to provide more secure authentication for a specific user across multiple systems, while biometrics are providing that functionality in an increasing number of systems. Both technologies can have a role in design of more secure computing environments.

What role does Trusted Computing and the TPM play in authentication?

The TPM provides secure storage and key generation capabilities, similar to other hardware authentication devices, so it can be used to create and/or store both user and platform identity credentials for use in authentication. The TPM can also protect and authenticate user passwords, thereby providing an effective solution of integrating strong, multifactor authentication directly into the computing platform. With the addition of complementary technologies such as smart cards, tokens and biometrics, the TPM enables true machine and user authentication.

Can the Trusted Platform Module control what software runs?

No. There is no ability to do this. The subsystem can only act as a 'slave' to higher level services and applications by storing and reporting pre-runtime configuration information. Other applications determine what is done with this information. At no time can the TCG building blocks 'control' the system or report the status of applications that are running.

Is TCG creating specifications for just one operating system or type of platform?

No. Specifications are operating system agnostic. Several members have Linux-based software stacks available. In addition to our work on the PC platform, we have a specification for Trusted Servers and are working to finalize specifications for other computing devices, including peripherals, mobile devices, storage and infrastructure.

Does TCG require that software be certified to run on a TCG-enabled platform?

The TCG design does not have any requirement that software be "certified" in order to use it. The specification talks in some length about ways of using the platform to create certificates for keys that are provably secure and yet not identify the platform they came from. TCG's technology has a passive role in a system. It can be used to securely record data and to securely store (and sign with) digital keys.

TCG architecture does not specify where to get these certificates or how much you pay for them. Free certificates work as well as certificates you pay for. There is no single source of certificates in the market today. Anyone can set themselves up as a Certificate Authority using any number of different Certificate Authority packages. TCG has recently put together an Infrastructure Work Group to look into some of the use cases to provide possible working models.