

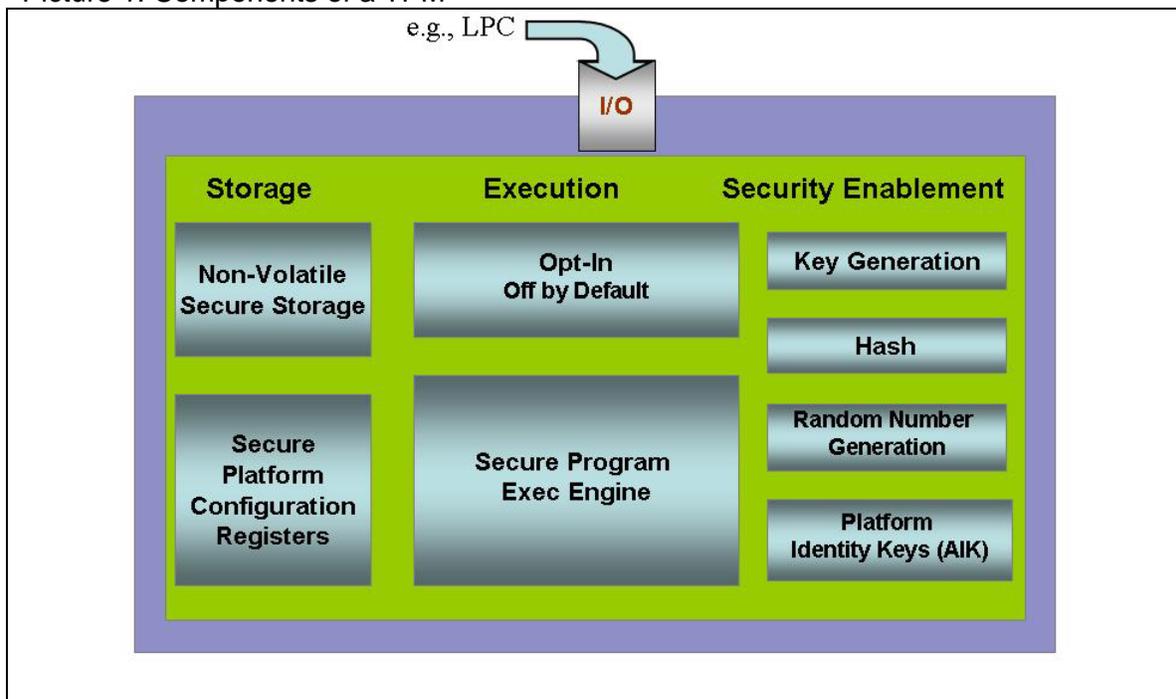


## Trusted Platform Module (TPM) Summary

TPM (Trusted Platform Module) is a computer chip (microcontroller) that can securely store artifacts used to authenticate the platform (your PC or laptop). These artifacts can include passwords, certificates, or encryption keys. A TPM can also be used to store platform measurements that help ensure that the platform remains trustworthy. Authentication (ensuring that the platform can prove that it is what it claims to be) and attestation (a process helping to prove that a platform is trustworthy and has not been breached) are necessary steps to ensure safer computing in all environments.

Trusted modules can be used in computing devices other than PCs, such as mobile phones or network equipment.

Picture 1: Components of a TPM



The nature of hardware-based cryptography ensures that the information stored in hardware is better protected from external software attacks. A variety of applications storing secrets on a TPM can be developed. These applications make it much harder to access information on computing devices without proper authorization (e.g., if the device was stolen). If the configuration of the platform has changed as a result of unauthorized

activities, access to data and secrets can be denied and sealed off using these applications.

However, it is important to understand that TPM cannot control the software that is running on a PC. TPM can store pre-run time configuration parameters, but it is other applications that determine and implement policies associated with this information.

Processes that need to secure secrets, such as digital signing, can be made more secure with a TPM. And mission critical applications requiring greater security, such as secure email or secure document management, can offer a greater level of protection when using a TPM. For example, if at boot time it is determined that a PC is not trustworthy because of unexpected changes in configuration, access to highly secure applications can be blocked until the issue is remedied (if a policy has been set up that requires such action). With a TPM, one can be more certain that artifacts necessary to sign secure email messages have not been affected by software attacks. And, with the use of remote attestation, other platforms in the trusted network can make a determination, to which extent they can trust information from another PC. Attestation or any other TPM functions do not transmit personal information of the user of the platform.

These capabilities can improve security in many areas of computing, including e-commerce, citizen-to-government applications, online banking, confidential government communications and many other fields where greater security is required. Hardware-based security can improve protection for VPN, wireless networks, file encryption (as in Microsoft's BitLocker) and password/PIN/credentials' management. TPM specification is OS-agnostic, and software stacks exist for several Operating Systems.

TPMs (current version is 1.2) use the following cryptographic algorithms: RSA, SHA1, and HMAC..

The Trusted Computing Group (TCG) is an international de facto standards body of approximately 140 companies engaged in creating specifications that define PC TPMs, trusted modules for other devices, trusted infrastructure requirements, APIs and protocols necessary to operate a trusted environment. After specifications are completed, they are released to the technology community and can be downloaded from the TCG Web Site.

Without standard security procedures and shared specifications, it is not possible for components of the trusted environment to interoperate, and trusted computing applications cannot be implemented to work on all platforms. A proprietary solution cannot ensure global interoperability and is not capable of providing a comparable level of assurance due to more limited access to cryptographic and security expertise and reduced availability for a rigorous review process. From the point of view of cryptography, for interoperability with the other elements of the platform, other platforms, and infrastructure, it is necessary for trusted modules to be able to use the same cryptographic algorithms. Although standard published algorithms may have weaknesses, these algorithms are thoroughly tested and are gradually replaced or improved when vulnerabilities are discovered. This is not true in the case of proprietary algorithms.

According to market research reports, over 100 million branded PCs and laptops with TPMs were sold in 2007. Server produces are beginning to ship, and a variety of

applications based on TPM, such as secure email or file encryption, have been implemented using TCG specifications. Trusted Network Connect (TNC) products that use TCG principles to enhance the security of communications are shipping, too. Draft specifications for storage (for hard drives) and mobile trusted modules (for mobile telephones) have been released.

For more information on applications for the TPM, see [https://www.trustedcomputinggroup.org/news/Industry\\_Data/TPM\\_applications\\_paper\\_March\\_28\\_2008.pdf](https://www.trustedcomputinggroup.org/news/Industry_Data/TPM_applications_paper_March_28_2008.pdf). Other white papers and documents are accessible via the organization's website, <https://www.trustedcomputinggroup.org/>.