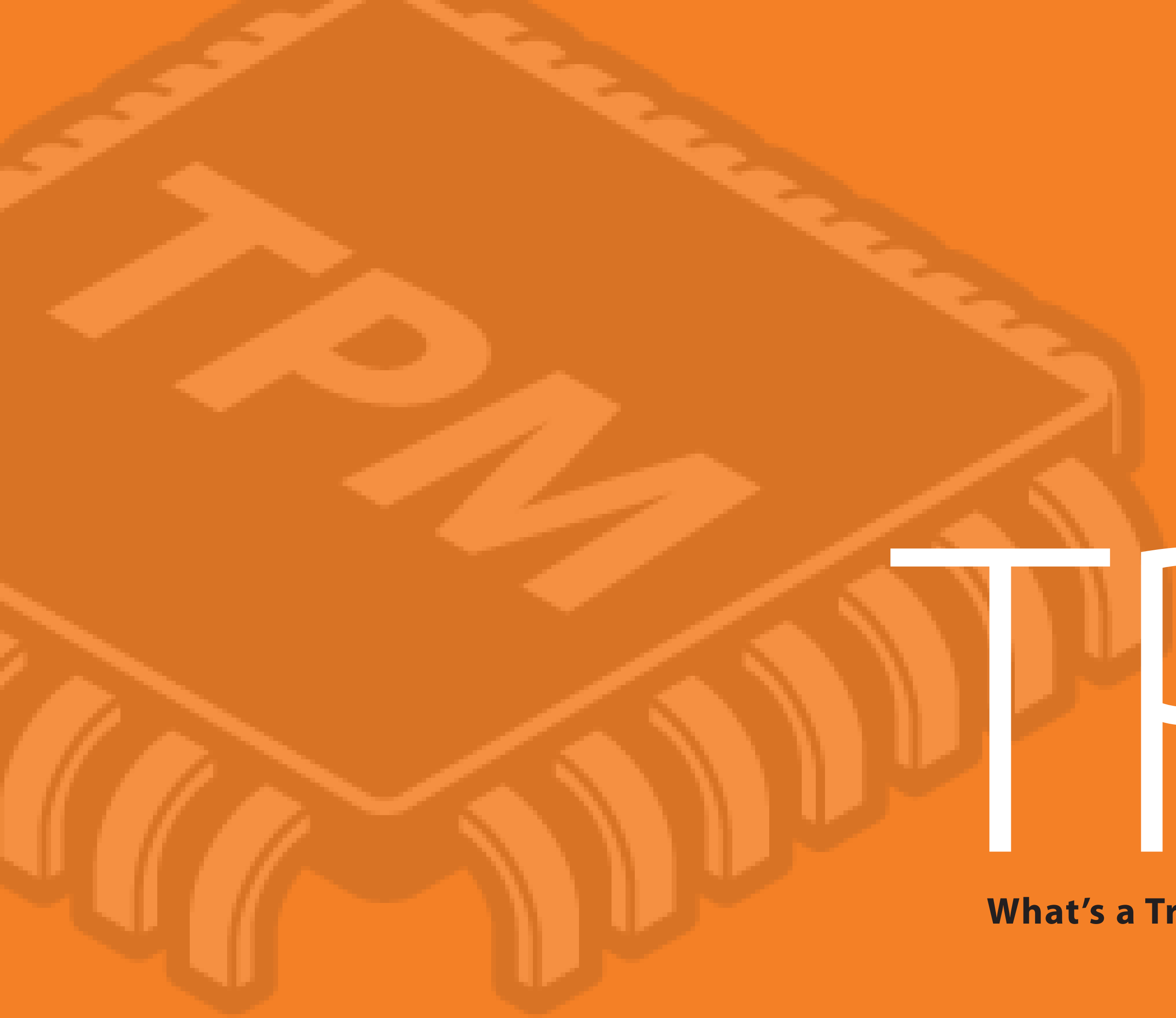
wave®



TPM

What’s a Trusted Platform Module?

> *“You may find your organization is in a similar situation to PwC, which may lead you to use TPM for strong authentication.”*
>
> *- Karl Wagner, PwC, Director, Global IT*

What is a TPM?

A Trusted Platform Module (TPM) is a standards-based security chip that's built into most of your laptop and desktop computers. In fact, it has shipped in more than 600 million laptop and desktop computers from Acer, Dell, HP, Lenovo, Panasonic, Samsung and Toshiba.

The TPM is a secure micro-controller with cryptographic features that provides a root of trust and enables the secure generation of keys and the ability to limit the use of them (to signing / verification or encryption / decryption). It also serves as a secure container for key storage and can safeguard other data deemed too sensitive for software protection alone.

The TPM standard was created almost a decade ago by the Trusted Computing Group (TCG), an international security standards organization.

How does it work?

The basic advantages of a TPM over traditional software are that a TPM can generate keys, store secrets and take measurements all within the secure boundary of a physical hardware chip — independent of a PC's operating system and its core processor. This means that the TPM keys cannot be copied or exported, the secrets it stores cannot be stolen or used unknowingly and the measurements it takes cannot be altered by malware.

In addition, TPMs have significant advantages over other hardware security devices, like OTP tokens, smart cards and USB tokens. Unlike these other technologies, the TPM is actually a permanent part of a PC: it's soldered onto the motherboard. And because it is, a TPM is the only token able to create a unique and permanent identity for each computer on your network. Further, since the TPM sits below the attack surface of firmware, drivers, boot loader and OS, it can securely create baseline measurements that can be used to validate the integrity of the PC, before granting it access to your network.

Trust Your Network PCs

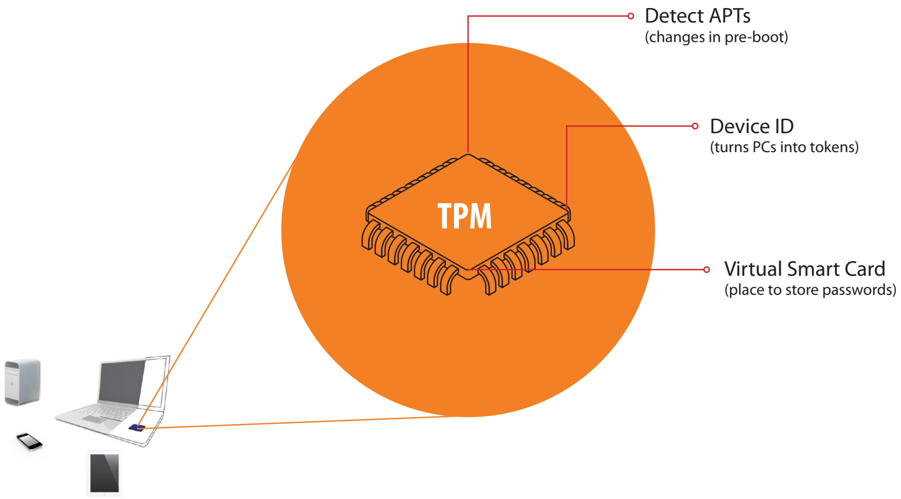
Wave's leading-edge security solutions build on a very simple principle:

Security starts with the device.

Far from being radically new or unproven, embedded security already prevents fraudulent use of cell phone and cable networks, Xbox LIVE and iTunes. All make a trusted endpoint device the cornerstone of network security.

When security starts with the device, you can:

- **Achieve zero-day protection against Advanced Persistent Threats (APTs)**
- **Trust the PCs that access your Cloud services**
- **Safeguard your systems from malware attacks**
- **Simplify your VPN and WiFi security and eliminate the costs of add-on tokens**
- **Assure the integrity of a computer's BIOS**
- **Allow for BYOD while ensuring network and information security**



03-000330/version 1.03 Release date: 10-25-2013

Wave Systems Corp.
480 Pleasant Street, Lee, MA 01238
(877) 228-WAVE • fax (413) 243-0045
www.wave.com