

# A Matter of TRUST

---

Secure Computing in an Age of Uncertainty

By Doug Anson, Dell

Network security is a hot topic in most IT shops these days, and rightly so. The Participation Age has ushered in a wave of unwanted participants—hackers, thieves, competitors, and terrorists. Securing client computers on “untrusted” networks requires both user security and machine security. This growing issue has spawned two technologies: smart cards, which address who can access network resources, and the Trusted Platform Module (TPM), which addresses what hardware can access network resources. These technologies are cornerstones in the IT industry’s vision of developing a “trusted computing” platform.

## User Security

User security refers to methods used to establish the identity of a user who’s logging onto a computer system or network. The method used can be as simple as a username and password or it can rely on a token<sup>1</sup> such as a smart card in combination with a username and password or biometric method.

A smart card is a credit card-sized electronic device with a built-in microprocessor and memory that is used for user identification. User information and credentials, including digital certificates and encryption keys, are securely stored within the card. Because of their versatility, smart cards are increasingly being issued to employees of large companies and organizations.

Smart cards are multifunctional: They can be used to log on the corporate network or gain entry to a building that is secured with

1. A TOKEN IS A SECURITY DEVICE IN THE POSSESSION OF AN AUTHORIZED USER. THE BEST KNOWN TOKEN DEVICE IS THE SMART CARD, A CREDIT-CARD SIZED DEVICE WITH AN INTEGRATED MICROPROCESSOR AND MEMORY.

badge readers at exterior doors. To log on the network, the employee inserts the smart card into a smart card reader that may be attached to or integrated into the computer, or embedded in the computer keyboard. The reader exchanges data with an authentication server, such as a **RADIUS** server, to complete the authentication “handshake.” The network infrastructure then enforces resource access based on the authenticated identity that has been established.

## Machine Security

In contrast to user security, machine security refers to measures designed to authenticate the computer system, rather than the user. For example, the following two scenarios require some level of machine security:

■ **IP Security (IPsec)**<sup>2</sup>—The IPsec protocol used on IP networks can be configured to require a networked computer to authenticate its identity to the network prior to generalized network access to resources. The computer uses a digital certificate to establish its identity to an authentication server before the computer attempts to use any network-available resources. In this way, network administrators can allow only supported client machines to access network resources.

■ **File Encryption on Local Drive**—Computer credentials can also be used to encrypt files stored on the local hard drive, thus “locking” the files to a particular machine. The machine’s credentials are required to unlock the files and access their content. These scenarios and others require that the local system

2. IPSEC IS A SECURITY PROTOCOL FROM THE INTERNET ENGINEERING TASK FORCE (IETF) THAT PROVIDES AUTHENTICATION AND ENCRYPTION OVER THE INTERNET OR A PRIVATE IP NETWORK. UNLIKE THE SECURE SOCKETS LAYER (SSL) PROTOCOL, WHICH PROVIDES SERVICES AT THE APPLICATION LAYER (LAYER 4) OF THE OPEN SYSTEM INTERCONNECTION (OSI) NETWORK MODEL AND SECURES TWO APPLICATIONS, IPSEC WORKS AT THE NETWORK LAYER (LAYER 3) AND SECURES EVERYTHING IN THE NETWORK.



be able to generate and store the secret encryption keys used to encrypt and decrypt data, digitally sign documents, and authenticate systems. The problem with the current PC platform is that there is no standardized way to securely store keys that are used for machine identity so that the keys can't be discovered if the system is stolen or otherwise compromised. The Trusted Platform Module (TPM) is an emerging technology that is designed to address this weakness in current platforms.

## Trusted Platform Module

TPM is an initial step toward the goal of standardizing a more secure PC platform. The TPM can be thought of as a smart card embedded on the system board and acts as a smart card for the machine.

The TPM is based on specifications developed by the **Trusted Computing Group (TCG)**. The TCG is an industry standards group formed to “develop, define, and promote open standards for trusted computing and security technologies, including hardware building blocks and software interfaces, across multiple platforms, peripherals, and devices.”<sup>3</sup> Members include **Dell, HP, IBM, Intel,** and **Microsoft**. Current TPM implementations are based on the TCG 1.1 specification. Vendors are developing products with TPM implementations based on the next-generation version, TCG 1.2.

The TPM has two components. The first is a secure microcontroller with cryptographic capabilities that is very similar to the micro-

controllers in smart cards. The second component is a proprietary software interface between the functions of the microcontroller and security-aware applications.

The TPM provides various cryptographic capabilities: hashing, random number generation, asymmetric key generation, and asymmetric encryption/decryption. Each TPM has a unique root key that is initialized during the silicon manufacturing process.

However, before a TPM can be enabled, its “owner” must be established. The end user establishes ownership of the computer system and its TPM via BIOS setup commands. These commands can't be issued remotely; instead, the TCG specification requires that the end user issue the commands at the local computer system. When completed successfully, the TPM has a unique owner, a “trust bond” is established, and the TPM can be used by TPM-aware software for security purposes. When coupled with software that can take advantage of its features, the TPM provides security that can be stronger than that contained in the system BIOS, operating system, or non-TPM applications.

Security implementations that rely on the TPM must also include “key escrow” services to securely back up and manage the unique keys associated with the TPM on each >>



Smart cards are best suited for user credential storage. The TPM is best suited to host credential storage.

3. WWW.TRUSTEDCOMPUTINGGROUP.ORG



computer system. In this way, if something happens to the system, its full TPM-enabled identity can be restored. Without this capability, it would be impossible, for instance, to unencrypt files encrypted with the TPM key. Key escrow services are provided by public key infrastructure (PKI) systems that manage asymmetric key exchanges.

## Smart Cards vs. TPMs

We see that smart card-based user authentication and TPM-based machine authentication are complementary, rather than competing, technologies. Table 1 presents appropriate uses of smart cards and TPM.

Smart cards are best suited for user credential storage. The TPM is best suited for host credential storage.

Table 1

User/Machine Authentication Scenarios	Smart Card	Trusted Platform Module (TPM)
User ID for virtual private network (VPN) access	Yes	No
User ID for domain logon	Yes	No
User ID for building access	Yes	No
User ID for secure e-mail	Yes	No
Host computer ID for VPN access	No	Yes
Host computer ID for domain access	No	Yes
Host computer ID for attestation (authentication of software applications)	No	Yes

## Future Secure Computing Platform

The TPM is only one piece of an industry vision of a future secure computing platform. Ideally, this platform cannot be compromised or accessed by unauthorized users or machines. The platform provides robust user authentication and protects data stored on the local drive. This vision implies secure software and built-in security hardware.

The future secure computing platform must encompass more than the secure generation

and storage of encryption keys provided by the TPM. A complete standard solution must also encompass the client operating system, the CPU and chip set, and methods to secure client system I/O devices such as keyboards, displays, and mouse devices. A number of initiatives are under way to begin to address these components.

## Secure CPU and Chip Set

The Intel LaGrande technology (LT) will provide hardware support for the parallel, protected execution environments. According to Intel, LT consists of processor, chip set, keyboard and mouse I/O, and graphics subsystem enhancements that provide the following capabilities:

- Protected and isolated execution environments with dedicated resources managed by the processor, chip set, and operating system kernel. These protected environments will run parallel to standard execution environments.
- Support for a hardware-based mechanism such as TPM to provide sealed storage of encryption keys and other secret data
- Protected communication between applications and USB keyboard and mouse devices.
- Protected communication between applications and display output.
- “Attestation” services, which provide authentication of software applications

Figure 1 depicts a sample future Intel LaGrande platform architecture that includes the TPM. The CPU and chip set are key areas affected by the new security initiatives.

## Progress

The industry is making progress toward a robust, standards-based machine authentication security solution. This solution includes comprehensive TPM functionality, native operating system support, and PKI infrastructure on the network. It is unclear when all of these elements will be in place and mature enough for end-to-end solutions to be

