Trusted Platform Modules Strengthen User and Platform Authenticity
January 2005

Computing and communications products with embedded Trusted Platform Modules (TPMs) advance the ability of businesses, institutions, government agencies, and consumers to conduct trustworthy electronic transactions. TPMs are special-purpose integrated circuits (ICs) built into a variety of platforms to enable strong user authentication and machine attestation—essential to prevent inappropriate access to confidential and sensitive information and to protect against compromised networks. Trusted Platform Modules utilize open standards and technologies to ensure interoperability of diverse products in mixed-vendor environments.

Trustworthy Transactions

Businesses of all sizes, institutions, government agencies, and consumers rely on millions of digital transactions everyday. The volume and the importance of these transactions are rapidly increasing. Wired and wireless systems used in digital interactions are woven into the very fabric of business and everyday life around the world. Being able to trust the identities of the participants, the authenticity of the contents, and the integrity of the systems involved in digital events is crucial. Robust security is essential for trusted communications; but it is surprising how many organizations rely on weak security solutions, believing they are engaged in trustworthy processes when they are not. It has been estimated that more than half of all desktop, laptop, and notebook PCs lack today's available software security features. To address the risks caused by inadequate security, integrated security hardware in the platform can not only strengthen the software solutions, but also assure that every platform comes with strong protection built in.

When the integrity of the services isn't reliable and cannot be proved, the consequence may be catastrophic. Victims of stolen personal, confidential, or sensitive information lose much more than data. Unauthorized changes to system parameters generate unintended expenses for system rebuilding and may jeopardize the future of an enterprise. If that's not bad enough, consider that corruption of important records—or even the *perception* of compromised integrity—may have severe legal consequences with criminal and civil penalties.

Intruders hack into networks with increasing frequency. Malicious corruption of records and inadequately protected systems regularly compromise legitimate transactions. Lost and stolen laptops can be a gold mine of critical information and a free pass to the network. Even cell phones and PDAs are under attack. Hardware-based, embedded security subsystems based on TPM chips provide reliable protections against these issues and enable truly cost-effective implementation and enforcement of strong security policies to ensure trustworthy transactions.

Strong User Authentication and Device Validation

Strong user authentication and device validation are essential for trusted digital interactions. Both are necessary to protect against inappropriate access to sensitive and confidential information and valued systems. Both are required to protect the integrity of the information, prevent corruption of the files, and ensure the integrity of those systems. Ultimately, it comes down to two basic questions:

   ▪ *Who are you and how do I know this is true?*

▪ *Can I trust this interaction and how do I know this is true?*

Who are you and how do I know this is true? All of the parties engaged in an important electronic transaction need to know that who they claim to be is really true. They could be corporate officers making 10K filings, doctors exchanging patient records, government clerks providing copies of birth certificates or deeds, businesses ordering critical parts, or consumers shopping on-line. The need to demonstrate their own authenticity and verify the reputed authenticity of the other party has never been more important. Software-only login and sign-on schemes provide only weak security. TPM-capable systems use both hardware and software to ensure spoof-proof user authentication to assure that the authenticity of the parties in digital transactions can be trusted.

Can I trust this interaction and how do I know this is true? It is also essential in trusted digital interactions to know that the systems, software, and records involved are what they claim to be. What if an on-line banking transaction is corrupted—wrong bank, wrong account, or the decimal point goes awry? What if confidential records are intercepted or misdirected and don't get to a patient's medical center or the SEC? Or, maybe, it is the right server, but the path leads to the wrong file or the file was corrupted after it was created? The integrity of the networks and resources must be ensured and it must be verifiable that they are used as intended.

It must also be assured that important records that were properly created and transmitted are also stored intact and uncorrupted. They must be retrievable at a later date exactly as they were created. Corrupted Social Security records, corporate 10K SEC filings, and medical records are but a few examples whose consequences can be devastating. In the United States, recent legislation imposes new requirements for safeguarding various types of sensitive data.

TPM-capable systems can play a strong role in assuring compliance with provisions of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 to protect medical records, as well as Graham-Leech-Bliley, Sarbanes-Oxley and similar regulations that impose privacy and validity requirements on corporate communications. Similar laws exist in other countries as well.

TPM-Capable Solutions Reduce Risk and Increase Reliability
Inadequate security has been tolerated because the risks were perceived as low and the solutions were perceived as cumbersome, expensive, and proprietary. These risks are no longer low and TPM-capable products provide easy to use, inexpensive solutions based on open standards. The trade-off between weak security versus unmanageable and proprietary security solutions is no longer an issue when network administrators can implement robust security policies based on open standards and protocols and deploy TPM-capable systems and software from many vendors.

User Authentication without TPM	User Authentication with TPM
▪ *Inadequate user ID and password protection makes "spoofing" very easy*	▪ Strong protections eliminate "spoofing"; verifies integrity of user log-in credentials
▪ *Multiple log-in IDs and passwords cause users to be careless; store secrets without protecting them; use weak protections*	▪ On-chip, protected storage of secrets reduces user burden; enables secure single sign-on; ensures strong protections
▪ *Storage of IDs and passwords in easily copied files; use of one set of secrets for access to all systems*	▪ Secure storage of IDs and passwords; multiple log-in secrets secured by the TPM
Platform Attestation without TPM	Platform Attestation with TPM
▪ *Easy to change settings and parameters for unauthorized access and malicious damage*	▪ Secure access prevents unauthorized access; secure hash comparison validates settings
▪ *Altered settings allow inappropriate access to valued networks and sensitive data*	▪ Validated settings ensure system integrity and prevent inappropriate access
▪ *Untrustworthy systems result in unreliable*	▪ Trustworthy systems result in reliable and

and untrustworthy practices	trustworthy practice; reduce support expenses

Stronger User Authentication with TPM Chips

Many systems and networks still rely on weak identification mechanisms with a single factor for identification—*something you know*. Even knowing two pieces of information—a user name and a user-defined password—doesn't make it stronger or really prove identity since it is so easy to capture and compromise this information.

Two-factor authentication relies on *something you know and something you have* and is stronger than single-factor authentication. Traditional two-factor authentication uses proprietary hardware tokens or password generators. TPM-capable systems provide strong two-factor authentication because the TPM is not a separate hardware token and it generates and stores the keys used by standards such as 802.1x, S-MIME email, and various types of Virtual Private Networks (VPNs). Because the security information is generated and stored in a protected manner, it is hard to capture or misuse. Even more security can be provided in TPM-capable equipment by adding biometric protections—*something you are*—such as user fingerprints to the sign-on requirements.

Secure Platform Attestation with TPMs

One frequent system attack involves making unauthorized changes to a platform's configuration. This allows misuse of the device and its contents as well as access to the networks to which the device is connected. In devices that use TPM chips, platform integrity is protected by secure storage of the platform configuration values *and* by secure reporting of the values. This enables attestation of the device by verifying that its configuration is intact. The mechanism is based on the chain of trust used in creating the hash values of the pre-boot information of the platform.

It is common industry practice to check the integrity of a platform by comparing configuration settings when a platform is rebooted against the settings when it was set up. A "hash" algorithm is used to calculate a value from information stored in the Platform Configuration Registers (PCRs) when the platform is setup. When the platform is re-booted, a new hash value is calculated and compared against the original. If the values match, the computer or cell phone or other platform starts up and login proceeds.

In unprotected systems, PCRs are accessible and the hash values are stored in system memory that is subject to compromise. In TPM-capable platforms, the hash value is calculated using the SHA-1 algorithm, access to the PCRs requires trusted authorization, and the hash values are stored within the TPMs in secure, non-volatile memory. These values are used to create Attestation Identity Keys (AIKs) that cannot be used unless a hash value is the same at the time of use as when the AIK was created. This makes it possible to determine if trusted-state configuration parameters are corrupted. If they are corrupted, use of the device may be denied.

Balanced Administration

The need for access and ease of use must be balanced with the responsibility to maintain the integrity of the network, services, and data. Using proven security methodologies that are rooted in hardware can significantly improve this balance. This hardware-tempered approach also streamlines user experiences without compromising security.

Changing functional requirements puts constant pressure on systems to support new products, services, and types of users. Network administrators face the difficult task of developing and enforcing unified security policies for network access and system integrity. Access to systems and resources by third-party services, corporate partners, and telecommuters makes security administration ever more daunting. TPM-capable products support robust integrated security policies because of the mechanisms employed for user authentication and platform attestation. Robust and enforceable security policies result in reliable systems, streamlined administration, and trustworthy operation.

Security Policy Requirements and Interoperability
Development and enforcement of appropriate security policies includes several specific requirements. A sustainable security policy needs to be able to meet these requirements in a cost-effective manner. When these requirements can be satisfied only with proprietary solutions, or they cannot be fully satisfied because of multi-vendor environments with incompatible components, the obstacles to deployment are often too great to overcome. The widespread adoption of TPM-capable solutions removes those obstacles and makes it possible to implement truly sustainable security policies. The use of open standards and participation of the leading manufacturers in the computing and communications industries makes this possible.

Security Policy Requirements	Open Standards for Interoperability
▪ Permit only authenticated users and devices to connect to the network	▪ IEEE 802.1x, IETF RADIUS, IETF EAP
▪ Enable administrator to establish security policies for anti-virus, patch levels, software versions, etc.	**Focus of TCG Efforts**
▪ Measure device configuration against security policies before its connection to the network is allowed	
▪ Identify devices that are not compliant	
▪ Quarantine non-compliant devices	
▪ Remediate non-compliant devices to ensure compliance to security policies	

TPM chips use standard software interfaces and work with other security methodologies to ensure deployment of secure applications with privacy protection and interoperability across multiple platforms. The architecture of TPM chips ensures maximum flexibility of implementation by system and device manufacturers and maximum flexibility of deployment by the owners of these solutions. Deployment of TPM-capable computing and communication devices provides greater security without lowering productivity or introducing new obstacles in manageability.

Software Isn't Enough
Software-only solutions have been used because of the simplicity of configuration, flexibility of deployment, and ease of management—the same features that make these solutions so vulnerable to attack. If it's simple to configure, it's also simple to hack into the configuration. Flexibility of deployment often means that access points are vulnerable. Ease of management too often means Supervisor Mode is not much more secure than User Mode.

Even traditional security mechanisms such as encryption keys, digital certificates, and firewalls are not as safe as they appear to be because they generally store the security information on an unprotected hard drive and in unprotected memory that are very vulnerable to unauthorized access. TPM-capable solutions make these software security methodologies more robust by ensuring secure storage of the digital secrets they use.

Applications without TPM	Applications with TPM
Regular E-mail: Easy to hack even with software-only private decryption keys.	**Secure E-mail with TPM**: The authentication and encryption keys are stored in the TPM, not in system memory. The keys are not accessible. The email is not accessible without the keys.
Unprotected digital signatures: Private signature keys are stored in system memory. A hacker can easily generate legally binding forgeries.	**TPM-Protected digital signatures**: Protect the private signature keys. Keys are stored inside the TPM and are not exposed in system memory during signing operations.

Unprotected systems and files: unauthorized access to the platform gains unauthorized access to files.	TPM-Protected platforms: Protect the settings of the platform to prevent corruption of the system or contents.

Enhancing Interoperability Optimizes Deployment

Trusted Platform Modules utilize open standards and technologies to ensure interoperability across platforms, operating systems, and product lines. This vendor-neutral approach to robust security is designed to meet the diverse needs of small, medium, and large enterprises with systems and services from a wide variety of suppliers. It is currently estimated that one-third of all enterprise PCs are replaced or upgraded each year in the United States. This level of financial expenditure and infrastructure renewal makes it crucial to maximize the return on investment and optimize the flexibility of deployment in the face of changing needs.

Hardware-Based Integrity

Trusted Platform Modules provide mechanisms to proactively establish more trusted relationships for remote or local access through secure user authentication and machine attestation. TPM chips protect encryption keys and digital signature keys to maintain data confidentiality and integrity. TPM chips are designed to protect key operations and other security tasks that would otherwise be performed on unprotected interfaces in unprotected communications. Especially important, TPM chips are specifically designed to protect platform and user authentication information from software-based attacks. They are designed to enhance platform security beyond the capabilities of software-only solutions.

TPM-capable products are built with the TPM chips soldered onto their printed circuit boards. Encryption keys and other critical security information are stored in non-volatile memory within the TPMs. The private keys stored in the TPM chips are protected by the TPM even when in use. This guarantees secure key management. By contrast, when security is provided by traditional, general-purpose CPUs, encryption keys and related security information are stored in general system memory. This use of system memory cannot guarantee secure key management; and, it gives system managers a false sense of trust.

Protected key storage enables TPM-capable systems to support affordable yet robust user authentication and platform attestation for secure local as well as remote access. The "root of trust" is based in hardware—the TPM—but can be extended to software. TPM-capable systems make storage of digital secrets (passwords, credit card numbers, digital signatures, etc.) more secure by protecting them from compromise and unauthorized use.

Time to Get On-Board

Since their introduction in 2003, leading manufacturers of hardware and software are producing TPM-capable products because the marketplace has demonstrated its acceptance of the TCG standards-based approach to security. Many vendors have TPM-capable desktop and laptop products on the market and more are on the way. In many of these products, the TPM capability is now standard equipment. Worldwide PC shipments reveal that tens of millions of TPM chips will have shipped by the end of 2004 for PC desktop and notebook computers with the trend expected to grow exponentially year by year. Current market data indicates that over 55% of all PCs and Notebook computers will be TPM-capable by the end of 2007.

Atmel, Fujitsu, Hewlett-Packard, IBM, Infineon, Intel, National Semiconductor, NTRU, Softex, STMicroelectronics, Utimaco Safeware AG, and Wave Systems have developed and market TPM chips, software, and TPM-capable motherboards and system-level products that comply with TCG hardware and software specifications.

PCs and other digital devices built around general-purpose microprocessors from AMD, Intel, IBM, ARM and other manufacturers support the use of TPM chips on-board. Operating systems such as Windows® and Linux also support the use of TPM chips. The security of embedded systems such as voting machines, set top boxes, POS terminals, and ATMs can also be

strengthened with TPM-subsystems. For information about TPM-based and TPM-compatible products, visit the TCG web site and link to the member companies' product information.

TPM Chip Vendors

Manufacturer	Product	Contact
Atmel	AT97SC3202, AT97SC3201, AT97SC3201S	www.atmel.com/products/Embedded
Infineon Technologies	SLD 9630_TT_1.1	www.infineon.com
National Semiconductor	Trusted IO - Super IO with embedded TPM	www.national.com/appinfo/advancedio/ safekeeper.html
STMicroelectronics	ST19W18, ST19WP18-TPM	www.st.com

TPM-based System Vendors

Manufacturer	Product	Contact
Fujitsu	Lifebook S7000, E8000, NAH	www.futjitsu.com/
Hewlett-Packard	D530 Desktops; nc4010, nc6000, nc8000, nw8000 notebooks	www.hp.com
IBM	ThinkPad notebooks,NetVista desktops	www.pc.ibm.com/security
Intel	D875GRH motherboard	www.intel.com/platforms/desktop/vision

TPM-Compatible Application Software

Application Type	Description	Vendors
File/Folder Encryption	Keys protected by TPM	HP, IBM, Infineon, Information Security Corp., Softex, Wave Systems
Full Harddisk Encryption	Encryption Keys are protected by the TPM. Keys are generated by the TPM.	Utimaco Safeware AG
Container Encryption	Keys for container access as well as content encryption are protected by the TPM.	Utimaco Safeware AG
Workgroup Security	Workgroup data is protected via encryption. Keys are stored in the TPM.	Utimaco Safeware AG
High Security User Authentication	Pre-Boot-Authentication authenticates user before operating system is up and running. SSO to operating system and applications. Credentials are secured by the TPM.	Utimaco Safeware AG
Machine Binding	Data on media is linked to the PC platform, enforced by TPM credentials.	Utimaco Safeware AG
Secured Remote Administration and Mutual Authentication	Mutual authentication of clients and servers for remote administration is secured by keys generated by the TPM.	Utimaco Safeware AG
Client-based Single Log-in	Username/Password auto fill lets users remember only 1 password and register others in TPM for auto fill as needed.	Utimaco Safeware AG, Cognizance, IBM, Softex, Wave Systems

Protected Information Repository	TPM wrapping/sealing capability protects sensitive personal or business information.	IBM, Softex, Wave Systems
E-mail Integration	Encryption, signature schemes supporting MS-CAPI or PKCS#11	Information Security Corp., Microsoft (Outlook), Netscape
Digital Signatures	Use digital signature applications in e-mail, PDF files, e-purchasing, etc.	Adobe (Acrobat), Microsoft (Internet Explorer), Netscape, Wave Systems
Enterprise Login	Platform authentication using TPM	Cognizance, Wave Systems
Remote Access	TPM-protected remote access credentials can be used for VPN, 802.1x, etc.	Checkpoint (VPN-1 Secure Client), RSA (SecurID), Wave Systems
Hardened PKI	Protect and manage credentials issued by Certificate Authority using TPM.	Checkpoint, PGP, RSA, VeriSign, Wave Systems
TPM System Backup and Recovery	Key recovery in cases of platform failure, platform replacement, or hard drive failure	Wave Systems
TPM and User Management	Manage TPM and user security policies	Wave Systems, IBM, Infineon
Platform Attestation	Privacy CA capabilities to create AIKs (Attestation Identity Keys) using TPM	Wave Systems

How It All Works

The TPM chip is a secure key generator and key cache management component that supports industry-standard cryptographic Application Program Interfaces (APIs). TPMs generate, store, and manage cryptographic keys in hardware (within the TPM). This leverages the resources of the platform and allows cost-effective hardening of the many applications that previously have relied solely on software encryption algorithms with keys stored in unsecured memory.

Each TPM function is based on established industry-standards. A true Random Number Generator (RNG) is used to create RSA key pairs internal to the TPM. The TPM chip's RNG generates the seed numbers for the cryptographic processor's encryption, decryption, and key generation functions. Performing the RSA calculations in the TPM instead of in the general system processor improves both system and encryption performance. The TPM generates, stores, and manages cryptographic keys in hardware, which "hardens" applications that originally relied on software-only encryption algorithms.

Several functions protect the TPM chip and facilitate enforcement of strong security policies:
- An *Endorsement Key* may be used by a platform's owner to anonymously establish that identity keys were generated in a TPM. This enables confirmation of the quality of the keys without identifying the specific TPM IC that generated the key.
- *Initialization and management functions* provide flexibility without compromising privacy. The owner of the platform may turn functionality on and off, reset the TPM chip, and take ownership of the platform. (The system *owner* is frequently not the *user* of the platform).
- *Direct Anonymous Attestation* (DAA) communicates information about the static or dynamic capabilities of a device that has a TPM on-board. This does not require disclosure of personally identifiable information and is under the platform owner's control. Users/owners can generate multiple keys for interaction with different parties while maintaining anonymity. DAA complements other attestation functions in the TPM architecture and can be implemented with or without a trusted third party.
- *Locality* allows owners of TPM-enabled devices to assign permissions to external software processes. Locality assumes that there are hardware or software processes outside the TPM chip that have different levels of trustworthiness.

- *Delegation* allows platform owners to delegate to software, an object, or other entity permission to use specific owner-authorized commands without enabling access to other commands in the TPM. For example, owners can withhold their passwords from untrusted entities.
- *Transport Protection* for commands sent to the TPM is used to help ensure the confidentiality of data exchanged between the TPM chip and remote software.
- *Monotonic Counters* help prevent common "replay" attacks in which stored data is compared to current values.
- *The Tick Counter* allows the TPM chip to perform time-related transaction sequencing.

Learn More about TCG and TPM

The Trusted Computing Group is an organization created to promote open standards for trusted computing and security technologies using non-proprietary hardware building blocks and software interfaces. TCG's goal is to facilitate enhanced end-to-end security across diverse platforms, including desktop and notebook computers, servers, peripherals, and other devices such as PDAs and cell phones.

Hardware and software specifications promoted by TCG are designed to enable more secure computing environments without compromising functional integrity with the primary goal of helping users to protect their information assets from compromise due to software attack and physical theft. Specifications and the resulting products enhance security for data storage, online business practices, and online commerce while protecting privacy and individual rights. For more information about TCG membership and the hardware and software specifications that pertain to Trusted Platform Modules, refer to www.trustedcomputinggroup.org/.