

# Building A Foundation of Trust in the PC

*The Trusted Computing Platform Alliance*

January 2000



## Contents

<b>THE TCPA VISION .....</b>	<b>1</b>
<b>PRIVACY.....</b>	<b>1</b>
<b>SECURITY .....</b>	<b>1</b>
<b>COMPLEMENTING EXISTING STANDARDS.....</b>	<b>2</b>
<b>TRUST AND OPEN PLATFORMS.....</b>	<b>2</b>
<b>LIMITATIONS OF SOFTWARE-BASED TRUST.....</b>	<b>2</b>
<b>HARDWARE-BASED TRUST .....</b>	<b>2</b>
<b>THE NEED FOR PLATFORM UBIQUITY .....</b>	<b>3</b>
<b>THE TRUSTED PLATFORM.....</b>	<b>3</b>
<b>THE TCPA SUBSYSTEM.....</b>	<b>4</b>
Scenario I: Remote Attestation.....	5
Scenario II: Privacy and Authenticated Anonymity .....	6
<b>CONCLUSION .....</b>	<b>6</b>
<b>FOR MORE INFORMATION .....</b>	<b>7</b>

## **The Trusted Computing Platform Alliance: Building a Foundation of Trust for the PC**

### **The TCPA Vision**

Business and commerce depend on trust. Since e-Business runs on the PC, enhancing trust in the computing platform is an issue of fundamental and growing importance for the PC industry.

In the spring of 1999, the TCPA was chartered to encourage industry participation in the development and adoption of an open specification for an improved computing platform. The goal of this effort is to build a solid foundation for improved trust in the PC over time. The TCPA participants further agreed that the specification for the trusted computing PC platform should focus on two areas—ensuring privacy and enhancing security.

### **Privacy**

Privacy is extremely important to every business and individual concerned about protecting confidential and personal information. In the computing context, privacy provides a way to prevent others from gaining access to information without the informed consent of its owners. Cell phones, telephone caller ID, credit cards and the Internet provides people with a dramatic new levels of freedom that can enhance business processes and personal lives, but these innovations come with a privacy price tag. All of these systems are capable of providing information, including financial and personal data that most users assume to be confidential. The TCPA believes that the ability to ensure such confidentiality through privacy controls is an essential prerequisite of a trusted system.

### **Security**

Computer security involves protecting data from unauthorized access. Traditional PC security in business ultimately depends on a chain of trust, beginning with the IT manager who must trust the computer's operating system, trust the PC manufacturer, trust the users of the system, and also trust that physical security is adequate. While physical security is a matter of keeping the doors locked at night, PC security is typically not so straightforward. A large part of every IT manager's time is spent contending with the myriad issues involved in keeping users up and running. This includes providing authenticated owners with access to authorized information and keeping unauthorized persons out.

An important goal of the TCPA is to provide stronger authentication of platforms and to enhance the integrity of internal and external networks. Stronger platform authentication and network integrity will enable IT managers to raise the level of trust for an external network, such as the Internet. In addition, the TCPA specification will define a baseline set of security features and capabilities that will be easy to deploy, use and manage by IT organizations.

## **Complementing Existing Standards**

Today's PCs provide a tremendous amount of trustworthiness to users. For example, businesses routinely depend on the ability to trust PC functions such as Secure Sockets Layer (SSL) to help transact online business with security. The objective of the TCPA is to enhance security at the level of the platform hardware, BIOS, system software and operating system. Such a comprehensive standard does not currently exist. The Alliance aims to create and deliver a specification proposal to a standard's body by mid-2000. This specification would be the foundation for a base-level security standard. It would complement existing capabilities, including the X.509 standard for digital certificates, IPSEC (Internet Protocol Security Protocol), IKE (Internet Key Exchange), VPN (Virtual Private Network), PKI (Public Key Infrastructure), PC/SC Specification for smart cards, biometrics, S/MIME (Secure Multi-Purpose Internet Mail Extensions), SSL and SET (Secure Electronic Transaction).

## **Trust and Open Platforms**

While the flexibility of the PC platform has allowed for phenomenal business growth, this same level of flexibility can conflict with the goal of making systems more trustworthy. PC users expect an open system—one that literally lets them do anything, anytime they choose. Conversely, the most drastic and extreme way to build “trust” into a computing system is to lock it up. IT Managers can control the software that their users can run, prevent third-party hardware installations, and effectively “weld the box shut”—creating a closed platform. The unfortunate side effect of this strategy is that it often eliminates many of the benefits of using a connected PC.

The PC industry has chosen an alternate approach that provides users with the ability to run the world's widest and deepest selection of software available. The industry also boasts the richest and most diverse hardware community and commands the most pervasive and diverse installed base. Because it offers freedom of choice, the PC has become the first choice for running websites and accessing the Web. While they enjoy this freedom, users also store sensitive data on their PCs, and they naturally expect that data to be protected. Moreover, as conventional businesses evolve into “e-Businesses,” the trustworthiness of PCs must continue to improve because increasing numbers of businesses depend on PCs for their success, and even their very existence.

## **Limitations of Software-Based Trust**

With the growing demand for trusted computing, the ability to protect the integrity of a PC through software alone is reaching its limitations. Even the most robust and tightly controlled PC operating systems cannot prevent unauthorized software from loading before the operating system itself loads. Once such unauthorized software has loaded, it can gain access to areas of the system that should not be accessible in a trusted environment.

## **Hardware-Based Trust**

There are e-Business security and privacy issues that software alone cannot address. At the same time, new e-business opportunities are emerging that demand even higher levels of trust. These imperatives are

driving the industry to take trusted computing to a higher level. To achieve this goal, the PC needs a foundation of trust based in hardware. This foundation for trusted computing should be extendable across systems and networks for multiple users. Most importantly, the system must be able to ensure that privacy and security can coexist with a system that also maintains the freedom of choice associated with the PC today.

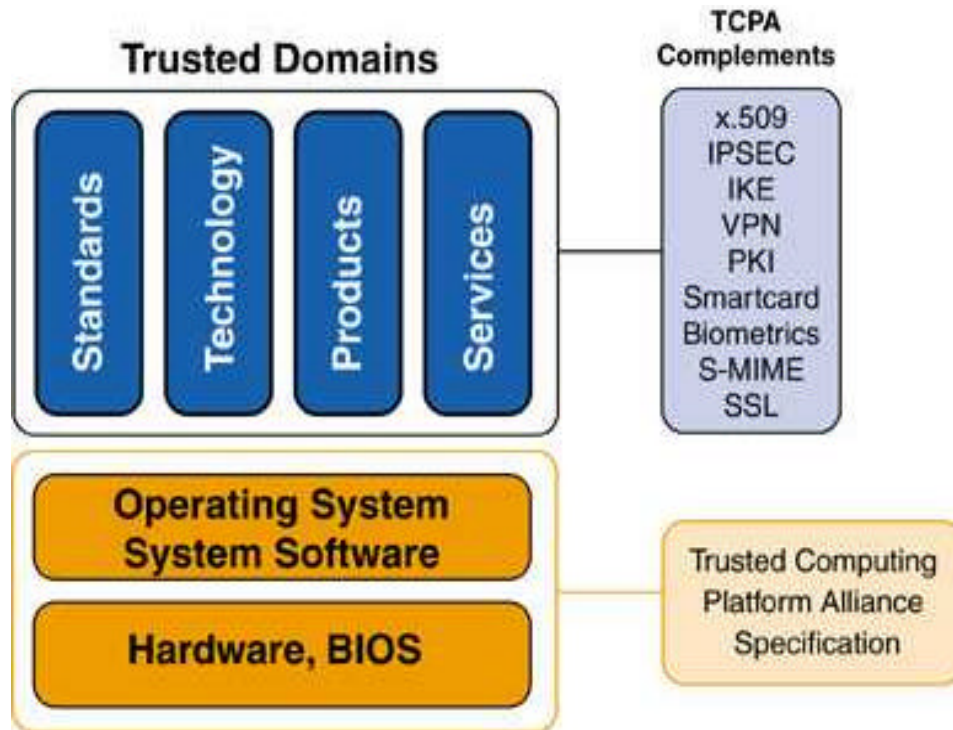
## **The Need for Platform Ubiquity**

The founding members of the TCPA agree that making the PC platform more secure requires a ubiquitous solution, supported by vendors throughout the industry. The concept of ubiquity is a fundamental one within the PC industry. It enables vendor choice, drives a high level of innovation and provides the basis for standardization. Achieving ubiquity in trusted computing is no exception. It implies that at some point, all PCs will have the ability to be trusted to some minimum level—a level that is higher than possible today—and to achieve this level of trust in the same way.

The objective of the TCPA is to make trust just as much a part of the PC platform as memory and graphics. Every PC will have hardware-based trust, and every piece of software on the system will be able to use it. With this goal in mind, the role of the TCPA is to define minimum platform hardware requirements and specify a consistent means of access.

## **The Trusted Platform**

To be a “trusted platform” a PC must be trusted by local users and remote entities, including users, software, websites, and all third parties. The basis for this trust is a declaration by a known authority that the platform can be trusted for an intended purpose. In other words, someone whom the owner trusts says with certainty that a platform is exactly what it says it is, and that the owner can trust the platform.



## The TCPA Subsystem

The TCPA specification advocates that a separate mechanism, called the Subsystem, can be trusted to the same degree by as many entities as possible. The TCPA Subsystem is designed to provide reliable mechanisms for the measurement and reporting of integrity metrics, and consists of two building blocks:

- A Trusted Platform Module (TPM), defined as the hardware instantiation of the TCPA specification.
- Software to perform integrity metrics, in conjunction with the TPM.

The Subsystem is designed to prevent the platform from logical, or software-based, attack. While the Subsystem can still be subverted by physical means, this mode of attack exposes only the secrets of the Subsystem on the local platform, and not on other connected platforms.

Through the Subsystem, the TCPA specification will create a hardware-based foundation for trust, based on a set of “integrity metrics.” These are defined as measurements of key platform characteristics that can be used to establish platform identity, such as BIOS, boot-loader, OS loader, and the OS security policy. Cryptographic hashing is employed to extend trust from the BIOS to other areas of the platform, in the following sequence:

1. The PC is turned-on.
2. The TCGA-compliant "BIOS Boot Block" and TPM have a "conversation." This attests that the BIOS can be trusted.
3. BIOS queries to ensure that user is authorized to use the platform.
4. The BIOS then has a "conversation" with the operating system (OS) loader and the TPM. This attests that the OS loader can be trusted.
5. The OS loader then has a "conversation" with the OS kernel. When the OS kernel loads, it knows what software has had access to the system ahead of it. This establishes that whatever happens within the system from that point forward is 100 percent controlled by the OS kernel.

This process is similar to the children's game of "telegraph" where each child in a circle repeats a phrase to the next child. Unlike the game of telegraph, cryptographic hashing ensures the phrase is passed with complete reliability. The core elements of trust that are built into the system through the TPM and TPM BIOS extend their trust to the boot loader. The boot loader extends its trust to the OS loader. The OS loader in turn extends its trust to the OS, which can then extend its trust to applications.

The following usage scenarios briefly illustrate the benefits of TCGA compliance.

### ***Scenario 1: Remote Attestation***

TCGA remote attestation allows an application (the "challenger") to trust a remote platform. This trust is built by obtaining integrity metrics for the remote platform, securely storing these metrics and then ensuring that the reporting of the metrics is secure.

For example, before making content available to a subscriber, it is likely that a service provider will need to know that the remote platform is trustworthy. The service provider's platform (the "challenger") queries the remote platform. During system boot, the challenged platform creates a cryptographic hash of the system BIOS, using an algorithm to create a statistically unique identifier for the platform. The integrity metrics are then stored.

When it receives the query from the challenger, the remote platform responds by digitally signing and then sending the integrity metrics. The digital signature prevents tampering and allows the challenger to verify the signature. If the signature is verified, the challenger can then determine whether the identity metrics are trustworthy. If so, the challenger, in this case the service provider, can then deliver the content. It is important to note that the TCGA process does not make judgments regarding the integrity metrics. It

merely reports the metrics and lets the challenger make the final decision regarding the trustworthiness of the remote platform.

### ***Scenario II: Privacy and Authenticated Anonymity***

Imagine that the PC has booted as described in the four-step sequence outlined earlier, and that the system can be trusted. It is now possible to present credentials for the system to a third party. In doing so, however, the user exposes the identity of his or her platform to the third party, and possibly runs the risk of providing more information than intended.

An alternative is to use a recognized and trusted entity within the industry that can verify that an identity belongs to a trusted platform. This is termed “anonymous authentication.”

Here is how it works in a TCPA-compliant subsystem:

The user goes to a third-party Authenticated Anonymity Website (AAWS), and requests site verification. Using the TCPA Subsystem, the AAWS provides the user with credentials, known as a “cert” or certification. Those credentials assert that the platform is authenticated by a trusted third party and that the platform can be trusted in certain ways. The AAWS asserts that the platform is unique, but it will not tell someone else anything that can be traced back to the user. For the purposes of the transaction, the platform is reliable, and also anonymous.

## **Conclusion**

The scenarios outlined here provide just two examples of how the TCPA-compliant Subsystem can improve the trustworthiness of the PC. It is important to realize that the TCPA does not aim to resolve all trust issues for all systems. Rather, the goal of the TCPA is to provide a consistent and standardized core foundation for trusted computing that anyone can use and extend.

With the growth of the Internet and connected computing, trust has become a pivotal issue for e-Business. While today’s trusted environments use security components that are well known within the industry, the current problem for users is that multiple software and hardware solutions are all trying to interact in a trusted manner. What is needed is a specification that can provides a ubiquitous and standardized means to simplify the deployment, use and manageability of security domains on PCs.

The objective of the TCPA is to develop a ubiquitous specification for standardized platform security and then submit this specification to a recognized standards body for publication. The TCPA specification will minimize the security problem for IT managers by providing way to optimize the value of the existing security infrastructure, while preserving the flexibility of the PC platform. At the same time, the TCPA specification can help create opportunities for new e-Business models by reducing security concerns.



The TCPA is open to participation from all segments of the electronics industry. All interested participants are encouraged to join the TCPA and help us deliver on the vision of trusted computing.

## For More Information

For more information on how to participate in the TCPA:

- Visit the TCPA website: [www.trustedpc.org](http://www.trustedpc.org)
- Contact the TCPA by e-mail [tcpa@trustedpc.org](mailto:tcpa@trustedpc.org)
- Write to:

TCPA Program Office  
c/o Intel Corporation  
M/S: HF3-77  
5200 NE Elam Young Parkway  
Hillsboro, OR 97124

*Phone: (503) 696-7954*  
*Fax: (503) 696-1896*