

# Trusted Computing Platform Alliance

## A Technical Overview of Trusted Computing



## Building the Foundation for Trusted Computing

Today most protection against computer viruses and unauthorized intrusions consists of adding and updating software that installs outer barriers and surveillance tools. The goal of Trusted Computing is to go much deeper, integrating progressive levels of trust into the actual hardware and pre-operating system environments. Once these environments are trusted, other portions of a computing platform (PC, PDA or other computing device) can be addressed to provide additional levels of trust.

In 1999, five companies — Compaq, HP, IBM, Intel and Microsoft — formed the Trusted Computing Platform Alliance as the first step in defining a standard for advancing and implementing the concepts of Trusted Computing. Today TCPA has over 170 members, including leading companies in hardware, software, communications, and other technologies. These companies are joined in an open alliance to develop the necessary technology and cooperation to make Trusted Computing a reality. The first level of trust will be achieved through adaptation of a TCPA specification for silicon technology.

### TCPA Goals

- Create a security standard across all platforms
- Provide protected storage of cryptographic and sensitive data by a TCPA device
- Enable the identity and authentication of a computing device to other computing devices
- Supply metrics providing reliable, trusted network environments
- Permit system owners and users to manage their privacy-sensitive information

## A New Approach to Computer Security

For years, computer security has consisted of adding layers (passwords, encryption and anti-virus software) between the outside world and the PC. With each new virus threat or attack, a layer has to be strengthened or a new one added. This band-aid approach only mends the tear. It doesn't address the core problem.

Through Trusted Computing, TCPA promotes a more integral solution. This solution incorporates progressively greater levels of assurance that a system and its applications are uncompromised. The immediate goal is specifying a way to ascertain a system's trustworthiness at any particular moment. In the future, there could be specifications for establishing trust in the inputs and outputs of a platform, as well as its communications and networking channels.

### Trusted Computing Requires Transactions and Computing Devices to be:

- **Trusted** – acting in a recognized and attestable manner
- **Reliable** – readily available for transactions and communications, as well as prepared to act against viruses and other intrusions
- **Safe** – able to stop unwanted intervention or observation
- **Protected** – sharing information with only those who are authorized
- **Private** – providing users a way to manage their privacy



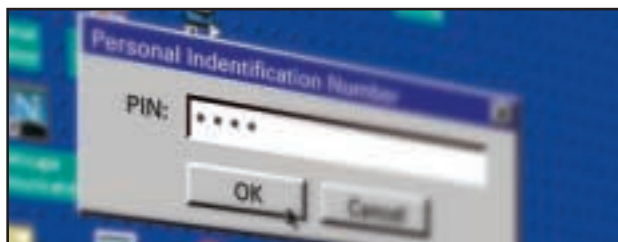
Trusted Clients provide attestation of their platform configuration. Prior to a transaction, servers and clients use this information to verify other servers and clients are operating in an uncompromised state.

## Components of the T CPA Series of Specifications

- Design Philosophies – The overall architecture and design philosophies for T CPA.
- Main Specification – Defines the T CPA device. Every T CPA device is called a Trusted Platform Module (TPM) and provides the basis for the platform's trustworthiness.
- T CPA Software Stack (TSS) – The software stack that allows applications to have access to the T CPA device.
- PC Specific Specification – Defines how to implement the platform-independent T CPA specification on the PC platform.
- Protection Profiles – The T CPA device and its connection to the platform will each have a Protection Profile which is evaluated by a certified evaluation lab.

The T CPA specification is platform neutral. T CPA devices are designed to be installed in cell phones, PDAs, mobile computers, and other devices. There would be a platform-specific specifications for each.

## Trusted Computing in Action



### Usage Model 1: Protection of Data

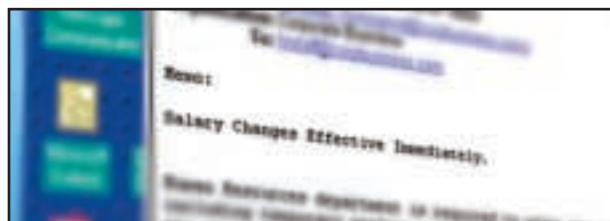
Keys can be bound to a specific platform. Further, the use of the key requires user authentication. Data can then be encrypted using a key that is bound to the platform and requires the user's authorization. Since the key is bound to the platform, even if an attacker obtains the key file and knows the authorization for the key (e.g., PIN), the data is safe because the key will only work when used on the specific platform. The attacker must obtain both the specific platform and possess the authorization for the key to decrypt the data.



### Usage Model 2: Attestation of the Platform's Trust State

A T CPA-enabled platform requests a service from a corporate server (e.g., e-mail). The server's policy is to send e-mail only to platforms that have policies and applications that protect the contents of the e-mail. The e-mail server requests the signed trust state of the client's platform. Based on the signed (therefore trusted) valid value returned, the server sends the requested e-mails to the now trusted client.

What happens in a case where the platform isn't T CPA-enabled? There is no way for the server to trust any "trust statement" from a software-only (i.e., non-T CPA) client — even if it is running software that would otherwise be trusted by the server. Software alone cannot provide the same level of trusted attestation as a T CPA device-based platform. Consequently, the e-mails are denied.



### Usage Model 3: Platform and User Authentication

A Human Resources department has client platforms for the entire HR staff, including temporary workers, administrative assistants, managers, and the vice president of HR. Even with user authentication, it is desirable to allow specific actions (e.g., salary changes) to originate from only specific and physically secure locations within the department. Using software-only platform authentication, a platform can spoof its location (e.g., spoof its physical network address) making the server believe it is the communicating with the one in the secured location. If the server instead considers only T CPA device-based platforms to be trusted, the rogue platform could not spoof its location. Salary change information would be safe from such a possible breach.

## The Value of Trusted Computing

**For computer owners:** Trusted Computing hardens computing devices to software-based attacks, integrating capabilities to better protect transactions through the addition of trusted hardware and operating systems. This will help make PCs more manageable, lowering the total cost of ownership by reducing risks of information theft.

**For business:** Trusted Computing reduces one of the greatest barriers to e-business — the fear that everything from credit card numbers to confidential corporate data could be stolen. It defines a security framework that will allay fears of sharing sensitive information and spur a new burst of growth in e-business.

**For OEMs:** Trusted Computing gives original equipment manufacturers a new way of adding value to their products and building trust in their brands. They can ensure interoperability with this new standard in computer security while differentiating their products with their own innovations.

## Find Out More

TCPA is helping to engineer a new world of trust. You can be a part of it. To learn more, visit:

[www.trustedcomputing.org](http://www.trustedcomputing.org)



TCPA Program Office  
Carol Burke, M/S JF1-229  
Intel Corporation  
2111 NE 25th Ave.  
Hillsboro, OR 97124  
Phone: 503.264.9660  
Fax: 503.264.0281