

## TCPA Specification/TPM Q&A

*Updated 16 October, 2002*

### Questions and Answers grouped by Categories: TPM, CA, Uniqueness, etc...

#### The technology, user privacy and controls, content protection

##### **1. Does the TPM “control” a user’s system?**

No. The TPM can store measurements of components of the user’s system, but the TPM is a passive device and “doesn’t decide” what software can or can’t run on a user’s system. The TPM provides the storage and reporting of the measurements of components of the user’s system that are reported to it. The TPM accepts any measurement that is reported. There is no capability for the TPM to determine whether a particular measurement is acceptable or not.

##### **2. Is the TPM intended to replace smart cards?**

No. TPMs and smart cards perform both similar and different functions. A SmartCard provides protection of information and authentication for individual users. A TPM provides protection of information and authentication for individual platforms. While there is some overlap between the uses of these two technologies they are, in fact, complimentary. We anticipate use models that take advantage of both TPM and smart card capabilities.

##### **3. To which extent are the keys and other protected data in a TPM physically protected? Could a skilled technician in a well-equipped laboratory read them like it seems they can on an ordinary smart card (electron microscopy, light refraction)?**

The TPM protection profile requires for some physical protection on the TPM. It does not specify the mechanism that the manufacturer needs to design in. The TPM manufacturers are all familiar with creating security chips. We would anticipate that some TPM's will have stronger physical protections than others. The market will determine what is appropriate.

##### **4. Is the real “goal” of TCPA to design a TPM to act as a DRM or Content Protection device?**

No. The TCPA wants to increase the trust that users and remote entities will have in the user’s platform. The increase in trust comes from the mechanisms provided by the TPM. One of these mechanisms is a report, or **attestation**, of the current configuration of the platform. A user or system owner may elect to attest remotely to this configuration. Knowledge and confirmation of the current software running on a system has been a desired feature for security systems for many years, not only for private users, but also especially for system administrators which are responsible for infrastructure security and reliability. For instance this could allow a system administrator to know that a user is operating the current version of the virus protection software. The TCPA is now attempting to provide that functionality. Application vendors will build applications supporting specific use models. Platform owners will determine which OS and applications to run on their platforms. The TCPA remains committed to thorough and open reviews with industry and government experts of this technology and its implications for use models.

## **TPM's in Computing Platforms**

### **5. Is the TPM based platform limited to a particular operating system or microprocessor?**

No. The TCGA specification is designed to be platform and OS agnostic. The TCGA specification is not limited to a specific platform, OS or CPU.

### **6. What does having a TPM in a system do for me?**

A TPM provides the first level of trust by hardening the base platform and system software in three areas:

- Protected Storage – hardware-protected storage of sensitive data
- Platform Authentication – attestable authentication of the platform
- Protected Cryptographic Processes – hardware protected key generation, random number generation, hash and digital signature
- Platform Trust State – the ability to communicate the attestable trust state of the platform.

Typical PCs without a TPM do not provide these values/benefits.

### **7. Do I need special software and does the party I conduct a transaction with also need the same software?**

Applications that use CAPI or PKCS11 can get some direct benefit from TPM enabled platforms using vendor-supplied modules. Applications that use advanced features of the TPM must be written to use the TPM functionality. TPM functionality can be exposed through direct use of the TPM or as additions to existing infrastructures.

### **8. Does the TPM provide a mechanism for general-purpose execution?**

No the TPM does not provide a general-purpose execution area. The TPM only executes on the defined set of TCGA functions. The TPM can encrypt and protect data (normally keys). After decryption of the data the TPM passes the decrypted data out of the TPM and has no further control of the data.

### **9. Can you use the TPM as an anti-piracy device?**

The TPM by itself is not intended, nor is it sufficient for anti-piracy uses. See question #4 for more details.

### **10. How do I know if I purchased a PC properly enabled with TCGA technology?**

The TCGA has provided an industry specification for the TPM. In addition to the specification the TCGA also defines Common Criteria Protection Profiles. These profiles provide a mechanism to have independent, third parties evaluations of TCGA solutions. This evaluation allows the marketplace and customers to make informed purchase decisions and to have reasonable assurance that the platform they are purchasing does provide the protections specified by TCGA.

### **11. Does TCPA certify platforms that include TPMs?**

No. The platform manufacturer needs to properly integrate the TPM into their platform design and should demonstrate that they have properly done this through the use of the appropriate protection profile. The TCPA, aside from creating the requirements for the attachment and the protection profile, does not directly certify platforms.

### **12. Does TCPA certify applications and OS's that utilize TPMs?**

No. The TCPA has no plans to create a "certifying authority" to certify OS's or applications as "trusted". The trust model the TCPA promotes for the PC is: 1) the owner runs whatever OS or applications they want; 2) the TPM assures reliable reporting of the state of the platform; and 3) the two parties engaged in the transaction determine if the other platform is trusted for the intended transaction.

### **Certification Authority**

TCPA works with and enhances existing PKI capabilities because the private keys are generated, stored, and used only in the protected storage of the TPM.

### **13. What is a "Certificate Authority (CA)"?**

A "Certification Authority" (CA) is the root of trust in the Public Key Infrastructure (PKI). A CA is an independent third party who issues and signs certificates that are used by an entity (person, website, platform, etc.) to convey information that can be trusted. The owner of a trusted platform might select a CA to provide attestable authentication of a trusted platform while maintaining the "privacy" of the owner's personal information. Another term sometimes used for such a CA is "Trusted Third Party" (TTP). Because their use is strictly limited, TCPA refers to these certificates as "credentials".

### **14. What value does TCPA add to existing Public Key Infrastructure (PKI)?**

While there are existing technologies to allow hardware protection of a private key (e.g., SmartCards), these keys are not *associated* with the platform. If a key is to be used by the platform itself to provide attestation and protect secrets and identities, it needs hardware protection such as provided by the TPM. Protection provided by software alone does not offer the same private key protection as provided by a platform with a TPM, with trusted platforms requiring certificates signed by a CA at several levels. A system administrator for example can identify the platforms that are connected or trying to access his network.

### **Uniqueness**

The TPM contains a value that is cryptographically unique. The value is only used to generate aliased ID's and is under the control of the platform owner.

### **15. What is attestation?**

Attestation is a core feature of Trusted Computing in which a platform communicates (or attests to) its state of operation. An example of attestation would be a system that measures a platform's current anti-virus definition file and stores that measurement on the TPM. When the platform wishes to prove what virus definition file is in use, the platform would attest to measurement of the AV def file by performing a digital

signature of the measurement and sending the signed message to the entity requiring information regarding the AV def file.

**16. Why does a unique identifier have to be on the platform?**

It is not possible to provide attestation without some form of identity associated with that attestation. The unique identifier provides this identity and is the basis for attestation. However, because of our concern for privacy, the TCGA has specified TCGA technology in such a way that this unique identifier is never directly used – only indirectly, and aliased through the use of certificates issued by the owner's selected Trusted Third Party (TPP).

The unique identifier is designed for use only to create a certificate request for an aliased ID from the Trusted Third Party (TPP). The owner of the platform has control over the exposure and use of both the unique identifier and all aliased IDs held by the TPM. There are two ways the owner controls this, as provided for in the TPM specification: The first is through the use of authentication. All uses of the TPM and the aliased ID's associated with it require authentication, which the owner controls. Second, the owner may *disable* the use of the TPM through the use of commands, physical "switches", or both. Remote enabling without the owner's permission is protected against by a requirement of physical presence (which means you have to be at the PC yourself) to "gate" these commands.

**17. What kinds of protections are in place to protect my personal information?**

Any personally identifiable information (PII) contained within the aliased ID is entered at the discretion of the platform owner. It may contain as little or as much PII as allowed or required by the application the owner chooses to use. A platform user may disable the TPM at any time, without the owner's knowledge or permission.

**18. Can any of this be used to track me on the web?**

At the heart of TCGA's privacy technology is the use of multiple aliased IDs. This increases the difficulty of someone conducting traffic analysis used to "track" network usage and subvert privacy.

**19. Are the unique keys in a TPM generated, and the public keys recorded by a Trusted Third Party (TPP), at the time of manufacture? If not, could a piece of software generate a key pair, pretend to be a TPM and have the public key certified?**

The unique key in the TPM, known as the endorsement key (EK), is generated during manufacturing. To validate that the EK comes from a valid TPM the manufacturer creates an endorsement credential that states that the EK in question comes from a valid TPM. So while anyone could create a SW EK and claim it comes from a valid TPM they would not have a valid endorsement credential to accompany that claim. This implies that those who rely on an EK will validate that it comes from a valid TPM.

**20. What happens if the EK within the TPM is compromised?**

A compromise of the EK on the platform would render the TPM useless. TCGA provides a common criteria protection profile requiring the TPM to meet EAL3+ to be evaluated. Customers should require evaluated systems. Suppliers will need to develop support models and policies to address this issue.

## **21. What if any one of the credentials (EK, Platform, Conformance) is compromised?**

This compromise does not occur as the result of an attack on an individual TPM; rather it occurs due to compromise of the key that signs the credential. Typically keys of this nature require protections on their use and storage. Exposure of the signing key must be addressed by the company who had the key in its control at the time, as just as would be expected for any other type of product-related failure. What is an appropriate response is a business decision that takes into account the various risks, customer concerns, costs and logistics in recovering from such a failure.

## **Processor Serial Number Comparison**

### **22. Why is this different than a processor serial number?**

The processor serial number was a unique number in the processor, which was intended to allow better asset management and customer support for IT groups and owners of numerous computers. The TPM is a device, distinct from the processor, which offers the platform owner the ability to opt-in into platform uniqueness. While the TPM contains a unique value, it is only used to create aliased ID's. The use of this unique value is under the strict control of the platform owner. Service providers never see the unique value. A service provider only sees an aliased ID, which does not expose the unique value. This design protects against the unique value being provided directly to service providers.

## **User Education**

### **23. What are you doing to educate the public?**

Public awareness of TCPA is beginning. Articles are in the news, both media and press, regarding security on computing platforms. TCPA founders and members have begun to talk openly about their solutions.

The TCPA organization will be proactive in educating developers of TCPA applications in the effective use of aliased IDs and with guidelines showing how to provide easy and obvious user interfaces for using these aliased IDs appropriately.

The TCPA encourages interested users to likewise inform themselves about platform security and software-based threats to their data and emerging security solutions for computing platforms. See [TCPA - Security Related Links](#) and other sources. Users should also ensure they fully understand the security features, user privacy controls and suppliers' privacy policies in Trusted Computing systems and applications once they reach the market.

## **OS Issues**

### **24. Does the TCPA support open source systems?**

Yes. The ability to use the TPM functionality is available to all developers of software. An open source project could determine to use TPM functionally today. The concepts of measurement, protected storage and attestation of measurements are fundamental concepts that hold true for any type of OS or application. The platforms that support TCPA today are not limited to only one OS and if open source developers provided applications that used the TPM functionality they would find support.