

TCPA Frequently Asked Questions, Rev 5.0

Updated 3 July 2002

1. What is the Trusted Computing Platform Alliance (TCPA)?

The TCPA is an industry working group, initially formed by Compaq, HP, IBM, Intel and Microsoft in October 1999 that is focusing on improving trust and security on computing platforms. Since that time, the TCPA has grown to over 150 participating companies. Information on how to join the TCPA can be found at www.trustedcomputing.org.

2. What are the goals of the TCPA?

Through the collaboration of hardware, software, communications and technology, vendors drive and implement TCPA specifications for an enhanced HW and Operating System based trusted computing platform that implements trust into client, server, networking, and communications platforms.

3. What are the key deliverables of the TCPA?

Main deliverables of the TCPA include:

- TCPA White papers, which describe the specification and how it improves computing.
- Specification version 1.1 has been developed by the members of the TCPA and published in July 2001.
- Define platform specific implementation guidelines.
- Provide advocacy for the proper use of TCPA on computing platforms.

4. When will the final specification be published?

Specification version 1.1 was published/released in July 2001 and can be accessed free of charge at www.trustedcomputing.org. The TCPA has also published two white papers, one providing an overview of the TCPA concepts and another that focuses on the benefits to IT. Both white papers are available for download from the TCPA website. Future specification revisions are anticipated as future requirements and threats evolve.

5. How will the industry benefit from the TCPA?

The TCPA has developed a Main specification version 1.1 that will help simplify and accelerate the deployment, use, and manageability of security capabilities on computers. TCPA PC Specific Information Specification version 1.0 should be used as a design guideline for PC specific implementations of trusted computing.

6. What types of capabilities are highlighted in the TCPA 1.1 Specification?

There are two areas addressed: 1) traditional cryptographic security building blocks such as protected persistent storage, digital signature and protected key exchange, hardware based key generation, and HW random number generation; 2) new capabilities such as platform integrity metrics (e.g., measuring the integrity of the BIOS, master boot record, and OS loader in the PC) and multiple aliased identities to better address privacy concerns in computing. The TCPA has defined a general purpose Trusted Subsystem that can be incorporated into a platform; the first target platform is the PC.

7. What applications and services will benefit from systems conforming to the T CPA specification?

A T CPA-enabled system offers a low cost standardized means of embedding security functionality in a platform, which means that improved levels of security can become ubiquitous, hence enabling and encouraging the development and use of applications and services that use security. Another such benefit is improved control of access to data. Previously such access has depended upon authorization or authentication. Now such access can also be linked to the state of the software in the platform. This enables the denial of access to data if rogue software, such as a virus, is introduced into a platform, because such introduction necessarily changes the software state of the platform. Other traditional features of the Subsystem, such as persistent storage and signing, will improve many applications and services such as Public Key Infrastructure (PKI) deployments and interactions, Web browsers using SSL, and email use of S-MIME among others.

8. Can you give an example of why one of these platforms is desirable?

Ubiquitous security in platforms encourages the development and use of security services. PKI related security processes, such as digital signature and key exchange, are protected through the secure T CPA subsystem. Access to data and secrets in a platform could be denied if the software environment in the platform is changed (by a virus, for example). Critical applications and capabilities such as secure email, secure web access, and local protection of data are thereby made much more secure when on a T CPA platform.

9. Does the T CPA Specification capabilities primarily benefit business or consumers most, or both?

The capabilities provided by a T CPA compliant platform will benefit both business and consumers and are being defined to be independent of a focus on specific market segments.

10. What are the licensing and/or royalty arrangements for the technologies outlined by the T CPA specification?

The T CPA spec is currently set up as a “just-publish” IP model.

11. When will platforms conforming to the T CPA spec become available?

Version 1.1 of the T CPA specification was released in July 2001 and can be accessed free of charge at www.trustedcomputing.org. Initial T CPA based platforms were announced in May 2002.

12. What do you mean by trust?

The ability to feel confident that the software environment in a platform is operating as expected. This is done by reliably measuring and reliably reporting (using aliasing) information about the platform.

13. What has the T CPA done to preserve privacy?

The T CPA believes that privacy is a necessary element of a trusted system. The T CPA Specification has taken specific steps to enhance trust while preserving privacy. The system owner has ultimate control and permissions over private information and must “opt-in” to utilize the T CPA subsystem. Integrity metrics can be reported by the T CPA platform, but do not restrict the choice and options of the owner preserving openness.

To further enhance privacy, the Specification allows the system owner to create multiple and/or anonymous identities to enhance personal security and remove avenues for identity cross-correlation.

The solutions support privacy principles in a number of ways:

1. The owner controls personalization.
2. The owner and user control the trust relationship.
3. Provides private object storage and digital signature capability.
4. Private personalization information is never exposed.
5. User keys are encrypted prior to transmission.
6. Supports multiple certificate authorities giving the user choice.

It is also important to know what the solutions are not:

1. They are not global identifiers.
2. They are not personalized before user interaction.
3. They are not fixed functions – it can be disabled permanently.
4. They are not controlled by others (only the owner controls).

14. What are the plans for TCPA Conformance, and what plans should OEMs, IHVs and ISVs make to prepare for TCPA Conformance Guidelines?

The TCPA has created protection profiles that describe the security and protections that a TCPA compliant system must meet. It is the responsibility of each vendor to review the protection profiles, create a product, write a security target that reflects the products response to the protection profiles and then have the security target and product evaluated by an independent accredited lab.

15. What timeframe is the TCPA focused on – long-term (2-4 years), short term (1-2 years), both? Will there be multiple versions of the spec delivered?

Based upon the completed version 1.1 of the Specification, we believe the TCPA has made great strides to develop a baseline of platform security building blocks. The work has also highlighted that additional system-level capabilities can be addressed by building upon the initial Specification. Currently, the TCPA committee is working to correct errata encountered in version 1.1 and is laying the groundwork for version 2.0. The definition and requirements for 2.0 are still being defined. Therefore the TCPA is focused on both short-, and long-term trusted platform evolution.

16. Does this mean I should wait to build (or deploy) a TCPA 1.1 system until a future revision comes out?

The TCPA 1.1 Specification adds significant additional trust capability and security building blocks to the platform than what exists today. Future Specification capabilities are in the process of being defined but we intend any future version to build upon the TCPA 1.1 Specification capabilities. Systems based on TCPA 1.1 have already been announced.

17. Is there something wrong with PC's today?

No. PC's today offer trust to customers – entire business segments depend on the trust they get within modern PC systems. As PC's evolve, so do the requirements for additional security capabilities that allow for trust in the computing environment of the future.

18. Does code, applets or drivers used on a TCPA-enabled system need to be signed to run?

No. The use of signed components depends upon the operating system environment in which the Subsystem operates.

19. How does a TCPA-enabled system protect against malicious and unknown use of its functions by an unauthorized user?

The TCPA capabilities that deal with sensitive or private information require the presentation of authorization data.

20. Does the TCPA spec 1.1 require a certain cryptographic algorithm (DES, AES, etc.)?

Yes. It requires RSA SHA-1 and HMAC. AES is not required in v1.1 of the specification, but may be required in future versions of the specification. The use of symmetric encryption is not required in the TPM.

21. How is this different than the “Clipper” chip?

The specification requires an open review of the implementation of a Subsystem. The specification of a TCPA Subsystem (and all its algorithms) is public knowledge. The specification requires that non-TCPA functions obtain access to secrets in the Subsystem via TCPA-functions, only. Anyone may therefore inspect the specification and discover what a Subsystem does and how it works, and what it does not do. The TCPA Subsystem does not use key-escrow.

22. How does TCPA relate to the recent Palladium announcement from Microsoft?

Microsoft is a founding member of the TCPA. Detailed Palladium questions should be directed to Microsoft at this time.