

TCPA Frequently Asked Questions, Rev 3.5

INFORMATION EMBARGO until 9AM EDT, Tuesday August 22, 2000

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 135 participating companies. Information on how to join the TCPA can be found at www.trustedpc.org.

2. What are the goals of the TCPA?

To develop a specification, based on the collaboration of PC industry platform, operating system, application, and technology vendors, that delivers a set of hardware and operating system security capabilities that customers can use to enhance the trust and security in their computing environments.

3. What will be the key deliverables of the TCPA?

Initially there will be a couple of main deliverables from the TCPA:

- TCPA Whitepapers, which will describe the specification and how it improves computing.
- A 1.0 Specification developed by the members of the TCPA for consideration and adoption.

4. When will the final specification be published?

The goal is to publish the 1.0 specification in Q4 CY2000 after a period of public review and comment of the recently release version 0.9 of the specification. 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.

5. How will the industry benefit from the TCPA?

The TCPA will develop a specification that will help simplify and accelerate the deployment, use, and manageability of security capabilities on computers.

6. What types of capabilities are being highlighted in the TCPA 1.0 Specification?

There are two areas addressed: 1) traditional security feature building blocks such as persistent storage, platform authentication (signing of data), and H/W random number generation; 2) new capabilities such as platform integrity metrics (self-inspection of the BIOS, master boot record, and OS loader in the PC) and anonymous/multiple identities to better address privacy concerns in computing. The TCPA is defining a general purpose Trusted Subsystem that can be incorporated into a platform, the first focus being the PC.

7. What applications and services will benefit from systems conforming to the TCPA spec?

A TCPA-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 TCPA 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 TCPA platform.

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

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

10. What will be the licensing and/or royalty arrangements for the technologies outlined by the TCPA specification?

The TCPA spec currently set up as a "just-publish" IP model.

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

The goal of the TCPA is to have a specification published by Q4 CY2000. The companies that design products to meet the specification will be the ones who determine when products will become available.

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 (but anonymously) reporting information about the platform.

13. What has the TCPA done to preserve privacy?

The TCPA believes that privacy is a necessary element of a trusted system. The TCPA 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 TCPA subsystem. Integrity metrics can be reported by the TCPA 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.

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 will create 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 work completed for Version 0.9 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. Therefore the TCPA is focused on both short-, and long-term trusted platform evolution.

16. Does that mean I should wait to build (or deploy) a TCPA 1.0 system until a future revision comes out?

The TCPA 1.0 Specification adds significant additional trust capability and security building blocks to the platform than what exists today. Future Specification capabilities have not been defined but we intend any future version to build upon the TCPA 1.0 Specification capabilities.

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 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 System protect against malicious and unknown use of its functions by an unauthorized user?

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

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

Yes. It requires RSA, DES, 3DES, plus SHA-1 and HMAC. AES is not required in v1.0 of the specification, but may be required in future versions of the specification.

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 does it, and what it does not do. The TCPA Subsystem does not use key-escrow.