Frequently Asked Questions:
Design, Implementation and Usage Principles Version 3.0

Q. What is the TCG Design, Implementation, and Usage Principles (Best Practices) document?

A. The TCG Best Practices document was created to provide recommendations and guidelines for best practices for developers, implementers, public and private sector be users of the TCG technology. Best practices guidelines are a recognized industry practice.

Q: What changes have been made in the Design, Implementation and Usage Principles (Best Practices) version 3.0 document?

A: The changes that have been made to the Best Practices and Principles document are not extensive and preserve the spirit of the previously released Best Practices document. TCG anticipates that Trusted Computing technologies will be adopted in a wider range of devices (for instance consumer electronic devices and embedded systems) and this revision simplifies adoption in the traditional PC ecosystem. In the new version of the document, the TPM is considered jointly with platform services (e.g. BIOS). As a result of this approach, the user opt-in is moved to the Operating System, for greater usability. Opt-in in the OS is recommended for all user driven TPM activities. The Best Practices and Principles now allow platform services use of some TPM functions.

Q: Why are these changes in the Design, Implementation and Usage Principles (Best Practices and Principles) document?

A: The TCG has adapted this document to meet the market requirements for adopting a new generation of Trusted Computing (TC) technologies. Trusted Computing is used or can be used in a wide variety of hardware devices for platform's security, including set top boxes, PCs, servers and other applications. The previous version of the document was PC-centric. These changes were made to encourage adoption of TPM and Trusted Computing technologies in general. Specifically, the current approach to provisioning and management of TPMs is frequently at variance with organizational practices.

Q: Who will benefit from these changes?

A: It will be easier for platform owners (i.e. IT departments) to provision and maintain TPMs. The owners' and users' roles will remain largely unchanged compared to the previous generation of TPM and other Trusted Computing technologies. The changes will also make it easier for TPM owners to opt-in and begin to use the TPM and for IT departments to provision and maintain TPM environments.

Q: Does the revised Design, Implementation and Usage Principles (Best Practices) document preserve the users' opt-in before the use of the TPM?

A: Yes, this version of the Best Practices recommendation preserves the spirit of the previous version of the Best Practices document. The users' opt-in to all the services involving users' data continues to be recommended.

Q. Why is opt-in required for the TPM application activation?

A: The opt-in is needed to protect TPM users' and owners privacy and choice, while offering greater usability and accessibility to all users including non-technical ones. By providing opt-in in a format that is easier to understand, it will give user greater control over TPM application activation, and does not require a user to acquire technical expertise to work with commands at the BIOS level.

Q. What does it mean that TPM can be available to platform services prior to the opt-in?

A: Prior to the platform owner's opt-in, platform services (BIOS in the case of a PC) will have access to required functionality in the TPM to protect system integrity. These activities do not involve user data or the user's ability to control his/her data.

Q. Why is the TPM available to platform services before user level opt-in?

A: The TCG developed this functionality in the new generation of TPMs, in order to align the TPM with current IT provisioning and management models in numerous organizational environments using TPMs as a critical element for Trusted Computing. This functionality is necessary to ensure adoption of Trusted Computing technologies and to offer greater protection to both the infrastructure and user data in today's computing environment in general. The TPM-using applications will still be activated by users with an opt-in.

Design, Implementation and Usage Principles Version 3.0 document is available at:
http://www.trustedcomputinggroup.org/resources/tcg_design_implementation_and_usage_principles_best_practices

Glossary of Common Trusted Computing Terms is available at:
http://www.trustedcomputinggroup.org/developers/glossary