

TRUSTED COMPUTING GROUP
FREQUENTLY ASKED QUESTIONS
PC CLIENT WORK GROUP "TCG PC CLIENT SPECIFIC IMPLEMENTATION SPECIFICATION FOR CONVENTIONAL BIOS VERSION 1.21"
February 2012

Q. What is this new specification from the PC Client Work Group?
A. This new specification is the PC Client BIOS implementations supporting TPM (Trusted Platform Module) 1.2. It defines the boot measurement events, platform configuration register usage, power state transition behavior and BIOS interfaces for the TPM. This is an update of an existing specification created several years ago.

Q. Why has the specification been updated?
A. Stakeholder feedback indicated a need to clarify the specification to make implementations more consistent.

Q. How is the specification different from the old PC Client specification?
A. The new specification details how boot measurement events are recorded and what their descriptions contain, how the TPM is enumerated to an operating system, and ACPI power state transitions.

Q. Will systems designed on this specification be compatible with those based on the old specification?
A. Yes, however, some of the clarifications may result in different event and PCR interpretations. This is not expected to impact solutions because solutions are usually flexible enough to accept a wide variety of events from different implementers or are designed for specific systems by collaborating closely with the implementer(s).

Q. Are there any significant differences in systems based on this specification compared to the old one?
A. No, but systems implementing the new specification will record an extra boot event indicating the version of the specification the platform implements.

Q. Where can I get the new specification?
A. The specification is available on the TCG website at
http://www.trustedcomputinggroup.org/files/resource_files/CB0B2BFA-1A4B-B294-D0C3B9075B5AFF17/TCG_PCClientImplementation_1-21_1_00.pdf

Copyright© 2012 Trusted Computing Group