Trusted Computing Group PC Client Work Group

TCG PC Client Specific Platform Firmware Profile Specification FAQ

March 2016

Q: What is this new specification from the PC Client Work Group?

A: This new specification is the PC Client Platform Firmware Profile for TPM 2.0 Systems. It takes the place of the PC Client Specific Implementation Specification for Conventional BIOS and the TCG EFI Platform Specification. This specification is intended for TPM 2.0 Systems. It defines the boot measurement events, platform configuration register usage, event reporting, platform power state transitions, predictive event logs, and support for the TCG Opal SSC Block SID specification.

Q: How is the specification different from the old PC Client Specifications?

A: It defines requirements for UEFI environments only. It defines the requirements for platform firmware initializing and interacting with TPM 2.0 devices, where the previous specifications dealt with TPM 1.2 devices. This specification adds support for cryptographically agile measurement logs. The method of retrieving the Event Log is different.

Q: Will Operating Systems and Applications designed to interact with the Platform Firmware and TPM on a system designed to older specifications work with this specification?

A: The TPM Library for 2.0 is not backwards compatible with Operating Systems and Applications designed to 1.2. If the Application and or OS is updated to retrieve the Event Log using the new method, the event logs can be parsed to retrieve the Specification ID Version Event from the log to determine what version of the Platform Firmware Specification the system supports.

Q: What is a cryptographically agile Event Log?

A: A cryptographically agile Event Log supports multiple Hash algorithms which produce different digest types and sizes. This enables platform firmware to produce a single event log for a platform with a TPM containing multiple PCR banks.

Q: What is a Predictive Event Log and what is it used to do?

A: A Predictive Event Log contains digests for all supported PCR banks, active and non-active. When a platform user or owner wants to change the Hash algorithm used to seal their keys, they may interact with an Operating System to request BIOS to produce a predictive event log. The predictive event log allows a consumer of a TPM key to reseal the key with the new PCR bank without having to expose the data protected by the key by decrypting it.

Q: What is required from a PC Client platform to support the Opal SSC Block SID specification?

A: PC Client platform firmware must implement the Physical Presence Operations (96-101).

Q: Where can I get the new specification?

A: http://www.trustedcomputinggroup.org/pc-client-specific-platform-firmware-profile-specification/

Contact: **Anne Price**
+1 (602)840-6495
press@trustedcomputinggroup.org