ERRATA

ERRATA

Errata Version 0.7
March 30, 2016

FOR

TCG PC Client Specific Platform Firmware Profile Specification

Specification Version 1.0
Revision 0.21
March 30, 2016

Contact: admin@trustedcomputinggroup.org

TCG Published

Disclaimers, Notices, and License Terms

Table of Contents

1. Introduction

This document describes errata and clarifications for the TCG PC Client Platform Firmware Profile (PFP) Specification v1.0 revision 21 as published. The information in this document is likely – but not certain – to be incorporated into a future version of the specification. Suggested fixes proposed in this document may be modified before being published in a later TCG Specification. Therefore, the contents of this document are not normative and only become normative when included in an updated version of the published specification. Note that since the errata in this document are non-normative, the patent licensing rights granted by Section 16.4 of the Bylaws do not apply.

2. Clarifications

2.1 Clarification 1

Section 1.2.15 Informative section paragraph 2 is not applicable to TPM 2.0 and can be ignored.

2.2 Clarification 2

Section 2.4 Informative. The statement “The Get Event Log call allows the OS to ask platform firmware to pass the platforms’ TCG event log to the OS.” contains a typo which could cause confusion. The statement should be read as: “The Get Event Log call allows the OS to ask platform firmware to pass the platform’s TCG event log to the OS.”

2.3 Clarification 3

Section 2.4.4 Normative 1 requires specification compliant firmware to measure all normative events in enabled PCR banks. It does not explicitly state what should be done with PCR banks that are not extended with measurements. For example, a TPM which defaults to an allocation of a SHA-1 bank of PCR and a SHA-256 bank of PCR, but the firmware only supports SHA-256 and thus only measures into the SHA-256 bank would leave the SHA-1 bank of PCR’s in an initialized state without measurements. The correct behavior for such a firmware would be to disable the SHA-1 bank by sending a TPM2_PCR_Allocate command that excludes unmeasured algorithms. The specification implies this, but does not explicitly state it.

2.4 Clarification 4

Section 2.4.4.6 Normative 3 under Entities that MUST be measured is unclear. The Entity that should measure configuration data is the UEFI Application running on the adapter card, not the Platform Firmware.

2.5 Clarification 5

Section 6.3 Normative 4 describes the behavior of firmware that allows a user to select the PCR bank HASH algorithm via an option in Setup. The option to change the HASH algorithm of the PCR bank will also change the measurement algorithm used by the firmware.

2.6 Clarification 6

Section 9.1.5 Informative third paragraph contains a typo. The statement “those that effect boot policy” should be “those that affect boot policy”.

2.7 Clarification 7

Section 9.2 Normative 2.e.iii contains a typo. The statement “the fields are densely packet” should state “the fields are densely packed”.

2.8 Clarification 8

Section 9.3.3 Table 7 Action Index 5 Purpose and Comments contains a typo. The statement “UEFI successfully existed Boot Services” should state “UEFI successfully exited Boot Services”.

3. Errata

3.1 Errata 1

TPM Dependency and Requirements Normative 4 is missing the Version and Revision of the TCG ACPI Specification. The Version and Revision should be Level 00 Revision 37.

3.2 Errata 2

Section 2.4.4.8 PCR[7] – Secure Boot Policy Measurements, Normative 5 under Entities that must be measured if the TPM is enabled, may be interpreted to mean that an EV_SEPARATOR event would be measured at this point, prior to measuring the Secure Boot database entries for UEFI drivers and applications as defined in normatives 6 and 7. This is incorrect. As the parenthetical statement in normative 5 implies, EV_SEPARATOR should be measured prior to the point at which Platform Firmware passes control to the Operating System as indicated by the call to Ready to Boot. The value of EV_SEPARATOR is inadvertently omitted in this section on PCR 7. EV_SEPARATOR for non-error cases is a digest of 0x00000000 or 0xFFFFFFFF. For error cases, EV_SEPARATOR is a digest of 0x00000001.

3.3 Errata 3

Section 6.3 does not correctly address the behavior of platform firmware with respect to display of the currently selected HASH algorithm. Platform firmware should display the currently selected algorithm, in addition to the available options for allocation. This is implied in the informative Table 2, but is not explicitly stated in the normative text.

3.4 Errata 4

Section 9.3.1 Table 5, Event EV_EFI_BOOT_SERVICES_APPLICATION Description is missing a Section Reference. The reference should be Section 2.4.4.5.

3.5 Errata 5

Section 10 is missing a requirement directing platform firmware to allocate PCR0-23 on selection of a HASH algorithm in setup or as a result of a PPI or EFI protocol request to change the PCR HASH algorithm. This requirement is implied in the remainder of the specification, but is not stated.