ERRATA

# ERRATA

**Errata Version 1.0**
**June 3, 2019**
**Published**

# FOR

## TCG PC Client Specific Platform Firmware Profile Specification

**Specification Version 1.04**
**June 3, 2019**

**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 v1.04 revision xx 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 Non-Host Platform Code in PCR[0]

The informative text in Section 2.3.4.1 includes text describing the measurement of non-host platforms. This text is incomplete. It should include the following statement: If a Non-Host Platform can be modified by an entity other than the Platform Firmware, it is measured in PCR[2].

## 2.2 Non-Host Platform Code in PCR[2]

The informative text in Section 2.3.4.3 does not describe the measurement of Non-Host Platform Code. It should include the following statement: If the platform contains a Non-Host Platform which can be updated by an entity other than the Platform Firmware, it is measured in PCR[2].

# 3. Errata

## 3.1 Errata 1 Non-Host Platform Components in PCR[0]

Normative 1 in Section 2.3.4.1 “Entities that SHOULD be measured if the TPM is enabled” is incomplete. The text should include a qualifying statement. The current text reads:

> “Components within Non-Host Platforms (e.g., firmware not intended to be executed by Host Platform’s CPU) that are not part of the Host Platform’s transitive trust chain but may affect the trust of the Host Platform or system. If measured, this event MUST be recorded using the event type EV_NONHOST_CODE. See Section **Error! Reference source not found.** (Event Types).”

The text should be interpreted to read:

> “Components within Non-Host Platforms (e.g. firmware not intended to be executed by Host Platform’s CPU) that can only be updated by Platform Firmware and are not part of the Host Platform’s transitive trust chain but may affect the trust of the Host Platform or system. If measured, this event MUST be recorded using the event type EV_NONHOST_CODE. See Section **Error! Reference source not found.** (Event Types).”

## 3.2 Errata 2 Non-Host Platform Configuration in PCR[1]

Normative 10 in Section 2.3.4.2 “Entities that MAY be measured if the TPM is enabled” is incomplete and incorrect. The current text reads:

> “Non-Host Platform configuration information. If the system contains a Non-Host Platform, Platform Firmware SHOULD use the event type EV_NONHOST_CONFIG to record any security-relevant configuration information or data. See Section **Error! Reference source not found.** (Event Types).”

The text should be interpreted to read:

> "Non-Host Platform configuration information. If the system contains a Non-Host Platform which can only be updated by Platform Firmware, Platform Firmware SHOULD measure the configuration and MUST use the event type EV_NONHOST_CONFIG to record any security-relevant configuration information or data. See Section **Error! Reference source not found.** (Event Types).”

## 3.3 Errata 3 Non-Host Platform Components in PCR[2]

Section 2.3.4.3 should contain a normative statement similar to Normative 1 in PCR[0] Entities that SHOULD be measured if the TPM is enabled. The missing text is as follows:

> “Components within Non-Host Platforms (e.g., firmware not intended to be executed by the Host Platform’s CPU) that can be updated by entities other than Platform Firmware and are not part of the Host Platform’s transitive trust chain but may affect the trust of the Host Platform or system. If measured, this event MUST be recorded using the event type EV_NON_HOST_CODE. See Section 9.4.1 (Event Types).”

## 3.4 Errata 4 Non-Host Platform Configuration in PCR[3]

Section 2.3.4.4 should contain a normative statement similar to Normative 10 in PCR[1]. The text should be interpreted to read:

"Non-Host Platform configuration information. If the system contains a Non-Host Platform which can be updated by entities other than Platform Firmware, Platform Firmware SHOULD measure the configuration and MUST use the event type EV_NONHOST_CONFIG to record any security-relevant configuration information or data. See Section **Error! Reference source not found.** (Event Types)."

## 3.5 Errata 5 Descriptions for Non-Host Platform measurements Table 9

The event description for EV_NONHOST_CODE in Table 9, Section 9.4.1 Event Types is incomplete. The text “Used for PCR[0] only” should be interpreted as “Used for PCR[0,2] only”. The Section reference should include a reference to Section 2.3.4.3.

The event description for EV_NONHOST_CONFIG is also incomplete. The text “Used for PCR[1] only” should be interpreted as “Used for PCR[1, 3]. The Section reference should include a reference to Section 2.3.4.4.