ERRATA

ERRATA

Errata Version 0.5
July 15, 2016

FOR

TCG EFI Protocol Specification

Specification Version 1.0
Revision 0.13
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 EFI Protocol Specification v1.0 revision 13 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 6.4.4 normative 1 uses language which might be confusing. It should be interpreted as if it reads: If the This parameter or the ProtocolCapability parameter are NULL, the functional call will return EFI_INVALID_PARAMETER.

2.2 Clarification 2

Section 6.4.4 normative 2 uses the mathematical symbol "<" which should be interpreted as "is less than". In this case, the reader may interpret the statements as if they read: If input ProtocolCapability.Size is less than the size of EFI_TCG2_BOOT_SERVICE_CAPABILITY up to and including the vendor ID field, the function will set ProtocolCapability.Size equal to the size of EFI_TCG2_BOOT_SERVICE_CAPABILITY up to and including the vendor ID field and will return the error code EFI_BUFFER_TOO_SMALL. The values of the fields after the vendor ID field will be undefined.

2.3 Clarification 3

Section 6.4.4 first paragraph will be clarified to read:

The EFI_TCG2_PROTOCOL.GetCapability() function call provides EFI protocol version and capability information as well as state information about the EFI TCG2 protocol. The caller SHALL set the Size field of the EFI_TCG2_BOOT_SERVICE_CAPABILITY structure that is allocated. The structure is not packed. Future versions of this function may add additional fields to the structure and increase its size. The Size value passed in by the caller will determine which fields the function will be able to populate.

2.4 Clarification 4

Section 6.4.4 normative 3 uses the mathematical symbol "<", which should be interpreted as "is less than". In this case, the reader may interpret the statement as if it reads: If input ProtocolCapability.Size is less than the size of EFI_TCG2_BOOT_SERVICE_CAPABILITY, the function will initialize the fields included in ProtocolCapability.Size. The values of the remaining fields will be undefined.

2.5 Clarification 5

Section 6.6.5, the last normative paragraph may be confusing to the reader. It should be interpreted to read:

The description of the construction of the event log is explicit in order to clearly define expected behavior. Other implementations that provide the same behavior at the protocol level are acceptable.

2.6 Clarification 6

Section 6.9.3 the first sentence will be clarified to read: This function first determines if the requested bitmap of PCR banks is valid.

2.7 Clarification 7

In Section 7, Table 21, the description of the Version field will be clarified to read: The version of this structure. Versioning allows to append new fields in the future.

2.8 Clarification 8

In Section 7, Table 21, the field name NumberOfEvent should be NumberOfEvents.

3. Errata

3.1 Errata 1

Section 2 under bullet point 3, the UEFI Specification version 2.4 (Errata B) should be UEFI Specification version 2.3.1c or later.

3.2 Errata 2

In Section 4 the list of unsigned integer types UINT8, UINT16, and UINT32 should include UINT64.

3.3 Errata 3

In Section 6.4.3, in Table 6, the description of TPMPresentFlag should be extended or replaced by “True = TPM is present”.

3.4 Errata 4

Section 6.7.3 normative text implies, but does not explicitly state that all TPM return codes except TPM2_RC_RETRY may be returned by firmware.