ERRATA

Errata Version 0.6
November 13, 2023

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

THIS ERRATA IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE.

Without limitation, TCG and its members and licensors disclaim all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification and to the implementation of this specification, and TCG disclaims all liability for cost of procurement of substitute goods or services, lost profits, loss of use, loss of data or any incidental, consequential, direct, indirect, or special damages, whether under contract, tort, warranty or otherwise, arising in any way out of use or reliance upon this specification or any information herein.

Contact the Trusted Computing Group at www.trustedcomputinggroup.org for information on specification licensing through membership agreements.

Any marks and brands contained herein are the property of their respective owners.

Table of Contents

1. Introduction 4
2. Clarifications 5
2.1 Clarification 1 – Section 6.4 EFI_TCG2_PROTOCOL.GetCapability 5
2.2 Clarification 2 – Section 6.4 EFI_TCG2_PROTOCOL.GetCapability 5
2.3 Clarification 3 – Section 6.4 EFI_TCG2_PROTOCOL.GetCapability 5
2.4 Clarification 4 – Section 6.4 EFI_TCG2_PROTOCOL.GetCapability 5
2.5 Clarification 5 – Section 6.6 EFI_TCG2_PROTOCOL.HashLogExtendEvent 5
2.6 Clarification 6 – Section 6.9 EFI_TCG2_PROTOCOL.SetActivePcrBanks 6
2.7 Clarification 7 – Section 7 Log entries after Get Event Log service 6
2.8 Clarification 8 – Section 7 Log entries after Get Event Log service 6
3. Errata 7
3.1 Errata 1 – Section 2 References 7
3.2 Errata 2 – Section 4 Abbreviations and Terminology 7
3.3 Errata 3 – Section 6.4 EFI_TCG2_PROTOCOL.GetCapability 7
3.4 Errata 4 – Section 6.7 EFI_TCG2_PROTOCOL.SubmitCommand 7
3.5 Errata 5 – Section 6.4 EFI_TCG2_PROTOCOL.GetCapability 8
3.6 Errata 6 – Section 6.4 EFI_TCG2_PROTOCOL.GetCapability 8

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 EFI_TCG2_PROTOCOL.GetCapability

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 EFI_TCG2_PROTOCOL.GetCapability

This Clarification is replaced by Errata 5.

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 EFI_TCG2_PROTOCOL.GetCapability

Section 6.4.4 first paragraph should be interpreted as if it reads:

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 EFI_TCG2_PROTOCOL.GetCapability

This Clarification is replaced by Errata 6.

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 EFI_TCG2_PROTOCOL.HashLogExtendEvent

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 EFI_TCG2_PROTOCOL.SetActivePcrBanks

Section 6.9.3 the first sentence should be interpreted as if it reads: This function first determines if the requested bitmap of PCR banks is valid.

2.7 Clarification 7 – Section 7 Log entries after Get Event Log service

In Section 7, Table 21, the description of the Version field should be interpreted as if it reads: The version of this structure. Versioning allows to append new fields in the future.

2.8 Clarification 8 – Section 7 Log entries after Get Event Log service

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

3. Errata

3.1 Errata 1 – Section 2 References

Current text in bullet point 3 is:

UEFI Specification version 2.4 (Errata B)

It should be:

UEFI Specification version 2.3.1c or later

3.2 Errata 2 – Section 4 Abbreviations and Terminology

Current text in list includes:

UINT8, UINT16, UINT32

It should be

UINT8, UINT16, UINT32, UINT64

3.3 Errata 3 – Section 6.4 EFI_TCG2_PROTOCOL.GetCapability

Current text in Section 6.4.3, in Table 6:

TPMPresentFlag	False = TPM not present

It should be extended to:

TPMPresentFlag	False = TPM not present, True = TPM is present

3.4 Errata 4 – Section 6.7 EFI_TCG2_PROTOCOL.SubmitCommand

Current text in Section 6.7.3:

The firmware SHALL not return TPM2_RC_RETRY prior to the completion of the call to ExitBootServices().

It should be changed to:

The firmware SHALL not return TPM2_RC_RETRY prior to the completion of the call to ExitBootServices(). All TPM return codes except TPM2_RC_RETRY may be returned by firmware.

3.5 Errata 5 – Section 6.4 EFI_TCG2_PROTOCOL.GetCapability

This function needs to support backward compatibility with OS's that were developed using the previous version of the specification. The function behavior is not clearly defined in the current specification.

Current text in Section 6.4.4 normative 2 is:

2. If the input ProtocolCapability.Size < size of the EFI_TCG2_BOOT_SERVICE_CAPABILITY up to and including the vendor ID field, the function will set ProtocolCapability.Size equal to size of the 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 remaining fields will be undefined.

The text should be replaced by:
2. If input ProtocolCapability.Size is less than the size of EFI_TCG2_BOOT_SERVICE_CAPABILITY up to and including the ManufacturerID field, the function will set ProtocolCapability.Size equal to sizeof(EFI_TCG2_BOOT_SERVICE_CAPABILITY) and will return the error code EFI_BUFFER_TOO_SMALL. The values of the remaining fields will be undefined.

3.6 Errata 6 – Section 6.4 EFI_TCG2_PROTOCOL.GetCapability

This function needs to support backward compatibility with OS's that were developed using the previous version of the specification. The function behavior is not clearly defined in the current specification.

Current text in Section 6.4.4 normative 3 is:

3. If the input ProtocolCapability.Size < sizeof(EFI_TCG2_BOOT_SERVICE_CAPABILITY) the function will initialize the fields included in ProtocolCapability.Size. The values of the remaining fields will be undefined.

The text should be replaced by:

3. If input ProtocolCapability.Size is equal to or greater than the size of EFI_TCG2_BOOT_SERVICE_CAPABILITY up to and including the ManufacturerID field and input ProtocolCapability.Size is less than the size of EFI_TCG2_BOOT_SERVICE_CAPABILITY, the function will initialize the fields up to and including the ManufacturerID field. The ProtocolCapability.Size is set to the size of EFI_TCG2_BOOT_SERVICE_CAPABILITY up to and including the ManufacturerID field. The values of the fields after ManufacturerID field will be undefined. The following return values SHALL be set in this case to override normative 4:

ProtocolCapability.StructureVersion.Minor = 0.

ProtocolCapability.ProtocolVersion.Minor = 0.