

E
R
R
A
T
A

Errata for TCG PC Client Platform TPM Profile for TPM 2.0
Version 1.07

Version 1

July 13, 2026

Contact: admin@trustedcomputinggroup.org

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 disclaims 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.

This document is copyrighted by Trusted Computing Group (TCG), and no license, express or implied, is granted herein other than as follows: You may not copy or reproduce the document or distribute it to others without written permission from TCG, except that you may freely do so for the purposes of (a) examining or implementing TCG specifications or (b) developing, testing, or promoting information technology standards and best practices, so long as you distribute the document with these disclaimers, notices, and license terms.

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.

CONTENTS

DISCLAIMERS, NOTICES, AND LICENSE TERMS 1

1 Introduction 3

2 Errata 4

 2.1 Errata 1 Table 3 Algorithm TPM_ALG_MLDSA Comments 4

 2.2 Errata 2 Table 3 PC Client Algorithms 4

 2.3 Errata 3 Table 16 Mandatory/Optional Commands 4

 2.4 Errata 4 TPM_LOC_CTRL_x.Seize 4

3 Clarifications 6

 3.1 Clarification 1 Table 3 PC Client Algorithms 6

 3.2 Clarification 2 Table 5 Mandatory/Optional Commands 6

1 Introduction

This document describes errata and clarifications for the TCG PC Client Platform TPM Profile for TPM 2.0 Version 1.07 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 Errata

2.1 Errata 1 Table 3 Algorithm TPM_ALG_MLDSA Comments

The second sentence in the comment for TPM_ALG_MLDSA contains a typographical error. The current text reads as follows:

This is a PQC signing algorithm

The TPM SHALL support either ML-DSA-65 or ML-DSA-87. The TPM SHOULD support ML-DSA-44, ML-DSA-65, **or** ML-DSA-87. ML-DSA support is mandatory as of PTP version 1.07.

The second sentence is corrected as follows:

This is a PQC signing algorithm

The TPM SHALL support either ML-DSA-65 or ML-DSA-87. The TPM SHOULD support ML-DSA-44, ML-DSA-65, **and** ML-DSA-87. ML-DSA support is mandatory as of PTP version 1.07.

This correction resolves an inconsistency with the first sentence that indicates the TPM is required to support either ML-DSA-65 or ML-DSA-87. The second sentence as stated implies that a TPM could only support ML-DSA-44 and meet the requirements. That interpretation conflicts with the first sentence.

2.2 Errata 2 Table 3 PC Client Algorithms

For TPM_ALD_ID values not listed in Table 3, the algorithm ID can be considered Optional as defined in Section 4.3 PC Client Algorithms.

2.3 Errata 3 Table 16 Mandatory/Optional Commands

The commands TPM2_Encapsulate and TPM2_Decapsulate were added in PTP 1.07 and made mandatory. The TPM Library Specification allows Platform TPM Profiles to designate what algorithms are required for these commands. Table 16 does not indicate if support for TPM_ALG_ECC is required or not. Support for TPM_ALG_ECC is not required for these commands in PTP 1.07.

2.4 Errata 4 TPM_LOC_CTRL_x.Seize

The specification section 6.5.3.5.2.1 TPM_LOC_CTRL bitfield Seize describes the required actions a CRB TPM takes when the Seize field is set by a higher locality than the currently active locality. The current text reads:

Field: Seize

1. If the write to TPM_LOC_CTRL_x.Seize occurs from a locality of higher priority than the current locality:
 - a. The TPM SHALL clear the TPM_LOC_STATE_x.activeLocality and TPM_LOC_STATE_x.locAssigned fields for any active locality of lower priority than the locality seizing the TPM.
 - b. The TPM SHALL NOT change the state of the TPM_LOC_STATE_x.locAssigned field for any locality except the one writing this field.
 - c. The TPM SHALL abort any command that is currently in process, as defined in Section 6.5.3.3 CRB Command Aborts.
2. If the write occurs from a locality that is equal to or lower than the current locality the TPM SHALL ignore the write.
3. A read from TPM_LOC_STATE_x.Seize SHALL return 0.

Normative 1.a and 1.b are incorrect and normative 3 contains a typographical error. The normative text should be interpreted to read:

Field: Seize

1. If the write to TPM_LOC_CTRL_x.Seize occurs from a locality of higher priority than the current locality:

- a. The TPM SHALL set the TPM_LOC_STATE_x.activeLocality field to the locality value of the locality seizing the TPM.
 - b. The TPM SHALL abort any command that is currently in process, as defined in Section 6.5.3.3 CRB Command Aborts.
2. If the write occurs from a locality that is equal to or lower than the current locality the TPM SHALL ignore the write.
3. A read from TPM_LOC_CTRL_x.Seize SHALL return 0.

2.5 Errata 5 Table 20 – Allocation of Register Space for FIFO and CRB Access

The table contains an undefined register at offset 001Ch titled TPM_INTF_CAPABILITYX_0 in both the FIFO Register Name and CRB Register Name columns. This an error. This address space should be marked as Reserved.

3 Clarifications

3.1 Clarification 1 Table 3 PC Client Algorithms

The description for the truncated SHAKE algorithms is inaccurate.

The current description states:

TPM_ALG_SHAKE_256_192	O	This is an extendible output function
TPM_ALG_SHAKE_256_256	O	This is an extendible output function
TPM_ALG_SHAKE_256_512	O	This is an extendible output function

The correct description is:

TPM_ALG_SHAKE_256_192	O	This is a hash function
TPM_ALG_SHAKE_256_256	O	This is a hash function
TPM_ALG_SHAKE_256_512	O	This is a hash function

3.2 Clarification 2 Table 5 Mandatory/Optional Commands

The description for TPM2_SignDigest includes a statement that a new capability allows a caller to discover which parameters and options the TPM supports for this command, such as support for external mu. This statement could be interpreted to mean that support for external mu is mandatory. Support for external mu is optional.