

# ERRATA

## ERRATA

Errata Version 0.3  
February 22, 2017

FOR

## TCG PC Client Platform Physical Presence Interface Specification

Specification Version 1.30  
Revision 0.52  
March 16, 2015

Contact: [admin@trustedcomputinggroup.org](mailto:admin@trustedcomputinggroup.org)

**TCG Published**

Copyright © TCG 2017

## 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.

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](http://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. Errata .....   | 5 |
| 2.1 Errata in Section 9, Table 2, Physical Presence Interface Operations Summary for TPM 2.0..... | 5 |

## 1. Introduction

This document describes errata and clarifications for the TCG PC Client Platform Physical Presence Interface Specification v1.30 revision 0.52 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 in Section 9, Table 2, Physical Presence Interface Operations Summary for TPM 2.0

Table 2 defines Physical Presence Interface (PPI) Operations that are defined for systems with TPM 2.0 and includes a column “When Physical Presence Confirmation is Required.” The behavior is defined by flags. For instance, the PPI Operation to clear a TPM (operation 5) requires physical presence confirmation when the flag “PPRequiredForClear is TRUE.” Other operations modify these flags. For instance, operation 17 SetPPRequiredForClear\_True will set the PPRequiredForClear flag to TRUE. Operation 17 itself does not require physical presence confirmation. The complimentary operation 18, on the other hand, “Always” requires physical presence confirmation. This is to prevent a malicious caller disabling the physical presence confirmation for clearing the TPM without a confirmation.

Other operations that manipulate similar flags have the requirements switched. The values in Table 2 contradict Table 4 in revision 52 of the PPI specification version 1.30. For instance, operation 25, SetPPRequiredForChangePCRs\_False, has no physical presence confirmation requirement, but should, and operation 26, SetPPRequiredForChangePCRs\_True, has the physical presence confirmation requirement “Always”, but should not.

The rows for these operations in Table 2 should be changed as follows:

| Operation Value | Operation Name                            | What the operation may change |  | Mandatory or Optional | When Physical Presence Confirmation is Required | May need additional boot cycle |
|-----------------|---|-------------------------------|--|-----------------------|---|--------------------------------|
|                 |   | TPM State                     | Persistent Firmware TPM Management Flags |                       |   |                                |
| ...             |   |                               |  |                       |   |                                |
| 25              | SetPPRequiredForChangePCRs_False          |                               | X  | O3                    | Always  |                                |
| 26              | SetPPRequiredForChangePCRs_True           |                               | X  | O3                    |   |                                |
| 27              | SetPPRequiredForTurnOn_False              |                               | X  | O4                    | Always  |                                |
| 28              | SetPPRequiredForTurnOn_True               |                               | X  | O4                    |   |                                |
| 29              | SetPPRequiredForTurnOff_False             |                               | X  | O5                    | Always  |                                |
| 30              | SetPPRequiredForTurnOff_True              |                               | X  | O5                    |   |                                |
| 31              | SetPPRequiredForChangeEPS_False           |                               | X  | O6                    | Always  |                                |
| 32              | SetPPRequiredForChangeEPS_True            |                               | X  | O6                    |   |                                |
| ...             |   |                               |  |                       |   |                                |
| 98              | SetPPRequiredForEnable_BlockSIDFunc_True  |                               |  | O8                    |   |                                |
| 99              | SetPPRequiredForEnable_BlockSIDFunc_False |                               |  | O8                    | Always  |                                |
| 100             | SetPPRequiredForDisable_BlockSIDFunc_True |                               |  | O9                    |   |                                |

| Operation Value | Operation Name                             | What the operation may change |  | Mandatory or Optional | When Physical Presence Confirmation is Required | May need additional boot cycle |
|-----------------|--|-------------------------------|--|-----------------------|---|--------------------------------|
|                 |  | TPM State                     | Persistent Firmware TPM Management Flags |                       |   |                                |
| 101             | SetPPRequiredForDisable_BlockSIDFunc_False |                               |  | O9                    | Always  |                                |
| ...             |  |                               |  |                       |   |                                |