

Errata for PC Client Platform TPM Profile for TPM 2.0

Version 1.05
Revision 14
September 4, 2020

Version 1.1
November 8, 2021

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, ERRATA OR SAMPLE.

Without limitation, TCG disclaims all liability, including liability for infringement of any proprietary rights, relating to use of information in this Errata and to the implementation of this Errata, 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 Errata 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 document 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 1 TPM_PT_NV_COUNTERS_MAX.....	4
2.2 Errata 2 Section 5.3.3 Timing and Protocol.....	4
2.3 Errata 3 Section 8.1.8 Availability after Reset	4
2.4 Errata 4 Section 8.3.5.12 TPM_DATA_CSUM.....	4

1 Introduction

This document describes errata and clarifications for the TCG PC Client Platform TPM Profile for TPM 2.0 v1.05 revision 14 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 1 TPM_PT_NV_COUNTERS_MAX

The TPM Library Specification allows the TPM to report a value of 0 for this property type when there is no fixed minimum and the number of counters that can be defined is determined by the available NV memory pool. The PTP requires a minimum value of 6, which contradicts the TPM Library Specification. A value of 0 is also permissible.

2.2 Errata 2 Section 5.3.3 Timing and Protocol

Normative 2 requires the TPM to respond within TIMEOUT_B to the indicated command. Normative 3 strongly recommends that the TPM respond within 250us and requires the TPM to respond within TIMEOUT_B to the indicated commands. These requirements contradict Table 17 – Command Timing in Section 6.5.1.3 Command Duration. The correct timeout is defined in Table 17.

Normative 2 and 3 do not describe any requirement for command timing and contradict the HASH_x command timing indicated in Table 17 – Command Timing in Section 6.5.1.3 Command Duration. The correct timing is defined in Table 17.

2.3 Errata 3 Section 8.1.8 Availability after Reset

The requirement for an I2C-TPM to be available for communication after deassertion of reset does not consider the additional time required to comply with FIPS 140-2 self-test requirements. The requirement for a FIPS 140-2 compliant TPM implemented with the I2C hardware interface is the same as for a FIPS 140-2 compliant TPM implemented to SPI and should be interpreted as stated in Section 7.6 Reset Timing normative 3.

2.4 Errata 4 Section 8.3.5.12 TPM_DATA_CSUM

Normatives 1.f.iii and 1.f.iv contain typographic errors in the Hexadecimal string. The number “16” is appended to the string. The numbers should be interpreted as follows:

1.f.iii String as written: 00 C1 00 00 00 0C 00 00 00 99 00 0116

1.f.iii Corrected String: 00 C1 00 00 00 0C 00 00 00 99 00 01₁₆

1.f.iv String as written: 80 01 00 00 00 0C 00 00 01 44 00 0016

1.f.iv Corrected String: 80 01 00 00 00 0C 00 00 01 44 00 00₁₆.