TRUSTED® COMPUTING GROUP

ERRATA

Errata for PC Client Platform TPM Profile for TPM 2.0 Version 1.05 Revision 14

Version 1.2
Revision 5
February 2, 2024

Contact: admin@trustedcomputinggroup.org

PUBLISHED

DISCLAIMERS, NOTICES, AND LICENSE TERMS

CONTENTS

1 Introduction

This document describes errata and clarifications for the TCG PC Client Platform TPM Profile for TPM 2.0 Version 1.05 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 Clarifications

2.1 Clarification 1 Section 7.6 Reset Timing

In certain cases, the TPM cannot fulfil the reset timing requirement for a SPI interface.

Normative 3 specifies a maximum startup time of 50ms for SPI TPMs that are compliant with FIPS 140-2 Self-Test requirements. Note that the startup time may be longer for TPMs that are FIPS 140-3 validated, as the Self-Test requirements are different from FIPS 140-2.

Firmware interacting with SPI TPMs (FIFO and CRB interface) that comply with FIPS 140-3 Self-Test may encounter TPMs that respond within the following timeouts:

- 200ms for the completion of _TPM_INIT instead of 50ms specified for TPMs that comply with FIPS 140-2.
- 1 second for the completion of _TPM_INIT when the TPM performs maintenance, recovery of NV or field upgrades.

2.2 Clarification 2 Section 8.1.8 Availability after reset

In certain cases, the TPM cannot fulfil the reset timing requirement for an I2C interface.

Normative 2 (corrected by Errata 3 Section 8.1.8 Availability after Reset) specifies a maximum startup time of 50ms for I2C TPMs that are compliant with FIPS 140-2 Self-Test requirements. Note that the startup time may be longer for TPMs that are FIPS 140-3 validated, as the Self-Test requirements are different from FIPS 140-2.

Firmware interacting with I2C TPMs that comply with FIPS 140-3 Self-Test may encounter TPMs that respond within the following timeouts:

- 200ms for the completion of _TPM_INIT instead of 50ms specified for TPMs that comply with FIPS 140-2.
- 1 second for the completion of _TPM_INIT when the TPM performs maintenance, recovery of NV or field upgrades.

3 Errata

3.1 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.

3.2 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.

3.3 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.

3.4 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 01$_{16}$

1.f.iii Corrected String: 00 C1 00 00 00 0C 00 00 00 99 00 01$_{16}$

1.f.iv String as written: 80 01 00 00 00 0C 00 00 01 44 00 00$_{16}$

1.f.iv Corrected String: 80 01 00 00 00 0C 00 00 01 44 00 00$_{16}$.

3.5 Errata 5 Section 6.5.3.3 Control Area Extension

Table 34 – TPM CRB Control Area Extension states that Clear bits 31:0 are Read Only. However, the correct property is Read / Write. In addition, the related description for Cancel command may be clarified in future PTP versions. Table 34 should be as follows:

Abbreviation:				TPM_CRB_CTRL_EXT_x
General Description:				Control Area Extension
Bit Descriptions:				
63:32	Read /Write	Remaining Bytes	0	Number of command/response bytes in a chunk that remain to be transferred
31:0	Read/ Write	Clear	0	Used by Software to cancel the transfer of command/response data chunks Writes (0000 0001h): Cancel a transaction using the chunk mechanism Cleared to 0 by the TPM once transaction has been cancelled.

3.6 Errata 6 Section 8.2.2.1 I2C Protocol Usage Scenarios

Table 53 — Register Behavior Based on Locality Setting for I2C defines the return values for TPM_DATA_CSUM Register for all locality scenarios. Table 53 is incorrect because the TPM may return the correct value or 0xFF when reading TPM_DATA_CSUM from state “Set for another locality“ or “Not set“.

The current table:

Set for This Locality		**Set for another Locality**		**Not Set**	
READ	**WRITE**	**READ**	**WRITE**	**READ**	**WRITE**
TPM_DATA_CSUM Register					
TPM returns correct value	Read-only register	TPM returns correct value	Read-only register	TPM returns correct value	Read-only register

The corrected table:

Set for This Locality		**Set for another Locality**		**Not Set**	
READ	**WRITE**	**READ**	**WRITE**	**READ**	**WRITE**
TPM_DATA_CSUM Register					
TPM returns correct value	Read-only register	TPM returns correct value or 0xFF	Read-only register	TPM returns correct value or 0xFF	Read-only register