TRUSTED® COMPUTING GROUP

ERRATA

# Errata for TCG Trusted Platform Module Library

Family “2.0”
Level 00 Revision 01.59
November 8, 2019

Version 1.1
June 18, 2020

Contact: admin@trustedcomputinggroup.org

PUBLISHED

# DISCLAIMERS, NOTICES, AND LICENSE TERMS

# CONTENTS



 

# 1 Introduction

This document describes errata and clarifications for the TCG Trusted Platform Module Library Family “2.0” Level 00 Revision 01.59 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.

The heading of each errata in section 2 indicates whether the errata affects the specification text or the reference code implementation. This is indicated by the word “spec text” or “code” in square brackets (“[]”).

 

# 2 Errata

## 2.1 TPM_SPEC Date Constants [spec text, code]

Table 6 in Part 2, 6.1 TPM_SPEC (Specification Version Values) should be replaced with:

**Table 6 — Definition of (UINT32) TPM_SPEC Constants <>**

| Name | Value | Comments |
|---|---|---|
| TPM_SPEC_FAMILY | 0x322E3000 | ASCII “2.0” with null terminator |
| TPM_SPEC_LEVEL | 00 | the level number for the specification |
| TPM_SPEC_VERSION | 159 | the version number of the spec (001.59 * 100) |
| TPM_SPEC_YEAR | 2020 | the year of the version |
| TPM_SPEC_DAY_OF_YEAR | 170 | the day of the year (June 18) |

That is, the spec date fields TPM_SPEC_YEAR and TPM_SPEC_DAY_OF_YEAR should be set to the date of this Errata document.

## 2.2 Non-orderly Shutdown - *failedTries* [code]

The following text in Part 1, 19.8.6 Non-orderly Shutdown describes the reference code implementation of TPM2_Startup() after a non-orderly Shutdown:

An alternative implementation sets an NV flag indicating that access to a DA protected object occurred during this boot cycle. After a non-orderly restart, if the flag is set, the TPM increments *failedTries* and clears the flag. If the flag is clear, there is no need to increment *failedTries*.

EXAMPLE This handles the case where a platform repeatedly does a non-orderly shutdown, possibly due to a low battery. Without the flag, *failedTries* would increment on each reboot and the TPM would go into lockout.

The reference code does not correctly implement the behavior described above if a DA protected object is accessed after a TPM2_Shutdown(). In this case, the NV flag (indicating that access to a DA protected object occurred during this boot cycle) is not set correctly. When a power loss happens, *failedTries* is not incremented on the next TPM2_Startup().

The check and increment of *failedTries* on TPM2_Startup() ensures that a failed authorization attempt is recorded by the TPM (e.g. because NV memory is unavailable).

## 2.3 ACT *preserveSignaled* [spec text, code]

The ACT *preserveSignaled* attribute is incorrectly described in the Library Spec Part 2 and 3, and is incorrectly implemented in the reference code in Part 4, 7.8.3.2 ActStartup(). The reference code always returns zero for the *preserveSignaled* attribute.

In Part 2, 8.12 TPMA_ACT, the following text should be added to the description of the ACT attribute structure.

The *preserveSignaled* action over a power cycle is:

 

- Cold (with power loss between Shutdown and Startup) TPM Reset, TPM Restart, TPM Resume
  - *preservedSignaled* is set to CLEAR
- Warm (no power loss between Shutdown and Startup) TPM Reset, TPM Restart, TPM Resume
  - *preserveSignaled* holds the state of *signaled* before the power cycle

NOTE 1: *preserveSignaled* allows startup software to determine if the startup cycle was likely initiated by an ACT event. If power was lost, it doesn't care.

In Part 2, 8.12 TPMA_ACT, Table 40 should be replaced with the following table:

**Table 40 — Definition of (UINT32) TPMA_ACT Bits**

| Bit | Name | Definition |
|---|---|---|
| 0 | signaled | **SET (1):** The ACT has signaled<br>**CLEAR (0):** The ACT has not signaled |
| 1 | preserveSignaled | Preserves the state of *signaled*, depending on the power cycle |
| 31:2 | Reserved | shall be zero |

In Part 3, 9.3 TPM2_Startup, in the general description of the command actions on TPM Reset and on TPM Restart, the following bullet point should be changed.

From:

- For each ACT the timeout is reset to zero, the *signaled* attribute is set to CLEAR (if *preserveSignaled* is CLEAR), and the *authPolicy* is set to the Empty Buffer and its hashAlg is set to TPM_ALG_NULL.

To:

- For each ACT the timeout is reset to zero, the *signaled* attribute is set to CLEAR, its *authPolicy* is set to the Empty Buffer, and its hashAlg is set to TPM_ALG_NULL.

That is, the condition in brackets "(if *preserveSignaled* is CLEAR)" should be removed.

In Part 3, 32.2 TPM2_ACT_SetTimeout, in the general description, the following sentence should be added:

When this command is successful, *preserveSignaled* will be CLEAR.

 