ERRATA

ERRATA

Errata Version 1.0
February 20, 2019

FOR

Protection Profile Automotive-Thin Specific TPM

Level 0 Version 1.0
December 12, 2018

Contact: admin@trustedcomputinggroup.org

TCG Published

Disclaimers, Notices, and License Terms

Table of Contents

1. Introduction

This document describes errata and clarifications for the TCG Protection Profile for Automotive-Thin Specific TPM Version 1.0 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 FIA_UAU.5.2 Multiple Authentication Mechanisms

Iteration (3) may be confusing. As clarification, if a sessionType of TPM_SE_HMAC is selected, the TPM is required to enforce HMAC authorization for the session.

3. Errata

3.1 Errata 1 Table 8

There are errors in Table 8. The first error is inclusion of the Operations Delete and Make Persistent on Row 4 Endorsement Primary Key. The second error is the inclusion of the security attributes TPMA_NV_PPWRITE and TPMA_NV_AUTHWRITE in row 7 NV storage. The third error is inclusion of the command TPM2_NV_ReadPublic in the operations section. These items should be considered removed.

3.2 Errata 2 FCS_COP.1.1/AES

The SFR currently contains a statement “the specified algorithm AES in the mode CFB” followed by a selection for additional modes. It is permissible to select “none” for additional modes. This interpretation negates the need for Application Note 8. Application Note 8 should be ignored. Additionally, the listings of ISO/IEC and NIST standards are misleading. The list should be interpreted as “that meet the following: ISO/IEC 10116 [27] and ISO/IEC 18033-3 [31] or NIST Pub -38a [22]”.

3.3 Errata 3 FCS_COP.1.1/ASYMMED

The first selection in this SFR is missing the option “none”. The statement should be interpreted as: “The TSF shall perform asymmetric decryption and [selection: none, encryption].”

3.4 Errata 4 FCS_COP.1.1/SIGN

The second selection is missing an assignment corresponding to the assignment in the first selection. The selection should be interpreted as: [selection: 2048 bits, 256 bits, [assignment: *other key sizes*].

3.5 Errata 5 FDP_ACC.1.1/NVM

Subject (3) ADMIN should not be included, as the Automotive-Thin TPM does not require this role. ADMIN should be considered removed.

3.6 Errata 6 FDP_ACC.1.1/Hier

Operation (3) is incorrectly included. TPM2_Load is not applicable to creation of primary objects. Operation (3)

3.7 Errata 7 FDP_ACC.1.1/ExIm

TPM2_ReadPublic is missing from the list of operations, but is referenced in a subsequent FDP_ACC.1 SFR. Object number (2) incorrectly lists platformAuth as the security attribute. The correct security attribute is authorization data.

3.8 Errata 8 FDP_ACF.1.1/NVM

Number (1) erroneously includes the role “ADMIN” in the list of subjects addressed. This role is not required by the Automotive-Thin TPM and as such should be considered removed.

3.9 Errata 9 FDP_ACF.1.2/States

Number (1) contains errors in the list of commands permitted. TPM2_FieldUpgradeStart and TPM2_FieldUpgradeData are not permitted from the Init state and should not be included.

3.10 Errata 10 FDP_ETC.2.4/ExIm

Number (1) contains a typo: “IV” should be interpreted as symIV.

3.11 Errata 11 FDP_ACF.1.2/AC

Numbers (3) and (4) erroneously include a HMAC sequence. This is not a mandatory command and should not be included. The HMAC sequence should be considered removed.

3.12 Errata 12 FDP_ACF.1.4/NVM

This SFR erroneously contains a condition following the assignment: “none”. This condition should be removed.