TRUSTED® COMPUTING GROUP

ERRATA

Errata for TPM 2.0 Automotive-Thin Profile Version 1.01 Revision 15

Version 1.0
November 4, 2019

Contact: admin@trustedcomputinggroup.org

PUBLISHED

DISCLAIMERS, NOTICES, AND LICENSE TERMS

CHANGE HISTORY

REVISION	DATE		DESCRIPTION
Version 1.0	10/12/2018		• EK certificates/templates handles correction • Fix reserved handles for keys • Fix TPM2_Vendor_TCG_Test command • Change ECC curve definition

CONTENTS

1 Introduction

This document describes errata and clarifications for the TCG TPM 2.0 Automotive-Thin profile v1.1 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 EK templates

In section 5.10 NV Storage handles, Table 5 mentions lists EK templates for RSA and ECC that may be populated in the TPM nonvolatile memory. In fact, the vendor populates the EK template only if he is NOT using a default Template to generate the EK associated with the certificate. Tables 6 and 7 define two default Templates. If the vendor uses these default templates to generate the EKs, he does not need to populate the EK template (RSA) and EK template (ECC) NV Indices listed in Table 5.

3 Errata

3.1 EK certificates NV Index handles definition

In section 5.10 NV Storage handles, Table 5 defines incorrect NV index handles for EK templates which are defined in TCG EK Credential Profile for TPM Family 2.0; Level 0, version 2.1.

This table must be replaced by the table below:

Table 1 – NV Index handles example

Reserved Indices	Value
EK Certificate (RSA)	0x01C00022
EK template (RSA)	0x01C00023
EK Certificate (ECC)	0x01C0002A
EK template (ECC)	0x01C0002B

3.2 Mandatory Reserved Handles

In section 5.11 Mandatory Reserved Handles, the text specifies the TPM implementation SHALL reserve handles for keys and especially for an EK. This requirement is incorrect. TPM 2.0 Automotive-Thin profile uses the method described in TPM 2.0 library specification 1.38, part 1, section 14.2. So, section 5.11 must be removed.

3.3 TPM2_Vendor_TCG_Test

In section 5.6 Supported TPM 2.0 Commands, Table 3 contains a list of TPM commands that the profile requires.

TPM2_Vendor_TCG_Test command must be removed from this table, since the TPM 2.0 library specification 1.38, part 3, section 32.1 states:

“This section contains commands that are vendor specific but made public in order to prevent proliferation. This specification does define TPM2_Vendor_TCG_Test() in order to have at least one command that can be used to ensure the proper operation of the command dispatch code when processing a vendor-specific command.”

3.4 Mandatory Algorithms and Curves

In section 5.3, requirements for asymmetric algorithms, the specification enumerates two elliptic curve algorithm identifiers for ECC 256 bits: TPM_ECC_NIST_P256, TPM_ECC_BN_P256. However, mandating a BN_256 curve is incompatible with another statement from Table 3 in section 5.6 saying that Anonymous Attestation commands are optional.

The text:

“• At least one of RSA 2048 bits or ECC 256 bits (TPM_ECC_NIST_P256, TPM_ECC_BN_P256). Additional asymmetric algorithms and key sizes are allowed “

must be replaced by:

"• At least one of RSA 2048 bits or ECC 256 bits (TPM_ECC_NIST_P256, and if the Anonymous Attestation commands are implemented, TPM_ECC_BN_P256). Additional higher key sizes are allowed."

3.5 Conditionally Mandatory ECC Constants

In section 5.5, mandating a BN_256 curve is incompatible with another statement from Table 3 in section 5.6 saying that Anonymous Attestation commands are optional.

The text:

"If ECC is implemented, then a TPM 2.0 implementation compliant with this Automotive-Thin TPM SHALL support TPM_ECC_NIST_P256 and TPM_ECC_BN_P256 ECC curves and the ECC constants described in tables 7 and 10 of the TCG Algorithm Registry **Error! Reference source not found. Error! Reference source not found.**. Other curves may be implemented."

must be replaced by:

"If ECC is implemented, then a TPM 2.0 implementation compliant with this Automotive-Thin TPM SHALL support the ECC constants (for the ECC curves defined in section 5.3) described in the tables of section 5.2 Curves parameters of the TCG Algorithm Registry **Error! Reference source not found. Error! Reference source not found.**."

