TRUSTED® COMPUTING GROUP

SPECIFICATION

TCG TPM Vendor ID Registry Family 1.2 and 2.0

Version 1.07
Revision 0.02
June 20, 2024

Contact: admin@trustedcomputinggroup.org

Public Review

Work in Progress

This document is an intermediate draft for comment only and is subject to change without notice. Readers should not design products based on this document.

DISCLAIMERS, NOTICES, AND LICENSE TERMS

CHANGE HISTORY

REVISION	DATE	DESCRIPTION
1.01/1.00	October 18, 2017	• Initial Release of Version 1.01.
1.02/1.00	April 8,2020	• Migrate to new TCG format • Added Scope section • Moved and added explanatory text • Cleaned up tables and syntax, removed unused columns • Added Simulator and Testing TPM Capabilities Vendor ID section • Added Cisco and FlySlice
1.03/0.90	May 28, 2020	• Incremented Version number only. This is because the “legacy” formatted version 1.01 was updated to 1.02 prior to this version being approved. No changes from this document’s 1.02. Public revision comment should be as above for 1.02 as the legacy document has no change history so will not conflict.
1.04/0.90	June 10, 2020	• Minor wording fixes
1.04/0.91	June 17, 2020	• Minor editing
1.05/0.91	April 06, 2021	• Added Huawei
1.06/0.91	April 28, 2021	• Migrate to specification template
1.06/0.92	November 15, 2022	• Added vendor Ant Group
1.06/0.93	December 2, 2022	• Added vendor HP Inc.
1.06/0.94	April 25, 2022	• Added vendor Solidigm
1.06/0.95	January 10, 2024	• Added Vendor NSING, SecEdge
1.07/0.1	May 7, 2024	• Added Wisekey
1.07/0.2	June 20, 2024	• Added section “TPM Settable Capabilities Vendor ID”

CONTENTS

1 SCOPE

This document defines the values returned by a TPM implementation. This allows entries (such as OS drivers, software stack, applications) to know the identity of the TPM implementer.

Additional values may be requested by contacting: vendor-id-request@trustedcomputinggroup.org.

1.1 Key Words

The key words “MUST,” “MUST NOT,” “REQUIRED,” “SHALL,” “SHALL NOT,” “SHOULD,” “SHOULD NOT,” “RECOMMENDED,” “MAY,” and “OPTIONAL” in this document normative statements are to be interpreted as described in RFC-2119, Key words for use in RFCs to Indicate Requirement Levels.

1.2 Statement Type

Please note a very important distinction between different sections of text throughout this document. There are two distinctive kinds of text: informative comment and normative statements. Because most of the text in this specification will be of the kind normative statements, the authors have informally defined it as the default and, as such, have specifically called out text of the kind informative comment. They have done this by flagging the beginning and end of each informative comment and highlighting its text in gray. This means that unless text is specifically marked as of the kind informative comment, it can be considered a kind of normative statements.

EXAMPLE: Start of informative comment

This is the first paragraph of 1–n paragraphs containing text of the kind *informative comment* ...

This is the second paragraph of text of the kind *informative comment* ...

This is the nth paragraph of text of the kind *informative comment* ...

To understand the TCG specification the user must read the specification. (This use of MUST does not require any action).

End of informative comment

2 FORMAT

The values in this document have no implied format or endianness. How these values are presented is defined by the specification using them such as the TPM Library and Platform Specific Specifications.

3 TPM Hardware Interface Vendor ID

These values are the TPM manufacturer-specific 16-bit VenID fields returned by the TPM interface defined in a Platform TPM Profile.

These values are chosen by the requestor. They are often PCI-SIG ID values assigned to them by the PCI Sig Standard Organization, however, there is no attempt by TCG to validate or coordinate these values with PCI-Sig Standards Organization. Therefore, no attempt should be made to associate the values returned by a TPM from this section with a particular vendor PCI-SIG value.

All values are 16-bit integers.

Table 1 TPM Hardware Interface Vendor ID

Assigned To	Value
AMD	0x1022
Ant Group	0x6688
Atmel	0x1114
Broadcom	0x14E4
Cisco	0xC5C0
FlySlice Technologies	0x232B
Fuzhou Rockchip	0x232A
Google	0x6666
HPI	0x103C
HPE	0x1590
Huawei	0x8888
IBM	0x1014
Infineon	0x15D1
Intel	0x8086
Lenovo	0x17AA
Microsoft	0x1414
National Semi	0x100B
Nationz	0x1B4E
NSING	0x9999
Nuvoton Technology[1]	0x1050
Qualcomm	0x1011
Samsung	0x144D
SecEdge	0x5ECE
Sinosun	0x19FA
SMSC	0x1055

[1] This value was formerly assigned to Winbond

Assigned To	Value
Solidigm	0x025E
STMicroelectronics	0x104A
Texas Instruments	0x104C
Wisekey	0x2406

4 TPM Capabilities Vendor ID

This is the value that is returned by the following commands:

For TPM Family 1.2:

TPM_GetCapability with the capability TPM_CAP_PROP_MANUFACTURER

For TPM Family 2.0:

TPM2_GetCapability with the capability TPM_CAP_TPM_PROPERTIES with the Property Tag TPM_PT_MANUFACTURER

These values are chosen by the requestor. They have been typically a Stock Market symbol but that is not a requirement.

In the tables in this section the column labeled “Hex” is the machine-readable definitive value. The column labeled ASCII is a visual representation of the hexadecimal value. The bracket quote characters are added as a visual delimiter only, they are not included in the value. A space in this column represents either 0x00 or 0x20 which is the choice of the requestor. All values are a 32-bit array of octets.

4.1 Product Implementations

These are TPM implementations intended for use in products in end-user applications with appropriate protections for Protected Capabilities and Shielded Locations as defined by a TCG Platform TPM Profile.

Table 2 - TPM Capabilities Vendor ID

Assigned to	Value (ASCII)	Hex
AMD	<AMD >	0x41 0x4D 0x44 0x00
Ant Group	<ANT >	0x41 0x4E 0x54 0x00
Atmel	<ATML>	0x41 0x54 0x4D 0x4C
Broadcom	<BRCM>	0x42 0x52 0x43 0x4D
Cisco	<CSCO>	0x43 0x53 0x43 0x4F
Flyslice Technologies	<FLYS>	0x46 0x4C 0x59 0x53
Fuzhou Rockchip	<ROCC>	0x52 0x4F 0x43 0x43
Google	<GOOG>	0x47 0x4F 0x4F 0x47
HPI	<HPI >	0x48 0x50 0x49 0x00
HPE	<HPE >	0x48 0x50 0x45 0x00
Huawei	<HISI>	0x48 0x49 0x53 0x49
IBM	<IBM >	0x49 0x42 0x4d 0x00
Infineon	<IFX >	0x49 0x46 0x58 0x00
Intel	<INTC>	0x49 0x4E 0x54 0x43
Lenovo	<LEN >	0x4C 0x45 0x4E 0x00
Microsoft	<MSFT>	0x4D 0x53 0x46 0x54

Assigned to	Value (ASCII)	Hex
National Semiconductor	<NSM >	0x4E 0x53 0x4D 0x20
Nationz	<NTZ >	0x4E 0x54 0x5A 0x00
NSING	<NSG >	0x4E 0x53 0x47 0x00
Nuvoton Technology	<NTC >	0x4E 0x54 0x43 0x00
Qualcomm	<QCOM>	0x51 0x43 0x4F 0x4D
Samsung	<SMSN>	0x53 0x4D 0x53 0x4E
SecEdge	<SECE>	0x53 0x45 0x43 0x45
Sinosun	<SNS >	0x53 0x4E 0x53 0x00
SMSC	<SMSC>	0x53 0x4D 0x53 0x43
STMicroelectronics	<STM >	0x53 0x54 0x4D 0x20
Texas Instruments	<TXN >	0x54 0x58 0x4E 0x00
Winbond	<WEC >	0x57 0x45 0x43 0x00
Wisekey	<SEAL>	0x53 0x45 0x41 0x4C

4.2 Simulator and Testing Implementations

These are TPM implementations intended for use in simulators and testing. There are no implied protections for Protected Capabilities and Shielded Locations for TPM's providing these identifiers. These values are used to indicate to software the nature of the TPM's implementation.

These values are not intended for use in production Virtual or Software-based TPMs. While perhaps similar in nature, Production Virtual or Software-based TPMs which are based on TCG defined specifications should use TCG assigned values in section 4.1 Product Implementations and if applicable section 3 TPM Hardware Interface Vendor ID.

Use of these values is by convention only and not enforced by TCG. The values below are not assigned to any particular vendor, however, TCG reserves the right to assign values to suppliers at a later time.

Table 3 - Vendor ID for Simulators and Testing

Assigned to	ASCII	Hex
Simulator 0	<SIM0>	0x53 0x49 0x4d 0x30
Simulator 1	<SIM1>	0x53 0x49 0x4d 0x31
Simulator 2	<SIM2>	0x53 0x49 0x4d 0x32
Simulator 3	<SIM3>	0x53 0x49 0x4d 0x33
Simulator 4	<SIM4>	0x53 0x49 0x4d 0x34
Simulator 5	<SIM5>	0x53 0x49 0x4d 0x35
Simulator 6	<SIM6>	0x53 0x49 0x4d 0x36
Simulator 7	<SIM7>	0x53 0x49 0x4d 0x37
Test 0	<TST0>	0x54 0x53 0x54 0x30
Test 1	<TST1>	0x54 0x53 0x54 0x31
Test 2	<TST2>	0x54 0x53 0x54 0x32
Test 3	<TST3>	0x54 0x53 0x54 0x33
Test 4	<TST4>	0x54 0x53 0x54 0x34
Test 5	<TST5>	0x54 0x53 0x54 0x35
Test 6	<TST6>	0x54 0x53 0x54 0x36
Test 7	<TST7>	0x54 0x53 0x54 0x37
Note to Editor: Before assigning new values, verify they do not conflict with Assigned values in Table 2 - TPM Capabilities Vendor ID above.		

5 TPM Settable Capabilities Vendor ID

The TPM Library specification defines settable capabilities, which can be set with TPM2_SetCapability and read with TPM2_GetCapability.

The TPM Library specification allows vendor-specific settable capabilities, which are identified via the two fields (“W” and “V”) in the capability value (TPM_CAP) shown in Table 4 (copied as reference from Part 2).

Start of informative comment

Table 4 - TPM Capability Fields Description

Bit	Name	Definition
22:16 (7)	W	Vendor Shall be zero if the capability is non-settable or if the capability is settable but non-vendor-specific. For settable, vendor-specific capabilities, identifies the vendor NOTE The vendor identification values may be defined by a TCG Registry.
23 (1)	V	TCG/Vendor indicator Shall be zero if the capability is non-settable. For settable capabilities, identifies whether the capability is vendor-specific **SET (1):** The capability is vendor-specific **CLEAR (0):** The capability is defined by TCG

End of informative comment

Table 5 defines the TPM settable capabilities vendor ID used in the “Vendor” field of TPM_CAP.

Table 5 - TPM Settable Capabilities Vendor ID

Assigned to	ASCII	Value (Hex)
AMD	<A>	0x41
Analogix	<X>	0x58
Ant Group	<T>	0x54
Google	<g>	0x67
Huawei	<H>	0x48
Infineon	<I>	0x49
Intel	<i>	0x69
Microsoft	<M>	0x4D
Nationz	<S>	0x53
NSING	<G>	0x47
Nuvoton Technology	<N>	0x4E
STMicroelectronics	<s>	0x73

Assigned to	ASCII	Value (Hex)
Wisekey	<W>	0x57

Note: The maximum value is 0x7F.

