TCG TPM Vendor ID Registry

Version 1.02

Revision 1.00

28 May 2020

When a TCG Platform TPM Profile uses a value from one of these tables, the endianness of the value is specified by that specification, and may vary between specifications.

1. TPM Hardware Interface Vendor ID

Begin Informative Comment:

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

End Informative Comment

	Value	Other Identifiers (e.g., String)	Others …
Size	*16 bits*	*TBD*	*TBD*
Format	*Integer*	*TBD*	*TBD*
Assigned By:	*TCG*	*TBD*	*TBD*
Assigned To:			
AMD	0x1022		
Atmel	0x1114		
Broadcom	0x14E4		
Cisco	0xC5C0		
FlySlice Technologies	0x232B		
HPE	0x1590		
IBM	0x1014		
Infineon	0x15D1		
Intel	0x8086		
Lenovo	0x17AA		
Microsoft	0x1414		
National Semi	0x100B		
Nationz	0x1B4E		
Qualcomm	0x1011		
SMSC	0x1055		
STMicroelectronics	0x104A		
Samsung	0x144D		
Sinosun	0x19FA		
Texas Instruments	0x104C		
Nuvoton Technology[1]	0x1050		
Fuzhou Rockchip	0x232A		
Google	0x6666		

Table 1 TPM Hardware Interface Vendor ID

[1] Formerly Winbond

Copyright © Trusted Computing Group 2020

2. TPM Capabilities Vendor ID (CAP_VID)

Begin Informative Comment:

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

End Informative Comment

In the table below the column labeled “Hex” is the normative value. The column labeled ASCII is an informative representation of the normative hexadecimal value.

	Value	
Size	*32 bits*	
Format	*Byte Array*	
Assigned By:	*TCG*	
Assigned to:	ASCII	Hex
AMD	‘AMD’	0x41 0x4D 0x44 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
HPE	‘HPE’	0x48 0x50 0x45 0x00
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
National Semiconductor	‘NSM ‘	0x4E 0x53 0x4D 0x20
Nationz	‘NTZ’	0x4E 0x54 0x5A 0x00
Nuvoton Technology	‘NTC’	0x4E 0x54 0x43 0x00
Qualcomm	‘QCOM’	0x51 0x43 0x4F 0x4D
SMSC	‘SMSC’	0x53 0x4D 0x53 0x43
ST Microelectronics	‘STM ‘	0x53 0x54 0x4D 0x20
Samsung	‘SMSN’	0x53 0x4D 0x53 0x4E
Sinosun	‘SNS’	0x53 0x4E 0x53 0x00
Texas Instruments	‘TXN’	0x54 0x58 0x4E 0x00
Winbond	‘WEC’	0x57 0x45 0x43 0x00
Fuzhou Rockchip	‘ROCC’	0x52 0x4F 0x43 0x43

Copyright © Trusted Computing Group 2020

Google	'GOOG'	0x47 0x4F 0x4F 0x47

Table 2 TPM Capabilities Vendor ID

Copyright © Trusted Computing Group 2020