Содержание

Security

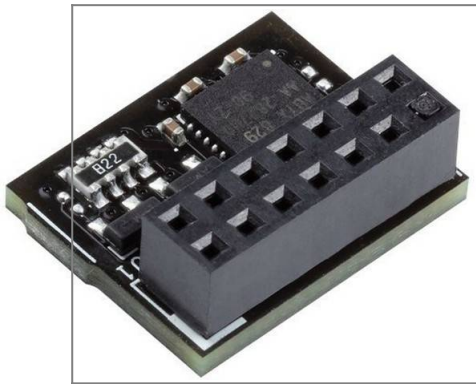
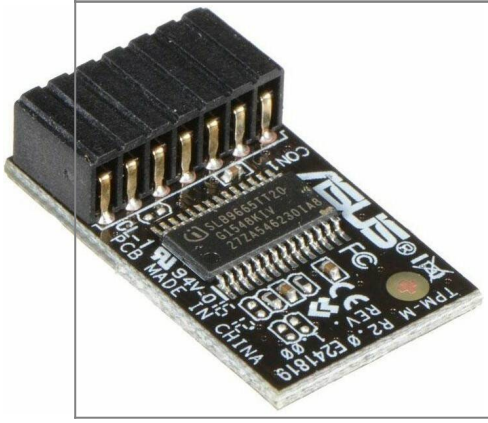
Manufacturers

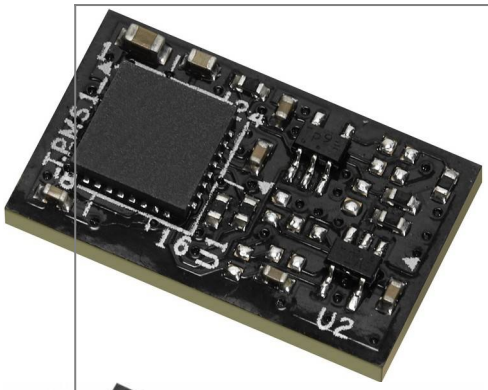
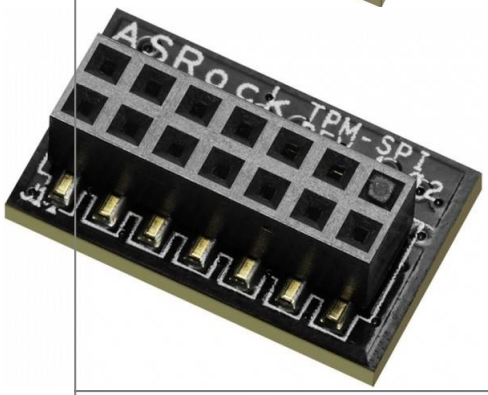
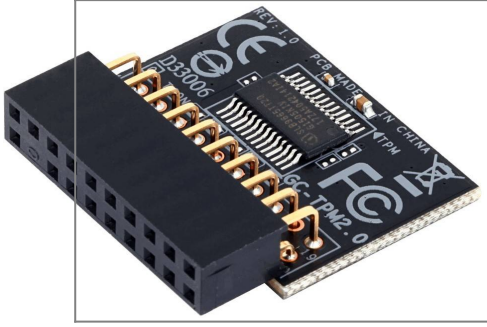
Nuvoton
Infineon

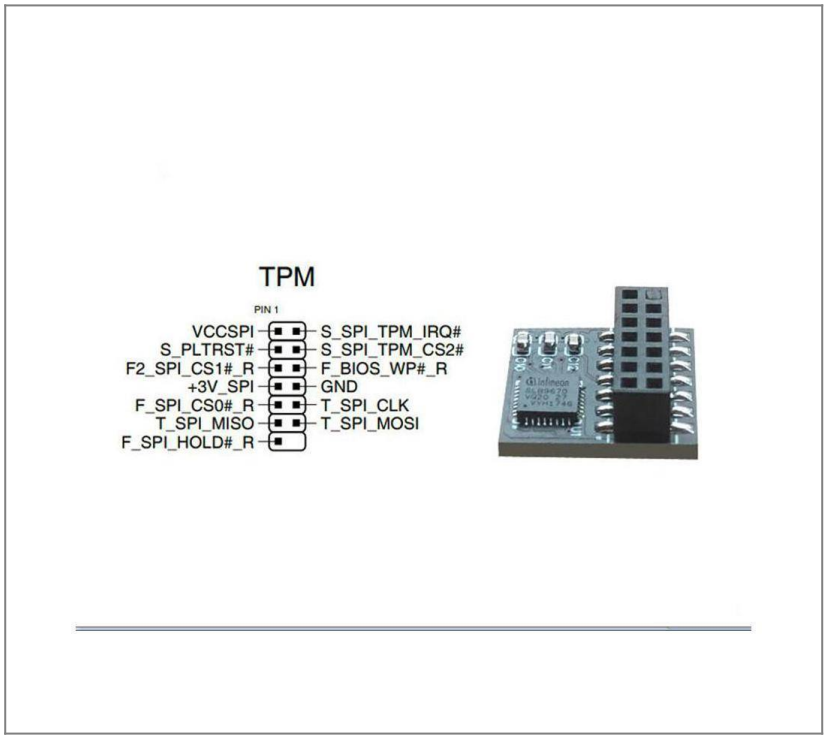
TMP Chip

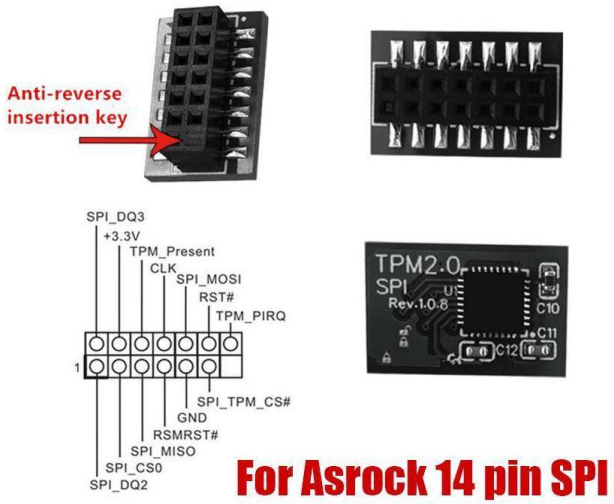
Part name	Interface	TPM ver	Manufacturer	Datasheet	IT link
NPCT650ABAYX	LPC\I2C\SPI	TPM1.2	Nuvoton	NPCT650ABAYX	IT
NPCT750AADYX	SPI	TPM2.0	Nuvoton	NPCT750AADYX	IT
SLB9665 (NFND)	LPC	TPM2.0	Infineon	SLB9665	
OPTIGA TPM SLB 9672 FW15	SPI	TMP2.0	Infineon	OPTIGA TPM SLB 9672 FW15	
OPTIGA TPM SLB 9672 FW16	SPI	TMP2.0	Infineon	OPTIGA TPM SLB 9673 FW26	
OPTIGA TPM SLB 9673 FW26	I2C	TMP2.0	Infineon	OPTIGA TPM SLB 9673 FW26	
SLB 9670VQ2.0	SPI	TMP2.0	Infineon	SLB 9670VQ2.0	
SLI 9670	SPI	TMP2.0	Infineon	SLI 9670	
SLM 9670	SPI	TMP2.0	Infineon	SLM 9670	

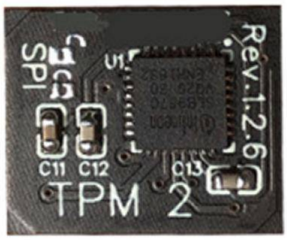
TMP Module

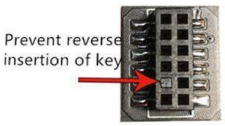
	ASUS	TPM-SPI OEM {20} (210287) / Pin Dimension: 14-1pin	Nuvoton NPCT750
	ASUS	TPM-M R2.0 , OEM {20} (230406)	Infineon SLB9665

 	Asrock	TPM-SPI, SPI interface, TPM 2.0	Infineon OPTIGA TPM SLB 9670?
	Gigabyte	GC-TPM2.0, TPM header key, LPC bus, (for Intel 200/100/8/9/99 series, AMD AM4, FM2 series) OEM	Infineon SLB9665

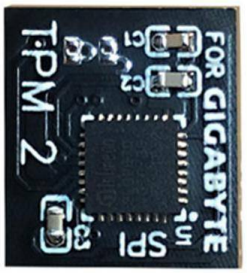








1	SPI Power	2	SPI Chip Select
3	Master In Slave Out (SPI Data)	4	Master Out Slave In (SPI Data)
5	Reserved	6	SPI Clock
7	Ground	8	SPI Reset
9	Reserved	10	No Pin
11	Reserved	12	Interrupt Request



Prevent reverse insertion of key

	Definition		Definition
1	Data Output	7	Chip Select
2	Power Supply(3.3V)	8	Ground Pin
3	No Pin	9	IRQ
4	No Effect	10	No Effect
5	Data Input	11	No Effect
6	CLK	12	RST