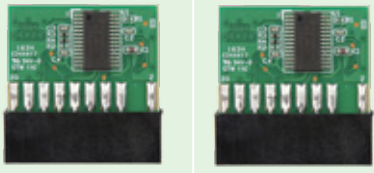


IEI Trusted Platform Module (TPM)

Hardware-based security solution for data protection and reliable authentication via TPM that stores key, passwords and digital certificates.

H/W Features

Solution	Infineon	
	SLB9660 TT1.2	SLB9665TT2.0
Features		
Secure Startup	Root of Trust Measurement of early boot devices	
Anti H/W Attack	Sensors and active shield	
TSS API Support	MS-CAP/ PKCS#11, #12	
H/W Certification		
Management Tool Function	1. TPM management 2. File & Folder En/De-cryption 3. Personal secure drive 4. Secure Email 5. Key transferring 6. Security policy configuration	
Market Segment	Complete TPM1.2/2.0 function	
TCG Specification	TCG 1.2/2.0 compliant trusted platform module	
Interface	Low pin count	
Software Structure	TCG software stack 1.2 complaint	
Cryptographic Accelerator	HAS-1/RSA algorithm	

IEI SBC with TPM support

Form factor	Model name	Form factor	Model name
PICMG1.3	PCIE-Q170-i2*	Micro-ATX	IMB-H110*
	PCIE-H810		IMB-Q870-i2
	PCIE-Q670		IMB-H810-i2
PICMG1.0	WSB-H810		IMB-Q770
Half-size PCIe	PICOe-HM650		IMB-Q670
Half-size PCISA	PCISA-BT		IMB-H610A/H610B
ATX	IMBA-C2360-i2*	Mini-ITX	KINO-DH310
	IMBA-Q170-i2*		tKINO-BW
	IMBA-H110*		KINO-DBT
	IMBA-BDE		KINO-SE/KBN-i2
	IMBA-H810		KINO-DH810
	IMBA-C2260-i2		eKINO-BT
	IMBA-Q870-i2		KINO-ABT-i2
	IMBA-H610		KINO-AQ870
	IMBA-Q670		KINO-QDM871-i1
EPIC SBC	NANO-QM871		KINO-QM770
	NANO-QM770		KINO-DH610
	NANO-HM650		KINO-AH612

* TPM 2.0 is supported by these models.

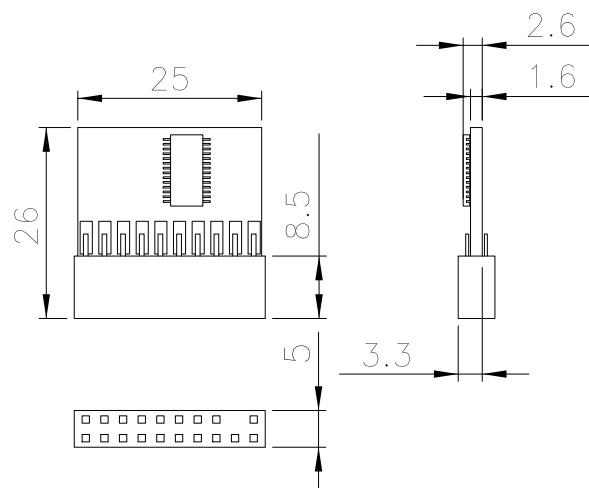
Pin Assignment

Pin	Singnal	Pin	Singnal	Pin	Singnal	Pin	Singnal
1	LCLK	6	VCC5	11	LAD0#	16	SERIRQ
2	GND	7	LAD3#	12	GND	17	GND
3	LFRAME#	8	LAD2#	13	SCL	18	CLKRUN#
4	KEYWAY	9	VCC3	14	SDA	19	LPCPD#
5	LRST#	10	LAD1#	15	SB3V	20	LDRQ#

Ordering Information

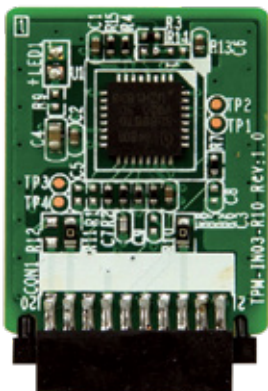
Model Name	Description
TPM-IN01-R20	20-pin Infineon TPM1.2 module, software management tool, firmware v4.4
TPM-IN02-R20	20-pin Infineon TPM2.0 module, software management tool, firmware v5.5

Dimensions (mm)

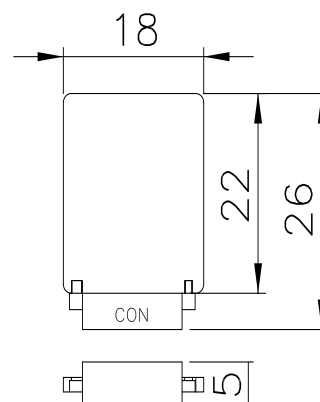


TPM-IN03

SPI TPM 2.0 module, software management tool, FW15.23



Dimensions (Unit: mm)



Specifications

Model	TPM-IN03
Interface	SPI interface
Solution	Infineon SPI TPM 2.0 with SLB9670VQ2.0 FW15.23
Management Tool Function	1. TPM management 2. File & Folder En/De-cryption 3. Personal secure drive 4. Secure email 5. Key transferring 6. Security policy configuration 7. SPI interface
Market Segment	Complete TPM 2.0 function
OS Support	Windows® & Linux
Operating Temperature	0°C ~ 60°C
Storage Temperature	-20°C ~ 70°C
Operating Humidity	5% ~ 95%, non-condensing
Dimensions (LxW):	26mm x 18mm

Packing List

1 x 20-pin TPM module

Ordering Information

Part No.	Description
TPM-IN03-R10	20-Pin Infineon SPI TPM 2.0 module with SLB9670VQ2.0, software management tool, FW15.23

SPI TPM Support List

Form factor	Model name	
Medical Panel PC	POCi-W22C-ULT5	
EPIC SBC	NANO-ULT5	KINO-ADL-N
	IMBAX-SP6	KINO-EHL2
	HPCIE-RPL-Q670	KINO-ADLPS
	PCIE-RPL-Q670	IMB-H420
	KINO-AM5	IMB-Q470
	IMBA-AM5	KINO-DH310
	IMB-AM5	IMBA-Q370
	IMB-MTL	PCIE-Q370
	IMB-V3000	SPCIE-C246
	KINO-MPHX	
DIN-Rail Embedded System	DRPC-230-ULT5	
	DRPC-330-A7K	