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 / Features	Infineon SLB9660 TT1.2	SLB9665TT2.0
		
Secure Startup	Root of Trust Measurement of early boot devices	
Anti H/W Attack	Sensors and active shield	
TSS API Support	MS-CAPI/PKCS#11, #12	
H/W Certification	EAL 4	
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*
	SPCIE-C236-i2*		IMB-Q870-i2
	SPCIE-C2260-i2		IMB-H810-i2
	PCIE-H810		IMB-Q770
	PCIE-Q670		IMB-Q670
PICMG1.0	WSB-H810		IMB-H610A/H610B
	WSB-H610	Mini-ITX	KINO-DH310
Half-size PCIe	PICOe-B650		tKINO-BW
	PICOe-HM650		KINO-DBT
Half-size PCISA	PCISA-BT		KINO-SE/KBN-i2
ATX	IMBA-C2360-i2*		KINO-DH810
	IMBA-Q170-i2*		eKINO-BT
	IMBA-H110*		KINO-ABT-i2
	IMBA-BDE		KINO-AQ870
	IMBA-H810		KINO-DQM871-i1
	IMBA-C2260-i2		KINO-QM770
	IMBA-Q870-i2		KINO-DH610
	IMBA-H610		KINO-AH612
	IMBA-Q670		
EPIC SBC	NANO-QM871		
	NANO-QM770		
	NANO-HM650		

* TPM 2.0 is supported by these models.

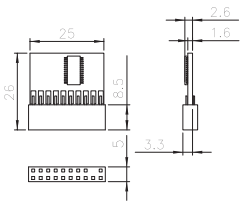
Pin Assignment

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

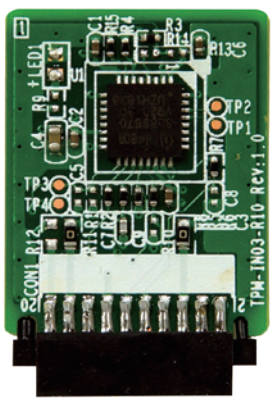
Dimensions (mm)



TPM-IN03

SPI TPM 2.0 module, software management tool, firmware v7.85

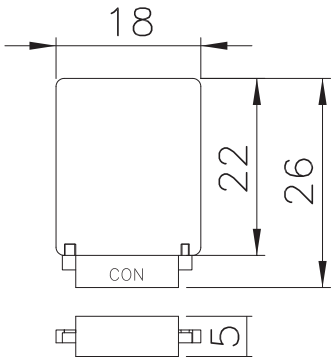
New



Specifications

- Interface
  SPI interface
- Solution
  Infineon SPI TPM 2.0 with SLB9670VQ2.0 FW7.85
- 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: TBD

Dimensions (Unit: mm)



SPI TPM Support List

Form factor	Model name
Medical Panel PC	POCi-W22C-ULT5
EPIC SBC	NANO-ULT5
DIN-Rail Embedded System	DRPC-230-ULT5
	DRPC-330-A7K

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, firmware v7.85.