



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 Comparison

Solution	Infineon SLB9635 TT1.2
Features	
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	
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 function
TCG Specification	TCG 1.2 compliance trusted platform module
Interface	Low pin count
Software Structure	TCG software stack 1.2 complaint
Cryptographic Accelerator	HAS-1/RSA algorithm

Ordering Information

Model Name	Description
TPM-IN01-R11	20-pin Infineon TPM module, software management tool, firmware V3.17

IEI SBC with TPM support

Form factor	Model name	Form factor	Model name
ATX	IMBA-H610	Mimi-ITX	KINO-AQ870
	IMBA-C2060		KINO-DQM810
	IMBA-Q670		KINO-QM770
	IMBA-G410		KINO-AQ670
	IMBA-G412ISA		KINO-DH610
	IMBA-XQ354		KINO-AH611
IMBA-9454G	KINO-AH612		
microATX	IMB-Q770		KINO-PV-D5253
	IMB-C2016		KINO-QM670
	IMB-H610		KINO-HM551
	IMB-H612	SPCIE-C2160	
	IMB-C2060	SPCIE-C2060	
	IMB-Q670	PCIE-H610	
5.25" SBC	IMB-Q354	PCIE-Q670	
	IMB-9454	PCIE-Q350	
	NOVA-PV	PCIE-9652	
EPIC	NOVA945GSE	WSB-H610	
	NANO-QM871	WSB-PV	
	NANO-QM770	WSB-Q354	
5.25" SBC	NANO-HM650	WSB-9452	
	NANO-HM551	PIC0e-B650	
		PIC0e-HM650	

Pin Assignment

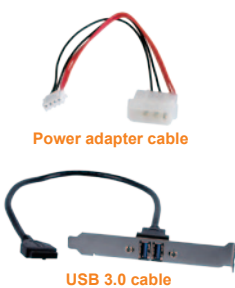
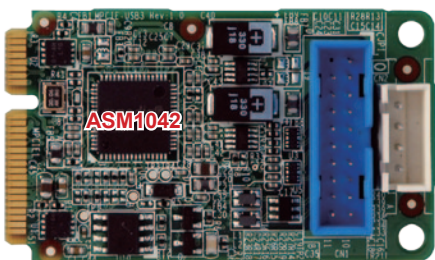


Pin	Signal	Pin	Signal
1	LCLK	11	LAD0#
2	GND	12	GND
3	LFRAME#	13	SCL
4	KEYWAY	14	SDA
5	LRST#	15	SB3V
6	VCC5	16	SERIRQ
7	LAD3#	17	GND
8	LAD2#	18	CLKRUN#
9	VCC3	19	LPD#
10	LAD1#	20	LDRQ#

TPM OS Supported List

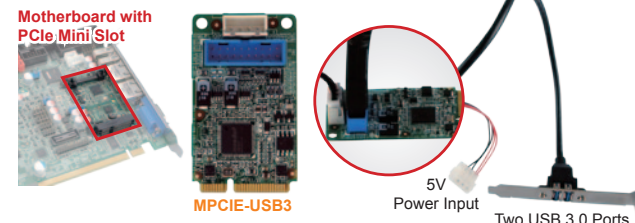
OS Supported	Infineon
Windows®	Windows® XP SP2, Windows® 7, Vista
Linux	Fedora 6 (Kernel 2.6.8 or above)

MPCIE-USB3 PCIe Mini USB 3.0 adapter card, RoHs



IEI USB 3.0 Expanded Solution

The MPCIE is applied to add additional super speed USB 3.0 ports for the motherboard with a PCIe Mini slot.



Specifications

- ◆ Form Factor: PCI Express Mini card
- ◆ USB 3.0 Controller: Asmedia ASM1042
- ◆ Internal Connector: 1 x 20-pin (2x10) box header
- ◆ Power Jack: 1 x 4-pin box header
- ◆ Compatible OS: Windows® 2000/XP/Server 2003/Server 2008/Vista/7, Linux kernel version 2.6.32 above
- ◆ Operating Temperature: -10°C ~ 60°C
- ◆ Operating Humidity: 5% ~ 95%, non-condensing
- ◆ Dimensions (LxW): 50 mm x 30 mm
- ◆ Weight: 70g

Packing List

1 x MPCIE-USB3 PCIe Mini USB 3.0 adapter card	
1 x Dual USB 3.0 type A port cable with bracket (P/N: 19800-010500-200-RS)	
1 x Power cable (P/N: 32102-020900-100-RS)	1 x QIG

Ordering Information

Part No.	Description
MPCIE-USB3-R10	PCIe Mini USB 3.0 adapter card, RoHs
19800-010500-200-RS	Dual USB 3.0 type A port cable with bracket

Features

1. Supports two external USB 3.0 type A ports
2. USB 3.0 provides up to 5Gbps of transferring rate
3. Backward compatible with USB 2.0 and USB 1.0/1.1 devices
4. Fully compliant with USB 3.0 rev 1.0 specifications and Intel® xHCI rev 0.96 specifications, with transfer rates up to 5Gbps
5. Compliant with PCI Express Mini specification 1.2

Dimensions (mm)

