

Packing List

Before you begin installing your card, please make sure that the following items have been shipped:

1. PCA-TPM 2.0 trusted platform module x1
2. 2-year quality warranty card x 1 P/N: 2190000902
3. Startup manual x 1 P/N: 20010TPM00
4. Screw x 1 P/N: 1930005258

If any of these items are missing or damaged, please contact your distributor or sales representative immediately.

Specifications

Standard Functions

- Trusted platform module compliant with TCG 2.0 specification and TSS 2.0 via LPC connector on CPU card.
- Adopting Infineon SLB9665TT2.0FW5.51 solution with common criteria security certification EAL level 4+.
- Hardware-based data protection solution for high security businesses such as banks, governments, insurance and confidential facilities in factories or power plants. Once the module disconnects with the SBC, the encrypted data can not be decrypted, even when password is provided.
- System support list

SBC
PCE-5129 (BIOS V2.0 or later)
PCE-5029 (BIOS V2.0 or later)
PCE-7129 (BIOS V2.0 or later)
PCE-4129 (BIOS V2.0 or later)
PCE-3029 (BIOS V2.0 or later)

For more information on this and other Advantech products, please visit our website at:

<http://www.advantech.com>

For technical support and service, please visit our support website at:

<http://support.advantech.com>

This manual is for the PCA-TPM Series.

Part No. 20010TPM00
 Print in China

1st Edition
 February 2017

Specifications(Cont.)

AIMB

AIMB-785 (BIOS V2.0 or later)

AIMB-705 (BIOS V2.0 or later)

Module IPC

MIC-7700 (BIOS V1.0 or later)

MIC-7500 (BIOS V1.13 or later)

AIMC-3202 (BIOS V2.0 or later)

AIMC-3422 (BIOS V2.0 or later)

AIIS-3400 (BIOS V2.0 or later)

AIIS-3410 (BIOS V2.0 or later)

ASMB

ASMB-585 (BIOS V1.13 or later)

ASMB-785 (BIOS V1.14 or later)

ASMB-813 (BIOS V2.01 or later)

ASMB-823 (BIOS V3.02 or later)

ASMB-913 (BIOS V2.01 or later)

ASMB-923 (BIOS V3.01 or later)

Build-in AP support OS List (TPM.msc)

Windows 7 SP1 x64 (Need to update hotfix – Fix459309)

Windows Server 2008 R2 SP1 x64 (Need to update hotfix – Fix459309)

Windows 8 x86 and x64

Windows 8.1 x86 and x64

Windows Server 2012 x64

Windows Server 2012 R2

Mechanical

- **Dimensions:** 31.5 mm x 30.5 mm
- **Power supply type:** 3.3 V, 5 V, 5 VSB
- **Power requirements:** 3.3 V @ 5 mA, 3.3 VSB @ 25 mA (Operation time)
- **Operating temperature:** 0 ~ 60° C
- **Operating humidity:** 40° C @ 85% RH, Non-Condensing
- **Storage temperature:** -40 ~ 85° C
- **Storage humidity:** 60° C @ 95% RH, Non-Condensing
- **Weight:** 0.12 kg

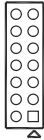
Jumpers and Connectors

There is one connector on the module to connect with SBC. The below table lists the functions of this connector.

Jumpers and connectors

Connectors

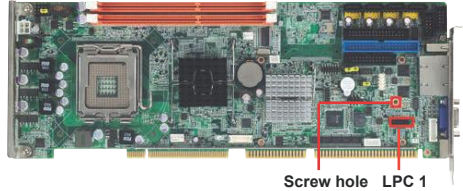
Label	Function
LPC1	Low pin count connector



Pin	Signal	Pin	Signal
1	LPC_AD1	2	CLK_TPM
3	LPC_AD0	4	#PLTRST
5	VCC3	6	#LFRAME
7	GND	8	LPC_AD3
9	N/A	10	LPC_AD2
11	N/A	12	LPC_SERIRQ
13	VCC	14	VCC5SB

Installation Guide

1. Please connect TPM module to the SBC LPC1 connector using the following steps.
 - 1). Locate LPC1 and the screw hole on your SBC. If your SBC is either PCA-6010/6011, PCE-5125, or PCA-6782, you will find two screw holes around LPC1. Please choose the screw on the inside of the SBC for those full-size products (please refer to picture 1), and the screw further from LPC1 for PCA-6782 (please refer to picture 2).

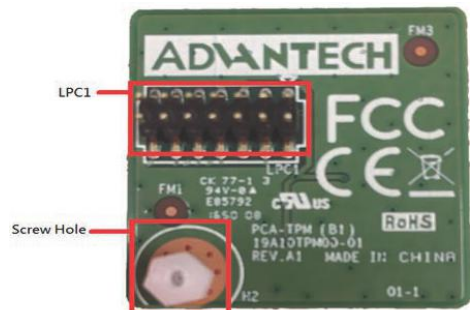


Picture 1



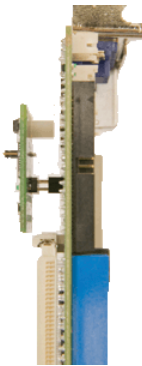
Picture 2

- 2). Locate LPC1 and the screw hole on PCA-TPM.

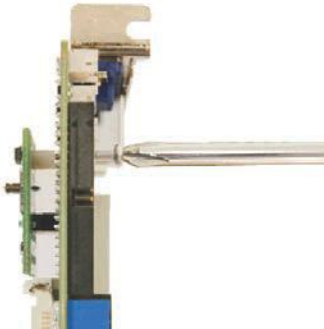


Installation Guide(Cont.)

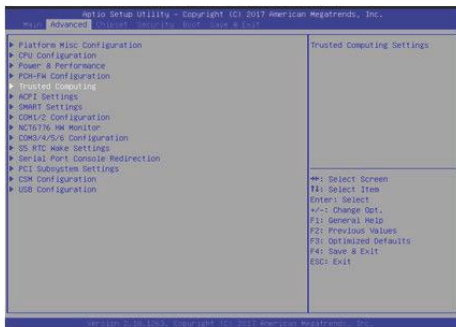
- 3). Connect PCA-TPM and SBC with LPC1 connector.



- 4). Align the screw holes, and fix securely with the screw.

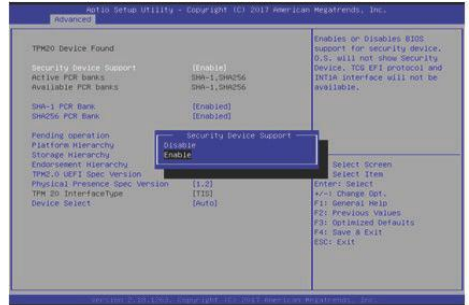


Enter the BIOS setup manual and select "Advanced" label.

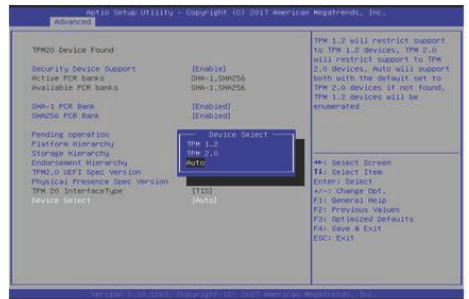


Installation Guide(Cont.)

Enable the "Security Device Support".



Select TPM 2.0 in Device Select.



2. For software installation, please refer to the appendix.

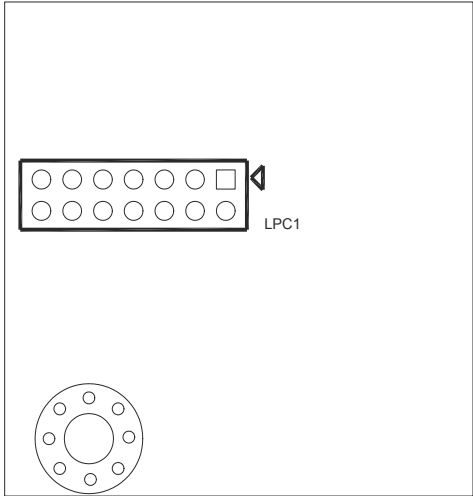


Figure 1: PCA-TPM Board Layout

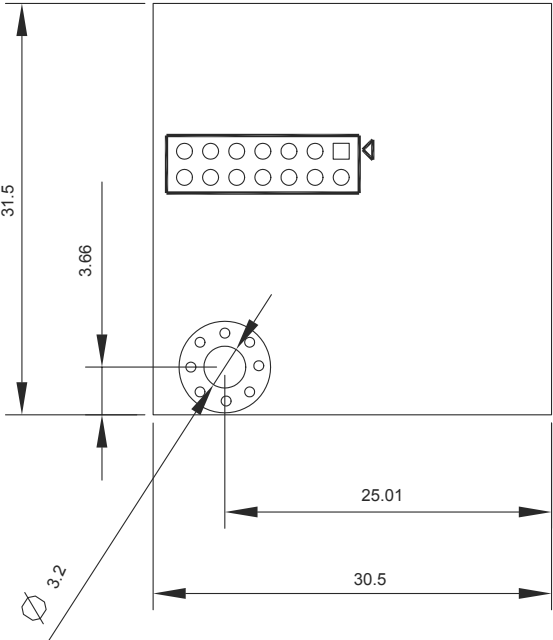
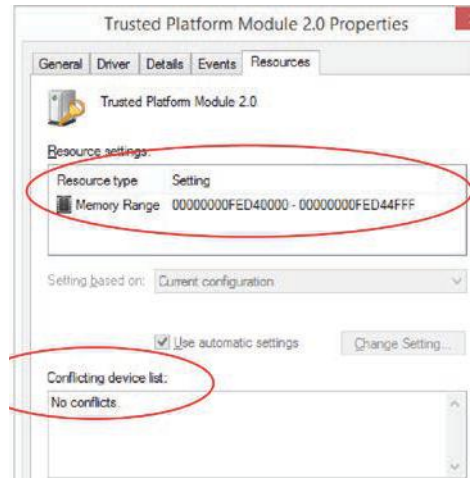
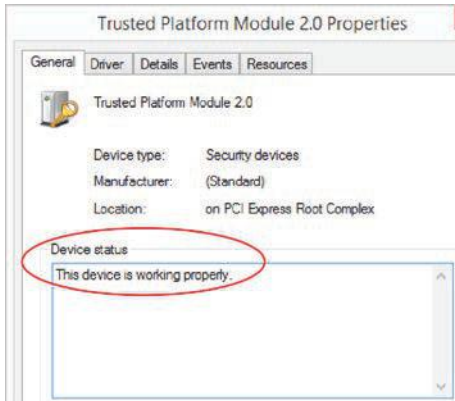
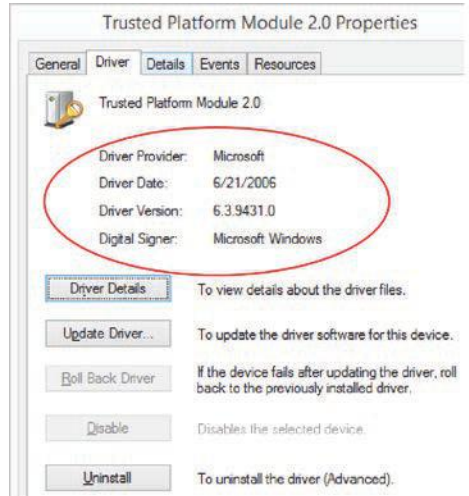
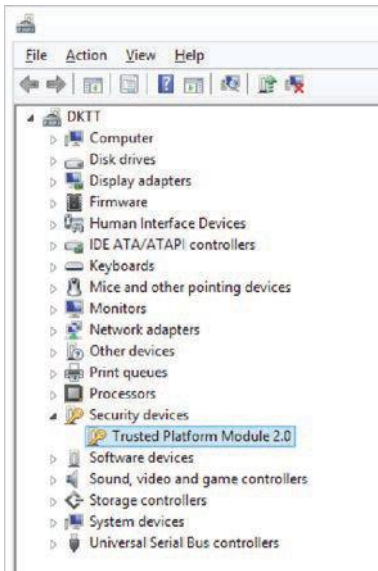


Figure 3: PCA-TPM Board Dimensions

Appendix

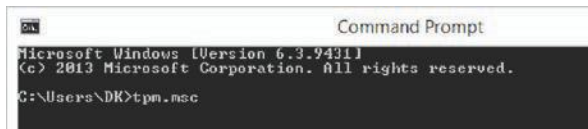
TPM setup under Windows OS

Enter the Device manager to check the TPM is work or not.

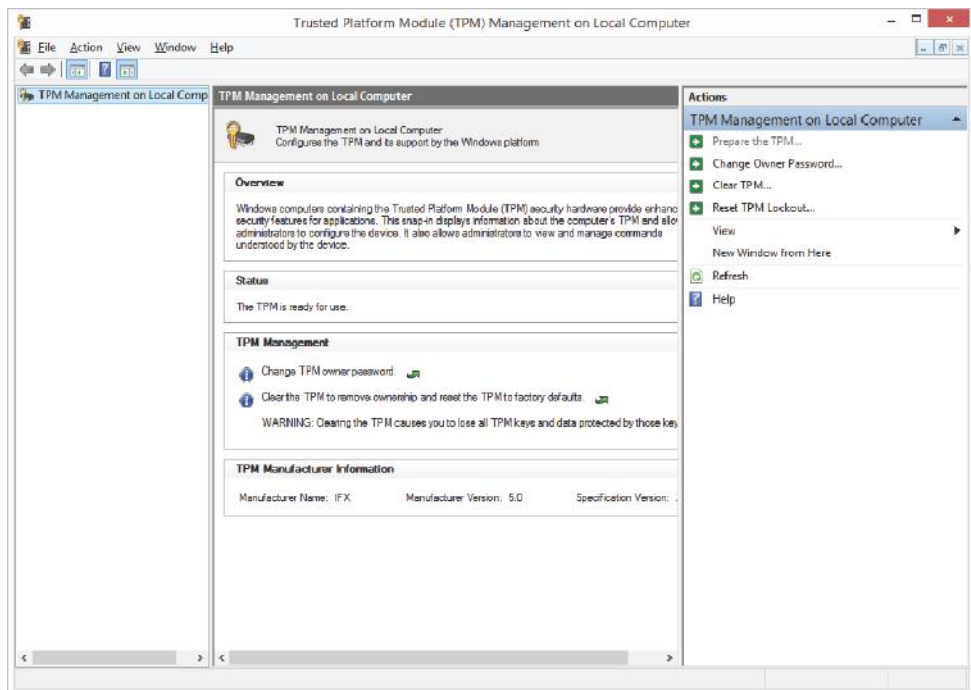


Appendix(Cont.)

Enter "tpm.msc" under command mode and start to setup the TPM.



```
Command Prompt
Microsoft Windows [Version 6.3.9431]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Users\DK>tpm.msc
```



Vertrieb durch



AMC – Analytik & Messtechnik GmbH Chemnitz

Heinrich-Lorenz-Str. 55
09120 Chemnitz

Tel.: +49/371/38388-0
Fax: +49/371/38388-99

E-Mail: info@amc-systeme.de

Web: www.amc-systeme.de