PCA-TPM
Trusted Platform Module TCG 1.2
Startup Manual

Packing List

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

1.	PCA-TPM trusted platform module x1	
2.	2-year quality warranty card x 1	P/N: 2190000902
3.	Startup manual x 1	P/N: 20020TPM01
4.	Screw x 1	P/N: 1930005258
5.	Driver CD x 1	P/N: 20620TPM00

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

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

http://www.advantech.com

http://www.advantech.com/eplatform

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

http://www.advantech.com/suppot/

This manual is for the PCA-TPM Series.

Part No. 20020TPM01
Print in Taiwan
2nd Edition
July 2011

Specifications

Standard Functions

- Trusted platform module compliant with TCG 1.2 specification and TSS 1.2 via LPC connector on CPU card.
- Adopting Infineon SLB9635TT1.2 FW3.17 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.
- SBC and operation system support list

SBC support list	
PICMG 1.3 system host boards	PCE-5125
PICMG 1.0 single board computers	PCA-6010, PCA-6011
Half-size single board computers	PCI-7020, PCI-7030, PCI-7031*, PCA-6782*

* PCI-7031/PCA-6782 standard version BIOS can not support PCA-TPM. In this case, an ODM BIOS is required.

OS support list
Win7 Ultimate (32 bit) Win7 Ultimate (64 bit) Windows XP Professional Edition (32 bit) Windows XP Professional Edition (64 bit) Windows Server 2003 Standard (32 bit) Windows Server 2003 Standard (64 bit) Windows Server 2003 Enterprise (32 bit) Windows Server 2003 Enterprise (64 bit) Windows Server 2008 Standard (32 bit) Windows Server 2008 Data center (32 bit)

Mechanical

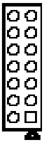
- **Dimensions:** 31.5 mm x 30.5 mm
- **Power supply type:** 3.3 V, 5 V, 5 VSB
- **Power requirements:** 3.3 V @ 5 mA, 3.3 VSB @ 25 mA (Operation time)
- **Operating temperature:** 0 ~ 60° C
- **Operating humidity:** 40° C @ 85% RH, Non-Condensing
- **Storage temperature:** -40 ~ 85° C
- **Storage humidity:**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

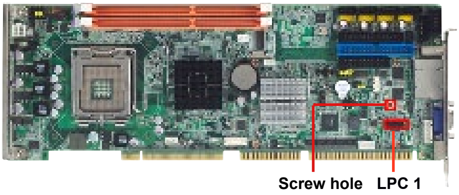


Pin	Signal	Pin	Signal
1	LPC_AD1	2	CLK_TPM
3	LPC_AD0	4	#PLTRST
5	VCC3	6	#LFRAME
7	GND	8	LPC_AD3
9	N/A	10	LPC_AD2
11	N/A	12	LPC_SERIRQ
13	VCC	14	VCC5SB

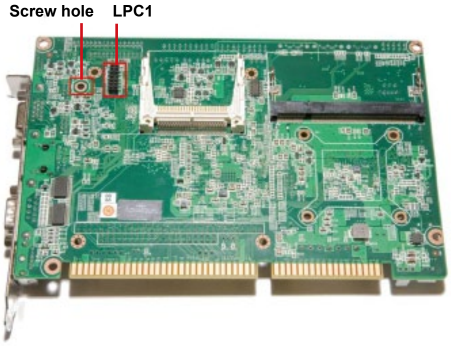
Installation Guide

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).

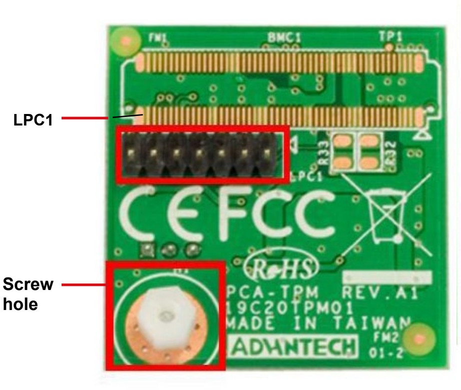


Picture 1

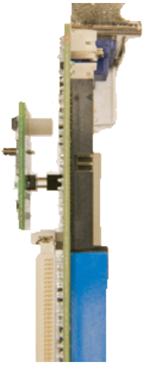


Picture 2

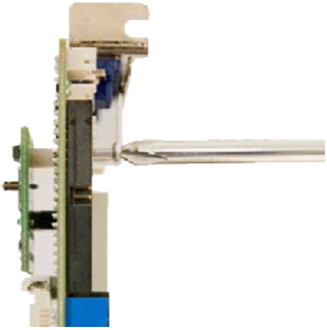
   2). Locate LPC1 and the screw hole on PCA-TPM.



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

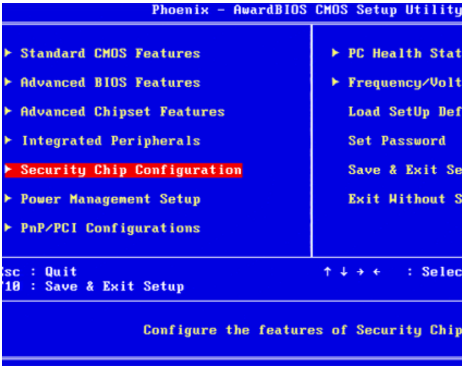


4). Align the screw holes, and fix securely with the screw.



2. After setting up the hardware configuration, users should also complete BIOS settings as well as software installation to start encryption and decryption processes.

   1). For BIOS settings, there are two kinds of BIOS menu for those SBC products. Please check the information below to find out corresponding instructions to enable the TPM function.
   For PCI-7020, PCI-7030, and PCA-6010, please follow instructions below to enable TPM.

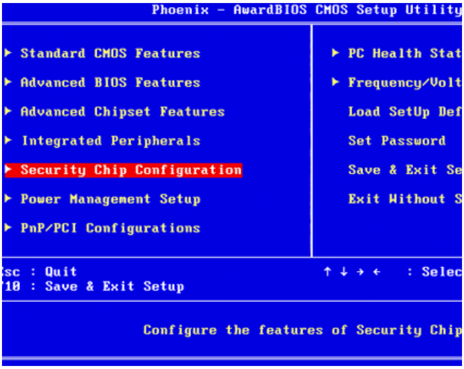


```
                         Phoenix - AwardBIOS CMOS Setup Utility

▶ Standard CMOS Features              ▶ PC Health Stat
▶ Advanced BIOS Features              ▶ Frequency/Volt
▶ Advanced Chipset Features             Load SetUp Def
▶ Integrated Peripherals                Set Password
▶ Security Chip Configuration           Save & Exit Se
▶ Power Management Setup                Exit Without S
▶ PnP/PCI Configurations

sc : Quit                              ↑ ↓ → ←   : Selec
10 : Save & Exit Setup

                    Configure the features of Security Chip
```



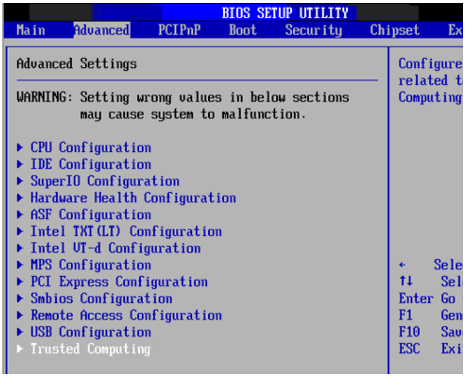
```
                         Phoenix - AwardBIOS CMOS Setup Utility

▶ Standard CMOS Features              ▶ PC Health Stat
▶ Advanced BIOS Features              ▶ Frequency/Volt
▶ Advanced Chipset Features             Load SetUp Def
▶ Integrated Peripherals                Set Password
▶ Security Chip Configuration           Save & Exit Se
▶ Power Management Setup                Exit Without S
▶ PnP/PCI Configurations

sc : Quit                              ↑ ↓ → ←   : Selec
10 : Save & Exit Setup

                    Configure the features of Security Chip
```

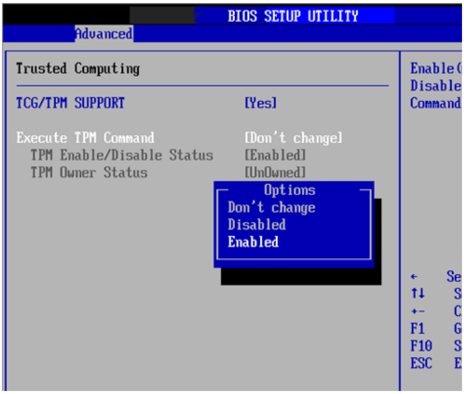
For PCA-6011, PCE-5125, PCI-7031, and PCA-6782, please follow instructions below to enable TPM.



```
                     BIOS SETUP UTILITY
 Main   Advanced   PCIPnP   Boot   Security   Chipset   Ex

 Advanced Settings                               Configure
                                                 related t
 WARNING: Setting wrong values in below sections Computing
          may cause system to malfunction.

 ▶ CPU Configuration
 ▶ IDE Configuration
 ▶ SuperIO Configuration
 ▶ Hardware Health Configuration
 ▶ ASF Configuration
 ▶ Intel TXT(LT) Configuration
 ▶ Intel VT-d Configuration
 ▶ MPS Configuration                             ←    Sele
 ▶ PCI Express Configuration                     ↑↓    Sel
 ▶ Smbios Configuration                          Enter Go
 ▶ Remote Access Configuration                   F1    Gen
 ▶ USB Configuration                             F10   Sav
 ▶ Trusted Computing                             ESC   Exi
```



```
                     BIOS SETUP UTILITY
          Advanced

 Trusted Computing                                Enable(
                                                  Disable
 TCG/TPM SUPPORT                [Yes]             Command

 Execute TPM Command            [Don't change]
   TPM Enable/Disable Status    [Enabled]
   TPM Owner Status             [UnOwned]
                              ┌─── Options ───┐
                              │ Don't change  │
                              │ Disabled      │
                              │ Enabled       │
                              └───────────────┘
                                                  ←    Se
                                                  ↑↓    S
                                                  +-    C
                                                  F1    G
                                                  F10   S
                                                  ESC   E
```

2). For software installation, there are two Application Programs (AP). One is the default AP within the OS and the other is the Infineon security platform settings tool on the driver CD. The table below shows the AP suggested for your OS.

Compatible software Operating System	Infineon security platform settings tool	OS built-in AP
Win7 Ultimate (32 bit)	v	v
Win7 Ultimate (64 bit)	v	v
Windows XP Professional Edition SP3 (32 bit)	v	
Windows XP Professional Edition SP2 (64 bit)	v	
Windows Sever 2003 Standard R2 SP2 (32 bit)	v	
Windows Sever 2003 Standard R2 SP2 (64 bit)	v	
Windows Sever 2003 Enterprise R2 SP2 (32 bit)	v	
Windows Sever 2003 Enterprise R2 SP2 (64 bit)	v	
Windows Server 2008 Standard SP2 (32 bit)	v	v
Windows Server 2008 Data center SP2 (32 bit)	v	

Board Layout

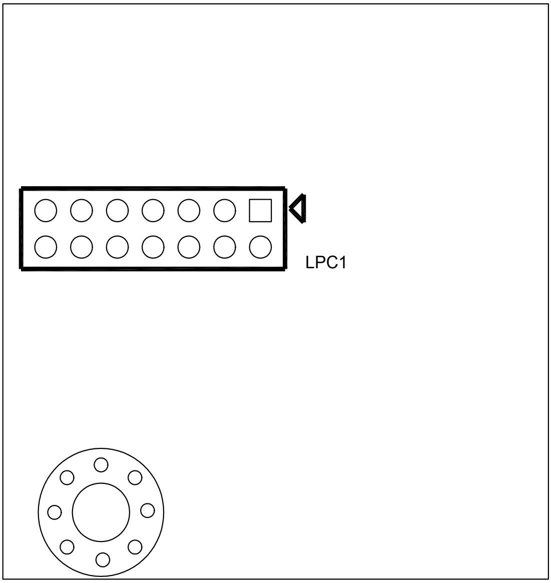


Figure 1: PCA-TPM Board Layout

Board Dimensions

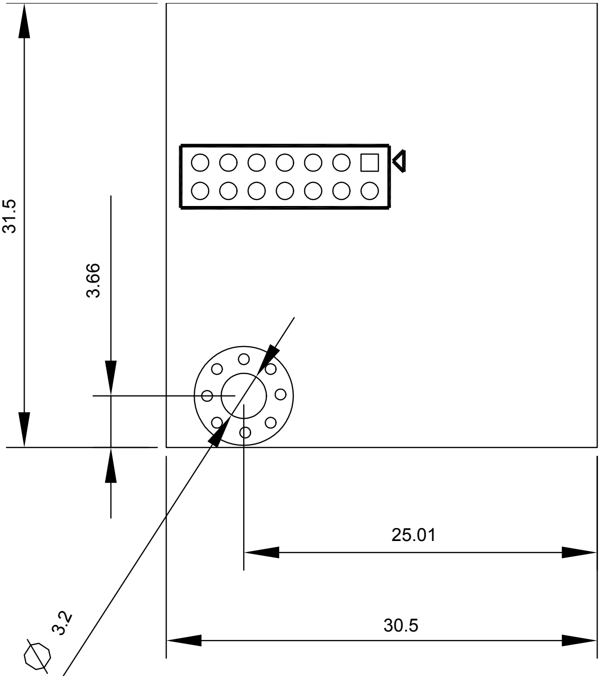


Figure 3: PCA-TPM Board Dimensions