



**IOB32**

**6830-xxx**

**No. 87-006833-000    Revision C**

**REFERENCE GUIDE**

**Trusted Platform Module (TPM)**

**And**

**I/O Expansion Board**

**WARRANTY**

The following is an abbreviated version of Trenton Technology's warranty policy for PICMG® 1.3 products. For a complete warranty statement, contact Trenton or visit our website at [www.TrentonTechnology.com](http://www.TrentonTechnology.com).

Trenton PICMG® 1.3 products are warranted against material and manufacturing defects for five years from date of delivery to the original purchaser. Buyer agrees that if this product proves defective Trenton Technology Inc. is only obligated to repair, replace or refund the purchase price of this product at Trenton Technology's discretion. The warranty is void if the product has been subjected to alteration, neglect, misuse or abuse; if any repairs have been attempted by anyone other than Trenton Technology Inc.; or if failure is caused by accident, acts of God, or other causes beyond the control of Trenton Technology Inc. Trenton Technology Inc. reserves the right to make changes or improvements in any product without incurring any obligation to similarly alter products previously purchased.

In no event shall Trenton Technology Inc. be liable for any defect in hardware or software or loss or inadequacy of data of any kind, or for any direct, indirect, incidental or consequential damages arising out of or in connection with the performance or use of the product or information provided. Trenton Technology Inc.'s liability shall in no event exceed the purchase price of the product purchased hereunder. The foregoing limitation of liability shall be equally applicable to any service provided by Trenton Technology Inc.

**RETURN POLICY**

A Return Material Authorization (RMA) number, obtained from Trenton Technology prior to return, must accompany products returned for repair. The customer must prepay freight on all returned items, and the customer is responsible for any loss or damage caused by common carrier in transit. Items will be returned from Trenton Technology via Ground, unless prior arrangements are made by the customer for an alternative shipping method.

To obtain an RMA number, call us at (800) 875-6031 or (770) 287-3100. We will need the following information:

- Return company address and contact
- Model name and model # from the label on the back of the product
- Serial number from the label on the back of the product
- Description of the failure

An RMA number will be issued. Mark the RMA number clearly on the outside of each box, include a failure report for each board and return the product(s) to our Utica, NY facility:

- TRENTON Technology Inc.
- 1001 Broad Street
- Utica, NY 13501
- Attn: Repair Department

Contact Trenton for our complete service and repair policy.

**TRADEMARKS**

IBM, PC/AT, VGA, EGA, OS/2 and PS/2 are trademarks or registered trademarks of International Business Machines Corp.

AMI and AMIBIOS are trademarks of American Megatrends Inc.

Windows XP, Windows Vista Ultimate and Microsoft are trademarks or registered trademarks of Microsoft Corp.

Atmel is a registered trademark of Atmel Corp.

EMBASSY Trust Suite and Wave are registered trademarks of Wave Systems Corp.

PICMG, SHB Express and the PICMG logo are trademarks or registered trademarks of the PCI Industrial Computer Manufacturers Group.

All other brand and product names may be trademarks or registered trademarks of their respective companies.

**LIABILITY DISCLAIMER**

This reference guide is as complete and factual as possible at the time of printing; however, the information in this reference guide may have been updated since that time. Trenton Technology Inc. reserves the right to change the functions, features or specifications of their products at any time, without notice.

In no event shall Trenton Technology Inc. be liable for any defect in hardware or software or loss or inadequacy of data of any kind, or for any direct, indirect, incidental or consequential damages arising out of or in connection with the performance or use of the product or information provided. Trenton Technology Inc.'s liability shall in no event exceed the purchase price of the product purchased hereunder. The foregoing limitation of liability shall be equally applicable to any service provided by Trenton Technology Inc.

Copyright © 2008 by Trenton Technology Inc. All rights reserved.

E-mail: [Support@TrentonTechnology.com](mailto:Support@TrentonTechnology.com)

Web: [www.TrentonTechnology.com](http://www.TrentonTechnology.com)



TRENTON Technology Inc.

2350 Centennial Drive • Gainesville, Georgia 30504

Sales: (800) 875-6031 • Phone: (770) 287-3100 • Fax: (770) 287-3150

---

*This page intentionally left blank*

# Table of Contents

<b>CHAPTER 1</b>	<b>SPECIFICATIONS</b> .....	<b>1-1</b>
	Introduction.....	1-1
	Models .....	1-1
	Features.....	1-1
	IOB32 (6830-002) - Board Layout Drawing .....	1-2
	IOB32 (6830-001) - Board Layout Drawing .....	1-2
	IOB32 (6830-002) Connectors.....	1-3
	IOB32 (6830-002) Connectors (continued) .....	1-4
	IOB32 (6830-001) Connectors.....	1-7
<b>CHAPTER 2</b>	<b>IOB32 TPM IMPLEMENTATION</b> .....	<b>2-1</b>
	Introduction.....	2-1
	System Requirements – Full TPM Implementation .....	2-1
	System Requirements – Basic TPM Implementation .....	2-1
	Process Steps - Full TPM Implementation .....	2-2
	Process Steps - Basic TPM Implementation Using Microsoft Vista Ultimate – Bit Locker .....	2-6
<b>CHAPTER 3</b>	<b>TPM APPLICATION CONSIDERATIONS AND CAUTIONS</b> .....	<b>3-1</b>
	TPM Default Settings.....	3-1
	Data Back Up.....	3-1
	Passwords, Migratable and Non-Migratable Keys .....	3-1
	TPM Cautions – Bit Locker .....	3-1
	TPM Cautions – EMBASSY TRUST SUITE (ETS).....	3-2
	TPM Cautions – Data Recovery.....	3-2
<b>APPENDIX A</b>	<b>REFERENCES</b> .....	<b>A-1</b>
	Notes:.....	A-2
	Notes:.....	A-3

**HANDLING PRECAUTIONS**

---

**WARNING:** This product has components that may be damaged by electrostatic discharge.

---

To protect your IOB32 from electrostatic damage, be sure to observe the following precautions when handling or storing the board:

- Keep the IOB32 in its static-shielded bag until you are ready to perform your installation.
- Handle the IOB32 by its edges.
- Do not touch the I/O connector pins.
- Do not apply pressure or attach labels to the IOB32.
- Use a grounded wrist strap at your workstation or ground yourself frequently by touching the metal chassis of the system before handling any components. The system must be plugged into an outlet that is connected to an earth ground.
- Use antistatic padding on all work surfaces.
- Avoid static-inducing carpeted areas.

**RECOMMENDED BOARD HANDLING PRECAUTIONS**

This IOB32 has components on both sides of the PCB. Some of these components are extremely small and subject to damage if the board is not handled properly. It is important for you to observe the following precautions when handling or storing the board to prevent components from being damaged or broken off:

- Handle the board only by its edges.
- Store the board in padded shipping material or in an anti-static board rack.
- Do not place an unprotected board on a flat surface.

## *Before You Begin*

### INTRODUCTION

The IOB32 operates on Trenton's TQ9, MCX- and MCG-series System Host Boards. It is important to be aware of the system considerations listed below before installing your IOB32 (6830-xxx) Trusted Platform Module (TPM) and I/O Expansion Board. Overall system performance may be affected by incorrect usage of these features. *Before* encrypting any data in a system using TPM, Trenton Technology strongly recommends backing up *all* critical data. Backing up critical data ensures that the data can be restored in the event of a hardware failure to a critical system component such as the TPM, SHB, or HDD and/or the loss of the TPM password(s) or keys.

### POTENTIAL DATA LOSS

Users of the IOB32 must take certain precautions when implementing TPM to ensure against unintended loss of data or access to their TPM-based computing platform. The data encryption software used with TPM implementations may become inaccessible or unrecoverable if:

- **The TPM passwords are lost** – *No TPM password recovery is available.*
- **A hard drive fails** – Regular system hard drive or other storage media data backup is *absolutely critical* in TPM installations. If the storage device that contains the TPM encrypted data fails, an image of the hard disk can only be restored from the backup in order to gain access to the encrypted data.
- **The SHB fails or is replaced** – Recovery procedures *may* allow migratable TPM access keys to be recovered and *may* be able to restore encrypted data. All non-migratable keys and their associated data will be lost in the event of an SHB failure or replacement. The EMBASSY<sup>®</sup> Trust Suite TPM software from Wave<sup>®</sup> Systems Corp. utilizes some migratable keys.
- **TPM Ownership is lost** – TPM ownership and data contents may be cleared to allow transfer of a system to a new owner. If the TPM ownership is cleared without taking the proper precautions, recovery procedures *may* allow recovery of the migratable keys and restoration of access to the encrypted data.

### SECURITY PRECAUTIONS

TPM is designed to provide computer platform security by using sophisticated data encryption techniques and platform user authentication. TPM essentially provides two different types of locks that protect the computer's data and platform access. Two different keys are needed for the TPM locks: migratable keys and non-migratable keys. The user must thoroughly understand the functions of the two TPM key types and develop a security plan that governs access to their system's TPM keys. For example a non-migratable key means just that, "the non-migratable TPM key **cannot** be moved or migrated from one platform to another". If a system with a TPM implementation has the TPM itself fail, all non-migratable keys and the data associated with these keys will be inaccessible and unrecoverable.

### OPERATING SYSTEMS SUPPORT FOR TPM - MICROSOFT<sup>®</sup> WINDOWS VISTA<sup>®</sup> ULTIMATE 32-BIT & 64-BIT

The Windows Vista Ultimate operating system supports a basic implementation of TPM that may be suitable for many applications. The Bit Locker instructions within the O/S utilize the Microsoft software stack that is built into to the Windows Vista Ultimate O/S to provide this basic TPM functionality.

### OPERATING SYSTEMS SUPPORT FOR TPM - MICROSOFT<sup>®</sup> WINDOWS XP PROFESSIONAL (SP2) 32-BIT AND WINDOWS VISTA ULTIMATE 32-BIT

More advanced TPM implementations require the use of the Trusted Software Stack (TSS). NTRU Cryptosystems, Inc. supplies a TSS called the NTRU Core TCG Software Stack or CTSS that is integral to the Atmel<sup>®</sup> TPM software driver built into the Trenton IOB32's firmware. A third party software program from Wave Systems Corp. called the EMBASSY Trust Suite (ETS) uses the CTSS to fully implement the TPM 1.2 instruction set when using the Windows XP 32-bit operating system. Currently, the ETS software only functions with the Windows XP (SP2) 32-bit and the Windows Vista Ultimate 32-bit operating systems.

*This page intentionally left blank*

## Chapter 1 Specifications

### INTRODUCTION

The IOB32 is designed to operate with Trenton's TQ9, MCX- and MCG-series of PICMG 1.3 System Host Boards. The IOB32 supports industrial computers that require the Trusted Platform Module (TPM) functionality and/or serial communication ports, PS/2 devices, floppy drive and parallel printer interfaces. There are two models of the IOB32 available and they are explained below.

### MODELS

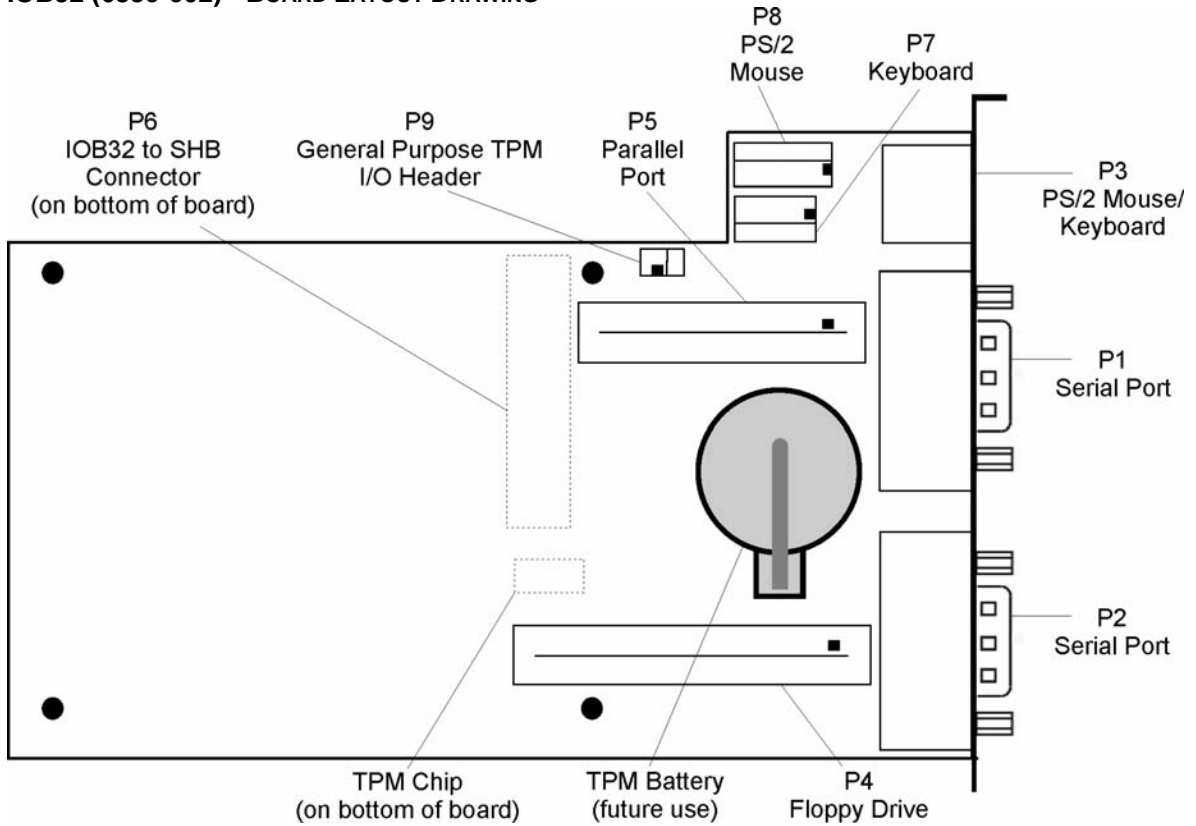
<u>Model #</u>	<u>Model Name</u>	<u>Description</u>
6830-001	IOB32NI	Supports TPM functionality <i>only</i>
6830-002	IOB32MC	Uses the IOB30MC I/O bracket* and supports PS2 devices, serial communication ports, floppy drive and parallel printer interfaces <i>plus</i> the TPM functionality

\*The 6830-002 version of the IOB32 uses the IOB30MC I/O bracket that is designed for use with the Trenton MCX/MCG-series of SHBs and the TQ9 SHB.

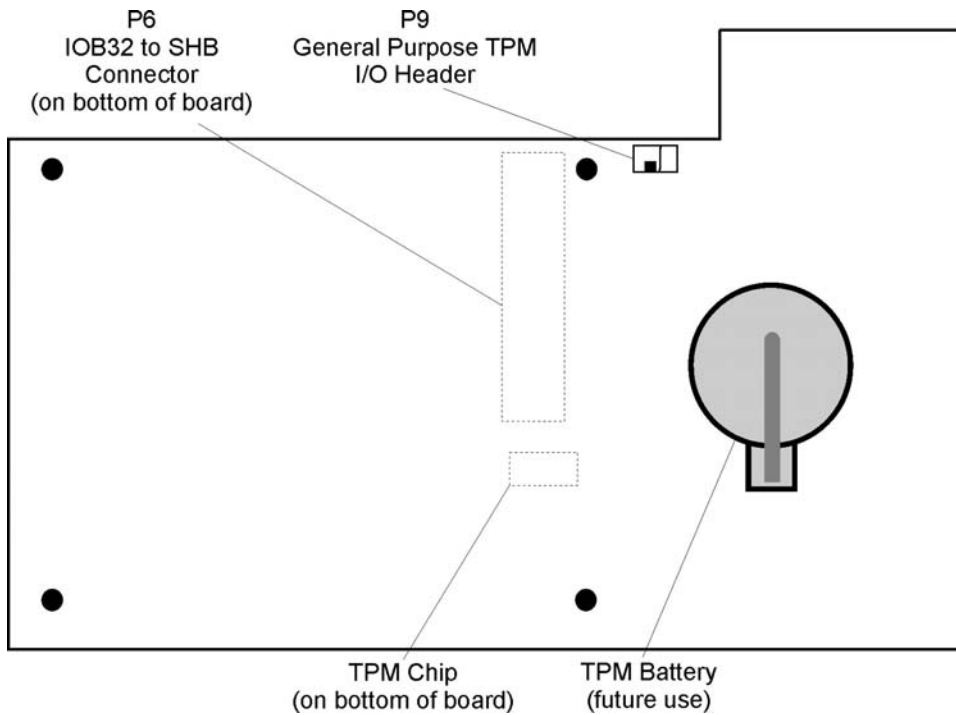
### FEATURES

- Controlled Impedance Connector and mounting posts provides robust connection with secured mounting to a Trenton PICMG 1.3 system host board (SHB)
- Legacy I/O support for PS2 devices, serial communication ports, floppy drive and parallel printer interfaces (6830-002 version)
- I/O bracket ports – MiniDin connector for PS2 mouse and keyboard and two DB-9 serial communication ports (6830-002 version)
- On-board headers support floppy drive and parallel printer interfaces (6830-002 version)
- On-board headers support separate PS2 keyboard and mouse connections (6830-002 version)
- TPM 1.2 compatibility *and* legacy I/O support (6830-002 version)
- TPM 1.2 compatibility *only* (6830-001 version)
- On-board battery will provide backup power to support a future Run Time Clock (RTC) capability planned for TPM, but not currently implemented the TPM device firmware

**IOB32 (6830-002) - BOARD LAYOUT DRAWING**



**IOB32 (6830-001) - BOARD LAYOUT DRAWING**



---

**IOB32 (6830-002) CONNECTORS**


---

**NOTE:** Pin 1 on the connectors is indicated by the square pad on the PCB.

---

- P1** - **Serial Port Connector**  
9 position "D" right angle, Spectrum #56-402-001

<u>Pin</u>	<u>Signal</u>	<u>Pin</u>	<u>Signal</u>
1	Carrier Detect	6	Data Set Ready-I
2	Receive Data-I	7	Request to Send-O
3	Transmit Data-O	8	Clear to Send-
4	Data Terminal Ready-O	9	Ring Indicator-I
5	Signal Gnd		

- P2** - **Serial Port Connector**  
9 position "D" right angle, Spectrum #56-402-001

<u>Pin</u>	<u>Signal</u>	<u>Pin</u>	<u>Signal</u>
1	Carrier Detect	6	Data Set Ready-I
2	Receive Data-I	7	Request to Send-O
3	Transmit Data-O	8	Clear to Send-
4	Data Terminal Ready-O	9	Ring Indicator-I
5	Signal Gnd		

- P3** - **PS/2 Mouse and Keyboard Connector**  
6 pin mini DIN, Tyco 5750071-1

<u>Pin</u>	<u>Signal</u>
1	Ms Data
2	Kbd Data
3	Gnd
4	Power (+5V fused) with self-resetting fuse
5	Ms Clock
6	Kbd Clock

**IOB32 (6830-002) CONNECTORS (CONTINUED)**

**P4 - Floppy Drive Connector**  
34 pin dual row header, Molex #702463401

<u>Pin</u>	<u>Signal</u>	<u>Pin</u>	<u>Signal</u>
1	Gnd	2	N-RPM
3	Gnd	4	NC
5	Gnd	6	D-Rate0
7	Gnd	8	P-Index
9	Gnd	10	N-Motoron 1
11	Gnd	12	N-Drive Sel2
13	Gnd	14	N-Drive Sel1
15	Gnd	16	N-Motoron 2
17	Gnd	18	N-Dir
19	Gnd	20	N-Stop Step
21	Gnd	22	N-Write Data
23	Gnd	24	N-Write Gate
25	Gnd	26	P-Track 0
27	Gnd	28	P-Write Protect
29	Gnd	30	N-Read Data
31	Gnd	32	N-Side Select
33	Gnd	34	Disk Change

**P5 - Parallel Port Connector**  
26 pin dual row header, Molex #702462601

<u>Pin</u>	<u>Signal</u>	<u>Pin</u>	<u>Signal</u>
1	Strobe	2	Auto Feed XT
3	Data Bit 0	4	Error
5	Data Bit 1	6	Init
7	Data Bit 2	8	Slct In
9	Data Bit 3	10	Gnd
11	Data Bit 4	12	Gnd
13	Data Bit 5	14	Gnd
15	Data Bit 6	16	Gnd
17	Data Bit 7	18	Gnd
19	ACK	20	Gnd
21	Busy	22	Gnd
23	Paper End	24	Gnd
25	Slct	26	NC

**IOB32 (6830-002) CONNECTORS (CONTINUED)**

**P6 - IOB32 to SHB Controlled Impedance Connector**  
76 pin controlled impedance connector,  
Samtec #MIT-038-05-FD

<u>Pin</u>	<u>Signal</u>	<u>Pin</u>	<u>Signal</u>
1	+12	2	+5V_STANDBY
3	NC	4	+5V_STANDBY
5	NC	6	+5V_DUAL
7	NC	8	+5V_DUAL
9	NC	10	NC
11	NC	12	NC
13	ICH_SMI#	14	ICH_RCIN#
15	ICH_SIOPME#	16	ICH_A20GATE
17	Gnd	18	Gnd
19	L_FRAME#	20	L_AD3
21	L_DRQ1#	22	L_AD2
23	L_DRQ0#	24	L_AD1
25	SERIRQ	26	L_AD0
27	Gnd	28	Gnd
29	PCLK14SIO	30	PCLK33LPC
31	Gnd	32	Gnd
33	SMBDATA_RESUME	34	IPMB_DAT
35	SBMCLK_RESUME	36	IPMB_CLK
37	SALRT#_RESUME	38	IPMB_ALRT#
39	Gnd	40	Gnd
41	EXP_CLK100	42	EXP_RESET#
43	EXP_CLK100#	44	ICH_WAKE#
45	Gnd	46	Gnd
47	C_PE_TXP4	48	C_PE_RXP4
49	C_PE_TXN4	50	C_PE_RXN4
51	Gnd	52	Gnd
53	C_PE_TXP3	54	C_PE_RXP3
55	C_PE_TXN3	56	C_PE_RXN3
57	Gnd	58	Gnd
59	C_PE_TXP2	60	C_PE_RXP2
61	C_PE_TXN2	62	C_PE_RXN2
63	Gnd	64	Gnd
65	C_PE_TXP1	66	C_PE_RXP1
67	C_PE_TXN1	68	C_PE_RXN1
69	Gnd	70	Gnd
71	+3.3V	72	+5V
73	+3.3V	74	+5V
75	+3.3V	76	+5v

**IOB32 (6830-002) CONNECTORS (CONTINUED)**

- P7** - **Keyboard Header**  
5 pin single row header, Amp #640456-5

<u>Pin</u>	<u>Signal</u>
1	Kbd Clock
2	Kbd Data
3	Key
4	Kbd Gnd
5	Kbd Power (+5V fused) with self resetting fuse

- P8** - **PS/2 Mouse Header**  
6 pin single row header, Amp #640456-6

<u>Pin</u>	<u>Signal</u>
1	Ms Data
2	Reserved
3	Gnd
4	Power (+5V fused) with self-resetting fuse
5	Ms Clock
6	Reserved

- P9** - **General Purpose TPM I/O Header**  
2 pin single row header, Amp #640456-2

<u>Pin</u>	<u>Signal</u>
1	Gnd
2	Contact Closure To/From the TPM Module

**IOB32 (6830-001) CONNECTORS****P6 - IOB32 to SHB Controlled Impedance Connector**

76 pin controlled impedance connector,  
Samtec #MIT-038-05-FD

<u>Pin</u>	<u>Signal</u>	<u>Pin</u>	<u>Signal</u>
1	+12	2	+5V_STANDBY
3	NC	4	+5V_STANDBY
5	NC	6	+5V_DUAL
7	NC	8	+5V_DUAL
9	NC	10	NC
11	NC	12	NC
13	ICH_SMI#	14	ICH_RCIN#
15	ICH_SIOPME#	16	ICH_A20GATE
17	Gnd	18	Gnd
19	L_FRAME#	20	L_AD3
21	L_DRQ1#	22	L_AD2
23	L_DRQ0#	24	L_AD1
25	SERIRQ	26	L_AD0
27	Gnd	28	Gnd
29	PCLK14SIO	30	PCLK33LPC
31	Gnd	32	Gnd
33	SMBDATA_RESUME	34	IPMB_DAT
35	SBMCLK_RESUME	36	IPMB_CLK
37	SALRT#_RESUME	38	IPMB_ALRT#
39	Gnd	40	Gnd
41	EXP_CLK100	42	EXP_RESET#
43	EXP_CLK100#	44	ICH_WAKE#
45	Gnd	46	Gnd
47	C_PE_TXP4	48	C_PE_RXP4
49	C_PE_TXN4	50	C_PE_RXN4
51	Gnd	52	Gnd
53	C_PE_TXP3	54	C_PE_RXP3
55	C_PE_TXN3	56	C_PE_RXN3
57	Gnd	58	Gnd
59	C_PE_TXP2	60	C_PE_RXP2
61	C_PE_TXN2	62	C_PE_RXN2
63	Gnd	64	Gnd
65	C_PE_TXP1	66	C_PE_RXP1
67	C_PE_TXN1	68	C_PE_RXN1
69	Gnd	70	Gnd
71	+3.3V	72	+5V
73	+3.3V	74	+5V
75	+3.3V	76	+5v

**P9 - General Purpose TPM I/O Header**

2 pin single row header, Amp #640456-2

<u>Pin</u>	<u>Signal</u>
1	Gnd
2	Contact Closure To/From the TPM Module

*This page intentionally left blank*

## Chapter 2 IOB32 TPM Implementation

### INTRODUCTION

The Trusted Platform Module or TPM is a component from the Atmel Corporation that is mounted on the bottom of a Trenton IOB32 board. The data protection and system access schemes of the past housed data encryption and security key operations in a computer's storage device or system memory. The results being that no matter how good the protection scheme was, the system was still vulnerable to attack. A TPM increases a systems' data security while providing a highly controlled level of access by placing key system operations and tasks within the protected environment of the TPM itself.

An IOB32 plugged into a Trenton PICMG 1.3 System Host Board (SHB) provides the TPM functionality that enables an industrial computer to meet the various Trusted Computing specifications and standards that have been defined by the Trusted Computing Group™. TPM is designed to provide computer platform security by using sophisticated data encryption techniques and platform user authentication.

The operating system software, NTRU CTSS (Core TCG Software Stack), TPM driver, TPM application software and the SHB's BIOS all work together to provide the software support needed to implement TPM. The BIOS is part of the SHB and the TPM driver from Trenton includes the CTSS. The CTSS is used by 3<sup>rd</sup> party TPM application software such as the EMBASSY® Trusted Suite (ETS) from Wave Systems Corp. to unlock the full feature set of the IOB32's TPM.

The TPM and the associated software mentioned in the previous paragraph provide two different types of locks that protect the computer's data and platform access. Two different keys are needed for the TPM locks: migratable keys and non-migratable keys. The use of keys and platform specific authentication information within the TPM help protect a system from a wide variety of software-based attacks.

Visit the Trusted Computing Group's website ([www.TrustedComputing.org](http://www.TrustedComputing.org)) to learn more about what TPM is and how it enables a system to operate as a "Trusted Computing" solution platform.

### SYSTEM REQUIREMENTS – FULL TPM IMPLEMENTATION

- Trenton MCX-series, or MCG-series or TQ9 System Host Board (SHB)
- Microsoft Windows XP Professional (SP2) 32-bit or Microsoft Windows Vista Ultimate 32-bit operating system
- Trenton/Atmel TPM Driver (includes NTRU CTSS - Core TCG Software Stack)
- Microsoft Internet Explorer 5.5 or later
- Adobe Acrobat 5.0 or later
- EMBASSY Trust Suite - TPM Application Software

### SYSTEM REQUIREMENTS – BASIC TPM IMPLEMENTATION

- Trenton MCX-series, or MCG-series or TQ9 System Host Board (SHB)
- Windows Vista Ultimate 32-bit or 64-bit operating systems
  - Bit Locker functionality used for basic TPM implementations
- Trenton/Atmel TPM Driver (includes NTRU CTSS - Core TCG Software Stack)
- Microsoft Internet Explorer 5.5 or later
- Adobe Acrobat 5.0 or later

The IOB32's TPM is defaulted to "OFF" and the SHB's Trusted Computing BIOS settings are defaulted to "NO" for TCG/TPM Support and "Disable" for Execute TPM Card. The following process steps walk you through installing the IOB32 and setting up the system's TPM software elements for Trusted Computing operation.

**PROCESS STEPS - FULL TPM IMPLEMENTATION**

1. Install the IOB32 by plugging the board into the SHB’s controlled impedance connector. Secure the IOB32 to the SHB using the included hardware and the mounting post on the SHB.
2. Install the combined SHB and IOB32 into the backplane and connect all of the system components including the keyboard and mouse.
3. Power up your system and enter the SHB’s BIOS set-up menus. Normally, the only POST routine visible on the screen is the memory test. The following screen displays when the system is powered on:



**Initial Power-On Screen**

4. Press <Del> to access the BIOS Setup Utility. If you have already entered a BIOS access password you will need to enter it in order to gain access to the SHB’s BIOS set-up menus. Refer to the *Password Entry* section of the SHB’s BIOS chapter if you need help with entering the SHB’s password.
5. Select the **Advanced** set-up menu from the BIOS Setup Utility Main Menu and the following Setup screen will be displays:

BIOS SETUP UTILITY	
Main	<b>Advanced</b>
PCIPnP	Boot
Security	Chipset
Exit	
<p>Advanced Settings</p> <hr/> <p>WARNING: Setting wrong values in below sections may cause system to malfunction.</p> <ul style="list-style-type: none"> <li>&gt; CPU Configuration</li> <li>&gt; IDE Configuration</li> <li>&gt; Floppy Configuration</li> <li>&gt; SuperIO Configuration</li> <li>&gt; ACPI Configuration</li> <li>&gt; AHCI Configuration</li> <li>&gt; MPS Configuration</li> <li>&gt; Remote Access (or PCI Express) Configuration</li> <li>&gt; <b>Trusted Computing</b></li> <li>&gt; USB Configuration</li> </ul>	<p>Configure settings related to Trusted Computing innovations</p>          <p>←→ Select Screen                      ↑↓ Select Item                      Enter Go to Sub Screen                      F1 General Help                      F10 Save and Exit                      ESC Exit</p>
V02.61 (C)Copyright 1985-2008, American Megatrends, Inc.	

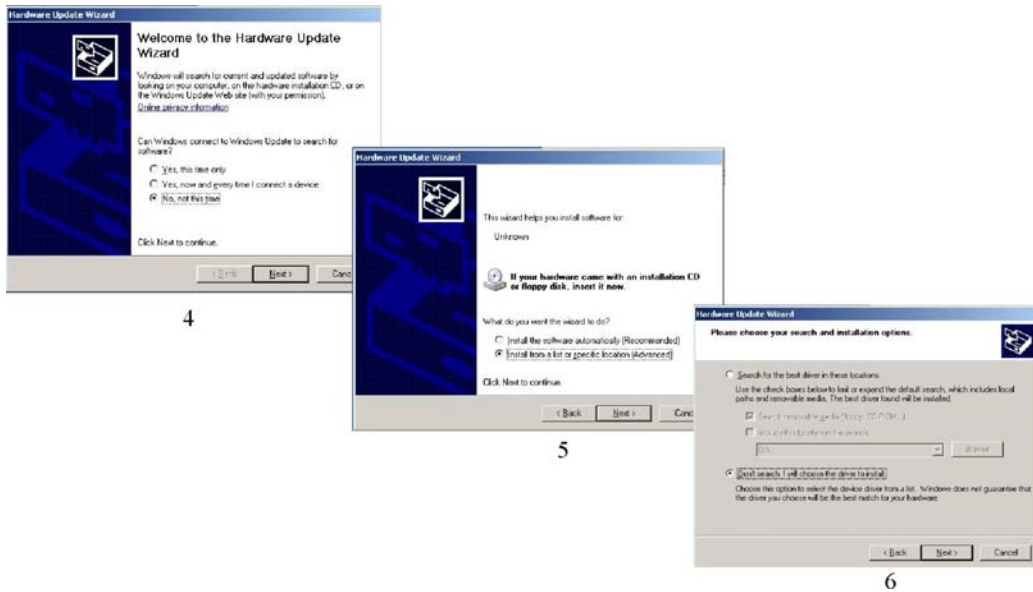
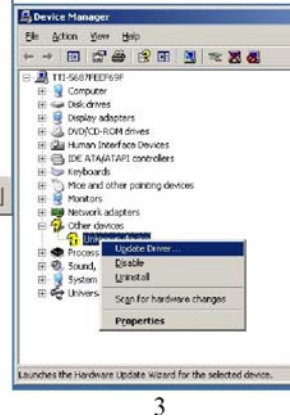
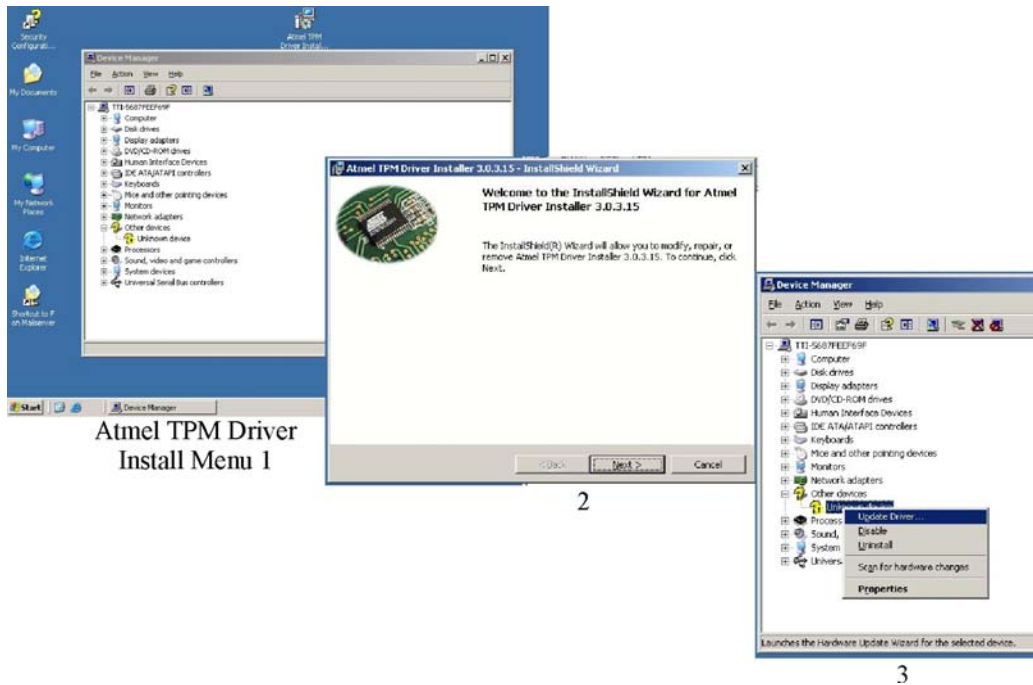
**Advanced Setup BIOS Screen**

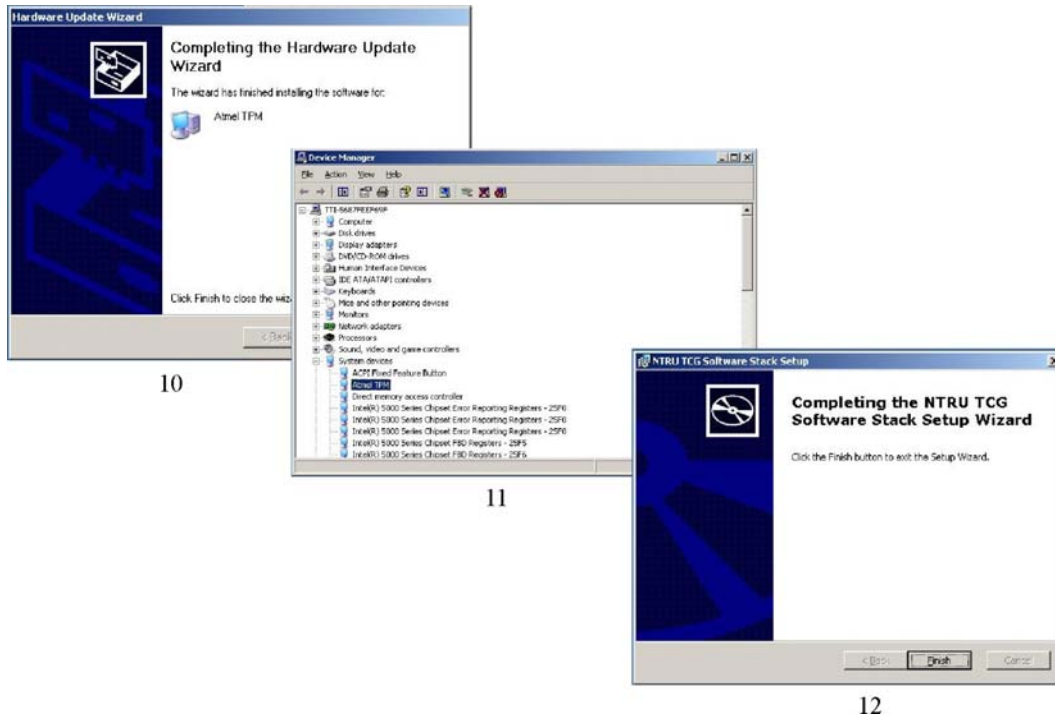
6. Cursor down to the Trusted Computing selection and hit enter to move to the TPM BIOS settings. The following TPM/SHB BIOS set-up menu will appear:

BIOS SETUP UTILITY	
<u>A</u> dvanced	
TCG/TPM Support [ Yes/No] {Note: if set to “No” the reset of this menu is blank, if set to “Yes” then the following TPM set-up parameters appear.}  Execute TPM Command [Don't Change/Disable/Enable] Clearing the TPM [Press Enter] TPM Enable/Disable Status [Enable] TPM Owner Status [Owned]	Enable (Activate)/Disable (Deactivate) command to TPM          ←→ Select Screen ↑↓ Select Item Enter Go to Sub Screen F1 General Help F10 Save and Exit ESC Exit
V02.61 (C)Copyright 1985-2008, American Megatrends, Inc.	

### Trusted Computing (TPM) Set-up BIOS Screen

7. Select “Yes” in the TCG/TPM Support line and “Enabled” in the Execute TPM Command line.
- a. Notes:
    - i. If you press enter while on the Clearing the TPM line the BIOS will ask you if you really want clear the TPM. The following wording will pop up
      1. “Clearing the TPM is the process of returning the TPM to factor defaults. It is possible the platform owner will change when in this state. Are you sure you want to clear it?”
    - ii. If you are unsure of this operation choose the “Cancel” option
  8. Hit F10 on your keyboard to save and exit the TPM/SHB BIOS parameter set –up and boot into the operating system.
  9. For the full TPM implementation the assumption is that the Windows XP or the Windows Vista 32-bit operating system and the EMBASSY Trust Suite software is being used in the application.
  10. Once the O/S is loaded and running, the TPM driver needs to be installed. This driver is a file on the Trenton Driver CD labeled the Atmel TPM Driver Installer 3.0-3.15 executable (.exe) file.
  11. Place the Trenton driver CD into the system and follow the driver installation step menus shown below.





12. Load the NTRU Core TCG Software Stack (CTSS) software. This executable (.exe) file is referred to as the NTRU and is also located in a file on the Trenton Driver CD called NTRU TCG Software Stack Set-Up.
13. Once the TPM driver and the TSS are loaded on the system, the EMBASSY Trust Suite (ETS) 6.1.2 software from Wave Systems Corp. needs to be installed.
14. Load the ETS software and follow the installation instructions.
15. Use the set-up wizards to customize the implementation of TPM on the system.
16. The ETS software is used to set-up virtual drive or vaults for storing encrypted data and protection the system. Migratable and Non Migratable Keys for the vaults can be set up and customized by using the Private Information Manager section of the ETS.
17. A part of the ETS called the EMBASSY Security Center is useful for managing the TPM passwords, setting the mission (i.e. user, guest and administrator privileges) and encrypting and decryption data.
18. The Learn section of the ETS provides a very good overview on all of the features of the ETS and how these features can be utilized in enabling a full implementation of TPM on your system.

**PROCESS STEPS - BASIC TPM IMPLEMENTATION USING MICROSOFT VISTA ULTIMATE – BIT LOCKER**

1. Follow process steps 1 through 8 in the Full TPM Implementation instructions listed on pages 2-2 through 2-3.
2. Boot into the Windows Vista Ultimate O/S to use the Bit Locker feature to implement basic TPM functionality
3. The Bit locker set-up menus can be found in the Control Panel of the O/S
  - a. Bit Locker provides a means to encrypt and decrypt data automatically on a storage device
    - i. Bit Locker Drive Encryption
  - b. Bit Locker provides a means to manage the keys necessary for TPM implementations
    - i. Manage Bit Locker Keys
  - c. When using Bit Locker it is not necessary to load the Atmel TPM Driver Installer 3.0-3.15 executable (.exe) file because this driver is built into the Windows Vista Ultimate operating system
4. Set up the drive encryption and keys using the Bit Locker Drive Encryption and the Manage Bit Locker Keys menus.

*This page intentionally left blank*



## Chapter 3 TPM Application Considerations and Cautions

### TPM DEFAULT SETTINGS

The TPM BIOS default settings are off [TCG/TPM Support = No] and deactivated [TPM Command = Disabled]. The system will not function as a Trusted Computing platform until these system host board BIOS settings are changed.

### DATA BACK UP

Regular system hard drive or other storage media data backup is *absolutely critical* in TPM installations. If the storage device that contains the TPM encrypted data fails, an image of the hard disk can only be restored from the backup in order to gain access to the encrypted data. *Before* encrypting any data in a system using TPM, Trenton Technology strongly recommends backing up *all* critical data. Backing up critical data ensures that the data can be restored in the event of a hardware failure to a critical system component such as the TPM, SHB, or HDD and/or the loss of the TPM password(s) or keys.

### PASSWORDS, MIGRATABLE AND NON-MIGRATABLE KEYS

- If a TPM password is lost there are no TPM password recovery procedures that are available and guaranteed to work 100% of the time. **DO NOT LOSE THE TPM PASSWORD!**
- A special 48-character code is created while implementing TPM that can be used to DEACTIVATE or UNLOCK data in a specific TPM and hardware system implementation. **DO NOT LOSE THIS 48-CHARACTER CODE!**
- Activated encryption keys and codes stay with a specific set of TPM-enabled hardware. Recovery procedures *may* allow migratable TPM access keys to be recovered and *may* be able to restore encrypted data. All non-migratable keys and their associated data will be lost in the event of an SHB failure or replacement. The EMBASSY<sup>®</sup> Trust Suite TPM software from Wave<sup>®</sup> Systems Corp. utilizes some migratable keys.
- TPM ownership and data contents may be cleared to allow transfer of a system to a new owner. If the TPM ownership is cleared without taking the proper precautions, recovery procedures *may* allow recovery of the migratable keys and restoration of access to the encrypted data.
- The CLEAR THE OWNER and CLEAR PRESENCE commands are key to re-working a specific TPM and hardware set up.
- The user must thoroughly understand the functions of the two TPM key types and develop a security plan that governs access to their system's TPM keys. For example a non-migratable key means just that, "the non-migratable TPM key **cannot** be moved or migrated from one platform to another". If a system with a TPM implementation has the TPM itself fail, all non-migratable keys and the data associated with these keys will be inaccessible and unrecoverable.

### TPM CAUTIONS – BIT LOCKER

Data key (i.e. password) storage locations that can be used in TPM applications when the Bit Locker feature of the Vista Ultimate O/S are the TPM itself, a USB storage drive, an unencrypted storage folder on a hard drive, or the key can be sent to a printer to have a hard copy of this 48-character TPM password.

Document where this password is located in the event that you need it to recover the system. **FAILURE TO SECURE AND MAINTAIN THIS PASSWORD KEY WILL RESULT IN A PERMANENT FAILURE OF THE SYSTEM AND/OR AN UNRECOVERABLE LOSS OF ALL ENCRYPTED DATA.**

The 48-character TPM password or key is needed to:

- Gain access to encrypted data
- Recover data from a system after failure and replacement of the TPM itself
- Recover data from a system after failure and replacement of the SHB itself
- Recover data from a system after replacement or upgrade of the SHB's BIOS

**TPM CAUTIONS – EMBASSY TRUST SUITE (ETS)**

Many of the same precautions regarding the password key exist and must be followed when using the ETS software.

The ETS has a feature called the EMBASSY Security Center that allows the password key to be edited and provides a method to encrypt and decrypt the TPM-secured data. Use the EMBASSY Trust Center to set what is called the mission. The Set Mission command is used to decide who has system User, Guest or Administration privileges. Use caution when granting administration privileges to a TPM-enabled system. The Private Implementation Manager is a feature of the ETS that allows the user to create what is called a “Virtual Vault”. This vault is essentially a virtual drive that can store migratable keys and encrypted data. This virtual drive connects the Virtual Vault to the TPM to enhance the storage protection of data and keys.

**TPM CAUTIONS – DATA RECOVERY**

Basic data recover or system access in a TPM-protected system is essentially the same regardless if TPM is implemented using Bit Locker or the ETS software. To gain access to the system or just the encrypted data the TPM password key must be read during system boot-up. If the key is on a media device such a USB jump drive, then this USB drive must be installed while the system is booting up. If the system is booting up and does not see the key a menu will be displayed asking for the password key to be entered. This is why it is extremely critical to secure and maintain the system’s TPM password key. Refer to the ETS help menus for more information on specific data recovery procedures.

## ***Appendix A      References***

Here are a list of reference URLs that can provide more detail on Trusted Computing and TPM implementation:

TRUSTED Computing Group – [www.TrustedComputing.org](http://www.TrustedComputing.org)

EMBASSY Trust Suite software – <http://www.wave.com/products/ets.asp>

Bit Locker – <http://www.microsoft.com/windows/products/windowsvista/features/details/bitlocker.msp>

Atmel - <http://www.atmel.com/products/Embedded/>

**NOTES:**

**NOTES:**