Intel® Trusted Platform Module (TPM module-AXXTPME3) Hardware User's Guide

Intel Order Number: G21682-003

DISCLAIMER

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked “reserved” or “undefined.” Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or go to: http://www.intel.com/design/literature.htm

Intel® is a trademark or registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

*Other names and brands may be claimed as the property of others.

Preface

This is the primary hardware guide for the Intel® Trusted Platform Module (TPM module). It contains installation instructions and specifications.

Audience

The people who benefit from this document are:

- Engineers who are designing an Intel® TPM module.
- Anyone installing an Intel® TPM module in their Intel® server system.

Organization

This document includes the following chapters and appendices:

- Chapter 1 provides a general overview of the Intel® TPM module.
- Chapter 2 describes the procedures for installing the Intel® TPM module.
- Chapter 3 provides the procedures for configuring the Intel® TPM module.
- Chapter 4 provides the characteristics and technical specifications for the Intel® TPM module.
- Appendix A provides safety instructions to be observed during installation and assembly.
- Appendix B provides regulatory and certification information.

Related Publication

This is the primary hardware guide for the Intel® TPM module. It contains installation instructions and specifications.

Table of Contents

List of Figures

List of Tables

1 Overview

The Intel® Trusted Platform Module (TPM) is a hardware-based security device that addresses the growing concern on boot process integrity and offers better data protection. TPM protects the system start-up process by ensuring it is tamper-free before releasing system control to the operating system. A TPM device provides secured storage to store data, such as security keys and passwords. In addition, a TPM device has encryption and hash functions. The Intel® TPM module implements TPM as per TPM PC Client specifications revision 1.2 by the Trusted Computing Group (TCG).

A TPM device is affixed to the motherboard of the server and is secured from external software attacks and physical theft. A pre-boot environment, such as the BIOS and operating system loader, uses the TPM to collect and store unique measurements from multiple factors within the boot process to create a system fingerprint. This unique fingerprint remains the same unless the pre-boot environment is tampered with. Therefore, it is used to compare to future measurements to verify the integrity of the boot process.

After the BIOS complete the measurement of its boot process, it hands off control to the operating system loader and in turn to the operating system. If the operating system is TPM-enabled, it compares the BIOS TPM measurements to those of previous boots to make sure the system was not tampered with before continuing the operating system boot process. Once the operating system is in operation, it optionally uses TPM to provide additional system and data security (for example, Microsoft Vista* supports Bitlocker drive encryption).

The Intel® TPM module is a common board across the series of Intel® servers and baseboards (for a list of supported servers and baseboards, please refer: http://www.intel.com/support/motherboards/server/sb/CS-032301.htm). The TPM module is a small board that provides hardware level security for the server. The TPM module docks into a connector on the baseboard and is retained by a tamper resistant screw.

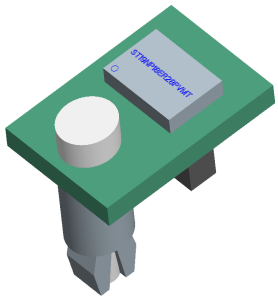


Figure 1. TPM module

2 Intel® Trusted Platform Module Hardware Installation

Requirements

- Intel® Trusted Platform Module , with the provided standoffs
- A host system/board with the TPM connector on the board

The TPM module docks into a connector on the baseboard and is retained by a tamper resistant screw. Below is a drawing of the physical dimension of the TPM module.

Note: *Measurements are in millimeters.*

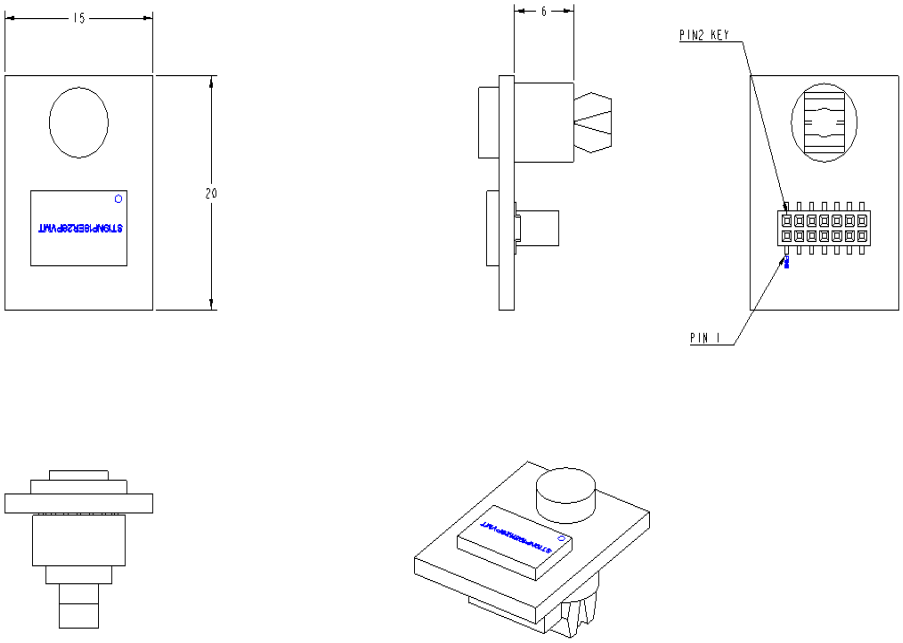


Figure 2. TPM module Dimensioned Drawing

Installing the TPM module

To install the TPM module, follow these steps:

1. Turn off the power to the system, all drives, enclosures, and system components. Remove the power cord(s).
2. Remove the server cover. For instructions, see your server system documentation.
3. Insert the standoff into the hole in the server/workstation board and insert the TPM module connector into the connector in the board. To locate the TPM module connector and the hole on your server/workstation board, see your server/workstation board documentation.
4. Press down gently but firmly to ensure that the module is properly seated in the connectors, and then tighten the tamper resistant screw.

3 Configuring the TPM module

TPM Security BIOS

The BIOS TPM support conforms to the TPM PC Client Specific – Implementation Specification for Conventional BIOS, version 1.2, and to the TPM Interface specification, version 1.2. The BIOS adheres to the Microsoft Vista BitLocker* requirement. The role of the BIOS for TPM security includes the following:

- Measures and stores the boot process in the TPM microcontroller to allow a TPM enabled operating system to verify system boot integrity.
- Produces EFI and legacy interfaces to a TPM-enabled operating system for using TPM.
- Produces ACPI TPM device and methods to allow a TPM-enabled operating system to send TPM administrative command requests to the BIOS.
- Verifies operator physical presence. Confirms and executes operating system TPM administrative command
- Provides BIOS Setup options to change TPM security states and to clear TPM ownership.

For additional details, refer to the TCG PC Client Specific Implementation Specification, the TCG PC Client Specific Physical Presence Interface Specification, and the Microsoft BitLocker* requirement documents.

Physical Presence

Administrative operations to the TPM require TPM ownership or physical presence indication by the operator to confirm the execution of administrative operations. The BIOS implements the operator presence indication by verifying the setup Administrator password.

A TPM administrative sequence invoked from the operating system proceeds as follows:

1. User makes a TPM administrative request through the operating system's security software.
2. The operating system requests the BIOS to execute the TPM administrative command through TPM ACPI methods and then resets the system.
3. The BIOS verifies the physical presence and confirms the command with the operator.
4. The BIOS executes TPM administrative command(s), inhibits BIOS Setup entry and boots directly to the operating system which requested the TPM command(s).

TPM Security Setup Options

The BIOS TPM Setup allows the operator to view the current TPM state and to carry out rudimentary TPM administrative operations. Performing TPM administrative options through the BIOS setup requires TPM physical presence verification.

Using BIOS TPM Setup, the operator can turn ON or OFF TPM functionality and clear the TPM ownership contents. After the requested TPM BIOS Setup operation is carried out, the option reverts to No Operation.

The BIOS TPM Setup also displays the current state of the TPM, whether TPM is enabled or disabled and activated or deactivated. Note that while using TPM, a TPM-enabled operating system or application may change the TPM state independent of the BIOS setup. When an operating system modifies the TPM state, the BIOS Setup displays the updated TPM state.

The BIOS Setup TPM Clear option allows the operator to clear the TPM ownership key and allows the operator to take control of the system with TPM. You use this option to clear security settings for a newly initialized system or to clear a system for which the TPM ownership security key was lost.

Security Screen

The Security screen provides fields to enable and set the user and administrative passwords and to lock out the front panel buttons so they cannot be used. The Intel® server boards support Intel® TPM module.

To access this screen from the Main screen, select the **Security** option.

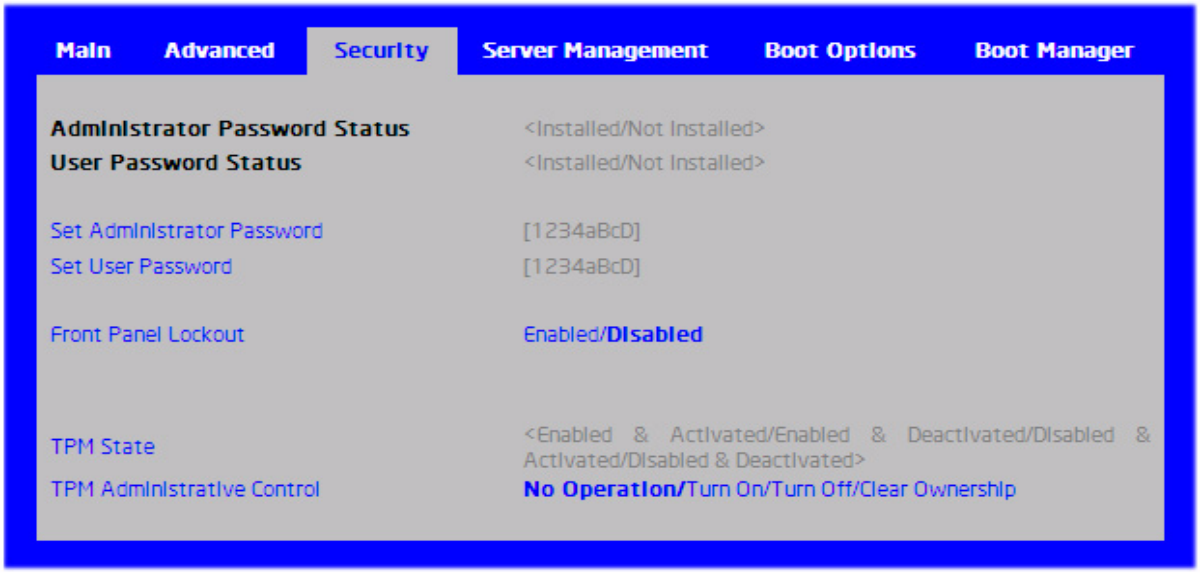


Figure 3. Setup Utility – TPM Configuration Screen

Table 1. TPM Setup Utility – Security Configuration Screen Fields

Setup Item	Options	Help Text	Comments
	• Enabled and Activated • Enabled and Deactivated • Disabled and Activated • Disabled and Deactivated	—	Information only. • Shows the current TPM device state. • A disabled TPM device will not execute commands that use TPM functions and TPM security operations will not be available. • An enabled and deactivated TPM is in the same state as a disabled TPM except setting of TPM ownership is allowed if not present already. • An enabled and activated TPM executes all commands that use TPM functions and TPM security operations will be available.
TPM Administrative Control	• No Operation • Turn On • Turn Off • Clear Ownership	• [No Operation] - No changes to current state. • [Turn On] - Enables and activates TPM. • [Turn Off] - Disables and deactivates TPM. • [Clear Ownership] - Removes the TPM ownership authentication and returns the TPM to a factory default state. ***Note:*** *The BIOS setting returns to [No Operation] on every boot cycle by default.*	

Intel® Trusted Execution Technology (Intel® TXT)

Overview

Intel® Trusted Execution Technology (Intel® TXT) for safer computing, formerly code named LaGrande Technology, is a versatile set of hardware extensions to Intel® processors and chipsets that enhance the platform with security capabilities such as measured launch and protected execution. Intel® TXT provides hardware-based mechanisms that help protect against software-based attacks and protects the confidentiality and integrity of data stored or created on the system. It does this by enabling an environment where applications can run within their own space, protected from all other software on the system. These capabilities provide the protection

mechanisms, rooted in hardware, that are necessary to provide trust in the application's execution environment. In turn, this can help to protect vital data and processes from being compromised by malicious software running on the platform. Long available on client platforms, Intel is now enabling Intel TXT on selected server platforms as well.

Intel® TXT hardware overview

Implementation of a Trusted Execution Technology-enabled platform requires a number of hardware enhancements. Key hardware elements of this platform are:

1. Processor: Extensions to the IA-32 architecture allow for the creation of multiple execution environments, or partitions. This allows for the coexistence of a standard (legacy) partition and protected partition, where software can run in isolation in the protected partition, free from being observed or compromised by other software running on the platform. Access to hardware resources (such as memory) is hardened by enhancements in the processor and chipset hardware. Other processor enhancements include: (1) event handling, to reduce the vulnerability of data exposed through system events, (2) instructions to manage the protected execution environment, (3) and instructions to establish a more secure software stack.
2. Chipset: Extensions to the chipset deliver support for key elements of this new, more protected platform. They include: (1) the capability to enforce memory protection policy, (2) enhancements to protect data access from memory, (3) protected channels to graphics and input/output devices, (4) and interfaces to the Trusted Platform Module [Version 1.2].
3. Keyboard and Mouse: Enhancements to the keyboard and mouse enable communication between these input devices and applications running in a protected partition to take place without being observed or compromised by unauthorized software running on the platform.
4. Graphics: Enhancements to the graphic subsystem enable applications running within a protected partition to send display information to the graphics frame buffer without being observed or compromised by unauthorized software running on the platform.
5. The TPM v. 1.2 device: Also called the Fixed Token, is bound to the platform and connected to the PC's LPC bus. The TPM provides the hardware-based mechanism to store or 'seal' keys and other data to the platform. It also provides the hardware mechanism to report platform attestations.

Note: *For a list of servers and baseboards support Intel® TXT, please refer: http://www.intel.com/support/motherboards/server/sb/CS-032301.htm.*

Enabling Intel® TXT on Intel® Server Board

The following steps describe how to set up Intel® TXT feature:

Intel® TXT Setup:

1. Go to BIOS Setup Menu, **Advanced** > **Processor Configuration,** set **Intel® VT for directed I/O** and **Intel® TXT** option as **Enabled**.
2. Press **F10** to save and exit. Now Intel® TXT is successfully enabled.

Intel® TPM Setup:

1. Enable TPM module: Go to BIOS setup Menu page, Security Tab, set administrator password.
2. After administrator password is setup, press **F10** to save and exit BIOS setup.
3. System will automatically reboot, go to BIOS setup Menu page, **Security** tab, set **TPM Administrative Control** as **Turn ON**, press **F10** to save and exit BIOS setup.
4. Go to BIOS setup Menu, **Security** Tab, TPM State should be **Enabled & Activated**.

4 Intel® Trusted Platform Module Characteristics

TPM module Connector List & Pinouts

The Intel® TPM module connects to the Intel® TPM module connector on the Intel® server board via the iPN FCI 20021321-00014D4LF, or equivalent connector on the server board.

Table 2. TPM module Connector Pin-out

Pin	Name	Pin	Name
	LPC_LAD<1>	2	Key Pin
3	GND	4	LPC_LAD<0>
5	LPC_FRAME_N	6	IRQ_SERIAL
7	GND	8	P3V3
9	CLK_33M_TPM	10	RST_IBMC_NIC_N
11	GND	12	LPC_LAD<3>
13	LPC_LAD<2>	14	GND

Appendix A: Installation/Assembly Safety Instructions

As you use your computer system, observe these safety guidelines:

- Do not operate your computer system with any cover(s) (such as computer covers, bezels, filler brackets, and front-panel inserts) removed.
- To help avoid damaging your computer, be sure the voltage selection switch on the power supply is set to match the alternating current (AC) power available at your location.
- To help avoid possible damage to the server board, wait five seconds after turning off the system before removing a component from the server board or disconnecting a peripheral device from the computer.
- To help prevent electric shock, plug the computer and peripheral power cables into properly grounded power sources. These cables are equipped with 3-prong plugs to ensure proper grounding. Do not use adapter plugs or remove the grounding prong from a cable. If you must use an extension cable, use a 3-wire cable with properly grounded plugs.
- To help protect your computer system from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply.
- Be sure nothing rests on your computer system's cables and that the cables are not located where they can be stepped on or tripped over.
- Do not spill food or liquids on your computer. If the computer gets wet, consult the documentation that came with it.
- Do not push any objects into the openings of your computer. Doing so can cause fire or electric shock by shorting out interior components.
- Keep your computer away from radiators and heat sources. Also, do not block cooling vents. Avoid placing loose papers underneath your computer; do not place your computer in a closed-in wall unit or on a rug.

When working inside your computer:

- Do not attempt to service the computer system yourself, except as explained in this guide and elsewhere in Intel documentation. Always follow installation and service instructions closely.
- Turn off your computer and any peripherals.
- Disconnect your computer and peripherals from their power sources. Also disconnect any telephone or telecommunications lines from the computer.

Doing so reduces the potential for personal injury or shock.

Additional safety guidelines:

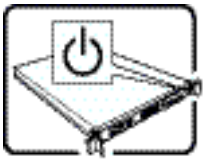
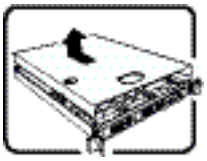
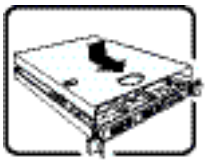
- When you disconnect a cable, pull on its connector or on its strain-relief loop, not on the cable itself. Some cables have a connector with locking tabs; if you are disconnecting this type of cable, press in on the locking tabs before disconnect the cable. As you pull connectors apart, keep them evenly aligned to avoid bending any connector pins. Also, before you connect a cable, make sure both connectors are correctly oriented and aligned.
- Handle components and cards with care. Do not touch the components or contacts on a card. Hold a card by its edges or by its metal mounting bracket. Hold a component such as a microprocessor chip by its edges, not by its pins.

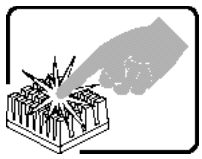
Protecting against electrostatic discharge

- Static electricity can harm delicate components inside your computer. To prevent static damage, discharge static electricity from your body before you touch any of your computer's electronic components, such as the microprocessor. You can do so by touching an unpainted metal surface, such as the metal around the card-slot openings at the back of the computer.
- As you continue to work inside the computer, periodically touch an unpainted metal surface to remove any static charge your body may have accumulated. In addition to the preceding precautions, you can also take the following steps to prevent damage from electrostatic discharge (ESD).
- When unpacking a static-sensitive component from its shipping carton, do not remove the component from the antistatic packing material until you are ready to install the component in your computer. Just before unwrapping the antistatic packaging, be sure to discharge static electricity from your body.
- When transporting a sensitive component, first place it in an antistatic container or packaging.
- Handle all sensitive components in a static-safe area. If possible, use antistatic floor pads and workbench pads.

English

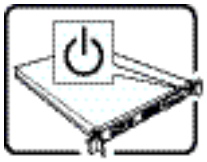
Read all caution and safety statements in this document before performing any of the instructions. See also Intel® *Server Boards and Server Chassis Safety Information* on the Resource CD and/or at http://www.intel.com/support/motherboards/server/sb/cs-010770.htm.

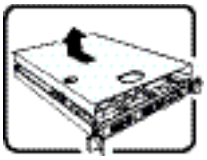
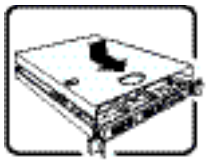
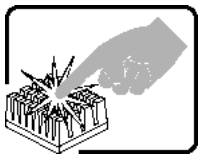
	The power button on the system does not turn off system AC power. To remove AC power from the system, you must unplug each AC power cord from the wall outlet or power supply. The power cord(s) is considered the disconnect device to the main (AC) power. The socket outlet that the system plugs into shall be installed near the equipment and shall be easily accessible.
	**SAFETY STEPS:** Whenever you remove the chassis covers to access the inside of the system, follow these steps: 1. Turn off all peripheral devices connected to the system. 2. Turn off the system by pressing the power button. 3. Unplug all AC power cords from the system or from wall outlets. 4. Label and disconnect all cables connected to I/O connectors or ports on the back of the system. 5. Provide some electrostatic discharge (ESD) protection by wearing an antistatic wrist strap attached to chassis ground of the system-any unpainted metal surface-when handling components. 6. Do not operate the system with the chassis covers removed.
	After you have completed the six SAFETY steps above, you can remove the system covers. To do this: 1. Unlock and remove the padlock from the back of the system if a padlock has been installed. 2. Remove and save all screws from the covers. 3. Remove the cover(s).
	For proper cooling and airflow, always reinstall the chassis covers before turning on the system. Operating the system without the covers in place can damage system parts. To install the covers: 1. Check first to make sure you have not left loose tools or parts inside the system. 2. Check that cables, add-in cards, and other components are properly installed. 3. Attach the covers to the chassis with the screws removed earlier, and tighten them firmly. 4. Insert and lock the padlock to the system to prevent unauthorized access inside the system. 5. Connect all external cables and the AC power cord(s) to the system.

	A microprocessor and heat sink may be hot if the system has been running. Also, there may be sharp pins and edges on some board and chassis parts. Contact should be made with care. Consider wearing protective gloves.

Deutsch

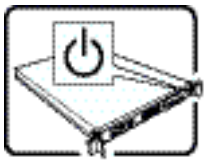
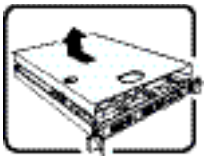
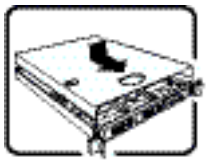
Lesen Sie zunächst sämtliche Warn- und Sicherheitshinweise in diesem Dokument, bevor Sie eine der Anweisungen ausführen. Beachten Sie hierzu auch die *Sicherheitshinweise zu Intel-Serverplatinen und -Servergehäusen* auf der Ressourcen-CD oder unter http://www.intel.com/support/motherboards/server/sb/cs-010770.htm.

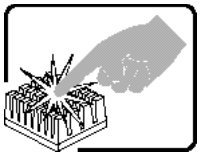
	Der Wechselstrom des Systems wird durch den Ein-/Aus-Schalter für Gleichstrom nicht ausgeschaltet. Ziehen Sie jedes Wechselstrom-Netzkabel aus der Steckdose bzw. dem Netzgerät, um den Stromanschluß des Systems zu unterbrechen. Die Stromkabel sind das "Unterbrechungsgerät" zur Hauptstromquelle. Die Steckdose, in die das System gesteckt wird, sollte sich in der Nähe des Gerätes befinden und leicht zugänglich sein.
	SICHERHEITSMASSNAHMEN: Immer wenn Sie die Gehäuseabdeckung abnehmen um an das Systeminnere zu gelangen, sollten Sie folgende Schritte beachten: 1. Schalten Sie alle an Ihr System angeschlossenen Peripheriegeräte aus. 2. Schalten Sie das System mit dem Hauptschalter aus. 3. Ziehen Sie den Stromanschlußstecker Ihres Systems aus der Steckdose. 4. Auf der Rückseite des Systems beschriften und ziehen Sie alle Anschlußkabel von den I/O Anschlüssen oder Ports ab. 5. Tragen Sie ein geerdetes Antistatik Gelenkband, um elektrostatische Ladungen (ESD) über blanke Metallstellen bei der Handhabung der Komponenten zu vermeiden. 6. Schalten Sie das System niemals ohne ordnungsgemäß montiertes Gehäuse ein.

	SICHERHEITSMASSNAHMEN: Immer wenn Sie die Gehäuseabdeckung abnehmen um an das Systeminnere zu gelangen, sollten Sie folgende Schritte beachten: 1. Schalten Sie alle an Ihr System angeschlossenen Peripheriegeräte aus. 2. Schalten Sie das System mit dem Hauptschalter aus. 3. Ziehen Sie den Stromanschlußstecker Ihres Systems aus der Steckdose. 4. Auf der Rückseite des Systems beschriften und ziehen Sie alle Anschlußkabel von den I/O Anschlüssen oder Ports ab. 5. Tragen Sie ein geerdetes Antistatik Gelenkband, um elektrostatische Ladungen (ESD) über blanke Metallstellen bei der Handhabung der Komponenten zu vermeiden. 6. Schalten Sie das System niemals ohne ordnungsgemäß montiertes Gehäuse ein.
	Zur ordnungsgemäßen Kühlung und Lüftung muß die Gehäuseabdeckung immer wieder vor dem Einschalten installiert werden. Ein Betrieb des Systems ohne angebrachte Abdeckung kann Ihrem System oder Teile darin beschädigen. Um die Abdeckung wieder anzubringen: 1. Vergewissern Sie sich, daß Sie keine Werkzeuge oder Teile im Innern des Systems zurückgelassen haben. 2. Überprüfen Sie alle Kabel, Zusatzkarten und andere Komponenten auf ordnungsgemäßen Sitz und Installation. 3. Bringen Sie die Abdeckungen wieder am Gehäuse an, indem Sie die zuvor gelösten Schrauben wieder anbringen. Ziehen Sie diese gut an. 4. Bringen Sie die Verschlußeinrichtung (Padlock) wieder an und schließen Sie diese, um ein unerlaubtes Öffnen des Systems zu verhindern. 5. Schließen Sie alle externen Kabel und den AC Stromanschlußstecker Ihres Systems wieder an.
	Der Mikroprozessor und der Kühler sind möglicherweise erhitzt, wenn das System in Betrieb ist. Außerdem können einige Platinen und Gehäuseteile scharfe Spitzen und Kanten aufweisen. Arbeiten an Platinen und Gehäuse sollten vorsichtig ausgeführt werden. Sie sollten Schutzhandschuhe tragen.

Français

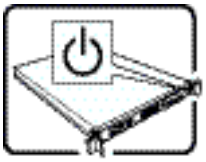
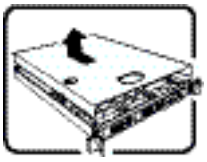
Lisez attention toutes les consignes de sécurité et les mises en garde indiquées dans ce document avant de suivre toute instruction. Consultez *Intel® Server Boards and Server Chassis Safety Information* sur le CD Resource CD ou bien rendez-vous sur le site http://www.intel.com/support/motherboards/server/sb/cs-010770.htm.

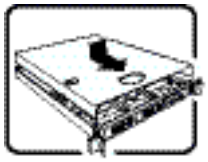
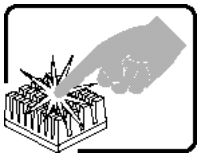
	Notez que le commutateur CC de mise sous tension /hors tension du panneau avant n'éteint pas l'alimentation CA du système. Pour mettre le système hors tension, vous devez débrancher chaque câble d'alimentation de sa prise. C'est le câble d'alimentation qui est considéré comme le moyen de se déconnecter du CA. La prise à laquelle le système est branché doit se situer à proximité de l'équipement et être facilement accessible.
	CONSIGNES DE SÉCURITÉ -Lorsque vous ouvrez le boîtier pour accéder à l'intérieur du système, suivez les consignes suivantes: 1. Mettez hors tension tous les périphériques connectés au système. 2. Mettez le système hors tension en mettant l'interrupteur général en position OFF (bouton-poussoir). 3. Débranchez tous les cordons d'alimentation c.a. du système et des prises murales. 4. Identifiez et débranchez tous les câbles reliés aux connecteurs d'E-S ou aux accès derrière le système. 5. Pour prévenir les décharges électrostatiques lorsque vous touchez aux composants, portez une bande antistatique pour poignet et reliez-la à la masse du système (toute surface métallique non peinte du boîtier). 6. Ne faites pas fonctionner le système tandis que le boîtier est ouvert.
	Une fois TOUTES les étapes précédentes accomplies, vous pouvez retirer les panneaux du système. Procédez comme suit: 1. Si un cadenas a été installé sur à l'arrière du système, déverrouillez-le et retirez-le. 2. Retirez toutes les vis des panneaux et mettez-les dans un endroit sûr. 3. Retirez les panneaux.
	Afin de permettre le refroidissement et l'aération du système, réinstallez toujours les panneaux du boîtier avant de mettre le système sous tension. Le fonctionnement du système en l'absence des panneaux risque d'endommager ses pièces. Pour installer les panneaux, procédez comme suit: 1. Assurez-vous de ne pas avoir oublié d'outils ou de pièces démontées dans le système. 2. Assurez-vous que les câbles, les cartes d'extension et les autres composants sont bien installés. 3. Revissez solidement les panneaux du boîtier avec les vis retirées plus tôt. 4. Remettez le cadenas en place et verrouillez-le afin de prévenir tout accès non autorisé à l'intérieur du système. 5. Rebranchez tous les cordons d'alimentation c. a. et câbles externes au système.

	Le microprocesseur et le dissipateur de chaleur peuvent être chauds si le système a été sous tension. Faites également attention aux broches aiguës des cartes et aux bords tranchants du capot. Nous vous recommandons l'usage de gants de protection.

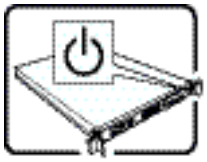
Español

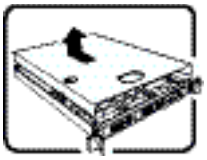
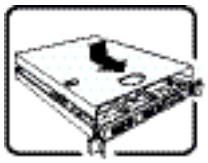
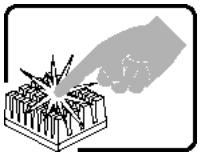
Lea todas las declaraciones de seguridad y precaucion de este documento antes de realizar cualquiera de las instrucciones. Vea Intel® *Server Boards and Server Chassis Safety Information* en el CD Resource y/o en http://www.intel.com/support/motherboards/server/sb/cs-010770.htm.

	Nótese que el interruptor activado/desactivado en el panel frontal no desconecta la corriente alterna del sistema. Para desconectarla, deberá desenchufar todos los cables de corriente alterna de la pared o desconectar la fuente de alimentación. Estos cables actúan como dispositivo de desconexión. La toma de corriente deberá estar situada cerca del equipo y ser de fácil acceso.
	INSTRUCCIONES DE SEGURIDAD: Cuando extraiga la tapa del chasis para acceder al interior del sistema, siga las siguientes instrucciones: 1. Apague todos los dispositivos periféricos conectados al sistema. 2. Apague el sistema presionando el interruptor encendido/apagado. 3. Desconecte todos los cables de alimentación CA del sistema o de las tomas de corriente alterna. 4. Identifique y desconecte todos los cables enchufados a los conectores E/S o a los puertos situados en la parte posterior del sistema. 5. Cuando manipule los componentes, es importante protegerse contra la descarga electrostática (ESD). Puede hacerlo si utiliza una muñequera antiestática sujetada a la toma de tierra del chasis - o a cualquier tipo de superficie de metal sin pintar. 6. No ponga en marcha el sistema si se han extraído las tapas del chasis.
	Después de completar las seis instrucciones de SEGURIDAD mencionadas, ya puede extraer las tapas del sistema. Para ello: 1. Desbloquee y extraiga el bloqueo de seguridad de la parte posterior del sistema, si se ha instalado uno. 2. Extraiga y guarde todos los tornillos de las tapas.Extraiga las tapas.

	Para obtener un enfriamiento y un flujo de aire adecuados, reinstale siempre las tapas del chasis antes de poner en marcha el sistema. Si pone en funcionamiento el sistema sin las tapas bien colocadas puede dañar los componentes del sistema. Para instalar las tapas: 1. Asegúrese primero de no haber dejado herramientas o componentes sueltos dentro del sistema. 2. Compruebe que los cables, las placas adicionales y otros componentes se hayan instalado correctamente. 3. Incorpore las tapas al chasis mediante los tornillos extraídos anteriormente, tensándolos firmemente. 4. Inserte el bloqueo de seguridad en el sistema y bloquéelo para impedir que pueda accederse al mismo sin autorización. 5. Conecte todos los cables externos y los cables de alimentación CA al sistema.
	Si el sistema ha estado en funcionamiento, el microprocesador y el disipador de calor pueden estar aún calientes. También conviene tener en cuenta que en el chasis o en el tablero puede haber piezas cortantes o punzantes. Por ello, se recomienda precaución y el uso de guantes protectores.

Italiano

	L'interruttore attivato/disattivato nel pannello anteriore non interrompe l'alimentazione in c.a. del sistema. Per interromperla, è necessario scollegare tutti i cavi di alimentazione in c.a. dalle prese a muro o dall'alimentazione di corrente. Il cavo è considerato il dispositivo d'interruzione dell'alimentazione principale (in c.a.). La presa alla quale si collega il sistema deve essere installata vicino all'unità e deve essere facilmente accessibile.

	PASSI DI SICUREZZA: Qualora si rimuovano le coperture del telaio per accedere all'interno del sistema, seguire i seguenti passi: 1. Spegnere tutti i dispositivi periferici collegati al sistema. 2. Spegnere il sistema, usando il pulsante spento/acceso dell'interruttore del sistema. 3. Togliere tutte le spine dei cavi del sistema dalle prese elettriche. 4. Identificare e sconnettere tutti i cavi attaccati ai collegamenti I/O od alle prese installate sul retro del sistema. 5. Qualora si tocchino i componenti, proteggersi dallo scarico elettrostatico (SES), portando un cinghia anti-statica da polso che è attaccata alla presa a terra del telaio del sistema - qualsiasi superficie non dipinta - . 6. Non far operare il sistema quando il telaio è senza le coperture.
	Dopo aver seguito i sei passi di SICUREZZA sopracitati, togliere le coperture del telaio del sistema come seque: 1. Aprire e rimuovere il lucchetto dal retro del sistema qualora ve ne fosse uno installato. 2. Togliere e mettere in un posto sicuro tutte le viti delle coperture. 3. Togliere le coperture.
	Per il giusto flusso dell'aria e raffreddamento del sistema, rimettere sempre le coperture del telaio prima di riaccendere il sistema. Operare il sistema senza le coperture al loro proprio posto potrebbe danneggiare i componenti del sistema. Per rimettere le coperture del telaio: 1. Controllare prima che non si siano lasciati degli attrezzi o dei componenti dentro il sistema. 2. Controllare che i cavi, dei supporti aggiuntivi ed altri componenti siano stati installati appropriatamente. 3. Attaccare le coperture al telaio con le viti tolte in precedenza e avvitarle strettamente. 4. Inserire e chiudere a chiave il lucchetto sul retro del sistema per impedire l'accesso non autorizzato al sistema. 5. Ricollegare tutti i cavi esterni e le prolunghe AC del sistema.
	Se il sistema è stato a lungo in funzione, il microprocessore e il dissipatore di calore potrebbero essere surriscaldati. Fare attenzione alla presenza di piedini appuntiti e parti taglienti sulle schede e sul telaio. È consigliabile l'uso di guanti di protezione.

Appendix B: Regulatory and Certification Information

Product Safety and EMC Compliance

This Intel® TPM module has been evaluated for regulatory compliance as an Intel end system, and is included as part of the end system certification. For information on end system certification, refer to the product regulatory certification for the end system level product.