Overview

HP Trusted Platform Module Options

The HP TPM (Trusted Platform Module) is a HP designed security solution, which has a TPM chip within it. The HP TPM solution is designed to make it evident if there are attempts to remove an installed module.

The TPM chip is a microcontroller chip which conforms to Trusted Computing Group specifications to securely store artifacts used to authenticate the server platform. These artifacts can include passwords, certificates and encryption keys. The TPM works with Microsoft Windows® BitLocker™ which is a data protection feature available in Microsoft Windows Server® 2008 R2 SP1 and later operating systems. BitLocker helps protect user data and helps ensure that a server running Windows Server has not been tampered with while the system was offline. Operating Systems like Windows Server® 2008 R2 SP1 and later, with BitLocker leverage the enhanced security capabilities of the TPM.

The HP TPM solutions come in two variants – the new HP Trusted Platform Module 2.0 Option and the earlier HP Trusted Platform Module Option (the TPM 1.2 version).

Compatibility

The new HP Trusted Platform Module 2.0 Option is supported by Microsoft Windows Server® 2012 and later. The HP Trusted Platform Module 2.0 Option works with HPE ProLiant Gen9 servers with UEFI Mode (as versus Legacy Mode).

The HP Trusted Platform Module Option (the TPM 1.2 version) is compatible with both HPE ProLiant Gen8 and HPE Gen9 servers.

Hewlett Packard Enterprise Gen9 servers purchased earlier require a minimum BIOS firmware revision of 2.00 to support the TPM 2.0 Option.

TPM modules are unique to a server

Hewlett Packard Enterprise server systems can have a TPM module (of any type) installed only once. It cannot be replaced with any other TPM module.

What's New

- HP Trusted Platform Module 2.0 Option

Models

HP Trusted Platform Module 2.0 Kit 745823-B21

NOTE: TPM 2.0 version. Compatible server platforms include all HPE Gen9 servers.

HP Trusted Platform Module Option 488069-B21

NOTE: This HP Trusted Platform Module Option (488069-B21) is the TPM 1.2 version. Compatible server platforms include Gen8 and Gen9 servers.

Standard Features

TPM standards	HP Trusted Platform Module 2.0 Option: The TPM chip within the module complies with Trusted Computing Group specification version 2.0 revision 116. The TPM chip (which is part of the HP designed module) has a Common Criteria certification level of EAL4+. HP Trusted Platform Module Option: The TPM chip within the module complies with the Trusted Computing Group specification version 1.2 revision 103. The TPM chip (which is part of the HP designed module) has a Common Criteria certification level of EAL4+.
Supported Operating Systems	The HP Trusted Platform Module 2.0 Option is designed to be used with Microsoft Windows Server® 2012 and Microsoft Windows Server® 2012 R2. The HP Trusted Platform Module Option is designed to be used with Microsoft Windows Server® 2008 R2 SP1, Microsoft Windows Server® 2012, and Microsoft Windows Server® 2012 R2.
Supported HPE BIOS	The HP Trusted Platform Module 2.0 Option requires a minimum Gen9 server BIOS of 2.00 the latest available BIOS be installed before installing the HP Trusted Platform Module 2.0 Option Kit. The HP Trusted Platform Module 2.0 Option is only supported in UEFI mode (as versus Legacy Mode) The TPM 1.2 version, the HP Trusted Platform Module Option is supported by HPE Gen8 and HPE Gen9 supported servers in either UEFI or Legacy modes.
Support Matrix	The HP Trusted Platform Module Options are designed to be installed onto the vacant TPM connector on supported servers. Once installed, the TPM module becomes a permanent part of the system board. It is not designed to be removed. The HP Trusted Platform Module 2.0 Option is available for supported HPE Gen9 servers. The TPM 1.2 version, the HP Trusted Platform Module is available for supported HPE Gen8 and HPE Gen9 servers. Please see the following URL for the latest list of supported servers and enclosures: **http://www.hp.com/go/proliantoptions**
Warranty	The HP Trusted Platform Module (which is the TPM 1.2 version module) and HP Trusted Platform Module 2.0 Option have a 3 year limited warranty regardless of the warranty period for the system in which they are installed.

Service and Support

Service and Support	**HPE Technology Services for Industry Standard Servers and BladeSystem** HPE Technology Services delivers confidence, reduces risk and helps customers realize agility and stability. Connect to Hewlett Packard Enterprise to help prevent problems and solve issues faster. Our support technology lets you to tap into the knowledge of millions of devices and thousands of experts to stay informed and in control, anywhere, any time. **Protect your business beyond warranty with HPE Care Pack Services** HPE Care Pack Services enable you to order the right service level, length of coverage and response time as you purchase your new server, giving you full entitlement for the term you select.
Connect your devices to HPE	Unlock all of the benefits of your technology investment by connecting your products to Hewlett Packard Enterprise. Achieve up to 77% reduction in down time, near 100% diagnostic accuracy and a single consolidated view of your environment. By connecting, you will receive 24x7monitoring, pre-failure alerts, automatic call logging, and automatic parts dispatch. HPE Proactive Care Service and HPE Datacenter Care Service customers will also benefit from proactive activities to help prevent issues and increase optimization. All of these benefits are already available to you with your server storage and networking products, securely connected to Hewlett Packard Enterprise support.
Service Coverage	For ProLiant servers and storage systems, the service on the main product covers Hewlett Packard Enterprise-branded hardware options not designated by Hewlett Packard Enterprise as requiring separate coverage that are qualified for the server, are purchased at the same time or afterward, and are internal to the enclosure. The service also covers external monitors up to 22 inches in size and tower UPS products during their supported life of up to 5 years beyond sales discontinuance. These items will be covered at the same service level as the main product.
For more information	To learn more on services for HPE ESSN Options, please contact your Hewlett Packard Enterprise sales representative or Hewlett Packard Enterprise Authorized Channel Partner. Or visit: **http://www.hp.com/services/proliant** or **http://www.hp.com/services/bladesystem**

Technical Specifications

Environment-friendly Products and Approach	**End-of-life Management and Recycling**	Hewlett Packard Enterprise offers end-of-life Hewlett Packard Enterprise product return, trade-in, and recycling programs in many geographic areas. For trade-in information, please go to **http://www.hp.com/go/green**. To recycle your product, please go to: **http://www.hp.com/go/green** or contact your nearest Hewlett Packard Enterprise sales office. Products returned to Hewlett Packard Enterprise will be recycled, recovered or disposed of in a responsible manner. The EU WEEE directive (2002/95/EC) requires manufacturers to provide treatment information for each product type for use by treatment facilities. This information (product disassembly instructions) is posted on the Hewlett Packard Enterprise web site at: **http://www.hp.com/go/green**. These instructions may be used by recyclers and other WEEE treatment facilities as well as Hewlett Packard Enterprise OEM customers who integrate and re-sell Hewlett Packard Enterprise equipment.

Summary of Changes

Date	Version History	Action	Description of Change
10-Jun-2016	From Version 1 to 2	Changed	Changes made throughout the QuickSpecs.

Sign up for updates

c04939549 - 15556 - Worldwide - V2 - 10-June-2016