Overview

Trusted Platform Module Options

The HPE Trusted Platform Module (TPM) works with programs such as Microsoft Windows® BitLocker™ to increase data security by storing the encryption startup key in hardware on the server, which provides a more secure environment by pairing the drive to the server. Pairing the drive to the server helps prevent the encrypted drive from being read if inserted in a different server. The HPE TPM can also store passwords, certificates, and encryption keys that can authenticate server hardware and software through remote assentation while the measured boot capability enhances the effectiveness of anti-malware solutions.

The HPE TPM options conform to the Trusted Computing Group specifications and provides hardware-based authentication and tamper detection preventing a TPM from being moved to another server or replaced.

Models

HPE Trusted Platform Module 2.0 Gen10 Option 864279-B21

Compatible with HPE Gen10 servers running Microsoft Windows Server® 2012 R2 or newer. Supports TPM 1.2 (UEFI and Legacy mode) and 2.0 (UEFI mode).

HPE Trusted Platform Module 2.0 Kit 745823-B21

Compatible with HPE Gen9 servers in UEFI mode running Microsoft Windows Server® 2012 or newer. Supports TPM 2.0 only.

HPE Trusted Platform Module Option 488069-B21

Compatible with HPE Gen8 and Gen9 servers running Microsoft Windows Server® 2008 R2 SP1 or newer. Supports TPM 1.2 only.

Standard Features

TPM Standards	HPE Trusted Platform Module 2.0 for Gen10: The chip within the module complies with the Trusted Computing Group specification for version 2.0 revision 1.16 (default) and version 1.2 revision 1.16, and meets Common Criteria certification level EAL4+. HPE Trusted Platform Module 2.0: The chip within the module complies with the Trusted Computing Group specification for version 2.0 revision 1.16 and meets Common Criteria certification level EAL4+. HPE Trusted Platform Module: 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 HPE designed module) has a Common Criteria certification level of EAL4+.
Supported Operating Systems	The HPE Trusted Platform Module 2.0 for Gen10 requires Microsoft Windows Server® 2012 R2 or newer. The HPE Trusted Platform Module 2.0 requires Microsoft Windows Server® 2012 or Microsoft Windows Server® 2012 R2. The HPE Trusted Platform Module requires Microsoft Windows Server® 2008 R2 SP1, Microsoft Windows Server® 2012, and Microsoft Windows Server® 2012 R2.
Supported HPE BIOS	The HPE Trusted Platform Module 2.0 for Gen10 is compatible with HPE Gen10 servers only. The HPE Trusted Platform Module 2.0 requires a minimum Gen9 server BIOS of 2.00 (the latest available BIOS is recommended) be installed before installing the HPE Trusted Platform Module 2.0 Option Kit. TPM 2.0 is supported in UEF mode. TPM 1.2 mode is supported in UEFI and Legacy modes. The HPE Trusted Platform Module 2.0 is supported in UEFI mode only and is not supported in Legacy Mode. The HPE Trusted Platform Module (TPM 1.2 version) is supported by HPE Gen8 and HPE Gen9 supported servers in either UEFI or Legacy modes.
Support Matrix	The 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 HPE Trusted Platform Module 2.0 for Gen10 is compatible with supported HPE Gen10 servers only. The HPE Trusted Platform Module 2.0 Option is available for supported HPE Gen9 servers. The TPM 1.2 version, the HPE 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.hpe.com/info/serveroptions**
Warranty	The HPE Trusted Platform Module and the HPE Trusted Platform Modules 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.hpe.com/services**

Technical Specifications

Environment-friendly Products and Approach

End-of-life Management and Recycling

Hewlett Packard Enterprise offers end-of-life product return, trade-in, and recycling programs, in many geographic areas, for our products. Products returned to Hewlett Packard Enterprise will be recycled, recovered or disposed of in a responsible manner.

http://www.hpe.com/recycle

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. 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.

http://www.hpe.com/recycle

Summary of Changes

Date	Version History	Action	Description of Change
11-Jul-2017	From Version 2 to 3	Changed	Overview and Standard Features were revised.
10-Jun-2016	From Version 1 to 2	Changed	Changes made throughout the QuickSpecs.

Sign up for updates

c04939549 - 15556 - Worldwide - V3 - 11-July-2017