



# Hewlett Packard Enterprise



## Interoperable

- Supports OASIS KMIP, NIST, and existing Hewlett Packard Enterprise standards
- Supports a growing range of Hewlett Packard Enterprise tape, disk, network, cloud, and partner data protection products and solutions
- Upgradeable to new software releases
- HPE ArcSight FlexConnector for ESKM is available

## Secure

- Hardened server appliance designed as a FIPS 140-2 Level 2 cryptographic module
- All software is included, preinstalled, digitally signed, and verified at startup
- Keys are always encrypted at rest and in motion; SSL/TLS encrypted communications for secure key management
- Strong mutual certificate authentication available for access to encryption keys
- Local Certificate Authority is included

## Scalable

- Clusters span and serve multiple data centers, locations, and regions
- Supports tens of thousands of key-using clients and millions of keys

## Reliable

- High-availability clustering, 2–8 nodes
- Performs automatic key replication, client load-balancing, and failover
- Fault-tolerant hardware with mirrored internal disks, dual power supplies, dual network ports, and redundant cooling

## Manageable

- Secure remote administrator access, easy to designate roles and privileges
- Scheduled backups and log rotations
- SNMP alerts and SIEM log monitoring

# HPE Enterprise Secure Key Manager 4.0

## Manage business-critical encryption keys for OASIS KMIP clients

### Enterprise data protection

#### Protecting sensitive information with data encryption

Organizations across all industry and public sectors are increasingly challenged to protect their sensitive information (cardholder data, patient records, personal identifying information, and intellectual property) from threats like unauthorized insider access, accidental disclosure, and theft by a range of hostile outsiders.

Auditors, regulators, and industry compliance mandates often require encryption of sensitive data-at-rest as a minimum standard of care and security best practice. When sensitive data at rest is encrypted, the risks of audit failures, financial losses, and damage to an organization's reputation are significantly reduced.

#### Key management is essential

When encryption is used to protect data at rest, strong key management practices with policy enforcement are needed to manage, protect, serve, and preserve underlying encryption keys over the life of the data. If encryption keys are compromised, data is compromised. If encryption keys are lost, data is lost and business continuity is impacted. Finally, if an organization cannot prove that data and keys were managed and protected under stated policies, it may fail compliance audits.

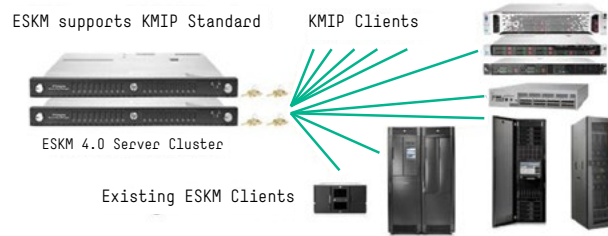
### Product overview

HPE Enterprise Secure Key Manager (ESKM) provides a complete solution for unifying and automating an organization's encryption controls by securely creating, protecting, serving, controlling, and auditing access to encryption keys for secure key management.

Enterprise Secure Key Manager (ESKM) now supports the OASIS Key Management Interoperability Protocol (KMIP) version 1.0, 1.1, and 1.2 clients, enabling the broadest range of data protection products, partners, and solutions. A client-side Software Developer Kit (SDK) is also available to Hewlett Packard Enterprise Partners and customers to enable native ESKM client integrations.

ESKM is designed as a fully integrated solution: an independent lab-validated secure server appliance. Standard capabilities include high availability clustering and failover, secure key database, key generation and retrieval services, identity and access management for administrators and encryption devices, secure backup and recovery, a local Certificate Authority, and strong audit logging for compliance validation.

## HPE Enterprise Secure Key Manager version 4.0



### ESKM HIGH-AVAILABILITY CLUSTER WITH ENROLLED CLIENT SYSTEMS

#### Software

##### Unified, secure, scalable encryption key management services

- Automate and enforce organizational data protection and compliance policies
- Secure key generation, retrieval, access, and auditing for enrolled clients
- Supports multiple key types, use cases, key-using client devices and applications
- Capacity for >2 million keys, >25,000 clients, and eight HPE ESKM nodes per distributed cluster

##### Strong auditable security

- Security hardened Linux®-based server appliance; all software is included and digitally signed
- All keys and backups are encrypted both at rest and in motion
- Granular control of key access to key owners and across administrator defined key-sharing groups
- Certificate-based mutual client-server authentication, secure administration, and audit logging
- ESKM 4.0 is designed to FIPS 140-2 Level 2 requirements, validation pending
- Locking front bezel, dual pick-resistant locks for security officer dual control

##### Reliable continuous access to business-critical encryption keys

- Supports mirrored storage internal, dual networks, dual power, and redundant cooling
- Native multisite high-availability clustering, encryption keys replicated securely and transparently to all nodes
- Comprehensive monitoring, recovery, scheduled backup, and restore functionality

##### Management

- Web browser GUI and Command Line Interface supported
- SSL/TLS and SSH for secure administrator remote access
- Terminal interface (serial RS-232C) for initial installation setup

#### Cryptography and security

Supports (in FIPS mode) AES (128, 192, 256), 3-key Triple DES, HMAC, and RSA (2048/3072/4096) key types  
Designed for NIST SP 800-131A and FIPS 140-2 Level 2 requirements

#### Physical characteristics and ports

Full configuration weight 36.4 lb (16.5 kg)  
Overall dimensions 31.3 (d) x 19.0 (w) x 1.7 (h) in. (79.5 x 48.3 x 4.32 cm)  
1U rack mount; dual locking front bezel, FIPS Level 2 physical security, and rack mount rail kit included  
2 autosensing 10/100/1000BASE-T (Ethernet) RJ-45 ports  
1 RS-232C serial console port, 1 video port

#### Processor, memory, and disk

Processor: 6-core Intel® Xeon® Processor E5-2640 @2.5 GHz  
Memory: 16 GB DDR3 DIMM; 15 MB L3 Cache  
Disk controller: HPE Smart Array, 1 GB flash-backed write cache  
Disk: Dual RAID-1 (mirror) SFF 300 Gb 15k rpm SAS disk drives  
Cooling: 6-fan variable-speed redundant cooling

#### Environment

Operating temperature 50°F to 95°F (10°C to 35°C) at sea level  
Altitude up to 10,000 ft. (3050 m) with a derating of maximum operating temperature of 1.0°C per 305 m (1.8°F per every 1000 ft.) above sea level; no direct sustained sunlight  
Operating relative humidity 10% to 90%, 82.4°F (28°C) maximum wet bulb temperature, noncondensing  
Non-operating/Storage temperature -22°F to 140°F (-30°C to 60°C); maximum change 20°C/hr (36°F/hr)  
Non-operating/Storage relative humidity 5% to 95%, 101.7°F (38.7°C) maximum wet bulb, noncondensing

#### Electrical and thermal characteristics

Maximum heat dissipation 290 BTU/hr (305.95 kJ/hr);  
Voltage 100–240 VAC auto-ranging, Frequency 50/60 Hz; Idle power 85 W, Maximum power 135 W  
**Note:** Idle power is the actual power consumption of the device with no ports connected or active.  
Each HPE Enterprise Security Key Manager (ESKM) node ships with dual redundant power supplies and two (2) IEC C13 to C14 power cords intended for rack mounting with dual PDUs and UPS for highest availability. HPE ESKM nodes may also be powered using two (2) regional power cords connecting to receptacles on separate branch circuits for highest availability.

## Ordering options for ESKM 4.0 software and servers



### ESKM 3.x to 4.0 Upgrade Kit and single node server LTU C8Z65AA

Software upgrade kit and LTU for one ESKM server. Installs version 4.0 software on existing ESKM 3.0 or 3.1 hardware.



### ESKM 4.0 single node server C8Z61AA

One ESKM 4.0 server node. Includes all hardware, accessories, preinstalled software, and documentation. Production clusters should be configured with a minimum of 2 and maximum of 8 nodes. Single nodes are suitable for ESKM test and development environments, and for expansion of production clusters.

<b>Prerequisites and limitations</b>	Requires verification of prior ESKM 3.0 or 3.1 server purchase and a current ESKM support agreement.	None. Single nodes are recommended only for ESKM test and development environments, and for expansion of production clusters.												
<b>Hardware</b>	Includes a mirror pair of disk drives pre-imaged with ESKM 4.0 software.	Single node ESKM server. Includes two power supplies and IEC-IEC power cords, null modem serial cable, 1U rack mounting hardware kit, and two sets of keys to the locking bezel.												
<b>Documentation</b>	Includes "Read Me First" card and document CD with user guide, installation guide, and release notes.	Includes "Read Me First" card and document CD with user guide, installation guide, and release notes.												
<b>Software</b>	ESKM 4.0 software is included and pre-installed on disks. Software upgrades to ESKM version 4.x are available free via electronic software delivery for each unit under a current Hewlett Packard Enterprise support contract.	ESKM 4.0 software is included and pre-installed on server node. Software upgrades to ESKM version 4.x are available free via electronic software delivery for each unit under a current Hewlett Packard Enterprise support contract.												
<b>Server LTU</b>	Includes ESKM 4.0 software LTU for one existing single server node.	Includes ESKM 4.0 software LTU for a single server node.												
<b>Client LTU</b>	Existing ESKM client licenses are preserved. Additional clients require additional client licenses, which may be purchased in any desired quantity (see table below).	Each ESKM 4.0 single node server includes one preinstalled ESKM client license. Additional clients require additional client licenses, which may be purchased in any desired quantity (see table below).												
	<table border="1"> <thead> <tr> <th>Order item#</th> <th>Client license item description</th> </tr> </thead> <tbody> <tr> <td>C8Z40AAE</td> <td>HPE ESKM 1-9 Per Client E-LTU</td> </tr> <tr> <td>C8Z41AAE</td> <td>HPE ESKM 10-24 Per Client E-LTU</td> </tr> <tr> <td>C8Z42AAE</td> <td>HPE ESKM 25-49 Per Client E-LTU</td> </tr> <tr> <td>C8Z43AAE</td> <td>HPE ESKM 50+ Per Client E-LTU</td> </tr> <tr> <td>C9B52AAE</td> <td>HPE ESKM Per HPE ProLiant Client E-LTU</td> </tr> </tbody> </table>	Order item#	Client license item description	C8Z40AAE	HPE ESKM 1-9 Per Client E-LTU	C8Z41AAE	HPE ESKM 10-24 Per Client E-LTU	C8Z42AAE	HPE ESKM 25-49 Per Client E-LTU	C8Z43AAE	HPE ESKM 50+ Per Client E-LTU	C9B52AAE	HPE ESKM Per HPE ProLiant Client E-LTU	
Order item#	Client license item description													
C8Z40AAE	HPE ESKM 1-9 Per Client E-LTU													
C8Z41AAE	HPE ESKM 10-24 Per Client E-LTU													
C8Z42AAE	HPE ESKM 25-49 Per Client E-LTU													
C8Z43AAE	HPE ESKM 50+ Per Client E-LTU													
C9B52AAE	HPE ESKM Per HPE ProLiant Client E-LTU													
<b>Support services</b>	ESKM server node to be upgraded must be covered under an existing support agreement.	Support services must be ordered at the same time as a single node ESKM server order.												
<b>Installation services</b>	ESKM installation or startup, upgrade, migration, and training services are available. Please contact your Hewlett Packard Enterprise sales representative or reseller.	ESKM installation/startup, upgrade, migration, and training services are available. Please contact your Hewlett Packard Enterprise sales representative or reseller.												



ESKM versions 3.0 and 3.1 are FIPS 140-2 Level 2 validated, FIPS certificate #1922, and ESKM 4.0 validation is pending.

## Resources

Learn more about  
HPE Enterprise Security  
Products, Services, and Solutions  
[hpe.com/software/DataSecurity](http://hpe.com/software/DataSecurity)

Find ESKM product details and  
related products at  
[hpe.com/software/eskm](http://hpe.com/software/eskm)

Contact your local  
Hewlett Packard Enterprise Sales  
Representative  
[DataSecurity.globalsales@hpe.com](mailto:DataSecurity.globalsales@hpe.com)

**Worldwide Technical Support**  
Data Security Support  
[DataSecurity.atalla.support@hpe.com](mailto:DataSecurity.atalla.support@hpe.com)

U.S. only: +1-800-500-7858  
Outside U.S.: +1-916-414-0216



Sign up for updates

★ Rate this document



## Unify data security and key management controls for all your sensitive data

ESKM helps protect sensitive information including payments cardholder data, customer and employee records, electronic health records, intellectual property, hosted cloud data, and national security and defense information with strong encryption key management.

ESKM helps organizations meet compliance and audit mandates including Payment Card Industry Data Security Standard (PCI-DSS), Health Insurance Portability and Accountability Act (HIPAA) or Health Information Technology for Economic and Clinical Health (HITECH), Graham Leach Bliley, Sarbanes-Oxley, state and international privacy laws, national security regulations, and internal policies, controls, and audits.

ESKM now supports the OASIS Key Management Interoperability Protocol (KMIP) standard and a growing range of Hewlett Packard Enterprise and partner encryption solutions for protecting sensitive data at rest wherever it resides from disk and tape media, to cloud.

ESKM scales easily to support large enterprises across multiple geographically distributed data centers, tens of thousands of encryption clients, and millions of keys.

ESKM supports applicable NIST and PCI standards and recommendations for cryptography, security, key management, and audit.

## HPE Enterprise Security and Services

### HPE Enterprise Security

Hewlett Packard Enterprise is a leading provider of security and compliance solutions for the modern enterprise to mitigate risk in their hybrid environment and defend against advanced threats. Based on market-leading solutions from HPE ArcSight, HPE Fortify and HPE Data Security, the HPE Security Intelligence Platform uniquely delivers the advanced correlation, application protection, and network defenses to protect today's hybrid IT infrastructure from sophisticated cyber threats.

### HPE Security Services

HPE ESP Global Services take a holistic approach to building and operating cyber security and response solutions and capabilities that support the cyber threat management and regulatory compliance needs of the world's largest enterprises. We use a combination of operational expertise—yours and ours—and proven methodologies to deliver fast, effective results, and demonstrate ROI. Our proven, use case-driven solutions combine market-leading technology together with sustainable business and technical process executed by trained and organized people.

Learn more at  
[hpe.com/software/eskm](http://hpe.com/software/eskm)  
[hpe.com/software/DataSecurity](http://hpe.com/software/DataSecurity)

© Copyright 2014–2015 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Intel Xeon is a trademark of Intel Corporation in the U.S. and other countries. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

4AA5-0654ENW, December 2015, Rev. 2