Solution brief

Manage business-critical keys with ease

HP Enterprise Secure Key Manager

Managing encryption keys is a challenging but important aspect of your information security plan. HP ESKM provides operational simplicity and high assurance return on investment for local and remote key management protection.

HP Secure Encryption with HP ESKM

Winner of the "Best Database Security Solution" Readers Trust Award

SC MAGAZINE AWARDS 2015 WINNER Honored in the U.S.

Secure data starts with protecting your keys

Cybercrime, mobile data access, cloud services, and other realities of doing business in a connected world make securing sensitive data more complex—and more critical—than ever. A well-rounded enterprise security plan includes strong storage encryption. When data-at-rest is encrypted, the audit risks of policy compliance, financial losses from a breach, and damage to your business reputation are reduced.

However, encryption itself is not sufficient without reliable management and protection of cryptographic keys. Compromised or misused keys that are improperly exposed or lost can derail the best security plans and leave you open to attack and audit failure. That makes high assurance key management with policy enforcement for managing, protecting, serving, and preserving encryption keys over the life of the data a critical element of your security plan.

Protect data wherever it resides

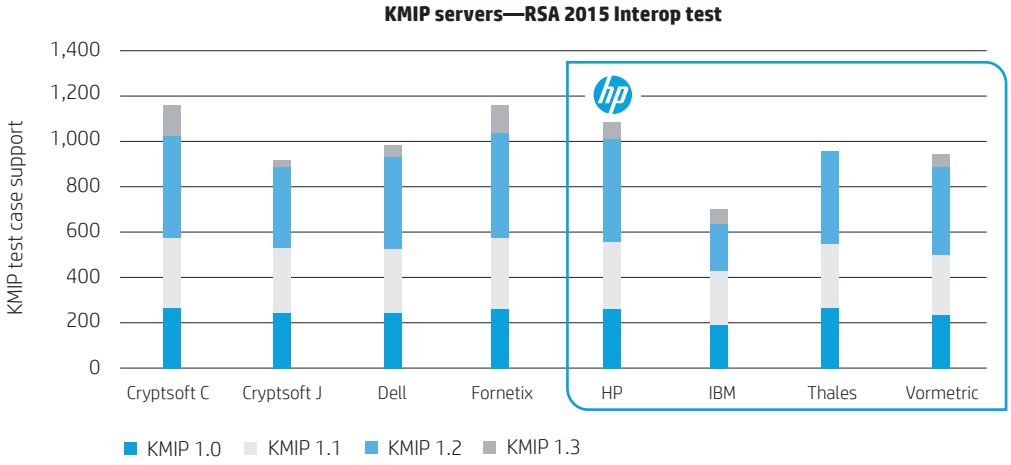
HP's enterprise data protection vision includes protecting sensitive data wherever it lives and moves in the enterprise, from servers to storage and cloud services. It includes HP Enterprise Secure Key Manager (ESKM), a complete solution for generating and managing keys by unifying and automating encryption controls. With it, you can securely serve, control, and audit access to encryption keys while enjoying enterprise-class security, scalability, reliability, and high availability that maintains business continuity.

Standard HP ESKM capabilities include high availability clustering and failover, identity and access management for administrators and encryption devices, secure backup and recovery, a local certificate authority, and a secure audit logging facility for policy compliance validation.

Together with HP Secure Encryption for protecting data-at-rest, ESKM will help you meet the highest government and industry standards for security, interoperability, and auditability.

HP Enterprise Secure Key Manager (ESKM)—OASIS KMIP Interop test 2015

ESKM leads KMIP compliance for servers



Source: OASIS KMIP Technical Committee

Meet audit and compliance mandates

- Payment Card Industry Data Security Standard (PCI-DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health (HITECH)
- Graham Leach Bliley
- Sarbanes-Oxley
- State and international privacy laws
- National security regulations

Enjoy wide support for industry standards

- OASIS Key Management Interoperability Protocol (KMIP) standard
- Applicable NIST and PCI standards and recommendations for cryptography, security, key management, and audit
- Federal Information Processing Standards (FIPS) 140-2

Reliable Security across the Global Enterprise

ESKM scales easily to support large enterprise deployment of HP Secure Encryption across multiple geographically distributed data centers, tens of thousands of encryption clients, and millions of keys.

The HP data encryption and key management portfolio uses ESKM to manage encryption for servers and storage including:

- HP Smart Array controllers for HP ProLiant servers
- HP NonStop VLE for disk, virtual tape, and tape storage
- HP Storage solutions including all StoreEver encrypting tape libraries, the HP XP7 Storage Array, and HP 3PAR

With certified compliance and support for the OASIS KMIP standard, ESKM also supports non-HP storage, server, and partner solutions that comply with the KMIP standard. This allows you to access the broad HP data security portfolio, while supporting heterogeneous infrastructure and avoiding vendor lock-in.

Benefits beyond security

When you encrypt data and adopt the HP ESKM unified key management approach with strong access controls that deliver reliable security, you ensure continuous and appropriate availability to keys while supporting audit and compliance requirements. You reduce administrative costs, human error, exposure to policy compliance failures, and the risk of data breaches and business interruptions. And you can also minimize dependence on costly media sanitization and destruction services.

Don't wait another minute to take full advantage of the encryption capabilities of your servers and storage. Contact your authorized HP sales representative or visit the link below to find out more about our complete line of data security solutions.

Learn more at
hp.com/go/eskm

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

4AA5-0620ENW, August 2015, Rev. 1