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

– Secure Key Management Solution Context
– HPE Enterprise Secure Key Manager
  – Solution Description
  – Use Cases
– Q&A
Odd Todd Video
Managing Encryption Keys -
Solution Context
Analogy: Don’t leave the keys in the car…

“Organizations must develop a business-led data-centric security strategy that will lead to the appropriate selection of either multiple siloed KM solutions or a single EKM.

As EKM products continue to mature and improve, clients will be better-able to implement a consistent, enterprise-class strategy — thereby protecting data, and achieving legal and regulatory compliance, while limiting risk in a demonstrable way, and reducing operational and capital costs.”

Gartner Hype Cycle for Data Security, 2015
Why do enterprises care about encryption?

Encryption is an area poised for wider adoption: 2nd highest ROI against cyber crime

Why is enterprise key management a challenge?

– Encryption is now an easy solution to protect confidential data…
  Well-proven defense against breaches—highly effective, often mandated as necessary cost
  Simple to implement: AES keys, standardized, now embedded—but…

– Key management is hard if not done correctly!
  Maintain central controls: Lose access to keys → lose access to the data
  Socially engineer policy: Who manages keys? What authorization for applications?
  Audit and prove compliance: Regulatory mandates expect evidence of protection

Can you coordinate and automate controls that protect access to keys across enterprise encrypted data, while maintaining efficient operations?
HPE Enterprise Key Manager - Solution Overview
HPE Enterprise Secure Key Manager
High-assurance protection for wide range of encryption use cases

– **Value Proposition**
  - Centrally manages encryption keys at a global enterprise scale
  - Separates keys from data to improve reliability & availability
  - Automates key operations—backup, rotation, logging…

– **Integrates largest HPE + 3rd party IT ecosystems**
  - ProLiant, 3PAR, NonStop, XP7, StoreEver, StoreOnce, Helion
  - KMIP-compliant partner applications & pre-qualified solutions

– **Features at a Glance**
  - **Easily Deployed**: 1U hardware appliance
  - **Highest Availability**: deployed in clusters up to 8 nodes
  - **Scalable for New Applications**: 25K clients, 2M keys
  - **Assurance Certified**: NIST FIPS 140-2 Level 2 & SNIA validated
  - **Interoperable**: industry-standard interface (KMIP) extensible

https://wiki.oasis-open.org/kmip/KnownKMIPImplementations
http://www.snia.org/forums/SSIF/kmip/results

storage security industry forum
https://www.snia.org
ESKM: Integrates data-at-rest encryption management

Business applications, data stores and processes

Servers (ProLiant)  Disk and Tape (3PAR, X7, StoreEver, StoreOnce)  Web/Cloud (HPE Helion / OpenStack)  Big Data (Vertica, Zettaset)  HPE Nonstop Applications & Databases  3rd party applications  Mainframe applications & databases  Enterprise applications  3rd party SaaS gateways  Production databases

HPE Portfolio  HPE Partner Ecosystem & KMIP-Compliant

ESKM Key Manager (FIPS 140-2 Appliance)  ESKM Clustering (2-8 Nodes)  Management Console

Management Console

Authentication & authorization sources (Active Directory)
Use Case #1

HPE Secure Encryption
What is HPE Secure Encryption?
Enterprise-class encryption solution for ProLiant Servers

**HP Secure Encryption** is a controller-based data encryption solution for HPE ProLiant Gen 8 and 9 servers that protects data at rest on any bulk storage attached to an HPE Smart Array Px3x and Px4 controllers.
HPE ESKM Use Case: Sensitive health records in private cloud

– **Customer Profile**
  - Major Healthcare IT Provider

– **Business Challenge**
  - Business owner: Application IT
  - Sensitive data: EHR, PHI, PII
  - Challenge: protect sensitive patient information in multi-tenant environment while maintaining HIPAA compliance – date at rest protection

– **Data Infrastructure**
  - Scale-out ProLiant server infrastructure
  - Mirrored data centers, each with multiple fully-isolated fault zones
  - 10K+ servers, 250K+ HDD/data center
HPE ESKM Use Case: Sensitive health records in private cloud

- **HPE Security Value Proposition**
  - Full disk encryption on ProLiant servers — no performance impact via controller
  - Remote key management separates keys from the sensitive data
  - Scale-out support for tens of thousands of server clients, multiple data centers and fault zones

- **HPE Solution Architecture**
  - HPE Secure Encryption
  - ProLiant servers, internal HDD storage, SmartArray Controllers (one per server)
  - Multiple HPE ESKM nodes per data center, 2-node cluster per fault zone

Do you have sensitive data in private cloud environments that needs protection?
Why HPE Secure Encryption with ESKM is Better

Maintain CPU or I/O performance encrypted
– Eliminate additional server capacity purchases

Eliminate disk DMR cost with “instant erase”
– Delete the key, destroy the data – no extra support cost, shredding cost or environmental waste

Eliminate complexity
– Eliminate hassles and expenses - Self Encrypting Drives (SEDs) are expensive, limited vendors, mostly not FIPS validated, require local unlock keys

Maintain open standards with no vendor lock-in
– Supports open standards key management (KMIP)

No dependence on TPMs, OS, or applications
– Low-touch administration, built-in high-availability, FIPS validated security, fully auditable

Comprehensive, versatile
– Full protection - Available on ProLiant Gen 8 and Gen 9 (DL, SL, BL, ML), HDD or SSD, SAS or SATA, boot drives
– Data wipe, data migration, online key rotation
Use Case #2

HPE ESKM for Cloud Use Cases
HPE ESKM key management for cloud use cases

**Public Cloud**
- Hosted HPE ESKM Tenant Keys
- Cloud Gateways

- IaaS Servers
- IaaS Storage

- Application Layer
  - (HPE SecureData)

**Private Cloud**
- HPE ESKM Appliance Cluster
  - Consistent Policy & Controls
  - Hardware-Level Assurance
  - High Availability Clustering
  - Cloud Application Mobility

- On Premise Application Keys

- 3rd Party (KMIP)

- HPE Infrastructure
  - Business Unit
  - Custom Apps

- On Premise HPE ESKM Application Keys

- HPE ESKM Appliance Cluster
  - Application Grouping
  - User & Key Separation
  - Top-Down IT & Audit Visibility
  - Security Practice Center of Excellence
Standards
What is KMIP?
Key Management Interoperability Protocol

- **Simplified encryption management across global organizations**
  - Align security policy – consistent controls, simplified audits
  - Improve cost of ownership – one system to learn, manage, and maintain
  - Future-proof IT – avoid vendor lock-in to old, unsupported technology
  - Enforce best practices – automate controls, applied universally
  - Increase ROI – re-use appliances for new solutions
  - Achieve faster time-to-value – pre-qualified compatibility

- **HPE background history and value**
  - OASIS TC founded with four industry-leading vendors, including HPE
  - Expanding ecosystem of partners and applications
  - Flexibility to address emerging solutions
OASIS KMIP Interoperability (2016)
ESKM KMIP compliance for management server solutions

HPE is the top EKM server vendor
HPE and ESKM: industry’s broadest portfolio of KMIP solutions
ESKM leads all others in KMIP compliance and interoperability

**HPE Security and Storage solutions**
- Enterprise Secure Key Manager 4.x **
- StoreEver MSL 6480 LTO-4/5/6 Tape Library **
- StoreServe 3PAR 7000, 7450, 8000, 10000, 20000
- XP7 and P9500 with DKA
- StoreEver ESL G3 LTO-4/5/6 Tape Library
- StoreEver MSL LTO-4/5/6 Tape Libraries (all models)
- StoreOnce (in process)
- HPE Helion (in process)
- HPE Autonomy (in process)

**Certified KMIP-conformant, SNIA SSIF test program**

**ESKM KMIP partner program**
- Bloombase
- Cryptsoft
- ETI-Net
- Fornetix
- Hitachi / HDS (in process)
- NetApp (in process)
- OpenStack community
- Project 6 Research
- ZettaSet

Others welcome—please contact Data Security!
Summary: Protect your business-critical application keys
High-assurance key management for your encrypted data

– **Value Proposition**
  - Centrally manages encryption keys at a global enterprise scale
  - Separates keys from data to improve reliability & availability
  - Automates key operations—backup, rotation, logging…

– **Integrates largest HPE + 3rd party storage ecosystem**
  - ProLiant, 3PAR, NonStop, XP7, StoreEver, StoreOnce, Helion
  - KMIP-compliant HPE partner applications & pre-qualified devices

– **Get Started with ESKM today…**
  - **Virtual appliance or HW demo**: easy to evaluate ESKM
  - **Easy deployment**: install and configure nodes quickly
  - **Simple licensing**: appliances, client licenses, support & services
  - **Highest availability**: Market-leading up to 8-node clustering
  - **Scales for future ROI re-use**: 25K clients, 2M keys, KMIP 1.3
“There are very few vendors that offer EKM today. ... The future of key management will depend on vendors’ ability to reduce complexity.” – Forrester

Easy ability to enable encryption in HPE products

Encryption keys managed in a FIPS-validated appliance

KMIP – avoid vendor lock-in and expand application coverage
Thank you

hpe.com/software/ESKM
Backup
Product Features & Functions
For HPE ESKM
Security & business continuity with market-leading interoperability

HPE 3PAR StoreServ (Disk and All-Flash Array)

HPE ProLiant Servers with built-in Secure Encryption

HPE StoreEver Tape Libraries

HPE StoreOnce Backup

HPE XP7 High End Storage

NonStop Servers

Partner SDKs

KMIP Clients

Connected MX

Openstack Barbican

BackBox Virtual tape

HPE Enterprise Secure Key Manager x 8

Openstack
Barbican

HPE Helion

OASIS
**HPE Enterprise Secure Key Manager**

Unified key management for the enterprise
ESKM appliances and client licensing – what to buy
ESKM clusters to 8 nodes with client licenses for storage, server & other devices

M6H81AA
ESKM v5 (single node)
(Includes 1 Client License)

2-node cluster (recommended)
Must run same major software revision

C8Z40AAE
ESKM Additional Client License
- Standard Per Client E-LTU
- Electronic delivery, customer proof of entitlement to use
- One license per enrolled “User” (defined as the encrypting device)
- Shared across ESKM cluster
- Volume discount pricing (10, 25, 50+ quantity)
- Secure Encryption & Clients
  - HPE SE (per server): C9A82AAE
  - ProLiant Server Client: C9B52AAE

H7J35A3
Support
- 3yr Foundation Care 24x7 w/ optional DMR SVC (1, 3, 4 or 5 yr. plans)
- HW 4-hour on-site response, plus SW telephone support (LTU, updates)

H8F22A1
Deployment Services
- Atalla ESKM Quick Start 2 Day
- Recommended 1 qty. per pair
Reliability, availability and recovery
HPE ESKM provides layers of protection and recovery for mission-critical keys

- DR Restore from Backup
- Client-Side Multi-Site Failover
- Replication with 2-8 Node Clusters
- Mirrored Disks, Dual Power, Dual NICs
- Field-Proven Reliable Hardware & Software
Users, groups & permissions – Clients, users & object groups
Managing cryptographic objects across applications according to owners

– Only a key creator (or its group members) can access a key to perform any operation
  – Example: Export and delete ESKM keys over XML protocol
  – Membership to ESKM groups is optional for granting access to a key

– **KMIP permission model:** access to KMIP managed objects by group members
  – User groups (source): users must belong to at least one group (same privileges)
  – Object groups (target): KMIP managed objects (e.g., keys) in a group are accessed by authorized user groups
Administrative privileges
Local user permissions

– Users with permissions can perform various operations for cryptographic objects
– Permissions are defined for the group, not the user—group members (users) can perform all operations
– Editing the policy to modify permissions requires determining a user’s default target and source group
Full visibility into keys and operations

- Fine-grain information recorded
- System, Audit, Activity, Client, KMIP Logs
- Signed for tamper evidence
- Exportable: ArcSight Flexconnector
- Complies with industry QSA requirements:
  - PCI, HIPAA, HITECH, etc.
Ports and Services

**Security Administrators**
- SSH
- SSL
- Serial Port
- CLI Admin Server
- GUI Admin Server
- Key DB
- ESKM local CA
- ESKM Cluster Sync SSL
- ESKM Cluster SSL
- Keys, Users, Policies
- Keys, Metadata

**ESKM Clients/Users**
- KMS Server SSL
- FTP, SFTP, SSH/SCP

**IT Services**
- LDAP Server
- LDAP Client
- NTP Server
- NTP Client
- Backup Server
- FTP, SFTP, SSH/SCP
- Syslog Server
- SNMP Agent
- FIPS Status Server
- Health Check Server
- NMS

**Monitoring**
- ArcSight/SIEM
ESKM appliances and client licensing
ESKM clusters to 8 nodes with client licenses for storage, server & other devices

**C8Z61AA**
ESKM 4.0 single node
(Includes 1 Client License)

**C8Z40AAE**
ESKM Additional Client License
- Standard Per Client E-LTU
- Electronic delivery, customer proof of entitlement to use
- One license per enrolled “User” (defined as the encrypting device)
- Shared across ESKM cluster
- Volume discount pricing (10, 25, 50+ quantity)
- Secure Encryption & Clients
  - HPE SE (per server): **C9A82AAE**
  - ProLiant Server Client: **C9B52AAE**

**H7J35A3**
Support
- 3yr Foundation Care 24x7 w/ optional DMR SVC (1, 3, 4 or 5 yr. plans)
- HW 4-hour on-site response, plus SW telephone support (LTU, updates)

**H8F22A1**
Deployment Services
- Atalla ESKM Quick Start 2 Day
- Recommended 1 qty. per pair
Our digital world is radically changing the risk landscape

Sophisticated cyber attacks
External disasters and internal failures
Cost and complexity of data protection
Regulatory pressures

Mobile and cloud dissolve the “perimeter”
Hyper-connected sensors and devices create new exposures
Massive data growth from multiple sources
Regulatory, privacy and compliance concerns
HPE Security - Data Security
Full data protection for key use cases

PCI /Compliance/ scope reduction

Data de-identification and privacy

Collaboration security for users, cloud apps, and data interactions
# HPE Security - Data Security

Full umbrella of data protection use cases

## Data Security (HPE Atalla & HPE Security Voltage)

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Solutions</th>
</tr>
</thead>
</table>
| **PCI / Compliance/ scope reduction** | HPE Atalla HSMs  
Secure payments applications with the most stringent compliance requirements, including Debit, EMV, Cloud-based payments with FIPS 140-2 Level 3+ appliance | HPE SecureData  
Reduce PCI costs up to 90% with P2P encryption; combine HPE Secure Stateless Tokenization (SST) with HPE Page-Integrated Encryption (PIE) for complete ecommerce protection |
| **Data de-identification and privacy** | HPE Enterprise Secure Key Manager  
Secure server, storage and cloud against losses, mishandling, and administrative and operational attacks, with KMIP standardized interoperability and HPE Secure Encryption | HPE SecureData  
Secure sensitive data while enabling business process with HPE Format-Preserving Encryption (FPE); enable analytics on sensitive data for Hadoop/Big Data; protect test data |
| **Collaboration security**       | HPE Cloud Access Security Protection (Adallom)  
Flexible architecture for visibility, governance and control for SaaS | HPE SecureMail and HPE SecureData  
Email security without PKI complexity using HPE Identity-Based Encryption (IBE); protect sensitive PII and PHI throughout the enterprise and cloud |