Solution Brief

UTIMACO ESKM and HPE ProLiant Deliver Enhanced Protection for Data at Rest

Powered by UTIMACO and HPE

Creating Trust in the Digital Society

Hewlett Packard Enterprise

utimaco®

Simplified Encryption Solution with Local or Cloud Key Management

Your Data at Rest Secured and in Compliance

To mitigate the potential impact of a compromise, it is crucial to minimize intruder access to data and sensitive information on disk.

Data loss has the potential not only to interrupt your daily business operations, but also leaves you vulnerable to legal liability and negative press. What's more, if you're in the financial services, healthcare, or other regulated industry, you are also responsible to comply with regulations such as the Payment Card Industry Data Security Standard (PCI-DSS), Common Criteria (CC), Federal Information Processing Standards (FIPS), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley (SOX), and a growing array of other data privacy regulations. VS-NfD approval is particularly crucial for government use cases in Europe.

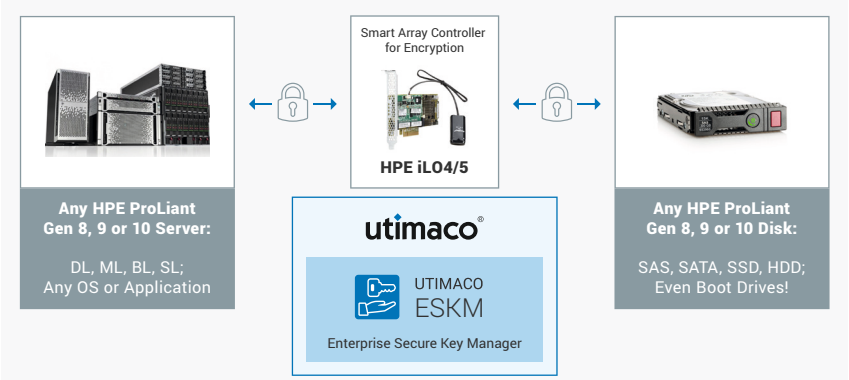
UTIMACO ESKM and HPE together is the ideal solution to help prevent data loss or data breach while delivering the best performance, optimal TCO and peace of mind through strong hardware-based security.

The types of data, if lost or compromised, could cause a major business and trust problem for your organization:

- **Payment card** data
- **Private customer data** including health records
- **Financial data** about your company or employees
- **Trade secrets** and intellectual property
- **Government records** and confidential data

HPE ProLiant and UTIMACO for Secure and Compliant Data at Rest Encryption

HPE Secure Encryption with UTIMACO ESKM
Enterprise-class encryption solution for ProLiant Servers



Key Features

- Native Protocol
- VMware Virtual Drive Coverage
- On-Prem or Cloud Key Management Powered by ESKM
- HPE Smart Array Controller Module Encrypted
- Encrypted Boot Volume

UTIMACO Enterprise Secure Key Manager

UTIMACO ESKM unifies and automates encryption controls by securely creating, protecting, serving, controlling, and auditing access to your business and mission critical encryption keys.

ESKM is a fully integrated solution that is a FIPS 140-2, PCI, validated and VS-NfD approved secure server appliance. The standard capabilities include high availability clustering and failover, a 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.

In addition, ESKM is available as a virtual appliance designed to be compliant with FIPS 140-2 Level 1 and as a hardware appliance designed to be compliant with FIPS 140-2 Level 2, 3 and 4, providing the right level of security for discrete environments.

Explore the capabilities of ESKM and **download the trial** for free.

Broad Encryption Coverage and Benefits

- Implement and enforce seperation of duties and dual access control by separating the data and keys managed individually
- Encrypt not just the HDD but cache too
- Any HDD or SSD in the HPE Smart Drive portfolio for HPE ProLiant servers is supported
- Remote key management mode allows central key management from just a few servers to 25,000 servers, millions of keys and thousands of highly available (HA) nodes with simplified deployment and management
- HPE Secure Encryption and HPE Data Sanitization help you comply with industry regulations and legislation such as PCI-DSS, HIPAA, and SOX
- Maintain CPU or I/O performance while encrypted
- Eliminate disk DMR cost with “instant erase” – Delete the key, destroy the data – no extra support cost, shredding cost nor environmental waste
- Eliminate complexity implies no hassles and lower expense, no more vendor lock-in as well as no dependency on the self-encrypting drives (SED) which are usually expensive, might not be FIPS validated and require local unlock keys
- Maintain open standards with no vendor lock-in – ESKM supports open standards key management (KMIP)
- No dependency on TPMs, OS or applications – Low-touch administration, built-in high availability, FIPS validated security with complete auditability
- Fully automated – iLO scripting aligned with smart storage array scripting for mass and automated deployment with ESKM self-registration support

UTIMACO ESKM Benefits

- The most interoperable and integrated key manager in the market
- Hardware-based security at the highest FIPS levels
- Custom integrations and scaled deployments
- Easy deployment with simple licensing
- Centralized root of trust
- Integration of vESKM with external HSMs to enhance security while managing the keys virtually
- Integration with the entire HPE ecosystem and third-party applications using KMIP

UTIMACO ESKM is the most interoperable and integrated key manager in the market.

Key Features

Key Control and Management Through a Single Pane of Glass

- **Control and manage** the keys throughout the key management lifecycle with digitally signed logs for auditing purposes
- **Reduce audit costs** and improve visibility

Hardware-Based Security at the Highest Level

- Locking front bezel and dual pick-resistant locks for **dual control by security officers**
- **Security hardened Linux-based** server appliance; designed as cryptographic module for FIPS 140-2 Levels 1, Level 2, Level 3 and Level 4 use cases
- **Support for mirrored internal storage**, dual networks, dual power and redundant cooling
- **Terminal interface** (serial RS-232C) and VGA for initial installation setup

Centralized Root of Trust

- **Store the cryptographic keys** in the foundation where all secure key operations including key retrieval of vESKM depends on
- Empower an **inherently trusted ecosystem**

Simplified Administration

- Configuration and **automated key replication through active-active cluster**
- **Automatic key replication**
- **Hands-off administration**
- **Automated backup** with audit logs

Integrates with the Broad Ecosystem of HPE and Third-Party Applications

- **ESKM KMIP Integrations** (BDT, Brocade, Cryptosoft, ETI-Net, Fornetix, Hitachi Vantara, IBM Db2, MongoDB, NetApp, OpenStack, Project 6 Research, Quantum, Spectra Logic, SUSE, VMware, Zettaset)
- **HPE Security and Storage Solutions**
  - Helion *(OpenStack Barbican + HPSE)*
  - MF Autonomy *(Connected MX Backup/ Recovery)*
  - Nimble
  - NonStop
  - Secure Encryption *(ProLiant/smart array controller)*
  - SimplyVity/Hyper Converged
  - StoreEver
  - StoreEver Tape Library
  - StoreOnce
  - StoreServe 3PAR
  - XP
  - XP Storage

Streamlining Data and Processes

- **Unified enterprise key management**
- **Reliable policy controls**
- **Centralized administration** with audit trail to assist with control attestation

Robust Scalability and High Availability

- **Geographically dispersed clusters** across datacenters
- **Full support for tens of thousands of clients,** thousands of virtual or hardware appliances **and millions of keys**
- **Highly redundant** hardware with failover

Custom Integrations and Scaled Deployments

- Using ESKM as a trusted key manager to **safeguard mission critical application keys** and to support custom use cases with open client libraries such as OpenKMIP and PyKMIP
- **Implementing auto-registration** with native XML-based KMS protocol
- **Offering the broadest range of client integrations** in the industry

Use Cases

One of the largest healthcare and insurance providers takes advantage of the centralized view of all nodes and keys through a single pane of glass with ESKM on HPE ProLiant to help protect data across tens of thousands of servers globally. ESKM and HPE ProLiant together has helped the client shorten the response time when security issues do occur. Thanks to the separation of duties and dual-access control implemented, this client has achieved the most stringent HIPAA compliance as desired.

In addition, a leading general aviation company counts on ProLiant and Storage Solutions as well as ESKM to protect data at rest including proprietary and third-party database solutions to ensure information security at application level towards a zero-trust policy.

HPE Trusted Supply Chain Process

HPE further extends its security capabilities in the server from distribution and shipping, through its complete lifecycle while it is active. The new features are built on top of the HPE exclusive silicon root of trust security technology. The hardened security features activated during the manufacturing process offers the following benefits:

- **Prevent booting of any compromised operating system (OS)** with new hardening to connect the server firmware security to the operating system by activating the Unified Extensible Firmware Interface (UEFI) secure boot.
- **Reduce attack surface** by setting the servers in high security mode to verify user authenticity, ensuring that more than four million lines of firmware code is valid and uncompromised.
- **Prevent tampering of server firmware and hardware using server configuration lock** to verify unauthorized addition of options (NICS, drives) or malicious activity by capturing the inventory or a “picture” of the server, its hardware and firmware at the factory as a baseline for validation and protection throughout the supply chain process.
- **Alert customers with embedded alarm and physical lock** if the server has been opened during the supply chain process when an intrusion detection latch, inserted on the server chassis, registers unauthorized opening even if the power is off.
- **Another key security measure from HPE** is the Distributed Intrusion Monitoring Engine (DIME) designed to detect malicious changes to kernel code and data, which rootkits often modify to hide the presence of malware.

About HPE

Hewlett Packard Enterprise (NYSE: HPE) is the global edge-to-cloud company that helps organizations accelerate outcomes by unlocking value from all of their data, everywhere. Built on decades of reimagining the future and innovating to advance the way people live and work, HPE delivers unique, open and intelligent technology solutions delivered as a service – spanning Compute, Storage, Software, Intelligent Edge, High Performance Computing and Mission Critical Solutions – with a consistent experience across all clouds and edges, designed to help customers develop new business models, engage in new ways, and increase operational performance.

For more information, visit: hpe.com

About UTIMACO

UTIMACO is a global platform provider of trusted Cybersecurity and Compliance solutions and services with headquarters in Aachen (Germany) and Campbell, CA (USA).

UTIMACO develops on-premises and cloud-based hardware security modules and key management solutions as well as compliance solutions for telecommunication providers in the field of regulation. UTIMACO is one of the world's leading manufacturers in both of these market segments.

450+ employees around the globe create innovative solutions and services to protect data, identities and communication networks with responsibility for global customers and citizens. Customers and partners in many different industries value the reliability and long-term investment security of UTIMACO's high-security products and solutions.

Find out more on utimaco.com

Headquarters Aachen, Germany

Headquarters Campbell, USA

Contact us

EMEA

UTIMACO IS GmbH

Germanusstrasse 4
52080 Aachen,
Germany

+49 241 1696 200

hsm@utimaco.com

Americas

UTIMACO Inc.

900 E Hamilton Ave., Suite 400
Campbell, CA 95008,
USA

+1 844 UTIMACO

hsm@utimaco.com

APAC

UTIMACO IS Pte Limited

50 Raffles Place,
Level 19, Singapore Land Tower,
Singapore 048623

+65 6631 2758

hsm@utimaco.com

For more information about UTIMACO® HSM products, please visit:

utimaco.com

Creating Trust in
the **Digital Society**

utimaco®