Product Brochure

Protect your data and keys with UTIMACO ESKM – Enterprise Secure Key Manager

The most interoperable and integrated key manager

UTIMACO ESKM

UTIMACO vESKM

Creating Trust in the Digital Society

utimaco®

The Data Security Needs and Challenges of Today's Enterprises

Today IT organizations face many challenges to security and business continuity. **24x7 business applications and services require continuous availability, data protection, and regulatory compliance,** but there are changing internal and external threats to consider in designing a robust architecture that combines high availability (HA) and high security elements.

UTIMACO's approach to enterprise security is providing customers the tools to defend themselves in this hostile environment and to disrupt the adversary criminal ecosystem. This includes educating users and improving systems to avoid security errors; blocking adversary access into enterprise networks and systems; detecting and removing adversaries quickly if they gain access; securing the sensitive information assets wherever they live and move; and lastly helping organizations adopt plans to mitigate and reduce damages when a breach occurs. **Today, organizations must assume they will be breached at some point and plan appropriately to respond.**

Valuable Assets That Enterprises Need to Protect:

- **Payment card holder data**
- **Electronic health records**
- **Personally identifiable information Intellectual property**
- **Confidential business records**
- **Hosted client data**
- **Defense and classified information**

UTIMACO ESKM

UTIMACO's solution for enterprise key management is ESKM – Enterprise Secure Key Manager. ESKM is deployed wherever customers use encrypted storage or communications to protect their sensitive information that can reside in tape libraries/media, in enterprise disk arrays, on storage area networks, in server attached storage, and in private and public cloud services.

When customers encrypt data and adopt a unified key management approach with ESKM, they store and serve keys with strong access controls and security. They ensure continuous availability to keys, and they support their internal and external audit and compliance requirements. **Customers adopting a unified key management architecture reduce their costs for administration, reduce the possibility of human error, reduce their exposure to audit and compliance failures, and reduce the risk of data breaches and business interruptions.** Lastly, they can eliminate dependence on costly media sanitization and destruction services.

Data encryption is a technology increasingly used in enterprises to protect sensitive data at rest and in motion. However, encryption itself is not sufficient without the proper management of the encryption keys. In this day and age, it is vital to have a centralized, scalable, and integrated key manager in your arsenal that interfaces with all the applications in the environment. Utimaco ESKM already supports industry standard key management protocol – KMIP, a more flexible and simpler native API – KMS.

UTIMACO
ESKM

Key Features

Highest Level of Security. Tamper-responsive with the ability to act in response to side-channel attacks with **FIPS 140-2 Level 1, Level 2, Level 3 and Level 4 (physical) compliant architecture;** certificate-based authentication and built-in CA.

Embedded HSMs.

- vESKM integrated with CC and VS-NfD certified UTIMACO CryptoServer LAN V5 HSM to **protect the keys at rest.**
- ESKM L3 and ESKM L4 (physical) protects the keys at rest with embedded UTIMACO CryptoServer HSMs.

Proving Compliance. Meet audit and compliance mandates with **controls for PCI-DSS, HIPAA, EU data privacy laws** and other regional privacy mandates.

Key Control and Management. ESKM provides a **single pane of glass for auditing controls** with digitally signed logs and key lifecycle activities to reduce audit costs and accelerate visibility.

Streamlining Data and Processes. Enables unified enterprise key management with reliable policy controls, centralized administration, and audit trails to **reduce operational costs and assist in control attestation.**

Easy Deployment and Simple Licensing. ESKM can be easily installed and configured; simply drop in as hardware or virtual appliance. Access transparent client licensing, with **no hidden costs attached to volume of keys or scalability.**

Robust Scalability and High Availability.
Geographically separate clusters across datacenters, **supporting thousands of clients, and millions of keys** with failover and highly redundant hardware.

- **Active-active cluster Configuration** and automated key replication across thousands of notes (ESKMs) per clusters.
- **Automatic key replication Hands-off administration,** automated backups, and audit logging.

Hardware

- Capacity for **>2 million keys, >25,000 clients, and thousands of ESKM nodes** per distributed cluster
- Locking front bezel, dual pick-resistant locks for **security officer dual control**
- **Encrypted redundant storage,** dual networks, dual power with enhanced cooling
- **Multiple interfaces** for initial installation setup

Software

- **All software is included,** pre-installed, digitally signed, and verified at startup
- Comprehensive **monitoring,** recovery, scheduled **backups,** and log rotations, **restore** functionality
- **Web browser GUI** and Command Line Interface supported
- Supports: **AES, 3-Key Triple DES, HMAC, RSA,** and **ECDSA** key types among others
- SNMP alerts and **SIEM log monitoring**
- TLS and on-demand backups with SSH key authentication, for **secure administrator remote access**

Compliance

- Designed for **NIST SP 800-131A** and **FIPS 140-2 Levels 1, 2, 3 and 4** (physical) requirements
- Certificate-based **mutual client-server authentication,** secure administration, and audit logging
- Conforms with **KMIP 1.0 through 2.1** specifications
- Performs **automatic key replication,** client load balancing and fail-over
- **Embedded Local Certificate Authority** as an option to protect keys in transit

Secure

- Meet NIST standards, validated to **FIPS 140-2 Level 1-4, Common Criteria**
- Encrypts keys in transit and at-rest
- Certificate-based authentication and built-in CA

Interoperable

- **Support OASIS KMIP** (Key Management Interoperability Protocol)
- Support RESTful interface
- No vendor lock-in
- Custom integrations using SDK

Available

- **Active-Active** cluster with thousands of nodes
- **Automatic key replication,** client failover
- **Highly redundant** hardware

Scalable

- Geographically **separated clusters** across datacenters
- Supports thousands of clients, and **millions of keys**

Managable

- Configuration and keys replicated across cluster automatically
- **Hands-off adminis-tration,** automated backups and audit logging
- Deploy as a Virtual Machine

Solution Benefits

Highly Interoperable

- ESKM is a certified Key Management Interoperability Protocol (KMIP) v2.1 offering, with market leading support for partner applications and pre-qualified solutions.
- Key management is reliant on the ability to integrate with other systems. That's why it is essential for organizations to choose a key manager that integrates out-of-the-box with varied deployments, as well as custom integrations. ESKM supports OASIS Key Management Interoperability Protocol (KMIP) that supports communication with clients for key management operations on cryptographic material, including symmetric and asymmetric keys, certificates, and templates. **By implementing KMIP with ESKM, organizations can achieve the following:**
  - **Streamline security policies** for consistent controls and compliance audits
  - **Save money and time** with a single system to learn, control, maintain, audit, and integrate new applications with no additional management required
  - **Mitigate vendor lock-in** and outdated technology
  - **Implement best practices** with universal, automated key lifecycle controls

ESKM leads all others in KMIP compliance and interoperability

- Cryptsoft
- ETI-Net
- Fornetix
- Hitachi Vantara
- NetApp
- OpenStack community
- Project 6 Research
- ZettaSet
- Vmware
- MongoDB
- IBM Db2
- Spectra Logic
- Quantum
- Bloombase
- BDT
- SUSE
- Brocade
- Panasas

ESKM KMIP Integrations

HPE Security and Storage Solutions

- StoreEver Tape Library
- StoreServe 3PAR
- XP
- StoreEver
- StoreOnce
- XP Storage
- NonStop
- Secure Encryption (Proliant/smart array controller)
- Helion (OpenStack Barbican + HPSE)
- SimpliVity/Hyper Converged
- Nimble
- MF Autonomy (Connected MX Backup/Recovery)

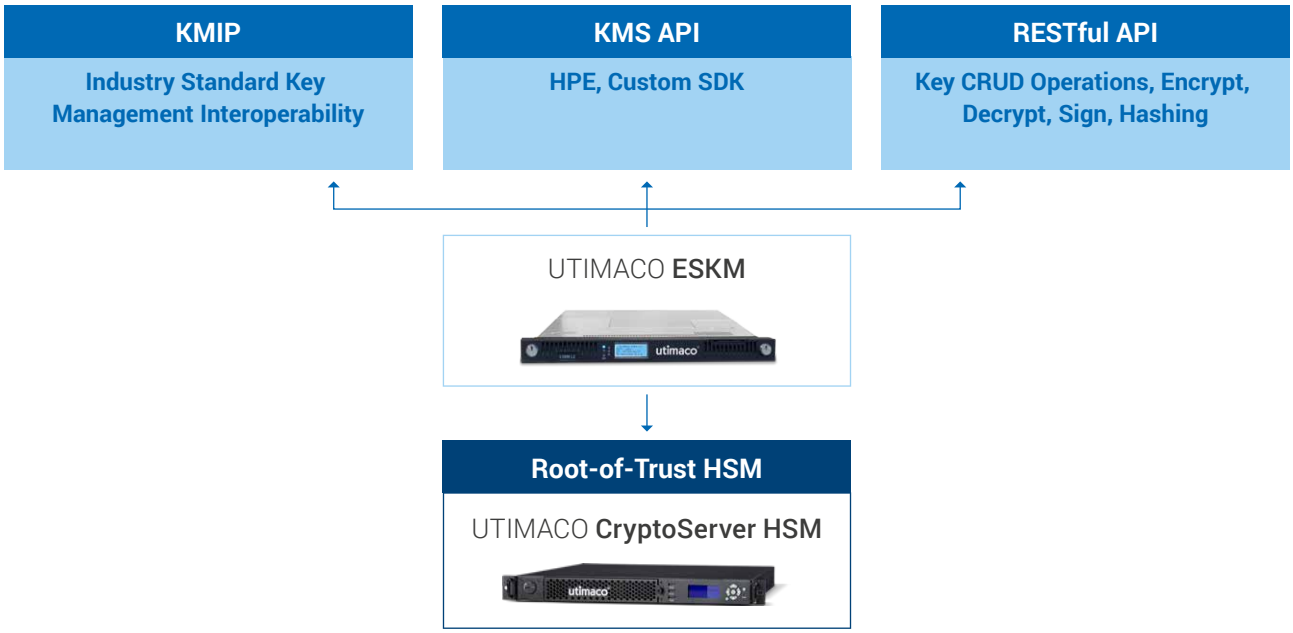
Hewlett Packard Enterprise

MICRO FOCUS

ESKM – the industry's broadest key management portfolio

Custom Integrations and Scaled Deployments

- Simplified RESTful API interface for key CRUD operations (Create, Read, Update, Delete), and crypto operations (Encrypt, Decrypt, Sign, Verify), that provides flexibility and ease of use supporting key management and encryption.



ESKM with 3 different interfaces: KMS API, KMIP, RESTful API.

- Integrated with open client libraries like KMIP, OpenKMIP and PyKMIP, ESKM can help safeguard the mission critical application keys as the trusted key manager for custom use cases.
- UTIMACO ESKM implements an XML based native Key Management System (KMS) protocol that is very easy to implement at scale. This KMS protocol supports auto-registration, which is always a challenge for scaled deployments. UTIMACO also provides a client library / SDK for custom integrations.
- Supporting these two protocols, ESKM stands out as the enterprise key manager of choice supporting the most client integration uses cases in the industry.
- NIC Teaming support – remove dependency on a single network interface adding redundancy.

Cloud Integrations and BYOK

ESKM is collaborating with both Google and Microsoft Azure to help organizations transition securely to the cloud. **With the BYOK – Bring Your Own Key – concept, enterprises encrypt their own data, retain control of their encryption keys, and do not give the control away to the CSP.**

Technical Specifications

Physical Security and Specifications

- **Appliance security**
  Rack-mountable (1U), physically fortified, doublelocking bezel, Medeco pick-resistant locks
- **Electrical security**
  Dual redundant power supplies, out-of-range temperature and voltage detection
- **Controls**
  Power on/off switch, unit ID switch, LCD control panel
- **Dimensions (WxDxH)**
  19 x 26 x 1.75 in
  (48.26 x 66.04 x 4.45 cm)
- **Weight**
  ESKM-L2: 24.9 lbs (11.3kg)
  ESKM-L3/L4: 27.8 lbs (12.6 kg)

Connectivity

- **Communications ethernet**
  TCP/IP, TLS 1.2 (only)
- **Connection**
  10/100/1000BASE-T (RJ45) auto-sensing

Electrical and Thermal Characteristics

- **Rated input voltage**
  100 to 127 VAC
  200 to 240 VAC
- **Rated input current**
  5 A – 3 A at 200 VAC
- **Rated input frequency**
  50 Hz to 60 Hz
- **Rated input power**
  350 W at 200 VAC
- **BTUs per hour**
  1195 at 100 VAC
  1195 at 200 VAC
- **Rated steady-state power**
  250 W at 100 VAC
  250 W at 200 VAC
- **Maximum peak power**
  400 W at 100 VAC (3 sec.)

Operating Environment

- **Operating temperature**
  0°C to 40°C (32°F to 104°F)
- **Operating relative humidity**
  5% to 95%, non-condensing

Certification/Compliance

- **Safety**
  UL/CUL, CE, TUV, BIS, BSMI, SII
- **Emissions**
  FCC Class B, VCCI, BSMI, C-Tick, IC, KCC
- **Environmental**
  RoHS, REACH

Implement a Virtual Key Management Strategy the Easy Way with Virtual ESKM

UTIMACO
vESKM

Virtual ESKM

UTIMACO's Virtual Enterprise Secure Key Manager (vESKM) is the virtual version of the most interoperable and integrated Key Manager in the market. It provides a pre-configured and hardened security virtual appliance that provides a unified service for creating, protecting, and delivering cryptographic keys to data encryption devices and applications across the distributed enterprise IT infrastructure. Through that it enables you to protect and ensure continuous access to business critical and sensitive, data-at-rest encryption keys locally and remotely. vESKM centralizes cryptographic processing, security policies and key management in a FIPS 140-2 Level 1 complaint platform.

With vESKM You Can Take Advantage of the Following Benefits:

- **Agile key management**
- **Reduced hardware and maintenance costs**
- **Scalable key management to support growing and changing workloads and spikes in demand**
- **Increased security on cloud platforms by maintaining key ownership**
- **Better support for custom applications**
- **Quick and easy deployment**
- **High availability**

Get a fully functional **60 day trial!***

vESKM can help simplify key management across the entire lifecycle while protecting the keys using HSMs as the root of trust. **It is fully integrable with CC and VS-NfD compliant UTIMACO CryptoServer.**

Protect Your Keys With a Centralized Root of Trust

While Cryptography is the single proven technology that delivers protection for your data, only the HSMs paired with the right key management solution are the underlying custodians of trust. To provide an additional layer of security, customers can protect their keys by integrating the UTIMACO **CryptoServer LAN V5** HSM with vESKM. UTIMACO is known for its cryptographic solutions and best-in-class HSMs that serve the payment and general purpose market segments. The UTIMACO CryptoServer is a general purpose HSM that protects the security of cryptographic key material for servers and applications.

The vESKM (FIPS 140-2 Level 1, deployed as a virtual appliance) or ESKM L2 (FIPS 140-2 Level 2, deployed as a hardware appliance) fully integrates with the UTIMACO GP Hardware Security Module: CryptoServer LAN V5 over the network, whereas the ESKM L3 and L4 integrates with embedded CryptoServer PCIe card. This integration further protects the cryptographic keys at rest and provides a centralized root of trust.

Getting Started

Experience first-hand the look and feel of the User Interface (UI) and feature set without setting up a dedicated system for proof of concept. Download the vESKM distributed as Open Virtual Appliance (OVA).

To find out more about ESMK, visit our product page.

For more information, please email hsm@utimaco.com

*Registration required

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, solutions for key management, data protection and identity management as well as data intelligence solutions for regulated critical infrastructures and Public Warning Systems. UTIMACO is one of the world's leading manufacturers in its key market segments.

500+ 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

…people, devices and digital identities
against natural disaster, terrorism and cyber crime.

…financial transactions, data at rest and in motion
against theft and sabotage.

We protect …

…data and ideas
Digital economy and digital transformation processes against theft, abuse and manipulation.

…investments
With proven, future-proof technology, products and solutions that meet regulation and compliance standards.

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

6 Temasek Boulevard
#23-04 Suntec Tower Four
Singapore 038986

+65 6993 8918

hsm@utimaco.com

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

utimaco.com

Creating Trust in
the **Digital Society**

utimaco®