ESKM v5.x

Enterprise Secure Key Manager (ESKM) provides a centralized key management hardware-based solution for unifying and automating an organization's encryption key controls by creating, protecting, serving, and auditing access to encryption keys for secure, reliable administration.

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

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

ESKM helps organizations to comply with regulatory audits 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 (GLBA), Sarbanes-Oxley (SOX), state and international privacy laws, national security regulations, and in addition supports internal policies, controls, and audits.

utimaco®

Key Management is essential

ESKM supports the OASIS Key Management Interoperability Protocol (KMIP) versions 1.0 through 2.0, enabling the broadest range of data protection applications and partner solutions. A client Software Development Kit (SDK) is also available to partners and customers to enable native protocol ESKM integrations.

ESKM is designed as a turnkey 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, local Certificate Authority, and signed audit logging for compliance attestation.

Product Highlights

Unified, secure, scalable encryption key management services

- Automate and enforce organizational data protection and compliance policies
- Secure encryption key generation, creation, protection, serving, auditing for enrolled clients
- Supports multiple key algorithms use cases, encryption client devices
- Capacity for >2 million keys, >25,000 clients, and 8 ESKM nodes per distributed cluster

Strong auditable security

- Security hardened Linux-based server appliance; all software is digitally signed
- All keys and backups are encrypted both at rest and in motion
- Granular control of key management access to key owners and across administrator defined key-sharing groups
- Certificate-based mutual client-server authentication, secure administration, and audit logging
- ESKM v5.x is designed to FIPS 140-2 Level 2
- Locking front bezel, dual pick-resistant locks for security officer dual control

Reliable continuous access to business-critical encryption keys

- Supports mirrored internal storage, dual networks, dual power, and redundant cooling
- Native multi-site 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
- TLS and SSH for secure administrator remote access
- Terminal interface (serial RS-232C) for initial installation setup

Cryptography and security

- Supports (among others): AES, 3-Key Triple DES, HMAC, RSA, and ECDSA key types
- Designed for NIST SP 800-131A and FIPS 140-2 Level 2 requirements
- Conforms with KMIP 1.0 through 2.0 specifications

Key Features

Interoperable

- Supports OASIS KMIP, NIST, and other security standards
- Supports a growing range of tape, disk, network, cloud, and desktop partner data protection products and solutions
- Upgradeable to new software releases

Secure

- Hardened server appliance designed as a FIPS 140-2 Level 2 cryptographic module
- Common Criteria Evaluation Assurance Level (EAL 2+) certified
- All software is included, pre-installed, digitally signed, and verified at startup
- Keys are always encrypted at-rest and in-motion; TLS encrypted communications
- Strong mutual certificate authentication available for client access to keys
- Local Certificate Authority as an option

Scalable

- Clusters span and serve multiple data centers, across geographic locations
- Supports tens of thousands of encryption clients and millions of keys

Reliable

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

Manageable

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

Technical Specifications

Physical Dimensions

- **Full configuration weight:** 32.8 lb (14.8 kg) Overall dimensions: 30.87 x 19.01 x 1.69 in. (78.4 x 48.3 x 4.3 cm)

- **Form factor:** 1U rack mount; dual locking front bezel, FIPS Level 2 physical security and rack mount rail kit included 2 auto-sensing

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 ESKM node ships with dual redundant power supplies and two IEC C13 to C14 power cords intended for rack mounting with dual PDUs and UPS for highest availability. ESKM nodes may also be powered using two regional power cords connecting to receptacles on separate branch circuits for highest availability

Hardware

- **Processor:** Intel Xeon 6-core E5-2620 v3 2.4+ GHz

- **Memory:** 32 GB PC4-2133P; 15 MB L3 Cache

- **Disk controller:** Smart Array P440ar

- **Disks:** Dual RAID-1 (mirror) 600 GB SAS, encrypted

- **Cooling:** 7 High Ambient Temperature Fans

Connectivity

- **Interfaces:** 10/100/1000BASE-T (Ethernet) RJ-45 ports, 1 RS-232C serial console port, 1 video port

Operating Environment

- **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

- **Relative humidity:** 10% to 90%, 82.4°F (28°C) maximum wet bulb temperature, non-condensing

Non-operating/Storage Environment

- **Temperature:** 22°F to 140°F (-30°C to 60°C); maximum change 20°C/hr (36°F/hr)

- **Relative humidity:** 5% to 95%, 101.7°F (38.7°C) maximum wet bulb, non-condensing

Ordering Options for ESKM V5.X Software and Servers

ESKM v5.x single node server HW-ESKM-V1 (Level 2)

- One ESKM v5.x server node. Includes all hardware, accessories, pre-installed software, and documentation. Production clusters should be configured with a minimum of 2 and maximum of 8 nodes.

Prerequisites and limitations

- Single nodes are generally recommended only for ESKM low production, test and development environments, and for expansion of production clusters.

Hardware

- 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.

Documentation

- Includes "Read Me First" card, user guide, installation guide, and release notes.

Software

- ESKM v5 software is included and pre-installed on the server node. Software upgrades to ESKM version 5.x are available for free via electronic software delivery for each unit under a current Utimaco support contract.

Server LTU

- Includes ESKM v5 software LTU for a single server node.

Client LTU

- Each ESKM v5 single node server includes one pre-installed ESKM client license. Additional clients require additional client licenses, which may be purchased in any desired quantity.

Support services

- Support services must be ordered at the same time as a single node ESKM server order.

Installation services

- ESKM installation/startup, upgrade, migration, and training services are available. Please contact your Utimaco sales representative or reseller.

utimaco ®

EMEA	**Americas**	**APAC**
Utimaco IS GmbH	**Utimaco Inc.**	**Utimaco IS Pte Limited**
Germanusstraße 4 52080 Aachen, Germany	900 E Hamilton Ave., Suite 400 Campbell, CA 95008, USA	80 Raffles Place, #32-01, UOB Plaza Singapore 048624
+49 241 1696 200	+1 844 UTIMACO	+65 6622 5347
hsm@utimaco.com	hsm@utimaco.com	hsm@utimaco.com

For more information about Utimaco HSM products, please visit:

hsm.utimaco.com