Encryption Key Management for Compliance

The Townsend Security Alliance Key Manager is an encryption key manager that is available as a hardware security module (HSM), virtual appliance (VMware), or in the cloud (Microsoft Azure, Amazon Web Services, vCloud, etc.) Alliance Key Manager easily integrates with your databases/applications and enables you to address audit requirements for encryption and key management as found in PCI-DSS, GDPR, HIPAA, and other privacy regulations.


Alliance Key Manager helps organizations meet compliance requirements with FIPS 140-2 compliant encryption key management. The symmetric encryption key management solution creates, manages, and distributes 128-bit, 192-bit, and 256-bit AES keys for any application or database running on any Enterprise operating system (Windows, Linux, IBM i (AS/400), IBM z).

Cost-Effective
Affordable key management solution for any size organization. Leverages current investment in encryption technologies via vendor-neutral solution.

Compatible
Accessible from any Enterprise platform including Windows, Linux, IBM i, IBM z, and others.

OASIS KMIP (Key Management Interoperability Protocol) compliant.

Reliable
Reduces risk of application failure through redundancy and mirroring.

Easy to Use
Ready-to-use client software speeds deployment and reduces IT costs.

Secure Administration
Protects against key loss through secure and authenticated administration.

Partner Friendly
Extensive partner program insures successful and compliant results for your end customers.
**Features**

OASIS KMIP (Key Management Interoperability Protocol) 1.1 Specification compliant

AES 128, 192, 256 bit symmetric keys

RSA 1024, 2048, 3072, 4096 bit asymmetric keys

Secure key retrieval with TLS

Encrypt / Decrypt with AES 128, 192, 256

Encrypt / Decrypt with AES ECB and CBC modes of encryption

Maximum keys: Unrestricted

Maximum clients: Unrestricted

High availability mirroring for failover and load balancing; mirror selective keys; multiple mirror servers. Active-Active or Active-Passive.

Key access controls by user and group

Dual control

Server management via secure web browser

Key management via Windows GUI console

Systems management with syslog-ng, logrotate, etc.

Tamper-evident case (HSM only)

---

**Validations**

FIPS-140-2 Level 1

AES Validation for 128, 192, 256-bit keys

RNG validation

SHA validation

HMAC validation

CE, FCC, RoHS

---

**Network Management**

NTP, Syslog-ng, automatic log rotation, secure encrypted and integrity checked backups

---

**Hardware Security Module**

1U Rackmount Chassis

- **Memory:** 8GB DDR4 ECC RAM
- **Processor:** Intel XEON E3-1220V5
- **Storage:** 2 x 128GB SSD, RAID, Hot Swap
- **Dimensions:** 16.8” (W) x 1.7” (H) x 16.8” (D)
- **Weight:** 37.0 lbs ship weight
- **Power:** Dual redundant 100/240 VAC (auto-range); 280W, 955 BTU/HR
- **Temperature:** 10°C ~ 35°C
- **Humidity:** 8 to 90%, non-condensing
- **Compliance:** CE, FCC, RoHS, VCCI
- **Rails:** 1 set of 2 rails, user specified

---

**Supported Cloud Platforms**

Amazon Web Services (AWS)

IBM Cloud for VMware

Microsoft Azure

Rackspace

VMware vCloud

VMware vCloud on AWS

---

**Supported Virtualization**

VMware
Native Database Support

**Microsoft SQL Server**
- Enterprise 2008+ or Standard 2019+ with EKM (TDE and Cell Level Encryption)

**IBM**
- DB2
- DB2/400 FIELDPROC

**Other Databases**
- MongoDB

Database/Application Support

**Microsoft SQL Server**
- 2005 All Editions
- 2008-2017 Express, Standard, Web Editions

**Other Databases**
- MySQL, SQLite, etc.

**Other Applications**
- Drupal

Languages

- Java
- Microsoft.NET (C#)
- C/C++
- Perl
- PHP
- RPG (IBM i)
- COBOL
- Python