Alliance Key Manager
Platforms, Applications, & SDKs

Alliance Key Manager = Strong Data Protection

Alliance Key Manager (AKM) provides the strong protection for encryption keys that is central to a secure encryption strategy. To help organizations rapidly deploy encryption for their applications and databases, Alliance Key Manager provides a number of encryption applications, software libraries, language SDKs, and sample code. These resources help organizations deploy encryption that is integrated with proper encryption key management.

Manage Risk and Meet Compliance

Alliance Key Manager is an encryption key manager that is available as a hardware security module (HSM), VMware, or in the cloud (Microsoft Azure, Amazon Web Services, vCloud, etc.) The solution 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, as well as meets emerging key management standards.

Townsend SECURITY

Compatible
Alliance Key Manager works with all major business platforms, cloud platforms, and leading encryption applications

OASIS KMIP (Key Management Interoperability Protocol) compliant

Cost-Effective
Affordable key management solution for any size Enterprise.

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

Deployment Options
- Hardware Security Module (HSM)
- VMware
- Cloud

www.townsendsecurity.com

724 Columbia Street NW, Suite 400, Olympia, WA 98501 | 800 357 1019 +1 360 359 4400 Fax 360 357 9047

Platforms

Hardware Security Module (HSM)

Alliance Key Manager allows you to easily and affordably meet encryption key management compliance requirements with a FIPS 140-2 compliant encryption key manager. Wherever your data is, Alliance Key Manager can protect it.

With built-in key replication, key retrieval, and administrative controls, Alliance Key Manager is a secure, reliable, and affordable key management solution for a wide variety of applications. Additionally, Alliance Key Manager supports on-appliance encryption and decryption services so that your encryption key is always kept separate from the data it protects.

VMware

Alliance Key Manager is available as a VMware virtual appliance. Using exactly the same software as the Hardware Security Module (HSM) with FIPS 140-2 compliance, the VMware instance can be deployed in your IT Data Center or in a cloud environment that supports the vCloud architecture. The VMware ESX, vSphere (ESXi), and vCloud platforms are supported by this option.

Cloud (AWS, Microsoft Azure)

Deployed as an AMI in Amazon Web Services or VM in Microsoft Azure, Alliance Key Manager in the cloud relies on the same FIPS 140-2 compliant technology as the company's flagship Alliance Key Manager HSM that is in use by over 3,000 customers worldwide. When Alliance Key Manager is launched for the first time, it will automatically generate a certificate authority, client-side credentials, and create encryption keys that you can immediately use with SQL Server, SharePoint, MySQL, and other applications you run in the cloud.

Libraries & SDKs

Windows .NET Client for C#	Perl
Java	IBM i RPG & COBOL
C/C++	IBM z COBOL
PHP & Python	Other Languages

Applications

Microsoft SQL Server

Alliance Key Manager includes the Key Connection for SQL Server application to help Microsoft users implement Transparent Data Encryption (TDE) and Cell Level Encryption (column level encryption) without the need for application development. This application installs as a service on SQL Server and provides the Extensible Key Management (EKM) provider software.

MongoDB

Alliance Key Manager for MongoDB offers unparalleled security, flexibility and affordability for all users of MongoDB Enterprise database. With no client-side software to install, you can deploy Alliance Key Manager anywhere you want - your IT data center, VMware deployment, and in the cloud.

VMware vSphere

Alliance Key Manager for vSphere Encryption enables VMware customers to use native vSphere and vSAN encryption to protect VMware images and digital assets while deploying a secure, compliant and affordable key manager. VMware customers can deploy multiple, redundant key servers as a part of the KMS Cluster configuration for maximum resilience and high availability.

Drupal CMS

Web developers using the popular Drupal CMS can deploy the Key Connection for Drupal module to implement strong encryption and key management for sensitive data. Townsend Security fully supports the Drupal Encrypt and Key modules and provides affordable key management options for Drupal customers.

IBM DB2 FIELDPROC

The Townsend Security Alliance AES/400 encryption solution automatically integrates with Alliance Key manager to provide automatic encryption using the IBM DB2 Field Procedures (FIELDPROC) exit point. IBM i customers can automatically encrypt multiple columns in a database table, including index columns, without application changes.