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), cloud HSM, VMware, or in the cloud (Microsoft Azure, Amazon Web Services, 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, HIPAA, and other privacy regulations, as well as meets emerging key management standards without putting business continuity at risk.

Townsend SECURITY

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

OASIS KMIP (Key Management Interoperability Protocol) 1.0 Specification 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)
- Cloud 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.

Cloud HSM

Consisting of a pair of production and high availability (HA) key servers, Alliance Key Manager Cloud HSM is hosted in geographically dispersed data centers under an ITIL-based control environment independently validated for compliance against PCI DSS and SOC frameworks. This option allows customers to meet the most stringent data security standards without having to deploy the key management solution in their own data center. Key servers are pre-positioned in the hosting data center for rapid deployment.

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, Oracle, SharePoint, MySQL, and other applications you run in the cloud.

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. With integrated support for multiple, redundant AKM key servers Microsoft customers can deploy encryption rapidly and without programming.

Drupal CMS

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

NetLib Encryptionizer

In partnership with NetLib, Townsend Security provides the Key Connection for Encryptionizer application to provide encryption key management for the NetLib Encryptionizer solution. As a plugin module, Key Connection for Encryptionizer is easy to install and provides compliant key management with Alliance Key Manager.

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.

Libraries & SDKs

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