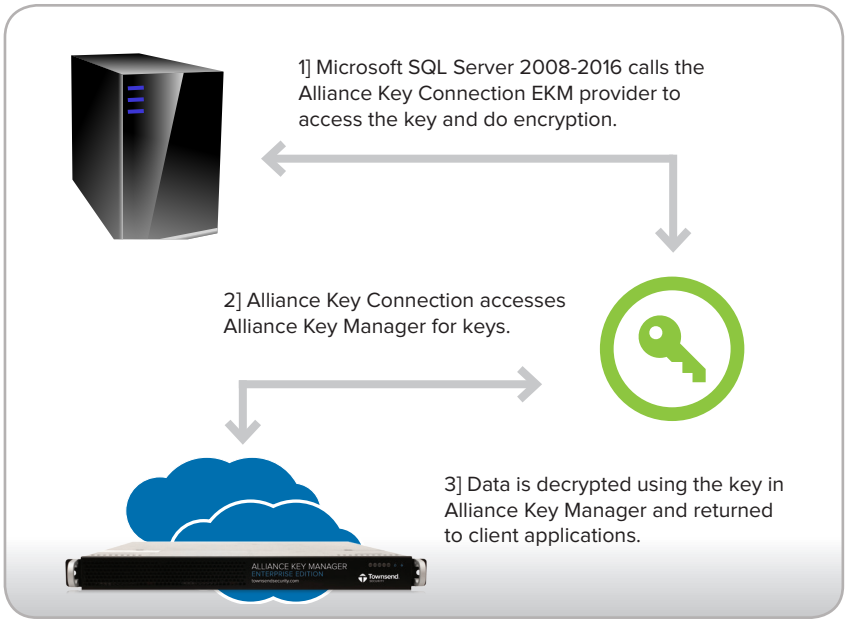
Alliance Key Manager for Microsoft SQL Server

Extensible Key Management (EKM)

Encryption Key Management for Compliance

Whether encrypting data with Transparent Data Encryption (TDE) or Cell Level Encryption on Microsoft SQL Server, managing the encryption keys with an encryption key manager is the best way to ensure the encrypted data remains secure. An encryption key manager will keep the encryption keys away from the encrypted data and address PCI-DSS, HIPAA, and other compliance requirements.

Alliance Key Manager easily integrates with Microsoft SQL Server 2008-2016 EKM and enables companies to address audit requirements for dual control and separation of duties by storing SQL Server 2008-2016 encryption keys securely with a FIPS 140-2 compliant key manager available as a hardware security module (HSM), Cloud HSM, VMware, or in the cloud (AWS, Microsoft Azrure, vCloud, etc.).



Townsend SECURITY

Cost Effective

Cost should not be a barrier to compliance. The cost model is built to scale from a single to multi-server environment. Any organization can now deploy a cost-effective, comprehensive and compliant solution to meet key management compliance requirements.

Meet Compliance Requirements for Separation of Duties & Dual Control

Store encryption keys and manage them separately from the encrypted data on a secure and certified solution. Enforce separation of duties and prevent administrators from having access to the encrypted data and encryption keys to meet compliance standards.

FIPS 140-2 Compliant

Assurance your key management solution has been validated to the highest standard for regulatory compliance.

Seamless Integration Protects SQL Server Encryption Keys

Alliance Key Manager connects effortlessly to the database and utilizes Microsoft's Extensible Key Management (EKM) capabilities to manage TDE and Cell Level encryption keys away from the protected data.

Automate Key Management Processes

Save time while addressing compliance requirements for key management. Automate all of your essential key management tasks including rotation, retrieval, and generation, for one server or many, in a central location.

www.townsendsecurity.com

724 Columbia Street NW, Suite 400, Olympia, WA 98501 | 800.357.1019 +1 360.359.4400 Fax 360.357.9047

Separate Key from Protected Data

Meet compliance requirements (PCI DSS, etc.) and enforce separation of duties and dual control for key management by storing encryption keys away the protected data. Alliance Key Manager easily connects with the Extensible Key Management (EKM) functionality in SQL Server 2008-2016, enabling administrators to centrally manage and secure keys outside of the database.

SQL Server TDE

Alliance Key Manager for SQL Server 2008-2016 includes native support for Transparent Data Encryption (TDE). When using TDE with SQL Server, the entire table space is automatically encrypted with no application changes required. The encryption key used to protect the SQL Server database is protected by an RSA key stored on the Alliance Key Manager HSM. Automatic failover to one or more High Availability key servers is supported. The Alliance Key Manager EKM provider software integrates with the Windows Certificate Store for Certificate Authority (CA), certificates, and private keys.

SQL Server Cell Level Encryption

Alliance Key Manager for SQL Server includes native support for Cell (column) Level Encryption. Cell level encryption requires changes to your SQL statements to integrate with the Alliance Key Manager EKM provider and key manager. Cell level encryption protects the specific column in the database and the other columns remain unencrypted. The symmetric key used by cell level encryption is stored on and protected by the key manager. Automatic failover to one or more High Availability key servers is supported. The Alliance Key Manager EKM software integrates with the Windows Certificate Store for Certificate Authority (CA), certificates, and private keys.

Key Change and Rotation Meet PCI Data Security Standards (PCI DSS)

Key rotation for TDE is fully supported. You can also automatically or manually rotate encryption keys when using cell level encryption. Security administrators can define the frequency of key rotation based on internal security policies. When a key change occurs, the new version is created and the old version is available for cryptographic operations.

Simplified Central Administration

An intuitive GUI application allows Security Administrators to easily create and manage encryption keys and access policies on the key manager. All access to security administration is authenticated using SSL/TLS client and server authentication, enabling multiple security administrators to log in and meet compliance regulations for dual control.

Windows Certificate Store Integration

Certificates used to authorize and authenticate a connection to the key server are stored in and protected by the Windows certificate store. Key Connection on the Windows platform handles certificate import, configuration, and security settings.

Key Caching for Application Resilience

Encryption keys can be retrieved and securely cached locally on the Windows server to reduce the impact of a failed network connection to the key manager. Key policy information is refreshed, and can be cleared on demand. This intelligent caching improves the resilience and performance of the key management strategy.

Key Mirroring for High Availability

Alliance Key Manager automatically mirrors EKM policies and encryption keys to one or more secondary key managers. In the event of a failover of a SQL Server instance or a key manager, the information is available for continued operation.

Platforms

Alliance Key Manager for SQL Server is offered as a Hardware Security Module (HSM), Cloud HSM, VMware, or in the Cloud (AWS, Microsoft Azure).

Townsend Security

Townsend Security provides data encryption & tokenization, key management, secure communications, and compliance logging solutions to Enterprise customers on a variety of server platforms including IBM i, IBM z, Windows, and Linux. The company can be reached on the web at www.townsendsecurity.com, or (800) 357-1019.