PRODUCT SHEET

Alliance Key Manager by Townsend Security

Alliance Key Manager Means Strong Data Protection

Alliance Key Manager by Townsend Security 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 a FIPS 140-2 compliant encryption key manager. The solution easily integrates with your databases/ applications and enables you to address audit requirements for encryptionand key management as found in PCIDSS, GDPR, HIPAA, and other privacy regulations, as well as meets emerging key management standards without putting business continuity at risk.

Compatible

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

FIPS 140-2 compliant

OASIS KMIP (Key Management Interoperability Protocol) compliant

Cost-Effective

Affordable key management solution for any size Enterprise with no additional client-side license or usage fees

Easy to Use

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

Deployment Options

- Hardware Security Module (HSM)
- VMware
- Cloud (AWS, Microsoft Azure)

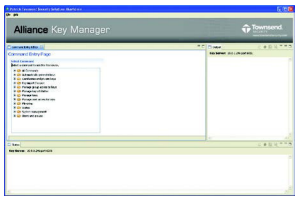
Key Management

Alliance Key Manager by Townsend Security generates symmetric encryption keys for all AES key sizes including 128-bit, 192-bit, and 256-bit encryption keys. Encryption keys are generated using a cryptographically secure pseudo-random number generator (CSPRNG) and are stored in a secure database. All encryption keys are protected by two layers of encryption as well as SHA-256 hash verification to prevent key corruption and key substitution. Encryption keys can be used with a wide variety of encryption algorithms such as AES, Blowfish, Twofish, and others.

Encryption keys can be either expiring or non-expiring to enforce key access policies as defined by the security administrator. Additionally, encryption keys can be created in advance of use and only available at a pre-determined future date. Encryption key management is restricted to the security administrator and all key management activity is logged to the system log audit trail.

Administration

Key management administration is provided through an application that uses a secure and authenticated TLS connection. Alliance Key Manager restricts the administrator session to a separate and private ethernet port on the server. Security administrators use the console to configure key management services, manage encryption keys, import and export keys, and backup the key database. All administrator functions are recorded by the system logging facility.



To support the special needs of OEM and ISV partners, Alliance Key Manager provides a programmable interface to all key management administrative functions. This means that key management can be automatically driven by applications and external systems.

Secure Key Retrieval

Applications retrieve encryption keys from the Alliance Key Manager server through a secure and mutually authenticated TLS TCP connection. Both the client and the server authenticate each other using standard TLS certificate exchange. This is the highest level of authentication necessary for complete end point security. Keys can be retrieved in three formats including Binary, Base16, and Base64 encoded for applications that cannot receive binary information.

Redundancy & Mirroring

Alliance Key Manager mirrors keys between multiple key management applications over a secure and mutually authenticated TLS connection for hot backup and disaster recovery support.

System & Compliance Logs

Alliance Key Manager creates system logs and a compliance audit trail that can be automatically transmitted to a log consolidation server or SIEM product. Logs are synchronized with an external time source and implement hash validation to prevent corruption of the log. For problem analysis, a user-enabled trace facility records the detailed activity of the server.

User & Group Control for Key Access

Security administrators can enforce user and group level controls over access to encryption keys. Encryption keys can be restricted to a specific list of users, a specific list of groups, or specific users within a group. Alliance Key Manager uses the distinguished name in certificates to enforce user and group controls which reduces administrative time and cost.

Ready to Use (RTU)

When Alliance Key Manager is launched for the first time, it will automatically generate a certificate authority, clientside credentials, and create encryption keys that you can immediately use with SQL Server, Oracle, MySQL, and other applications where you are encrypting data.

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. The solution has been validated for PCI DSS in VMware by Coalfire, a PCI-qualified QSA assessor and independent IT and audit firm.

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, 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.

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.

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.

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

Syncsort's Assure 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#
- Java I
- C/C++
- PHP & Python
- Perl
- BM i RPG & COBOL
- IBM z COBOL
- Other Languages

Key Change & Rotation

Automatically or manually rotate encryption keys. 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 moved to a historical database and available for cryptographic operations.

On-Board Encryption Services

For applications that require the highest level of security, you can use the on-board encryption and decryption services. The encryption key never leaves the key manager with onboard encryption services.

Technical Specifications

Features

- AES 128, 192, 256 bit 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, active-active, mirroring for failover and load balancing
- Key access controls by user and group
- Dual control Server management via secure web browser
- Systems management with syslog-ng, logrotate, etc.
- Tamper-evident case option for HSM

Certifications & Validations

- NIST AES compliance (ECB and CBC modes of encryption)
- NIST SHA validation
- NIST compliant RNG (x9.31)
- NIST HMAC validation
- NIST FIPS 140-2, level 1
- RoHS compliant, FCC, CE

Interfaces

- TLS authenticated secure communications
- GUI console for key management
- Secure web application for server management