Alliance Key Manager
Solution Brief

Enterprise Encryption Key Management

On the road to protecting sensitive data assets, data encryption remains one of the most difficult goals. A major barrier to achieving encryption has been the lack of an affordable Enterprise encryption key management solution — until now.

Alliance Key Manager (AKM) is a solution that provides Enterprise customers, OEMs, and ISVs with a secure method of managing encryption keys for their data security applications. Alliance Key Manager deploys as a key server appliance in any data center environment. With built-in key replication, key retrieval, encryption and administrative controls, Alliance Key Manager is a secure, reliable, and affordable key management solution for a wide variety of applications.

About 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, Linux, and UNIX. The company can be reached on the web at www.townsendsecurity.com, or (800) 357-1019.

Townsend SECURITY

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.

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

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

www.townsendsecurity.com

Key Management

Alliance Key Manager 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.

Key Naming and Versioning

When a security administrator creates a key it is given a user-friendly name. The encryption key is referred to by this name for all key management and key retrieval operations. A key is also automatically assigned a version name. The key name will remain the same throughout the life of the key. A new version name will be assigned each time the key is manually or automatically changed. An historical database of previous versions is maintained to allow older versions of the key to be used for cryptographic operations.

Key Change and Rotation

New encryption keys can be manually created by the security administrator, or can be automatically generated by Alliance Key Manager. For automatically generated keys the security administrator defines the frequency of key rotation. When a key change occurs, the new version is created and the old version is moved to the historical database. Old versions are available for cryptographic operations based on security administrator policy.

Key Encryption Keys (KEK) can be rotated at any time by the cryptographic security administrator. The data encryption keys are re-encrypted with new KEK to meet compliance regulations such as PCI Data Security Standards.

Secure Key Retrieval

Applications retrieve encryption keys from the Alliance Key Manager server through a secure and mutually-authenticated TLS 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.

A standard request/response data protocol is used in a single session environment for key requests and delivery. Permanent TCP sessions are not allowed and sensitive data is never communicated in the clear. Key retrieval libraries and sample application code are provided for all of the major Enterprise servers such as Windows, Linux, AIX, Solaris, IBM I, and IBM z. Assistance and documentation is available to enable key retrieval on other platforms. Encryption keys can be retrieved in one of three formats: Binary, Base16 encoded (also known as hex encoded), and Base64 encoded. The last two data formats are designed to be friendly to applications that cannot receive binary information.

On-Device Encryption

Alliance Key Manager supports NIST-validated on-device encryption so that encryption keys never have to leave the device. This is an attractive option for Internet-facing web applications that process sensitive data. When there is more risk of exposure of encryption keys, you can use on-device encryption which never exposes encryption keys in the user application environment. All data to be encrypted or decrypted is protected by mutually authenticated TLS encrypted communications.

Key Mirroring

Alliance Key Manager can automatically mirror encryption keys to one or more instances of Alliance Key Manager for hot backup and disaster recovery support. Key mirroring is accomplished over a secure and mutually-authenticated TLS connection. Mirroring is real-time and bi-directional to support the deployment of complex mesh and hub-and-spoke networks of servers.

In addition to backup and recovery support, key mirroring provides load balanced key retrieval operations in environments where there is a high volume of key retrieval activity.

Key Metadata

The encryption key store supports up to 16 fields of user data. This is any information that a customer, OEM, or ISV wants to associate with an encryption key. Metadata expands the flexibility of key management for special uses in areas such as payment systems and tape archival. Alliance Key Manager supports query operations against the key store based on the contents of the metadata.

Key Import and Export

The security administrator can import and export encryption keys through the security administrator console. Key export can be used to transfer encryption keys to non-networked devices such as stand-alone point-of-sale terminals, or to vendors or customers outside of the organization. Encryption key import enables a customer to receive encryption keys from vendors and customers outside of the Enterprise. Binary, Base16, Base64, and RSA encrypted formats are supported for key import and export operations.

Password and Pass Phrase Protection

In addition to managing encryption keys, Alliance Key Manager can receive and store pass phrases used in application programs. The same key retrieval interface is used for pass phrase retrieval as for encryption key retrieval. By using AKM for pass phrase management you can avoid storing pass phrases in user application code or unsecured database files.

User and 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.

Administration

Key management administration is provided through a Windows GUI application 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.

General system administration is restricted to the security administrator and protected by TLS encryption. No general <root> access is allowed to the system, and all activity is recorded by the system logging facility. General system administration includes tasks such as configuring IP addresses, system logging, etc.

To support the special needs of OEM and ISV partners, Alliance Key Manager provides a programmable interface to all key management administrative functions.

Platforms

Hardware Security Module (HSM)

Alliance Key Manager is provided on a reliable appliance platform with dual disks, RAID protection, dual power supplies, and flexible hardware support options. A one-year warranty is included with the server. Customers can elect to have the servers delivered, installed, and configured through a comprehensive installation program.

Cloud HSM

Alliance Key Manager is available as a dedicated, cloud HSM in our contracted hosting facility. The hosting provider is PCI DSS certified for their data center infrastructure allowing you to fully comply with PCI data security mandates while deploying an affordable solution. This option allows cloud application providers 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. Alliance Key Manager in VMware can help you meet PCI Data Security Standards for encryption key management when deployed according to the PCI virtualization guidelines. The VMware ESX, vSphere (ESXi), and vCloud platforms are supported by this option.

Amazon Web Services

Deployed as an AMI in Amazon Web Services, Alliance Key Manager for AWS 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 for AWS 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 AWS.

Microsoft Azure

The same FIPS 140-2 validated key management solution available in Townsend Security's hardware security module (HSM) can also run as a virtual machine in Microsoft Azure. You can easily deploy the best encryption key management solution for your cloud applications directly in Microsoft Azure and leverage all of the management options provided by Microsoft.

IBM Cloud

As enterprises adopt Public and Private clouds, they bring their sensitive data with them – customer names, email addresses and other personally identifiable information (PII). While compliance regulations require protecting this information, encrypting this data has been a challenge for organizations who store sensitive data in the cloud. By deploying Alliance Key Manager for IBM Cloud, customers can achieve their security and efficiency goals in a cloud environment.

IBM PureSystems

Alliance Key Manager enabled on IBM PureFlex System includes integrated patterns of expertise designed to automate and optimize the deployment and maintenance of workloads. Deployment expertise can accelerate your time to value up to 100 times versus traditional systems. Consolidation and management expertise drives automation to significantly reduce manual processes that consumes too many staff hours. Optimization expertise also allows the infrastructure to flex to unexpected demands without requiring expensive surplus capacity. This system is designed to provide a simplified experience and reduce IT complexity without compromising flexibility.

Systems Management

Alliance Key Manager integrates with the native syslog-ng system logging facility of the operating system and captures all key retrieval, key management, and system administration activity. Alliance Key Manager can report all system logs to a central log management and alerting facility, or SIEM product, for a permanent audit trail of key management activity.

Because system log time stamps are important for accurate audit trails of activity, Alliance Key Manager implements a time synchronization facility. Time synchronization is configured and activated through the administrator's console.

Encryption key server backup is provided through a security administrator console option. Backups can be created on the key server disk and copied to a secure backup facility.

Certifications

NIST FIPS-140-2 Level 1
NIST AES Validation
NIST SHA Validation
NIST compliant RNG (x9.31)
NIST HMAC Validation

OEM and ISV Support Program

Many OEMs and ISVs implement strong encryption to protect user data, but use insecure methods for creating, storing, and distributing encryption keys. The Townsend Alliance Partner program provides OEMs and ISVs with a partner-friendly method of deploying Alliance Key Manager with their existing applications. The partner program provides training, best practices consultation, and products to the OEM and ISV to ensure success with key management solutions.

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.