Alliance Key Manager & The Cloud

Cloud Security Alliance "Security Guidance"

The Cloud Security Alliance and Alliance Key Manager

The Cloud Security Alliance (www.cloudsecurityalliance.org) is an independent organization of cloud vendors, users, and security experts whose mission is "To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing." As a part of this mission the organization has published a Security Guidance document to help vendors and customers achieve more secure applications in cloud environments. The published guidance is now in its second edition and is available from the organization's web site.

The guidance provides recommendations for encryption key management in the section "Domain 11 – Encryption and Key Management". In this document we show how Alliance Key Manager from Townsend Security helps meet the recommendations of the Cloud Security Alliance.

Townsend SECURITY

Affordable
Alliance Key Manager is available in affordable deployment options:

- Hardware Security Module (HSM)
- VMware virtual appliance
- Hosted in PCI certified infrastructure
- Cloud-based solution - Multi-tennant, Virtual Private Cloud, or Dedicated

Reliable
Hardware and software redundancy insure that you will never lose encryption services or encryption keys. Redundancy is provided through:

- Dual RAID controlled disk drives and dual power supplies
- Real time, bi-directional key mirroring
- On demand and scheduled backups
- High availability hot failover
- Load balancing support

FIPS 140-2 Compliant
Meets Level 1 compliance (certificate #1449)

www.townsendsecurity.com

724 Columbia Street NW, Suite 400, Olympia, WA 98501 | 800 357 1019 +1 360 359 4400 Fax 360.357.9047

Domain 11 - Encryption & Key Management (extract)

Key Management: Existing cloud service providers may provide basic encryption key schemes to secure cloud based application development and services, or they may leave all such protective measures up to their customers. While cloud service providers are progressing towards supporting robust key management schemes, more work is needed to overcome barriers to adoption. Emerging standards should solve this problem in the near future, but work is still in progress. There are several key management issues and challenges within Cloud Computing:

Secure key stores. Key stores must themselves be protected, just as any other sensitive data. They must be protected in storage, in transit, and in backup. Improper key storage could lead to the compromise of all encrypted data.

Alliance Key Manager protects all data encryption keys in storage using key-encryption keys and authentication keys per NIST recommendations. Key retrieval, distribution, and mirroring is performed using secure and mutually authenticated SSL/TLS communications. All backups of the key server are encrypted with separate keys, and key-encrypting keys are backed up separately from data-encrypting keys.

Access to key stores. Access to key stores must be limited to the entities that specifically need the individual keys. There should also be policies governing the key stores, which use separation of roles to help control access; an entity that uses a given key should not be the entity that stores that key.

Alliance Key Manager provides separation of roles between key users and security administrators, with dual control of security administration functions. Alliance Key Manager supports the separate of key storage from the entity that uses the key.

Key backup and recoverability. Loss of keys inevitably means loss of the data that those keys protect. While this is an effective way to destroy data, accidental loss of keys protecting mission critical data would be devastating to a business, so secure backup and recovery solutions must be implemented.

Alliance Key Manager implements additional encryption for backup and recovery of the key store. Additionally, the backup of the data-encrypting keys is separated from the backup of the key-encrypting keys so that the backup images can be stored in physically separate locations.

There are a number of standards and guidelines applicable to key management in the cloud. The OASIS Key Management Interoperability Protocol (KMIP) is an emerging standard for interoperable key management in the cloud. The IEEE 1619.3 standards cover storage encryption and key management, especially as they pertain to storage IaaS.

Alliance Key Manager conforms to the NIST FIPS 140-2 standard for cryptographic modules, and is FIPS 140 certified. Additionally, AKM supports the KMIP specification for key retrieval, key import and export, and key creation in Alliance Key Manager 3.0 and above.

Recommendations

In this section we present each recommendation from the Cloud Security Alliance, and document how Alliance Key Manager helps cloud providers and end customers meet these recommendations.

Use encryption to separate data holding from data usage.

Alliance key manager implements NIST best practices for encryption of key material and separates data-encrypting keys from key-encrypting keys. Cloud providers and end users can protect data at rest to separate and control data holding from data usage (non-active instances of data, backup images, etc.)

Segregate the key management from the cloud provider hosting the data, creating a chain of separation. This protects both the cloud provider and customer from conflicts when compelled to provide data due to a legal mandate.

Alliance Key Manager customers have a number of options available to meet this recommendation. AKM can be hosted on a different cloud vendor's platform where there is confidence in the ability to manage the legal mandates. Or, customers can host the Alliance Key Manager in a Virtual Private Cloud (VPC), Enterprise private cloud environment, or in their own IT infrastructure. Any platform can be used where the concerns about legal mandates are clear.

When stipulating encryption in the contract language, assure that the encryption adheres to existing industry and government standards, as applicable.

Alliance Key Manager adheres to the National Institute of Standards and Technology (NIST) best practices for encryption key management, and is FIPS-140-2 Level 1 certified (In Process). Customers can rest assured that their deployments of Alliance Key Manager will help them meet PCI Data Security Standards (PCI DSS), HIPAA and HITECH

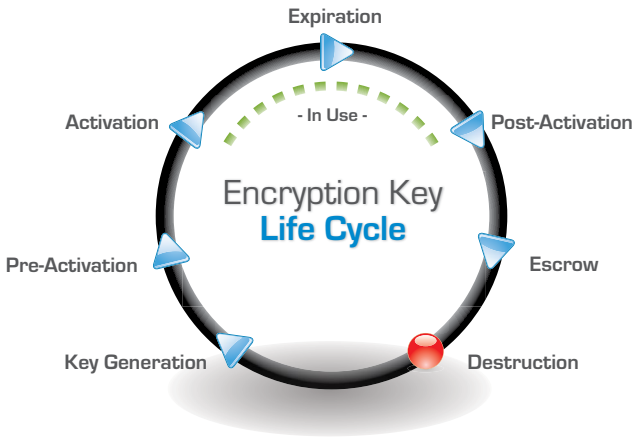
data security standards, and state and federal privacy mandates for encryption key management.

Understand whether and how cloud provider facilities provide role management and separation of duties.

Regardless of the platform where Alliance Key Manager is deployed, the solution meets NIST standards for role management and separation of duties. Configuration options allow requiring two independent log-ins for security administrators who manage keys. Key users are separated from key managers using PKI infrastructure and additional key server controls.

In cases where the cloud provider must perform key management, understand whether the provider has defined processes for a key management life cyle: how keys are generated, used, stored, backed up, recovered, rotated, and deleted. Further, understand whether the same key is used for every customer or if each customer has its own key set.

Townsend Security works with cloud providers to enable proper key management services and best practices. For cloud providers who do not offer key management services, or cannot meet industry best practices for key management, Townsend Security can work with end customers to provide an alternative that meets regulatory requirements. Alliance Key Manager implements NIST recommendations for key lifecycle processes and controls.



Assure regulated and/or sensitive customer data is encrypted in transit over the cloud provider's internal network, in addition to being encrypted at rest. This will be up to the cloud customer to implement in IaaS environments, a shared responsibility between customer and provider in PaaS environments, and the cloud provider's responsibility in SaaS environments.

Alliance Key Manager enforces encrypted transfer of encryption keys as they are delivered to applications in the cloud. AKM also helps customers protect data as it moves over the cloud internal network by supporting encryption at the source, and decryption at the destination.

End customers using different operating systems in the cloud can use AKM as the central key repository for all environments.

In IaaS environments, understand how sensitive information and key material otherwise protected by traditional encryption may be exposed during usage. For example, virtual machine swap files and other temporary data storage locations may also need to be encrypted.

Alliance Key Manager implements a state-less, thread-based architecture for key management and key retrieval functions. There are no communication sessions or temporary files that contain unprotected key material or other sensitive information which could lead to loss during periods of low activity when the application may be swapped out of main memory. Cloud providers can implement protection of swap files and other temporary storage and know that there will not be additional potential losses from the key manager.

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.