White Paper

Encryption Key Management in the AWS Cloud

www.townsendsecurity.com

724 Columbia Street NW, Suite 400 • Olympia, WA 98501 • 360.359.4400 • 800.357.1019 • fax 360.357.9047 • www.townsendsecurity.com

Introduction

At the Amazon re:Invent summit of 2014 the Amazon Web Services group announced a new AWS Key Management Service (AWS KMS). Positioned as a cost effective method of generating encryption keys and the enablement of an encryption service, AWS customers are asking how this new service affects them and how they can evaluate its use in their AWS applications.

While the new AWS Key Management Service will help some AWS customers better protect their sensitive data in the AWS cloud, it will not meet minimum standards and security requirements for many organizations, and it will lock customers and partners into the Amazon cloud platform. Selecting a key management system is the most important part of an encryption strategy. This document identifies some key issues with the new AWS KMS service and how the Townsend Security key management solution, Alliance Key Manager for AWS, addresses these issues.

Management of Key Encryption Keys (KEK)

The AWS KMS service implements a layered combination of Hardware Security Modules (HSMs) and multi-tenant virtual software appliances called Hardened Security Appliances (HSAs) to protect key encryption keys. While these KEK keys are protected with redundant, mirrored HSMs, they do not implement all of the common key management functions normally found in professional key management systems. The AWS KMS hardware security modules that maintain the root KEK remains under the exclusive control of, and administration by, Amazon and cannot be managed by AWS customers.

> Unlike the AWS KMS service, Alliance Key Manager for AWS puts the control of Key Encryption Keys fully under the AWS customer's control. Key Encryption Keys are not managed by Amazon and are not accessed or managed by Townsend Security. Only the AWS customer can manage Key Encryption Keys.

Management of Data Encryption Keys (DEK)

When data encryption keys are generated and retrieved from the AWS KMS service, they are not stored and managed within the HSA/HSM environment. Keys are exported to the end-customer's EC2 instance and the customer must manage the life cycle of the DEK. While the DEK is encrypted with a Customer Master Key stored on the HSA, the DEK is stored and exposed to loss in the end-customer EC2 environment. AWS customers must implement appropriate procedures for backup and restore, activation, de-activation, escrow, and related steps. The AWS KMS protection of DEK does not follow recognized industry standards.

> Alliance Key Manager generates, stores, protects, and manages DEK through the life cycle of the key according to industry standards. Web and key management interfaces to the key manager separate functions so that Network Administration and Crypto Security Administration enforces Separation of Duties and Dual Control of key management functions.

Multi-Tenant Key Management

Like most services provided by AWS, the key management service is multi-tenant. That is, many different AWS customers use the HSAs that provide the key management service. This means that multiple AWS customers in addition to you use the same key management HSA instance, and that both trusted and untrusted environments may access the same AWS key management service. It is not possible to deploy the AWS Key Management Service as a dedicated AWS instance, or as a dedicated, non-shared virtual private cloud service.

> Alliance Key Manager runs as a dedicated EC2 instance without multi-tenant application or key sharing. All encryption keys and access policy are dedicated to the AWS customer. Alliance Key Manager can be deployed in an AWS virtual private cloud environment and isolated using AWS segmentation.

Cross-Region Key and Access Control Mirroring

The AWS Key Management Service provides for redundancy and failover within a single AWS region. However, it is not possible to provide redundancy and failover of the AWS KMS across regions. For most AWS customers, the ability to failover to another AWS region is a core aspect of their high availability and business recovery strategy. Without the ability to mirror AWS KMS keys and policy across regions the AWS customer's environment is at risk of catastrophic interruption.

> Alliance Key Manager fully supports cross-region mirroring of encryption keys and key access policies, with support for mirroring to multiple regions simultaneously. You can also mirror keys to secondary key servers located outside of AWS in your own data center or a hosting facility.

© 2017 Townsend Security

Cross-Cloud and Extra-Cloud Key Management

The AWS KMS service is tied to the Amazon Web Services cloud infrastructure. Applications that are external to AWS cannot access these services, and the interface to the AWS KMS service is not implemented anywhere outside of the Amazon cloud. Additionally, key encryption keys are restricted to the AWS cloud environment and cannot be mirrored to external key management systems. Using the AWS KMS service locks you into the Amazon cloud platform.

Alliance Key Manager for AWS fully supports cross-cloud and outside-of-the-cloud key management integration. You can share the Alliance Key Manager instance with external applications and you can mirror encryption keys and access policies to other cloud service provider platforms, external cloud HSMs, and user-deployed HSMs and VMware instances in hosted or private data centers. Alliance Key Manager preserves your independence from any cloud service provider and provides for enterprise Hybrid cloud implementations.

Hybrid Cloud Key Management

Many organizations are deploying Hybrid clouds to achieve better security, integration with core, non-cloud back-office applications, and as a part of a cloud migration strategy. The AWS KMS only runs in the AWS environment and does not provide encryption key management and access control for external user applications. This means that AWS customers must have multiple, incompatible key management systems thus increasing risk and adding complexity and cost.

Alliance Key Manager deploys across all aspects of the Hybrid cloud environment supporting AWS cloud instances, other cloud platforms, external Cloud HSMs, traditional HSMs and VMware implementations. All Alliance Key Manager platforms use the same management and key usage interfaces making integration and migration of applications and encryption key management easy to achieve.

Dedicated Customer Key Management and Administration

The AWS Key Management Service is a combination of Amazon controlled and managed back-end systems and customer managed keys. The AWS customer has no control or knowledge of administrative activities performed by Amazon. Activities performed by Amazon may include maintenance of HSMs, re-establishment of key encryption keys, and legally required surrender of key material to governmental or law enforcement agencies.

Alliance Key Manager system administration and key management is dedicated to you, the AWS customer, and is not managed or controlled by Townsend Security or by Amazon. Neither Amazon nor Townsend Security have direct access to your encryption keys. Townsend Security cannot provide governmental agencies or law enforcement agencies access to your keys.

User Controlled Key Backup and Restore

The AWS Key Management Service splits encryption key backup and restore responsibilities between you and Amazon. Amazon is responsible for backup and restore of the HSMs and Key Encryption Keys (KEK). You are responsible for backup and restore of the Data Encryption Keys (DEK). When you generate keys for retrieval and storage in your AWS instance, you must backup the keys and restore them as appropriate. Processes you implement can only recover the loss of a data encryption key.

Alliance Key Manager provides backup and restore facilities for both Key Encryption Keys (KEK) and Data Encryption Keys (DEK). In the event of a catastrophic loss of your AWS application, your keys are fully backed up to external storage that you specify. Additionally, Alliance Key Manager provides real-time mirroring of encryption keys and access policies to one or more failover key servers. These failover key servers can be in the AWS cloud or external to the cloud.

Key Management System Logs

Key management systems are critical components of your business application environment, and active monitoring of all components in this environment is crucial to a good security strategy. While the AWS KMS service provides audit logs of key use, AWS KMS customers do not have ready access to the system logs of the hardened security appliances (HSAs) and hardware security modules (HSMs) that make up the service. Additionally, AWS customers have no access to the virtualization and operating system logs. This defeats a critical part of the security of your application.

Alliance Key Manager provides audit logs, web logs, and system logs directly available to AWS customers so that they can implement active monitoring of the key management system to meet security best practices and compliance regulations. These logs can be sent in real time to a log collection or SIEM solution in the AWS cloud, or external to the cloud.

© 2017 Townsend Security

KMIP Standard Key Management

Industry standards are important for customers who want to achieve good security and a measure of independence from any one key management vendor. The OASIS Key Management Interoperability Protocol (KMIP) is an important key management industry standard that is supported by all professional key management systems. The AWS KMS service does not support the KMIP standard, providing only a proprietary interface.

Alliance Key Manager supports the OASIS KMIP standard and provably interoperates with a variety of third party applications.

Bring Your Own Keys

AWS Key Management Service supports the concept of "Bring your own keys". This is a KMS key import service that allows you to create a data encryption key outside of the AWS cloud platform and import it into the KMS service. While the ability to import a key to KMS is somewhat helpful from a key custody point of view, it suffers many limitations including the lack of full lifecycle key management, shared and non-transparent administration, full system logging of key access, poor cross-region and non-cloud key mirroring, and the lack of access to key encryption keys. Further, periodic rotation of keys requires manual intervention by the AWS customer.

As mentioned above Alliance Key Manager provides a complete lifecycle management approach to key management in the AWS cloud. With dedicated key management and administrative services you have full control over your encryption key strategy and can easily mirror keys into and out of the AWS cloud.

FIPS 140-2 Compliance

Encryption key management systems perform a critical role in the protection of sensitive data. They should implement provably strong, standard encryption methods, generate cryptographically strong encryption keys, and properly protect the keys from corruption and loss. All professional key management solutions are validated to the National Institute of Standards and Technology FIPS 140-2 standard through a NIST validation process. While FIPS 140-2 validation is not currently possible in cloud environments, good cloud key management solutions will use FIPS 140-2 validated applications. The AWS KMS system has not been validated to this standard.

Alliance Key Manager HSMs and Cloud HSMs are FIPS 140-2 compliant. The Alliance Key Manager for AWS solution runs the same binary identical key management application as the HSM solution. With Alliance Key Manager for AWS customers can have a high level of confidence in the key management implementation and the cryptographic functions provided by AKM.

Summary

AWS customers and partners who need to control the encryption keys that protect their data in the AWS cloud, who need to meet industry standards for encryption and key management, who wish to retain independence from their cloud service provider, who need to properly secure and monitor the key management system, and who need a full encryption key life cycle management system will benefit from deploying Alliance Key Manager in the Amazon Web Services cloud.

Resources

Web Page: Alliance Key Manager for AWS

Podcast: Encrypting Data in AWS

Video: Alliance Key Manager for AWS

Townsend Security

Townsend Security creates data privacy solutions that help organizations meet evolving compliance requirements and mitigate the risk of data breaches and cyber-attacks. Over 3,000 companies worldwide trust Townsend Security's NIST and FIPS 140-2 compliant solutions to meet the encryption and key management requirements in PCI DSS, HIPAA/HITECH, FISMA, GLBA/FFIEC, SOX, and other regulatory compliance requirements.

You can contact Townsend Security for an initial consultation at the following locations:

Web: www.townsendsecurity.com
Phone: (800) 357-1019 or (360) 359-4400
International: +1 360 359 4400
Email: info@townsendsecurity.com
Twitter: @townsendsecure

© 2017 Townsend Security