White Paper

Encryption Key Management System vs Service:

KMS Differences Explained

Townsend SECURITY

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

In IT technology and security, the language and three-letter acronyms we use can sometimes make things more confusing than they need to be. That's true with encryption key management systems and services that are available today. So let's sort out the language, TLAs, and try to reduce some of the confusion in this area.

HINT: In the following discussion, pay special attention to the words ***"system***" and "***service***". I've added emphasis below to help with clarity.

Enterprise Key Management System

An Enterprise Key Management System is a security appliance (hardware or software) that manages encryption keys through their entire lifecycle - key creation, key activation, key use, key expiration or retirement, key escrow, and key destruction. The "Enterprise" part of this descriptive phrase is often dropped, and these types of system are often referred to as Key Management Systems. The word "Enterprise" is often used to indicate that the key management system can be used for a wide variety of purposes within an organization.

Key Management Systems may be hardware devices (usually hardware security modules, or HSMs), software appliances (think VMware virtual machines), or cloud instances. Their use is dedicated to a single organization and usually managed by security professionals within that organization providing the organization exclusive custody of the encryption keys. Key Management Systems are usually validated to the FIPS 140-2 standard by the National Institute of Standards and Technology (NIST).

Category: "Key Management System"; or "Enterprise Key Management System"

Three-Letter Acronym: Usually "KMS"; less frequently "EKMS"

Here at Townsend Security we provide our Alliance Key Manager as a Key Management System available as a Hardware Security Module (HSM), VMware virtual appliance, and as a dedicated cloud instance (Azure, AWS) and is FIPS 140-2 compliant.

Cloud Service Provider: Key Management Service

A cloud service provider's Key Management Service is generally a multi-tenant, encryption key storage service managed by the cloud service provider that provides a subset of encryption key lifecycle management. Administrative duties for encryption keys are a shared responsibility of the cloud service provider and the organization that uses the keys. This means that the organization is sharing custody (ownership and access) to encryption keys.

Cloud-based Key Management **Services** are not FIPS 140-2 validated, but may be partially backed by Key Management **Systems** which are. Examples of cloud service provider key management services include Amazon Web Services Key Management Service (AWS KMS), Microsoft Azure's Key Vault (Azure KV), and Google Cloud Platform's Customer-Managed Encryption keys (GCP CMEK, also known as GCP Cloud KMS).

The cloud service provider's use of the "KMS" acronym adds substantially to the confusion. Just remember that cloud service providers implement a multi-tenant, shared "**service**" and not a dedicated key management "**system**".

Category: "Key Management Service"; or "Cloud Key Management Service"

Three-Letter Acronym: Usually "KMS", "KV" or "CMEK"; less frequently "Cloud KMS"

Townsend Security is not a cloud service provider and does not provide multi-tenant, shared custody key management services.

ISV Solutions for the Cloud: Key Management Systems

Independent Software Vendors (ISVs) provide Key Management **Systems** that are not managed or accessed by the cloud service provider or the ISV, and which are dedicated to the user organization. This means that the cloud user is not sharing custody (ownership and access) to encryption keys and has full and exclusive management, ownership, and access to encryption keys. ISV cloud Key Management **Systems** provide support for the entire key management lifecycle including key creation (key establishment), key activation, key distribution, key backup and escrow, and key destruction.

ISV Key Management **Systems** are not FIPS 140-2 validated, but may be based on software that is FIPS 140-2 compliant.

An ISV's use of the "KMS" acronym more closely reflects the Enterprise Key Management System described above. These are key management systems that are dedicated to a single organization and which support the entire lifecycle of key creation, key distribution, and key escrow.

Category: "Key Management System"; or "Cloud Key Management System"

Three-Letter Acronym: Usually "KMS" or "Cloud KMS"

Townsend Security provides its Alliance Key Manager solution as a dedicated, single tenant, Key Management **System** on the Amazon Web Services and Microsoft Azure cloud platforms. The solution can be located in the relevant Marketplace.

Cloud Service Provider: Bring Your Own Key

One small variation on the theme of cloud service provider Key Management Services involves the ability to import your own encryption key to the cloud service. In this case the cloud service is not creating the encryption key for you, but is allowing you to bring an encryption key that you have created, or which you manage outside of the cloud, to the cloud's key management service. In this case the key you bring is imported into the multi-tenant, shared key management service and is then available through the cloud service provider key management service interface. Although you have exclusive control over the creation of the key and may store it outside of the cloud, it is important to remember that the storage and management of the imported encryption key is a shared responsibility between you and the cloud service provider. You do NOT have exclusive control of the key after it is imported to the cloud.

Category: "Key Management Service"; or "Cloud Key Management Service"; often "Bring Your Own Key" or "Customer-Supplied Encryption Key"

Three-Letter Acronym: "BYOK" or "CSEK" (Google Cloud Platform)

Townsend Security fully supports bringing your own key to Alliance Key Manager Key Management System for the Azure and AWS clouds. Key custody remains fully with the organization and is not shared with the cloud service provider nor with Townsend Security.

Summary

A rose is a rose is a rose.

However, a Key Management **Service** is NOT a Key Management **System**.

When discussing encryption key management care must be taken to understand the meaning of KMS. It can be quite different depending on the context. I hope this blog helps clarify the language and issues around key management.

About 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-validated 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.

We invite you to learn more about us and view comments on the latest happenings in the security and encryption space by going to our blog.