**AWS Key Management Service**

***SERVICE Description***

Easily create and control the keys used to encrypt or digitally sign your data.

***Brief explanation of the service***

A managed service that enables you to easily encrypt your data. KMS provides a highly available key storage, management, and auditing solution for you to encrypt data within your own applications and control the encryption of stored data across AWS services.

**Use cases / Considerations**

**Features**

* KMS is integrated with CloudTrail, which provides you the ability to audit who used which keys, on which resources, and when.
* Customer master keys (CMKs) are used to control access to data encryption keys that encrypt and decrypt your data.
* You can choose to have KMS automatically rotate master keys created within KMS once per year without the need to re-encrypt data that has already been encrypted with your master key.
* To help ensure that your keys and your data is highly available, KMS stores multiple copies of encrypted versions of your keys in systems that are designed for 99.999999999% durability.
* You can connect directly to AWS KMS through a private endpoint in your VPC instead of connecting over the Internet. When you use a VPC endpoint, communication between your VPC and AWS KMS is conducted entirely within the AWS network.
* You can define VPC Endpoint policies, enabling you to increase the granularity of your security controls by specifying which principals can access your endpoint, which API calls they can make, and which resources they can access.

**Concepts**

* **Customer Master Keys (CMKs)** – You can use a CMK to encrypt and decrypt up to 4 KB of data. Typically, you use CMKs to generate, encrypt, and decrypt the data keys that you use outside of KMS to encrypt your data. Master keys are 256-bits in length.
* There are three types of CMKs:

|  |  |  |  |
| --- | --- | --- | --- |
| **Type of CMK** | **Can view** | **Can manage** | **Used only for my AWS account** |
| Customer managed CMK | Yes | Yes | Yes |
| AWS managed CMK | Yes | No | Yes |
| AWS owned CMK | No | No | No |

* + ***Customer managed CMKs*** are CMKs that you create, own, and manage. You have full control over these CMKs, including establishing and maintaining their key policies, IAM policies, and grants, enabling and disabling them, rotating their cryptographic material, adding tags, creating aliases that refer to the CMK, and scheduling the CMKs for deletion.
  + ***AWS managed CMKs*** are CMKs in your account that are created, managed, and used on your behalf by an AWS service that integrates with KMS. You can view the AWS managed CMKs in your account, view their key policies, and audit their use in CloudTrail logs. However, you cannot manage these CMKs or change their permissions. And, you cannot use AWS managed CMKs in cryptographic operations directly; the service that creates them uses them on your behalf.
  + ***AWS owned CMKs*** are not in your AWS account. They are part of a collection of CMKs that AWS owns and manages for use in multiple AWS accounts. AWS services can use AWS owned CMKs to protect your data. You cannot view, manage, or use AWS owned CMKs, or audit their use.
* **Data keys** – Encryption keys that you can use to encrypt data, including large amounts of data and other data encryption keys.
  + You can use CMKs to generate, encrypt, and decrypt data keys. However, KMS does not store, manage, or track your data keys, or perform cryptographic operations with data keys.
  + Data keys can be generated at 128-bit or 256-bit lengths and encrypted under a master key you define.
* **Key Policies** – When you create a CMK, permissions that determine who can use and manage that CMK are contained in a document called the key policy.
* **Grants** – A grant is an alternative to the key policy. You can use grants to give long-term access that allows AWS principals to use your customer managed CMKs.
* **Grant Tokens** – When you create a grant, the permissions specified in the grant might not take effect immediately due to eventual consistency. If you need to mitigate the potential delay, use a grant token instead.
* When you enable ***automatic key rotation*** for a customer managed CMK, KMS generates new cryptographic material for the CMK every year. KMS also saves the CMK’s older cryptographic material so it can be used to decrypt data that it encrypted.
* An *alias* is an optional display name for a CMK. Each CMK can have multiple aliases, but each alias points to only one CMK. The alias name must be unique in the AWS account and region.

**Importing Keys**

* A CMK contains the **key material** used to encrypt and decrypt data. When you create a CMK, by default AWS KMS generates the key material for that CMK. But you can create a CMK without key material and then import your own key material into that CMK.
* When you import key material, you can specify an expiration date. When the key material expires, KMS deletes the key material and the CMK becomes unusable. You can also delete key material on demand.

**Deleting Keys**

* Deleting a CMK deletes the key material and all metadata associated with the CMK and is irreversible. You can no longer decrypt the data that was encrypted under that CMK, which means that data becomes unrecoverable.
* You can create a CloudWatch alarm that sends you a notification when a user attempts to use the CMK while it is pending deletion.
* You can temporarily disable keys so they cannot be used by anyone.
* KMS supports custom key stores backed by AWS CloudHSM clusters. A key store is a secure location for storing cryptographic keys.
* You can connect directly to AWS KMS through a private endpoint in your VPC instead of connecting over the internet. When you use a VPC endpoint, communication between your VPC and AWS KMS is conducted entirely within the AWS network.

**Pricing considerations**

AWS Key Management Service provides a free tier of 20,000 requests/month calculated [across all regionsthat the service is available.](https://aws.amazon.com/about-aws/global-infrastructure/regional-product-services/)

You are not charged for the creation and storage of AWS managed CMKs. These keys are automatically created on your behalf when you first attempt to encrypt a resource in an AWS service that integrates with AWS KMS. You can neither manage the lifecycle or access permissions on AWS managed keys.

\*\*\*Requests to the GenerateDataKeyPair and GenerateDataKeyPairWithoutPlaintext APIs and requests to APIs such as Sign, Verify, Encrypt, Decrypt, and GetPublicKey that reference asymmetric CMKs are excluded from the free tier.

Each customer master key (CMK) that you create in AWS Key Management Service (KMS) costs $1/month until you delete it, regardless of where the underlying key material was generated by the service, a custom key store, or you imported it.

For a CMK with key material generated by the service, if you opt-in to have it automatically rotate the key each year, each new key version raises the cost of the CMK by $1/month.

**More details**

Official AWS page: <https://aws.amazon.com/kms/>

AWS Key Management Service (KMS) for Data Encryption: <https://k21academy.com/amazon-web-services/amazon-aws-key-management-service-kms/>

Comparison of AWS Key Management Service and AWS CloudHSM: <https://blog.kindite.com/aws-kms-vs-aws-cloudhsm>