

Key Management Service

User Guide (Paris)

Issue 04
Date 2020-12-11



Copyright © Huawei Technologies Co., Ltd. 2021. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

1 Introduction.....	1
1.1 Concepts.....	1
1.1.1 KMS.....	1
1.1.2 CMK.....	1
1.1.3 Default Master Key.....	1
1.1.4 DEK.....	2
1.1.5 HSM.....	2
1.1.6 Envelope Encryption.....	2
1.1.7 TRNG.....	2
1.2 Application Scenarios.....	2
1.3 Functions.....	3
1.4 Accessing and Using KMS.....	4
1.4.1 How to Access KMS.....	4
1.4.2 How to Use KMS.....	4
1.4.3 Related Services.....	5
1.4.4 User Permissions.....	7
2 Management.....	8
2.1 Creating a Key.....	8
2.2 Creating CMKs Using Imported Key Material.....	9
2.2.1 Overview.....	9
2.2.2 Importing Key Material.....	10
2.2.3 Deleting Key Material.....	15
2.3 Scheduling the Deletion of One or Multiple CMKs.....	16
2.4 Rotating CMKs.....	17
2.4.1 Context.....	17
2.4.2 Enabling Key Rotation.....	19
2.5 Managing CMKs.....	20
2.5.1 Querying a CMK.....	20
2.5.2 Changing the Alias and Description of a CMK.....	22
2.5.3 Enabling One or Multiple CMKs.....	23
2.5.4 Disabling One or Multiple CMKs.....	24
2.5.5 Canceling the Scheduled Deletion of One or Multiple CMKs.....	25
3 FAQs.....	27

3.1 What Is Key Management Service?.....	27
3.2 What Is a Customer Master Key?.....	27
3.3 What Is a Data Encryption Key?.....	27
3.4 Why Cannot I Delete a CMK Immediately?.....	27
3.5 Which Cloud Services Can Use KMS for Encryption?.....	28
3.6 How Does KMS Charge?.....	28
3.7 Are Disabled CMKs Billable?.....	28
A Change History.....	29

1 Introduction

1.1 Concepts

1.1.1 KMS

Key Management Service (KMS) is a secure, reliable, and easy-to-use service that helps users centrally manage and safeguard their Customer Master Keys (CMKs).

This service uses hardware security modules (HSMs) to protect CMKs. HSMs help you create and control CMKs with ease. All CMKs are protected by root keys in HSMs to avoid leakage caused by human error. KMS implements access control and log-based tracking on all operations involving CMKs. Additionally, it provides use records of all CMKs, meeting your audit and regulatory compliance requirements.

1.1.2 CMK

A Customer Master Key (CMK) is a Key Encryption Key (KEK) created by a user using KMS. It is used to encrypt and protect Data Encryption Keys (DEKs). One CMK can be used to encrypt one or multiple DEKs.

1.1.3 Default Master Key

A Default Master Key is automatically created by another cloud service using KMS, such as Object Storage Service (OBS). The alias of a Default Master Key ends with **/default**.

You can use the management console to query the status of Default Master Keys, but cannot disable or schedule the deletion of Default Master Keys.

Table 1-1 Default Master Keys

Alias	Cloud Service
obs/default	OBS

Alias	Cloud Service
evs/default	Elastic Volume Service (EVS)
ims/default	Image Management Service (IMS)
sfs/default	Scalable File Service (SFS)

 **NOTE**

A Default Master Key is automatically created when a user employs the KMS encryption function for the first time in another cloud service.

1.1.4 DEK

Data Encryption Keys (DEKs) are used by users to encrypt data.

1.1.5 HSM

A hardware security module (HSM) is a hardware device that securely produces, stores, manages, and uses CMKs. In addition, it provides encryption processing services.

1.1.6 Envelope Encryption

Envelope encryption is an encryption method that enables DEKs to be stored, transmitted, and used in "envelopes." As a result, CMKs are not used to directly encrypt and decrypt data.

1.1.7 TRNG

A true random number generator (TRNG) is a device that generates unpredictable random numbers by physical procedures instead of computer programs.

1.2 Application Scenarios

KMS provides central management and control capabilities of CMKs for Object Storage Service (OBS), Elastic Volume Service (EVS), Image Management Service (IMS), Scalable File Service (SFS), and user applications. It is perfectly suited for data encryption and decryption scenarios.

- For OBS, KMS applies to object encryption on OBS.

 **NOTE**

OBS is an object-based storage service that provides customers with massive, secure, reliable, and cost-effective data storage capabilities, including but not limited to bucket creation, modification, deletion, and management, as well as object upload, download, deletion, and general management. OBS can store all file types, and is suitable for individual subscribers, websites, enterprises, and developers. For more information about OBS, see *Object Storage Service User Guide*.

- For EVS, KMS applies to data encryption in EVS disks.

NOTE

Based on a distributed architecture, an EVS disk is a virtual block storage device that can be elastically scaled up and down. EVS disks can be operated online. Using them is the same as using common server hard disks. Compared with traditional hard disks, EVS disks have higher data reliability and I/O throughput and are easier to use. EVS disks can be used in file systems, databases, and system software applications that require block storage devices. For more information about EVS, see the *Elastic Volume Service User Guide*.

- For IMS, KMS applies to the creation of encrypted private images.

NOTE

IMS provides easy-to-use self-service image management functions. You can apply for an Elastic Cloud Server (ECS) using either a private image or a public image. You can also create a private image using an existing ECS or an external image file. For more information about IMS, see the *Image Management Service User Guide*.

- For SFS, KMS applies to data encryption for files in SFS.

NOTE

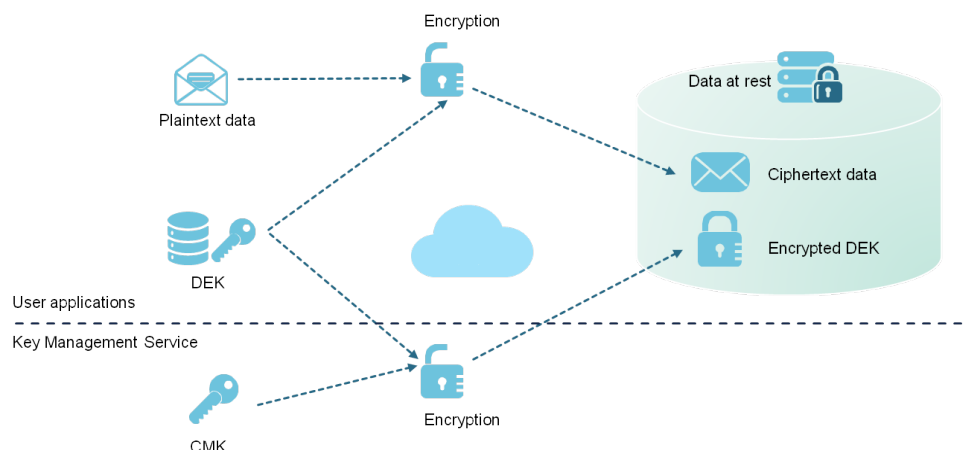
SFS provides high-performance file storage that is scalable on demand. It can be shared with multiple ECSs. For more information, see the *Scalable File Service User Guide*.

- For user applications

To encrypt plaintext data, a user application can call the necessary KMS API to generate a DEK, which can then be used to encrypt the plaintext data. Then the application can store the encrypted data. In addition, the user application can call the necessary KMS APIs to create CMKs. DEKs can be stored in ciphertext after being encrypted with the CMKs. **Figure 1-1** shows envelope encryption working principles.

To ensure the security of the user's encrypted data, KMS does not save DEKs in plaintext or ciphertext. Instead, it manages the CMKs of users to enable users to obtain and use DEKs securely.

Figure 1-1 Envelope encryption working principles



1.3 Functions

KMS provides the following functions:

- Manages CMKs.
Using the KMS console or APIs, you can perform the following operations on CMKs:
 - Creating, querying, enabling, disabling, scheduling the deletion of, and canceling the deletion of CMKs
 - Importing CMKs and deleting CMK material
 - Modifying the aliases and description of CMKs
 - Enabling key rotation
- Creates, encrypts, and decrypts DEKs.
You can create, encrypt, and decrypt a DEK by calling KMS APIs. For details, see the *Key Management Service API Reference*.
- Generates hardware true random numbers.
You can generate 512-bit hardware true random numbers using a KMS API. The 512-bit hardware true random numbers can be used as or serve as basis for keys and encryption parameters. For details, see the *Key Management Service API Reference*.

1.4 Accessing and Using KMS

1.4.1 How to Access KMS

The public cloud provides a web-based service management platform. You can access KMS using HTTPS-compliant APIs or the management console.

- Management console
If you have registered with the public cloud, you can log in to the management console directly. Then choose **Security > Key Management Service**.
- API
You can access KMS using APIs. For details, see the *Key Management Service API Reference*.

1.4.2 How to Use KMS

Working with OBS

Users can upload objects to and download them from Object Storage Service (OBS) in common mode or server-side encryption mode. When users upload objects in encryption mode, data is encrypted at the server side and then securely stored on OBS in ciphertext. When users download encrypted objects, the data in ciphertext is decrypted at the server side and then provided to users in plaintext. OBS supports the server-side encryption with KMS-managed keys (SSE-KMS) mode. In SSE-KMS mode, OBS uses the keys provided by KMS for server-side encryption.

For details about how to upload objects to OBS in SSE-KMS mode, see the *Object Storage Service User Guide*.

Working with EVS

If you enable the encryption function when creating an EVS disk and select a CMK provided by KMS to encrypt the EVS disk, data stored to the EVS disk is automatically encrypted.

For details about how to use the encryption function of EVS, see the *Elastic Volume Service User Guide*.

Working with IMS

When creating a private image using an external image file, you can enable the private image encryption function and select a CMK provided by KMS to encrypt the image.

For details about how to use the private image encryption function of Image Management Service (IMS), see the *Image Management Service User Guide*.

Working with SFS

When creating a file system on SFS, the CMK provided by KMS can be selected to encrypt the file system, so that files stored in the file system are automatically encrypted.

For details about how to use the encryption function of SFS, see the *Scalable File Service User Guide*.

Working with RDS

When creating a database instance, you can enable the disk encryption function of the database instance and select a CMK created on KMS to encrypt the disk of the database instance. The enablement of disk encryption will enhance data security.

For details about how to use the disk encryption function of RDS, see the *Relational Database Service User Guide*.

Working with User Applications

To encrypt plaintext data, a user application can call the necessary KMS APIs to generate a DEK. The DEK can then be used to encrypt the plaintext data. Then the application can store the encrypted data. In addition, the user application can call the necessary KMS APIs to create CMKs. DEKs can be stored in ciphertext after being encrypted with the CMKs. For details, see the *Key Management Service API Reference*.

1.4.3 Related Services

OBS

KMS provides central management and control capabilities of CMKs for Object Storage Service (OBS). It is used for server-side encryption with KMS-managed keys (SSE-KMS) function of OBS.

EVS

KMS provides central management and control capabilities of CMKs for Elastic Volume Service (EVS). It is applied to the encryption function of EVS.

IMS

KMS provides central management and control capabilities of CMKs for Image Management Service (IMS). It is applied to the private image encryption function of IMS.

SFS

KMS provides central management and control capabilities of CMKs for Scalable File Service (SFS). It is applied to the file system encryption function of SFS.

CTS

Cloud Trace Service (CTS) provides you with a history of KMS operations. After enabling CTS, you can view all generated traces to review and audit performed KMS operations. For details, see the *Cloud Trace Service User Guide*.

Table 1-2 KMS operations supported by CTS

Operation	Resource Type	Trace Name
Creating a CMK	cmk	createKey
Creating a DEK	cmk	createDataKey
Creating a plaintext-free DEK	cmk	createDataKeyWithoutPlaintext
Enabling a CMK	cmk	enableKey
Disabling a CMK	cmk	disableKey
Encrypting a DEK	cmk	encryptDataKey
Decrypting a DEK	cmk	decryptDataKey
Scheduling the deletion of a CMK	cmk	scheduleKeyDeletion
Canceling the scheduled deletion of a CMK	cmk	cancelKeyDeletion
Generating random numbers	rng	genRandom
Changing the alias of a CMK	cmk	updateKeyAlias
Changing the description of a CMK	cmk	updateKeyDescription

Operation	Resource Type	Trace Name
Prompting risks about CMK deletion	cmk	deleteKeyRiskTips

IAM

Identity and Access Management (IAM) provides the permission management function for KMS. Only users who have KMS Administrator permissions can use KMS. To apply for KMS Administrator permissions, contact a user with Security Administrator permissions. For details, see the *Identity and Access Management User Guide*.

1.4.4 User Permissions

The public cloud system provides two types of permissions by default: user management and resource management. User management refers to the management of users, user groups, and user groups' rights. Resource management refers to the control of operations that can be performed by users on cloud service resources.

2 Management

2.1 Creating a Key

Scenario

This section describes how to create a CMK on the KMS management console. You can create up to 100 CMKs, excluding Default Master Keys.

The CMK is perfectly suited for but not limited to the following scenarios:

- Server-side encryption on OBS
- Encryption of data on EVS disks
- Encryption of private images on IMS
- File system encryption on SFS
- DEK encryption and decryption for user applications

NOTE

Aliases of Default Master Keys end with **/default**. It is not allowed to use aliases ending with **/default** for your CMKs.

Prerequisites

You have obtained an account and its password for logging in to the management console.

Procedure

- Step 1** Log in to the management console.
- Step 2** Choose **Security > Key Management Service**. The **Key Management Service** page is displayed.
- Step 3** Click **Create Key** in the upper right corner of the page. In the dialog box that is displayed, enter the alias and description of the key.
 - **Alias** is the alias of the CMK to be created.

- (Optional) **Description** is the description of the CMK.

Step 4 Click **OK**.

In the CMK list, you can view created CMKs. The default status of a CMK is **Enabled**.

----End

Related Operations

- For details about how to upload objects with server-side encryption, see section **Uploading a File with Server-Side Encryption** in the *Object Storage Service User Guide*.
- For details about how to encrypt data on EVS disks, see section **Creating an EVS Disk** in the *Elastic Volume Service User Guide*.
- For details about how to encrypt private images, see section **Encrypting an Image** in the *Image Management Service User Guide*.
- For details about how to encrypt the file system on SFS, see section **Creating a File System** in the *Scalable File Service User Guide*.
- For details about how to create a DEK and a plaintext-free DEK, see sections **Creating a DEK** and **Creating a Plaintext-Free DEK** in the *Key Management Service API Reference*.
- For details about how to encrypt and decrypt a DEK for a user application, see sections **Encrypting a DEK** and **Decrypting a DEK** in the *Key Management Service API Reference*.

2.2 Creating CMKs Using Imported Key Material

2.2.1 Overview

A CMK contains key metadata (key ID, key alias, description, key status, and creation date) and the key material used for encrypting and decrypting data.

- When a user uses the KMS Console to create a CMK, the KMS automatically generates a key material for the CMK.
- If you want to use your own key material, you can use the key import function on KMS Console to create a CMK whose key material is empty, and import the key material to the CMK.

Important Notes

- **Security**
You need to ensure that random sources meet your security requirements when using them to generate key material. When using the import key function, you need to be responsible for the security of your key material. Save the original backup of the key material so that the backup key material can be imported to the KMS in time when the key material is deleted accidentally.
- **Availability and Durability**

Before importing the key material into KMS, you need to ensure the availability and durability of the key material.

Differences between the imported key material and the key material generated by KMS are shown in [Table 2-1](#).

Table 2-1 Differences between the imported key material and the key material generated by KMS

Key Material Source	Difference
CMKs using the imported key material	<ul style="list-style-type: none"> • You can delete the key material, but cannot delete the CMK and its metadata. • When importing the key material, you can set the expiration time of the key material. After the key material expires, the KMS automatically deletes the key material within 24 hours, but does not delete the CMK and its metadata. It is recommended that you save a copy of the material on your local device because it may be used for re-import in cases of invalid key material or unintended deletion of key material.
CMKs using KMS generated key material	<ul style="list-style-type: none"> • The key material cannot be manually deleted. • You cannot set the expiration time for key material.

- Association
When a key material is imported to a CMK, the CMK is permanently associated with the key material. Other key material cannot be imported into the CMK.
- Uniqueness
If you use the CMK created using the imported key material to encrypt data, the encrypted data can be decrypted only by the CMK that has been used to encrypt the data, because the metadata and key material of the CMK must be consistent.

2.2.2 Importing Key Material

Scenario

If you want to use your own key material instead of the KMS-generated material, you can use the console to import your key material to KMS. CMKs created using imported material and KMS-generated material are managed together by KMS.

This section describes how to import key material through KMS Console.

 **NOTE**

- A CMK with imported material works in the same way as one using KMS-generated material, that is, you enable and disable them as well as schedule their deletion and cancel their scheduled deletion in the same way.
- You can only import 256-bit symmetric keys.

Prerequisites

- You have obtained an account and its password for logging in to the management console.
- You have prepared the key material to be imported.

Procedure

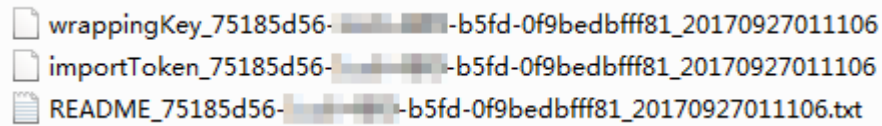
- Step 1** Log in to the management console.
- Step 2** Choose **Security > Key Management Service**. The **Key Management Service** page is displayed.
- Step 3** In the upper right corner, click **Import Key**.
- Step 4** In the **Import Key** dialog box, set the alias and description of the key.
- Step 5** Click **security and durability** to read and confirm information regarding the security and durability of the imported key.
- Step 6** Select **I understand the security and durability of using an imported key**, and create a CMK whose key material is empty.
- Step 7** Click **Next** to go to the **Download the Import Items** step. Select a key-wrapping algorithm according to [Table 2-2](#).

Table 2-2 Key wrapping algorithms

Algorithm	Description	Configuration
RSAES_OAEP_SHA_256	RSA encryption algorithm that uses OAEP and has the SHA-256 hash function	Choose an algorithm from the drop-down list box. <ol style="list-style-type: none"> 1. If the HSMs support the RSAES_OAEP_SHA_256 algorithm, use RSAES_OAEP_SHA_256 to encrypt the key material. 2. If the HSMs do not support OAEP, use RSAES_PKCS1_V1_5 to encrypt the key material. <p>NOTICE The RSAES_OAEP_SHA_1 encryption algorithm is no longer secure. Exercise caution when performing this operation.</p>
RSAES_PKCS1_V1_5	RSA encryption algorithm (v1.5) of Public-Key Cryptography Standards number 1 (PKCS #1)	
RSAES_OAEP_SHA_1	RSA encryption algorithm that uses Optimal Asymmetric Encryption Padding (OAEP) and has the SHA-1 hash function	

- Step 8** Click **Download**. The following files are downloaded: **wrappingKey**, **importToken**, and **README**. These are displayed in **Figure 2-1**.

Figure 2-1 Downloaded files



- **wrappingKey_CMK ID_download time** is a wrapping key used to encrypt the key material.
- **importToken_CMK ID_download time** is an import token used to import key material to KMS.
- **README_CMK ID_download time** is a description file recording information such as a CMK's serial number, wrapping algorithm, wrapping key name, token file name, and the expiration time of the token file and wrapping key.

NOTICE

The wrapping key and import token expire within 24 hours of creation. If they have expired, download them again.

Alternatively, you can obtain the wrapping key and import token by calling the API.

1. Call the **get-parameters-for-import** API to obtain the wrapping key and import token.

The following example describes how to obtain the wrapping key and import token of a CMK (ID: **43f1ffd7-18fb-4568-9575-602e009b7ee8**; encryption algorithm: **RSAES_PKCS1_V1_5**).

public_key: The content of the wrapping key (Base-64 encoding) returned after calling the API

import_token: Content of the import token (Base-64 encoding) returned after calling the API

- Request example

```
{
  "key_id": "43f1ffd7-18fb-4568-9575-602e009b7ee8",
  "wrapping_algorithm": "RSAES_PKCS1_V1_5"
}
```

- Response example:

```
{
  "key_id": "43f1ffd7-18fb-4568-9575-602e009b7ee8",
  "public_key": "public key base64 encoded data",
  "import_token": "import token base64 encoded data",
  "expiration_time": 1501578672
}
```

2. Save the wrapping key, and convert its format according to the following procedure. Only the key material that is encrypted using the converted wrapping key can be imported to the management console.
 - a. Copy the content of the wrapping key **public_key**, save it to the **.txt** file as **PublicKey.b64**.

- b. Run the following command to convert the Base-64 coding of the **PublicKey.b64** file to binary data, and save the converted file as **PublicKey.bin**:
openssl enc -d -base64 -A -in PublicKey.b64 -out PublicKey.bin
3. Save the import token, copy the content of the **import_token** token, paste it to a **.txt** file, and save the file as **ImportToken.b64**.

Step 9 You use the downloaded **wrappingKey** file to encrypt the key material to be imported.

- Method 1: Use the downloaded wrapping key to encrypt the key material on your HSM. For details, see the operation guide of your HSM.
- Method 2: Use OpenSSL to encrypt the key material.

 **NOTE**

If you need to run the **openssl pkeyutl** command, the OpenSSL version must be 1.0.2 or later.

The following example describes how to use the downloaded wrapping key to encrypt the generated key material (256-bit symmetric key). The procedure is as follows:

- a. Run the following command to generate the key material (256-bit symmetric key) and save the generated key material as **PlaintextKeyMaterial.bin**:
openssl rand -out PlaintextKeyMaterial.bin 32
- b. Use the downloaded wrapping key to encrypt the key material and save the encrypted key material as **EncryptedKeyMaterial.bin**.

Replace **PublicKey.bin** in the command with the name of the wrapping key *wrappingKey_key ID_download time* downloaded in [Step 8](#).

Table 2-3 Encrypting the generated key material using the downloaded wrapping key

Wrapping Key Algorithm	Key Materials Encryption
RSAES_OAEP_SHA_256	openssl pkeyutl -in PlaintextKeyMaterial.bin -inkey PublicKey.bin -out EncryptedKeyMaterial.bin -keyform der -pubin -encrypt -pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256

Wrapping Key Algorithm	Key Materials Encryption
RSAES_PKCS1_V1_5	<pre>openssl rsautl -encrypt -in PlaintextKeyMaterial.bin -pkcs -inkey PublicKey.bin -keyform der -pubin -out EncryptedKeyMaterial.bin</pre>
RSAES_OAEP_SHA_1	<pre>openssl pkeyutl -in PlaintextKeyMaterial.bin -inkey PublicKey.bin -out EncryptedKeyMaterial.bin -keyform der -pubin -encrypt -pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha1</pre>

Step 10 Click **Next** to go to the **Import Key Material** step. Configure the parameters as described in [Table 2-4](#).

Table 2-4 Parameters for importing key material

Parameter	Description
Key ID	Random ID of a CMK generated during the CMK creation
Key material	<ol style="list-style-type: none"> Use the key material encrypted by the wrappingKey file downloaded in Step 8. Click Import to import the key material.

Step 11 Click **Next** to go to the **Import Key Token** step. Configure the parameters as described in [Table 2-5](#).

Table 2-5 Parameters for importing a key token

Parameter	Description
Key ID	Random ID of a CMK generated during the CMK creation
Token	Select the importToken downloaded in Step 8 .

Parameter	Description
Key material expiration mode	<ul style="list-style-type: none"> • Key material will never expire: This option specifies that key material will not expire after import. • Key material expires on: This option specifies the expiration time of the key material. By default, the key material expires in 24 hours after import. When the key material expires, KMS will delete them in 24 hours, making the CMK unusable and the CMK status Pending import.

Step 12 Click **OK**.

NOTICE

Key material can be successfully imported when it matches the corresponding CMK ID and token.

Your imported material is displayed in the list of CMKs. The default status of an imported CMK is **Enabled**.

----End

2.2.3 Deleting Key Material

Scenario

When importing key material, you can specify the expiration time. After the key material expires, KMS deletes it, and the status of the CMK changes to **Pending import**. You can manually delete the key material as needed. The effect of expiration of the key material is the same as that of manual deletion of the key material.

This section describes how to delete imported key material on the management console.

NOTE

- After the key material is deleted, if you need to re-import the key material, the key material to be imported must be the same as that has been deleted.
- After the same key material is re-imported, you can use the CMK to decrypt all data encrypted using this key before deletion.

Prerequisites

- You have obtained an account and its password for logging in to the management console.
- You have imported the key material for a CMK.
- The material source of the CMK is **External**.
- The CMK status is **Enabled** or **Disabled**.

Procedure

- Step 1** Log in to the management console.
- Step 2** Choose **Security > Key Management Service**. The **Key Management Service** page is displayed.
- Step 3** In the row containing the desired CMK, click **Delete Key Material**.
- Step 4** In the dialog box that is displayed, click **OK**.

After the deletion, the CMK will become unavailable and its status changes to **Pending import**.

----End

2.3 Scheduling the Deletion of One or Multiple CMKs

Scenario

This section describes how to use the management console to schedule the deletion of one or multiple unwanted CMKs.

If deletion is scheduled for a CMK, the deletion will not take effect immediately. Instead, it will take effect after a waiting period of 7 to 1096 days. Before the specified deletion date, you can cancel the deletion if you want to use the CMK. Once the scheduled deletion has taken effect, the CMK will be deleted permanently and you will not be able to decrypt data encrypted by it. Therefore, you are advised to exercise caution when performing this operation.

Before deleting the CMK, confirm that it is not in use and will not be used.

NOTE

Default Master Keys created by KMS cannot be scheduled for deletion.

Prerequisites

- You have obtained an account and its password for logging in to the management console.
- The CMK you want to schedule deletion for is in **Enabled** or **Disabled** status.

Procedure

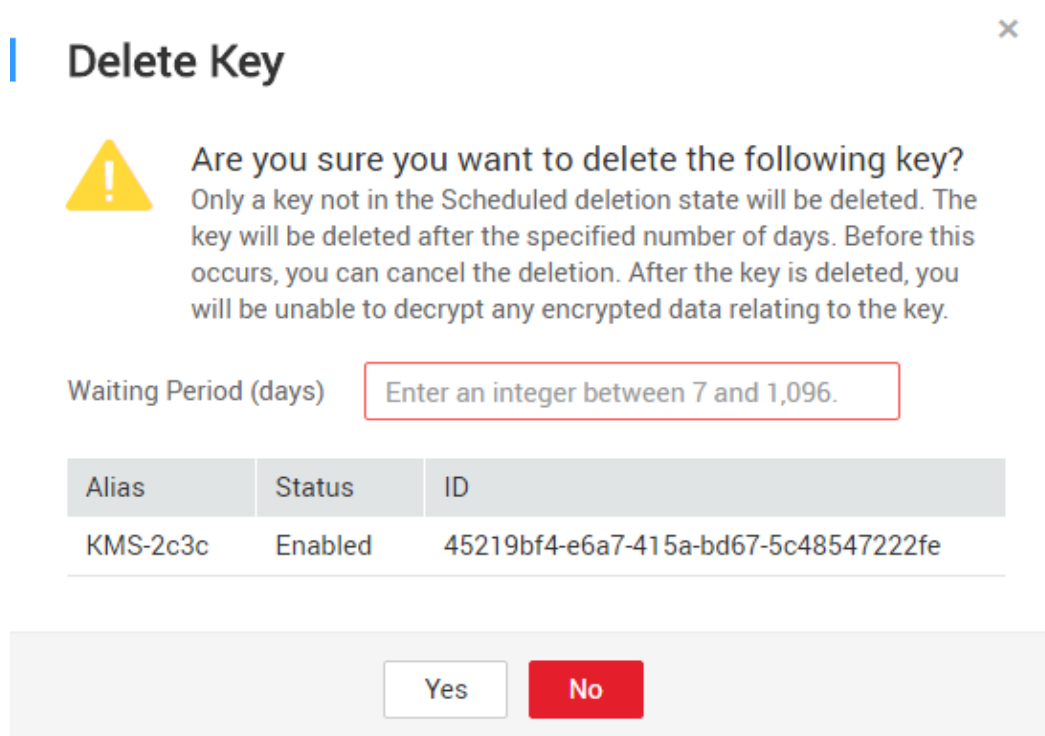
- Step 1** Log in to the management console.
- Step 2** Choose **Security > Key Management Service**. The **Key Management Service** page is displayed.
- Step 3** In the row containing the desired CMK, click **Delete**.

Figure 2-2 Scheduling the deletion for one CMK

<input type="checkbox"/> Alias	Status	ID	Created	Operation
<input type="checkbox"/> KMS-2c3c	Enabled	45219bf4-e6a7-415a-bd67-5c48547222fe	04/23/2018 15:59:23 GMT+08:00	Disable Delete
<input type="checkbox"/> KMS-1d08	Enabled	543be26f-76e0-4b39-aeef-b573ad10ac66	04/23/2018 15:59:18 GMT+08:00	Disable Delete
<input type="checkbox"/> KMS-fa92	Enabled	a415baed-191b-4871-a07d-230c516850d6	04/23/2018 15:59:14 GMT+08:00	Disable Delete

Step 4 In the dialog box that is displayed, enter the number of days after which you want the deletion to take effect.

Figure 2-3 Scheduling a deletion time



Step 5 Click **Yes** to schedule the deletion.

NOTE

To delete multiple CMKs at a time, select them and click **Delete** in the upper left corner of the list.

----End

2.4 Rotating CMKs

2.4.1 Context

Security risks exist when a DEK is extensively and repeatedly used. For security purposes, you can configure KMS to create new key materials for the CMK.

New key materials can be created in two methods:

- Manual key rotation

Create a CMK on the KMS management console to replace the original CMK.

NOTE

If cloud services (such as OBS) use a CMK to encrypt and decrypt data, you need to create a new CMK on the KMS management console and replace the original one used for KMS encryption on OBS Console.

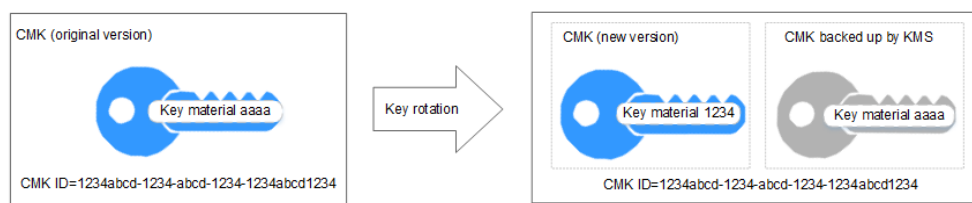
- Automatic key rotation

Enable rotation for an existing CMK so that KMS automatically generates new key material for the CMK.

Key rotation only changes the key material of a CMK. The CMK's attributes (such as ID, alias, description, and permissions settings) remain unchanged.

The key rotation function enables KMS to automatically rotate CMKs according to the specified rotation interval (365 days by default). For a CMK with the key rotation function enabled, a new version is generated upon each rotation. See [Figure 2-4](#) for details.

Figure 2-4 Working principle of key rotation



KMS retains all versions associated of the CMK, so that you can decrypt any ciphertext encrypted using the CMK.

- KMS uses the latest version of the CMK to encrypt data.
- KMS uses the same version of the CMK to decrypt data as that used to encrypt the data.

Table 2-6 Key rotation modes

Key Type	Support for Key Rotation
Default Master Key	Keys cannot be rotated.
Imported CMK	Keys can only be rotated manually.
Disabled CMK	KMS does not rotate disabled CMKs and keeps their rotation status unchanged. After a CMK is enabled, if the backup CMK has been used for longer than the rotation period, KMS will immediately rotate keys. If the backup CMK has been used for shorter than the rotation period, KMS will implement the original rotation plan.

Key Type	Support for Key Rotation
CMK in pending deletion status	KMS does not rotate CMKs in pending deletion status. After you cancel the deletion of a CMK, the previous key rotation status will be restored. If the backup CMK has been used for longer than the rotation period, KMS will immediately rotate keys. If the backup CMK has been used for shorter than the rotation period, KMS will implement the original rotation plan.

2.4.2 Enabling Key Rotation

Scenario

This section describes how to enable rotation for a key on the KMS console.

By default, automatic key rotation is disabled for a CMK. Every time you enable key rotation, KMS automatically rotates CMKs based on the rotation period you set.

Prerequisites

- You have obtained an account and its password for logging in to the management console.
- The CMK is in **Enabled** status.
- The **Origin** of the CMK is **KMS**.

Procedure

Step 1 Log in to the management console.




Step 2 Choose **Security > Key Management Service**. The **Key Management Service** page is displayed.

Step 3 Click the alias of the desired CMK to view its details.

Step 4 Click **Rotation Policy**.

Step 5 Click  to set the **Key Rotation** status to  (enabled). [Table 2-7](#) provides more details.

Table 2-7 Description of the parameters for enabling rotation for a CMK

Parameter	Description
Key Rotation	<p>Rotation switch. The default status is  (disabled).</p> <p> : disabled</p> <p> : enabled</p> <p>After rotation is enabled, the CMK will be rotated based on your set period.</p> <p>NOTE KMS does not rotate a disabled CMK for which rotation has been enabled. KMS rotates it when it is enabled again. If it has been longer than the rotation period since the CMK was rotated last time, KMS will rotate the CMK within 24 hours.</p>
Rotation Period (day)	<p>Rotation period (day). The value is an integer ranging from 30 to 365. The default value is 365.</p> <p>Set the period based on how often a CMK is used. If it is frequently used, set a short period; otherwise, set a long one.</p>

----End

2.5 Managing CMKs

2.5.1 Querying a CMK

Scenario

This section describes how to use the management console to view the information about a CMK, such as its alias, status, ID, and creation time. The status of a CMK can be **Enabled**, **Disabled**, **Pending deletion**, or **Pending import**.

Prerequisites

You have obtained an account and its password for logging in to the management console.

Procedure

- Step 1** Log in to the management console.
- Step 2** Choose **Security > Key Management Service**. The **Key Management Service** page is displayed.
- Step 3** In the CMK list you can view details about the CMKs.

Figure 2-5 CMK list

Alias	Status	ID	Created	Operation
<input type="checkbox"/> KMS-1126	Enabled	efb913a0-7a3f-4a0e-9aff-e9a91b2b5694	05/14/2018 11:45:48 GMT+08:00	Disable Delete
<input type="checkbox"/> KMS-ef51	Enabled	4b0eb93e-db25-4498-adb0-68303dbf19aa	05/14/2018 11:45:44 GMT+08:00	Disable Delete
<input type="checkbox"/> KMS-e4f0	Enabled	c22a39e6-eb68-488b-8fa8-fa9df89f55fd	05/14/2018 11:45:42 GMT+08:00	Disable Delete

NOTE



- Select the CMK status from the drop-down list of **All statuses**. Then the CMK list displays only the CMKs in the corresponding state.
- Enter the alias of a CMK in the search box on top of the CMK list. Click  or press Enter to search for the specified CMK.
- You can click  at the upper right corner on top of the CMK list to show or hide columns of the CMK list.

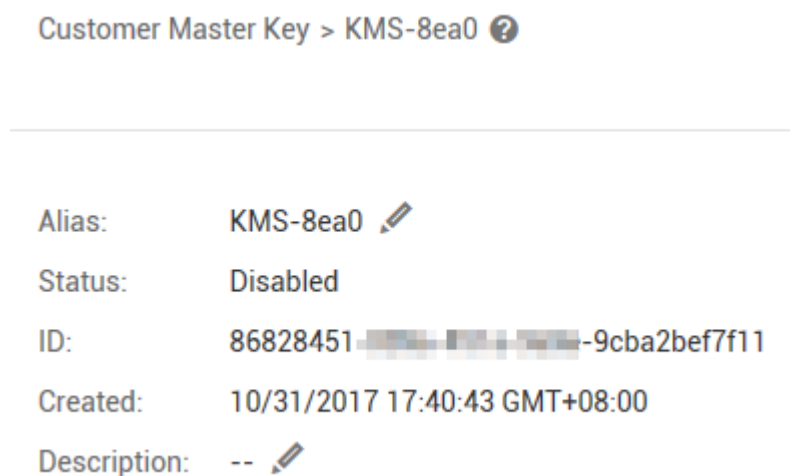
Table 2-8 describes the parameters of a CMK list.

Table 2-8 CMK list parameters

Parameter	Description
Alias	Alias of a CMK
Status	Status of a CMK, which can be one of the following: <ul style="list-style-type: none"> • Enabled The CMK is enabled. • Disabled The CMK is disabled. • Pending deletion The CMK is scheduled for deletion. • Pending import If your CMK does not have the key material, its status is Pending import.
ID	Random ID of a CMK generated during the CMK creation
Creation Time	Creation time of the CMK
Expiration Time	Expiration time of the key material. When the material expires, the CMK becomes an empty CMK.
Origin	Source of key material, which can be one of the following: <ul style="list-style-type: none"> • External You import the key material for the CMK. • Key Management Service The CMK uses KMS-generated material.

Step 4 You can click the alias of a CMK to view its details.

Figure 2-6 Viewing CMK details



----End

2.5.2 Changing the Alias and Description of a CMK

Scenario

The alias of a CMK is a user-friendly name designed to help you locate the CMK easier.

This section describes how to change the alias and description of a CMK on the KMS management console.

NOTICE

- A Default Master Key (the alias suffix of which is **/default**) does not allow alias and description changes.
- The alias and description of a CMK cannot be changed if the CMK is in **Pending deletion** status.

Prerequisites

- You have obtained an account and its password for logging in to the management console.
- The **Status** of a CMK is **Enabled** or **Disabled**.

Procedure

Step 1 Log in to the management console.

Step 2 Choose **Security > Key Management Service**. The **Key Management Service** page is displayed.

Step 3 Click the alias of the desired CMK. Details about the CMK are displayed.


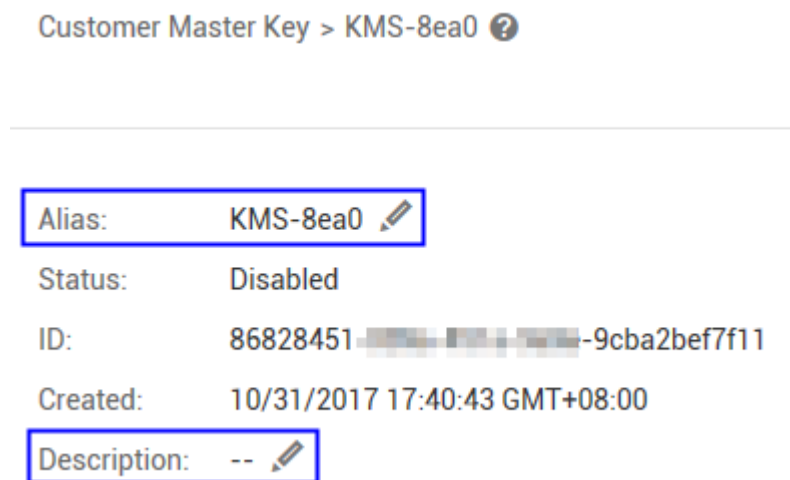

Step 4 To change the alias or description of the CMK, click  next to the value of **Alias** or **Description**.

Figure 2-7 CMK details



 **NOTE**

- The alias must be 1 to 255 characters in length. Only digits, letters, underscores (_), hyphens (-), colons (:), and forward slashes (/) are allowed.
- Length of the description cannot exceed 255 characters.

Step 5 Click  to save the changes.

----End

2.5.3 Enabling One or Multiple CMKs

Scenario

This section describes how to use the management console to enable one or multiple CMKs. Only enabled CMKs can be used to encrypt/decrypt data. A new CMK is in the **Enabled** state by default.

Prerequisites

- You have obtained an account and its password for logging in to the management console.
- The CMK you want to enable is in **Disabled** status.

Procedure

Step 1 Log in to the management console.

Step 2 Choose **Security > Key Management Service**. The **Key Management Service** page is displayed.

Step 3 In the row containing the desired CMK, click **Enable**.

Figure 2-8 Enabling one CMK

<input type="checkbox"/> Alias	Status	ID	Created	Operation
<input type="checkbox"/> KMS-2c3c	❌ Disabled	45219bf4-e6a7-415a-bd67-5c48547222fe	04/23/2018 15:59:23 GMT+08:00	Enable Delete
<input type="checkbox"/> KMS-1d08	❌ Disabled	543be26f-76e0-4b39-aeef-b573ad10ac66	04/23/2018 15:59:18 GMT+08:00	Enable Delete
<input type="checkbox"/> KMS-fa92	❌ Disabled	a415baed-191b-4871-a07d-230c516850d6	04/23/2018 15:59:14 GMT+08:00	Enable Delete

Step 4 In the dialog box that is displayed, click **Yes** to enable the CMK.

NOTE

To enable multiple CMKs at a time, select them and click **Enable** in the upper left corner of the list.

----End

2.5.4 Disabling One or Multiple CMKs

Scenario

This section describes how to use the management console to disable one or multiple CMKs, thereby protecting data in urgent cases.

After being disabled, a CMK cannot be used to encrypt or decrypt any data. Before using a disabled CMK to encrypt or decrypt data, you must enable it by following instructions in [Enabling One or Multiple CMKs](#).

NOTE

Default Master Keys created by KMS cannot be disabled.

Prerequisites

- You have obtained an account and its password for logging in to the management console.
- The CMK you want to disable is in **Enabled** status.

Procedure

Step 1 Log in to the management console.

Step 2 Choose **Security > Key Management Service**. The **Key Management Service** page is displayed.

Step 3 In the row containing the desired CMK, click **Disable**.

Figure 2-9 Disabling one CMK

<input type="checkbox"/> Alias	Status	ID	Created	Operation
<input type="checkbox"/> KMS-2c3c	✅ Enabled	45219bf4-e6a7-415a-bd67-5c48547222fe	04/23/2018 15:59:23 GMT+08:00	Disable Delete
<input type="checkbox"/> KMS-1d08	✅ Enabled	543be26f-76e0-4b39-aeef-b573ad10ac66	04/23/2018 15:59:18 GMT+08:00	Disable Delete
<input type="checkbox"/> KMS-fa92	✅ Enabled	a415baed-191b-4871-a07d-230c516850d6	04/23/2018 15:59:14 GMT+08:00	Disable Delete

Step 4 In the dialog box that is displayed, click **Yes** to disable the CMK.

 **NOTE**

To disable multiple CMKs at a time, select them and click **Disable** in the upper left corner of the list.

----End

2.5.5 Canceling the Scheduled Deletion of One or Multiple CMKs

Scenario

This section describes how to use the management console to cancel the scheduled deletion of one or multiple CMKs prior to deletion execution.

Prerequisites

- You have obtained an account and its password for logging in to the management console.
- The CMK for which you want to cancel the scheduled deletion is in **Pending deletion** status.




Procedure

Step 1 Log in to the management console.

Step 2 Choose **Security > Key Management Service**. The **Key Management Service** page is displayed.

Step 3 In the row containing the desired CMK, click **Cancel Deletion**.

Figure 2-10 Canceling the scheduled deletion of one CMK

<input type="checkbox"/> Alias ↕	Status	ID	Created ↕	Operation
<input type="checkbox"/> KMS-2c3c	 Scheduled deletion	45219bf4-e6a7-415a-bd67-5c48547222fe	04/23/2018 15:59:23 GMT+08:00	Cancel Deletion
<input type="checkbox"/> KMS-1d08	 Scheduled deletion	543be26f-76e0-4b39-aeef-b573ad10ac66	04/23/2018 15:59:18 GMT+08:00	Cancel Deletion
<input type="checkbox"/> KMS-fa92	 Scheduled deletion	a415baed-191b-4871-a07d-230c516850d6	04/23/2018 15:59:14 GMT+08:00	Cancel Deletion

Step 4 In the displayed dialog box, click **OK** to cancel the scheduled deletion for the CMK.

- If the CMK is created using imported material, its status becomes **Disabled** after the cancelation. To enable the CMK, see [Enabling One or Multiple CMKs](#).
- If the CMK is created using imported material and no key material has been imported for it, its status becomes **Pending import** after the cancelation. To use the CMK, perform [Creating CMKs Using Imported Key Material](#).

 **NOTE**

To cancel the deletion of multiple CMKs at a time, select them and click **Cancel Deletion** in the upper left corner of the list.

----End

3 FAQs

3.1 What Is Key Management Service?

Key Management Service (KMS) is a secure, reliable, and easy-to-use service that helps users centrally manage and safeguard their Customer Master Keys (CMKs).

This service uses hardware security modules (HSMs) to protect CMKs. HSMs help you create and control CMKs with ease. All CMKs are protected by root keys in HSMs to avoid leakage caused by human error. KMS implements access control and log-based tracking on all operations involving CMKs. Additionally, it provides CMK operation records, meeting your audit and regulatory compliance requirements.

3.2 What Is a Customer Master Key?

A Customer Master Key (CMK) is a Key Encryption Key (KEK) created by a user using KMS. It is used to encrypt and protect Data Encryption Keys (DEKs). One CMK can be used to encrypt one or multiple DEKs.

3.3 What Is a Data Encryption Key?

A data encryption key (DEK) is used to encrypt data.

3.4 Why Cannot I Delete a CMK Immediately?

The decision to delete a CMK should be taken with caution. Before deletion, confirm that the CMK's encrypted data has all been migrated. Once the CMK is deleted, you will not be able to decrypt data with it. Therefore, KMS offers a waiting period of 7 to 1096 days for the deletion to finally take effect. On the scheduled day of deletion, the CMK will be permanently deleted. However, prior to the scheduled day, you can still cancel the deletion.

3.5 Which Cloud Services Can Use KMS for Encryption?

Object Storage Service (OBS), Elastic Volume Service (EVS), Image Management Service (IMS), and Scalable File Service (SFS) can use KMS for encryption.

3.6 How Does KMS Charge?

KMS is charged per use. No minimum fee is required. Once a CMK is created, it will be charged by hour. The billable items are CMKs under your account and API requests beyond the free-of-charge range.

3.7 Are Disabled CMKs Billable?

Yes.

A disabled CMK is still kept and maintained by KMS. You can enable it whenever you need it. Therefore, a disabled CMK is still billable. The billing stops only when the CMK is deleted.

A Change History

Released On	Description
2020-12-11	This is the fourth official release. Modified the section "Enabling Rotation for a CMK".
2019-11-21	This is the third official release. <ul style="list-style-type: none">• Added sections about CMK import.• Added sections about key rotation.• Added description about relationships between KMS and SFS, as well as how to use these services together with KMS.
2019-04-25	This is the second official release. Added the following FAQs: <ul style="list-style-type: none">• How Does KMS Charge?• Are Disabled CMKs Billable?
2019-04-04	This is the first official release.