ALIBABA CLOUD

Alibaba Cloud

Key Management Service

API Reference

Document Version: 20220318

Alibaba Cloud

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	**Danger:** Resetting will result in the loss of user configuration data.
Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	**Warning:** Restarting will cause business interruption. About 10 minutes are required to restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	**Notice:** If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	**Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.List of operations by function

The following tables list API operations available for use in Key Management Service (KMS).

Key service operations

- **CMK management**

  Customer master key (CMK) management operations are used to create and modify CMKs and manage their lifecycles.

Operation	Description
CreateKey	Creates a CMK. You can use key material created in KMS or import external key material to the CMK. Importing external key material is known as Bring Your Own Key (BYOK). This operation is the first step of BYOK.
GetParametersForImport	Queries key material to be imported. This operation is the second step of BYOK.
ImportKeyMaterial	Imports key material to a CMK. This operation is the final step of BYOK.
EnableKey	Changes the status of a CMK to Enabled.
DisableKey	Changes the status of a CMK to Disabled.
SetDeletionProtection	Enables or disables deletion protection for a CMK.
ScheduleKeyDeletion	Schedules the deletion of a CMK. After you call this operation, the CMK enters the Pending Deletion state. The CMK is automatically deleted after the specified waiting period elapses.
CancelKeyDeletion	Cancels the scheduled deletion of a CMK. You can cancel the scheduled deletion of a CMK before the specified waiting period elapses. After the scheduled deletion is canceled, the CMK enters the Enabled state again.
DeleteKeyMaterial	Deletes key material of a CMK. You can directly delete key material that is imported from an external source. After key material of a CMK is deleted, the CMK enters the Pending Import state.
DescribeKey	Queries the information about a CMK.
ListKeys	Queries all CMKs of the current Alibaba Cloud account in the current region.
UpdateKeyDescription	Updates the description of a CMK.

- **Key version management**

  Operations for key version management are used to rotate CMKs.

Operation	Description
DescribeKeyVersion	Queries the information about a key version.
ListKeyVersions	Queries all key versions of a CMK.
UpdateRotationPolicy	Updates the rotation policy of a symmetric CMK. If automatic rotation is enabled, KMS automatically generates a key version on a regular basis.
CreateKeyVersion	Creates a key version for a CMK. This operation is available only for asymmetric CMKs.

- **Cryptographic operations**

  You can perform cryptographic operations on data, such as data encryption and decryption. The operations in the following table are used to perform cryptographic operations.

Operation	Description
Encrypt	Encrypts data by using a specific CMK. This operation is used to encrypt data of no more than 6 KB online.
GenerateDataKey	Generates a random number and encrypts the random number with a specific CMK. The ciphertext and plaintext of the random number are returned. The random number can be used as a data key to encrypt or decrypt a large amount of local data.
GenerateDataKeyWithoutPlaintext	Generates a random number and encrypts the random number with a specific CMK. Only the ciphertext of the random number is returned. The random number can be used as a data key to encrypt or decrypt a large amount of local data.
ExportDataKey	Encrypts a data key by using a specific public key and exports the data key.
GenerateAndExportDataKey	Generates a random data key, encrypts the data key by using a specific CMK and public key, and returns the ciphertext generated by using the CMK and that generated by using the public key.
Decrypt	Decrypts the ciphertext that is generated by calling the Encrypt or GenerateDataKey operation. You do not need to specify a CMK for decryption.
ReEncrypt	Re-encrypts ciphertext. When you call this operation, KMS first decrypts the specified ciphertext and then uses a different CMK to encrypt the generated plaintext or data key. Ciphertext is returned.
AsymmetricSign	Uses the private key of an asymmetric CMK to generate a digital signature.
AsymmetricVerify	Uses the public key of an asymmetric CMK to verify a digital signature that is generated by using the private key.
AsymmetricDecrypt	Uses the private key of an asymmetric CMK to decrypt the data that is encrypted by using the public key.

Operation	Description
AsymmetricEncrypt	Uses the public key of an asymmetric CMK to encrypt data.
GetPublicKey	Queries the public key of an asymmetric CMK. You can use the public key to encrypt data or verify digital signatures offline.

- **Alias management**

  An alias is an independent object in KMS. An alias must be bound to a unique CMK. You can set the KeyId parameter in specific operations to an alias to specify a CMK.

Operation	Description
CreateAlias	Creates an alias and binds it to a CMK.
UpdateAlias	Binds an existing alias to a different CMK ID.
DeleteAlias	Deletes an alias.
ListAliases	Queries all aliases of the current Alibaba Cloud account in the current region.
ListAliasesByKeyId	Queries all aliases that are bound to a specific CMK.

Secrets Manager operations

Secrets Manager operations are used to manage, protect, distribute, and rotate secrets.

Operation	Description
CreateSecret	Creates a secret and stores the secret value in the initial version.
ListSecrets	Queries all secrets of the current Alibaba Cloud account in the current region.
DeleteSecret	Deletes a secret.
DescribeSecret	Queries the metadata of a secret.
GetSecretValue	Queries a secret value.
PutSecretValue	Stores the secret value of a new version into a secret.
UpdateSecret	Updates the metadata of a secret.
UpdateSecretVersionStage	Updates the stage label that marks a secret version.
RestoreSecret	Restores a deleted secret.
ListSecretVersionIds	Queries all versions of a secret.
GetRandomPassword	Queries a random password string.

Certificate operations

Certificate operations are used to create, delete, update, and query certificates. Certificate operations are also used to verify the signatures on certificates.

Operation	Description
CreateCertificate	Creates a certificate.
UploadCertificate	Imports a certificate and a certificate chain issued by a certificate authority (CA) into Certificates Manager.
GetCertificate	Queries a certificate that is managed by Certificates Manager.
DescribeCertificate	Queries the information about a certificate.
UpdateCertificateStatus	Updates the status of a certificate.
DeleteCertificate	Deletes a certificate and the private key and certificate chain of the certificate.
CertificatePrivateKeySign	Generates a digital signature by using a specific certificate.
CertificatePublicKeyVerify	Verifies a digital signature by using a specific certificate.
CertificatePublicKeyEncrypt	Encrypts data by using a specific certificate.
CertificatePrivateKeyDecrypt	Decrypts data by using a specific certificate.

Tag management operations

CMKs support tags. You can add multiple tags to a CMK. A tag is defined by a pair of TagKey and TagValue.

Operation	Description
TagResource	Adds tags to or modifies existing tags of a CMK or secret.
UntagResource	Removes a tag from a CMK or secret.

Operation	Description
ListResourceTags	Queries all tags of a CMK or secret.

Other operations

Operation	Description
DescribeRegions	Queries available regions for the current Alibaba Cloud account.
OpenKmsService	Activates KMS for the current Alibaba Cloud account.
DescribeAccountKmsStatus	Queries the status of KMS for the current Alibaba Cloud account.

2.Impact of CMK status on API operations

In KMS, a CMK may be in the Enabled, Disabled, or PendingDeletion state.

A BYOK-based CMK may also be in the PendingImport state. To check whether a CMK is a BYOK-based CMK, you can call the DescribeKey operation. For a BYOK-based CMK, the value of Origin is *EXTERNAL*.

In most cases, a newly created CMK is in the Enabled state. A newly created BYOK-based CMK is in the PendingImport state.

Only CMKs in the Enabled state can be used to encrypt or decrypt data or data keys. In other API operations, different results are returned depending on CMK states.

A CMK in the PendingDeletion state is deleted permanently after the scheduled waiting period elapses.

The following table lists the relationship between CMK states and expected results of API operations.

Expected result	HTTP Status Code
Success	200
Rejected.Enabled	409
Rejected.Disabled	409
Rejected.PendingDeletion	409
Rejected.PendingImport	409
Rejected.StateModifiedFailed	409

Common API operations

API operation	Enabled	Disabled	PendingDeletion	PendingImport
CreateKey	Success	Success	Success	Success
GenerateDataKey	Success	Rejected.Disabled	Rejected.PendingDeletion	Rejected.PendingImport
GenerateDataKeyWithoutPlaintext	Success	Rejected.Disabled	Rejected.PendingDeletion	Rejected.PendingImport
Encrypt	Success	Rejected.Disabled	Rejected.PendingDeletion	Rejected.PendingImport
Decrypt	Success	Rejected.Disabled	Rejected.PendingDeletion	Rejected.PendingImport
ListKeys	Success	Success	Success	Success
DescribeKey	Success	Success	Success	Success
UpdateKeyDescription	Success	Success	Rejected.PendingDeletion	Success
EnableKey	Success	Success	Rejected.StateModifiedFailed	Rejected.StateModifiedFailed
DisableKey	Success	Success	Rejected.StateModifiedFailed	Rejected.StateModifiedFailed
ScheduleKeyDeletion	Success	Success	Rejected.StateModifiedFailed	Success
CancelKeyDeletion	Rejected.StateModifiedFailed	Rejected.StateModifiedFailed	Success	Rejected.StateModifiedFailed
CreateAlias	Success	Success	Rejected.StateModifiedFailed	Success
DeleteAlias	Success	Success	Success	Success
ListAliases	Success	Success	Success	Success
TagResource	Success	Success	Rejected.PendingDeletion	Success
UntagResource	Success	Success	Rejected.PendingDeletion	Success
ListResourceTags	Success	Success	Success	Success
DescribeKeyVersion	Success	Success	Success	Success
ListKeyVersions	Success	Success	Success	Success
UpdateRotationPolicy	Success	Rejected.Disabled	Rejected.PendingDeletion	Rejected.PendingImport

Special API operations

UpdateAlias:

- This operation is affected only by the state of the destination CMK.
- When the destination CMK is in the PendingDeletion state, `Rejected.PendingDeletion` is returned. Otherwise, `Success` is returned.

BYOK-specific API operations

API operation	Enabled	Disabled	PendingDeletion	PendingImport
GetParametersForImport	Success	Success	Success	Success

API operation	Enabled	Disabled	PendingDeletion	PendingImport
ImportKeyMaterial	Success	Success	Rejected.StateModifiedFailed	Success
DeleteKeyMaterial	Success	Success	Success	Success

3.Make API requests

To send a Key Management Service (KMS) API request, you must send an HTTPS GET or HTTPS POST request to the KMS endpoint. You must add the request parameters that correspond to the API operation being called. After you call the API, the system returns a response. The request and response are encoded in UTF-8.

Request syntax

KMS API operations use the RPC protocol. You can call KMS API operations by sending HTTPS GET or HTTPS POST requests.

The request syntax is as follows:

```
https://Endpoint/?Action=xx&Parameters
```

The following table describes the parameters in the request syntax.

Parameter	Description
Endpoint	The endpoint of the KMS API. For more information, see Endpoints.
Action	The name of the operation being performed. For example, to create a customer master key (CMK), you must set the Action parameter to CreateKey.
Version	The version number of the API. The version number of the KMS API is *2016-01-20*.
Parameters	The request parameters for the operation. Separate multiple parameters with ampersands (&). Request parameters include both common parameters and operation-specific parameters. Common parameters include the API version number and authentication information. For more information, see Common parameters.

Sample requests

The following sample request is used to call the CreateKey operation to create a CMK.

> **Note** The sample requests in the KMS API reference are formatted for better readability.

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=CreateKey
Format=json
&Version=2016-01-20
&AccessKeyId=te****
&Signature=YlrFhyqDZQ1ThNYARrv3Ptaxqf****
&SignatureMethod=HMAC-SHA1
&Timestamp=2016-03-25T09:36:58Z
&SignatureVersion=1.0
...
```

Endpoints

Region	RegionId	Public endpoint	VPC endpoint
Japan (Tokyo)	ap-northeast-1	kms.ap-northeast-1.aliyuncs.com	kms-vpc.ap-northeast-1.aliyuncs.com
Singapore (Singapore)	ap-southeast-1	kms.ap-southeast-1.aliyuncs.com	kms-vpc.ap-southeast-1.aliyuncs.com
Australia (Sydney)	ap-southeast-2	kms.ap-southeast-2.aliyuncs.com	kms-vpc.ap-southeast-2.aliyuncs.com
Malaysia (Kuala Lumpur)	ap-southeast-3	kms.ap-southeast-3.aliyuncs.com	kms-vpc.ap-southeast-3.aliyuncs.com
Indonesia (Jakarta)	ap-southeast-5	kms.ap-southeast-5.aliyuncs.com	kms-vpc.ap-southeast-5.aliyuncs.com
Philippines (Manila)	ap-southeast-6	kms.ap-southeast-6.aliyuncs.com	kms-vpc.ap-southeast-6.aliyuncs.com
India (Mumbai)	ap-south-1	kms.ap-south-1.aliyuncs.com	kms-vpc.ap-south-1.aliyuncs.com
China (Hangzhou)	cn-hangzhou	kms.cn-hangzhou.aliyuncs.com	kms-vpc.cn-hangzhou.aliyuncs.com
China (Shanghai)	cn-shanghai	kms.cn-shanghai.aliyuncs.com	kms-vpc.cn-shanghai.aliyuncs.com
China (Qingdao)	cn-qingdao	kms.cn-qingdao.aliyuncs.com	kms-vpc.cn-qingdao.aliyuncs.com
China (Beijing)	cn-beijing	kms.cn-beijing.aliyuncs.com	kms-vpc.cn-beijing.aliyuncs.com
China (Zhangjiakou)	cn-zhangjiakou	kms.cn-zhangjiakou.aliyuncs.com	kms-vpc.cn-zhangjiakou.aliyuncs.com
China (Hohhot)	cn-huhehaote	kms.cn-huhehaote.aliyuncs.com	kms-vpc.cn-huhehaote.aliyuncs.com
China (Ulanqab)	cn-wulanchabu	kms.cn-wulanchabu.aliyuncs.com	kms-vpc.cn-wulanchabu.aliyuncs.com
China (Shenzhen)	cn-shenzhen	kms.cn-shenzhen.aliyuncs.com	kms-vpc.cn-shenzhen.aliyuncs.com
China (Heyuan)	cn-heyuan	kms.cn-heyuan.aliyuncs.com	kms-vpc.cn-heyuan.aliyuncs.com
China (Guangzhou)	cn-guangzhou	kms.cn-guangzhou.aliyuncs.com	kms-vpc.cn-guangzhou.aliyuncs.com
China (Chengdu)	cn-chengdu	kms.cn-chengdu.aliyuncs.com	kms-vpc.cn-chengdu.aliyuncs.com

Region	RegionId	Public endpoint	VPC endpoint
Germany (Frankfurt)	eu-central-1	kms.eu-central-1.aliyuncs.com	kms-vpc.eu-central-1.aliyuncs.com
UK (London)	eu-west-1	kms.eu-west-1.aliyuncs.com	kms-vpc.eu-west-1.aliyuncs.com
UAE (Dubai)	me-east-1	kms.me-east-1.aliyuncs.com	kms-vpc.me-east-1.aliyuncs.com
China (Hong Kong)	cn-hongkong	kms.cn-hongkong.aliyuncs.com	kms-vpc.cn-hongkong.aliyuncs.com
US (Virginia)	us-east-1	kms.us-east-1.aliyuncs.com	kms-vpc.us-east-1.aliyuncs.com
US (Silicon Valley)	us-west-1	kms.us-west-1.aliyuncs.com	kms-vpc.us-west-1.aliyuncs.com
China East 1 Finance	cn-hangzhou-finance	kms.cn-hangzhou-finance.aliyuncs.com	None
China East 2 Finance	cn-shanghai-finance-1	kms.cn-shanghai-finance-1.aliyuncs.com	kms-vpc.cn-shanghai-finance-1.aliyuncs.com
China South 1 Finance	cn-shenzhen-finance-1	kms.cn-shenzhen-finance-1.aliyuncs.com	kms-vpc.cn-shenzhen-finance-1.aliyuncs.com

Protocols

You must call KMS API operations by sending HTTPS requests.

KMS supports only Transport Layer Security (TLS) 1.0 and later versions. KMS does not support SSL 2.0 or SSL 3.0.

4.Request signatures

You must sign all API requests to ensure security. Alibaba Cloud uses the request signature to verify the identity of the API caller. If you use HTTPS to send an API request, you must include the signature in the request.

Signature overview

You must add the signature to the Key Management Service API request in the following format:

```
https://Endpoint/?SignatureVersion=1.0&SignatureMethod=HMAC-SHA1&Signature=CT9X0VtwR86fNWSnsc6v8YGOjuE%3D&
```

A signature contains the following parameters:

- SignatureMethod: the encryption method of the signature string. Set the value to HMAC-SHA1.
- SignatureVersion: the version of the signature encryption algorithm. Set the value to 1.0.
- Signature: the signature string generated after the request is symmetrically encrypted by using the AccessKey secret.

The HMAC-SHA1 algorithm specified in RFC 2104 is used for encryption. The AccessKey secret is used to calculate the hash-based message authentication code (HMAC) value of the encoded and sorted query string, and the HMAC value is used as the signature string. Request signatures include operation-specific parameters. Therefore, the signature of a request varies based on the request parameters. To calculate a signature, perform the steps in this topic.

```
Signature = Base64( HMAC-SHA1( AccessKey Secret, UTF-8-Encoding-Of(StringToSign)) )
```

Step 1: Compose and encode a string-to-sign

1. Use request parameters to construct a canonicalized query string.
   i. by arranging the request parameters (including all common and operation-specific parameters except Signature) in alphabetical order.

   > **Note** If you use the GET method to submit the request, these parameters are the part located after the question mark (?) and connected by the ampersands (&) in the request uniform resource identifier (URI).

   ii. Encode the names and values of the arranged request parameters in the request URL by using the unicode transformation format (UTF)-8 character set. The following table describes the encoding rules.

Character	Encoding rule
Uppercase letters, lowercase letters, digits, hyphens (-), underscores (_), periods (.), and tildes (~)	These characters do not need to be encoded.
Other characters	These characters must be percent encoded in `%XY` format. `XY` represents the ASCII code of the characters in hexadecimal notation. For example, double quotation marks (") are encoded as `%22`.
Extended UTF-8 characters	These characters are encoded in `%XY%ZA...` format.

Space characters	Spaces must be encoded as `%20`. Do not encode spaces as plus signs (+).
	This encoding method is different from the `application/x-www-form-urlencoded` MIME encoding algorithm (such as the `java.net.URLEncoder` class provided by the Java standard library). However, you can apply the encoding algorithm and replace the plus sign (+) in the encoded string with `%20`, the asterisk (*) with `%2A`, and `%7E` with the tilde (~). To do this, you can use the following `percentEncode` method:
	`private static final String ENCODING = "UTF-8";`
	`private static String percentEncode(String value) throws UnsupportedEncodingException`
	`{`
	`return value != null ? URLEncoder.encode(value, ENCODING).replace("+", "%20").replace("*", "%2A").replace("%7E", "~") : null;`
	`}`

   iii. Connect the encoded parameter names and their values by using equal signs (=).
   iv. Sort the connected parameter name and value pairs in the order specified in step i and connect the pairs by using ampersands (&) to obtain the canonicalized query string.
2. Use the canonicalized query string to construct a string-to-sign in the following way:

```
StringToSign=
      HTTPMethod + "&" +
      percentEncode("/") + "&" +
       percentEncode(CanonicalizedQueryString)
```

In the preceding rules:

- HTTPMethod: the HTTP method used to submit a request, such as GET.
- percentEncode("/"): specifies the encoded value (%2F) of a forward slash (/). The encoding follows the URL encoding rules.
- percentEncode(CanonicalizedQueryString): specifies the encoded canonicalized query string based on the URL encoding rules.

Step 2: Calculate the signature string

1. Calculate the HMAC value of the string-to-sign based on RFC 2104.

   > **Note** Use the SHA1 algorithm to calculate the HMAC value of the string-to-sign. The combination of your AccessKey secret and an ampersand (&) (ASCII code 38) that follows the secret is used as the key for the HMAC calculation.

2. Encode the HMAC value in Base64 to obtain the signature string
3. Add the signature string to the request as the Signature parameter.

> **Note** When the obtained signature value is submitted as the final request parameter value, the value must be URL-encoded like other parameters based on rules defined in RFC 3986.

Examples

The CreateKey operation is used as an example to introduce the signature method.

Request URL before the request is signed:

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=CreateKey
&SignatureVersion=1.0
&Format=json
&Version=2016-01-20
&AccessKeyId=testid
&SignatureMethod=HMAC-SHA1
&Timestamp=2016-03-28T03:13:08Z
```

`StringToSign` for the request URL:

```
GET&%2F&AccessKeyId%3Dtestid%26Action%3DCreateKey%26Format%3Djson%26SignatureMethod%3DHMAC-SHA1%26SignatureVersion%3D1.0%26Timestamp%3D2016-03-28T03%
253A13%253A08Z%26Version%3D2016-01-20
```

If the AccessKey ID is testid and the AccessKey secret is testsecret, the key that is used to calculate the HMAC value of the string-to-sign is testsecret&.

The signature value is `41wk2SSX1GJh7fwnc5eqOfiJPF****`.

Request URL after the request is signed:

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=CreateKey
&SignatureVersion=1.0
&Format=json
&Version=2016-01-20
&AccessKeyId=testid
&SignatureMethod=HMAC-SHA1
&Timestamp=2016-03-28T03:13:08Z
&Signature=41wk2SSX1GJh7fwnc5eqOfiJPF****
```

5.Common parameters

This topic describes the parameters that are common to all API requests and responses.

Common request parameters

Parameter	Type	Required	Description
Format	String	No	The response format. Valid values: • JSON (default) • XML
Version	String	Yes	The version number of the API. The value must be in the YYYY-MM-DD format. Set the value to 2016-01-20.
AccessKeyId	String	Yes	The AccessKey ID provided to you by Alibaba Cloud.
Signature	String	Yes	The signature string of the current request.
SignatureMethod	String	Yes	The encryption method of the signature string. Set the value to HMAC-SHA1.
Timestamp	String	Yes	The timestamp of the request. Specify the time in the ISO 8601 standard in the yyyy-MM-ddTHH:mm:ssZ format. The time must be in UTC. For example, use 2013-01-10T12:00:00Z to indicate January 10, 2013, 20:00:00 (UTC+8).
SignatureVersion	String	Yes	The version of the signature encryption algorithm. Set the value to 1.0.

Sample requests

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=CreateKey
Format=json
&Version=2016-01-20
&AccessKeyId=te****
&Signature=YlrFhyqDZQ1ThNYARrv3Ptaxqf****
&SignatureMethod=HMAC-SHA1
&Timestamp=2016-03-25T09:36:58Z
&SignatureVersion=1.0
```

Common response parameters

Responses can be returned in either the JSON or XML format. You can specify the response format in the request. The default response format is JSON. Every response returns a unique RequestId regardless of whether the call is successful.

- An HTTP `2xx` status code indicates a successful call.
- An HTTP `4xx` or `5xx` status code indicates a failed call.

Sample responses

- XML format

```
<?xml version="1.0" encoding="utf-8"?>
    <!--Result Root Node-->
    <KMS>
        <!--Return Request Tag-->
        <RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
        <!--Return Result Data-->
    </KMS>
```

- JSON format

```
{
    "RequestId":"4C467B38-3910-447D-87BC-AC049166F216"
    /*Return Result Data*/
}
```

6.Sample responses

API responses use the HTTP response format where a 2xx status code indicates a successful call and a 4xx or 5xx status code indicates a failed call. Sample responses in API Reference are formatted in a way that is easier for you to read. The actual responses are not formatted with line breaks or indentation.

Sample success responses

`XML` format

```
<?xml version="1.0" encoding="UTF-8"?>
<!--Result Root Node-->
<Interface Name+Response>
    <!--Return Request Tag-->
    <RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
    <!--Return Result Data-->
</Interface Name+Response>
```

`JSON` format

```
{
    "RequestId": "4C467B38-3910-447D-87BC-AC049166F216",
    /* Return Result Data */
}
```

Sample error responses

If an error occurs when you call an API operation, no result data is returned. You can troubleshoot an error based on error codes specific to an API operation and error codes described in the Common error codes section of this topic.

If an error occurs when you call an API operation, the HTTP status code, error code, error message, and ID of the request are returned in the response. If you cannot troubleshoot the error based on the error code and error message, you can provide Alibaba Cloud technical support with the ID of the request to locate the request log. The following sample responses indicate the error that occurs when the required timestamp is not provided.

`XML` format

```
<KMS>
     <HttpStatus>400</HttpStatus>
     <Code>IllegalTimestamp</Code>
     <Message>The input parameter "Timestamp" that is mandatory for processing this request is not supplied.</Message>
     <RequestId>3b237773-bc2c-4bea-95fc-319a1a5baa68</RequestId>
</KMS>
```

`JSON` format

```
{
     "HttpStatus": 400,
     "Code": "IllegalTimestamp",
     "Message": "The input parameter \"Timestamp\" that is mandatory for processing this request is not supplied.",
     "RequestId": "e85db688-a2d3-44ca-9790-4259f59e90d8"
}
```

Common error codes

Error code	Error message	HTTP status code
InternalFailure	Internal Failure.	500
ServiceUnavailableTemporary	Service Unavailable Temporary.	503
InvalidAccessKeyId.NotFound	The AccessKey ID provided does not exist in our records.	404
Forbidden.KeyNotFound	The specified Key is not found.	404
Forbidden.KeyVersionNotFound	The specified Key version is not found.	404
Forbidden.AliasNotFound	The specified Alias is not found.	404
Forbidden.NoPermission	This operation is forbidden by permission system.	403
Forbidden.AccessKey	This AccessKey is not enabled.	403
UnsupportedHTTPMethod	This http method is not supported.	403
Forbidden.UbsmsInvalidUserid	Userid Invalid For Ubsms.	403
Forbidden.UbsmsInvalidBid	Your account partner does not have KMS Service.	403
Forbidden.KmsServiceNotEnabled	Kms service is not Enabled for current user. Please get access permission first.	403
Forbidden.ProhibitedByRiskControl	Current user is Prohibited By Risk Control.	403
Forbidden.InDebtOverdue	Current user is indebted Overdue.	403

Error code	Error message	HTTP status code
Forbidden.InDebt	Current user is indebted.	403
ParseRequestParameterException	Server parse parameters exception. Please check your input params.	400
MissingParameter	The parameter "< parameter name >" is needed but not provided.	400
InvalidParameter	The specified parameter "< parameter name >" is not valid.	400
IncompleteSignature	The request signature does not conform to Alibaba Cloud standards.	400
IllegalTimestamp	The input parameter "Timestamp" that is required for processing this request is not supplied.	400
Rejected.LimitExceeded	The request was rejected because user create resource limit was exceeded.	400
AliasAlreadyExists	AliasName Already Exists.	400
InvalidKeyMaterial	key material is invalid.	400
InvalidImportToken	import token is invalid.	400
ExpiredImportToken	import token is expired.	400
Unsupported.Origin	This key origin is not valid for this api.	400
Unsupported.Alias	Alias is not valid for this api.	400
Unsupported.ProtectionLevel	This protection level is not valid for this region	400
Rejected.StateModifiedFailed	Keystate modified failed.	409
Rejected.Disabled	The request was rejected because the key state is Disabled.	409
Rejected.PendingDeletion	The request was rejected because the key state is PendingDeletion.	409
Rejected.PendingImport	The request was rejected because the key state is PendingImport.	409

7.Obtain an AccessKey pair

You can create an AccessKey pair for an Alibaba Cloud account or a RAM user. When you call API operations, you must use the AccessKey pair to complete identity verification.

Context

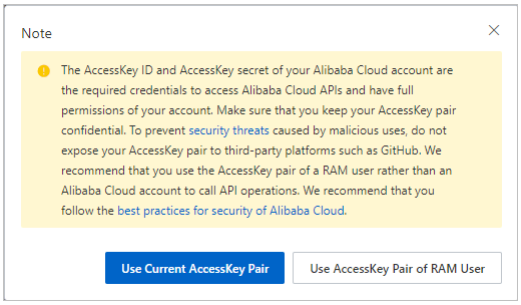
An AccessKey pair consists of an AccessKey ID and an AccessKey secret.

- The AccessKey ID is used to identify a user.
- The AccessKey secret is used to verify the identity of the user. You must keep your AccessKey secret strictly confidential.

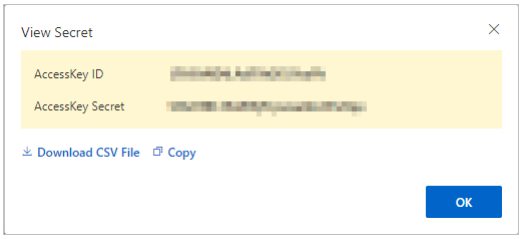
Warning If the AccessKey pair of your Alibaba Cloud account is leaked, your resources are exposed to potential risks. We recommend that you use the AccessKey pair of a RAM user to call API operations. This prevents the AccessKey pair of your Alibaba Cloud account from being leaked.

Procedure

1. Log on to the Alibaba Cloud Management Console by using your Alibaba Cloud account.
2. In the upper-right corner of the page, move the pointer over the profile picture and click **AccessKey Management**.
3. In the **Note** dialog box, click Use Current AccessKey Pair or Use AccessKey Pair of RAM User.



   - Obtain the AccessKey pair of the Alibaba Cloud account
     a. In the Note dialog box, click **Use Current AccessKey Pair**.
     b. On the **AccessKey Pair** page, click **Create AccessKey Pair**.
     c. In the **View Secret** dialog box, view the AccessKey ID and AccessKey secret. Click **Download CSV File** to download the AccessKey pair or click **Copy** to copy the AccessKey pair.

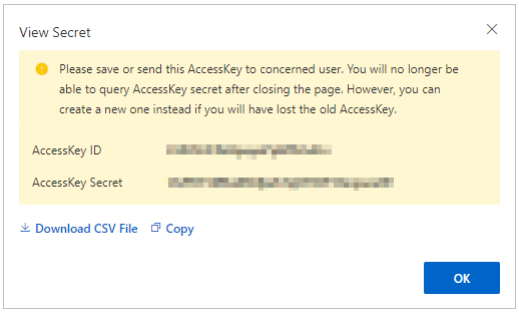


   - Obtain the AccessKey pair of a RAM user
     a. Click **Use AccessKey Pair of RAM User**. Then, you are redirected to the RAM console.
     b. On the **Users** page of the RAM console, find the RAM user whose AccessKey pair you want to obtain.

     Note If you do not have a RAM user, create one first. For more information, see Create a RAM user.

     c. Click the name of the RAM user in the User Logon Name/Display Name column.
     d. In the **User AccessKeys** section of the **Authentication** tab, click **Create AccessKey**.

e. In the **View Secret** dialog box, view the AccessKey ID and AccessKey secret. Click **Download CSV File** to download the AccessKey pair or click **Copy** to copy the AccessKey pair.



Note

- An AccessKey secret is displayed only after you click Create AccessKey. You cannot query the AccessKey secret in subsequent operations. Therefore, you must back up your AccessKey secret.
- If your AccessKey pair is leaked or lost, you must create another AccessKey pair. You can create a maximum of two AccessKey pairs for each RAM user.

8.Key

8.1. CreateKey

Creates a customer master key (CMK).

Usage notes

A CMK can be symmetric or asymmetric. Symmetric CMKs are used to generate data keys that can be used to encrypt large amounts of data. You can also use symmetric CMKs to encrypt less than 6 KB of data. For more information, see GenerateDataKey. Asymmetric CMKs are used to encrypt data, decrypt data, generate digital signatures, and verify digital signatures. However, you cannot use asymmetric CMKs to generate data keys.

The following table describes different types of CMKs and the operations that are supported by the CMKs.

CMK category	CMK type	Description	Encryption and decryption	Signature generation and verification
Symmetric CMK	Aliyun_AES_256	An advanced Encryption Standard (AES) key with a length of 256 bits.	Supported	Not supported
Symmetric CMK	Aliyun_AES_128	An AES key with a length of 128 bits. Only Dedicated KMS supports this CMK type.	Supported	Not supported
Symmetric CMK	Aliyun_AES_192	An AES key with a length of 192 bits. Only Dedicated KMS supports this CMK type.	Supported	Not supported
Symmetric CMK	Aliyun_SM4	SM4 key.	Supported	Not supported
Asymmetric CMK	RSA_2048	A Rivest-Shamir-Adleman (RSA) key with a length of 2,048 bits.	Supported	Supported
Asymmetric CMK	RSA_3072	A RSA key with a length of 3,072 bits.	Supported	Supported
Asymmetric CMK	EC_P256	National Institute of Standards and Technology (NIST) P-256 (secp256r1) .	Not supported	Supported
Asymmetric CMK	EC_P256K	Standards for Efficient Cryptography Group (SECG) elliptic curve secp256k1.	Not supported	Supported
Asymmetric CMK	EC_SM2	256-bit elliptic curve over the prime field that is defined in GB/T 32918.	Supported	Supported

Note

- If the value of the KeySpec parameter that is used to create a symmetric CMK is prefixed with `Aliyun_`, a standard cryptographic algorithm is used, but non-standard ciphertext is generated. An asymmetric CMK can be used to generate standard ciphertext or signatures.
- You can use an RSA CMK to perform one of the two types of operations: encrypt and decrypt data, and generate and verify signatures. You cannot use the RSA CMK to perform both two types of operations.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	CreateKey	The operation that you want to perform. Set the value to CreateKey.
Description	String	No	key description example	The description of the CMK. The description can be 0 to 8,192 characters in length.

Parameter	Type	Required	Example	Description
KeySpec	String	No	Aliyun_AES_256	The type of the CMK. Valid values: • Aliyun_AES_256 • Aliyun_AES_128 • Aliyun_AES_192 • Aliyun_SM4 • RSA_2048 • RSA_3072 • EC_P256 • EC_P256K • EC_SM2 Note • The default type of the CMK is Aliyun_AES_256. • Only Dedicated KMS supports Aliyun_AES_128 and Aliyun_AES_192.
KeyUsage	String	No	ENCRYPT/DECRYPT	The usage of the CMK. Valid values: • ENCRYPT/DECRYPT: encrypts or decrypts data. • SIGN/VERIFY: generates or verifies a digital signature.
Origin	String	No	Aliyun_KMS	The source of key material. Valid values: • Aliyun_KMS (default value) • EXTERNAL Note • The value of this parameter is case-sensitive. • If you set the KeySpec parameter to an asymmetric CMK type, you are not allowed to set the Origin parameter to EXTERNAL. • If you set the Origin parameter to EXTERNAL, you must import key material. For more information, see Import key material.
ProtectionLevel	String	No	SOFTWARE	The protection level of the CMK. Valid values: • SOFTWARE (default value) • HSM Note • The value of this parameter is case-sensitive. • Assume that you set this parameter to HSM. If you set the Origin parameter to Aliyun_KMS, the CMK is created in a managed hardware security module (HSM). If you set the Origin parameter to EXTERNAL, you can import an external key to the managed HSM.
EnableAutomaticRotation	Boolean	No	false	Specifies whether to enable automatic key rotation. Valid values: • true • false (default value) Note If you set the Origin parameter to EXTERNAL or the KeySpec parameter to an asymmetric CMK type, automatic key rotation is unavailable.
RotationInterval	String	No	365d	The interval for automatic key rotation. Specify the value in the integer[unit] format. The following units are supported: d (day), h (hour), m (minute), and s (second). For example, you can use either 7d or 604800s to specify a seven-day interval. The interval can range from 7 days to 730 days. Note If you set the EnableAutomaticRotation parameter to true, you must also specify this parameter. If you set the EnableAutomaticRotation parameter to false, you can leave this parameter unspecified.

For more information about common request parameters, see Common parameters.

Response parameters

Parameter	Type	Example	Description
KeyMetadata	Struct		The metadata of the CMK.
Arn	String	acs:kms:cn-qingdao:154035569884****:key/d6bee1cb-2e14-4277-ba6b-73786b21****	The Alibaba Cloud Resource Name (ARN) of the CMK.
AutomaticRotation	String	Disabled	Indicates whether automatic key rotation is enabled. Valid values: • Enabled: Automatic key rotation is enabled. • Disabled: Automatic key rotation is disabled. • Suspended: Automatic key rotation is suspended. For more information, see Automatic key rotation. Note Automatic key rotation is available only for symmetric CMKs.
CreationDate	String	2016-03-25T10:42:40Z	The time when the CMK was created. The time is displayed in UTC.
Creator	String	154035569884****	The creator of the CMK.
DeleteDate	String	2020-07-06T18:22:03Z	The time when the CMK is scheduled for deletion. For more information, see ScheduleKeyDeletion. Note This value is returned only when the value of the KeyState parameter is PendingDeletion.
Description	String	key description example	The description of the CMK.
KeyId	String	d6bee1cb-2e14-4277-ba6b-73786b21****	The ID of the CMK. The ID is globally unique.
KeySpec	String	Aliyun_AES_256	The type of the CMK.
KeyState	String	Enabled	The status of the CMK. For more information, see Impact of CMK status on API operations.
KeyUsage	String	ENCRYPT/DECRYPT	The usage of the CMK.
LastRotationDate	String	2019-06-06T18:22:03Z	The time when the last rotation was performed. The time is displayed in UTC. For a new CMK, the value of this parameter is the time when the initial version of the CMK was generated.
MaterialExpireTime	String	2020-07-06T18:22:03Z	The time when the key material for the CMK expires. The time is displayed in UTC. If the parameter is empty, the key material of the CMK does not expire.
NextRotationDate	String	2020-07-06T18:22:03Z	The time when the next rotation will be performed. Note This value is returned only when the value of the AutomaticRotation parameter is Enabled or Suspended.
Origin	String	Aliyun_KMS	The source of the key material for the CMK.
PrimaryKeyVersion	String	7ce1d081-06cb-42e6-aab6-5c5de030****	The ID of the primary key version of the symmetric CMK. Note • The primary key version of a symmetric CMK is an active encryption key. KMS uses the primary key version of a specified CMK to encrypt data. • This parameter is unavailable for asymmetric CMKs.

Parameter	Type	Example	Description
ProtectionLevel	String	SOFTWARE	The protection level of the CMK.
RotationInterval	String	31536000s	The period of automatic key rotation. Unit: seconds. The value is in the format of an integer followed by the letter s. For example, if the rotation period is seven days, this parameter is set to 604800s. This value is returned only when the value of the AutomaticRotation parameter is Enabled or Suspended.
RequestId	String	36c7e41a-3f2c-45f7-9bdd-d1dc1e7e7e06	The ID of the request.

Examples

Sample requests

```
https://[Endpoint]/?Action=CreateKey
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
      <KeyMetadata>
            <CreationDate>2021-04-12T06:00:54Z</CreationDate>
            <Description></Description>
            <KeyId>d6bee1cb-2e14-4277-ba6b-73786b21****</KeyId>
            <KeySpec>Aliyun_AES_256</KeySpec>
            <KeyState>Enabled</KeyState>
            <KeyUsage>ENCRYPT/DECRYPT</KeyUsage>
            <PrimaryKeyVersion>7ce1d081-06cb-42e6-aab6-5c5de030****</PrimaryKeyVersion>
            <DeleteDate></DeleteDate>
            <Creator>154035569884****</Creator>
            <Arn>acs:kms:cn-qingdao:154035569884****:key/d6bee1cb-2e14-4277-ba6b-73786b21****</Arn>
            <Origin>Aliyun_KMS</Origin>
            <MaterialExpireTime></MaterialExpireTime>
            <ProtectionLevel>SOFTWARE</ProtectionLevel>
            <LastRotationDate>2021-04-12T06:00:54Z</LastRotationDate>
            <AutomaticRotation>Disabled</AutomaticRotation>
      </KeyMetadata>
      <RequestId>36c7e41a-3f2c-45f7-9bdd-d1dc1e7e7e06</RequestId>
</KMS>
```

`JSON` format

```
{
  "KeyMetadata": {
    "CreationDate": "2021-04-12T06:00:54Z",
    "Description": "",
    "KeyId": "d6bee1cb-2e14-4277-ba6b-73786b21****",
    "KeySpec": "Aliyun_AES_256",
    "KeyState": "Enabled",
    "KeyUsage": "ENCRYPT/DECRYPT",
    "PrimaryKeyVersion": "7ce1d081-06cb-42e6-aab6-5c5de030****",
    "DeleteDate": "",
    "Creator": "154035569884****",
    "Arn": "acs:kms:cn-qingdao:154035569884****:key/d6bee1cb-2e14-4277-ba6b-73786b21****",
    "Origin": "Aliyun_KMS",
    "MaterialExpireTime": "",
    "ProtectionLevel": "SOFTWARE",
    "LastRotationDate": "2021-04-12T06:00:54Z",
    "AutomaticRotation": "Disabled"
  },
  "RequestId": "36c7e41a-3f2c-45f7-9bdd-d1dc1e7e7e06"
}
```

Error codes

For a list of error codes, visit the API Error Center.

8.2. GetParametersForImport

Obtains the parameters that are used to import key material for a customer master key (CMK).

Usage notes

- The returned parameters can be used to call the ImportKeyMaterial operation.
- You can import key material only for CMKs whose Origin parameter is set to EXTERNAL.
- The public key and import token that are returned when you call the GetParametersForImport operation must be used together. The public key and import token can be used to import key material only for CMKs that are specified for the call.
- The public key and import token that are returned by each call of the GetParametersForImport operation must be unique.

- You must specify the type of the public key and the encryption algorithm that are used to encrypt key material. The following table lists the types of public keys and the encryption algorithms that are supported for each type.

Public key type	Encryption algorithm	Description
RSA_2048	RSAES_PKCS1_V1_5 RSAES_OAEP_SHA_1 RSAES_OAEP_SHA_256	Keys of all regions and all protection levels are supported. Dedicated Key Management Service (KMS) does not support RSAES_OAEP_SHA_1.
EC_SM2	SM2PKE	The SM2 algorithm is developed and approved by the State Cryptography Administration of China. The SM2 algorithm can be used only to import key material for a CMK whose ProtectionLevel is set to HSM. KMS supports the SM2 algorithm by using a managed hardware security module (HSM) that is deployed in mainland China. For more information, see Overview of Managed HSM.

This topic provides an example on how to import key material for a CMK whose ID is `1234abcd-12ab-34cd-56ef-12345678****` by using the `RSAES_PKCS1_V1_5` encryption algorithm and a public key of the `RSA_2048` type. The returned parameters include the ID of the CMK, the pubic key that is used to encrypt key material, the import token that is used to import key material, and the time when the import token expires.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	GetParametersForImport	The operation that you want to perform. Set the value to GetParametersForImport.
KeyId	String	Yes	1234abcd-12ab-34cd-56ef-12345678****	The ID of the CMK. The ID is globally unique. **Note** You can import key material only for CMKs whose Origin parameter is set to EXTERNAL.
WrappingAlgorithm	String	Yes	RSAES_PKCS1_V1_5	The algorithm that is used to encrypt key material.
WrappingKeySpec	String	Yes	RSA_2048	The type of the public key that is used to encrypt key material.

For more information about common request parameters, see Common parameters.

Response parameters

Parameter	Type	Example	Description
ImportToken	String	Base64String	The import token that is used to import key material. The import token is valid for 24 hours. The value of this parameter is required when you call the ImportKeyMaterial operation.
KeyId	String	1234abcd-12ab-34cd-56ef-12345678****	The ID of the CMK. The ID is globally unique. The value of this parameter is required when you call the ImportKeyMaterial operation.
PublicKey	String	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAlls4uIBxD0GG84C+lGBO6Dhpf1J3XimC6cPmPNaKKJMOzoX4tD+C+r7aZv8lZ3vnPfxuxvy/YwG+whUxTEEFUdqJTOlzhPfYucupqKM92crVHluG+xtMVeHKjyTr+UrtKCsQikqHT+19yDRN/RMoo2HUx0gmEnRyXd8t3JyUXun9FdoxKA08GrsV7nodb9ZsoBLhnev7tTLcXvLyKW6XG1ZQCQm6dPnbnwLeDXR7uK0Lqn9PM28mBldaiQUQxj2XbM1CoJA+JiyVX3Ptdb+4rqukb4Rb05B80Bs9xV/cf7Flku08l7xGhrGiQFq+DFXwQWtwihXHZxz3LhldU+4ZPwID****	The public key that is used to encrypt key material. The public key is encoded in Base64.
RequestId	String	8cdf51fd-bcd6-d79a-0ef4-e52c9b5466dc	The ID of the request.

Parameter	Type	Example	Description
TokenExpireTime	String	2018-01-25T00:01:02Z	The time when the import token expires.

Examples

Sample requests

```
https://[Endpoint]/?Action=GetParametersForImport
&KeyId=1234abcd-12ab-34cd-56ef-12345678****
&WrappingAlgorithm=RSAES_PKCS1_V1_5
&WrappingKeySpec=RSA_2048
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
    <ImportToken>Base64String</ImportToken>
    <PublicKey>MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAlls4uIBxD0GG84C+lGBO6Dhpf1J3XimC6cPmPNaKKJMOzoX4tD+C+r7aZv8lZ3vnPfxuxvy/YwG+whUxTEEFUdqJTO
IzhPfYucupqKM92crVHIuG+xtMVeHKjyTr+UrtKCsQikqHT+19yDRN/RMoo2HUx0gmEnRyXd8t3JyUXun9FdoxKA08GrsV7nodb9ZsoBLhnev7tTLcXvLyKW6XG1ZQCQm6dPnbnwLeDXR7uK0Lqn9
PM28mBIdaiQUQxj2XbM1CoJA+JiyVX3Ptdb+4rqukb4Rb05B80Bs9xV/cf7FIku08l7xGhrGiQFq+DFXwQWtwihXHZxz3LhldU+4ZPwID****</PublicKey>
    <KeyId>1234abcd-12ab-34cd-56ef-12345678****</KeyId>
    <TokenExpireTime>2018-01-25T00:01:02Z</TokenExpireTime>
    <RequestId>8cdf51fd-bcd6-d79a-0ef4-e52c9b5466dc</RequestId>
</KMS>
```

`JSON` format

```
{
        "ImportToken":"Base64String",
        "PublicKey":"MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAlls4uIBxD0GG84C+lGBO6Dhpf1J3XimC6cPmPNaKKJMOzoX4tD+C+r7aZv8lZ3vnPfxuxvy/YwG+whUxTEEF
UdqJTOIzhPfYucupqKM92crVHIuG+xtMVeHKjyTr+UrtKCsQikqHT+19yDRN/RMoo2HUx0gmEnRyXd8t3JyUXun9FdoxKA08GrsV7nodb9ZsoBLhnev7tTLcXvLyKW6XG1ZQCQm6dPnbnwLeDXR7u
K0Lqn9PM28mBIdaiQUQxj2XbM1CoJA+JiyVX3Ptdb+4rqukb4Rb05B80Bs9xV/cf7FIku08l7xGhrGiQFq+DFXwQWtwihXHZxz3LhldU+4ZPwID****",
        "KeyId":"1234abcd-12ab-34cd-56ef-12345678****",
        "TokenExpireTime":"2018-01-25T00:01:02Z",
        "RequestId":"8cdf51fd-bcd6-d79a-0ef4-e52c9b5466dc"
}
```

Error codes

For a list of error codes, visit the API Error Center.

8.3. ImportKeyMaterial

Call the ImportKeyMaterial operation to import the key material.

Call CreateKey when creating a CMK, you can select its key material source as external. **Origin** set to **EXTERNAL**. This API is used to import the key material into the CMK.

- To view the CMK **Origin**, see DescribeKey.
- Before importing key material, you need to call the GetParametersForImport obtain the parameters required to import the key material, including the public key and import token.

> **Note**
> - The key type of the pair is **Aliyun_AES_256** the key material must be 256 bits. The key type must be **Aliyun_SM4** the CMK and key material must be 128 bits.
> - You can set the expiration time for the key material, or you can set it to never expire.
> - You can reimport the key material and reset the expiration time for the specified CMK at any time, but the same key material must be imported.
> - After the imported key material expires or is deleted, the specified CMK is unavailable until the same key material are imported again.
> - A Key material can be imported to multiple cmks, but any Data or Data Key encrypted by one CMK cannot be decrypted by another CMK.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ImportKeyMaterial	The operation that you want to perform. Set the value to **ImportKeyMaterial**.

Parameter	Type	Required	Example	Description
EncryptedKeyMaterial	String	Yes	bCPZx7I6v6KXsqEpr2OXKxuj2CCRtKdwp75Bw+BGncYqBdfjFBYRtOE6HRlT0oeiRDWzwnw9OA54OL36smDJrq4Lo9x0CyYDiuKnRkcKtMtlzW0din7Pd7IlZWWRdVueiw2qpzl7PkUWQGTdsdbzpfJJQ+qj/cRIrk/E83UGyeyytSpgnb+lu0xEYcPajRyWNsbi98N3pqqQzHXNNHO2NJqHlnQgglqTiBEjkGeKFhfKmTc3vjulIdVa3EaVIN6lwWfgx+UUYSrvbA77WDYKlDsZ4SbK2/T7za9Tp1qU7Ynqba7OKGVVj7PMbiaO80AxWZnjUMYCgEp5w7V+seOXqw==	Use **GetParametersForImport** the Returned public key and the base64-encoded key material.
ImportToken	String	Yes	Base64String	By calling **GetParametersForImport** the import token.
KeyId	String	Yes	1234abcd-12ab-34cd-56ef-12345678****	The ID of the CMK to be imported.
KeyMaterialExpireUnix	Long	Yes	0	The time when the key material expires. If this parameter is not specified or set this parameter to 0, the key material does not expire. **Note** The value cannot be earlier than the time when the API is called (based on the server time).

Response parameters

Prameter	Type	Sample response	Description
RequestId	String	ec1017 cf-ead4-f3ca-babc-c3b34f3dbecb	The ID of the request.

Examples

Sample requests

```
https://[Endpoint]/? Action=ImportKeyMaterial
&EncryptedKeyMaterial=bCPZx7I6v6KXsqEpr2OXKxuj2CCRtKdwp75Bw+BGncYqBdfjFBYRtOE6HRlT0oeiRDWzwnw9OA54OL36smDJrq4Lo9x0CyYDiuKnRkcKtMtlzW0din7Pd7IlZWWRdVueiw2qpzl7PkUWQGTdsdbzpfJJQ+qj/cRIrk/E83UGyeyytSpgnb+lu0xEYcPajRyWNsbi98N3pqqQzHXNNHO2NJqHlnQgglqTiBEjkGeKFhfKmTc3vjulIdVa3EaVIN6lwWfgx+UUYSrvbA77WDYKlDsZ4SbK2/T7za9Tp1qU7Ynqba7OKGVVj7PMbiaO80AxWZnjUMYCgEp5w7V+seOXqw==
&ImportToken=Base64String
&KeyId=1234abcd-12ab-34cd-56ef-12345678****
&KeyMaterialExpireUnix=0
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
    <RequestId>ec1017cf-ead4-f3ca-babc-c3b34f3dbecb</RequestId>
</KMS>
```

`JSON` format

```
{
        "RequestId":"ec1017cf-ead4-f3ca-babc-c3b34f3dbecb"
}
```

Error codes

For a list of error codes, visit the API Error Center.

8.4. EnableKey

Enables a customer master key (CMK) to encrypt and decrypt data.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description

Parameter	Type	Required	Example	Description
Action	String	Yes	EnableKey	The operation that you want to perform. Set the value to EnableKey.
KeyId	String	Yes	1234abcd-12ab-34cd-56ef-12345678****	The globally unique ID of the CMK.

Response parameters

Parameter	Type	Example	Description
RequestId	String	efb1cbbd-a093-4278-bc03-639dd4fcc207	The ID of the request.

Examples

Sample requests

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=EnableKey
&KeyId=1234abcd-12ab-34cd-56ef-12345678****
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
      <RequestId>efb1cbbd-a093-4278-bc03-639dd4fcc207</RequestId>
</KMS>
```

`JSON` format

```
{
"RequestId": "efb1cbbd-a093-4278-bc03-639dd4fcc207"
}
```

Error codes

For a list of error codes, visit the API Error Center.

8.5. DisableKey

Disables a specified CMK.

If a customer master key (CMK) is disabled, the ciphertext encrypted by using this CMK cannot be decrypted until you re-enable it. You can call the EnableKey operation to enable the CMK.

In this example, the CMK whose ID is `1234abcd-12ab-34cd-56ef-12345678****` is disabled.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DisableKey	The operation that you want to perform. Set the value to DisableKey.
KeyId	String	Yes	1234abcd-12ab-34cd-56ef-12345678****	The ID of the CMK. The ID must be globally unique.

For more information about common request parameters, see Common parameters.

Response parameters

Parameter	Type	Example	Description
RequestId	String	2fe70ce2-3303-4fd6-b3ac-472fb2705c62	The ID of the request.

Examples

Sample requests

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=DisableKey
&KeyId=1234abcd-12ab-34cd-56ef-12345678****
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
      <RequestId>2fe70ce2-3303-4fd6-b3ac-472fb2705c62</RequestId>
</KMS>
```

`JSON` format

```
{
    "RequestId": "2fe70ce2-3303-4fd6-b3ac-472fb2705c62"
}
```

Error codes

For a list of error codes, visit the API Error Center.

8.6. SetDeletionProtection

Enables or disables deletion protection for a customer master key (CMK).

Precautions:

- After you enable deletion protection for a CMK, you cannot delete the CMK. If you want to delete the CMK, you must first disable deletion protection for the CMK.
- Before you can call the SetDeletionProtection operation, make sure that the required CMK is not in the Pending Deletion state. You can call the DescribeKey operation to query the CMK status, which is specified by the KeyState parameter.

You can enable deletion protection for the CMK whose Alibaba Cloud Resource Name (ARN) is `acs:kms:cn-hangzhou:123213123****:key/0225f411-b21d-46d1-be5b-93931c82****` by using parameter settings provided in this topic. The CMK ARN is specified by the ProtectedResourceArn parameter.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	SetDeletionProtection	The operation that you want to perform. Set the value to SetDeletionProtection.
EnableDeletionProtection	Boolean	Yes	true	Specifies whether to enable deletion protection. Valid values: • true: enables deletion protection • false: disables deletion protection
ProtectedResourceArn	String	Yes	acs:kms:cn-hangzhou:123213123****:key/0225f411-b21d-46d1-be5b-93931c82****	The ARN of the CMK for which you want to set deletion protection. You can call the DescribeKey operation to query the CMK ARN.
DeletionProtectionDescription	String	No	The CMK is being used by XXX. Deletion protection is set.	The description of deletion protection. Note This parameter takes effect only when you set the EnableDeletionProtection parameter to true.

For more information about common request parameters, see Common parameters.

Response parameters

Parameter	Type	Example	Description
RequestId	String	3455b9b4-95c1-419d-b310-db6a53b09a39	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=SetDeletionProtection
&EnableDeletionProtection=true
&ProtectedResourceArn=acs:kms:cn-hangzhou:123213123****:key/0225f411-b21d-46d1-be5b-93931c82****
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
      <RequestId>3455b9b4-95c1-419d-b310-db6a53b09a39</RequestId>
</KMS>
```

`JSON` format

```
{
    "RequestId":"3455b9b4-95c1-419d-b310-db6a53b09a39"
}
```

Error codes

For a list of error codes, visit the API Error Center.

8.7. ScheduleKeyDeletion

Deletes a specified CMK.

During the scheduled deletion time, the CMK is in the PendingDeletion state and cannot be used to encrypt data, decrypt data, or generate data keys.

After a CMK is deleted, it cannot be recovered, and the data and ciphertext data keys encrypted by using this CMK cannot be decrypted. Therefore, to prevent you from deleting CMKs by mistake, KMS allows you to only schedule key deletion tasks. You cannot immediately delete CMKs. If you want to delete a CMK, call the DisableKey operation to disable it.

You must specify a waiting period of 7 to 30 days when you call this operation. The waiting period starts from the time you submit the request. You can call the CancelKeyDeletion operation to cancel the deletion before the waiting period ends.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ScheduleKeyDeletion	The operation that you want to perform. Set the value to ScheduleKeyDeletion.
KeyId	String	Yes	1234abcd-12ab-34cd-56ef-12345678****	The globally unique ID of the CMK.
PendingWindowInDays	Integer	No	7	The number of days before the CMK is deleted. During this period, the CMK is in the PendingDeletion state. After this period ends, you cannot cancel the deletion. Valid values: 7 to 30. Unit: days.

Response parameters

Parameter	Type	Example	Description
RequestId	String	3da5b8cc-8107-40ac-a170-793cd181d7b7	The ID of the request.

Examples

Sample requests

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=ScheduleKeyDeletion
&KeyId=1234abcd-12ab-34cd-56ef-12345678****
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
      <RequestId>3da5b8cc-8107-40ac-a170-793cd181d7b7</RequestId>
</KMS>
```

`JSON` format

```
{
"RequestId": "3da5b8cc-8107-40ac-a170-793cd181d7b7"
}
```

Error codes

HttpCode	Error code	Error message	Description
400	Throttling	Request was denied due to request throttling.	The error message returned because your traffic in this period has exceeded the limit. If your business requirements are not met, submit a ticket.
404	Forbidden.KeyNotFound	The specified Key is not found.	The error message returned because the specified key does not exist.

For a list of error codes, visit the API Error Center.

8.8. CancelKeyDeletion

Cancels the deletion of a CMK.

When the deletion of a CMK is canceled, the CMK returns to the Enabled state.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	CancelKeyDeletion	The operation that you want to perform. Set the value to CancelKeyDeletion.
KeyId	String	Yes	1234abcd-12ab-34cd-56ef-12345678****	The globally unique ID of the CMK.

Response parameters

Parameter	Type	Example	Description
RequestId	String	3da5b8cc-8107-40ac-a170-793cd181d7b7	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=CancelKeyDeletion
&KeyId=1234abcd-12ab-34cd-56ef-12345678****
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
      <RequestId>3da5b8cc-8107-40ac-a170-793cd181d7b7</RequestId>
</KMS>
```

`JSON` format

```
{
"RequestId": "3da5b8cc-8107-40ac-a170-793cd181d7b7"
}
```

Error codes

For a list of error codes, visit the API Error Center.

8.9. DeleteKeyMaterial

Deletes the key material that you imported.

This operation does not delete the CMK that is created by using the key material.

If the CMK is in the PendingDeletion state, the state of the CMK and the scheduled deletion time do not change after you call this operation. If the CMK is not in the PendingDeletion state, the state of the CMK changes to PendingImport after you call this operation.

After you delete the key material, you can upload only the same key material into the CMK.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DeleteKeyMaterial	The operation that you want to perform. Set the value to DeleteKeyMaterial.
KeyId	String	Yes	1234abcd-12ab-34cd-56ef-12345678****	The globally unique ID of the CMK.

Response parameters

Parameter	Type	Example	Description
RequestId	String	4162a6af-bc99-40b3-a552-89dcc8aaf7c8	The ID of the request.

Examples

Sample requests

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=DeleteKeyMaterial
&KeyId=1234abcd-12ab-34cd-56ef-12345678****
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
    <RequestId>4162a6af-bc99-40b3-a552-89dcc8aaf7c8</RequestId>
</KMS>
```

`JSON` format

```
{
        "RequestId": "4162a6af-bc99-40b3-a552-89dcc8aaf7c8"
}
```

Error codes

For a list of error codes, visit the API Error Center.

8.10. DescribeKey

Queries the information about a customer master key (CMK).

You can query the information about the CMK `05754286-3ba2-4fa6-8d41-4323aca6****` by using parameter settings provided in this topic. The information includes the creator, creation time, status, and deletion protection status of the CMK.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeKey	The operation that you want to perform. Set the value to DescribeKey.
KeyId	String	Yes	05754286-3ba2-4fa6-8d41-4323aca6****	The ID of the CMK. You can also set this parameter to an alias that is bound to the CMK. For more information, see Overview of aliases.

Response parameters

Parameter	Type	Example	Description
KeyMetadata	Struct		The metadata of the CMK.
Arn	String	acs:kms:cn-hangzhou:154035569884****:key/05754286-3ba2-4fa6-8d41-4323aca6****	The Alibaba Cloud Resource Name (ARN) of the CMK.

Parameter	Type	Example	Description
AutomaticRotation	String	Disabled	Indicates whether automatic rotation is enabled. Valid values: • Enabled • Disabled • Suspended For more information, see Automatic key rotation. Note Only symmetric CMKs support automatic rotation.
CreationDate	String	2021-05-20T06:34:21Z	The time when the CMK was created. The time is displayed in UTC.
Creator	String	154035569884****	The user who created the CMK. The value is an Alibaba Cloud account.
DeleteDate	String	2021-05-26T18:22:03Z	The time at which the CMK is scheduled for deletion. The time is displayed in UTC. For more information, see ScheduleKeyDeletion. Note This parameter is returned only when the value of the KeyState parameter is PendingDeletion.
DeletionProtection	String	Enabled	Indicates whether deletion protection is enabled. Valid values: • Enabled • Disabled
DeletionProtectionDescription	String	The CMK is being used by XXX. Deletion protection is set.	The description of deletion protection.
Description	String	key description example	The description of the CMK.
KeyId	String	05754286-3ba2-4fa6-8d41-4323aca6****	The ID of the CMK.
KeySpec	String	Aliyun_AES_256	The type of the CMK.
KeyState	String	Enabled	The status of the CMK. For more information, see Impact of CMK status on API operations.
KeyUsage	String	ENCRYPT/DECRYPT	The purpose of the CMK.
LastRotationDate	String	2021-05-20T06:34:21Z	The time when the last rotation was performed. The time is displayed in UTC. For a new CMK, the value of this parameter is the time when the initial version of the CMK was generated.
MaterialExpireTime	String	2021-07-06T18:22:03Z	The time when the key material of the CMK expires. The time is displayed in UTC. If the value is empty, the key material of the CMK does not expire.
NextRotationDate	String	2021-07-06T18:22:03Z	The time at which the next rotation is scheduled for execution. Note This parameter is returned only when the value of the AutomaticRotation parameter is Enabled or Suspended.
Origin	String	Aliyun_KMS	The source of the key material for the CMK.
PrimaryKeyVersion	String	515e0b0a-624f-45ab-92b5-54f9b551****	The ID of the current primary key version for the symmetric CMK.
ProtectionLevel	String	HSM	The protection level of the CMK.

Parameter	Type	Example	Description
RotationInterval	String	31536000s	The interval for automatic rotation. Unit: seconds. For example, if the value is 604800s, automatic rotation is performed at a 7-day interval. **Note** This parameter is returned only when the value of the AutomaticRotation parameter is Enabled or Suspended.
RequestId	String	f1fdfa9d-bd49-418b-942f-8f3e3ec00a4f	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeKey
&KeyId=05754286-3ba2-4fa6-8d41-4323aca6****
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
      <KeyMetadata>
            <CreationDate>2021-05-20T06:34:21Z</CreationDate>
            <Description></Description>
            <KeyId>05754286-3ba2-4fa6-8d41-4323aca6****</KeyId>
            <KeySpec>Aliyun_AES_256</KeySpec>
            <KeyState>Enabled</KeyState>
            <KeyUsage>ENCRYPT/DECRYPT</KeyUsage>
            <PrimaryKeyVersion>515e0b0a-624f-45ab-92b5-54f9b551****</PrimaryKeyVersion>
            <DeleteDate></DeleteDate>
            <Creator>154035569884****</Creator>
            <Arn>acs:kms:cn-hangzhou:154035569884****:key/05754286-3ba2-4fa6-8d41-4323aca6****</Arn>
            <Origin>Aliyun_KMS</Origin>
            <MaterialExpireTime></MaterialExpireTime>
            <ProtectionLevel>HSM</ProtectionLevel>
            <LastRotationDate>2021-05-20T06:34:21Z</LastRotationDate>
            <AutomaticRotation>Disabled</AutomaticRotation>
            <DeletionProtection>Enabled</DeletionProtection>
      </KeyMetadata>
      <RequestId>f1fdfa9d-bd49-418b-942f-8f3e3ec00a4f</RequestId>
</KMS>
```

`JSON` format

```
{
    "KeyMetadata": {
        "CreationDate": "2021-05-20T06:34:21Z",
        "Description": "",
        "KeyId": "05754286-3ba2-4fa6-8d41-4323aca6****",
        "KeySpec": "Aliyun_AES_256",
        "KeyState": "Enabled",
        "KeyUsage": "ENCRYPT/DECRYPT",
        "PrimaryKeyVersion": "515e0b0a-624f-45ab-92b5-54f9b551****",
        "DeleteDate": "",
        "Creator": "154035569884****",
        "Arn": "acs:kms:cn-hangzhou:154035569884****:key/05754286-3ba2-4fa6-8d41-4323aca6****",
        "Origin": "Aliyun_KMS",
        "MaterialExpireTime": "",
        "ProtectionLevel": "HSM",
        "LastRotationDate": "2021-05-20T06:34:21Z",
        "AutomaticRotation": "Disabled",
        "DeletionProtection": "Enabled"
    },
    "RequestId": "f1fdfa9d-bd49-418b-942f-8f3e3ec00a4f"
}
```

Error codes

HTTP status code	Error code	Error message	Description
404	Forbidden.KeyNotFound	The specified Key is not found.	The error message returned because the specified CMK is not found.

For a list of error codes, visit the API Error Center.

8.11. ListKeys

Queries all CMKs of the current Alibaba Cloud account in the current region.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ListKeys	The operation that you want to perform. Set the value to ListKeys.
PageNumber	Integer	No	1	The number of the page to return. Pages start from page 1. Default value: 1.
PageSize	Integer	No	10	The number of entries to return on each page. Valid values: 1 to 100. Default value: 10.
Filters	String	No	[{"Key":"KeyState", "Values": ["Enabled","Disabled"]}]	The CMK filter. The filter consists of one or more key-values pairs. You can specify a maximum of 10 key-values pairs. • Key ◦ Description: the property that you want to filter. ◦ Type: string. ◦ Valid values: ▪ KeyState: the status of a key. ▪ KeySpec: the type of a key. ▪ KeyUsage: the usage of a key. ▪ ProtectionLevel: the protection level. ▪ CreatorType: the type of the creator. • Values ◦ Description: the value to be included after filtering. ◦ Format: string array. ◦ Length: 0 to 10. ◦ Valid values: ▪ When Key is set to KeyState, the value can be Enabled, Disabled, PendingDeletion, or PendingImport. ▪ When Key is set to KeySpec, the value can be Aliyun_AES_256, Aliyun_SM4, RSA_2048, EC_P256, EC_P256K, or EC_SM2. Note: You can create the keys of the EC_SM2 or Aliyun_SM4 type only in regions that support Managed HSMs and pass the State Cryptography Administration (SCA) certification. For more information about the regions, see Supported regions. If your region does not support EC_SM2 and Aliyun_SM4, the two values are ignored if they are specified. ▪ When Key is set to KeyUsage, the value can be ENCRYPT/DECRYPT (data encryption and decryption), or SIGN/VERIFY (digital signature generation and verification). ▪ When Key is set to ProtectionLevel, the value can be SOFTWARE (software) or HSM (hardware). Only certain regions support HSM. For more information about the regions, see Supported regions . If your region does not support HSM, the value is ignored if it is specified. ▪ If Key is set to CreatorType, the value can be User (used to obtain the CMK created by the current account) or Service (used to obtain the CMK created by other cloud products authorized by the current account). The logical relationship between different keys is AND, and the logical relationship between multiple values in the same key is OR. Example: `[ {"Key":"KeyState", "Values": ["Enabled","Disabled"]}, {"Key":"KeyState", "Values": ["PendingDeletion"]}, {"Key":"KeySpec", "Values": ["Aliyun_AES_256"]} ]` . In this example, the semantics are: `(KeyState=Enabled OR KeyState=Disabled OR KeyState=PendingDeletion) AND (KeySpec=Aliyun_AES_256)` .

Response parameters

Parameter	Type	Example	Description
Keys	Array of Key		The CMK.
Key			
KeyArn	String	acs:kms:cn-hangzhou:123456:key/80e9409f-78fa-42ab-84bd-83f40c81****	The Alibaba Cloud Resource Name (ARN) of the CMK.
KeyId	String	08c33a6f-4e0a-4a1b-a3fa-7ddfa1d4****	The ID of the CMK.
PageNumber	Integer	1	The page number of the returned page.
PageSize	Integer	10	The number of entries returned per page.
RequestId	String	1050b8f1-b264-496d-a782-6299cbaf15f8	The ID of the request.
TotalCount	Integer	3	The total number of CMKs.

Examples

Sample requests

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=ListKeys
&PageNumber=1
&PageSize=10
&Filters=[{"Key":"KeyState", "Values":["Enabled","Disabled"]}]
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
        <Keys>
                <Key>
                        <KeyId>80e9409f-78fa-42ab-84bd-83f40c81****</KeyId>
                        <KeyArn>acs:kms:cn-hangzhou:123456:key/80e9409f-78fa-42ab-84bd-83f40c81****</KeyArn>
                </Key>
                <Key>
                        <KeyId>8fbb1226-a06f-4c57-8887-daa5b627****</KeyId>
                        <KeyArn>acs:kms:cn-hangzhou:123456:key/8fbb1226-a06f-4c57-8887-daa5b627****</KeyArn>
                </Key>
                  </Keys>
        <TotalCount>3</TotalCount>
        <PageNumber>1</PageNumber>
        <PageSize>10</PageSize>
        <RequestId>bc29ec35-3373-48d1-8202-520fd78d****</RequestId>
</KMS>
```

`JSON` format

```
{
        "Keys": {
                "Key": [
                        {
                                "KeyId": "80e9409f-78fa-42ab-84bd-83f40c81****",
                    "KeyArn": "acs:kms:cn-hangzhou:123456:key/80e9409f-78fa-42ab-84bd-83f40c81****"
                        },
                        {
                                "KeyId": "8fbb1226-a06f-4c57-8887-daa5b627****",
                    "KeyArn": "acs:kms:cn-hangzhou:123456:key/8fbb1226-a06f-4c57-8887-daa5b627****"
                        }
                    ],
                "TotalCount": 3,
        "PageNumber": 1,
        "PageSize": 10,
        "RequestId": "bc29ec35-3373-48d1-8202-520fd78d****"
}
```

Error codes

For a list of error codes, visit the API Error Center.

8.12. UpdateKeyDescription

Updates the description of a specified CMK.

This operation replaces the description of the CMK (the Description value in DescribeKey) with the value that you specify. You can add, modify, or delete the description of the CMK through this operation.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	UpdateKeyDescription	The operation that you want to perform. Set the value to UpdateKeyDescription.
Description	String	Yes	key description example	The description of the CMK. This description includes the purpose of the CMK, such as the types of data that you want to protect and applications that can use the CMK.
KeyId	String	Yes	1234abcd-12ab-34cd-56ef-12345678****	The globally unique ID of the CMK.

Response parameters

Parameter	Type	Example	Description
RequestId	String	3455b9b4-95c1-419d-b310-db6a53b09a39	The ID of the request.

Examples

Sample requests

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=UpdateKeyDescription
&Description=key description example
&KeyId=1234abcd-12ab-34cd-56ef-12345678****
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
   <RequestId>3455b9b4-95c1-419d-b310-db6a53b09a39</RequestId>
</KMS>
```

`JSON` format

```
{
 "RequestId": "3455b9b4-95c1-419d-b310-db6a53b09a39"
}
```

Error codes

For a list of error codes, visit the API Error Center.

8.13. DescribeKeyVersion

Queries detailed information about a specified customer master key (CMK) version.

This topic provides an example on how to query the information about a version of the CMK `1234abcd-12ab-34cd-56ef-12345678****`. The ID of the CMK version is `2ab1a983-7072-4bbc-a582-584b5bd8****`. The response shows that the creation time of the CMK version is `2016-03-25T10:42:40Z`.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeKeyVersion	The operation that you want to perform. Set the value to DescribeKeyVersion.
KeyId	String	Yes	1234abcd-12ab-34cd-56ef-12345678****	The globally unique ID of the CMK. You can also set this parameter to an alias that is bound to the CMK. For more information, see Alias overview.

Parameter	Type	Required	Example	Description
KeyVersionId	String	Yes	2ab1a983-7072-4bbc-a582-584b5bd8****	The globally unique ID of the CMK version. You can call the ListKeyVersions operation to query the versions of the CMK.

For more information about common request parameters, see Common parameters.

Response parameters

Parameter	Type	Example	Description
KeyVersion	Struct		The metadata of the CMK version.
CreationDate	String	2016-03-25T10:42:40Z	The date and time when the CMK version was created. The time is displayed in UTC.
KeyId	String	1234abcd-12ab-34cd-56ef-12345678****	The globally unique ID of the CMK. **Note** If you set the KeyId parameter in the request to an alias of the CMK, the ID of the CMK to which the alias is bound is returned.
KeyVersionId	String	2ab1a983-7072-4bbc-a582-584b5bd8****	The globally unique ID of the CMK version.
RequestId	String	7021b6ec-4be7-4d3c-8a68-1e85d4d515a0	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeKeyVersion
&KeyId=1234abcd-12ab-34cd-56ef-12345678****
&KeyVersionId=2ab1a983-7072-4bbc-a582-584b5bd8****
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
        <RequestId>7021b6ec-4be7-4d3c-8a68-1e85d4d515a0</RequestId>
        <KeyVersion>
                <CreationDate>2016-03-25T10:42:40Z</CreationDate>
                <KeyId>1234abcd-12ab-34cd-56ef-12345678****</KeyId>
                <KeyVersionId>2ab1a983-7072-4bbc-a582-584b5bd8****</KeyVersionId>
        </KeyVersion>
</KMS>
```

`JSON` format

```
{
    "RequestId":"7021b6ec-4be7-4d3c-8a68-1e85d4d515a0",
    "KeyVersion":{
        "CreationDate":"2016-03-25T10:42:40Z",
        "KeyId":"1234abcd-12ab-34cd-56ef-12345678****",
        "KeyVersionId":"2ab1a983-7072-4bbc-a582-584b5bd8****"
        }
}
```

Error codes

For a list of error codes, visit the API Error Center.

8.14. ListKeyVersions

Queries all versions of a specified CMK.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description

Parameter	Type	Required	Example	Description
Action	String	Yes	ListKeyVersions	The operation that you want to perform. Set the value to ListKeyVersions.
KeyId	String	Yes	0b30658a-ed1a-4922-b8f7-a673ca9c****	The globally unique ID of the CMK. You can also set this parameter to an alias that is bound to the CMK. For more information, see Use aliases.
PageNumber	Integer	Yes	1	The number of the page to return. Pages start from page 1. Default value: 1.
PageSize	Integer	No	10	The number of entries to return on each page. Valid values: 0 to 101. Default value: 10.

Response parameters

Parameter	Type	Example	Description
KeyVersions	Array		An array that consists of key versions.
KeyVersion			
CreationDate	String	2016-03-25T10:42:40Z	The date and time when the CMK version was created. The time is displayed in UTC.
KeyId	String	0b30658a-ed1a-4922-b8f7-a673ca9c****	The globally unique ID of the CMK. Note If you set the KeyId parameter to the alias of the CMK, the ID of the CMK to which the alias is bound is returned.
KeyVersionId	String	1e3304fd-68ac-4d5b-8886-ae5f01a1****	The globally unique ID of the CMK version.
PageNumber	Integer	1	The page number of the returned page.
PageSize	Integer	10	The number of entries returned per page.
RequestId	String	f71204c4-53cd-4eea-b405-653ba2db7e86	The ID of the request.
TotalCount	Integer	3	The total number of returned key versions.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=ListKeyVersions
&KeyId=1234abcd-12ab-34cd-56ef-12345678****
&PageNumber=1
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
        <RequestId>f71204c4-53cd-4eea-b405-653ba2db7e86</RequestId>
        <KeyVersions>
                <KeyVersion>
                        <KeyId>0b30658a-ed1a-4922-b8f7-a673ca9c****</KeyId>
                        <KeyVersionId>1e3304fd-68ac-4d5b-8886-ae5f01a1****</KeyVersionId>
                        <CreationDate>2019-08-06T10:22:03Z</CreationDate>
                </KeyVersion>
                <KeyVersion>
                        <KeyId>0b30658a-ed1a-4922-b8f7-a673ca9c****</KeyId>
                        <KeyVersionId>2ab1a983-7072-4bbc-a582-584b5bd8****</KeyVersionId>
                        <CreationDate>2019-08-06T10:19:18Z</CreationDate>
                </KeyVersion>
                <KeyVersion>
                        <KeyId>0b30658a-ed1a-4922-b8f7-a673ca9c****</KeyId>
                        <KeyVersionId>6a69c763-388a-4708-9fc0-4322266b****</KeyVersionId>
                        <CreationDate>2019-08-06T10:17:04Z</CreationDate>
                </KeyVersion>
        </KeyVersions>
        <TotalCount>3</TotalCount>
        <PageNumber>1</PageNumber>
        <PageSize>10</PageSize>
</KMS>
```

`JSON` format

```
{
    "KMS": {
        "RequestId": "f71204c4-53cd-4eea-b405-653ba2db7e86",
        "KeyVersions": {
            "KeyVersion": [
                {
                    "KeyId": "0b30658a-ed1a-4922-b8f7-a673ca9c****",
                    "KeyVersionId": "1e3304fd-68ac-4d5b-8886-ae5f01a1****",
                    "CreationDate": "2019-08-06T10:22:03Z"
                },
                {
                    "KeyId": "0b30658a-ed1a-4922-b8f7-a673ca9c****",
                    "KeyVersionId": "2ab1a983-7072-4bbc-a582-584b5bd8****",
                    "CreationDate": "2019-08-06T10:19:18Z"
                },
                {
                    "KeyId": "0b30658a-ed1a-4922-b8f7-a673ca9c****",
                    "KeyVersionId": "6a69c763-388a-4708-9fc0-4322266b****",
                    "CreationDate": "2019-08-06T10:17:04Z"
                }
            ]
        },
        "TotalCount": 3,
        "PageNumber": 1,
        "PageSize": 10
    }
}
```

Error codes

For a list of error codes, visit the API Error Center.

8.15. UpdateRotationPolicy

Updates a key rotation policy.

When automatic key rotation is enabled, KMS automatically creates a new key version after the preset rotation period arrives and sets it as the primary key version. Automatic rotation policy cannot be defined in the following cases:

- The specified CMK is an asymmetric key.
- The specified CMK is a key managed by Alibaba Cloud Services.
- The specified CMK is a BYOK (an external key imported into KMS).
- The specified CMK is not in the **Enabled** state.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	UpdateRotationPolicy	The operation that you want to perform. Set the value to UpdateRotationPolicy.

Parameter	Type	Required	Example	Description
EnableAutomaticRotation	Boolean	Yes	true	Specifies whether to enable automatic key rotation. Valid values: true and false.
KeyId	String	Yes	1234abcd-12ab-34cd-56ef-12345678****	The globally unique ID of the CMK.
RotationInterval	String	No	30d	The period of automatic key rotation. It must be in the integer[unit] format. The unit can be d (day), h (hour), m (minute), or s (second). For example, both **7d** and **604800s** represent a seven-day period. Valid values: 7 to 730 days. **Note** When **EnableAutomaticRotation** is set to true, this parameter is required. When EnableAutomaticRotation is set to false, this parameter is ignored.

Response parameters

Parameter	Type	Example	Description
RequestId	String	efb1cbbd-a093-4278-bc03-639dd4fcc207	The ID of the request.

Examples

Sample requests

```
https://[Endpoint]/?Action=UpdateRotationPolicy
&EnableAutomaticRotation=true
&KeyId=1234abcd-12ab-34cd-56ef-12345678****
&RotationInterval=30d
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
    <RequestId>efb1cbbd-a093-4278-bc03-639dd4fcc207</RequestId>
</KMS>
```

`JSON` format

```
{
    "RequestId": "efb1cbbd-a093-4278-bc03-639dd4fcc207"
}
```

Error codes

8.16. CreateKeyVersion

Creates a version for a customer master key (CMK).

Limits:

- You can create a version only for an asymmetric CMK that is in the Enabled state. You can call the CreateKey operation to create an asymmetric CMK and the DescribeKey operation to query the status of the CMK. The status is specified by the KeyState parameter.
- The minimum interval for creating a version of the same CMK is seven days. You can call the DescribeKey operation to query the time when the last version of a CMK was created. The time is specified by the LastRotationDate parameter.
- If a CMK is in a private key store, you cannot create a version for the CMK.
- You can create a maximum of 50 versions for a CMK in the same region.

You can create a version for the CMK whose ID is `0b30658a-ed1a-4922-b8f7-a673ca9c****` by using the parameter settings provided in this topic.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	CreateKeyVersion	The operation that you want to perform. Set the value to CreateKeyVersion.

Parameter	Type	Required	Example	Description
KeyId	String	Yes	0b30658a-ed1a-4922-b8f7-a673ca9c****	The ID of the CMK. The ID must be globally unique. **Note** You can also set the value to an alias that is bound to the CMK. For more information, see Overview of aliases.

Response parameters

Parameter	Type	Example	Description
KeyVersion	Struct		The metadata of the version.
CreationDate	String	2019-08-02T10:38:27Z	The date and time when the version was created. The time is displayed in UTC.
KeyId	String	0b30658a-ed1a-4922-b8f7-a673ca9c****	The ID of the CMK. The ID must be globally unique.
KeyVersionId	String	c0a3d5dc-0b47-4199-a050-b289349a****	The ID of the version.
RequestId	String	b96f250a-4b75-498c-91be-22c6928f85be	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=CreateKeyVersion
&KeyId=0b30658a-ed1a-4922-b8f7-a673ca9c****
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
    <KeyVersion>
        <KeyId>0b30658a-ed1a-4922-b8f7-a673ca9c****</KeyId>
        <KeyVersionId>c0a3d5dc-0b47-4199-a050-b289349a****</KeyVersionId>
        <CreationDate>2019-08-02T10:38:27Z</CreationDate>
    </KeyVersion>
    <RequestId>b96f250a-4b75-498c-91be-22c6928f85be</RequestId>
</KMS>
```

`JSON` format

```
{
        "KeyVersion": {
                "KeyId": "0b30658a-ed1a-4922-b8f7-a673ca9c****",
                "KeyVersionId": "c0a3d5dc-0b47-4199-a050-b289349a****",
                "CreationDate": "2019-08-02T10:38:27Z"
        },
        "RequestId": "b96f250a-4b75-498c-91be-22c6928f85be"
}
```

Error codes

For a list of error codes, visit the API Error Center.

8.17. Encrypt

Encrypts plaintext by using a symmetric CMK.

- KMS uses the primary version of a specified CMK to encrypt data.
- Only data of 6 KB or less can be encrypted. For example, you can call this operation to encrypt RSA keys, database access passwords, or other sensitive information.
- When you migrate encrypted data across regions, you can call this operation in the destination region to encrypt the plaintext of the data key that is used to encrypt the migrated data in the source region. This way, the ciphertext of the data key is generated in the destination region. You can also call the Decrypt operation to decrypt the data key.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	Encrypt	The operation that you want to perform. Set the value to Encrypt.
KeyId	String	Yes	1234abcd-12ab-34cd-56ef-12345678****	The globally unique ID of the CMK. You can also set this parameter to an alias that is bound to the CMK. For more information, see Use aliases.
Plaintext	String	Yes	SGVsbG8gd29y****	The plaintext to be encrypted. The plaintext must be Base64 encoded.
EncryptionContext	Json	No	{"Example":"Example"}	A JSON string that consists of key-value pairs. If you specify this parameter, an equivalent value is required when you call the Decrypt operation. For more information, see EncryptionContext.

Response parameters

Parameter	Type	Example	Description
CiphertextBlob	String	DZhOWVmZDktM2QxNi00ODk0LWJkNGYtMWZjNDNmM2YyYWJmaaSl+TztSIMe43nbTH/Z1Wr4XfLftKhAciUmDQXuMRl4WTvKhxjMThjK****	The ciphertext of the data that is encrypted by using the primary CMK version.
KeyId	String	1234abcd-12ab-34cd-56ef-12345678****	The globally unique ID of the CMK. If you set the KeyId parameter to an alias, the ID of the CMK to which the alias is bound is returned.
KeyVersionId	String	86a9efd9-3d16-4894-bd4f-1fc43f3f****	The ID of the key version that is used to encrypt the plaintext. It is the primary version of the CMK.
RequestId	String	475f1620-b9d3-4d35-b5c6-3fbdd941423d	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=Encrypt
&KeyId=1234abcd-12ab-34cd-56ef-12345678****
&Plaintext=SGVsbG8gd29y****
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
        <RequestId>475f1620-b9d3-4d35-b5c6-3fbdd941423d</RequestId>
        <CiphertextBlob>DZhOWVmZDktM2QxNi00ODk0LWJkNGYtMWZjNDNmM2YyYWJmaaSl+TztSIMe43nbTH/Z1Wr4XfLftKhAciUmDQXuMRl4WTvKhxjMThjK****</CiphertextBlob>
        <KeyId>1234abcd-12ab-34cd-56ef-12345678****</KeyId>
        <KeyVersionId>86a9efd9-3d16-4894-bd4f-1fc43f3f****</KeyVersionId>
</KMS>
```

`JSON` format

```
{
    "RequestId":"475f1620-b9d3-4d35-b5c6-3fbdd941423d",
    "CiphertextBlob":"DZhOWVmZDktM2QxNi00ODk0LWJkNGYtMWZjNDNmM2YyYWJmaaSl+TztSIMe43nbTH/Z1Wr4XfLftKhAciUmDQXuMRl4WTvKhxjMThjK****",
    "KeyId":"1234abcd-12ab-34cd-56ef-12345678****",
    "KeyVersionId":"86a9efd9-3d16-4894-bd4f-1fc43f3f****"
}
```

Error codes

For a list of error codes, visit the API Error Center.

8.18. GenerateDataKey

Generates a random data key that is used to locally encrypt data.

This operation creates a random data key, encrypts the data key by using the specified customer master key (CMK), and returns the plaintext and ciphertext of the data key. You can use the plaintext of the data key to locally encrypt your data without using KMS and store the encrypted data together with the ciphertext of the data key. You can obtain the plaintext of the data key from the Plaintext parameter in the response and the ciphertext of the data key from the CiphertextBlob parameter in the response.

The CMK that you specify in the request of this operation is only used to encrypt the data key and is not involved in the generation of the data key. KMS does not record or store the generated data key. Therefore, you need to store the ciphertext of the data key in persistent storage.

We recommend that you locally encrypt data by performing the following steps:

1. Call the GenerateDataKey operation.
2. Use the plaintext of the data key that you obtain to locally encrypt data in your own system. Then, delete the plaintext of the data key from the memory.
3. Store the encrypted data together with the ciphertext of the data key that you obtain.

We recommend that you locally decrypt data by performing the following steps:

- Call the Decrypt operation to decrypt the locally stored ciphertext of the data key. The plaintext of data key is then returned.
- Use the plaintext of the data key to encrypt local data in an offline manner and then clear the plaintext of the data key.

In this example, a random data key is generated for the CMK whose ID is `1234abcd-12ab-34cd-56ef-12345678****`.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	GenerateDataKey	The operation that you want to perform. Set the value to GenerateDataKey.
KeyId	String	Yes	1234abcd-12ab-34cd-56ef-12345678****	The ID of the CMK. The ID must be globally unique. You can also set this parameter to an alias that is bound to the CMK. For more information, see Alias overview.
KeySpec	String	No	AES_256	The type of the data key that you want to generate. Valid values: • AES_256: a 256-bit symmetric key • AES_128: a 128-bit symmetric key Note We recommend that you use the KeySpec or NumberOfBytes parameter to specify the length of a data key. If none of the parameters are specified, KMS generates a 256-bit data key. If both parameters are specified, KMS ignores the KeySpec parameter.
NumberOfBytes	Integer	No	256	The length of the data key that you want to generate. Valid values: 1 to 1024. Unit: bytes.
EncryptionContext	Json	No	{"Example":"Example"}	The JSON string that consists of key-value pairs. If you specify this parameter, an equivalent value is required when you call the Decrypt operation. For more information, see EncryptionContext.

For more information about common request parameters, see Common parameters.

Response parameters

Parameter	Type	Example	Description
CiphertextBlob	String	ODZhOWVmZDktM2QxNi00ODk0LWJkNGYtMWZjNDNmM2YyYWJmS7FmDBBQ0BkKsQrtRnidtPwirmDcS0ZuJCU41xxAAWk4Z8qsADfbV0b+i6kQmlvj79dJdGOvtX69Uycs901qOjop4bTS****	The ciphertext of the data key that is encrypted by using the primary version of the specified CMK.
KeyId	String	599fa825-17de-417e-9554-bb032cc6****	The ID of the CMK. The ID must be globally unique. Note If you set the KeyId parameter in the request to an alias of the CMK, the ID of the CMK to which the alias is bound is returned.
KeyVersionId	String	2ab1a983-7072-4bbc-a582-584b5bd8****	The ID of the CMK version. The ID must be globally unique.
Plaintext	String	QmFzZTY0IGVuY29kZWQgcGxhaW50ZXh0	The Base64 encoded plaintext of the data key.
RequestId	String	7021b6ec-4be7-4d3c-8a68-1e85d4d515a0	The ID of the request.

Examples

Sample requests

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=GenerateDataKey
&KeyId=1234abcd-12ab-34cd-56ef-12345678****
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
        <CiphertextBlob>ODZhOWVmZDktM2QxNi00ODk0LWJkNGYtMWZjNDNmM2YyYWJmS7FmDBBQ0BkKsQrtRnidtPwirmDcS0ZuJCU41xxAAWk4Z8qsADfbV0b+i6kQmlvj79dJdGOvtX69Uycs901qOjop4bTS****</CiphertextBlob>
        <KeyId>599fa825-17de-417e-9554-bb032cc6****</KeyId>
        <KeyVersionId>2ab1a983-7072-4bbc-a582-584b5bd8****</KeyVersionId>
        <Plaintext>QmFzZTY0IGVuY29kZWQgcGxhaW50ZXh0</Plaintext>
        <RequestId>7021b6ec-4be7-4d3c-8a68-1e85d4d515a0</RequestId>
</KMS>
```

`JSON` format

```
{
       "CiphertextBlob": "ODZhOWVmZDktM2QxNi00ODk0LWJkNGYtMWZjNDNmM2YyYWJmS7FmDBBQ0BkKsQrtRnidtPwirmDcS0ZuJCU41xxAAWk4Z8qsADfbV0b+i6kQmlvj79dJdGOvtX69Uycs901qOjop4bTS****",
       "KeyId": "599fa825-17de-417e-9554-bb032cc6****",
       "KeyVersionId": "2ab1a983-7072-4bbc-a582-584b5bd8****",
       "Plaintext": "QmFzZTY0IGVuY29kZWQgcGxhaW50ZXh0",
       "RequestId": "7021b6ec-4be7-4d3c-8a68-1e85d4d515a0"
}
```

Error codes

For a list of error codes, visit the API Error Center.

8.19. GenerateDataKeyWithoutPlaintext

Generates a random data key, which can be used to encrypt local data.

This operation creates a random data key, encrypts the data key by using a specific symmetric CMK, and returns the ciphertext of the data key. This operation serves the same purpose as the GenerateDataKey operation. The only difference is that this operation does not return the plaintext of the data key.

The CMK that you specify in the request of this operation is only used to encrypt the data key and is not involved in the generation of the data key. KMS does not record or store the generated data key.

Note

- This operation applies to the scenario when you do not need to use the data key to immediately encrypt data. Before you can use the data key to encrypt data, you must call the Decrypt operation to decrypt the ciphertext of the data key.
- This operation is also suitable for a distributed system with different trust levels. For example, a system stores data in different partitions based on a preset trust policy. A module creates different partitions and generates different data keys for each partition in advance. This module is not involved in data production and consumption after it completes initialization of the control plane. This module is the key provider. When producing and consuming data, modules on the control plane obtain the ciphertext of the data key for a partition first. After decrypting the ciphertext of the data key, modules on the control plane use the plaintext of the data key to encrypt or decrypt data and then clear the plaintext of the data key from the memory. In such a system, the key provider does not need to obtain the plaintext of the data key. It only needs to have the permissions to call the GenerateDataKeyWithoutPlaintext operation. The data producers or consumers do not need to generate new data keys. They only need to have the permissions to call the Decrypt operation.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	GenerateDataKeyWithoutPlaintext	The operation that you want to perform. Set the value to GenerateDataKeyWithoutPlaintext.
KeyId	String	Yes	1234abcd-12ab-34cd-56ef-12345678****	The globally unique ID of the CMK. You can also set this parameter to an alias that is bound to the CMK. For more information, see Use aliases.

Parameter	Type	Required	Example	Description
KeySpec	String	No	AES_256	The length of the data key that you want to generate. Valid values: • AES_256: 256-bit symmetric key • AES_128: 128-bit symmetric key **Note** We recommend that you use the KeySpec or NumberOfBytes parameter to specify the length of a data key. If both of them are not specified, KMS generates a 256-bit data key. If both of them are specified, KMS ignores the KeySpec parameter.
NumberOfBytes	Integer	No	256	The length of the data key that you want to generate. Valid values: 1 to 1024. Unit: bytes.
EncryptionContext	Json	No	{"Example":"Example"}	A JSON string that consists of key-value pairs. If you specify this parameter, an equivalent value is required when you call the Decrypt operation. For more information, see EncryptionContext.

Response parameters

Parameter	Type	Example	Description
CiphertextBlob	String	ODZhOWVmZDktM2QxNi00ODk0LWJkNGYtMWZjNDNmM2YyYWJmS7FmDBBQ0BkKsQrtRnidtPwirmDcS0ZuJCU41xxAAWk4Z8qsADfbV0b+i6kQmlvj79dJdGOvtX69Uycs901qOjop4bTS****	The ciphertext of the data that is encrypted by using the primary CMK version.
KeyId	String	599fa825-17de-417e-9554-bb032cc6****	The globally unique ID of the CMK. **Note** If you set the KeyId parameter to an alias, the ID of the CMK to which the alias is bound is returned.
KeyVersionId	String	2ab1a983-7072-4bbc-a582-584b5bd8****	The ID of the key version that is used to encrypt the plaintext. It is the primary version of the CMK.
RequestId	String	7021b6ec-4be7-4d3c-8a68-1e85d4d515a0	The ID of the request.

Examples

Sample requests

```
https://[Endpoint]/?Action=GenerateDataKeyWithoutPlaintext
&KeyId=1234abcd-12ab-34cd-56ef-12345678****
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
        <RequestId>7021b6ec-4be7-4d3c-8a68-1e85d4d515a0</RequestId>
        <CiphertextBlob>ODZhOWVmZDktM2QxNi00ODk0LWJkNGYtMWZjNDNmM2YyYWJmS7FmDBBQ0BkKsQrtRnidtPwirmDcS0ZuJCU41xxAAWk4Z8qsADfbV0b+i6kQmlvj79dJdGOvtX69
Uycs901qOjop4bTS****</CiphertextBlob>
        <KeyId>599fa825-17de-417e-9554-bb032cc6****</KeyId>
        <KeyVersionId>2ab1a983-7072-4bbc-a582-584b5bd8****</KeyVersionId>
</KMS>
```

`JSON` format

```
{
    "RequestId":"7021b6ec-4be7-4d3c-8a68-1e85d4d515a0",
    "CiphertextBlob":"ODZhOWVmZDktM2QxNi00ODk0LWJkNGYtMWZjNDNmM2YyYWJmS7FmDBBQ0BkKsQrtRnidtPwirmDcS0ZuJCU41xxAAWk4Z8qsADfbV0b+i6kQmlvj79dJdGOvtX69Uyc
s901qOjop4bTS****",
    "KeyId":"599fa825-17de-417e-9554-bb032cc6****",
    "KeyVersionId":"2ab1a983-7072-4bbc-a582-584b5bd8****"
}
```

Error codes

For a list of error codes, visit the API Error Center.

8.20. ExportDataKey

Encrypts a data key by using a specific public key and exports the data key.

You can call the GenerateDataKeyWithoutPlaintext operation to generate a data key, which is encrypted by a CMK. If you want to distribute the data key to other regions or cryptographic modules, you can call the ExportDataKey operation to use a public key to encrypt the data key.

Then, you can import the ciphertext of the data key to the cryptographic module where the private key is stored. This way, the data key is securely distributed from KMS to the cryptographic module. After the data key is imported to the cryptographic module, you can use it to encrypt or decrypt data.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ExportDataKey	The operation that you want to perform. Set the value to ExportDataKey.
CiphertextBlob	String	Yes	ODZhOWVmZDktM2QxNi00ODk0LWJkNGYtMWZjNDNmM2YyYWJmS7FmDBBQ0BkKsQrtRnidtPwirmDcS0ZuJCU41xxAAWk4Z8qsADfbV0b+i6kQmlvj79dJdGOvtX69Uycs901q********	The ciphertext of the data key encrypted by using a CMK.
PublicKeyBlob	String	Yes	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAndKfC2ReLL2+y8a0+ZBBeAft/uBYo86GZiYJuflqgUzKxpyuvlo3uQkBv6b+nx+0tz8g8v7GhpPWMSW5L9mNHYsvYFsa7jTxsYdt17yj6GlUHPuMIs8hr5qbwl38lHU1ila7nYWwE2fb3ePOvLDACRJVgGpU0yxioW80d2QD+9aU4jF5dlAahcfgsNzo2CXzCUc1+xbmNuq7Rp+H9VJB9dyYOwqnW3RhOLBo21FzpORapf0UiRlrHRpk1V6ez+aE1dofaYh/9bh0m6iox j7j5hpZbWccuEZTMBKd+cbuBkRhJzc6Tti6qwZbDiu4fUwbZS0Tqpuo1UadiyxMW**********	A Base64-encoded public key.
WrappingAlgorithm	String	Yes	RSAES_OAEP_SHA_256	The encryption algorithm based on which you want to use the public key specified by PublicKeyBlob to encrypt the data key. For more information about encryption algorithms, see AsymmetricDecrypt. Valid values: • RSAES_OAEP_SHA_256 • RSAES_OAEP_SHA_1 • SM2PKE
WrappingKeySpec	String	Yes	RSA_2048	The key type of the public key specified by PublicKeyBlob. For more information about key types, see Introduction to asymmetric keys. Valid values: • RSA_2048 • EC_SM2
EncryptionContext	Json	No	{"Example":"Example"}	A JSON string that consists of key-value pairs. If you specify this parameter when you use a CMK to encrypt the data key, an equivalent value is required here. For more information, see EncryptionContext.

Response parameters

Parameter	Type	Example	Description

Parameter	Type	Example	Description
ExportedDataKey	String	BQKP+1zK6+ZEMxTP5qaVzcsgXtWplYBKm0NXdSnB5FzliFxE1bSiu4dnEIlca2JpeH7yz1/S6fed630H+hIH6DoM25fTLNcKj+mFB0Xnh9m2+HN59Mn4qyTfcUeadnfCXSWcGBouhXFwcdd2rJ3n337bzTf4jm659gZu3L0i6PLuxM9p7mqdwO0cKJPfGVfhnfMz+f4alMg79WB/NNyE2lyX7/qxvV49ObNrrJbKSFiz8Djocaf0IESNLMbfYI5bXjWkJlX92DQbKhibtQW8ZOJ//ZC6t0AWcUoKL6QDm/dg5koQalcleRinpB+QadFm894sLbVZ9+N4GVs*******	The data key encrypted by using the public key and then exported.
KeyId	String	202b9877-5a25-46e3-a763-e20791b5****	The ID of the CMK that is used to decrypt the specified ciphertext of the data key. This parameter is the globally unique ID of the CMK.
KeyVersionId	String	2ab1a983-7072-4bbc-a582-584b5bd8****	The ID of the CMK version that is used to decrypt the specified ciphertext of the data key.
RequestId	String	4bd560a1-729e-45f1-a3d9-b2a33d61046b	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=ExportDataKey
&CiphertextBlob=ODZhOWVmZDktM2QxNi00ODk0LWJkNGYtMWZjNDNmM2YyYWJmS7FmDBBQ0BkKsQrtRnidtPwirmDcS0ZuJCU41xxAAWk4Z8qsADfbV0b+i6kQmlvj79dJdGOvtX69Uycs901q*
*******
&PublicKeyBlob=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAndKfC2ReLL2+y8a0+ZBBeAft/uBYo86GZiYJuflqgUzKxpyuvlo3uQkBv6b+nx+0tz8g8v7GhpPWMSW5L9mNHYsvYF
sa7jTxsYdt17yj6GlUHPuMIs8hr5qbwl38IHU1iIa7nYWwE2fb3ePOvLDACRJVgGpU0yxioW80d2QD+9aU4jF5dlAahcfgsNzo2CXzCUc1+xbmNuq7Rp+H9VJB9dyYOwqnW3RhOLBo21FzpORapf0
UiRlrHRpk1V6ez+aE1dofaYh/9bh0m6ioxj7j5hpZbWccuEZTMBKd+cbuBkRhJzc6Tti6qwZbDiu4fUwbZS0TqpuolUadiyxMW********
&WrappingAlgorithm=RSAES_OAEP_SHA_256
&WrappingKeySpec=RSA_2048
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
        <KeyId>202b9877-5a25-46e3-a763-e20791b5****</KeyId>
        <KeyVersionId>2ab1a983-7072-4bbc-a582-584b5bd8****</KeyVersionId>
        <ExportedDataKey>BQKP+1zK6+ZEMxTP5qaVzcsgXtWplYBKm0NXdSnB5FzliFxE1bSiu4dnEIlca2JpeH7yz1/S6fed630H+hIH6DoM25fTLNcKj+mFB0Xnh9m2+HN59Mn4qyTfcU
eadnfCXSWcGBouhXFwcdd2rJ3n337bzTf4jm659gZu3L0i6PLuxM9p7mqdwO0cKJPfGVfhnfMz+f4alMg79WB/NNyE2lyX7/qxvV49ObNrrJbKSFiz8Djocaf0IESNLMbfYI5bXjWkJlX92DQbKhi
btQW8ZOJ//ZC6t0AWcUoKL6QDm/dg5koQalcleRinpB+QadFm894sLbVZ9+N4GVs*******</ExportedDataKey>
        <RequestId>4bd560a1-729e-45f1-a3d9-b2a33d61046b</RequestId>
</KMS>
```

`JSON` format

```
{
    "KeyId": "202b9877-5a25-46e3-a763-e20791b5****",
    "KeyVersionId": "2ab1a983-7072-4bbc-a582-584b5bd8****",
    "ExportedDataKey": "BQKP+1zK6+ZEMxTP5qaVzcsgXtWplYBKm0NXdSnB5FzliFxE1bSiu4dnEIlca2JpeH7yz1/S6fed630H+hIH6DoM25fTLNcKj+mFB0Xnh9m2+HN59Mn4qyTfcUead
nfCXSWcGBouhXFwcdd2rJ3n337bzTf4jm659gZu3L0i6PLuxM9p7mqdwO0cKJPfGVfhnfMz+f4alMg79WB/NNyE2lyX7/qxvV49ObNrrJbKSFiz8Djocaf0IESNLMbfYI5bXjWkJlX92DQbKhibtQ
W8ZOJ//ZC6t0AWcUoKL6QDm/dg5koQalcleRinpB+QadFm894sLbVZ9+N4GVs*******",
    "RequestId": "4bd560a1-729e-45f1-a3d9-b2a33d61046b"
}
```

Error codes

HTTP status code	Error code	Error message	Description
500	InternalFailure	Internal Failure.	The error message returned because an internal error has occurred. Try again later. If the error persists, submit a ticket.

For a list of error codes, visit the API Error Center.

8.21. GenerateAndExportDataKey

Randomly generates a data key and uses a CMK and a public key to encrypt the data key. This operation returns both the ciphertext of the data key encrypted by using the CMK and that encrypted by using the public key.

We recommend that you perform the following steps to import your data key to a cryptographic module:

- Call the GenerateAndExportDataKey operation to generate a data key and obtain both the ciphertext of the data key encrypted by using the CMK and that encrypted by using the public key.

- Store the ciphertext of the data key encrypted by using the CMK in KMS Secrets Manager or in a storage service such as ApsaraDB. This ciphertext is used for backup and restoration.
- Import the ciphertext of the data key encrypted by using the public key to the cryptographic module where the private key is stored. Then, you can use the data key to encrypt or decrypt data.

> **Note** The CMK that you specify in the request of this operation is only used to encrypt the data key and is not involved in the generation of the data key. KMS does not record or store the data keys randomly generated by calling this operation. You must take note of the data keys and the returned ciphertext.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	GenerateAndExportDataKey	The operation that you want to perform. Set the value to GenerateAndExportDataKey.
KeyId	String	Yes	1234abcd-12ab-34cd-56ef-12345678****	The globally unique ID of the CMK. You can also set this parameter to an alias that is bound to the CMK. For more information, see Use aliases.
PublicKeyBlob	String	Yes	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAndKfC2ReLL2+y8a0+ZBBeAft/uBYo86GZiYJuflqgUzKxpyuvlo3uQkBv6b+nx+0tz8g8v7GhpPWMSW5L9mNHYsvYFsa7jTxsYdt17yj6GlUHPuMIs8hr5qbwl38lHU1ila7nYWwE2fb3ePOvLDACRJVgGpU0yxioW80d2QD+9aU4jF5dlAahcfgsNzo2CXzCUc1+xbmNuq7Rp+H9VJB9dyYOwqnW3RhOLBo21FzpORapf0UiRlrHRpk1V6ez+aE1dofaYh/9bh0m6iox j7j5hpZbWccuEZTMBKd+cbuBkRhJzc6Tti6qwZbDiu4fUwbZS0Tqpuo1UadiyxMW**********	A Base64-encoded public key.
WrappingAlgorithm	String	Yes	RSAES_OAEP_SHA_256	The encryption algorithm based on which you want to use the public key specified by PublicKeyBlob to encrypt the data key. For more information about encryption algorithms, see AsymmetricDecrypt. Valid values: • RSAES_OAEP_SHA_256 • RSAES_OAEP_SHA_1 • SM2PKE
WrappingKeySpec	String	Yes	RSA_2048	The key type of the public key specified by PublicKeyBlob. For more information about key types, see Introduction to asymmetric keys. Valid values: • RSA_2048 • EC_SM2
KeySpec	String	No	AES_256	The length of the data key that you want to generate. Valid values: • AES_256: a 256-bit symmetric key • AES_128: a 128-bit symmetric key **Note** We recommend that you use the KeySpec or NumberOfBytes parameter to specify the length of a data key. If both parameters are not specified, KMS generates a 256-bit data key. If both parameters are specified, KMS ignores the KeySpec parameter.
NumberOfBytes	Integer	No	32	The length of the data key that you want to generate. Valid values: 1 to 1024. Unit: bytes.

Parameter	Type	Required	Example	Description
EncryptionContext	Json	No	{"Example":"Example"}	A JSON string of key-value pairs. If you specify this parameter here, an equivalent value is required when you decrypt or re-encrypt the data key. For more information, see EncryptionContext.

Response parameters

Parameter	Type	Example	Description
CiphertextBlob	String	ODZhOWVmZDktM2QxNi00ODk0LWJkNGYtMWZjNDNmM2YyYWJmS7FmDBBQ0BkKsQrtRnidtPwirmDcS0ZuJCU41xxAAWk4Z8qsADfbV0b+i6kQmlvj79dJdGOvtX69Uycs901qOjop4bTS****	The ciphertext of the data key encrypted by using the primary CMK version.
ExportedDataKey	String	BQKP+1zK6+ZEMxTP5qaVzcsgXtWplYBKm0NXdSnB5FzliFxE1bSiu4dnEIlca2JpeH7yz1/S6fed630H+hIH6DoM25fTLNcKj+mFB0Xnh9m2+HN59Mn4qyTfcUeadnfCXSWcGBouhXFwcdd2rJ3n337bzTf4jm659gZu3L0i6PLuxM9p7mqdwO0cKJPfGVfhnfMz+f4alMg79WB/NNyE2lyX7/qxvV49ObNrrJbKSFiz8Djocaf0IESNLMbfYI5bXjWkJlX92DQbKhibtQW8ZOJ//ZC6t0AWcUoKL6QDm/dg5koQalcleRinpB+QadFm894sLbVZ9+N4GVs*******	The data key encrypted by using the public key and then exported.
KeyId	String	599fa825-17de-417e-9554-bb032cc6****	The globally unique ID of the CMK. Note If you set the KeyId parameter to an alias, the ID of the CMK to which the alias is bound is returned.
KeyVersionId	String	2ab1a983-7072-4bbc-a582-584b5bd8****	The ID of the CMK version that is used to encrypt the plaintext. It is the primary version of the CMK.
RequestId	String	7021b6ec-4be7-4d3c-8a68-1e85d4d515a0	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=GenerateAndExportDataKey
&KeyId=1234abcd-12ab-34cd-56ef-12345678****
&PublicKeyBlob=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAndKfC2ReLL2+y8a0+ZBBeAft/uBYo86GZiYJuflqgUzKxpyuvlo3uQkBv6b+nx+0tz8g8v7GhpPWMSW5L9mNHYsvYFsa7jTxsYdt17yj6GlUHPuMIs8hr5qbwl38IHU1iIa7nYWwE2fb3ePOvLDACRJVgGpU0yxioW80d2QD+9aU4jF5dlAahcfgsNzo2CXzCUc1+xbmNuq7Rp+H9VJB9dyYOwqnW3RhOLBo21FzpORapf0UiRlrHRpk1V6ez+aE1dofaYh/9bh0m6ioxj7j5hpZbWccuEZTMBKd+cbuBkRhJzc6Tti6qwZbDiu4fUwbZS0Tqpuo1UadiyxMW********
&WrappingAlgorithm=RSAES_OAEP_SHA_256
&WrappingKeySpec=RSA_2048
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
        <KeyId>202b9877-5a25-46e3-a763-e20791b5****</KeyId>
        <KeyVersionId>2ab1a983-7072-4bbc-a582-584b5bd8****</KeyVersionId>
        <CiphertextBlob>ODZhOWVmZDktM2QxNi00ODk0LWJkNGYtMWZjNDNmM2YyYWJmS7FmDBBQ0BkKsQrtRnidtPwirmDcS0ZuJCU41xxAAWk4Z8qsADfbV0b+i6kQmlvj79dJdGOvtX69Uycs901qOjop4bTS****</CiphertextBlob>
        <ExportedDataKey>BQKP+1zK6+ZEMxTP5qaVzcsgXtWplYBKm0NXdSnB5FzliFxE1bSiu4dnEIlca2JpeH7yz1/S6fed630H+hIH6DoM25fTLNcKj+mFB0Xnh9m2+HN59Mn4qyTfcUeadnfCXSWcGBouhXFwcdd2rJ3n337bzTf4jm659gZu3L0i6PLuxM9p7mqdwO0cKJPfGVfhnfMz+f4alMg79WB/NNyE2lyX7/qxvV49ObNrrJbKSFiz8Djocaf0IESNLMbfYI5bXjWkJlX92DQbKhibtQW8ZOJ//ZC6t0AWcUoKL6QDm/dg5koQalcleRinpB+QadFm894sLbVZ9+N4GVs*******</ExportedDataKey>
        <RequestId>4bd560a1-729e-45f1-a3d9-b2a33d61046b</RequestId>
</KMS>
```

`JSON` format

```
{
    "KeyId": "202b9877-5a25-46e3-a763-e20791b5****",
    "KeyVersionId": "2ab1a983-7072-4bbc-a582-584b5bd8****",
    "CiphertextBlob":"ODZhOWVmZDktM2QxNi00ODk0LWJkNGYtMWZjNDNmM2YyYWJmS7FmDBBQ0BkKsQrtRnidtPwirmDcS0ZuJCU41xxAAWk4Z8qsADfbV0b+i6kQmlvj79dJdGOvtX69Uycs901qOjop4bTS****",
    "ExportedDataKey": "BQKP+1zK6+ZEMxTP5qaVzcsgXtWplYBKm0NXdSnB5FzliFxE1bSiu4dnEIlca2JpeH7yz1/S6fed630H+hIH6DoM25fTLNcKj+mFB0Xnh9m2+HN59Mn4qyTfcUeadnfCXSWcGBouhXFwcdd2rJ3n337bzTf4jm659gZu3L0i6PLuxM9p7mqdwO0cKJPfGVfhnfMz+f4alMg79WB/NNyE2lyX7/qxvV49ObNrrJbKSFiz8Djocaf0IESNLMbfYI5bXjWkJlX92DQbKhibtQW8ZOJ//ZC6t0AWcUoKL6QDm/dg5koQalcleRinpB+QadFm894sLbVZ9+N4GVs*******",
    "RequestId": "207596a2-36d3-4840-b1bd-f87044699bd7"
}
```

Error codes

HTTP status code	Error code	Error message	Description
404	Forbidden.KeyNotFound	The specified Key is not found.	The error message returned because the specified key does not exist.

For a list of error codes, visit the API Error Center.

8.22. Decrypt

Decrypts the ciphertext that is specified by the CiphertextBlob parameter.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	Decrypt	The operation that you want to perform. Set the value to Decrypt.
CiphertextBlob	String	Yes	DZhOWVmZDktM2QxNi00ODk0LWJkNGYtMWZjNDNmM2YyYWJmaaSl+TztSIMe43nbTH/Z1Wr4XfLftKhAciUmDQXuMRl4WTvKhxjMThjK****	The ciphertext that you want to decrypt. You can generate the ciphertext by calling the following operations: • GenerateDataKey • Encrypt • GenerateDataKeyWithoutPlaintext
EncryptionContext	Json	No	{"Example":"Example"}	The JSON string that consists of key-value pairs. **Note** If you specify the EncryptionContext parameter when you call the GenerateDataKey, Encrypt, or GenerateDataKeyWithoutPlaintext operation, you must specify the same context when you call the Decrypt operation. For more information, see EncryptionContext.

Response parameters

Parameter	Type	Example	Description
KeyId	String	202b9877-5a25-46e3-a763-e20791b5****	The ID of the customer master key (CMK) that is used to decrypt the ciphertext. It is the GUID of the CMK.
KeyVersionId	String	2ab1a983-7072-4bbc-a582-584b5bd8****	The ID of the CMK version that is used to decrypt the ciphertext.
Plaintext	String	tRYXuCwgja12xxO1N/gZERDDCLw9doZEQiPDk/Bv****	The plaintext that is generated after decryption.
RequestId	String	207596a2-36d3-4840-b1bd-f87044699bd7	The ID of the request.

Examples

Sample requests

```
https://[Endpoint]/?Action=Decrypt
&CiphertextBlob=DZhOWVmZDktM2QxNi00ODk0LWJkNGYtMWZjNDNmM2YyYWJmaaSl+TztSIMe43nbTH/Z1Wr4XfLftKhAciUmDQXuMRl4WTvKhxjMThjK****
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
        <KeyId>202b9877-5a25-46e3-a763-e20791b5****</KeyId>
        <KeyVersionId>2ab1a983-7072-4bbc-a582-584b5bd8****</KeyVersionId>
        <Plaintext>tRYXuCwgja12xxO1N/gZERDDCLw9doZEQiPDk/Bv****</Plaintext>
        <RequestId>4bd560a1-729e-45f1-a3d9-b2a33d61046b</RequestId>
</KMS>
```

`JSON` format

```
{
    "KeyId": "202b9877-5a25-46e3-a763-e20791b5****",
    "KeyVersionId": "2ab1a983-7072-4bbc-a582-584b5bd8****",
    "Plaintext": "tRYXuCwgja12xxOlN/gZERDDCLw9doZEQiPDk/Bv****",
    "RequestId": "207596a2-36d3-4840-b1bd-f87044699bd7"
}
```


Error codes

For a list of error codes, visit the API Error Center.

8.23. ReEncrypt

Re-encrypts ciphertext. When you call this operation, KMS first decrypts the specified ciphertext and then uses a different CMK to encrypt the obtained plaintext data or data key and return ciphertext.

You can call this operation in the following scenarios:

- After the CMK that was used to encrypt your data is rotated, you can call this operation to use the latest CMK version to re-encrypt the data. For more information about automatic key rotation, see Configure automatic key rotation.
- The CMK that was used to encrypt your data remains unchanged, but EncryptionContext is changed. In this scenario, you can call this operation to re-encrypt the data.
- You can call this operation to use a CMK in KMS to re-encrypt data or a data key that was previously encrypted by a different CMK.

To use the ReEncrypt operation, you must have two permissions:

- kms:ReEncryptFrom on the source CMK
- kms:ReEncryptTo on the destination CMK
- For simplicity, you can specify kms:ReEncrypt* to allow both of the preceding permissions.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ReEncrypt	The operation that you want to perform. Set the value to ReEncrypt.
CiphertextBlob	String	Yes	ODZhOWVmZDktM2QxNi00ODk0LWJkNGYtMWZjNDNmM2YyYWJmS7FmDBBQ0BkKsQrtRnidtPwirmDcS0ZuJCU41xxAAWk4Z8qsADfbV0b+i6kQmlvj79dJdGOvtX69Uycs901q********	The ciphertext that you want to re-encrypt. You can set this parameter to the ciphertext that is returned after a symmetric or asymmetric encryption operation. • Symmetric encryption: the ciphertext returned after you call the Encrypt, GenerateDataKey, GenerateDataKeyWithoutPlaintext, or GenerateAndExportDataKey operation • Asymmetric encryption: the public key-encrypted ciphertext returned after you call the GenerateAndExportDataKey operation, or the ciphertext encrypted by using the public key of an asymmetric key pair outside KMS
DestinationKeyId	String	Yes	1234abcd-12ab-34cd-56ef-12345678****	The ID of the symmetric CMK that is used to re-encrypt the ciphertext after the ciphertext is decrypted.
SourceKeyId	String	No	5c438b18-05be-40ad-b6c2-3be6752c****	The ID of the CMK that is used to decrypt the ciphertext. This parameter is the globally unique ID of the CMK. Note If you set CiphertextBlob to the public key-encrypted ciphertext that is returned after an asymmetric encryption operation, specify this parameter.
SourceKeyVersionId	String	No	2ab1a983-7072-4bbc-a582-584b5bd8****	The ID of the CMK version that is used to decrypt the ciphertext. Note If you set CiphertextBlob to the public key-encrypted ciphertext that is returned after an asymmetric encryption operation, specify this parameter.

Parameter	Type	Required	Example	Description
SourceEncryptionAlgorithm	String	No	RSAES_OAEP_SHA_256	The encryption algorithm based on which the public key is used to encrypt the ciphertext specified by CiphertextBlob. For more information about encryption algorithms, see AsymmetricDecrypt. Valid values: • RSAES_OAEP_SHA_256 • RSAES_OAEP_SHA_1 • SM2PKE **Note** If you set CiphertextBlob to the public key-encrypted ciphertext that is returned after an asymmetric encryption operation, specify this parameter.
SourceEncryptionContext	Json	No	{"Example":"Example"}	A JSON string that consists of key-value pairs. If you specify EncryptionContext when you call the Encrypt, GenerateDataKey, GenerateDataKeyWithoutPlaintext, or GenerateAndExportDataKey operation to encrypt the data or data key, an equivalent value is required here. For more information, see EncryptionContext. **Note** If you set CiphertextBlob to the ciphertext that is returned after a symmetric encryption operation, specify this parameter.
DestinationEncryptionContext	Json	No	{"Example":"Example"}	A JSON string that consists of key-value pairs. This parameter specifies the EncryptionContext that is used to re-encrypt the decrypted data or data key.

Response parameters

Parameter	Type	Example	Description
CiphertextBlob	String	DZhOWVmZDktM2QxNi00ODk0LWJkNGYtMWZjNDNmM2YyYWJmaaSl+TztSIMe43nbTH/Z1Wr4XfLftKhAciUmDQXuMRl4WTvKhxjMThjK****	The ciphertext re-encrypted.
KeyId	String	2ab1a983-7072-4bbc-a582-584b5bd8****	The ID of the CMK that is used to decrypt the original ciphertext. This parameter is the globally unique ID of the CMK.
KeyVersionId	String	202b9877-5a25-46e3-a763-e20791b5****	The ID of the CMK version that is used to decrypt the original ciphertext.
RequestId	String	207596a2-36d3-4840-b1bd-f87044699bd7	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=ReEncrypt
&CiphertextBlob=ODZhOWVmZDktM2QxNi00ODk0LWJkNGYtMWZjNDNmM2YyYWJmS7FmDBBQ0BkKsQrtRnidtPwirmDcS0ZuJCU41xxAAWk4Z8qsADfbV0b+i6kQmlvj79dJdGOvtX69Uycs901q*
*******
&DestinationKeyId=1234abcd-12ab-34cd-56ef-12345678****
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
        <KeyId>202b9877-5a25-46e3-a763-e20791b5****</KeyId>
        <KeyVersionId>2ab1a983-7072-4bbc-a582-584b5bd8****</KeyVersionId>
        <CiphertextBlob>DZhOWVmZDktM2QxNi00ODk0LWJkNGYtMWZjNDNmM2YyYWJmaaSl+TztSIMe43nbTH/Z1Wr4XfLftKhAciUmDQXuMRl4WTvKhxjMThjK****</CiphertextBlob
>
        <RequestId>4bd560a1-729e-45f1-a3d9-b2a33d61046b</RequestId>
</KMS>
```

`JSON` format

```
{
    "KeyId": "202b9877-5a25-46e3-a763-e20791b5****",
    "KeyVersionId": "2ab1a983-7072-4bbc-a582-584b5bd8****",
    "CiphertextBlob": "DZhOWVmZDktM2QxNi00ODk0LWJkNGYtMWZjNDNmM2YyYWJmaaSl+TztSIMe43nbTH/Z1Wr4XfLftKhAciUmDQXuMRl4WTvKhxjMThjK****",
    "RequestId": "4bd560a1-729e-45f1-a3d9-b2a33d61046b"
}
```

Error codes

HTTP status code	Error code	Error message	Description
500	InternalFailure	Internal Failure.	The error message returned because an internal error has occurred. Try again later. If the error persists, submit a ticket.

For a list of error codes, visit the API Error Center.

8.24. AsymmetricSign

Generates a digital signature by using an asymmetric key.

This operation supports only asymmetric keys for which the **Usage** parameter is set to **SIGN/VERIFY**. The following table describes the supported signature algorithms.

Key type	Algorithm	Description
RSA_2048	RSA_PSS_SHA_256	RSASSA-PSS using SHA-256 and MGF1 with SHA-256
RSA_2048	RSA_PKCS1_SHA_256	RSASSA-PKCS1-v1_5 using SHA-256
RSA_3072	RSA_PSS_SHA_256	RSASSA-PSS using SHA-256 and MGF1 with SHA-256
RSA_3072	RSA_PKCS1_SHA_256	RSASSA-PKCS1-v1_5 using SHA-256
EC_P256	ECDSA_SHA_256	ECDSA on the P-256 Curve(secp256r1) with a SHA-256 digest
EC_P256K	ECDSA_SHA_256	ECDSA on the P-256K Curve(secp256k1) with a SHA-256 digest
EC_SM2	SM2DSA	SM2 elliptic curve public key encryption algorithm

Note When you calculate the SM2 signature based on GB/T 32918, the **Digest** parameter is used to calculate the digest value of the combination of Z(A) and M, rather than the SM3 digest value. M indicates the original message to be signed. Z(A) indicates the hash value for User A. The hash value is defined in GB/T 32918.

In this example, the asymmetric key whose ID is `5c438b18-05be-40ad-b6c2-3be6752c****` and version ID is `2ab1a983-7072-4bbc-a582-584b5bd8****` and the signature algorithm `RSA_PSS_SHA_256` are used to generate a digital signature for the digest `ZOyIygCyaOW6GjVnihtTFtIS9PNmskdyMlNKiuy****=`.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	AsymmetricSign	The operation that you want to perform. Set the value to AsymmetricSign.
Algorithm	String	Yes	RSA_PSS_SHA_256	The signature algorithm.
Digest	String	Yes	ZOyIygCyaOW6GjVnihtTFtIS9PNmskdyMlNKiu****=	The digest that is generated for the original message by using a hash algorithm. The hash algorithm is specified by the Algorithm parameter. **Note** • The value must be encoded in Base64. • For more information about how to calculate message digests, see the **Preprocess signature: compute a message digest** section of the Generate and verify a digital signature by using an asymmetric CMK topic.

Parameter	Type	Required	Example	Description
KeyId	String	Yes	5c438b18-05be-40ad-b6c2-3be6752c****	The GUID of the customer master key (CMK). Note You can also set this parameter to an alias that is bound to the CMK. For more information, see Alias overview.
KeyVersionId	String	Yes	2ab1a983-7072-4bbc-a582-584b5bd8****	The version ID of the CMK. The ID must be globally unique.

For more information about common request parameters, see Common parameters.

Response parameters

Parameter	Type	Example	Description
KeyId	String	5c438b18-05be-40ad-b6c2-3be6752c****	The GUID of the CMK. Note If you set the KeyId parameter in the request to an alias, the ID of the CMK to which the alias is bound is returned.
KeyVersionId	String	2ab1a983-7072-4bbc-a582-584b5bd8****	The version ID of the CMK. The ID is globally unique.
Value	String	M2CceNZH00ZgL9ED/ZHFp21YRAvYeZHknJUc207OCZ0N9wNn9As4z2bON3FF3je+1Nu+2+/8Zj50HpMTpzYpMp2R93cYmACCmhaYoKydxylbyGzJR8y9likZRCrkD38lRoS40aBBvv/6iRKzQuo9EGYVcel36cMNg00VmYNBy3pa1rwg3gA4l3cy6kjayZja1WGPkVhrVKsrJMdbpl0ApLjXKuD8rw1n1XLCwCUEL5eLPljTZaAveqdOFQOiZnZEGI27qIiZe7I1fN8tcz6anS/gTM7xRKE++5egEvRWlTQQTJeApnPSiUPA+8ZykNdelQsOQh5SrGoyI4A5pq****==	The calculated signature. Note The value is encoded in Base64.
RequestId	String	475f1620-b9d3-4d35-b5c6-3fbdd941423d	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=AsymmetricSign
&Algorithm=RSA_PSS_SHA_256
&Digest=ZOyIygCyaOW6GjVnihtTFtIS9PNmskdyMlNKiu****=
&KeyId=5c438b18-05be-40ad-b6c2-3be6752c****
&KeyVersionId=2ab1a983-7072-4bbc-a582-584b5bd8****
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
    <KeyId>5c438b18-05be-40ad-b6c2-3be6752c****</KeyId>
    <KeyVersionId>2ab1a983-7072-4bbc-a582-584b5bd8****</KeyVersionId>
    <Value>M2CceNZH00ZgL9ED/ZHFp21YRAvYeZHknJUc207OCZ0N9wNn9As4z2bON3FF3je+1Nu+2+/8Zj50HpMTpzYpMp2R93cYmACCmhaYoKydxylbyGzJR8y9likZRCrkD38lRoS40aBBvv
/6iRKzQuo9EGYVcel36cMNg00VmYNBy3pa1rwg3gA4l3cy6kjayZja1WGPkVhrVKsrJMdbpl0ApLjXKuD8rw1n1XLCwCUEL5eLPljTZaAveqdOFQOiZnZEGI27qIiZe7I1fN8tcz6anS/gTM7xRKE
++5egEvRWlTQQTJeApnPSiUPA+8ZykNdelQsOQh5SrGoyI4A5pq****==</Value>
    <RequestId>475f1620-b9d3-4d35-b5c6-3fbdd941423d</RequestId>
</KMS>
```

`JSON` format

```
{
  "KeyId": "5c438b18-05be-40ad-b6c2-3be6752c****",
  "KeyVersionId": "2ab1a983-7072-4bbc-a582-584b5bd8****",
  "Value": "M2CceNZH00ZgL9ED/ZHFp21YRAvYeZHknJUc207OCZ0N9wNn9As4z2bON3FF3je+1Nu+2+/8Zj50HpMTpzYpMp2R93cYmACCmhaYoKydxylbyGzJR8y9likZRCrkD38lRoS40aBBv
v/6iRKzQuo9EGYVcel36cMNg00VmYNBy3pa1rwg3gA4l3cy6kjayZja1WGPkVhrVKsrJMdbpl0ApLjXKuD8rw1n1XLCwCUEL5eLPljTZaAveqdOFQOiZnZEGI27qIiZe7I1fN8tcz6anS/gTM7xRK
E++5egEvRWlTQQTJeApnPSiUPA+8ZykNdelQsOQh5SrGoyI4A5pq****==",
  "RequestId": "475f1620-b9d3-4d35-b5c6-3fbdd941423d"
}
```

Error codes

For a list of error codes, visit the API Error Center.

8.25. AsymmetricVerify

Verifies a digital signature by using an asymmetric key.

This operation supports only asymmetric keys for which the **Usage** parameter is set to **SIGN/VERIFY**. The following table describes the supported signature algorithms.

Key type	Algorithm	Description
RSA_2048	RSA_PSS_SHA_256	RSASSA-PSS using SHA-256 and MGF1 with SHA-256
RSA_2048	RSA_PKCS1_SHA_256	RSASSA-PKCS1-v1_5 using SHA-256
RSA_3072	RSA_PSS_SHA_256	RSASSA-PSS using SHA-256 and MGF1 with SHA-256
RSA_3072	RSA_PKCS1_SHA_256	RSASSA-PKCS1-v1_5 using SHA-256
EC_P256	ECDSA_SHA_256	ECDSA on the P-256 Curve(secp256r1) with a SHA-256 digest
EC_P256K	ECDSA_SHA_256	ECDSA on the P-256K Curve(secp256k1) with a SHA-256 digest
EC_SM2	SM2DSA	SM2 elliptic curve public key encryption algorithm

Note When you calculate the SM2 signature based on GB/T 32918, the **Digest** parameter is used to calculate the digest value of the combination of Z(A) and M, rather than the SM3 digest value. M indicates the original message to be signed. Z(A) indicates the hash value for User A. The hash value is defined in GB/T 32918.

In this example, the asymmetric key whose ID is `5c438b18-05be-40ad-b6c2-3be6752c****` and version ID is `2ab1a983-7072-4bbc-a582-584b5bd8****` and the signature algorithm RSA_PSS_SHA_256 are used to verify the digital signature `M2CceNZH00ZgL9ED/ZHFp21YRAvYeZHknJUc207OCZ0N9wNn9As4z2bON3FF3je+1Nu+2+/8Zj50HpMTpzYpMp2R93cYmACCmhaYoKydxylbyGzJR8y9likZRCrkD38lRoS40aBBvv/6iRKzQuo9EGYV` of the digest `ZOyIygCyaOW6GjVnihtTFtIS9PNmskdyMlNKiuyjfzw=` .

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	AsymmetricVerify	The operation that you want to perform. Set the value to AsymmetricVerify.
Algorithm	String	Yes	RSA_PSS_SHA_256	The signature algorithm.
Digest	String	Yes	ZOylygCyaOW6GjVnihtTFtIS9PNmskdyMlNKiuy****=	The digest that is generated for the original message by using a hash algorithm. The hash algorithm is specified by the **Algorithm** parameter. **Note** The value must be encoded in Base64.
KeyId	String	Yes	5c438b18-05be-40ad-b6c2-3be6752c****	The globally unique ID (GUID) of the CMK. **Note** You can also set this parameter to an alias that is bound to the CMK. For more information, see Use aliases.
KeyVersionId	String	Yes	2ab1a983-7072-4bbc-a582-584b5bd8****	The ID of the CMK version. The ID must be globally unique.
Value	String	Yes	M2CceNZH00ZgL9ED/ZHFp21YRAvYeZHknJUc207OCZ0N9wNn9As4z2bON3FF3je+1Nu+2+/8Zj50HpMTpzYpMp2R93cYmACCmhaYoKydxylbyGzJR8y9likZRCrkD38lRoS40aBBvv/6iRKzQuo9EGYVcel36cMNg00VmYNBy3pa1rwg3gA4l3cy6kjayZja1WGPkVhrVKsrJMdbpl0ApLjXKuD8rw1n1XLCwCUEL5eLPljTZaAveqdOFQOiZnZEGl27qliZe7I1fN8tcz6anS/gTM7xRKE++5egEvRWlTQQTJeApnPSiUPA+8ZykNdelQsOQh5SrGoyI4A5pq****==	The signature value to be verified. **Note** The value must be encoded in Base64.

For more information about common request parameters, see Common parameters.

Response parameters

Parameter	Type	Example	Description
KeyId	String	5c438b18-05be-40ad-b6c2-3be6752c****	The GUID of the CMK. **Note** If you set the KeyId parameter in the request to an alias, the ID of the CMK to which the alias is bound is returned.
KeyVersionId	String	2ab1a983-7072-4bbc-a582-584b5bd8****	The version of the CMK that is used to verify the signature.
Value	Boolean	true	Indicates whether the signature passed the verification.
RequestId	String	475f1620-b9d3-4d35-b5c6-3fbdd941423d	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=AsymmetricVerify
&Algorithm=RSA_PSS_SHA_256
&Digest=ZOyIygCyaOW6GjVnihtTFtIS9PNmskdyMlNKiuy****=
&KeyId=5c438b18-05be-40ad-b6c2-3be6752c****
&KeyVersionId=2ab1a983-7072-4bbc-a582-584b5bd8****
&Value=M2CceNZH00ZgL9ED/ZHFp21YRAvYeZHknJUc207OCZ0N9wNn9As4z2bON3FF3je+1Nu+2+/8Zj50HpMTpzYpMp2R93cYmACCmhaYoKydxylbyGzJR8y9likZRCrkD38lRoS40aBBvv/6iR
KzQuo9EGYVcel36cMNg00VmYNBy3pa1rwg3gA413cy6kjayZja1WGPkVhrVKsrJMdbpl0ApLjXKuD8rw1n1XLCwCUEL5eLPljTZaAveqdOFQOiZnZEGI27qIiZe7I1fN8tcz6anS/gTM7xRKE++5e
gEvRWlTQQTJeApnPSiUPA+8ZykNdelQsOQh5SrGoyI4A5pq****==
&<Common request parameters>|
```

Sample success responses

`XML` format

```
<KMS>
    <KeyId>5c438b18-05be-40ad-b6c2-3be6752c****</KeyId>
    <KeyVersionId>2ab1a983-7072-4bbc-a582-584b5bd8****</KeyVersionId>
    <Value>true</Value>
    <RequestId>475f1620-b9d3-4d35-b5c6-3fbdd941423d</RequestId>
</KMS>
```

`JSON` format

```
{
  "KeyId": "5c438b18-05be-40ad-b6c2-3be6752c****",
  "KeyVersionId": "2ab1a983-7072-4bbc-a582-584b5bd8****",
  "Value": true,
  "RequestId": "475f1620-b9d3-4d35-b5c6-3fbdd941423d"
}
```

Error codes

For a list of error codes, visit the API Error Center.

8.26. AsymmetricDecrypt

Decrypts data by using an asymmetric key.

This operation supports only asymmetric keys for which the **Usage** parameter is set to **ENCRYPT / DECRYPT** . The following table describes the supported encryption algorithms.

Key type	Algorithm	Description	Maximum length in bytes
RSA_2048	RSAES_OAEP_SHA_256	RSAES-OAEP using SHA-256 and MGF1 with SHA-256	256
RSA_2048	RSAES_OAEP_SHA_1	RSAES-OAEP using SHA1 and MGF1 with SHA1	256
RSA_3072	RSAES_OAEP_SHA_256	RSAES-OAEP using SHA-256 and MGF1 with SHA-256	384
RSA_3072	RSAES_OAEP_SHA_1	RSAES-OAEP using SHA1 and MGF1 with SHA1	384

Key type	Algorithm	Description	Maximum length in bytes
EC_SM2	SM2PKE	SM2 elliptic curve public key encryption algorithm	6144

In this example, the asymmetric key whose ID is `5c438b18-05be-40ad-b6c2-3be6752c****` and version ID is `2ab1a983-7072-4bbc-a582-584b5bd8****` and the decryption algorithm `RSAES_OAEP_SHA_1` are used to decrypt the ciphertext `BQKP+1zK6+ZEMxTP5qaVzcsgXtWplYBKm0NXdSnB5FzliFxE1bSiu4dnEIlca2JpeH7yz1/S6fed630H+hIH6DoM25fTLNcKj+mFB0Xnh9m2+HN59Mn4qyTfcUeadnfCXSWcGBouhXFwcdd2rJ3n337b`.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	AsymmetricDecrypt	The operation that you want to perform. Set the value to AsymmetricDecrypt.
KeyId	String	Yes	5c438b18-05be-40ad-b6c2-3be6752c****	The globally unique ID (GUID) of the CMK. **Note** You can also set this parameter to an alias that is bound to the CMK. For more information, see Use aliases.
Algorithm	String	Yes	RSAES_OAEP_SHA_1	The asymmetric decryption algorithm to use.
CiphertextBlob	String	Yes	BQKP+1zK6+ZEMxTP5qaVzcsgXtWplYBKm0NXdSnB5FzliFxE1bSiu4dnEIlca2JpeH7yz1/S6fed630H+hIH6DoM25fTLNcKj+mFB0Xnh9m2+HN59Mn4qyTfcUeadnfCXSWcGBouhXFwcdd2rJ3n337bzTf4jm659gZu3L0i6PLuxM9p7mqdwO0cKJPfGVfhnfMz+f4alMg79WB/NNyE2lyX7/qxvV49ObNrrJbKSFiz8Djocaf0IESNLMbfYI5bXjWkJlX92DQbKhibtQW8ZOJ//ZC6t0AWcUoKL6QDm/dg5koQalcleRinpB+QadFm894sLbVZ9+N4GVsv1W****==	The ciphertext that you want to decrypt. **Note** • The value must be encoded in Base64. • You can call the AsymmetricEncrypt operation to generate the ciphertext.
KeyVersionId	String	Yes	2ab1a983-7072-4bbc-a582-584b5bd8****	The ID of the CMK version. The ID must be globally unique.

For more information about common request parameters, see Common parameters.

Response parameters

Parameter	Type	Example	Description
KeyId	String	5c438b18-05be-40ad-b6c2-3be6752c****	The GUID of the CMK. **Note** If you set the KeyId parameter in the request to an alias, the ID of the CMK to which the alias is bound is returned.
KeyVersionId	String	2ab1a983-7072-4bbc-a582-584b5bd8****	The version of the CMK that is used to decrypt the ciphertext.
Plaintext	String	SGVsbG8gd29ybGQ=	The Base64-encoded plaintext that was generated after decryption.
RequestId	String	475f1620-b9d3-4d35-b5c6-3fbdd941423d	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=AsymmetricDecrypt
&KeyId=5c438b18-05be-40ad-b6c2-3be6752c****
&Algorithm=RSAES_OAEP_SHA_1
&CiphertextBlob=BQKP+1zK6+ZEMxTP5qaVzcsgXtWplYBKm0NXdSnB5FzliFxE1bSiu4dnEIlca2JpeH7yz1/S6fed630H+hIH6DoM25fTLNcKj+mFB0Xnh9m2+HN59Mn4qyTfcUeadnfCXSWcG
BouhXFwcdd2rJ3n337bzTf4jm659gZu3L0i6PLuxM9p7mqdwO0cKJPfGVfhnfMz+f4alMg79WB/NNyE2lyX7/qxvV49ObNrrJbKSFiz8Djocaf0IESNLMbfYI5bXjWkJlX92DQbKhibtQW8ZOJ//Z
C6t0AWcUoKL6QDm/dg5koQalcleRinpB+QadFm894sLbVZ9+N4GVsv1W****==
&KeyVersionId=2ab1a983-7072-4bbc-a582-584b5bd8****
&<Common request parameters>|
```

Sample success responses

`XML` format

```
<KMS>
    <KeyId>5c438b18-05be-40ad-b6c2-3be6752c****</KeyId>
    <KeyVersionId>2ab1a983-7072-4bbc-a582-584b5bd8****</KeyVersionId>
    <Plaintext>SGVsbG8gd29ybGQ=</Plaintext>
    <RequestId>475f1620-b9d3-4d35-b5c6-3fbdd941423d</RequestId>
</KMS>
```

`JSON` format

```
{
  "KeyId": "5c438b18-05be-40ad-b6c2-3be6752c****",
  "KeyVersionId": "2ab1a983-7072-4bbc-a582-584b5bd8****",
  "Plaintext": "SGVsbG8gd29ybGQ=",
  "RequestId": "475f1620-b9d3-4d35-b5c6-3fbdd941423d"
}
```

Error codes

For a list of error codes, visit the API Error Center.

8.27. AsymmetricEncrypt

Encrypts data by using an asymmetric customer master key (CMK).

This operation is supported only when the asymmetric CMK has the **usage** attribute of **ENCRYPT/DECRYPT**. The following table lists supported encryption algorithms.

KeySpec	Algorithm	Description	Maximum number of bytes that can be encrypted
RSA_2048	RSAES_OAEP_SHA_256	RSAES-OAEP using SHA-256 and MGF1 with SHA-256	190
RSA_2048	RSAES_OAEP_SHA_1	RSAES-OAEP using SHA1 and MGF1 with SHA1	214
RSA_3072	RSAES_OAEP_SHA_256	RSAES-OAEP using SHA-256 and MGF1 with SHA-256	318
RSA_3072	RSAES_OAEP_SHA_1	RSAES-OAEP using SHA1 and MGF1 with SHA1	342
EC_SM2	SM2PKE	SM2 public key encryption algorithm based on elliptic curves	6047

You can use the asymmetric CMK whose ID is `5c438b18-05be-40ad-b6c2-3be6752c****` and version ID is `2ab1a983-7072-4bbc-a582-584b5bd8****` and the algorithm `RSAES_OAEP_SHA_1` to encrypt the plaintext `SGVsbG8gd29ybGQ=` based on the parameter settings provided in this topic.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	AsymmetricEncrypt	The operation that you want to perform. Set the value to AsymmetricEncrypt.
Algorithm	String	Yes	RSAES_OAEP_SHA_1	The encryption algorithm that you want to use.

Parameter	Type	Required	Example	Description
KeyId	String	Yes	5c438b18-05be-40ad-b6c2-3be6752c****	The ID of the CMK. The ID must be globally unique. **Note** You can also set the value to an alias that is bound to the CMK. For more information, see Overview of aliases.
KeyVersionId	String	Yes	2ab1a983-7072-4bbc-a582-584b5bd8****	The version ID of the CMK. The ID must be globally unique. **Note** You can call the ListKeyVersions operation to query the versions of a CMK. The ID of a version is specified by the KeyVersionId parameter.
Plaintext	String	Yes	SGVsbG8gd29ybGQ=	The plaintext that you want to encrypt. The plaintext must be Base64-encoded.

For more information about common request parameters, see Common parameters.

Response parameters

Parameter	Type	Example	Description
KeyId	String	5c438b18-05be-40ad-b6c2-3be6752c****	The ID of the CMK. **Note** If you set the KeyId parameter in the request to an alias, the ID of the CMK to which the alias is bound is returned.
KeyVersionId	String	2ab1a983-7072-4bbc-a582-584b5bd8****	The version ID of the CMK that is used to encrypt the plaintext.
CiphertextBlob	String	BQKP+1zK6+ZEMxTP5qaVzcsgXtWplYBKm0NXdSnB5FzliFxE1bSiu4dnEllca2JpeH7yz1/S6fed630H+hIH6DoM25fTLNcKj+mFB0Xnh9m2+HN59Mn4qyTfcUeadnfCXSWcGBouhXFwcdd2rJ3n337bzTf4jm659gZu3L0i6PLuxM9p7mqdwO0cKJPfGVfhnfMz+f4alMg79WB/NNyE2lyX7/qxvV49ObNrrJbKSFiz8Djocaf0IESNLMbfYI5bXjWkJlX92DQbKhibtQW8ZOJ//ZC6t0AWcUoKL6QDm/dg5koQalcleRinpB+QadFm894sLbVZ9+N4GVsv1Wbjwg==	The Base64-encoded ciphertext that was generated after encryption.
RequestId	String	475f1620-b9d3-4d35-b5c6-3fbdd941423d	The ID of the request.

Examples

Sample requests

```
https://[Endpoint]/?Action=AsymmetricEncrypt
&KeyId=5c438b18-05be-40ad-b6c2-3be6752c****
&KeyVersionId=2ab1a983-7072-4bbc-a582-584b5bd8****
&Algorithm=RSAES_OAEP_SHA_1
&Plaintext=SGVsbG8gd29ybGQ=
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
    <KeyId>5c438b18-05be-40ad-b6c2-3be6752c****</KeyId>
    <KeyVersionId>2ab1a983-7072-4bbc-a582-584b5bd8****</KeyVersionId>
    <CiphertextBlob>RKF5WeXJtusIrvuPOjpkA/55EKzi8Wmc/eJ2fQUKphvL750jtInSX1wijw/7jGxUaTHTW6tgIJl2ReN1aI1/wxqGxdzScwsMHxCBncnzQsZF+Fi4UFpI9pr4A1wc2u5Ngwyx9uA4K/kJ5bkS4NvmanxssAPZfSfbJSrAWlCP11tSOCd54tQVGj4XK9tP9bJDKzKis1NClsOXZtNPX88kUqr3LkgFCsD07IwiePAfI2tn2fzeisje1Q7/d6VkF48c3ZE0DAmnLRujt3yRRGDaKUkI6SUDjuKD4yqBUX15/DKfJtya+JIPQGiO2IEPlhL7+NMT17U0tKtK5ZPNEwxfZw==</CiphertextBlob>
    <RequestId>475f1620-b9d3-4d35-b5c6-3fbdd941423d</RequestId>
</KMS>
```

`JSON` format

```
{
  "KeyId": "5c438b18-05be-40ad-b6c2-3be6752c****",
  "KeyVersionId": "2ab1a983-7072-4bbc-a582-584b5bd8****",
  "CiphertextBlob": "RKF5WeXJtusIrvuPOjpkA/55EKzi8Wmc/eJ2fQUKphvL750jtInSX1wijw/7jGxUaTHTW6tgIJl2ReN1aI1/wxqGxdzScwsMHxCBncnzQsZF+Fi4UFpI9pr4A1wc2u5N
gwyx9uA4K/kJ5bkS4NvmanxssAPZfSfbJSrAWlCP11tS0Cd54tQVGj4XK9tP9bJDKzKis1NClsOXZtNPX88kUqr3LkgFCsD07IwiePAfI2tn2fzeisje1Q7/d6VkF48c3ZE0DAmnLRujt3yRRGDaK
UkI6SUDjuKD4yqBUX15/DKfJtya+JIPQGiO2IEPlhL7+NMT17U0tKtK5ZPNEwxfZw==",
  "RequestId": "475f1620-b9d3-4d35-b5c6-3fbdd941423d"
}
```


Error codes

For a list of error codes, visit the API Error Center.

8.28. GetPublicKey

Obtains the public key of an asymmetric key pair. You can use the public key to encrypt local data and verify signatures.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	GetPublicKey	The operation that you want to perform. Set the value to GetPublicKey.
KeyId	String	Yes	5c438b18-05be-40ad-b6c2-3be6752c****	The globally unique ID of the CMK. You can also set this parameter to an alias that is bound to the CMK. For more information, see Use aliases.
KeyVersionId	String	Yes	2ab1a983-7072-4bbc-a582-584b5bd8****	The globally unique ID of the CMK version.

Response parameters

Parameter	Type	Example	Description
KeyId	String	5c438b18-05be-40ad-b6c2-3be6752c****	The globally unique ID of the CMK. Note If you set the KeyId parameter to the alias of the CMK, the ID of the CMK to which the alias is bound is returned.
KeyVersionId	String	2ab1a983-7072-4bbc-a582-584b5bd8****	The version of the CMK that is used to encrypt the plaintext.
PublicKey	String	-----BEGIN PUBLIC KEY-----\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAs5Yu9AEgATN2/e3nUz1K\nEy6ng8MSPutcse2/VECG/NUF9C6D4IsJ64ShzY3dcn34WYzTOe916eMJFxyrNrSw\nHtc4UOR5AvaoRrfpgu2uq+i70/ZXrWL+pGb1hgZV8cWheIHMxwrR3liQlM5qN7EF\n9BdyWtyBfUGsp0Bn1VqlPc5G0x0a9xU2z9YtP994yDenNVIoIQ6Cov1lIEuwXAb2\n7boC41ePXwD0JWt41sP+rgCmpjBx00puIG+IlnoReEgI1ZGYmK98GgA/XzmNjZiD\nyvXJZAcM33Ue85+PkR5iHTtSEbi4QAoqpJabprUzz3Fin2j1dRrcacxGb7p31A9c\nJQIDAQAB\n-----END PUBLIC KEY-----\n	The public key returned in the PEM format.
RequestId	String	475f1620-b9d3-4d35-b5c6-3fbdd941423d	The ID of the request.

Examples

Sample requests

```
https://[Endpoint]/?Action=GetPublicKey
&KeyId=5c438b18-05be-40ad-b6c2-3be6752c****
&KeyVersionId=2ab1a983-7072-4bbc-a582-584b5bd8****
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
    <KeyId>5c438b18-05be-40ad-b6c2-3be6752c****</KeyId>
    <KeyVersionId>2ab1a983-7072-4bbc-a582-584b5bd8****</KeyVersionId>
    <PublicKey>-----BEGIN PUBLIC KEY-----\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAs5Yu9AEgATN2/e3nUz1K\nEy6ng8MSPutcse2/VECG/NUF9C6D4IsJ64ShzY3d
cn34WYzTOe916eMJFxyrNrSw\nHtc4UOR5AvaoRrfpgu2uq+i70/ZXrWL+pGb1hgZV8cWheIHMxwrR3IiQlM5qN7EF\n9BdyWtyBfUGsp0Bn1VqlPc5G0x0a9xU2z9YtP994yDenNVIoIQ6Cov1lI
EuwXAb2\n7boC41ePXwD0JWt41sP+rgCmpjBx00puIG+IlnoReEgI1ZGYmK98GgA/XzmNjZiD\nyvXJZAcM33Ue85+PkR5iHTtSEbi4QAoqpJabprUzz3Fin2j1dRrcacxGb7p31A9c\nJQIDAQAB
\n-----END PUBLIC KEY-----\n</PublicKey>
    <RequestId>475f1620-b9d3-4d35-b5c6-3fbdd941423d</RequestId>
</KMS>
```

`JSON` format

```
{
  "KeyId": "5c438b18-05be-40ad-b6c2-3be6752c****",
  "KeyVersionId": "2ab1a983-7072-4bbc-a582-584b5bd8****",
  "PublicKey": "-----BEGIN PUBLIC KEY-----\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAs5Yu9AEgATN2/e3nUz1K\nEy6ng8MSPutcse2/VECG/NUF9C6D4IsJ64ShzY3
dcn34WYzTOe916eMJFxyrNrSw\nHtc4UOR5AvaoRrfpgu2uq+i70/ZXrWL+pGb1hgZV8cWheIHMxwrR3IiQlM5qN7EF\n9BdyWtyBfUGsp0Bn1VqlPc5G0x0a9xU2z9YtP994yDenNVIoIQ6Cov1l
IEuwXAb2\n7boC41ePXwD0JWt41sP+rgCmpjBx00puIG+IlnoReEgI1ZGYmK98GgA/XzmNjZiD\nyvXJZAcM33Ue85+PkR5iHTtSEbi4QAoqpJabprUzz3Fin2j1dRrcacxGb7p31A9c\nJQIDAQA
B\n-----END PUBLIC KEY-----\n",
  "RequestId": "475f1620-b9d3-4d35-b5c6-3fbdd941423d"
}
```

Error codes

For a list of error codes, visit the API Error Center.

8.29. CreateAlias

Creates an alias for a customer master key (CMK).

Usage notes:

- Each alias can be bound to only one CMK at a time.
- The aliases of CMKs in the same region must be unique.

This topic provides an example on how to create an alias that is named `alias/example` for the CMK `1234abcd-12ab-34cd-56ef-12345678****`.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	CreateAlias	The operation that you want to perform. Set the value to CreateAlias.
AliasName	String	Yes	alias/example	The name of the alias. The name must be 1 to 255 characters in length and must include the `alias/` prefix.
KeyId	String	Yes	1234abcd-12ab-34cd-56ef-12345678****	The globally unique ID of the CMK.

Response parameters

Parameter	Type	Example	Description
RequestId	String	1d2baaf3-d357-46c2-832e-13560c2bd9cd	The ID of the request.

Examples

Sample requests

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=CreateAlias
&AliasName=alias/example
&KeyId=1234abcd-12ab-34cd-56ef-12345678****
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
        <RequestId>1d2baaf3-d357-46c2-832e-13560c2bd9cd</RequestId>
</KMS>
```

`JSON` format

```
{
    "RequestId": "1d2baaf3-d357-46c2-832e-13560c2bd9cd"
}
```

Error codes

For a list of error codes, visit the API Error Center.

8.30. UpdateAlias

Associates an existing alias with a different CMK ID.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	UpdateAlias	The operation that you want to perform. Set the value to UpdateAlias.
AliasName	String	Yes	alias/example	The alias that you want to associate with a different CMK ID. The value must be 1 to 255 characters in length and must include the alias/ prefix.
KeyId	String	Yes	1234abcd-12ab-34cd-56ef-12345678****	The CMK ID with which you want to associate the alias. This parameter is the globally unique ID of the CMK.

Response parameters

Parameter	Type	Example	Description
RequestId	String	1d2baaf3-d357-46c2-832e-13560c2bd9cd	The ID of the request.

Examples

Sample requests

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=UpdateAlias
&AliasName=alias/example
&KeyId=1234abcd-12ab-34cd-56ef-12345678****
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
        <RequestId>1d2baaf3-d357-46c2-832e-13560c2bd9cd</RequestId>
</KMS>
```

`JSON` format

```
{
       "RequestId": "1d2baaf3-d357-46c2-832e-13560c2bd9cd"
}
```

Error codes

HTTP status code	Error code	Error message	Description
400	Throttling	Request was denied due to request throttling.	The error message returned because your traffic in this period has exceeded the limit. If your business requirements are not met, submit a ticket.
404	Forbidden.KeyNotFound	The specified Key is not found.	The error message returned because the specified CMK does not exist.

For a list of error codes, visit the API Error Center.

8.31. DeleteAlias

Deletes an alias.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DeleteAlias	The operation that you want to perform. Set the value to DeleteAlias.
AliasName	String	Yes	alias/example	The alias that you want to delete. The value must be 1 to 255 characters in length and must include the alias/ prefix.

Response parameters

Parameter	Type	Example	Description
RequestId	String	4c8ae23f-3a42-6791-a4ba-1faa77831c28	The ID of the request.

Examples

Sample requests

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=DeleteAlias
&AliasName=alias/example
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
        <RequestId>4c8ae23f-3a42-6791-a4ba-1faa77831c28</RequestId>
</KMS>
```

`JSON` format

```
{
        "RequestId": "4c8ae23f-3a42-6791-a4ba-1faa77831c28"
}
```

Error codes

For a list of error codes, visit the API Error Center.

8.32. ListAliases

Queries all aliases in the current region for the current account.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ListAliases	The operation that you want to perform. Set the value to ListAliases.
PageNumber	Integer	No	1	The number of the page to return. Pages start from page 1. Default value: 1.
PageSize	Integer	No	10	The number of entries to return on each page. Valid values: 0 to 100. Default value: 10.

Response parameters

Parameter	Type	Example	Description
Aliases	Array of Alias		The alias of the user.

Parameter	Type	Example	Description
Alias			
AliasArn	String	acs:kms:cn-hangzhou:123456:alias/ExampleAlias1	The Alibaba Cloud Resource Name (ARN) of the alias.
AliasName	String	alias/ExampleAlias1	The ID of the alias.
KeyId	String	08c33a6f-4e0a-4a1b-a3fa-7ddfa1d****	The CMK to which the alias belongs.
PageNumber	Integer	1	The page number of the returned page.
PageSize	Integer	10	The number of entries returned per page.
RequestId	String	1b57992c-834b-4811-a889-f8bac1ba0353	The ID of the request.
TotalCount	Integer	1	The total number of returned aliases.

Examples

Sample requests

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=ListAliases
&PageNumber=1
&PageSize=10
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
          <Aliases>
                    <Alias>
                              <AliasName>alias/ExampleAlias1</AliasName>
                              <KeyId>08c33a6f-4e0a-4a1b-a3fa-7ddfa1****</KeyId>
                              <AliasArn>acs:kms:cn-hangzhou:123456:alias/ExampleAlias1</AliasArn>
                    </Alias>
          </Aliases>
          <TotalCount>1</TotalCount>
          <PageNumber>1</PageNumber>
          <PageSize>10</PageSize>
          <RequestId>1b57992c-834b-4811-a889-f8bac1ba0353</RequestId>
</KMS>
```

`JSON` format

```
{
        "Aliases": {
                "Alias": [
                        {
                                "AliasName": "alias/ExampleAlias1",
                                "KeyId": "08c33a6f-4e0a-4a1b-a3fa-7ddfa1d****",
                                "AliasArn": "acs:kms:cn-hangzhou:123456:alias/ExampleAlias1"
                        }
        ]
        },
        "TotalCount": 1,
        "PageNumber": 1,
        "PageSize": 10,
        "RequestId": "1b57992c-834b-4811-a889-f8bac1ba0353"
}
```

Error codes

For a list of error codes, visit the API Error Center.

8.33. ListAliasesByKeyId

Queries all aliases bound to a CMK.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ListAliasesByKeyId	The operation that you want to perform. Valid values: ListAliasesByKeyId
KeyId	String	Yes	1234abcd-12ab-34cd-56ef-12345678****	The globally unique ID of the CMK.
PageNumber	Integer	Optional	1	The number of the page to return. Value range: integers greater than 0. Default value: 1.
PageSize	Integer	Optional	10	The number of entries to return on each page. Valid values: 0 to 101. Default value: 10.

Response parameters

Prameter	Type	Sample response	Description
TotalCount	Integer	1	The total number of returned cmks.
PageNumber	Integer	1	The number of the page to return.
PageSize	Integer	10	The number of entries returned per page.
RequestId	String	1 b57992 c-834b-4811-a889-f8bac1ba0353	The ID of the request.
Aliases	Array		The alias of the field.
KeyId	String	08 c33a6 f-4e0a-4a1b-a3fa-7ddfa1d4 function compute instance *	The CMK to which the alias belongs.
AliasName	String	alias/ExampleAlias1	The unique identifier of the alias.
AliasArn	String	acs:kms:cn-hangzhou:123456:alias/ExampleAlias1	The ARN of the alias.

Examples

Sample requests

```
https://kms.cn-hangzhou.aliyuncs.com/? Action=ListAliasesByKeyId
&PageNumber=1
&PageSize=10
&KeyId=<cmkid>
&<Common request parameters>
```

Sample success responses

`XML` format

```
//xml response
<KMS>
        <Aliases>
                <Alias>
                        <AliasName>alias/ExampleAlias1</AliasName>
                        <KeyId>08c33a6f-4e0a-4a1b-a3fa-7ddfa1d4****</KeyId>
                        <AliasArn>acs:kms:cn-hangzhou:123456:alias/ExampleAlias1</AliasArn>
                </Alias>
        </Aliases>
        <TotalCount>1</TotalCount>
        <PageNumber>1</PageNumber>
        <PageSize>10</PageSize>
        <RequestId>1b57992c-834b-4811-a889-f8bac1ba0353</RequestId>
</KMS>
```

`JSON` format

```
//json response
{
        "Aliases": {
                "Alias": [
                        {
                                "AliasName": "alias/ExampleAlias1",
                                "KeyId": "08c33a6f-4e0a-4a1b-a3fa-7ddfa1d4****",
                                "AliasArn": "acs:kms:cn-hangzhou:123456:alias/ExampleAlias1"
                        }
        ]
        },
        "TotalCount": 1,
        "PageNumber": 1,
        "PageSize": 10,
        "RequestId": "1b57992c-834b-4811-a889-f8bac1ba0353"
}
```

Error codes

HTTP status code	Error code	Error message	Description
400	Throttling	Request was denied due to request throttling.	This message returned because your traffic in this period has exceeded the limit. If your business requirements are not met, submit a ticket.

9.Secrets

9.1. CreateSecret

Creates a secret and stores its initial version.

You must specify the secret name, the secret value stored in the initial version, and the version number. The initial version is marked with ACSCurrent.

You can specify a symmetric customer master key (CMK) as the encryption key to encrypt the secret value. If you do not specify an encryption key, Secrets Manager creates a CMK to encrypt the secret value. This CMK is used as the default encryption key for all the secrets that are created by your Alibaba Cloud account in the current region. Secrets Manager encrypts only the secret value of each version. Secrets Manager does not encrypt the metadata such as the secret name, version number, or state label.

To use a specified CMK to encrypt the secret value, you must have the `kms:GenerateDataKey` permission on the CMK.

In this example, a generic secret whose name is `mydbconninfo` is created. The initial version number of the secret is specified in the `VersionId` parameter, and the value is `v1`. The secret value is specified in the `SecretData` parameter, and the value is `{"user":"root","passwd":"****"}`.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	CreateSecret	The operation that you want to perform. Set the value to CreateSecret.
SecretData	String	Yes	null	The value of the secret to be created. Secrets Manager encrypts the secret value and stores the encrypted value in the initial version. • If you set the SecretType parameter to Generic that indicates a generic secret, you can customize the secret value. • If you set the SecretType parameter to Rds that indicates a managed ApsaraDB RDS secret, the secret value must be in the format of `{"Accounts":[{"AccountName":"","AccountPassword":""}]}`. In the preceding format, `AccountName` indicates the username of the account that is used to connect to your ApsaraDB RDS instance, and `AccountPassword` indicates the password of the account. • If you set the SecretType parameter to RAMCredentials that indicates a managed RAM secret, the secret value must be in the format of `{"AccessKeys":[{"AccessKeyId":"","AccessKeySecret":"",}]}`. In the preceding format, `AccessKeyId` indicates the AccessKey ID of the RAM user and `AccessKeySecret` indicates the AccessKey secret of the RAM user. You must specify all the AccessKey pairs of the RAM user. • If you set the SecretType parameter to ECS that indicates a managed ECS secret, the secret value must be in one of the following formats: ◦ `{"UserName":"","Password": ""}`: In the format, `UserName` indicates the username that is used to log on to the ECS instance, and `Password` indicates the password that is used to log on to the ECS instance. ◦ `{"UserName":"","PublicKey": "", "PrivateKey": ""}`: In the format, `PublicKey` indicates the SSH public key that is used to log on to the ECS instance, and `PrivateKey` indicates the SSH private key that is used to log on to the ECS instance.
SecretName	String	Yes	mydbconninfo	The name of the secret. The name must be 1 to 64 characters in length and can contain letters, digits, and the following special characters: `_/+=.@-`. The following list describes the name requirements for different types of secrets: • If the SecretType parameter is set to Generic or Rds, the name cannot start with `acs/`. • If the SecretType parameter is set to RAMCredentials, the value of the SecretName parameter is fixed as `$Auto`. In this case, KMS automatically generates a secret name that starts with `acs/ram/user/`. The name includes the display name of RAM user. • If the SecretType parameter is set to ECS, the name must start with `acs/ecs/`.
VersionId	String	Yes	v1	The initial version number. Version numbers are unique in each secret object.

Parameter	Type	Required	Example	Description
EncryptionKeyId	String	No	00aa68af-2c02-4f68-95fe-3435d330****	The ID of the CMK that is used to encrypt the secret value. If you do not specify this parameter, Secrets Manager automatically creates a CMK to encrypt the secret value. **Note** The CMK must be a symmetric key.
SecretDataType	String	No	text	The type of the secret value. Valid values: • text • binary **Note** If you set the SecretType parameter to Rds, RAMCredentials, or ECS, the SecretDataType parameter must be set to text.
Description	String	No	mydbinfo	The description of the secret.
Tags	String	No	[{\"TagKey\":\"key1\",\"TagValue\":\"val1\"},{\"TagKey\":\"key2\",\"TagValue\":\"val2\"}]	The tags of the secret.
SecretType	String	No	Rds	The type of the secret. Valid values: • Generic: indicates a generic secret. • Rds: indicates a managed ApsaraDB RDS secret. • RAMCredentials: indicates a managed RAM secret. • ECS: indicates a managed ECS secret.

Parameter	Type	Required	Example	Description
ExtendedConfig	Json	No	null	The extended configuration of the secret. This parameter specifies the properties of the secret of the specific type. The description can be up to 1,024 characters in length. • If you set the SecretType parameter to Generic, you do not need to specify this parameter. • If you set the SecretType parameter to Rds, you must specify the following fields in the ExtendedConfig parameter: ◦ SecretSubType: required. The subtype of the secret. Valid values: ▪ SingleUser: Secrets Manager manages the ApsaraDB RDS secret in single-account mode. When the secret is rotated, the password of the specified account is reset to a new random password. ▪ DoubleUsers: Secrets Manager manages the ApsaraDB RDS secret in dual-account mode. One account is referenced by the ACSCurrent version, and the other account is referenced by the ACSPrevious version. When the secret is rotated, the password of the account referenced by the ACSPrevious version is reset to a new random password. Then, Secrets Manager switches the referenced accounts between the ACSCurrent and ACSPrevious versions. ◦ DBInstanceId: required. The ApsaraDB RDS instance to which the ApsaraDB RDS account belongs. ◦ CustomData: optional. The custom data. The value is a collection of key-value pairs in the JSON format. A maximum of 10 key-value pairs can be specified. Separate multiple key-value pairs with commas (,). Example: `{"Key1": "v1", "fds":"fdsf"}`. The default value is a pair of empty braces (`{}`). • If you set the SecretType parameter to RAMCredentials, you must specify the following fields in the ExtendedConfig parameter: ◦ SecretSubType: required. The subtype of the secret. Set the value to RamUserAccessKey. ◦ UserName: required. The name of the RAM user. ◦ CustomData: optional. The custom data. The value is a collection of key-value pairs in the JSON format. A maximum of 10 key-value pairs can be specified. Separate multiple key-value pairs with commas (,). The default value is a pair of empty braces (`{}`). • If you set the SecretType parameter to ECS, you must specify the following fields in the ExtendedConfig parameter: ◦ SecretSubType: required. The subtype of the secret. Valid values: ▪ Password: the password that is used to log on to the ECS instance. ▪ SSHKey: the SSH public and private keys that are used to log on to the ECS instance. ◦ RegionId: required. The ID of the region in which the ECS instance resides. ◦ InstanceId: required. The ID of the ECS instance. ◦ CustomData: optional. The custom data. The value is a collection of key-value pairs in the JSON format. A maximum of 10 key-value pairs can be specified. Separate multiple key-value pairs with commas (,). The default value is a pair of empty braces (`{}`). **Note** This parameter is required if you set the SecretType parameter to Rds, RAMCredentials, or ECS.
EnableAutomaticRotation	Boolean	No	true	Specifies whether to enable automatic rotation. Valid values: • true: indicates that automatic rotation is enabled. • false: indicates that automatic rotation is disabled. This is the default value. **Note** This parameter is valid if you set the SecretType parameter to Rds, RAMCredentials, or ECS.

Parameter	Type	Required	Example	Description
RotationInterval	String	No	30d	The interval for automatic rotation. Valid values: 6 hours to 8,760 hours (365 days). The value is in the `integer[unit]` format. The unit can be d (day), h (hour), m (minute), or s (second). For example, both 7d and 604800s indicate a seven-day interval. **Note** This parameter is required if you set the EnableAutomaticRotation parameter to true. This parameter is ignored if you set the EnableAutomaticRotation parameter to false or does not specify the EnableAutomaticRotation parameter.

For more information about common request parameters, see Common parameters.

Response parameters

Parameter	Type	Example	Description
Arn	String	acs:kms:cn-hangzhou:154035569884****:secret/mydbconninfo	The Alibaba Cloud Resource Name (ARN) of the secret.
AutomaticRotation	String	Enabled	Indicates whether automatic rotation is enabled. Valid values: • Enabled: indicates that automatic rotation is enabled. • Disabled: indicates that automatic rotation is disabled. • Invalid: indicates that the status of automatic rotation is abnormal. In this case, Secrets Manager cannot automatically rotate the secret. **Note** This parameter is returned if you set the SecretType parameter to Rds, RAMCredentials, or ECS.
ExtendedConfig	String	{\"SecretSubType\":\"SingleUser\", \"DBInstanceId\":\"rm-uf667446pc955****\", \"CustomData\":{} }	The extended configuration of the secret. **Note** This parameter is returned if you set the SecretType parameter to Rds, RAMCredentials, or ECS.
NextRotationDate	String	2020-07-06T18:22:03Z	The time when the next rotation will be performed. **Note** This parameter is returned if automatic rotation is enabled.
RequestId	String	3bf02f7a-015b-4f93-be0f-cc043fda2dd3	The ID of the request.
RotationInterval	String	604800s	The interval for automatic rotation. The value is in the `integer[unit]` format. The `unit` field has a fixed value of s. For example, if the value is 604800s, automatic rotation is performed at a 7-day interval. **Note** This parameter is returned if automatic rotation is enabled.
SecretName	String	mydbconninfo	The name of the secret.
SecretType	String	Rds	The type of the secret. Valid values: • Generic: indicates a generic secret. • Rds: indicates a managed ApsaraDB RDS secret. • RAMCredentials: indicates a managed RAM secret. • ECS: indicates a managed ECS secret.
VersionId	String	v1	The version number of the secret.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=CreateSecret
&SecretData={"user":"root","passwd":"****"}
&SecretName=mydbconninfo
&VersionId=v1
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
      <Arn>acs:kms:cn-hangzhou:154035569884****:secret/mydbconninfo</Arn>
      <SecretName>mydbconninfo</SecretName>
      <VersionId>v1</VersionId>
      <RequestId>3bf02f7a-015b-4f93-be0f-cc043fda2dd3</RequestId>
      <SecretType>Generic</SecretType>
 </KMS>
```

`JSON` format

```
{
    "Arn": "acs:kms:cn-hangzhou:154035569884****:secret/mydbconninfo",
    "SecretName": "mydbconninfo",
    "VersionId": "v1",
    "RequestId": "3bf02f7a-015b-4f93-be0f-cc043fda2dd3",
    "SecretType": "Generic"
}
```

Error codes

HttpCode	Error code	Error message	Description
400	InvalidParameter	The specified parameter is invalid.	The error message returned because the format of the specified parameter is invalid.
400	Rejected.LimitExceeded	The secret quota is exceeded.	The error message returned because the secret quota is used up.
403	Forbidden.NoPermission	You are not authorized to perform the operation.	The error message returned because you are not authorized to perform the operation.
404	Forbidden.ResourceNotFound	The resource is not found.	The error message returned because the specified resource does not exist.
409	Rejected.ResourceExist	The resource already exists.	The error message returned because the specified resource already exists.
409	Rejected.ResourceInDeleteWindow	The secret is planned to be deleted.	The error message returned because the secret is to be deleted.
500	InternalFailure	An internal error occurred.	The error message returned because an internal error occurred.
429	Rejected.Throttling	The QPS upper limit is exceeded.	The error message returned because the queries per second (QPS) has reached the upper limit.

For a list of error codes, visit the API Error Center.

9.2. ListSecrets

Queries all secrets created by your Alibaba Cloud account in the current region.

This operation returns the metadata information stored in secret objects and does not return encrypted secret values.

In this example, the secrets created by the current account in the current region are returned. The `PageNumber` parameter is set to `1`, and the `PageSize` parameter is set to `2`, which indicates that two secrets are to be returned.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ListSecrets	The operation that you want to perform. Set the value to ListSecrets.

Parameter	Type	Required	Example	Description
FetchTags	String	No	false	Specifies whether to return the resource tags of the secret. Valid values: • true: The resource tags are returned. • false: The resource tags are not returned. This is the default value.
PageNumber	Integer	No	1	The number of the page to return. Pages start from page 1. Default value: 1.
PageSize	Integer	No	2	The number of entries to return on each page. Valid values: 1 to 100 Default value: 10.
Filters	String	No	[{"Key":"SecretName", "Values":["$Val1","$Val2"]}]	The secret filter. Filters are key-values pairs. You can specify one key-values pair or leave this parameter empty. If you filter resources based on tag keys or values, up to 4,000 resources can be returned in the response. To query more than 4,000 resources, call the ListTagResources operation. • Key ◦ Description: the property that you want to filter. ◦ Type: string. ◦ Valid values: ▪ SecretName: the secret name. ▪ Description: the description of the secret. ▪ TagKey: the tag key. ▪ TagValue: the tag value. • Values ◦ Description: the value to be included after filtering. ◦ Type: string. ◦ Length: 0 to 10. ◦ Valid values: ▪ If the Key field is set to SecretName, the value must be 1 to 192 characters in length and can contain letters, digits, and special characters. The special characters include `underscores (_), forward slashes (/), plus signs (+), equal signs (=), periods (.), at signs (@), and hyphens (-)`. ▪ If the Key field is set to Description, the value must be 1 to 256 characters in length. ▪ If the Key field is set to TagKey, the value must be 1 to 256 characters in length and can contain letters, digits, and special characters. The special characters include `forward slashes (/), underscores (_), hyphens (-), periods (.), plus signs (+), equal signs (=), at signs (@), and colons (:)`. ▪ If the Key field is set to TagValue, the value must be 1 to 256 characters in length and can contain letters, numbers, and special characters. The special characters include `forward slashes (/), underscores (_), hyphens (-), periods (.), plus signs (+), equal signs (=), at signs (@), and colons (:)`. The logical relationship between values for a key in the Filters parameter is OR. Example: `[ {"Key":"SecretName", "Values":["sec1","sec2"]} ]`. In this example, the semantics are `SecretName=sec 1 OR SecretName=sec 2`

Response parameters

Parameter	Type	Example	Description
PageNumber	Integer	1	The page number of the returned page.
PageSize	Integer	2	The number of entries returned per page.
RequestId	String	6a6287a0-ff34-4780-a790-fdfca900557f	The ID of the request.
SecretList	Array of Secret		The list of secrets.

Parameter	Type	Example	Description
Secret			
CreateTime	String	2020-07-17T07:59:05Z	The time when the secret was created.
PlannedDeleteTime	String	2020-08-17T07:59:05Z	The time when the secret is scheduled to be deleted.
SecretName	String	secret001	The name of the secret.
SecretType	String	Generic	The type of the secret. Valid values: • Generic: indicates a standard secret. • Rds: indicates a managed ApsaraDB RDS secret.
Tags	Array of Tag		The resource tags of the secret. If the FetchTags parameter is set to false or is not specified, this parameter is not returned.
Tag			
TagKey	String	key1	The tag key.
TagValue	String	val1	The tag value.
UpdateTime	String	2020-07-17T07:59:05Z	The time when the secret was updated.
TotalCount	Integer	55	The number of returned secrets.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=ListSecrets
&PageNumber=1
&PageSize=2
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
   <SecretList>
      <Secret>
         <SecretName>secret001</SecretName>
         <SecretType>Generic</SecretType>
         <CreateTime>2020-07-17T07:59:05Z</CreateTime>
         <UpdateTime>2020-07-17T07:59:05Z</UpdateTime>
      </Secret>
      <Secret>
         <SecretName>cache_client</SecretName>
         <SecretType>Generic</SecretType>
         <CreateTime>2020-07-23T11:56:29Z</CreateTime>
         <UpdateTime>2021-01-12T02:15:42Z</UpdateTime>
      </Secret>
   </SecretList>
   <RequestId>6a6287a0-ff34-4780-a790-fdfca900557f</RequestId>
   <PageNumber>1</PageNumber>
   <PageSize>2</PageSize>
   <TotalCount>55</TotalCount>
</KMS>
```

`JSON` format

```
{
 "SecretList": {
  "Secret": [
   {
    "SecretName": "secret001",
    "SecretType": "Generic",
    "CreateTime": "2020-07-17T07:59:05Z",
    "UpdateTime": "2020-07-17T07:59:05Z"
   },
   {
    "SecretName": "cache_client",
    "SecretType": "Generic",
    "CreateTime": "2020-07-23T11:56:29Z",
    "UpdateTime": "2021-01-12T02:15:42Z"
   }
  ]
 },
 "RequestId": "6a6287a0-ff34-4780-a790-fdfca900557f",
 "PageNumber": 1,
 "PageSize": 2,
 "TotalCount": 55
}
```


Error codes

For a list of error codes, visit the API Error Center.

9.3. DeleteSecret

Deletes a secret.

If you call this operation without specifying a recovery period, the deleted secret can be recovered within 30 days.

If you specify a recovery period, the deleted secret can be recovered within the recovery period. You can also forcibly delete a secret. A forcibly deleted secret cannot be recovered.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DeleteSecret	The operation that you want to perform. Set the value to **DeleteSecret**.
SecretName	String	Yes	secret001	The name of the secret you want to delete.
ForceDeleteWithoutRecovery	String	No	false	Specifies whether to forcibly delete the secret. If this parameter is set to true, the secret cannot be recovered. Valid values: • **true** • **false** (default value)
RecoveryWindowInDays	String	No	10	Specifies the recovery period of the secret if you do not forcibly delete it. Default value: 30

Response parameters

Parameter	Type	Example	Description
PlannedDeleteTime	String	2020-02-21T23:36:07.713703651+08:00	The time when the secret is scheduled to be deleted.
RequestId	String	38bbed2a-15e0-45ad-98d4-816ad2ccf4ea	The ID of the request.
SecretName	String	secret001	The name of the secret.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DeleteSecret
&SecretName=secret001
&<Common request parameters>
```

Sample success responses

`XML` format

```
<SecretName>secret001</SecretName>
<RequestId>38bbed2a-15e0-45ad-98d4-816ad2ccf4ea</RequestId>
<PlannedDeleteTime>2020-02-21T23:36:07.713703651+08:00</PlannedDeleteTime>
```

`JSON` format

```
{
    "SecretName": "secret001",
    "RequestId": "38bbed2a-15e0-45ad-98d4-816ad2ccf4ea",
    "PlannedDeleteTime": "2020-02-21T23:36:07.713703651+08:00"
}
```

Error codes

For a list of error codes, visit the API Error Center.

9.4. DescribeSecret

Obtains the metadata of a secret.

This operation returns the metadata information about a secret. This operation does not return the encrypted secret value.

In this example, the metadata of the secret named `secret001` is queried.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeSecret	The operation that you want to perform. Set the value to DescribeSecret.
SecretName	String	Yes	secret001	The name of the secret.
FetchTags	String	No	true	Specifies whether to return the resource tags of the secret. Valid values: • true: The resource tags are returned. • false: The resource tags are not returned. This is the default value.

For more information about common request parameters, see Common parameters.

Response parameters

Parameter	Type	Example	Description
Arn	String	acs:kms:cn-hangzhou:154035569884****:secret/secret001	The Alibaba Cloud Resource Name (ARN) of the secret.
AutomaticRotation	String	Enabled	Indicates whether automatic rotation is enabled. Valid values: • Enabled: indicates that automatic rotation is enabled. • Disabled: indicates that automatic rotation is disabled. • Invalid: indicates that the status of automatic rotation is abnormal. In this case, Secrets Manager cannot automatically rotate the secret. **Note** This parameter is returned only for a managed ApsaraDB RDS secret, a managed RAM secret, or a managed ECS secret.
CreateTime	String	2020-02-21T15:39:26Z	The time when the secret was created.
Description	String	userinfo	The description of the secret.
EncryptionKeyId	String	00aa68af-2c02-4f68-95fe-3435d330****	The ID of the customer master key (CMK) that is used to encrypt the secret value.

Parameter	Type	Example	Description
ExtendedConfig	String	{\"SecretSubType\":\"SingleUser\", \"DBInstanceId\":\"rm-uf667446pc955****\", \"CustomData\":{} }	The extended configuration of the secret. **Note** This parameter is returned only for a managed ApsaraDB RDS secret, a managed RAM secret, or a managed ECS secret.
LastRotationDate	String	2020-07-05T08:22:03Z	The time when the last rotation was performed. **Note** This parameter is returned if the secret was rotated.
NextRotationDate	String	2020-07-06T18:22:03Z	The time when the next rotation will be performed. **Note** This parameter is returned if automatic rotation is enabled.
PlannedDeleteTime	String	2020-03-21T15:45:12Z	The time when the secret is scheduled to be deleted.
RequestId	String	93348dfb-3627-4417-8d90-487a76a909c9	The ID of the request.
RotationInterval	String	3153600s	The interval for automatic rotation. The value is in the `integer[unit]` format. The `unit` field has a fixed value of s. For example, if the value is 604800s, automatic rotation is performed at a 7-day interval. **Note** This parameter is returned if automatic rotation is enabled.
SecretName	String	secret001	The name of the secret.
SecretType	String	Rds	The type of the secret. Valid values: • Generic: indicates a generic secret. • Rds: indicates a managed ApsaraDB RDS secret. • RAMCredentials: indicates a managed RAM secret. • ECS: indicates a managed ECS secret.
Tags	Array of Tag		The resource tags of the secret. This parameter is not returned if you set the FetchTags parameter to false or does not specify the FetchTags parameter.
Tag			
TagKey	String	key1	The key of the tag.
TagValue	String	val1	The value of the tag.
UpdateTime	String	2020-02-21T15:39:26Z	The time when the secret was updated.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeSecret
&SecretName=secret001
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
      <Arn>acs:kms:cn-hangzhou:154035569884****:secret/secret001</Arn>
      <SecretName>secret001</SecretName>
      <Description>userinfo</Description>
      <CreateTime>2021-01-08T10:50:05Z</CreateTime>
      <UpdateTime>2021-01-08T10:50:05Z</UpdateTime>
      <RequestId>93f84812-66d2-467a-9aec-61f6f53919dc</RequestId>
      <SecretType>Rds</SecretType>
      <AutomaticRotation>Disabled</AutomaticRotation>
      <ExtendedConfig>{"SecretSubType":"SingleUser", "DBInstanceId":"rm-uf667446pc955****",  "CustomData":{} }</ExtendedConfig>
</KMS>
```

`JSON` format

```
{
    "Arn": "acs:kms:cn-hangzhou:154035569884****:secret/secret001",
    "SecretName": "secret001",
    "Description": "userinfo",
    "CreateTime": "2021-01-08T10:50:05Z",
    "UpdateTime": "2021-01-08T10:50:05Z",
    "RequestId": "93f84812-66d2-467a-9aec-61f6f53919dc",
    "SecretType": "Rds",
    "AutomaticRotation": "Disabled",
    "ExtendedConfig": "{\"SecretSubType\":\"SingleUser\", \"DBInstanceId\":\"rm-uf667446pc955****\",  \"CustomData\":{} }"
}
```

Error codes

For a list of error codes, visit the API Error Center.

9.5. GetSecretValue

Obtains a secret value.

If you do not specify a version number or stage label, Secrets Manager returns the secret value of the version marked with ACSCurrent.

If a customer master key (CMK) is specified to encrypt the secret value, you must also have the `kms:Decrypt` permission on the CMK to call the GetSecretValue operation.

In this example, the value of the secret named `secret001` is obtained. The secret value is returned in the `SecretData` parameter. The secret value is `testdata1`.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	GetSecretValue	The operation that you want to perform. Set the value to GetSecretValue.
SecretName	String	Yes	secret001	The name of the secret.
VersionStage	String	No	ACSCurrent	The stage label that marks the secret version. If you specify this parameter, Secrets Manager returns the secret value of the version that is marked with the specified stage label. Default value: ACSCurrent. **Note** For a managed ApsaraDB RDS secret, a managed RAM secret, or a managed ECS secret, Secrets Manager can return only the secret value of the version marked with ACSPrevious or ACSCurrent.
VersionId	String	No	00000000000000000000000000000001	The version number of the secret value. If you specify this parameter, Secrets Manager returns the secret value of the specified version. **Note** This parameter is ignored for a managed ApsaraDB RDS secret, a managed RAM secret, or a managed ECS secret.

Parameter	Type	Required	Example	Description
FetchExtendedConfig	Boolean	No	true	Specifies whether to obtain the extended configuration of the secret. Valid values: • true • false: This is the default value. **Note** This parameter is ignored for a generic secret.

For more information about common request parameters, see Common parameters.

Response parameters

Parameter	Type	Example	Description
AutomaticRotation	String	Enabled	Indicates whether automatic rotation is enabled. Valid values: • Enabled: indicates that automatic rotation is enabled. • Disabled: indicates that automatic rotation is disabled. • Invalid: indicates that the status of automatic rotation is abnormal. In this case, Secrets Manager cannot automatically rotate the secret. **Note** This parameter is returned only for a managed ApsaraDB RDS secret, a managed RAM secret, or a managed ECS secret.
CreateTime	String	2020-02-21T15:39:26Z	The time when the secret was created.
ExtendedConfig	String	{\"SecretSubType\":\"SingleUser\", \"DBInstanceId\":\"rm-uf667446pc955****\", \"CustomData\":{} }	The extended configuration of the secret. **Note** This parameter is returned if you set the FetchExtendedConfig parameter to true. This parameter is returned only for a managed ApsaraDB RDS secret, a managed RAM secret, or a managed ECS secret.
LastRotationDate	String	2020-07-05T08:22:03Z	The time when the last rotation was performed. **Note** This parameter is returned if the secret was rotated.
NextRotationDate	String	2020-07-06T18:22:03Z	The time when the next rotation will be performed. **Note** This parameter is returned if automatic rotation is enabled.
RequestId	String	6a3e9c36-1150-4881-84d3-eb8672fcafad	The ID of the request.
RotationInterval	String	604800s	The interval for automatic rotation. The value is in the `integer[unit]` format. The `unit` field has a fixed value of s. For example, if the value is 604800s, automatic rotation is performed at a 7-day interval. **Note** This parameter is returned if automatic rotation is enabled.

Parameter	Type	Example	Description
SecretData	String	testdata1	The secret value. Secrets Manager decrypts the ciphertext of the secret value and returns the plaintext of the secret value in this parameter. • For a generic secret, the secret value of the specified version is returned. • For a managed ApsaraDB RDS secret, the value is returned in the following format: `{"AccountName":"","AccountPassword":""}` . • For a managed RAM secret, the secret value is returned in the following format: `{"AccessKeyId":"Adfdsfd","AccessKeySecret":"fdsfdsf","GenerateTimestamp": "2016-03-25T10:42:40Z"}` . • For a managed ECS secret, the secret value is returned in one of the following formats: ◦ `{"UserName":"root","Password":"H5asdasdsads****"}` : The secret value is returned in this format if the ECS secret is a password. ◦ `{"UserName":"root","PublicKey":"ssh-rsa ****mKwnVix9YTFY9Rs= imported-openssh-key","PrivateKey": "d6bee1cb-2e14-4277-ba6b-73786b21****"}` : The secret value is returned in this format is the ECS secret is a pair of SSH keys. The private key is in the Privacy Enhanced Mail (PEM) format.
SecretDataType	String	binary	The type of the secret value. Valid values: • text • binary
SecretName	String	secret001	The name of the secret.
SecretType	String	Generic	The type of the secret. Valid values: • Generic: indicates a generic secret. • Rds: indicates a managed ApsaraDB RDS secret. • RAMCredentials: indicates a managed RAM secret. • ECS: indicates a managed ECS secret.
VersionId	String	00000000000000000000000000000001	The version number of the secret value.
VersionStages	List	{ "VersionStage": ["ACSCurrent"] }	The stage labels that mark the secret versions.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=GetSecretValue
&SecretName=secret001
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
      <SecretName>secret001</SecretName>
      <VersionId>00000000000000000000000000000001</VersionId>
      <SecretData>testdata1</SecretData>
      <SecretType>Generic</SecretType>
      <SecretDataType>binary</SecretDataType>
      <VersionStages>
            <VersionStage>ACSCurrent</VersionStage>
      </VersionStages>
      <CreateTime>2020-07-23T11:56:29Z</CreateTime>
      <RequestId>6a3e9c36-1150-4881-84d3-eb8672fcafad</RequestId>
</KMS>
```

`JSON` format

```
{
    "SecretName": "secret001",
    "VersionId": "00000000000000000000000000000001",
    "SecretData": "testdata1",
    "SecretType": "Generic",
    "SecretDataType": "binary",
    "VersionStages": {
        "VersionStage": [
            "ACSCurrent"
        ]
    },
    "CreateTime": "2020-07-23T11:56:29Z",
    "RequestId": "6a3e9c36-1150-4881-84d3-eb8672fcafad"
}
```


Error codes

For a list of error codes, visit the API Error Center.

9.6. PutSecretValue

Stores the secret value of a new version into a secret object.

This operation is used to store secret values of new versions. It cannot be used to modify the secret value of an existing version.

By default, the newly stored secret value is marked with ACSCurrent, and the original version marked with ACSCurrent is marked with ACSPrevious. If you specify the VersionStage parameter, the newly stored secret value is marked with the specified stage label.

You must specify a version number. Secrets Manager performs operations based on the following rules:

- If the specified version number does not exist in the secret object, Secrets Manager creates the new version and stores the secret value.
- If the specified version number already exists in the secret object and the secret value of the existing version is the same as the secret value that you specify, Secrets Manager ignores the request and returns a success message. The request is idempotent.
- If the specified version number already exists in the secret object but the secret value of the existing version is different from the secret value that you specify, Secrets Manager rejects the request and returns a failure message.

Limits: This operation is available only for standard secrets.

In this example, the secret value of a new version is stored into the `secret001` secret. The `VersionId` parameter is set to `00000000000000000000000000000203`, and the `SecretData` parameter is set to `importantdata`.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	PutSecretValue	The operation that you want to perform. Set the value to PutSecretValue.
SecretData	String	Yes	importantdata	The secret value. It is encrypted and then stored in a specified new version.
SecretName	String	Yes	secret001	The name of the secret.
VersionId	String	Yes	00000000000000000000000000000203	The version number of the secret value that you want to store. Version numbers are unique in each secret object.
SecretDataType	String	No	text	The type of the secret value. Valid values: • text: This is the default value. • binary
VersionStages	String	No	{"VersionStage": ["ACSCurrent"] }	The stage label that marks the new secret version. If you do not specify this parameter, Secrets Manager marks it with ACSCurrent.

For more information about common request parameters, see Common parameters.

Response parameters

Parameter	Type	Example	Description
RequestId	String	f94ec9d3-2d10-4922-9a5c-5dcd5ebcb5e8	The ID of the request.
SecretName	String	secret001	The name of the secret.

Parameter	Type	Example	Description
VersionId	String	00000000000000000000000000000000000203	The version number of the secret value.
VersionStages	List	{"VersionStage": ["ACSCurrent"]}	The stage labels that mark the version.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=PutSecretValue
&SecretData=importantdata
&SecretName=secret001
&VersionId=00000000000000000000000000000000000203
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
   <SecretName>secret001</SecretName>
   <VersionId>00000000000000000000000000000000000203</VersionId>
   <VersionStages>
      <VersionStage>ACSCurrent</VersionStage>
   </VersionStages>
   <RequestId>f94ec9d3-2d10-4922-9a5c-5dcd5ebcb5e8</RequestId>
</KMS>
```

`JSON` format

```
{
 "SecretName": "secret001",
 "VersionId": "00000000000000000000000000000000000203",
 "VersionStages": {
  "VersionStage": [
   "ACSCurrent"
  ]
 },
 "RequestId": "f94ec9d3-2d10-4922-9a5c-5dcd5ebcb5e8"
}
```

Error codes

For a list of error codes, visit the API Error Center.

9.7. UpdateSecret

Updates the metadata of a secret.

In this example, the metadata of the `secret001` secret is updated. The `Description` parameter is set to `datainfo`.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	UpdateSecret	The operation that you want to perform. Set the value to UpdateSecret.
SecretName	String	Yes	secret001	The name of the secret.
Description	String	No	datainfo	The description of the secret.
ExtendedConfig.CustomData	Json	No	{"DBName":"app1","Port":"3306"}	The custom data in the extended configuration of the secret. **Note** • If this parameter is specified, the existing extended configuration of the secret is updated. • This parameter is unavailable for standard secrets.

For more information about common request parameters, see Common parameters.

Response parameters

Parameter	Type	Example	Description
RequestId	String	5b75d8b1-5b6a-4ec0-8e0c-c08befdfad47	The ID of the request.
SecretName	String	secret001	The name of the secret.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=UpdateSecret
&Description=datainfo
&SecretName=secret001
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
   <SecretName>secret001</SecretName>
   <RequestId>5b75d8b1-5b6a-4ec0-8e0c-c08befdfad47</RequestId>
</KMS>
```

`JSON` format

```
{
    "SecretName":"secret001",
    "RequestId": "5b75d8b1-5b6a-4ec0-8e0c-c08befdfad47"
}
```

Error codes

For a list of error codes, visit the API Error Center.

9.8. UpdateSecretVersionStage

Updates the stage label that marks a secret version.

You can use this operation to achieve the following purposes:

- Use a specified stage label to mark a new secret version.
- Remove a specific stage label from an existing secret version.

Limits: This operation is available only for standard secrets.

In this example, the stage label that marks the version of the `secret001` secret is updated. The stage label `ACSCurrent` is used to mark the `002` version.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	UpdateSecretVersionStage	The operation that you want to perform. Set the value to UpdateSecretVersionStage.
SecretName	String	Yes	secret001	The name of the secret.
VersionStage	String	Yes	ACSCurrent	The specified stage label. Valid values: • ACSCurrent • ACSPrevious • Custom stage label
RemoveFromVersion	String	No	001	The version from which you want to remove the specified stage label. **Note** You must specify at least one of the RemoveFromVersion and MoveToVersion parameters.

Parameter	Type	Required	Example	Description
MoveToVersion	String	No	002	The version to which you want to apply the specified stage label. Note • You must specify at least one of the RemoveFromVersion and MoveToVersion parameters. • If the VersionStage parameter is set to ACSCurrent or ACSPrevious, this parameter is required.

Response parameters

Parameter	Type	Example	Description
RequestId	String	8cad259f-4d77-40ec-bbd7-b9c47a423bb9	The ID of the request.
SecretName	String	secret001	The name of the secret.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=UpdateSecretVersionStage
&SecretName=secret001
&VersionStage=ACSCurrent
&MoveToVersion=002
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
   <SecretName>secret001</SecretName>
   <RequestId>8cad259f-4d77-40ec-bbd7-b9c47a423bb9</RequestId>
</KMS>
```

`JSON` format

```
{
 "SecretName": "secret001",
 "RequestId": "8cad259f-4d77-40ec-bbd7-b9c47a423bb9"
}
```

Error codes

For a list of error codes, visit the API Error Center.

9.9. RestoreSecret

Restores a deleted secret.

You can only use this operation to restore a deleted secret that is within its recovery period. If you set **ForceDeleteWithoutRecovery** to **true** when you delete the secret, you cannot restore it.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	RestoreSecret	The operation that you want to perform. Set the value to **RestoreSecret**.
SecretName	String	Yes	secret001	The name of the secret you want to restore.

Response parameters

Parameter	Type	Example	Description
RequestId	String	e4885adf-548f-4ca5-8075-f540bbd3a55f	The ID of the request.

Parameter	Type	Example	Description
SecretName	String	secret001	The name of the secret.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=RestoreSecret
&SecretName=secret001
&<Common request parameters>
```

Sample success responses

`XML` format

```
<RequestId>e4885adf-548f-4ca5-8075-f540bbd3a55f</RequestId>
<SecretName>secret001</SecretName>
```

`JSON` format

```
{
    "RequestId": "e4885adf-548f-4ca5-8075-f540bbd3a55f",
    "SecretName": "secret001"
}
```

Error codes

For a list of error codes, visit the API Error Center.

9.10. ListSecretVersionIds

You can call this operation to query all versions of a secret.

The secret value is not included in the returned information. By default, deprecated secret versions are not returned.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ListSecretVersionIds	The operation that you want to perform. Set the value to **ListSecretVersionIds**.
SecretName	String	Yes	secret001	The name of the secret you want to delete.
IncludeDeprecated	String	No	false	Specifies whether to return deprecated secret versions. Valid values: true and false. Default value: **false**.
PageNumber	Integer	No	1	The page number of the returned page.
PageSize	Integer	No	10	The number of entries to return on each page.

Response parameters

Parameter	Type	Example	Description
PageNumber	Integer	1	The page number of the returned page.
PageSize	Integer	10	The number of entries returned per page.
RequestId	String	5b75d8b1-5b6a-4ec0-8e0c-c08befdfad47	The ID of the request.
SecretName	String	secret001	The name of the secret you want to delete.
TotalCount	Integer	4	The number of entries returned on the current page.
VersionIds	Array		The list of secret versions.

Parameter	Type	Example	Description
CreateTime	String	2020-02-21T15:39:26Z	The time when the secret version was created.
VersionId	String	00000000000000000000000000000000000203	The version of the secret.
VersionStages	List	{ "VersionStage": ["ACSCurrent", "UStage1", "Ustage2"] }	The stage labels that mark the secret version.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=ListSecretVersionIds
&<Common request parameters>
```

Sample success responses

`XML` format

```
<SecretName>secret001</SecretName>
<VersionIds>
    <VersionId>
        <VersionId>00000000000000000000000000000000203</VersionId>
        <VersionStages>
            <VersionStage>ACSCurrent</VersionStage>
            <VersionStage>UStage1</VersionStage>
            <VersionStage>Ustage2</VersionStage>
        </VersionStages>
    </VersionId>
    <VersionId>
        <VersionId>00000000000000000000000000000001</VersionId>
        <VersionStages>
            <VersionStage>ACSPrevious</VersionStage>
        </VersionStages>
    </VersionId>
</VersionIds>
<RequestId>5b75d8b1-5b6a-4ec0-8e0c-c08befdfad47</RequestId>
<PageNumber>1</PageNumber>
<PageSize>10</PageSize>
<TotalCount>4</TotalCount>
```

`JSON` format

```
{
    "SecretName": "secret001",
    "VersionIds": {
        "VersionId": [
            {
                "VersionId": "00000000000000000000000000000203",
                "VersionStages": {
                    "VersionStage": [
                        "ACSCurrent",
                        "UStage1",
                        "Ustage2"
                    ]
                }
            },
            {
                "VersionId": "00000000000000000000000000000001",
                "VersionStages": {
                    "VersionStage": [
                        "ACSPrevious"
                    ]
                }
            }
        ]
    },
    "RequestId": "5b75d8b1-5b6a-4ec0-8e0c-c08befdfad47",
    "PageNumber": 1,
    "PageSize": 10,
    "TotalCount": 4
}
```

Error code

For a list of error codes, visit the API Error Center.

9.11. GetRandomPassword

Obtains a random password string.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	GetRandomPassword	The operation that you want to perform. Set the value to GetRandomPassword.
PasswordLength	String	No	32	The number of bytes that the password to be generated contains. Valid values: 8 to 128. Default value: 32
ExcludeCharacters	String	No	ABCabc	The characters that are not included in the password to be generated. Valid values: `Valid characters: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ! \"#$%&'()*+,-. /:;<=>? @[\] your_project_id} ~ .` This parameter is empty by default.
ExcludeLowercase	String	No	false	Specifies whether to exclude lowercase letters. Valid values: • true • false
ExcludeUppercase	String	No	false	Specifies whether to exclude uppercase letters. Valid values: • true • false
ExcludeNumbers	String	No	false	Specifies whether to exclude digits. Valid values: • true • false
ExcludePunctuation	String	No	false	Specifies whether to exclude special characters. Valid values: • true • false
RequireEachIncludedType	String	No	true	Specifies whether to include all the preceding character types. Valid values: • true • false

Response parameters

Parameter	Type	Example	Description
RandomPassword	String	lxGn>NMmNB(y?iZ<Yc,_H/{2GC'U****	The generated random password.
RequestId	String	6b0cbe25-5e33-467e-972e-7a83c6c97604	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=GetRandomPassword
&<Common request parameters>
```

Sample success responses

`XML` format

```
<RequestId>6b0cbe25-5e33-467e-972e-7a83c6c97604</RequestId>
<RandomPassword>IxGn>NMmNB(y? iZ<Yc,_H/{2GC'U****</RandomPassword>
```

`JSON` format

```
{"RequestId":"6b0cbe25-5e33-467e-972e-7a83c6c97604","RandomPassword":"IxGn>NMmNB(y? iZ<Yc,_H/{2GC'U****"}
```

Error code

For a list of error codes, visit the API Error Center.

9.12. RotateSecret

Manually rotates a secret.

Limits:

• A secret of each Alibaba Cloud account can be rotated for a maximum of 50 times per hour.

• The RotateSecret operation is unavailable for standard secrets.

In this example, the `RdsSecret/Mysql5.4/MyCred` secret is manually rotated, and the version number of the secret is set to `000000123` after the secret is rotated.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	RotateSecret	The operation that you want to perform. Set the value to RotateSecret.
SecretName	String	Yes	RdsSecret/Mysql5.4/MyCred	The name of the secret.
VersionId	String	Yes	000000123	The version number of the secret after the secret is rotated. **Note** The version number is used to ensure the idempotence of the request. Secrets Manager uses this version number to prevent your application from creating the same version of the secret when the application retries a request. If a version number already exists, Secrets Manager ignores the request for rotation and returns a success message.

Response parameters

Parameter	Type	Example	Description
Arn	String	acs:kms:cn-hangzhou:154035569884****:secret/RdsSecret/Mysql5.4/MyCred	The Alibaba Cloud Resource Name (ARN) of the secret.
SecretName	String	RdsSecret/Mysql5.4/MyCred	The name of the secret.
VersionId	String	000000123	The version number of the secret after the secret is rotated.
RequestId	String	10257c86-269d-43aa-aaf3-90ed4144bb7c	The ID of the request.

For more information about common request parameters, see Common parameters.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=RotateSecret
&SecretName=RdsSecret/Mysql5.4/MyCred
&VersionId=000000123
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
   <Arn>acs:kms:cn-hangzhou:154035569884****:secret/RdsSecret/Mysql5.4/MyCred</Arn>
   <SecretName>RdsSecret/Mysql5.4/MyCred</SecretName>
   <VersionId>000000123</VersionId>
   <RequestId>10257c86-269d-43aa-aaf3-90ed4144bb7c</RequestId>
</KMS>
```

`JSON` format

```
{
 "Arn": "acs:kms:cn-hangzhou:154035569884****:secret/RdsSecret/Mysql5.4/MyCred",
 "SecretName": "RdsSecret/Mysql5.4/MyCred",
 "VersionId": "000000123",
 "RequestId": "10257c86-269d-43aa-aaf3-90ed4144bb7c"
}
```

Error codes

For a list of error codes, visit the API Error Center.

9.13. UpdateSecretRotationPolicy

Updates the rotation policy of a secret.

After automatic rotation is enabled, Secrets Manager schedules the first automatic rotation by adding the preset rotation interval to the timestamp of the last rotation.

Limits: The UpdateSecretRotationPolicy operation cannot be used to update the rotation policy of standard secrets.

In this example, the rotation policy of the `RdsSecret/Mysql5.4/MyCred` secret is updated in the following way:

- The `EnableAutomaticRotation` parameter is set to `true`, which indicates that automatic rotation is enabled.
- The `RotationInterval` parameter is set to `30d`, which indicates that the interval for automatic rotation is 30 days.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	UpdateSecretRotationPolicy	The operation that you want to perform. Set the value to UpdateSecretRotationPolicy.
EnableAutomaticRotation	Boolean	Yes	true	Specifies whether to enable automatic rotation. Valid values: • true: indicates that automatic rotation is enabled. • false: indicates that automatic rotation is disabled. This is the default value.
SecretName	String	Yes	RdsSecret/Mysql5.4/MyCred	The name of the secret.
RotationInterval	String	No	30d	The interval for automatic rotation. Valid values: 6 hours to 8,760 hours (365 days). Specify the interval in the `integer[unit]` format, where `integer` indicates the interval and `unit` indicates the time unit. The unit can be d (day), h (hour), m (minute), or s (second). For example, both 7d and 604800s indicate a seven-day interval. **Note** If the EnableAutomaticRotation parameter is set to true, this parameter is required. Otherwise, you do not need to specify this parameter.

For more information about common request parameters, see Common parameters.

Response parameters

Parameter	Type	Example	Description
SecretName	String	RdsSecret/Mysql5.4/MyCred	The name of the secret.
RequestId	String	2c124f6f-4210-499f-b88a-69f54004d2d8	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=UpdateSecretRotationPolicy
&EnableAutomaticRotation=true
&SecretName=RdsSecret/Mysql5.4/MyCred
&RotationInterval=30d
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
   <SecretName>RdsSecret/Mysql5.4/MyCred</SecretName>
   <RequestId>2c124f6f-4210-499f-b88a-69f54004d2d8</RequestId>
</KMS>
```

`JSON` format

```
{
    "SecretName": "RdsSecret/Mysql5.4/MyCred",
    "RequestId": "2c124f6f-4210-499f-b88a-69f54004d2d8"
}
```

Error codes

For a list of error codes, visit the API Error Center.

10.Certificate

10.1. CreateCertificate

Creates a certificate.

To create a certificate, you must specify the type of the asymmetric key. Certificates Manager generates a private key and returns a certificate signing request (CSR). Submit the CSR in the Privacy Enhanced Mail (PEM) format to a certificate authority (CA) to obtain the formal certificate and certificate chain. Then, call the UploadCertificate operation to import the certificate into Certificates Manager.

In this example, a certificate is created and the CSR is obtained.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	CreateCertificate	The operation that you want to perform. Set the value to CreateCertificate.
KeySpec	String	Yes	RSA_2048	The type of the key. Valid values: • RSA_2048 • EC_P256 • EC_SM2
Subject	String	Yes	CN=userName,OU=kms,O=aliyun,C=CN	The certificate subject, which is the owner of the certificate. Specify the value in the distinguished name (DN) format, as defined in RFC 2253. A DN is a sequence of relative distinguished names (RDNs). RDNs are key-value pairs in the format of `attribute1=value1,attribute2=value2`. Separate multiple RDNs with commas (,). The Subject parameter consists of the following fields: • CN: required. The name of the certificate subject. • C: required. The two-character country or region code in the ISO 3166-1 standard. For example, CN indicates China. • O: required. The legal name of the enterprise, company, organization, or institution. • OU: required. The name of the department. • ST: optional. The name of the province, municipality, autonomous region, or special administrative region. • L: optional. The name of the city.
SubjectAlternativeNames	Json	No	["test1.example.com","test2.example.com"]	The subject alternative names. A domain name list is supported. A maximum of 10 domain names are supported.
ExportablePrivateKey	Boolean	No	true	Specifies whether the private key of the certificate can be exported for use. Valid values: • true: The private key of the certificate can be exported for use. This is the default value. • false: The private key of the certificate cannot be exported for use. We recommend that you set this parameter to false to protect keys with a higher security level.

For more information about common request parameters, see Common parameters.

Response parameters

Parameter	Type	Example	Description
Arn	String	acs:kms:cn-hangzhou:154035569884****:certificate/98e85c94-52d0-40c9-b3b2-afda52f4****	The Alibaba Cloud Resource Name (ARN) of the certificate.
CertificateId	String	9a28de48-8d8b-484d-a766-dec4****	The ID of the certificate. It is the globally unique identifier (GUID) of the certificate in Certificates Manager.

Parameter	Type	Example	Description
Csr	String	-----BEGIN CERTIFICATE REQUEST----- \nMIIDADCCAegCAQAwgboxCzAJBgNVBAYTAkNOMREwDwYDVQQIEwhaaGVqaWFuZzER\n****\nmkj4rg==\n-----END CERTIFICATE REQUEST-----\n	The CSR in the PEM format.
RequestId	String	15a735a1-8fe6-45cc-a64c-3c4ff839334e	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=CreateCertificate
&KeySpec=RSA_2048
&Subject=CN=userName,OU=kms,O=aliyun,C=CN
&<Common request parameters>
```

Sample success responses

`JSON` format

```
{
 "CertificateId": "98e85c94-52d0-40c9-b3b2-afda52f4****",
 "Arn": "acs:kms:cn-hangzhou:154035569884****:certificate/98e85c94-52d0-40c9-b3b2-afda52f4****",
 "Csr": "-----BEGIN CERTIFICATE REQUEST-----\nMIIDADCCAegCAQAwgboxCzAJBgNVBAYTAkNOMREwDwYDVQQIEwhaaGVqaWFuZzER\n****\nmkj4rg==\n-----END CERTIFICATE REQUEST-----\n",
 "RequestId": "15a735a1-8fe6-45cc-a64c-3c4ff839334e"
}
```

Error codes

HTTP status code	Error code	Error message	Description
404	InvalidAccessKeyId.NotFound	The specified AccessKey ID does not exist.	The error message returned because the specified AccessKey ID does not exist. Check whether a valid AccessKey ID is specified when you call the operation.

For a list of error codes, visit the API Error Center.

10.2. UploadCertificate

Imports a certificate and certificate chain issued by a certificate authority (CA) into Certificates Manager.

In this example, a certificate issued by a CA is imported into Certificates Manager. The ID of the certificate in Certificates Manager is `12345678-1234-1234-1234-12345678****`.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	UploadCertificate	The operation that you want to perform. Set the value to UploadCertificate.
Certificate	String	Yes	-----BEGIN CERTIFICATE----- (X.509 Certificate PEM Content) -----END CERTIFICATE-----	The certificate issued by the CA, which is in the Privacy Enhanced Mail (PEM) format.
CertificateId	String	Yes	12345678-1234-1234-1234-12345678****	The ID of the certificate. It is the globally unique identifier (GUID) of the certificate in Certificates Manager.
CertificateChain	String	No	-----BEGIN CERTIFICATE----- (Sub CA Certificate PEM Content) -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- (Sub CA Certificate PEM Content) -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- (Root CA Certificate PEM Content) -----END CERTIFICATE-----	The certificate chain issued by the CA, which is in the PEM format.

For more information about common request parameters, see Common parameters.

Response parameters

Parameter	Type	Example	Description
RequestId	String	15a735a1-8fe6-45cc-a64c-3c4ff839334e	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=UploadCertificate
&Certificate=-----BEGIN CERTIFICATE-----  (X.509 Certificate PEM Content)  -----END CERTIFICATE-----
&CertificateId=12345678-1234-1234-1234-12345678****
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
        <RequestId>15a735a1-8fe6-45cc-a64c-3c4ff839334e</RequestId>
</KMS>
```

`JSON` format

```
{
    "RequestId": "15a735a1-8fe6-45cc-a64c-3c4ff839334e"
}
```

Error codes

HttpCode	Error code	Error message	Description
404	InvalidAccessKeyId.NotFound	The specified AccessKey ID does not exist.	The error message returned because the specified AccessKey ID does not exist. Check whether a valid AccessKey ID is specified when you call the operation.

For a list of error codes, visit the API Error Center.

10.3. GetCertificate

Queries a certificate that is managed by Certificates Manager.

In this example, the certificate whose ID is `9a28de48-8d8b-484d-a766-dec4****` is queried. The certificate, certificate chain, certificate ID, and certificate signing request (CSR) are returned.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	GetCertificate	The operation that you want to perform. Set the value to GetCertificate.
CertificateId	String	Yes	9a28de48-8d8b-484d-a766-dec4****	The ID of the certificate. It is the globally unique identifier (GUID) of the certificate in Certificates Manager.

For more information about common request parameters, see Common parameters.

Response parameters

Parameter	Type	Example	Description
Certificate	String	-----BEGIN CERTIFICATE----- (X.509 Certificate PEM Content) -----END CERTIFICATE-----	The certificate in the Privacy Enhanced Mail (PEM) format.
CertificateChain	String	-----BEGIN CERTIFICATE----- (Sub CA Certificate PEM Content) -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- (Sub CA Certificate PEM Content) -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- (Root CA Certificate PEM Content) -----END CERTIFICATE-----	The certificate chain in the PEM format.

Parameter	Type	Example	Description
CertificateId	String	9a28de48-8d8b-484d-a766-dec4****	The ID of the certificate.
Csr	String	-----BEGIN CERTIFICATE REQUEST----- MIICxjCCAa4CAQAwPzELMAkGA1UEBhMCQ04xDzANBgNVBAoTBmFsaXl1bjEMMAoGA1UECxMDa21zMREwDwY****-----END CERTIFICATE REQUEST-----	The CSR in the PEM format.
RequestId	String	b3e104b4-0319-4a20-ab7f-9fef6****	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=GetCertificate
&CertificateId=9a28de48-8d8b-484d-a766-dec4****
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
   <Csr>-----BEGIN CERTIFICATE REQUEST-----MIICxjCCAa4CAQAwPzELMAkGA1UEBhMCQ04xDzANBgNVBAoTBmFsaXl1bjEMMAoGA1UECxMDa21zMREwDwY****-----END CERTIFICATE REQUEST-----</Csr>
   <RequestId>b3e104b4-0319-4a20-ab7f-9fef6****</RequestId>
   <CertificateId>9a28de48-8d8b-484d-a766-dec4****</CertificateId>
   <CertificateChain>-----BEGIN CERTIFICATE-----  (Sub CA Certificate PEM Content)  -----END CERTIFICATE-----  -----BEGIN CERTIFICATE-----  (Sub CA Certificate PEM Content)  -----END CERTIFICATE-----  -----BEGIN CERTIFICATE-----  (Root CA Certificate PEM Content)  -----END CERTIFICATE-----</CertificateChain>
   <Certificate>-----BEGIN CERTIFICATE-----  (X.509 Certificate PEM Content)  -----END CERTIFICATE-----</Certificate>
</KMS>
```

`JSON` format

```
{
 "Csr": "-----BEGIN CERTIFICATE REQUEST-----MIICxjCCAa4CAQAwPzELMAkGA1UEBhMCQ04xDzANBgNVBAoTBmFsaXl1bjEMMAoGA1UECxMDa21zMREwDwY****-----END CERTIFICATE REQUEST-----",
 "RequestId": "b3e104b4-0319-4a20-ab7f-9fef6****",
 "CertificateId": "9a28de48-8d8b-484d-a766-dec4****",
 "CertificateChain": "-----BEGIN CERTIFICATE-----  (Sub CA Certificate PEM Content)  -----END CERTIFICATE-----  -----BEGIN CERTIFICATE-----  (Sub CA Certificate PEM Content)  -----END CERTIFICATE-----  -----BEGIN CERTIFICATE-----  (Root CA Certificate PEM Content)  -----END CERTIFICATE-----",
 "Certificate": "-----BEGIN CERTIFICATE-----  (X.509 Certificate PEM Content)  -----END CERTIFICATE-----"
}
```

Error codes

HttpCode	Error code	Error message	Description
404	InvalidAccessKeyId.NotFound	The specified AccessKey ID does not exist.	The error message returned because the specified AccessKey ID does not exist. Check whether a valid AccessKey ID is specified when you call the operation.

For a list of error codes, visit the API Error Center.

10.4. DescribeCertificate

Queries information about a certificate.

In this example, the information about the certificate whose ID is `9a28de48-8d8b-484d-a766-dec4****` is queried. The certificate information includes the certificate ID, creation time, certificate issuer, validity period, serial number, and signature algorithm.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeCertificate	The operation that you want to perform. Set the value to DescribeCertificate.
CertificateId	String	Yes	9a28de48-8d8b-484d-a766-dec4****	The ID of the certificate. The ID must be globally unique in Certificates Manager.

For more information about common request parameters, see Common parameters.

Response parameters

Parameter	Type	Example	Description
Arn	String	acs:kms:cn-hangzhou:159498693826****:certificate/9a28de48-8d8b-484d-a766-dec4****	The Alibaba Cloud Resource Name (ARN) of the certificate.
CertificateId	String	9a28de48-8d8b-484d-a766-dec4****	The ID of the certificate. The ID must be globally unique in Certificates Manager.
CreatedAt	String	2020-10-13T03:05:03Z	The time when the certificate was created.
ExportablePrivateKey	Boolean	true	Indicates whether the private key of the certificate can be exported for use. Valid values: • true: The private key of the certificate can be exported for use. This is the default value. • false: The private key of the certificate cannot be exported for use.
Issuer	String	CN=testCA,OU=kms,O=aliyun,C=CN	The certificate issuer in the distinguished name (DN) format.
KeySpec	String	RSA_2048	The type of the key.
NotAfter	String	2022-10-13T03:09:00Z	The end of the validity period of the certificate.
NotBefore	String	2020-10-13T03:09:00Z	The beginning of the validity period of the certificate.
RequestId	String	edb671a3-c5a1-4ebe-a1de-d748b640bdf2	The ID of the request.
Serial	String	12345678	The serial number of the certificate.
SignatureAlgorithm	String	ECDSA-SHA256	The signature algorithm of the certificate. Valid values: • RSA2048-SHA256 • ECDSA-SHA256 • SM2-SM3
Status	String	ACTIVE	The status of the certificate. Valid values: • PENDING: The certificate is to be imported. • ACTIVE: The certificate is enabled. • INACTIVE: The certificate is disabled. • REVOKED: The certificate is revoked.
Subject	String	CN=userName,OU=aliyun,O=aliyun,C=CN	The subject of the certificate, which is in the DN format.
SubjectAlternativeNames	List	["test1.example.com","test2.example.com"]	The alias of the certificate subject. A domain name list is supported. A maximum of 10 domain names are supported.
SubjectKeyIdentifier	String	79 36 26 DE 9F F5 15 E3 56 DC ****	The public key identifier of the certificate subject.
SubjectPublicKey	String	-----BEGIN PUBLIC KEY----- MIIBIjA ----END PUBLIC KEY-----	The public key of the certificate.
Tags	Map	[{\"TagKey\":\"S1key1\",\"TagValue\":\"S1val1\"},{\"TagKey\":\"S1key2\",\"TagValue\":\"S2val2\"}]	The tag of the certificate.
UpdatedAt	String	2020-12-23T06:10:13Z	The time when the certificate was updated.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeCertificate
&CertificateId=9a28de48-8d8b-484d-a766-dec4****
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
      <Status>ACTIVE</Status>
      <RequestId>edb671a3-c5a1-4ebe-a1de-d748b640bdf2</RequestId>
      <Issuer>CN=testCA,OU=kms,O=aliyun,C=CN</Issuer>
      <CertificateId>9a28de48-8d8b-484d-a766-dec4****</CertificateId>
      <CreatedAt>2020-10-13T03:05:03Z</CreatedAt>
      <KeySpec>RSA_2048</KeySpec>
      <SubjectAlternativeNames>[\"test1.example.com\",\"test2.example.com\"]</SubjectAlternativeNames>
      <SignatureAlgorithm>ECDSA-SHA256</SignatureAlgorithm>
      <SubjectKeyIdentifier>79 36 26 DE 9F F5 15 E3 56 DC ********</SubjectKeyIdentifier>
      <NotAfter>2022-10-13T03:09:00Z</NotAfter>
      <ExportablePrivateKey>true</ExportablePrivateKey>
      <UpdatedAt>2020-10-13T03:15:00Z</UpdatedAt>
      <Subject>CN=userName,OU=aliyun,O=aliyun,C=CN</Subject>
      <Serial>12345678</Serial>
      <SubjectPublicKey>-----BEGIN PUBLIC KEY----- MIIBIjA -----END PUBLIC KEY-----</SubjectPublicKey>
      <NotBefore>2020-10-13T03:09:00Z</NotBefore>
      <Arn>acs:kms:cn-hangzhou:159498693826****:certificate/9a28de48-8d8b-484d-a766-dec4****</Arn>
      <Tags>[{\"TagKey\":\"S1key1\",\"TagValue\":\"S1val1\"},{\"TagKey\":\"S1key2\",\"TagValue\":\"S2val2\"}]</Tags>
</KMS>
```

`JSON` format

```
{
    "Status": "ACTIVE",
    "RequestId": "edb671a3-c5a1-4ebe-a1de-d748b640bdf2",
    "Issuer": "CN=testCA,OU=kms,O=aliyun,C=CN",
    "CertificateId": "9a28de48-8d8b-484d-a766-dec4****",
    "CreatedAt": "2020-10-13T03:05:03Z",
    "KeySpec": "RSA_2048",
    "SubjectAlternativeNames": "[\"test1.example.com\",\"test2.example.com\"]",
    "SignatureAlgorithm": "ECDSA-SHA256",
    "SubjectKeyIdentifier": "79 36 26 DE 9F F5 15 E3 56 DC ********",
    "NotAfter": "2022-10-13T03:09:00Z",
    "ExportablePrivateKey": "true",
    "UpdatedAt": "2020-10-13T03:15:00Z",
    "Subject": "CN=userName,OU=aliyun,O=aliyun,C=CN",
    "Serial": "12345678",
    "SubjectPublicKey": "-----BEGIN PUBLIC KEY----- MIIBIjA -----END PUBLIC KEY-----",
    "NotBefore": "2020-10-13T03:09:00Z",
    "Arn": "acs:kms:cn-hangzhou:159498693826****:certificate/9a28de48-8d8b-484d-a766-dec4****",
    "Tags": "[{\"TagKey\":\"S1key1\",\"TagValue\":\"S1val1\"},{\"TagKey\":\"S1key2\",\"TagValue\":\"S2val2\"}]"
}
```

Error codes

HttpCode	Error code	Error message	Description
404	Certificate.NotFound	The specified certificate is not found.	The error message returned because the specified certificate does not exist.

For a list of error codes, visit the API Error Center.

10.5. UpdateCertificateStatus

Updates the status of a certificate.

In this example, the status of the certificate whose ID is `9a28de48-8d8b-484d-a766-dec4****` is updated to INACTIVE.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	UpdateCertificateStatus	The operation that you want to perform. Set the value to UpdateCertificateStatus.
CertificateId	String	Yes	9a28de48-8d8b-484d-a766-dec4****	The ID of the certificate. The ID must be globally unique in Certificates Manager.

Parameter	Type	Required	Example	Description
Status	String	Yes	INACTIVE	The status of the certificate. Valid values: • INACTIVE: The certificate is disabled. • ACTIVE: The certificate is enabled. • REVOKED: The certificate is revoked. **Note** If the certificate is in the REOVKED state, you can use the certificate only to verify a signature, but not to generate a signature.

For more information about common request parameters, see Common parameters.

Response parameters

Parameter	Type	Example	Description
RequestId	String	e3f57fe0-9ded-40b0-9caf-a3815f2148c1	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=UpdateCertificateStatus
&CertificateId=9a28de48-8d8b-484d-a766-dec4****
&Status=INACTIVE
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
   <RequestId>e3f57fe0-9ded-40b0-9caf-a3815f2148c1</RequestId>
 </KMS>
```

`JSON` format

```
{
 "RequestId": "e3f57fe0-9ded-40b0-9caf-a3815f2148c1"
}
```

Error codes

HttpCode	Error code	Error message	Description
404	Certificate.NotFound	The specified certificate is not found.	The error message returned because the specified certificate does not exist.

For a list of error codes, visit the API Error Center.

10.6. DeleteCertificate

Deletes a certificate and its private key and certificate chain.

After the certificate and its private key and certificate chain are deleted, they cannot be restored. Proceed with caution.

In this example, the certificate whose ID is `9a28de48-8d8b-484d-a766-dec4****` and its private key and certificate chain are deleted.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DeleteCertificate	The operation that you want to perform. Set the value to DeleteCertificate.
CertificateId	String	Yes	9a28de48-8d8b-484d-a766-dec4****	The ID of the certificate. It is the globally unique identifier (GUID) of the certificate in Alibaba Cloud Certificate Manager.

For more information about common request parameters, see Common parameters.

Response parameters

Parameter	Type	Example	Description
RequestId	String	d97f6c33-ca26-4de2-a580-0e2fd1c5bfb0	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=DeleteCertificate
&CertificateId=9a28de48-8d8b-484d-a766-dec4****
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
   <RequestId>d97f6c33-ca26-4de2-a580-0e2fd1c5bfb0</RequestId>
</KMS>
```

`JSON` format

```
{
 "RequestId": "d97f6c33-ca26-4de2-a580-0e2fd1c5bfb0"
}
```

Error codes

HttpCode	Error code	Error message	Description
404	Certificate.NotFound	The specified certificate is not found.	The error message returned because the specified certificate does not exist.

For a list of error codes, visit the API Error Center.

10.7. CertificatePrivateKeySign

Generates a digital signature by using a specified certificate.

The signature algorithm in the request parameters must match the key type. The following table describes the mapping between signature algorithms and key types.

Algorithm	Key type
RSA_PKCS1_SHA_256	RSA_2048
RSA_PSS_SHA_256	RSA_2048
ECDSA_SHA_256	EC_P256
SM2DSA	EC_SM2

In this example, the certificate whose ID is `12345678-1234-1234-1234-12345678****` and the signature algorithm `ECDSA_SHA_256` are used to generate a digital signature for the raw data `VGhlIHF1aWNrIGJyb3duIGZveCBqdW1wcyBvdmVyIHRoZSBsYXp5IGRvZy4=`.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	CertificatePrivateKeySign	The operation that you want to perform. Set the value to CertificatePrivateKeySign.

Parameter	Type	Required	Example	Description
Algorithm	String	Yes	ECDSA_SHA_256	The signature algorithm. Valid values: • RSA_PKCS1_SHA_256 • RSA_PSS_SHA_256 • ECDSA_SHA_256 • SM2DSA **Note** The SM2DSA signature algorithm is supported only in regions where managed hardware security modules (HSMs) are used in mainland China. For more information, see Managed HSM overview.
CertificateId	String	Yes	12345678-1234-1234-1234-12345678****	The ID of the certificate. It is the globally unique identifier (GUID) of the certificate in Certificates Manager.
Message	String	Yes	VGhlIHF1aWNrIGJyb3duIGZveCBqdW1wcyBvdmVyIHRoZSBsYXp5IGRvZy4=	The data to be signed. The value must be encoded in Base64. For example, if the data to be signed in the hexadecimal format is `[0x31, 0x32, 0x33, 0x34]`, set this parameter to the Base64-encoded value `MTIzNA==`. If the MessageType parameter is set to RAW, the size of the data must be less than or equal to 4 KB. If the size of the data is greater than 4 KB, you can set the MessageType parameter to DIGEST and set the Message parameter to the digest of the data. The digest is also called hash value. You can compute the digest of the data on an on-premises machine. Certificates Manager uses the digest that you compute in your own certificate application system. The message digest algorithm that you use must match the specified signature algorithm. Comply with the following mapping between signature algorithms and message digest algorithms: • If the signature algorithm is RSA_PKCS1_SHA_256, RSA_PSS_SHA_256, or ECDSA_SHA_256, the message digest algorithm must be SHA-256. • If the signature algorithm is SM2DSA, the message digest algorithm must be SM3. **Note** If the key type of the certificate is EC_SM2 and the MessageType parameter is set to DIGEST, the value of the Message parameter is `e` that is described in GB/T 32918.2-2016 6.1.
MessageType	String	Yes	RAW	The type of the message. Valid values: • RAW: the raw data. This is the default value. • DIGEST: the message digest (hash value) of the raw data.

For more information about common request parameters, see Common parameters.

Response parameters

Parameter	Type	Example	Description
CertificateId	String	12345678-1234-1234-1234-12345678****	The ID of the certificate.
RequestId	String	5979d897-d69f-4fc9-87dd-f3bb73c40b80	The ID of the request.
SignatureValue	String	ZOylygCyaOW6Gj****MlNKiuyjfzw=	The signature value. The value is encoded in Base64.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=CertificatePrivateKeySign
&Algorithm=ECDSA_SHA_256
&CertificateId=12345678-1234-1234-1234-12345678****
&Message=VGhlIHF1aWNrIGJyb3duIGZveCBqdW1wcyBvdmVyIHRoZSBsYXp5IGRvZy4=
&MessageType=RAW
&<Common request parameters>|
```

Sample success responses

`XML` format

```
<KMS>
      <CertificateId>12345678-1234-1234-1234-123456789012</CertificateId>
      <SignatureValue>ZOyIygCyaOW6Gj****MlNKiuyjfzw=</SignatureValue>
      <RequestId>5979d897-d69f-4fc9-87dd-f3bb73c40b80</RequestId>
</KMS>
```

`JSON` format

```
{
  "CertificateId": "12345678-1234-1234-1234-123456789012",
  "SignatureValue": "ZOyIygCyaOW6Gj****MlNKiuyjfzw=",
  "RequestId": "5979d897-d69f-4fc9-87dd-f3bb73c40b80"
}
```

Error codes

HTTP status code	Error code	Error message	Description
404	Certificate.NotFound	The specified certificate is not found.	The error message returned because the specified certificate does not exist.

For a list of error codes, visit the API Error Center.

10.8. CertificatePublicKeyVerify

Verifies a digital signature by using a specified certificate.

The signature algorithm in the request parameters must match the key type. The following table describes the mapping between signature algorithms and key types.

Algorithm	Key type
RSA_PKCS1_SHA_256	RSA_2048
RSA_PSS_SHA_256	RSA_2048
ECDSA_SHA_256	EC_P256
SM2DSA	EC_SM2

In this example, the certificate whose ID is `12345678-1234-1234-1234-12345678****` and the signature algorithm `ECDSA_SHA_256` are used to verify the digital signature `ZOyIygCyaOW6Gj****MlNKiuyjfzw=` of the raw data `VGhlIHF1aWNrIGJyb3duIGZveCBqdW1wcyBvdmVyIHRoZSBsYXp5IGRvZy4=`.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	CertificatePublicKeyVerify	The operation that you want to perform. Set the value to CertificatePublicKeyVerify.
Algorithm	String	Yes	ECDSA_SHA_256	The signature algorithm. Valid values: • RSA_PKCS1_SHA_256 • RSA_PSS_SHA_256 • ECDSA_SHA_256 • SM2DSA **Note** The SM2DSA signature algorithm is supported only in regions where managed hardware security modules (HSMs) are used in mainland China. For more information, see Managed HSM overview.
CertificateId	String	Yes	12345678-1234-1234-1234-12345678****	The ID of the certificate. It is the globally unique identifier (GUID) of the certificate in Certificates Manager.

Parameter	Type	Required	Example	Description
Message	String	Yes	VGhlIHF1aWNrIGJyb3duIGZveCBqdW1wcyBvdmVyIHRoZSBsYXp5IGRvZy4=	The raw data that is signed. The value must be encoded in Base64. For example, if the raw data in the hexadecimal format is `[0x31, 0x32, 0x33, 0x34]`, set this parameter to the Base64-encoded value `MTIzNA==`. If the MessageType parameter is set to RAW, the size of the data must be less than or equal to 4 KB. If the size of the data is greater than 4 KB, you can set the MessageType parameter to DIGEST and set the Message parameter to the digest of the data. The digest is also called hash value. You can compute the digest of the data on an on-premises machine. Certificates Manager uses the digest that you compute in your own certificate application system. The message digest algorithm that you use must match the specified signature algorithm. Comply with the following mapping between signature algorithms and message digest algorithms: • If the signature algorithm is RSA_PKCS1_SHA_256, RSA_PSS_SHA_256, or ECDSA_SHA_256, the message digest algorithm must be SHA-256. • If the signature algorithm is SM2DSA, the message digest algorithm must be SM3. **Note** If the key type of the certificate is EC_SM2 and the MessageType parameter is set to DIGEST, the value of the Message parameter is `e` that is described in GB/T 32918.2-2016 6.1.
MessageType	String	Yes	RAW	The type of the message. Valid values: • RAW: the raw data. This is the default value. • DIGEST: the message digest (hash value) of the raw data.
SignatureValue	String	Yes	ZOyIygCyaOW6Gj****MlNKiuyjfzw=	The signature value. The value must be encoded in Base64.

For more information about common request parameters, see Common parameters.

Response parameters

Parameter	Type	Example	Description
CertificateId	String	12345678-1234-1234-1234-12345678****	The ID of the certificate.
RequestId	String	5979d897-d69f-4fc9-87dd-f3bb73c40b80	The ID of the request.
SignatureValid	Boolean	true	The verification result. Valid values: • true: The signature is valid. • false: The signature is invalid.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=CertificatePublicKeyVerify
&Algorithm=ECDSA_SHA_256
&CertificateId=12345678-1234-1234-1234-12345678****
&Message=VGhlIHF1aWNrIGJyb3duIGZveCBqdW1wcyBvdmVyIHRoZSBsYXp5IGRvZy4=
&MessageType=RAW
&SignatureValue=ZOyIygCyaOW6Gj****MlNKiuyjfzw=
&<Common request parameters>|
```

Sample success responses

`XML` format

```
<KMS>
   <CertificateId>12345678-1234-1234-1234-12345678****</CertificateId>
   <SignatureValid>true</SignatureValid>
   <RequestId>5979d897-d69f-4fc9-87dd-f3bb73c40b80</RequestId>
</KMS>
```

`JSON` format

```
{
  "CertificateId": "12345678-1234-1234-1234-12345678****",
  "SignatureValid": "true",
  "RequestId": "5979d897-d69f-4fc9-87dd-f3bb73c40b80"
}
```

Error codes

HTTP status code	Error code	Error message	Description
404	InvalidAccessKeyId.NotFound	The specified AccessKey ID does not exist.	The error message returned because the specified AccessKey ID does not exist. Check whether a valid AccessKey ID is specified when you call the operation.

For a list of error codes, visit the API Error Center.

10.9. CertificatePublicKeyEncrypt

Encrypts data by using a specific certificate.

Limit: The encryption algorithm in the request parameters must match the key type.

The following table describes the mapping between encryption algorithms and key types.

Algorithm	Key Type
RSAES_OAEP_SHA_1	RSA_2048
RSAES_OAEP_SHA_256	RSA_2048
SM2PKE	EC_SM2

In this example, the certificate whose ID is `12345678-1234-1234-1234-12345678****` and the encryption algorithm `RSAES_OAEP_SHA_256` are used to encrypt the data `VGhlIHF1aWNrIGJyb3duIGZveCBqdW1wcyBvdmVyIHRoZSBsYXp5IGRvZy4=`.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	CertificatePublicKeyEncrypt	The operation that you want to perform. Set the value to CertificatePublicKeyEncrypt.
Algorithm	String	Yes	RSAES_OAEP_SHA_256	The encryption algorithm. Valid values: • RSAES_OAEP_SHA_1 • RSAES_OAEP_SHA_256 • SM2PKE **Note** The SM2PKE encryption algorithm is supported only in regions in mainland China. In these regions, managed hardware security modules (HSMs) are used. For more information, see Overview of managed HSM.
CertificateId	String	Yes	12345678-1234-1234-1234-12345678****	The ID of the certificate. It is the globally unique identifier (GUID) of the certificate in Certificates Manager.
Plaintext	String	Yes	VGhlIHF1aWNrIGJyb3duIGZveCBqdW1wcyBvdmVyIHRoZSBsYXp5IGRvZy4=	The data that you want to encrypt. The value must be encoded in Base64. For example, if the hexadecimal data that you want to encrypt is `[0x31, 0x32, 0x33, 0x34]`, the Base64-encoded data is `MTIzNA==`. The size of data that can be encrypted varies based on the encryption algorithm that you use: • RSAES_OAEP_SHA_1: 214 bytes • RSAES_OAEP_SHA_256: 190 bytes • SM2PKE: 6,047 bytes If the size of data that you want to encrypt exceeds the preceding limits, you can call the GenerateDataKey operation to generate a data key to encrypt the data. Then, call the CertificatePublicKeyEncrypt operation to encrypt the data key.

For more information about common request parameters, see Common parameters.

Response parameters

Parameter	Type	Example	Description
CertificateId	String	12345678-1234-1234-1234-12345678****	The ID of the certificate.
CiphertextBlob	String	ZOyIygCyaOW6Gj****MlNKiuyjfzw=	The ciphertext after data is encrypted. The value is encoded in Base64.
RequestId	String	5979d897-d69f-4fc9-87dd-f3bb73c40b80	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=CertificatePublicKeyEncrypt
&Algorithm=RSAES_OAEP_SHA_256
&CertificateId=12345678-1234-1234-1234-12345678****
&Plaintext=VGhlIHF1aWNrIGJyb3duIGZveCBqdW1wcyBvdmVyIHRoZSBsYXp5IGRvZy4=
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
        <CertificateId>12345678-1234-1234-1234-12345678****</CertificateId>
        <CiphertextBlob>ZOyIygCyaOW6Gj****MlNKiuyjfzw=</CiphertextBlob>
        <RequestId>5979d897-d69f-4fc9-87dd-f3bb73c40b80</RequestId>
</KMS>
```

`JSON` format

```
{
  "CertificateId": "12345678-1234-1234-1234-12345678****",
  "CiphertextBlob": "ZOyIygCyaOW6Gj****MlNKiuyjfzw=",
  "RequestId": "5979d897-d69f-4fc9-87dd-f3bb73c40b80"
}
```

Error codes

HttpCode	Error code	Error message	Description
404	Certificate.NotFound	The specified certificate is not found.	The error message returned because the specified certificate does not exist.

For a list of error codes, visit the API Error Center.

10.10. CertificatePrivateKeyDecrypt

Decrypts data by using a specific certificate.

Limit: The encryption algorithm in the request parameters must match the key type.

The following table describes the mapping between encryption algorithms and key types.

Algorithm	Key Type
RSAES_OAEP_SHA_1	RSA_2048
RSAES_OAEP_SHA_256	RSA_2048
SM2PKE	EC_SM2

In this example, the certificate whose ID is `12345678-1234-1234-1234-12345678****` and the encryption algorithm `RSAES_OAEP_SHA_256` are used to decrypt the data `ZOyIygCyaOW6Gj****MlNKiuyjfzw=`.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	CertificatePrivateKeyDecrypt	The operation that you want to perform. Set the value to CertificatePrivateKeyDecrypt.
Algorithm	String	Yes	RSAES_OAEP_SHA_256	The encryption algorithm. Valid values: • RSAES_OAEP_SHA_1 • RSAES_OAEP_SHA_256 • SM2PKE **Note** The SM2PKE encryption algorithm is supported only in regions in mainland China. In these regions, managed hardware security modules (HSMs) are used. For more information, see Overview of managed HSM.
CertificateId	String	Yes	12345678-1234-1234-1234-12345678****	The ID of the certificate. It is the globally unique identifier (GUID) of the certificate in Certificates Manager.
CiphertextBlob	String	Yes	ZOyIygCyaOW6Gj****MlNKiuyjfzw=	The data that you want to decrypt. The value must be encoded in Base64.

For more information about common request parameters, see Common parameters.

Response parameters

Parameter	Type	Example	Description
CertificateId	String	12345678-1234-1234-1234-12345678****	The ID of the certificate.
Plaintext	String	VGhlIHF1aWNrIGJyb3duIGZveCBqdW1wcyBvdmVyIHRoZSBsYXp5IGRvZy4	The plaintext after data is decrypted. The value is encoded in Base64.
RequestId	String	5979d897-d69f-4fc9-87dd-f3bb73c40b80	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=CertificatePrivateKeyDecrypt
&Algorithm=RSAES_OAEP_SHA_256
&CertificateId=12345678-1234-1234-1234-12345678****
&CiphertextBlob=ZOyIygCyaOW6Gj****MlNKiuyjfzw=
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
        <CertificateId>12345678-1234-1234-1234-12345678****</CertificateId>
        <Plaintext>VGhlIHF1aWNrIGJyb3duIGZveCBqdW1wcyBvdmVyIHRoZSBsYXp5IGRvZy4</Plaintext>
        <RequestId>5979d897-d69f-4fc9-87dd-f3bb73c40b80</RequestId>
</KMS>
```

`JSON` format

```
{
  "CertificateId": "12345678-1234-1234-1234-12345678****",
  "Plaintext": "VGhlIHF1aWNrIGJyb3duIGZveCBqdW1wcyBvdmVyIHRoZSBsYXp5IGRvZy4",
  "RequestId": "5979d897-d69f-4fc9-87dd-f3bb73c40b80"
}
```

Error codes

HttpCode	Error code	Error message	Description
404	Certificate.NotFound	The specified certificate is not found.	The error message returned because the specified certificate does not exist.

For a list of error codes, visit the API Error Center.

11.Tag

11.1. TagResource

Attaches tags to a customer master key (CMK), secret, or certificate.

You can attach up to 10 tags to a CMK, secret, or certificate.

In this example, the tags `[{\"TagKey\":\"S1key1\",\"TagValue\":\"S1val1\"},{\"TagKey\":\"S1key2\",\"TagValue\":\"S2val2\"}]` are attached to the CMK whose ID is `08c33a6f-4e0a-4a1b-a3fa-7ddf****`.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	TagResource	The operation that you want to perform. Set the value to TagResource.
Tags	String	Yes	[{\"TagKey\":\"S1key1\",\"TagValue\":\"S1val1\"},{\"TagKey\":\"S1key2\",\"TagValue\":\"S2val2\"}]	One or more tags. Format: tag object array. Tag object attributes: • TagKey: the tag key. • TagValue: the tag value.
KeyId	String	No	08c33a6f-4e0a-4a1b-a3fa-7ddf****	The ID of the CMK. The ID must be globally unique. **Note** You can set only one of the KeyId, SecretName, and CertificateId parameters.
SecretName	String	No	MyDbC****	The name of the secret. **Note** You can set only one of the KeyId, SecretName, and CertificateId parameters.
CertificateId	String	No	770dbe42-e146-43d1-a55a-1355db86****	The ID of the certificate. **Note** You can set only one of the KeyId, SecretName, and CertificateId parameters.

For more information about common request parameters, see Common parameters.

Response parameters

Parameter	Type	Example	Description
RequestId	String	4162a6af-bc99-40b3-a552-89dcc8aaf7c8	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=TagResource
&KeyId=08c33a6f-4e0a-4a1b-a3fa-7ddf****
&Tags=[{\"TagKey\":\"S1key1\",\"TagValue\":\"S1val1\"},{\"TagKey\":\"S1key2\",\"TagValue\":\"S2val2\"}]
&<Common request parameters>|
```

Sample success responses

`XML` format

```
<KMS>
    <RequestId>4162a6af-bc99-40b3-a552-89dcc8aaf7c8</RequestId>
</KMS>
```

`JSON` format

```
{
    "RequestId":"4162a6af-bc99-40b3-a552-89dcc8aaf7c8"
}
```

Error codes

For a list of error codes, visit the API Error Center.

11.2. UntagResource

Detaches tags from a customer master key (CMK), secret, or certificate.

In this example, the tags whose tag keys are tagkey1 and tagkey2 are detached from the CMK whose ID is `08c33a6f-4e0a-4a1b-a3fa-7ddf****`.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	UntagResource	The operation that you want to perform. Set the value to UntagResource.
TagKeys	String	Yes	["tagkey1","tagkey2"]	One or more tag keys. Separate multiple tag keys with commas (,). You need to specify only the tag keys, not the tag values. Each tag key must be 1 to 128 bytes in length.
KeyId	String	No	08c33a6f-4e0a-4a1b-a3fa-7ddf****	The ID of the CMK. The ID must be globally unique. **Note** You can set only one of the KeyId, SecretName, and CertificateId parameters.
SecretName	String	No	MyDbC****	The name of the secret. **Note** You can set only one of the KeyId, SecretName, and CertificateId parameters.
CertificateId	String	No	770dbe42-e146-43d1-a55a-1355db86****	The ID of the certificate. **Note** You can set only one of the KeyId, SecretName, and CertificateId parameters.

For more information about common request parameters, see Common parameters.

Response parameters

Parameter	Type	Example	Description
RequestId	String	4162a6af-bc99-40b3-a552-89dcc8aaf7c8	The ID of the request.

Examples

Sample requests

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=UntagResource
&KeyId=08c33a6f-4e0a-4a1b-a3fa-7ddf****
&TagKeys=["tagkey1","tagkey2"]
&<Common request parameters>|
```

Sample success responses

`XML` format

```
<KMS>
    <RequestId>4162a6af-bc99-40b3-a552-89dcc8aaf7c8</RequestId>
</KMS>
```

`JSON` format

```
{
    "RequestId": "4162a6af-bc99-40b3-a552-89dcc8aaf7c8"
}
```

Error codes

For a list of error codes, visit the API Error Center.

11.3. ListResourceTags

Obtains the tags of a customer master key (CMK).

Request format: KeyId="string"

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ListResourceTags	The operation that you want to perform. Set the value to ListResourceTags.
KeyId	String	Yes	1234abcd-12ab-34cd-56ef-12345678****	The globally unique identifier of the key of the CMK whose tags you want to obtain.

Response parameters

Parameter	Type	Example	Description
RequestId	String	4162a6af-bc99-40b3-a552-89dcc8aaf7c8	The ID of the request.
Tags	Array		An array of Tag data.
Tag			
KeyId	String	33caea95-c3e5-4 b3 e-a9c6-cec76e4e specific parameter values *	The globally unique identifier of the key of the CMK.
TagKey	String	Project	A tag key.
TagValue	String	Test	A tag value.

Examples

Sample requests

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=ListResourceTags
&KeyId=<keyid>
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
        <RequestId>0f900dad-c747-4170-9962-1bfb6b31436b</RequestId>
        <Tags>
            <Tag>
                <KeyId>33caea95-c3e5-4b3e-a9c6-cec76e4e****</KeyId>
                <TagKey>Project</TagKey>
                <TagValue>Test</TagValue>
            </Tag>
        </Tags>
</KMS>
```

`JSON` format

```
{
    "RequestId": "4162a6af-bc99-40b3-a552-89dcc8aaf7c8",
    "Tags": {
            "Tag": [
                {
                    "KeyId": "33caea95-c3e5-4b3e-a9c6-cec76e4e****",
                    "TagKey": "Project",
                    "TagValue": "Test"
                }
            ]
        }
}
```

Error codes

HTTP status code	Error code	Error message	Description
400	Throttling	Request was denied due to request throttling.	This message returned because your traffic in this period has exceeded the limit. If your business requirements are not met, submit a ticket.

For a list of error codes, visit the API Error Center.

12.Other API operations

12.1. DescribeRegions

Queries available regions.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeRegions	The operation that you want to perform. Set the value to DescribeRegions.

Response parameters

Parameter	Type	Example	Description
Regions	Array of Region		The region.
Region			
RegionId	String	cn-hangzhou	The region ID.
RequestId	String	815240e2-aa37-4c26-9cca-05d4df3e8fe6	The ID of the request.

Examples

Sample requests

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=DescribeRegions
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
   <Regions>
      <Region>
         <RegionId>cn-beijing</RegionId>
      </Region>
      <Region>
         <RegionId>cn-hangzhou</RegionId>
      </Region>
   </Regions>
   <RequestId>815240e2-aa37-4c26-9cca-05d4df3e8fe6</RequestId>
</KMS>
```

`JSON` format

```
{
        "Regions": {
                "Region": [
                        {
                                "RegionId": "cn-beijing"
                        },
                        {
                                "RegionId": "cn-hangzhou"
                        }
                ]
        },
        "RequestId": "815240e2-aa37-4c26-9cca-05d4df3e8fe6"
}
```

Error codes

For a list of error codes, visit the API Error Center.

12.2. OpenKmsService

Activates Key Management Service (KMS) under your Alibaba cloud account.

When you call this operation, note that:

- KMS is a paid service. For more information about the billing method, see Billing description.

- An Alibaba Cloud account can activate KMS only once.
- Make sure that your Alibaba Cloud account has passed real-name authentication.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	OpenKmsService	The operation that you want to perform. Set the value to OpenKmsService.

Response parameters

Parameter	Type	Example	Description
RequestId	String	3455b9b4-95c1-419d-b310-db6a53b09a39	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=OpenKmsService
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
      <RequestId>3455b9b4-95c1-419d-b310-db6a53b09a39</RequestId>
</KMS>
```

`JSON` format

```
{
  "RequestId": "3455b9b4-95c1-419d-b310-db6a53b09a39"
}
```

Error codes

HTTP status code	Error code	Error message	Description
400	CreateLXOrderFailed	Create order failed.	The error message returned because the order has failed to be created.
400	Forbidden.NoRealNameAuthentication	Real name authentication is needed.	The error message returned because you have not completed real-name verification.
400	Forbidden.Opened	Your kms service has been opened.	The error message returned because you have activated KMS.

For a list of error codes, visit the API Error Center.

12.3. DescribeAccountKmsStatus

Queries the status of Key Management Service (KMS) under your Alibaba Cloud account.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeAccountKmsStatus	The operation that you want to perform. Set the value to DescribeAccountKmsStatus.

Response parameters

Parameter	Type	Example	Description

Parameter	Type	Example	Description
AccountStatus	String	Enabled	The status of KMS under your Alibaba cloud account. Valid values: • Enabled: KMS is enabled. • NotEnabled: KMS is disabled. • Index: Your account is overdue, and KMS stops providing services. Note If your Alibaba Cloud account is overdue, top up your account in a timely manner to avoid impacts on your services. • Suspended: KMS is suspended.
RequestId	String	3455b9b4-95c1-419d-b310-db6a53b09a39	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=DescribeAccountKmsStatus
```

Sample success responses

`XML` format

```
<KMS>
    <AccountStatus>Enabled</AccountStatus>
    <RequestId>3455b9b4-95c1-419d-b310-db6a53b09a39</RequestId>
</KMS>
```

`JSON` format

```
{
  "AccountStatus": "Enabled",
  "RequestId": "3455b9b4-95c1-419d-b310-db6a53b09a39"
}
```

Error codes

For a list of error codes, visit the API Error Center.