

Alibaba Cloud Key Management Service

API Reference

Issue: 20191021

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 due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall 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 the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. 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 bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequent

ial, exemplary, incidental, 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 contact Alibaba Cloud directly if you discover any errors in this document

.

Document conventions

Style	Description	Example
	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.
	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.
	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.
	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 <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>

Style	Description	Example
{} or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

Contents

Legal disclaimer	I
Document conventions	I
1 Calling method	1
1.1 Overview.....	1
1.2 Request structure.....	1
1.3 Common parameters.....	4
1.4 Signature.....	5
1.5 Responses.....	8
2 Effects of CMK states on API operations	13
3 API operations by function	16
4 API list	19
4.1 CreateKey.....	19
4.2 GetParametersForImport.....	23
4.3 ImportKeyMaterial.....	25
4.4 EnableKey.....	27
4.5 DisableKey.....	28
4.6 ScheduleKeyDeletion.....	29
4.7 CancelKeyDeletion.....	30
4.8 DeleteKeyMaterial.....	31
4.9 DescribeKey.....	32
4.10 UpdateKeyDescription.....	34
4.11 ListKeys.....	36
4.12 Encrypt.....	37
4.13 GenerateDataKey.....	40
4.14 GenerateDataKeyWithoutPlaintext.....	43
4.15 Decrypt.....	46
4.16 CreateAlias.....	48
4.17 UpdateAlias.....	49
4.18 DeleteAlias.....	51
4.19 ListAliases.....	52
4.20 ListAliasesByKeyId.....	53
4.21 TagResource.....	55
4.22 UntagResource.....	58
4.23 ListResourceTags.....	59
4.24 DescribeRegions.....	60
4.25 DescribeKeyVersion.....	62
4.26 ListKeyVersions.....	63
4.27 UpdateRotationPolicy.....	65

1 Calling method

1.1 Overview

KMS query requests are HTTP POST and GET requests. A request contains the required parameters and the syntax of the operation to perform. Then the API server returns the result of this request.

1. [Request structure](#)
2. [Common parameters](#)
3. [Responses](#)
4. [Signature](#)

1.2 Request structure

Service endpoints

The following table lists the service access endpoints of the KMS API.

Region	RegionId	Public network endpoint	Private network endpoint
Asia Pacific NE 1 (Tokyo)	ap-northeast-1	kms.ap-northeast-1.aliyuncs.com	kms-vpc.ap-northeast-1.aliyuncs.com
Asia Pacific SE 1 (Singapore)	ap-southeast-1	kms.ap-southeast-1.aliyuncs.com	kms-vpc.ap-southeast-1.aliyuncs.com
Asia Pacific SE 2 (Sydney)	ap-southeast-2	kms.ap-southeast-2.aliyuncs.com	kms-vpc.ap-southeast-2.aliyuncs.com
Asia Pacific SE 3 (Kuala Lumpur)	ap-southeast-3	kms.ap-southeast-3.aliyuncs.com	kms-vpc.ap-southeast-3.aliyuncs.com
Asia Pacific SE 5 (Jakarta)	ap-southeast-5	kms.ap-southeast-5.aliyuncs.com	kms-vpc.ap-southeast-5.aliyuncs.com

Region	RegionId	Public network endpoint	Private network endpoint
Asia Pacific SOU 1 (Mumbai)	ap-south-1	kms.ap-south-1.aliyuncs.com	kms-vpc.ap-south-1.aliyuncs.com
China East 1 (Hangzhou)	cn-hangzhou	kms.cn-hangzhou.aliyuncs.com	kms-vpc.cn-hangzhou.aliyuncs.com
China East 2 (Shanghai)	cn-shanghai	kms.cn-shanghai.aliyuncs.com	kms-vpc.cn-shanghai.aliyuncs.com
China North 1 (Qingdao)	cn-qingdao	kms.cn-qingdao.aliyuncs.com	kms-vpc.cn-qingdao.aliyuncs.com
China North 2 (Beijing)	cn-beijing	kms.cn-beijing.aliyuncs.com	kms-vpc.cn-beijing.aliyuncs.com
China North 3 (Zhangjiakou)	cn-zhangjiakou	kms.cn-zhangjiakou.aliyuncs.com	kms-vpc.cn-zhangjiakou.aliyuncs.com
China North 5 (Hohhot)	cn-huhehaote	kms.cn-huhehaote.aliyuncs.com	kms-vpc.cn-huhehaote.aliyuncs.com
China South 1 (Shenzhen)	cn-shenzhen	kms.cn-shenzhen.aliyuncs.com	kms-vpc.cn-shenzhen.aliyuncs.com
EU Central 1 (Frankfurt)	eu-central-1	kms.eu-central-1.aliyuncs.com	kms-vpc.eu-central-1.aliyuncs.com
Middle East 1 (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 East 1 (Virginia)	us-east-1	kms.us-east-1.aliyuncs.com	kms-vpc.us-east-1.aliyuncs.com
US West 1 (Silicon Valley)	us-west-1	kms.us-west-1.aliyuncs.com	kms-vpc.us-west-1.aliyuncs.com
China East 1 (Hangzhou finance cloud)	cn-hangzhou-finance	kms.cn-hangzhou-finance.aliyuncs.com	None

Region	RegionId	Public network endpoint	Private network endpoint
China East 2 (Shanghai finance cloud)	cn-shanghai-finance-1	kms.cn-shanghai-finance-1.aliyuncs.com	kms-vpc.cn-shanghai-finance-1.aliyuncs.com
China South 1 (Shenzhen finance cloud)	cn-shenzhen-finance-1	kms.cn-shenzhen-finance-1.aliyuncs.com	kms-vpc.cn-shenzhen-finance-1.aliyuncs.com
UK (London)	eu-west-1	kms.eu-west-1.aliyuncs.com	kms-vpc.eu-west-1.aliyuncs.com

Interaction protocol

KMS API requests are HTTPS POST and GET request messages.

SSLv2 and SSLv3 are not supported. TLS1.0 and later versions are supported.

Request method

A POST or GET request is a URL encoded with the parameter value that the interface you access requires.

Request parameters

For each request, the operation to be executed, namely, the *Action* parameters (for example, *CreateKey*), must be specified. Each operation must include the *Common parameters* and the specific request parameters of the specified operations.

Character encoding

Requests and returned results are both encoded using UTF-8.

1.3 Common parameters

Common request parameters are used in each API.

Common request parameters

Name	Type	Required	Description
Format	String	No	The format of the response text. JSON and XML are supported. The default format is XML.
Version	String	Yes	The API version in the format YYYY-MM-DD. The current version is 2016-01-20.
AccessKeyId	String	Yes	An alphanumeric token issued by Alibaba Cloud for user authentication.
Signature	String	Yes	Signing requests. For more information, see Signature .
SignatureMethod	String	Yes	The hash algorithm to create the request signature. HMAC-SHA1 is used.
Timestamp	String	Yes	The time stamp of the request. The date and time at which a request is signed, in the format YYYY-MM-DDThh:mm:ssZ. Example: 2014-05-26T12:00:00Z

Name	Type	Required	Description
SignatureVersion	String	Yes	The signature version used to sign a request. The current version is 1.0.

Example

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

Common response parameters

Each time you send an API request, a unique RequestId is returned, whether the request is successful or not.

Example

XML example

```
<KMS>
<RequestId>348d9445-e39a-4d80-907d-298cc6c94447</RequestId>
<!--Returned results-->
</KMS>
```

JSON example

```
{
  "RequestId": "284b2b80-9b17-4546-a093-adfbae512a54"
}
```

1.4 Signature

When you send HTTP requests to Alibaba Cloud, you sign the requests so that Alibaba Cloud can identify who sent them. You sign requests with your AccessKey,

which consists of an AccessKey ID and AccessKey secret. You can apply for an AccessKey for your primary account and manage it on our official site.

Signature process

1. Create a canonical request.

- Sort the parameter names by character code point in ascending order. The parameters to sort include the common request parameters and the parameter of the API to call.



Note:

When you submit a request using the GET method, these parameters are the parameters part of the request URI "?" and connected by "&").

- Encode (URL) the name and value of each request parameter. Use the UTF-8 character set for coding. The coding rules are:
 - Uppercase and lowercase letters, numbers, hyphens (-), underscores (_), periods (.), and tildes (~) need not be encoded.
 - Other characters are encoded as "%XY", where XY is the hexadecimal representation of the character in ASCII. The double quotation mark (") is coded as %22
 - An English space () is encoded as %20 rather than the plus sign (+).



Note:

Generally, libraries that support URL encoding (e.g. Java's `java.net.URLEncoder`) are all encoded according to the rules for the "application/x-www-form-urlencoded" MIME type. If this encoding method is used, replace the plus signs (+) in the encoded strings with %20,

the asterisks (*) with %2A, and change %7E back to the tilde (~) to conform to the encoding rules described above.

- Connect the encoded parameter names and values with the English equals sign (=).
- Then, order the parameter name and value pairs connected by equals signs in alphabetical order and connect them with the & symbol to produce the Canonicalized Query String.

Use the Canonicalized Query String obtained in the preceding step to construct the string for signature calculation according to the following rules:

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

HTTPMethod: indicates the HTTP method used for request submission, for example, GET. - **percentEncode("/"):** the coded value for the character “/” according to the URL encoding rules described above, namely, “%2F” .

percentEncode(CanonicalizedQueryString) indicates the encoded string of the Canonicalized Query String constructed in step 1.b, produced by following the URL encoding rules described in 1.b.

2. Use the preceding signature string to calculate the signature's HMAC value based on [RFC2104](#) definitions. Note: The Key used for signature calculation is the Access Key Secret held by the user added with a "&" character (ASCII:38), and the SHA1 hashing algorithm is used.
3. According to Base64 encoding rules, encode the preceding HMAC value, which gives you the signature value.
4. Add the obtained signature value to the request parameters as the “Signature” parameter, which completes the request signing process.



Note:

Note: When the obtained signature value is submitted to the KMS server as the final request parameter value, the value will be URL encoded like other parameters according to RFC3986 rules.

Examples

Take `CreateKey` as an example, the request URL before signature is:

```
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
```

CanonicalizedQueryString is:

```
AccessKeyId=testid&Action=CreateKey&Format=json&SignatureMethod=HMAC-
SHA1&SignatureVersion=1.0&Timestamp=2016-03-28T03%3A13%3A08Z&Version=
2016-01-20
```

StringToSign is:

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

If the Access Key ID is `testid`, the Access Key Secret is `testsecret`, and the Key used for HMAC calculation is `testsecret&`, the calculated signature value is:

```
s/OdVWMTmNGagvWlljdAJ7Itsew=
```

The signed request URL is (with the Signature parameter added):

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=CreateKey
&SignatureVersion=1.0
&Format=json
&Version=2016-01-20
&AccessKeyId=F585*****APMU
&SignatureMethod=HMAC-SHA1
&Timestamp=2016-03-28T03:13:08Z
&Signature=41wk2SSX1GJh7fwnc5eq0fiJPF****
```

1.5 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. Response data

can be returned in the JSON format. If you make an API request by using third-party tools, you can customize the response format in the request parameters.

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

When an error occurs during an API call, response data is not returned. You can locate the cause of an error based on the corresponding error code and [Common error codes](#).

When an error occurs during a call, an HTTP status code of 4xx or 5xx is returned. The returned message includes the specific error code and message. It also contains a globally unique request ID (RequestId) and the ID of the site you accessed with this request (HostId). If you cannot locate the cause of a failed API call, we recommend that you contact Alibaba Cloud customer service with the corresponding HostId and RequestId to help resolve the issue.

XML format (an expired request)

```
<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 (an expired request)

```
{
  "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	Description	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	Description	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.Protection Level	This protection level is not valid for this region	400
Rejected.StateModifiedFailed	Keystate modified failed.	409

Error code	Description	HTTP status code
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

2 Effects of CMK states on API operations

In KMS, each CMK has three states: Enabled, Disabled, and PendingDeletion.

For a BYOK with its Origin value set to External in [KeyMetadata parameters](#), it also may be in the PendingImport state.

A newly created CMK is usually in the Enabled state. A BYOK is in the PendingImport state when it is created.

Only CMKs in the Enabled state can be used in the Encrypt and Decrypt API operations. Different results may be returned for other API operations depending on CMK states.

A CMK in the PendingDeletion state will be deleted permanently after scheduled period for CMK deletion expires.

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

API operation	Enabled	Disabled	PendingDeletion	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

API operation	Enabled	Disabled	PendingDeletion	PendingImport
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:

- Is affected only by the states of the destination CMK, but not the states of the source 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
ImportKeyMaterial	Success	Success	Rejected. StateModifiedFailed	Success
DeleteKeyMaterial	Success	Success	Success	Success

3 API operations by function

The following tables list API operations available for use in KMS. For more information, see [OpenAPI Explorer](#).

Alibaba Cloud also provides a command line tool for you to learn APIs and for the purpose of command line automation. For more information about how to install and use the command line tool, see [Alibaba Cloud CLI](#).

Key management

Key management API operations are used to create and modify keys and manage their lifecycle.

Operation	Description
CreateKey	Creates a CMK. You can also choose to let KMS generate key materials, or upload your own key materials. CreateKey is the first step to create a Bring Your Own Key (BYOK).
GetParametersForImport	Obtains key materials, which is the second step to create a BYOK.
ImportKeyMaterial	Imports key materials to the CMK, which is the final step to create a BYOK.
EnableKey	Modifies the key status to Enabled.
DisableKey	Modifies the key status to Disabled.
ScheduleKeyDeletion	Schedules key deletion. The key status changes to PendingDeletion. A CMK in the PendingDeletion state will be deleted when the scheduled period expires.
CancelKeyDeletion	Cancels the scheduled deletion of a CMK . You can cancel a scheduled deletion request after it is submitted and before the end of the scheduled period. After the scheduled deletion is canceled, the CMK returns to the Enabled state.

Operation	Description
<i>DeleteKeyMaterial</i>	Deletes key materials of a CMK. You can directly delete key materials of a BYOK . After key materials are deleted, the BYOK is in the PendingImport state.
<i>DescribeKey</i>	Queries detailed information about a specified CMK.
<i>ListKeys</i>	Lists all CMKs within the current region that belong to the current Alibaba Cloud account.
<i>UpdateKeyDescription</i>	Updates the description of a CMK.

Key version management

Key version management API operations are used for CMK rotation.

Operation	Description
<i>DescribeKeyVersion</i>	Queries a key version.
<i>ListKeyVersions</i>	Lists all key versions of a specified CMK.
<i>UpdateRotationPolicy</i>	Updates the CMK rotation policy. If automatic rotation is enabled, KMS automatically generates a new key version on a periodic basis.

Key operation

Key operation API operations are used to perform data operations involving keys such as encryption and decryption.

Operation	Description
<i>Encrypt</i>	Uses a specified CMK to encrypt data . This operation is used for online encryption of data of no more than 6 KB.
<i>GenerateDataKey</i>	Generates a random number. After the random number is encrypted with the specified CMK, its ciphertext and plaintext are returned. The random number can be used as a data key to encrypt or decrypt a large amount of data locally.

Operation	Description
<i>GenerateDataKeyWithoutPlaintext</i>	Generates a random number. After the random number is encrypted with the specified CMK, its ciphertext is returned . The random number can be used as a data key to encrypt or decrypt a large amount of data locally.
<i>Decrypt</i>	Decrypts ciphertexts generated with the <code>Encrypt</code> or <code>GenerateDataKey</code> API operation. You do not need to specify the CMK for decryption.

Alias management

An alias is an independent object that must be bound to a unique CMK. Then it can be used to replace the `KeyId` of the CMK.

Operation	Description
<i>CreateAlias</i>	Creates an alias and binds it to a CMK.
<i>UpdateAlias</i>	Binds a specified alias to a new CMK.
<i>DeleteAlias</i>	Deletes a specified alias.
<i>ListAliases</i>	Lists all aliases of an Alibaba Cloud account in the current region.
<i>ListAliasesByKeyId</i>	Lists all aliases bound to a specified CMK.

Tag management

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

Operation	Description
<i>TagResource</i>	Adds or modifies the tags of a CMK.
<i>UntagResource</i>	Deletes the specified tag of a CMK.
<i>ListResourceTags</i>	Lists all tags of a CMK.

4 API list

4.1 CreateKey


You can call this operation to create a customer master key (CMK).


A CMK is used to directly encrypt a small amount of data (up to 6 KB of data).

However, it's often used to generate data keys for encrypting a large amount of data.

For more information, see [GenerateDataKey](#).

Request parameters

Parameter	Type	Required	Description
Origin	String	No	<p>The source of the key material for the CMK to create.</p> <p>Valid values: Aliyun_KMS and EXTERNAL.</p> <div style="background-color: #f0f0f0; padding: 5px;">  Note: The default value is Aliyun_KMS. The value of this parameter is case sensitive. </div> <p>If you select EXTERNAL, you must #unique_38.</p>
Description	String	No	<p>The description of the CMK to create . The description must be 0 to 8,192 characters in length.</p>

KeyUsage	String	No	<p>The purpose of the CMK to create. Default value: ENCRYPT/DECRYPT</p>
ProtectionLevel	String	No	<p>The protection level of the CMK to create.</p> <p>Valid value: SOFTWARE and HSM. When this parameter is set to HSM:</p> <ul style="list-style-type: none"> · If the Origin parameter is set to Aliyun_KMS , the CMK is created in Managed HSM. · If the Origin parameter is set to EXTERNAL, you can import external keys to Managed HSM. <div style="background-color: #f0f0f0; padding: 5px;">  Note: The default value is SOFTWARE. The value of this parameter is case sensitive. </div>

Response parameters

Parameter	Type	Description
KeyMetadata	<i>KeyMetadata parameters</i>	The metadata of the CMK created.

KeyMetadata parameters

Parameter	Type	Description
CreationDate	Timestamp	The date and time when the CMK was created. The time is displayed in UTC.
Description	String	The description of the CMK.
KeyId	String	The globally unique ID of the CMK.
KeyState	String	The status of the CMK. For more information, see Effects of CMK states on API operations .
KeyUsage	String	The purpose of the CMK. Default value: ENCRYPT/DECRYPT.
DeleteDate	Timestamp	The scheduled date to delete CMK. The time is displayed in UTC. <ul style="list-style-type: none"> • If the value is empty, the CMK will not be deleted. • This value is returned only when the KeyState value is PendingDeletion.
Creator	String	The creator of the CMK.
Arn	String	The Alibaba Cloud Resource Name (ARN) of the CMK.
Origin	String	The source of the key material for the CMK.
MaterialExpireTime	String	The time when the key material for the CMK expires. The time is displayed in UTC. If the value is empty, the key material for the CMK does not expire.

ProtectionLevel	String	The protection level of the CMK.
------------------------	---------------	---

Examples

Sample requests

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=CreateKey
&Description=<your key description>
&KeyUsage=ENCRYPT/DECRYPT
&Origin=<key origin, default Aliyun_KMS>
&ProtectionLevel=HSM
&<Common request parameters>
```

Sample responses

JSON format

```
//json response
{
  "KeyMetadata": {
    "CreationDate": "2016-03-25T10:42:40Z",
    "Description": "key description example",
    "KeyId": "08c33a6f-4e0a-4a1b-a3fa-7ddfa1d4****",
    "KeyState": "Enabled",
    "KeyUsage": "ENCRYPT/DECRYPT",
    "DeleteDate": "",
    "Creator": "123456",
    "Arn": "acs:kms:cn-hangzhou:123456:key/08c33a6f-4e0a-4a1b-a3fa-7ddfa1d4****",
    "Origin": "Aliyun_KMS",
    "MaterialExpireTime": "",
    "ProtectionLevel": "HSM"
  },
  "RequestId": "3455b9b4-95c1-419d-b310-db6a53b09a39"
}
```

XML format

```
//xml response
<KMS>
  <KeyMetadata>
    <CreationDate>2016-03-25T10:40:47Z</CreationDate>
    <Description>key description example</Description>
    <KeyId>08c33a6f-4e0a-4a1b-a3fa-7ddfa1d4****</KeyId>
    <KeyState>Enabled</KeyState>
    <KeyUsage>ENCRYPT/DECRYPT</KeyUsage>
    <DeleteDate></DeleteDate>
    <Creator>123456</Creator>
    <Arn>acs:kms:cn-hangzhou:123456:key/08c33a6f-4e0a-4a1b-a3fa-7ddfa1d4****</Arn>
    <Origin>Aliyun_KMS</Origin>
    <MaterialExpireTime></MaterialExpireTime>
    <ProtectionLevel>HSM</ProtectionLevel>
  </KeyMetadata>
  <RequestId>6cb4bf6b-d9c9-4660-af5f-2328378e7257</RequestId>
```

</KMS>

4.2 GetParametersForImport

Returns the items you need in order to import key material into KMS from your existing key management infrastructure. The returned items are used in the subsequent *ImportKeyMaterial* request.



Note:

- This CMK's `Origin` must be `EXTERNAL`.
- This operation returns a public key, an import token, and the import token expiration time. The public key is base64 encoded. The import token is valid for 24 hours.
- You must specify the wrapping key (public key) type (`RSA_2048` is supported) and the wrapping algorithm (`RSAES_PKCS1_V1_5`, `RSAES_OAEP_SHA_1`, and `RSAES_OAEP_SHA_256` are supported).
- The public key and import token can be used only to encrypt and import the CMK ID specified in this API request.
- The public key and import token from the same response must be used together.
- The algorithm used to encrypt the key material must be the one specified in the API request.
- Each request to this API returns a different pair of public key and import token.

Request parameters

Name	Type	Required	Description
KeyId	String	Yes	Globally unique identifier of the CMK. The <code>Origin</code> must be <code>EXTERNAL</code> .
WrappingAlgorithm	String	Yes	The algorithm used to encrypt the key material before importing it.

WrappingKeySpec	String	Yes	The type of wrapping key (public key) to return in the response.
------------------------	---------------	------------	---

Response parameters

Name	Type	Description
KeyId	String	The identifier of the CMK to use in a subsequent ImportKeyMaterial request.
ImportToken	String	The identifier of the CMK to use in a subsequent ImportKeyMaterial request.
PublicKey	String	The public key to use to encrypt the key material before importing it.
TokenExpireTime	String	The time when the import token expires.

Examples

Request example

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=GetParametersForImport
&KeyId=<external key id>
&WrappingAlgorithm=<key material encryption algorithm>
&WrappingKeySpec=RSA_2048
&<Common Request Parameters>
```

Response example**JSON format**

```
//json response
{
  "ImportToken":"ImportToken",
  "PublicKey":"PublicKey",
  "KeyId":"KeyId",
  "TokenExpireTime":"2018-01-25T00:01:02Z",
  "RequestId":"8cdf51fd-bcd6-d79a-0ef4-e52c9b5466dc"
}
```

XML format

```
//xml response
<KMS>
  <ImportToken>ImportToken</ImportToken>
```



```
<PublicKey>PublicKey</PublicKey>
<KeyId>KeyId</KeyId>
<TokenExpireTime>2018-01-25T00:01:02Z</TokenExpireTime>
<RequestId>8cdf51fd-bcd6-d79a-0ef4-e52c9b5466dc</RequestId>
</KMS>
```

4.3 ImportKeyMaterial

When you call *CreateKey* to create a CMK, you can set `Origin` to `EXTERNAL` and do not import the key material. This API is used to import the key material into the CMK.

- To check the `Origin` of a CMK, call *DescribeKey*.
- Before calling this API, call *GetParametersForImport* to get the key material ready to import. It returns a public key and an import token. Use the public key to encrypt the key material.



Note:

- The key material must be a 256-bit symmetric key.
- You can set the expiration time for the key material, or you can set it to never expire.
- You can always reimport the same key material and reset the expiration time, but you cannot import a different key material to the specified CMK.
- 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.

Request parameters

Name	Type	Required	Description
EncryptedKeyMaterial	String	Yes	Base64-encoded key material to import.
ImportToken	String	Yes	The import token you get by calling <i>GetParametersForImport</i> .

KeyMaterialExpireUnix	Timestamp	No	The time at which the imported key material expires . - If the value is omitted, or is specified as 0, the key material does not expire. - The value cannot be earlier than the timestamp at which you call the API (Base on the time set on the API server).
------------------------------	------------------	-----------	--

Response parameters

Name	Type	Description
RequestId	String	ID of this request.

Examples

Request example

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=ImportKeyMaterial
&EncryptedKeyMaterial=<your encrypted key material>
&ImportToken=<import token from GetParametersForImport>
&KeyMaterialExpireUnix=1518307200
&<Common Request Parameters>
```

Response example**JSON format**

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

XML format

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

```
</KMS>
```

4.4 EnableKey

Sets the state of the specified CMK to Enabled, thereby permitting its use for cryptographic operations.

Request parameters

Name	Type	Required	Description
KeyId	String	Yes	Globally unique identifier of the CMK.

Response parameters

Name	Type	Description
RequestId	String	ID of the request.

Examples

Request example

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=EnableKey
&KeyId=<cmkid>
&<Common Request Parameters>
```

Response example

JSON format

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

XML format

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

```
</KMS>
```

4.5 DisableKey

Sets the state of a CMK to Disabled. The ciphertext encrypted using the CMK cannot be decrypted until the CMK is enabled again.

Request parameters

Name	Type	Required	Description
KeyId	String	Yes	Globally unique identifier of the CMK.

Response parameters

Name	Type	Description
RequestId	String	The ID of this request.

Examples

Request example

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=DisableKey
&KeyId=<cmkid>
&<Common Request Parameters>
```

Response example

JSON format

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

XML format

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

</KMS>

4.6 ScheduleKeyDeletion

Schedules the deletion of a CMK.

- During waiting period, the key is in `PendingDeletion` state and cannot be used for encryption, decryption, or data key generation.
- A deleted CMK cannot be recovered. The data it encrypted, and the `DataKey` it generated cannot be decrypted again. Therefore, you must make a request to KMS for deleting a CMK. We recommend that you use [DisableKey](#) instead if possible.
- You must specify a waiting period when you make the request. The period must be between 7 and 30 days. You can use [CancelKeyDeletion](#) to cancel the request after submission but before the waiting period ends.
- The CMK is deleted within 24 hours after the waiting period ends. The API server uses UTC format. For example, a user makes a request at 14:00, Sep 10, 2016. The waiting period is 7 days. KMS deletes the CMK within 24 hours after 14:00, Sep 17
-

Request parameters

Name	Type	Required	Description
KeyId	String	Yes	Globally unique identifier of the CMK.
PendingWindowInDays	Integer	Yes	The waiting period, specified in number of days. During this period, you can cancel the CMK in <code>PendingDeletion</code> status. After the waiting period expires, you cannot cancel the deletion. The value must be between 7 and 30.

Response parameters

Name	Type	Description
RequestId	String	The ID of this request.

Examples

Request example

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=ScheduleKeyDeletion
&KeyId=<your-key-id>
&PendingWindowInDays=[7~30]
&<Common Request Parameters>
```

Response example**JSON format**

```
//json response
{
  "RequestId": "52ac67cb-3d3d-4ada-b4e2-7047660d3ce9"
}
```

XML format

```
//xml response
<KMS>
  <RequestId>52ac67cb-3d3d-4ada-b4e2-7047660d3ce9</RequestId>
</KMS>
```

4.7 CancelKeyDeletion

Cancels the deletion of a CMK. When this operation is successful, the CMK is set to Enabled state.

Request parameters

Name	Type	Required	Description
KeyId	String	Yes	Globally unique identifier of the CMK.

Response parameters

Name	Type	Description
RequestId	String	The ID of this request.

Examples

Request example

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=CancelKeyDeletion
&KeyId=<cmkid>
&<Common Request Parameters>
```

Response example**JSON format**

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

XML format

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

4.8 DeleteKeyMaterial

Deletes the imported key material.

- This operation does not cause the deletion of the specified CMK.
- If the specified CMK is in PendingDeletionstate, this operation does not change the CMK' s state or the scheduled deletion time. If the CMK is not in PendingDeletion state, it changes the CMK' s state to PendingImport.
- After you delete the key material, you can reimport the same key material into the CMK. You cannot import a different key material.

Request parameters

Name	Type	Required	Description
KeyId	String	Yes	Globally unique identifier of the CMK.

Response parameters

Name	Type	Description
RequestId	String	The ID of this request.

Examples

Request example

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=DeleteKeyMaterial
&KeyId=<external key id>
&<Common Request Parameters>
```

Response example**JSON format**

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

XML format

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

4.9 DescribeKey

You can call this operation to query detailed information about a specified CMK.

Request parameters

Parameter	Type	Required	Description
KeyId	String	Yes	The globally unique ID of the CMK to query. You can use aliases in the request. For more information, see #unique_39 .

Response parameters

Parameter	Type	Description
KeyMetadata	<i>KeyMetadata parameters</i>	The metadata of the CMK queried.

KeyMetadata parameters

Parameter	Type	Description
-----------	------	-------------

CreationDate	Timestamp	The date and time when the CMK was created. The time is displayed in UTC.
Description	String	The description of the CMK.
KeyId	String	The globally unique ID of the CMK.
KeyState	String	The status of the CMK. For more information, see Effects of CMK states on API operations .
KeyUsage	String	The purpose of the CMK.
DeleteDate	Timestamp	The scheduled date to delete CMK. For more information, see ScheduleKeyDeletion . This value is returned only when the KeyState value is PendingDeletion.
Creator	String	The creator of the CMK.
Arn	String	The Alibaba Cloud Resource Name (ARN) of the CMK.
Origin	String	The source of the key material for the CMK.
MaterialExpireTime	String	The time when the key material for the CMK expires. The time is displayed in UTC. If the value is empty, the key material for the CMK does not expire.
ProtectionLevel	String	The protection level of the CMK.

Examples

Sample requests

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=DescribeKey
&KeyId=<your-key-id>
```

&<Common request parameters>

Sample responses

JSON format

```
//json response
{
  "KeyMetadata": {
    "CreationDate": "2016-03-25T10:42:40Z",
    "Description": "key description example",
    "KeyId": "08c33a6f-4e0a-4a1b-a3fa-7ddf****",
    "KeyState": "Enabled",
    "KeyUsage": "ENCRYPT/DECRYPT",
    "DeleteDate": "",
    "Creator": "123456",
    "Arn": "acs:kms:cn-hangzhou:123456:key/08c33a6f-4e0a-4a1b-a3fa-7ddf****",
    "Origin": "Aliyun_KMS",
    "MaterialExpireTime": "",
    "ProtectionLevel": "HSM"
  },
  "RequestId": "3455b9b4-95c1-419d-b310-db6a53b09a39"
}
```

XML format

```
//xml response
<KMS>
  <KeyMetadata>
    <CreationDate>2016-03-25T10:40:47Z</CreationDate>
    <Description>key description example</Description>
    <KeyId>08c33a6f-4e0a-4a1b-a3fa-7ddf****</KeyId>
    <KeyState>Enabled</KeyState>
    <KeyUsage>ENCRYPT/DECRYPT</KeyUsage>
    <DeleteDate></DeleteDate>
    <Creator>123456</Creator>
    <Arn>acs:kms:cn-hangzhou:123456:key/08c33a6f-4e0a-4a1b-a3fa-7ddf****</Arn>
    <Origin>Aliyun_KMS</Origin>
    <MaterialExpireTime></MaterialExpireTime>
    <ProtectionLevel>HSM</ProtectionLevel>
  </KeyMetadata>
  <RequestId>6cb4bf6b-d9c9-4660-af5f-2328378e7257</RequestId>
</KMS>
```

4.10 UpdateKeyDescription

You can call this operation to update the description of a specified CMK.

This operation replaces the description of the CMK (the `Description` value in [KeyMetadata parameters](#)) with the value that you specify. You can add, modify, or delete the description of a CMK through this operation.

Request parameters

Parameter	Type	Required	Description
KeyId	String	Yes	The globally unique ID of the CMK.
Description	String	Yes	The description of the CMK. It usually involves the purpose of the CMK, such as the data types to be protected by the CMK or the applications that can use the CMK.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=UpdateKeyDescription
&KeyId=<cmkid>
&Description=<your key description>
&<Common request parameters>
```

Sample responses**JSON format**

```
//json response
{
  "RequestId": "475f1620-b9d3-4d35-b5c6-3fbdd941423d"
}
```

XML format

```
//xml response
<KMS>
  <RequestId>475f1620-b9d3-4d35-b5c6-3fbdd941423d</RequestId>
```

</KMS>

4.11 ListKeys

Returns a list of all CMKs in the caller's account and region.

Request parameters

Name	Type	Required	Description
PageNumber	Integer	No	The current page number. It must be an integer greater than 0. The default value is 1.
PageSize	Integer	No	The number of items on each page. It must be an integer greater than 0 and no more than 101. The default value is 10.

Response parameters

Name	Type	Description
KeyId	String	Globally unique identifier of the key.
TotalCount	Integer	The total number of keys.
PageNumber	Integer	The current page number.
PageSize	Integer	The number of items on each page.

Examples

Request example

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=ListKeys
&PageNumber=1
&PageSize=10
&<Common Request Parameters>
```

Response example

JSON format

```
//json response
{
  "Keys": {
    "Key": [
      {
        "KeyId": "08c33a6f-4e0a-4a1b-a3fa-7ddfa1d4****"
      },
      {
        "KeyId": "0e478b7a-4262-4802-b8cb-00d3fb40****"
      },
      {
        "KeyId": "1abf9b4e-d3dd-4d4b-b9b2-2829043a****"
      }
    ]
  },
  "TotalCount": 3,
  "PageNumber": 1,
  "PageSize": 10,
  "RequestId": "1fbcd12a-1b7f-468f-84a3-1ff3444dfd8b"
}
```

XML format

```
//xml response
<KMS>
  <Keys>
    <Key>
      <KeyId>08c33a6f-4e0a-4a1b-a3fa-7ddfa1d4****</
KeyId>
    </Key>
    <Key>
      <KeyId>0e478b7a-4262-4802-b8cb-00d3fb40****</
KeyId>
    </Key>
    <Key>
      <KeyId>1abf9b4e-d3dd-4d4b-b9b2-2829043a****</
KeyId>
    </Key>
  </Keys>
  <TotalCount>3</TotalCount>
  <PageNumber>1</PageNumber>
  <PageSize>10</PageSize>
  <RequestId>1050b8f1-b264-496d-a782-6299cbaf15f8</RequestId>
</KMS>
```

4.12 Encrypt

You can call this operation to encrypt plaintext with a specified CMK.

- **KMS uses the primary version of a specified CMK to encrypt data.**


- Only data which do not exceed 6 KB in size can be encrypted, such as RSA keys, database keys, or other sensitive user data.
- If you migrate encrypted data from one region to another, you can call this operation to encrypt the plaintext of the data key to be used for encrypting data in the previous region. By doing this, you can provide a ciphertext of the data key that is recognized by the new region and can be decrypted by calling the [Decrypt](#) API in the new region.

Request parameters

Parameter	Type	Required	Description
KeyId	String	Yes	The globally unique ID of the CMK. This parameter can also be specified as an alias bound to the CMK. For more information, see #unique_39 .
Plaintext	String	Yes	The plaintext to be encrypted which must be encoded in Base64.
EncryptionContext	String to string map	No	The JSON string of the key-value pair. If you specify this parameter here, it is also required when you call the <code>Decrypt</code> API operation. For more information, see #unique_40 .

Response parameters

Parameter	Type	Decription
-----------	------	------------

KeyId	String	<p>The globally unique ID of the CMK.</p> <div style="background-color: #f0f0f0; padding: 5px;">  Note: If an alias of the CMK is used as the value of the KeyId parameter, the ID of the CMK that the alias is bound to will be returned in the response. </div>
KeyVersionId	String	The ID of the key version used to encrypt plaintext . It is the primary key version of the specified CMK.
CiphertextBlob	String	The ciphertext of the data key encrypted with the primary CMK version.
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=Encrypt
&KeyId=<cmkid or aliasname>
&Plaintext=<data need encrypt>
&EncryptionContext={"Example":"Example"}
&<Common request parameters>
```

Sample responses

JSON format

```
//json response
{
  "KeyId": "your-key-id",
  "KeyVersionId": "2ab1a983-7072-4bbc-a582-584b5bd8ecf3",
  "CiphertextBlob": "CiphertextBlob",
  "RequestId": "475f1620-b9d3-4d35-b5c6-3fbbd941423d"
}
```

XML format

```
//xml response
<KMS>
  <KeyId>your-key-id</KeyId>
  <KeyVersionId>2ab1a983-7072-4bbc-a582-584b5bd8ecf3</KeyVersionId>
```

```
<CiphertextBlob>CiphertextBlob</CiphertextBlob>
<RequestId>475f1620-b9d3-4d35-b5c6-3fbdd941423d</RequestId>
</KMS>
```

4.13 GenerateDataKey

You can call this operation to generate a random data key, which can be used to encrypt local data.

This operation creates a random data key, encrypts the data key with the specified CMK, and returns the ciphertext and plaintext of the data key. You can use the plaintext of the data key to encrypt local data in services other than KMS in an offline manner. You must store the ciphertext of the data key when you store the encrypted data. You can obtain the plaintext of the data key by querying the `Plaintext` value in the response and the ciphertext of the data key by querying the `CiphertextBlob` value in the response.

The CMK that you specify in the request of this operation is only used to encrypt the data key and is independent of generation of the data key. KMS does not record or store the generated data key, so you need to implement persistence of the data key cipher.



Note:



We recommend that you encrypt local data in the following way:

- Call the `GenerateDataKey` API operation to obtain the plaintext and ciphertext of the data key.
- Use the plaintext of the data key that you can obtain by querying the `Plaintext` value in the response to encrypt local data in an offline manner and then clear the plaintext of the data key.
- Store the encrypted data along with the ciphertext of the data key that you can obtain by querying the `CiphertextBlob` value in the response.

We recommend that you decrypt local data in the following way:


- Call the `Decrypt` API 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.

Request parameters

Parameter	Type	Required	Description
KeyId	String	Yes	The globally unique ID of the CMK. This parameter can also be specified as an alias bound to the CMK. For more information, see #unique_39 .
KeySpec	String	No	<p>Specifies the length of the generated data key. AES_256 indicates 256-bit symmetric keys and AES_128 indicates 128-bit symmetric keys.</p> <p>Valid values: AES_256 and AES_128</p> <div style="background-color: #f0f0f0; padding: 10px;"> <p> Note:</p> <p>We recommend that you use the KeySpec or NumberOfBytes parameter to specify the length of data keys.</p> <ul style="list-style-type: none"> • If neither of the two parameters is specified, KMS generates 256-bit data keys. • If both of them are specified, the KeySpec value is ignored. </div>
NumberOfBytes	Integer	No	<p>Specifies the length of the generated data key. Unit: bytes.</p> <p>Valid values: 1 to 1024</p> <div style="background-color: #f0f0f0; padding: 10px;"> <p> Note:</p> <p>We recommend that you use the KeySpec or NumberOfBytes parameter to specify the length of data keys.</p> <ul style="list-style-type: none"> • If neither of the two parameters is specified, KMS generates 256-bit data keys. • If both of them are specified, the KeySpec value is ignored. </div>

Encryption Context	String to string map	No	The JSON string of the key-value pair. If you specify this parameter here, it is also required when you call the Decrypt API operation. For more information, see #unique_40.
---------------------------	-----------------------------	-----------	--

Response parameters

Parameter	Type	Description
KeyId	String	<p>The globally unique ID of the CMK.</p> <div style="background-color: #f0f0f0; padding: 5px;">  Note: If an alias of the CMK is used as the value of the KeyId parameter, the ID of the CMK that the alias is bound to will be returned in the response. </div>
KeyIdVersionId	String	The ID of the key version used to encrypt plaintext . It is the primary key version of the specified CMK.
Plaintext	String	The plaintext of the data key which is encoded in Base64.
CiphertextBlob	String	The ciphertext of the data key encrypted with the primary CMK version.

Examples

Sample requests

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=GenerateDataKey
&KeyId=<cmkid or aliasname>
&KeySpec=AES_256
&EncryptionContext={"Example":"Example"}
&<Common request parameters>
```

Sample responses

JSON format

```
//json response
{
  "CiphertextBlob": "CiphertextBlob",
  "KeyId": "599fa825-17de-417e-9554-bb032cc6****",
  "KeyVersionId": "2ab1a983-7072-4bbc-a582-584b5bd8ecf3",
  "Plaintext": "Base64 encoded plaintext",
  "RequestId": "7021b6ec-4be7-4d3c-8a68-1e85d4d515a0"
}
```

XML format

```
//xml response
<KMS>
  <CiphertextBlob>CiphertextBlob</CiphertextBlob>
  <KeyId>599fa825-17de-417e-9554-bb032cc6****</KeyId>
  <KeyVersionId>2ab1a983-7072-4bbc-a582-584b5bd8ecf3</KeyVersion
Id>
  <Plaintext>Base64 encoded plaintext</Plaintext>
  <RequestId>7021b6ec-4be7-4d3c-8a68-1e85d4d515a0</RequestId>
</KMS>
```

4.14 GenerateDataKeyWithoutPlaintext

You can call this operation to generate a random data key, which can be used to encrypt local data.

This operation creates a random data key, encrypts the data key with the specified CMK, and returns the ciphertext of the data key. This operation serves the same purpose as the [GenerateDataKey](#) API operation, but it does not return the plaintext of the data key.

Like in the [GenerateDataKey](#) API operation, the CMK that you specify in the request of this operation is only used to encrypt the data key and is independent of generation of the data key. KMS does not record or store the generated data key, so you need to implement persistence of the data key cipher.




Note:


This operation is suitable for a system that does not require the data key to encrypt data immediately, because you must call the [Decrypt](#) API operation to decrypt the data key cipher before using the data key to encrypt data.

This operation is also fit for a distributed system with different trust levels. The system stores data in different partitions based on the preset trust policy. A module creates different partitions and generates different data keys for these partitions


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 data key ciphertext of a partition first. After decrypting the data key ciphertext, modules on the control plane the data key plaintext to encrypt or decrypt data and then clear the data key plaintext from the memory. In such a system, the key provider does not obtain data key plaintext and only need to have the permissions call the `GenerateDataKeyWithoutPlaintext` API operation. The data producer or consumer does not generate new data keys and only need to have the permissions call the `Decrypt` API operation.

Request parameters

Parameter	Type	Required	Description
KeyId	String	Yes	The globally unique ID of the CMK. This parameter can also be specified as an alias bound to the CMK. For more information, see #unique_39 .
KeySpec	String	No	<p>Specifies the length of the generated data key. <code>AES_256</code> indicates 256-bit symmetric keys and <code>AES_128</code> indicates 128-bit symmetric keys.</p> <p>Valid values: <code>AES_256</code> and <code>AES_128</code></p> <div style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p> Note:</p> <p>We recommend that you use the <code>KeySpec</code> or <code>NumberOfBytes</code> parameter to specify the length of data keys.</p> <ul style="list-style-type: none"> • If neither of the two parameters is specified, KMS generates 256-bit data keys. • If both of them are specified, the <code>KeySpec</code> value is ignored. </div>

NumberOfBytes	Integer	No	<p>Specifies the length of the generated data key. Unit: bytes.</p> <p>Valid values: 1 to 1024</p> <div style="background-color: #f0f0f0; padding: 5px;">  Note: We recommend that you use the <code>KeySpec</code> or <code>NumberOfBytes</code> parameter to specify the length of data keys. <ul style="list-style-type: none"> • If neither of the two parameters is specified, KMS generates 256-bit data keys. • If both of them are specified, the <code>KeySpec</code> value is ignored. </div>
EncryptionContext	String to string map	No	<p>The JSON string of the key-value pair. If you specify this parameter here, it is also required when you call the <code>Decrypt</code> API operation. For more information, see #unique_40.</p>

Response parameters

Parameter	Type	Description
KeyId	String	<p>The globally unique ID of the CMK.</p> <div style="background-color: #f0f0f0; padding: 5px;">  Note: If an alias of the CMK is used as the value of the <code>KeyId</code> parameter, the ID of the CMK that the alias is bound to will be returned in the response. </div>
KeyVersionId	String	<p>The ID of the key version used to encrypt plaintext. It is the primary key version of the specified CMK.</p>

CiphertextBlob	String	The ciphertext of the data key encrypted with the primary CMK version.
-----------------------	---------------	---

Examples

Sample requests

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=GenerateDataKey
&KeyId=<cmkid or aliasname>
&KeySpec=AES_256
&EncryptionContext={"Example":"Example"}
&<Common request parameters>
```

Sample responses**JSON format**

```
//json response
{
  "CiphertextBlob": "CiphertextBlob",
  "KeyId": "599fa825-17de-417e-9554-bb032cc6****",
  "KeyVersionId": "2ab1a983-7072-4bbc-a582-584b5bd8ecf3",
  "RequestId": "7021b6ec-4be7-4d3c-8a68-1e85d4d515a0"
}
```

XML format

```
//xml response
<KMS>
  <CiphertextBlob>CiphertextBlob</CiphertextBlob>
  <KeyId>599fa825-17de-417e-9554-bb032cc6****</KeyId>
  <KeyVersionId>2ab1a983-7072-4bbc-a582-584b5bd8ecf3</KeyVersion
Id>
  <RequestId>7021b6ec-4be7-4d3c-8a68-1e85d4d515a0</RequestId>
</KMS>
```

4.15 Decrypt

You can call this operation to decrypt ciphertext.

The ciphertext to be decrypted can be generated with the following API operations:

- [GenerateDataKey](#)
- [Encrypt](#)
- [GenerateDataKeyWithoutPlaintext](#)

Request parameters

Parameter	Type	Required	Description
-----------	------	----------	-------------

CiphertextBlob	String	Yes	The ciphertext to be decrypted.
EncryptionContext	String	No	The JSON string of the key-value pair. If you specify this parameter in the Encrypt or GenerateDataKey API operation, it is also required when you call the Decrypt API operation. For more information, see #unique_40.

Response parameters

Parameter	Type	Description
KeyId	String	The globally unique ID of the CMK. It is the ID of the CMK used to decrypt ciphertext.
KeyVersionId	String	The ID of the key version used to decrypt ciphertext.
Plaintext	String	The decrypted plaintext.

Examples

Sample requests

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=Decrypt
&CiphertextBlob=<your ciphertextblob>
&EncryptionContext={"Example":"Example"}
&<Common request parameters>
```

Sample responses**JSON format**

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

```
}

```

XML format

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

4.16 CreateAlias

Creates an alias for a CMK.



Note:

- Each CMK can have multiple aliases, but each alias points to only one CMK.
- The alias name must be unique in one account and region.
- You can use [UpdateAlias](#) to update the mapping between the alias and the key.

Request parameters

Name	Type	Required	Description
AliasName	String	Yes	- The display name of the key. You can use the alias to call APIs such as <code>Encrypt</code> , <code>GenerateDataKey</code> , and <code>DescribeKey</code> . - Not including the prefix, the minimum length of an alias is 1 and the maximum length is 255. - The prefix <code>alias/</code> must be included.
KeyId	String	Yes	Globally unique identifier of the CMK.

Response parameters

Name	Type	Description
RequestId	String	ID of the request.

Examples

Request example

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=CreateAlias
&KeyId=<cmkid>
&AliasName=<alias/example>
&<Common Request Parameters>
```

Response example**JSON format**

```
//json response
{
  "RequestId": "53790170-1096-4ed2-9c3a-244d75c8740a"
}
```

XML format

```
//xml response
<KMS>
  <RequestId>53790170-1096-4ed2-9c3a-244d75c8740a</RequestId>
</KMS>
```

4.17 UpdateAlias

Associates an existing alias with a different CMK.

Request parameters

Name	Type	Required	Description
------	------	----------	-------------

AliasName	String	Yes	<p>The name of the alias to be modified.</p> <ol style="list-style-type: none"> 1. The prefix <code>alias/</code> must be included. 2. Excluding the prefix, the minimum length of an alias is 1 and the maximum length is 255.
KeyId	String	Yes	Globally unique identifier of the CMK.

Response parameters

Name	Type	Description
RequestId	String	The ID of this request.

Examples

Request example

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=UpdateAlias
&AliasName=<alias name>
&KeyId=<target keyid>
&<Common Request Parameters>
```

Response example**JSON format**

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

XML format

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

```
</KMS>
```

4.18 DeleteAlias

Deletes the specified alias.

Request parameters

Name	Type	Required	Description
AliasName	String	Yes	<p>The alias to be deleted.</p> <ul style="list-style-type: none"> • The prefix <code>alias/</code> must be included. • Excluding the prefix, the minimum length of an alias is 1 and the maximum length is 255.

Response parameters

Name	Type	Description
RequestId	String	The ID of this request.

Examples

Request example

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=DeleteAlias
&AliasName=<alias name>
&<Common Request Parameters>
```

Response example

JSON format

```
//json response
{
    "RequestId": "4c8ae23f-3a42-6791-a      4ba-1faa77831c28"
}
```

XML format

```
//xml response
<KMS>
```

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

4.19 ListAliases

Gets a list of all aliases in the caller' s account and region.

Request parameters

Name	Type	Required	Description
PageNumber	Integer	No	The current page number. Valid value: an integer greater than 0. The default value is 1.
PageSize	Integer	No	The number of items on each page . Valid value: an integer between 0 and 101. The default value is 10. The default is 10.

Response parameters

Name	Type	Description
AliasName	String	The unique identifier of an alias.
AliasArn	String	The ARN of the alias.
KeyId	String	The CMK associated with an alias.
TotalCount	Integer	The total number of items returned.
PageNumber	Integer	The current page number.
PageSize	Integer	The number of items on each page.

Examples

Request example

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

&<Common Request Parameters>

Response example

JSON format

```
//json response
{
  "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"
}
```

XML format

```
//xml response
<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>
```

4.20 ListAliasesByKeyId

Lists all aliases associated with the CMK.

Request parameters

Name	Type	Required	Description
------	------	----------	-------------

PageNumber	Integer	No	The current page number. Valid value: An integer greater than 0. The default value is 1.
PageSize	Integer	No	The number of items on each page. Valid value: An integer between 0 and 101. The default value is 10.
KeyId	String	Yes	Globally unique identifier of the CMK.

Response parameters

Name	Type	Description
AliasName	String	The unique identifier of an alias.
AliasArn	String	The ARN of the alias.
KeyId	String	The CMK queried.
TotalCount	Integer	The total number of items returned.
PageNumber	Integer	The current page number.
PageSize	Integer	The number of items on each page.

Examples

Request example

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

Response example**JSON format**

```
//json response
{
    "Aliases": {
```

```

        "Alias": [
            {
                "AliasName": "alias/ExampleAlias1",
                "KeyId": "08c33a6f-4e0a-4a1b-a3fa-7ddfa1d4xxxx",
                "AliasArn": "acs:kms:cn-hangzhou:123456:alias/ExampleAlias1"
            }
        ],
        "TotalCount": 1,
        "PageNumber": 1,
        "PageSize": 10,
        "RequestId": "1b57992c-834b-4811-a889-f8bac1ba0353"
    }

```

XML format

```

//xml response
<KMS>
    <Aliases>
        <Alias>
            <AliasName>alias/ExampleAlias1</AliasName>
            <KeyId>08c33a6f-4e0a-4a1b-a3fa-7ddfa1d4xxxx</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>

```

4.21 TagResource

You can call this operation to add or modify the tags of a CMK.

Description

A CMK can have more than one tag. A tag is defined by a pair of tag key and tag value.



Note:

You can add up to 10 tags for each CMK.

For more information about tag keys and tag values, see [Tag description](#).

Request format


```
KeyId="string"&Tags=[{ "TagKey": "string","TagValue": "string"} ]
```

Request parameters

Parameter	Type	Required ?	Example	Description
KeyId	String	Yes	external key id	The GUID of the key.
Tags	JSON	Yes	[{"TagKey": "Project", "TagValue": "Test"}]	<p>One or more tags. Format: tag array. Each Tag consists of a pair of:</p> <ul style="list-style-type: none"> TagKey: the tag key. TagValue: the tag value. <p>For more information about tag keys and tag values, see Tag description.</p>

Tag description

Parameter	Type	Required ?	Example	Description
TagKey	String	Yes	Project	<p>The tag key.</p> <p>It must be 1 to 128 characters in length.</p> <p>It can contain uppercase and lowercase letters, digits, forward slashes (/), underscores (_), hyphens (-), periods (.), plus signs (+), equal signs (=), at signs (@), and semicolons (:).</p>

Parameter	Type	Required ?	Example	Description
TagValue	String	Yes	Test	<p>The tag value.</p> <p>It can be up to 256 characters in length.</p> <p>It can contain uppercase and lowercase letters, digits, forward slashes (/), underscores (_), hyphens (-), periods (.), plus signs (+), equal signs (=), at signs (@), and semicolons (:).</p> <div style="background-color: #f0f0f0; padding: 5px;">  Note: Tag keys of a CMK must be unique. When you call TagResource and specify an existing tag key, the current specified tag value will overwrite the original tag value. </div>

Sample requests

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=TagResource
&KeyId=<external key id>
&Tags=<tags>
&<Common request parameters>
```

Response parameters

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

Sample responses

JSON format

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

XML format

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

4.22 UntagResource

You can call this operation to delete the specified tags of a CMK.

Request format

```
KeyId="string"&TagKeys=["tagkey1","tagkey2"]
```

Request parameters

Parameter	Type	Required?	Example	Description
KeyId	String	Yes	external key id	The GUID of the key.
TagsKeys	JSON	Yes	["tagkey1","tagkey2"]	One or more tag keys. Only the tag keys are required, and tag values are not required. Format: string array. Each string in the array must be 1 to 128 characters in length.

Sample requests

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=UntagResource
&KeyId=<external key id>
&TagKeys=<tagkeys>
```

```
&<Common request parameters>
```

Response parameters

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

Sample responses

JSON format

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

XML format

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

4.23 ListResourceTags

You can call this operation to list the tags of a CMK.

Request format

```
KeyId="string"
```

Request parameters

Parameter	Type	Required ?	Example	Description
KeyId	String	Yes	key id	The GUID of the key.

Sample requests

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=ListResourceTags
&KeyId=<key id>
```

&<Common request parameters>

Response parameters

Parameter	Type	Example	Description
RequestId	String	4162a6af -bc99- 40b3-a552- 89dcc8aaf7c8	The request ID.
TagKey	String	Project	The tag key.
TagValue	String	Test	The tag value.

Sample responses

JSON format

```
{
  "RequestId": "4162a6af-bc99-40b3-a552-89dcc8aaf7c8",
  "Tags": {
    "Tag": [
      {
        "KeyId": "33caea95-c3e5-4b3e-a9c6-cec76e4eaf83",
        "TagKey": "Project",
        "TagValue": "Test"
      }
    ]
  }
}
```

XML format

```
<KMS>
  <RequestId>0f900dad-c747-4170-9962-1bfb6b31436b</RequestId>
  <Tags>
    <Tag>
      <KeyId>33caea95-c3e5-4b3e-a9c6-cec76e4eaf83</KeyId>
      <TagKey>Project</TagKey>
      <TagValue>Test</TagValue>
    </Tag>
  </Tags>
</KMS>
```

4.24 DescribeRegions

Returns available regions for the specified account.

Request parameters

Name	Type	Required	Description
------	------	----------	-------------

Action	String	Yes	Action interface name. Value: DescribeRegions.
---------------	---------------	------------	---

Response parameters

Name	Type	Description
RegionId	String	Region ID.

Examples

Request example

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

Response example

JSON format

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

XML format

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

</KMS>

4.25 DescribeKeyVersion

You can this operation to query metadata information of a specified key version.

Request parameters

Parameter	Type	Required	Description
KeyId	String	Yes	The globally unique ID of the CMK.
KeyVersionId	String	Yes	The ID of the key version.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
KeyVersion	<i>KeyVersion</i>	The array that consists of KeyVersion data.

KeyVersion

Parameter	Type	Decription
KeyId	String	The globally unique ID of the CMK.
KeyVersionId	String	The ID of the key version.
CreationDate	Timestamp	The time when the CMK was created. The time is displayed in UTC.

Examples

Sample requests

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=DescribeKeyVersion
&KeyId=<cmkid>
&KeyVersionId=<key version id>
&<Common request parameters>
```

Sample responses

JSON format

```
//json response
{
  "KeyVersion": {
    "KeyId": "0b30658a-ed1a-4922-b8f7-a673ca9c440b",
    "KeyVersionId": "6a69c763-388a-4708-9fc0-4322266bf2d0",
    "CreationDate": "2019-08-06T10:17:04Z"
  },
  "RequestId": "80b4eac8-9f51-452a-a859-0c9b06b283c1"
}
```

XML format

```
//xml response
<KMS>
  <KeyVersion>
    <KeyId>0b30658a-ed1a-4922-b8f7-a673ca9c440b</KeyId>
    <KeyVersionId>2ab1a983-7072-4bbc-a582-584b5bd8ecf3</KeyVersionId>
    <CreationDate>2016-03-25T10:40:47Z</CreationDate>
  </KeyVersion>
  <RequestId>b0ae52a2-33a4-43de-b68c-849f81d09f5d</RequestId>
</KMS>
```

4.26 ListKeyVersions

You can call this operation to list all key versions of a specified CMK.

Request parameters

Parameter	Type	Required	Description
KeyId	String	Yes	The globally unique ID of the CMK.
PageSize	Integer	No	The number of entries to return on each page. Valid values: 0 to 101. Default value: 10.
PageNumber	Integer	No	The number of the page to return. Pages start from page 1. Default value: 1.

Response parameters

Parameter	Type	Description
-----------	------	-------------

RequestId	String	The ID of the request.
PageSize	Integer	The number of entries returned per page.
PageNumber	Integer	The page number of the returned page.
TotalCount	Integer	The total number of returned key versions.
KeyVersions	<i>KeyVersion</i>	The array that consists of KeyVersion data.

Examples

Sample requests

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

Sample responses

JSON format

```
//json response
{
  "RequestId": "1e76f572-4a9b-4be2-a296-ae3069318070",
  "KeyVersions": {
    "KeyVersion": [
      {
        "KeyId": "0b30658a-ed1a-4922-b8f7-
a673ca9c440b",
        "KeyVersionId": "1e3304fd-68ac-4d5b-
8886-ae5f01a1af61",
        "CreationDate": "2019-08-06T10:22:03Z"
      },
      {
        "KeyId": "0b30658a-ed1a-4922-b8f7-
a673ca9c440b",
        "KeyVersionId": "2ab1a983-7072-4bbc-
a582-584b5bd8ecf3",
        "CreationDate": "2019-08-06T10:19:18Z"
      },
      {
        "KeyId": "0b30658a-ed1a-4922-b8f7-
a673ca9c440b",
        "KeyVersionId": "6a69c763-388a-4708-
9fc0-4322266bf2d0",
        "CreationDate": "2019-08-06T10:17:04Z"
      }
    ]
  },
  "TotalCount": 3,
  "PageNumber": 1,
}
```



```
    "PageSize": 10
  }
```

XML format

```
//xml response
<KMS>
  <RequestId>f71204c4-53cd-4eea-b405-653ba2db7e86</RequestId>
  <KeyVersions>
    <KeyVersion>
      <KeyId>0b30658a-ed1a-4922-b8f7-a673ca9c440b</
KeyId>
      <KeyVersionId>1e3304fd-68ac-4d5b-8886-
ae5f01a1af61</KeyVersionId>
      <CreationDate>2019-08-06T10:22:03Z</CreationDa
te>
    </KeyVersion>
    <KeyVersion>
      <KeyId>0b30658a-ed1a-4922-b8f7-a673ca9c440b</
KeyId>
      <KeyVersionId>2ab1a983-7072-4bbc-a582-
584b5bd8ecf3</KeyVersionId>
      <CreationDate>2019-08-06T10:19:18Z</CreationDa
te>
    </KeyVersion>
    <KeyVersion>
      <KeyId>0b30658a-ed1a-4922-b8f7-a673ca9c440b</
KeyId>
      <KeyVersionId>6a69c763-388a-4708-9fc0-
4322266bf2d0</KeyVersionId>
      <CreationDate>2019-08-06T10:17:04Z</CreationDa
te>
    </KeyVersion>
  </KeyVersions>
  <TotalCount>3</TotalCount>
  <PageNumber>1</PageNumber>
  <PageSize>10</PageSize>
</KMS>
```


4.27 UpdateRotationPolicy

You can call this operation to update a key rotation policy.

When automatic key rotation is enabled, KMS automatically creates a new key version after the preset rotation period from the last rotation task and sets it as the primary key version. No automatic rotation policy can be defined in the following cases:

- The specified CMK is a key managed by KMS for other cloud services.
- The specified CMK is a BYOK (an external key imported into KMS).
- The specified CMK is not in the Enabled state.

Request parameters

Parameter	Type	Required	Description
KeyId	String	Yes	The globally unique ID of the CMK.
EnableAutomaticRotation	Boolean	Yes	Specifies whether to enable automatic key rotation. Valid values: true and false.
RotationInterval	String	No	<p>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.</p> <div style="background-color: #f0f0f0; padding: 10px;"> <p> Note:</p> <ul style="list-style-type: none"> • When EnableCustomization is set to true, this parameter is required. • When EnableCustomization is set to false, this parameter is ignored. </div>

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://kms.cn-hangzhou.aliyuncs.com/?Action=UpdateRotationPolicy
&KeyId=<key id>
&EnableAutomaticRotation=true
&RotationInterval=30d
&<Common request parameters>
```

Sample responses**JSON format**

```
//json response
{
    "RequestId": "80b4eac8-9f51-452a-a859-0c9b06b283c1"
```

```
}
```

XML format

```
//xml response  
<KMS>  
  <RequestId>b0ae52a2-33a4-43de-b68c-849f81d09f5d</RequestId>  
</KMS>
```