Alibaba Cloud KeyManagementService

API Reference

Issue: 20190819

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, consequential, 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 content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, 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 the Alibaba Cloud website, product programs, or content 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.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information 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.
	This warning information 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 restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click OK.
`Courier font`	It is used for commands.	Run the `cd / d C :/ windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

Style	Description	Example
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich {stand | slave}`

Contents

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. #unique_5
2. #unique_6
3. #unique_7
4. #unique_8

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-zhangjiako u.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
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, #unique_10), must be specified. Each operation must include the #unique_6 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 #unique_8.
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
& AccessKeyI  d = testid
& Signature = YlrFhyqDZQ  1ThNYARrv3  Ptaxqf ****
& SignatureM  ethod = HMAC - SHA1
& Timestamp = 2016 - 03 - 25T09 : 36 : 58Z
& SignatureV  ersion = 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 - 298cc6c944  47 </
 RequestId >
<!— Returned   results -->
</ KMS >
```

`JSON` **example**

```
{
" RequestId ": " 284b2b80 - 9b17 - 4546 - a093 - adfbae512a  54 "
}
```

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:

```
StringToSi  gn =
HTTPMethod  + “&” +
percentEnc  ode (“/”) + ”&” +
percentEnc  ode ( Canonicali  zedQuerySt  ring )
```

  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 sting 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
& SignatureV  ersion = 1 . 0
& Format = json
& Version = 2016 - 01 - 20
& AccessKeyI  d = testid
& SignatureM  ethod = HMAC - SHA1
& Timestamp = 2016 - 03 - 28T03 : 13 : 08Z
```

`Canonicali zedQuerySt ring` is:

```
 AccessKeyI  d = testid & Action = CreateKey & Format = json &
 SignatureM  ethod = HMAC - SHA1 & SignatureV  ersion = 1 . 0 &
 Timestamp = 2016 - 03 - 28T03 % 3A13 % 3A08Z & Version = 2016 - 01 -
 20
```

`StringToSi gn` is:

```
 GET &% 2F & AccessKeyI  d % 3Dtestid & Action % 3DCreateKe  y &
 Format % 3Djson & SignatureM  ethod % 3DHMAC - SHA1 & SignatureV
 ersion % 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 / OdVWMTmNGa  gvWlljdAJ7  Itsew =
```

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

```
 https :// kms . cn - hangzhou . aliyuncs . com /? Action = CreateKey
& SignatureV  ersion = 1 . 0
& Format = json
& Version = 2016 - 01 - 20
& AccessKeyI  d = F585 ******** APMU
& SignatureM  ethod = HMAC - SHA1
& Timestamp = 2016 - 03 - 28T03 : 13 : 08Z
& Signature = 41wk2SSX1G  Jh7fwnc5eq  OfiJPF ****
```

1.5 Response structure

After you make an API request, an HTTP status code is returned. 2xx indicates that the request has succeeded; 4xx or 5xx indicates that an error occurred while processing the request. The response text is JSON formatted.

If you make the API request by using tools that are not provided by Alibaba Cloud, you can customize the response format in the request parameters.

In the example responses we present as follows, we use line breaks to separate the original whole line of text for readability.

Successful response example

`XML` example:

```
<?  xml   version =" 1 . 0 "  encoding =" UTF - 8 "? >
<! -- Result   Root   Node -->
< InterfaceN  ame + Response >
    <! --  Return   Request   Tag  -->
 < RequestId > 4C467B38 - 3910 - 447D - 87BC - AC049166F2  16 </
 RequestId >
    <! --  Return   Result   Data  -->
</ InterfaceN  ame + Response >
```

`JSON` example:

```
{
    " RequestId ": " 4C467B38 - 3910 - 447D - 87BC - AC049166F2  16 ",
    /*  Return   Result   Data  */
}
```

Unsuccessful response example

After an error is encountered in an interface call, no result data will be returned. The caller can locate the error cause according to the error code and Public error codes corresponding to each interface.

When an error occurs in a call, the HTTP request will return an HTTP status code of 4xx or 5xx. The returned message body contains the specific error code and error message. The message body also contains a globally unique RequestId and the requested HostId. If the caller cannot find the cause of the error, he can contact AliCloud customer service and provide the HostId and RequestId to help us solve the problem as quickly as possible.

`XML` example (request expiration)

```
< KMS >
< HttpStatus > 400 </ HttpStatus >
< Code > IllegalTim  estamp </ Code >
< Message > The   input   parameter  " Timestamp "  that   is
 mandatory   for   processing   this   request   is   not   supplied .
 </ Message >
< RequestId > 3b237773 - bc2c - 4bea - 95fc - 319a1a5baa  68 </
 RequestId >
 </ KMS >
```

```
```

`JSON` example (request expiration)

```
{
" HttpStatus ":  400
" Code ": " IllegalTim  estamp "
" Message ": " The   input   parameter  " Timestamp "  that   is
 mandatory   for   processing   this   request   is   not   supplied
 ."
" RequestId ": " e85db688 - a2d3 - 44ca - 9790 - 4259f59e90  d8 "
}
```

Public error codes

Error code	Error message	HTTP status code
InternalFailure	Internal Failure.	500
SerivceUnavailableTemporary	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.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

Error code	Error message	HTTP status code
Forbidden.InDebtOverdue	Current user is indebted Overdue.	403
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
Rejected.StateModifiedFailed	Keystate modified failed.	409

Error code	Error message	HTTP status code
Rejected.Disabled	The request was rejected because the key state is Disabled.	409
Rejetced.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 Impact of CMK states on API call

In Key Management Service (KMS), each Customer Master Key (CMK) has three states: Enabled, Disabled, and PendingDeletion. If the key is an external key (when its Origin is EXTERNAL in KeyMetaData), it may also be in the PendingImport state.

A new CMK is usually in the Enabled state by default. When creating a new external key, however, it is in the PendingImport state.

Only CMKs in the Enabled state can be used for encryption or decryption. Other APIs may return different responses depending on the key state.

CMKs in the PendingDeletion state are permanently deleted once the pre-deletion time runs out.

he following table shows key states and the expected responses of API calls.

Expected responses	HttpStatusCode
Success	200
Rejected.Enabled	409
Rejected.Disabled	409
Rejected.PendingDeletion	409
Rejected.PendingImport	409
Rejected.StateModifiedFailed	409

API	Enabled	Disabled	PendingDeletion	PendingImport
CreateKey	Success	Success	Success	Success
GenerateDataKey	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

API	Enabled	Disabled	PendingDeletion	PendingImport
DescribeKey	Success	Success	Success	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

Special API

UpdateAlias

- It is affected only by the state of the “target key”, not the state of the “original key”.
- If the “target key” is in the PendingDeletion state, Rejected.PendingDeletion is returned. If not, Success is returned.

Exclusive API for the External Key

API	Enabled	Disabled	PendingDeletion	PendingImport
GetParametersForImport	Success	Success	Success	Success
ImportKeyMaterial	Success	Success	Rejected.StateModifiedFailed	Success

API	Enabled	Disabled	PendingDeletion	PendingImport
DeleteKeyMaterial	Success	Success	Success	Success

3 List of operations by function

This topic lists the APIs in KMS. For more information, see related documentation.

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 APIs

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

API	Description
#unique_10	Creates a CMK. You can also choose to let KMS generate key material, or upload your own key material. CreateKey is the first step to create a BYOK (Bring Your Own Key).
#unique_17	Obtains the key material, which is the second step to create a BYOK.
#unique_18	Imports the key material to the CMK, which is the final step to create a BYOK.
#unique_19	Modifies the key status to enabled.
#unique_20	Modifies the key status to disabled.
#unique_21	Schedules key deletion. The key status changes to PendingDeletion. A CMK in the PendingDeletion state will be deleted when the scheduled period expires.
#unique_22	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.
#unique_23	Deletes the key material of a CMK. You can directly delete the key material of BYOK. After the key material is deleted, the BYOK is in the PendingImport state.

API	Description
#unique_24	Queries detailed information about a specified CMK.
#unique_25	Lists all CMKs within the current region that belong to the current Alibaba Cloud account.

Key operation APIs

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

API	Description
#unique_26	Uses a specified CMK to encrypt data. The API is used for online encryption of data of no more than 6 KB.
#unique_27	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.
#unique_28	Decrypts ciphertexts generated with the Encrypt or GenerateDataKey API. You do not need to specify the CMK for decryption.

Alias management APIs

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

API	Description
#unique_29	Creates an alias and binds it to a CMK.
#unique_30	Binds a specified alias to the new CMK.
#unique_31	Deletes a specified alias.
#unique_32	Lists all aliases of an Alibaba Cloud account in the current region.

API	Description
#unique_33	Lists all aliases bound to the specified CMK.

Tag management APIs

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

API	Description
#unique_34	Adds or modifies the tags of a CMK.
#unique_35	Deletes the specified tag of a CMK.
#unique_36	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 amout 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 #unique_27.

Request parameters

Parameter	Type	Required	Description
Origin	String	No	The source of the key material for the CMK to create. Valid values: Aliyun_KMS and EXTERNAL. Note: The default value is Aliyun_KMS. The value of this parameter is case sensitive. If you select EXTERNAL, you must #unique_39.
Description	String	No	The description of the CMK to create . The description must be 0 to 8,192 characters in length .

KeyUsage	String	No	The purpose of the CMK to create. Default value: ENCRYPT/DECRYPT
ProtectionLevel	String	No	The protection level of the CMK to create. Valid value: SOFTWARE and HSM. When this parameter is set to HSM: · 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. Note: The default value is SOFTWARE. The value of this parameter is case sensitive.

Response parameters

Parameter	Type	Description
KeyMetadata	KeyMetadata parameters	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 #unique_40.
KeyUsage	String	The purpose of the CMK. Default value: ENCRYPT/DECRYPT.
DeleteDate	Timestamp	The scheduled period before the CMK is deleted. The time is displayed in UTC. · 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
& Descriptio  n =< your   key   descriptio  n >
& KeyUsage = ENCRYPT / DECRYPT
& Origin =< key   origin ,  default   Aliyun_KMS >
& Protection  Level = HSM
&< Common   request   parameters >
```

Sample responses

`JSON` format

```
// json   response
{
        " KeyMetadat  a ": {
                " CreationDa  te ": " 2016 - 03 - 25T10 : 42 : 40Z ",
                " Descriptio  n ": " key   descriptio  n   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 ",
                " MaterialEx  pireTime ":"",
                " Protection  Level ":" HSM "
        },
        " RequestId ": " 3455b9b4 - 95c1 - 419d - b310 - db6a53b09a
 39 "
}
```

`XML` format

```
// xml   response
< KMS >
 < KeyMetadat  a >
        < CreationDa  te > 2016 - 03 - 25T10 : 40 : 47Z </ CreationDa
 te >
        < Descriptio  n > key   descriptio  n   example </ Descriptio
 n >
        < 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 >
        < MaterialEx  pireTime ></ MaterialEx  pireTime >
        < Protection  Level > HSM </ Protection  Level >
```

```
 </ KeyMetadat  a >
 < RequestId > 6cb4bf6b - d9c9 - 4660 - af5f - 2328378e72  57 </
 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 #unique_18 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 `Origin` must be `EXTERNAL`.
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 #unique_18 request.
ImportToken	String	The identifier of the CMK to use in a subsequent #unique_18 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 =
 GetParamet  ersForImpo  rt
& KeyId =< external   key   id >
& WrappingAl  gorithm =< key   material   encryption   algorithm >
& WrappingKe  ySpec = RSA_2048
&< Common   Request   Parameters >
```

Response example

`JSON` format

```
// json   response
{
        " ImportToke  n ":" ImportToke  n ",
        " PublicKey ":" PublicKey ",
        " KeyId ":" KeyId ",
        " TokenExpir  eTime ":" 2018 - 01 - 25T00 : 01 : 02Z ",
        " RequestId ":" 8cdf51fd - bcd6 - d79a - 0ef4 - e52c9b5466  dc
 "
}
```

`XML` format

```
// xml   response
```

```
< KMS >
  < ImportToke  n > ImportToke  n </ ImportToke  n >
  < PublicKey > PublicKey </ PublicKey >
  < KeyId > KeyId </ KeyId >
  < TokenExpir  eTime > 2018 - 01 - 25T00 : 01 : 02Z </ TokenExpir
 eTime >
  < RequestId > 8cdf51fd - bcd6 - d79a - 0ef4 - e52c9b5466  dc </
 RequestId >
</ KMS >
```

4.3 ImportKeyMaterial

When you call #unique_10 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 #unique_24.
- Before calling this API, call #unique_17 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 `GetParamet ersForImpo rt`.
KeyMateria lExpireUnix	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 =
 ImportKeyM  aterial
& EncryptedK  eyMaterial =< your   encrypted   key   material >
& ImportToke  n =< import   token   from   GetParamet  ersForImpo  rt
 >
& KeyMateria  lExpireUni  x = 1518307200
&< Common   Request   Parameters >
```

Response example

`JSON` format

```
// json   response
{
        " RequestId ":" ec1017cf - ead4 - f3ca - babc - c3b34f3dbe  cb
 "
}
```

`XML` format

```
// xml   response
```

```
< KMS >
  < RequestId > ec1017cf - ead4 - f3ca - babc - c3b34f3dbe  cb </
 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 - 639dd4fcc2  07 "
}
```

`XML` format

```
// xml   response

< KMS >
    < RequestId > efb1cbbd - a093 - 4278 - bc03 - 639dd4fcc2  07 </
 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 - 472fb2705c  62 "
}
```

`XML` format

```
// xml   response
< KMS >
    < RequestId > 2fe70ce2 - 3303 - 4fd6 - b3ac - 472fb2705c  62 </
 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 #unique_20 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 #unique_22 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 PendingDeletion 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 =
 ScheduleKe  yDeletion
& KeyId =< your - key - id >
& PendingWin  dowInDays =[ 7 ~ 30 ]
&< Common   Request   Parameters >
```

Response example

`JSON` format

```
// json   response
{
" RequestId ": " 52ac67cb - 3d3d - 4ada - b4e2 - 7047660d3c  e9 "
}
```

`XML` format

```
// xml   response
< KMS >
    < RequestId > 52ac67cb - 3d3d - 4ada - b4e2 - 7047660d3c  e9 </
 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 =
 CancelKeyD  eletion
```

```
& KeyId =< cmkid >
&< Common   Request   Parameters >
```

Response example

`JSON` format

```
// json   response
{
" RequestId ": " 3da5b8cc - 8107 - 40ac - a170 - 793cd181d7  b7 "
}
```

`XML` format

```
// xml   response
< KMS >
    < RequestId > 3da5b8cc - 8107 - 40ac - a170 - 793cd181d7  b7 </
 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 =
 DeleteKeyM  aterial
& KeyId =< external   key   id >
&< Common   Request   Parameters >
```

Response example

`JSON` format

```
// json   response
{
        " RequestId ": " 4162a6af - bc99 - 40b3 - a552 - 89dcc8aaf7
 c8 "
}
```

`XML` format

```
// xml   response
< KMS >
  < RequestId > 4162a6af - bc99 - 40b3 - a552 - 89dcc8aaf7  c8 </
 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_49.

Response parameters

Parameter	Type	Description
KeyMetadata	KeyMetadata parameters	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 #unique_40.
KeyUsage	String	The purpose of the CMK.
DeleteDate	Timestamp	The scheduled date to delete CMK. For more information, see #unique_21. 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 =
 DescribeKe  y
& KeyId =< your - key - id >
&< Common   request   parameters >
```

Sample responses

`JSON` format

```
// json   response
{
        " KeyMetadat  a ": {
                " CreationDa  te ": " 2016 - 03 - 25T10 : 42 : 40Z ",
                " Descriptio  n ": " key   descriptio  n   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 ",
                " MaterialEx  pireTime ":"",
                " Protection  Level ":" HSM "
        },
        " RequestId ": " 3455b9b4 - 95c1 - 419d - b310 - db6a53b09a
 39 "
}
```

`XML` format

```
// xml   response
< KMS >
 < KeyMetadat  a >
        < CreationDa  te > 2016 - 03 - 25T10 : 40 : 47Z </ CreationDa
 te >
        < Descriptio  n > key   descriptio  n   example </ Descriptio
 n >
        < 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 >
        < MaterialEx  pireTime ></ MaterialEx  pireTime >
        < Protection  Level > HSM </ Protection  Level >
 </ KeyMetadat  a >
 < RequestId > 6cb4bf6b - d9c9 - 4660 - af5f - 2328378e72  57 </
 RequestId >
```

```
</ KMS >
```

4.10 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 - 1ff3444dfd
 8b "
}
```

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 - 6299cbaf15  f8
 </ RequestId >
</ KMS >
```

4.11 Encrypt

Encrypts plaintext into ciphertext by using a CMK.

- You can encrypt up to 6 KB of arbitrary data, such as an RSA key, a database password, or other sensitive information.
- To move encrypted data from one region to another, you can use this API to encrypt in the new region the plaintext data key that was used to encrypt the data in the original region. An encrypted data key is generated in the new region. You can #unique_28 the data key in the new region.

Request parameters

Name	Type	Required	Description
KeyId	String	Yes	Globally unique identifier of CMK. You can user aliases to call this API. For more information, see #unique_49.
Plaintext	String	Yes	Plaintext to be encrypted. The value is Base64-encoded.
EncryptionContext	String to string map	No	The JSON string of key-value pairs. If you specify this parameter, you need to provide the same parameter when you call `Decrypt`. For more information, see #unique_52.

Response parameters

Name	Type	Description

KeyId	String	Globally unique identifier of CMK. If you use an alias in request, the CMK ID of the alias is returned.
CiphertextBlob	String	Encrypted ciphertext.

Examples

Request example

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

Response example

`JSON` format

```
// json   response
{
 " KeyId ": " your - key - id ",
 " Ciphertext  Blob ": " Ciphertext  Blob ",
 " RequestId ": " 475f1620 - b9d3 - 4d35 - b5c6 - 3fbdd94142  3d "
}
```

`XML` format

```
// xml   response
< KMS >
 < KeyId > your - key - id </ KeyId >
 < Ciphertext  Blob > Ciphertext  Blob </ Ciphertext  Blob >
 < RequestId > 475f1620 - b9d3 - 4d35 - b5c6 - 3fbdd94142  3d </
 RequestId >
</ KMS >
```

4.12 GenerateDataKey

Returns a data encryption key that you can use in your application to encrypt data locally.

This operation returns a plaintext copy of the data key in the `Plaintext` field of the response, and an encrypted copy of the data key in the `Ciphertext  Blob` field.

Note:

- We recommend that you use the following pattern to encrypt data locally in your application:
  - Use this operation (`GenerateDa taKey`) to get a data encryption key.
  - Use the plaintext data encryption key (returned in the `Plaintext` field of the response) to encrypt data locally, then erase the plaintext data key from memory.
  - Store the encrypted data key (returned in the `Ciphertext Blob` field of the response) alongside the locally encrypted data.
- To decrypt data locally:
  - Use the #unique_28 operation to decrypt the encrypted data key returned by `Ciphertext Blob` into a `Plaintext` copy of the data key.
  - Use the `Plaintext` data key to decrypt data locally, then erase the `Plaintext` data key from memory.
- When neither `KeySpec` nor `NumberOfBy tes` is specified, the default value of `KeySpec` is AES_256.
- When both `NumberOfBy tes` and `KeySpec` are specified, `NumberOfBy tes` prevails.

Request parameters

Name	Type	Required	Description
KeyId	String	Yes	Globally unique identifier of CMK. You can user aliases to call this API. For more information, see #unique_49.
KeySpec	String	No	The length and type of the data key. AES_256 refers to a 256-bit symmetric key. AES_128 refers to a 128-bit symmetric key.

NumberOfBytes	Integer	No	The length of the data key in bytes. Valid value: 1 to 1, 024.
EncryptionContext	String to string map	No	The json sting of key-value pairs. If you specify this parameter, you need to provide the same parameter when you call `Decrypt`. For more information, see #unique_52.

Response parameters

Name	Type	Description
KeyId	String	Globally unique identifier of CMK. If you use an alias in request, the CMK ID of the alias is returned.
Plaintext	String	Base64-encoded plaintext key.
CiphertextBlob	String	Encrypted data key.

Examples

Request example

```
 https :// kms . cn - hangzhou . aliyuncs . com /? Action =
 GenerateDa  taKey
& KeyId =< cmkid   or   aliasname >
& KeySpec = AES_256
& Encryption  Context ={" Example ":" Example "}
&< Common   Request   Parameters >
```

Response example

`JSON` format

```
// json   response
{
        " Ciphertext  Blob ": " Ciphertext  Blob ",
        " KeyId ": " 599fa825 - 17de - 417e - 9554 - bb032cc6 ****",
        " Plaintext ": " Base64   encoded   plaintext ",
```

```
        " RequestId ": " 7021b6ec - 4be7 - 4d3c - 8a68 - 1e85d4d515
 a0 "
}
```

`XML` format

```
// xml   response
< KMS >
        < Ciphertext  Blob > Ciphertext  Blob </ Ciphertext  Blob >
        < KeyId > 599fa825 - 17de - 417e - 9554 - bb032cc6 ****</
 KeyId >
        < Plaintext > Base64   encoded   plaintext </ Plaintext >
        < RequestId > 7021b6ec - 4be7 - 4d3c - 8a68 - 1e85d4d515  a0
 </ RequestId >
</ KMS >
```

4.13 Decrypt

Decrypts the ciphertext in `Ciphertext Blob`.

Ciphertext can be generated by the following APIs:

- #unique_27
- #unique_26

Request parameters

Name	Type	Required	Description
CiphertextBlob	String	Yes	Ciphertext to be decrypted.
EncryptionContext	String	No	JSON string of key-value pairs. If you specify this parameter in the `Encrypt` or `GenerateDataKey` API, you need to provide the same parameter before you can decrypt the ciphertext. For more information, see #unique_52.

Response parameters

Name	Type	Description
KeyId	String	Globally unique identifier of CMK. ID of the CMK used by the encrypted ciphertext.
Plaintext	String	Decrypted plaintext.

Examples

Request example

```
 https :// kms . cn - hangzhou . aliyuncs . com /? Action = Decrypt
& Ciphertext  Blob =< your   ciphertext  blob >
& Encryption  Context ={" Example ":" Example "}
&< Common   Request   Parameters >
```

Response example

`JSON` format

```
// json   response
{
" KeyId ": " 202b9877 - 5a25 - 46e3 - a763 - e20791b5 ****"
" Plaintext ": " Plaintext "
" RequestId ": " 207596a2 - 36d3 - 4840 - b1bd - f87044699b  d7 "
}
```

`XML` format

```
// xml   response
< KMS >
        < KeyId > 202b9877 - 5a25 - 46e3 - a763 - e20791b5 ****</
 KeyId >
        < Plaintext > Plaintext </ Plaintext >
        < RequestId > 4bd560a1 - 729e - 45f1 - a3d9 - b2a33d6104  6b
 </ RequestId >
</ KMS >
```

4.14 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 #unique_30 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 `Encrypt`, `GenerateDataKey`, and `DescribeKey`. - Not including the prefix, the minimum length of an alias is 1 and the maximum length is 255. - The prefix `alias/` 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>
&<CommonRequestParameters>
```

Response example

`JSON` format

```
// json response
{
    "RequestId": "53790170-1096-4ed2-9c3a-244d75c874a0"
```

```
}
```

`XML` format

```
// xml   response
< KMS >
    < RequestId > 53790170 - 1096 - 4ed2 - 9c3a - 244d75c874  0a </
 RequestId >
</ KMS >
```

4.15 UpdateAlias

Associates an existing alias with a different CMK.

Request parameters

Name	Type	Required	Description
AliasName	String	Yes	The name of the alias to be modified. 1. The prefix `alias /` 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 =
 UpdateAlia  s
& AliasName =< alias   name >
& KeyId =< target   keyid >
```

```
&< Common   Request   Parameters >
```

Response example

`JSON` format

```
// json   response
{
        " RequestId ": " 1d2baaf3 - d357 - 46c2 - 832e - 13560c2bd9
 cd "
}
```

`XML` format

```
// xml   response
< KMS >
        < RequestId > 1d2baaf3 - d357 - 46c2 - 832e - 13560c2bd9  cd
 </ RequestId >
</ KMS >
```

4.16 DeleteAlias

Deletes the specified alias.

Request parameters

Name	Type	Required	Description
AliasName	String	Yes	The alias to be deleted. · The prefix `alias /` 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 =
 DeleteAlia  s
& AliasName =< alias   name >
&< Common   Request   Parameters >
```

Response example

`JSON` format

```
// json   response
{
        " RequestId ": " 4c8ae23f - 3a42 - 6791 - a        4ba -
 1faa77831c  28 "
}
```

`XML` format

```
// xml   response
< KMS >
        < RequestId > 4c8ae23f - 3a42 - 6791 - a   4ba - 1faa77831c
 28 </ RequestId >
</ KMS >
```

4.17 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 =
 ListAliase  s
& PageNumber = 1
& PageSize = 10
&< Common   Request   Parameters >
```

Response example

`JSON` format

```
// json   response
{
        " Aliases ": {
                " Alias ": [
                        {
                                " AliasName ": " alias / ExampleAli
 as1 ",
                                " KeyId ": " 08c33a6f - 4e0a - 4a1b -
 a3fa - 7ddfa1d ****",
                                " AliasArn ": " acs : kms : cn -
 hangzhou : 123456 : alias / ExampleAli  as1 "
                        }
        ]
        },
        " TotalCount ":  1 ,
        " PageNumber ":  1 ,
        " PageSize ":  10 ,
        " RequestId ": " 1b57992c - 834b - 4811 - a889 - f8bac1ba03
 53 "
}
```

`XML` format

```
// xml   response
< KMS >
        < Aliases >
                < Alias >
                        < AliasName > alias / ExampleAli  as1 </
 AliasName >
                        < KeyId > 08c33a6f - 4e0a - 4a1b - a3fa -
 7ddfa1 ****</ KeyId >
                        < AliasArn > acs : kms : cn - hangzhou :
 123456 : alias / ExampleAli  as1 </ AliasArn >
                </ Alias >
        </ Aliases >
        < TotalCount > 1 </ TotalCount >
        < PageNumber > 1 </ PageNumber >
        < PageSize > 10 </ PageSize >
        < RequestId > 1b57992c - 834b - 4811 - a889 - f8bac1ba03  53
 </ RequestId >
</ KMS >
```

4.18 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 =
 ListAliase  sByKeyId
& PageNumber = 1
& PageSize = 10
& KeyId =< cmkid >
&< Common   Request   Parameters >
```

Response example

`JSON` format

```
// json   response
{
        " Aliases ": {
                " Alias ": [
                        {
                                " AliasName ": " alias / ExampleAli
 as1 ",
                                " KeyId ": " 08c33a6f - 4e0a - 4a1b -
 a3fa - 7ddfa1d4xx  xx ",
                                " AliasArn ": " acs : kms : cn -
 hangzhou : 123456 : alias / ExampleAli  as1 "
                        }
        ]
        },
        " TotalCount ":  1 ,
        " PageNumber ":  1 ,
        " PageSize ":  10 ,
        " RequestId ": " 1b57992c - 834b - 4811 - a889 - f8bac1ba03
 53 "
}
```

`XML` format

```
// xml   response
< KMS >
        < Aliases >
                < Alias >
```

```
                        < AliasName > alias / ExampleAli  as1 </
 AliasName >
                        < KeyId > 08c33a6f - 4e0a - 4a1b - a3fa -
 7ddfa1d4xx  xx </ KeyId >
                        < AliasArn > acs : kms : cn - hangzhou :
 123456 : alias / ExampleAli  as1 </ AliasArn >
                </ Alias >
        </ Aliases >
        < TotalCount > 1 </ TotalCount >
        < PageNumber > 1 </ PageNumber >
        < PageSize > 10 </ PageSize >
        < RequestId > 1b57992c - 834b - 4811 - a889 - f8bac1ba03  53
 </ RequestId >
</ KMS >
```

4.19 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.

Parameter	Type	Required?	Example	Description
Tags	JSON	Yes	[{"TagKey": "Project", "TagValue": "Test"}]	One or more tags. Format: tag array. Each Tag consists of a pair of: · TagKey : the tag key. · TagValue : the tag value. For more information about tag keys and tag values, see Tag description.

Tag description

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

Parameter	Type	Required?	Example	Description
TagValue	String	Yes	Test	The tag value. It can be up to 256 characters in length. It can contain uppercase and lowercase letters, digits, forward slashes (/), underscores (_), hyphens (-), periods (.), plus signs (+), equal signs (=), at signs (@), and semicolons (:). 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.

Sample requests

```
https :// kms . cn - hangzhou . aliyuncs . com /? Action =
TagResourc e
& 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 - 89dcc8aaf7  c8 "
}
```

XML format

```
< KMS >
  < RequestId > 4162a6af - bc99 - 40b3 - a552 - 89dcc8aaf7  c8 </
 RequestId >
</ KMS >
```

4.20 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 =
 UntagResou  rce
& 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 - 89dcc8aaf7  c8 "
}
```

XML format

```
< KMS >
  < RequestId > 4162a6af - bc99 - 40b3 - a552 - 89dcc8aaf7  c8 </
 RequestId >
</ KMS >
```

4.21 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 =
 ListResour  ceTags
```

```
& 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 - 89dcc8aaf7  c8 ",
    " Tags ": {
            " Tag ": [
                {
                    " KeyId ": " 33caea95 - c3e5 - 4b3e - a9c6 -
 cec76e4eaf  83 ",
                    " TagKey ": " Project ",
                    " TagValue ": " Test "
                }
            ]
        }
}
```

XML format

```
< KMS >
        < RequestId > 0f900dad - c747 - 4170 - 9962 - 1bfb6b3143  6b
 </ RequestId >
        < Tags >
            < Tag >
                < KeyId > 33caea95 - c3e5 - 4b3e - a9c6 - cec76e4eaf
 83 </ KeyId >
                < TagKey > Project </ TagKey >
                < TagValue > Test </ TagValue >
            </ Tag >
        </ Tags >
```

```
</ KMS >
```

4.22 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 =
 DescribeRe  gions
&< Common   Request   Parameters >
```

Response example

`JSON` format

```
// json   response
{
        " Regions ": {
                " Region ": [
                        {
                                " RegionId ": " cn - beijing "
                        },
                        {
                                " RegionId ": " cn - hangzhou "
                        }
                ]
        },
        " RequestId ": " 815240e2 - aa37 - 4c26 - 9cca - 05d4df3e8f
 e6 "
}
```

`XML` format

```
// xml   response
< KMS >
 < Regions >
  < Region >
```

```
    < RegionId > cn - beijing </ RegionId >
   </ Region >
   < Region >
    < RegionId > cn - hangzhou </ RegionId >
   </ Region >
  </ Regions >
  < RequestId > 815240e2 - aa37 - 4c26 - 9cca - 05d4df3e8f  e6 </
  RequestId >
</ KMS >
```