

Alibaba Cloud KeyManagementService

API Reference

Issue: 20190318

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.
<code>Courier</code> font	It is used for commands.	Run the <code>cd / d C :/ windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[] or [a b]	It indicates that it is a optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>

Style	Description	Example
<code>{}</code> or <code>{a b}</code>	It indicates that it is a required value, and only one item can be selected.	<code>switch {stand slave}</code>

Contents

Legal disclaimer.....	I
Generic conventions.....	I
1 Calling method.....	1
1.1 Request structure.....	1
1.2 Signature.....	3
2 API list.....	7
2.1 CreateKey.....	7

1 Calling method

1.1 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
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

Region	RegionId	Public network endpoint	Private network endpoint
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
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
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`.

1.2 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=testid&Action=CreateKey&
Format=json&SignatureMethod=HMAC-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 0fiJPFg % 3D
```

2 API list


2.1 CreateKey

Creates a customer master key (CMK).

You can use a CMK to encrypt small amounts of data (a maximum of 6 KB). Typically, you use CMKs to generate data keys that you can use to encrypt large amounts of data.

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

Request parameters

Name	Type	Required	Description
Origin	String	No	<p>The source of the key material for the CMK.</p> <p>Valid values: Aliyun_KMS and EXTERNAL.</p> <div> Note: Default value: Aliyun_KMS. Note that the values are case sensitive.</div> <p>If you choose EXTERNAL, you need to Import key material.</p>
Description	String	No	<p>The description of the CMK.</p> <p>Length constraints : Minimum length of 0 characters. Maximum length of 8192 characters.</p>
KeyUsage	String	No	<p>The intended use of the CMK. Default value: ENCRYPT/DECRYPT.</p>

Response parameters

Name	Type	Description
KeyMetadata	KeyMetadata	The metadata associated with the CMK.

KeyMetadata

Name	Type	Description
CreationDate	Timestamp	The date and time (in UTC format) when the CMK is created.
Description	String	The description of the CMK.
KeyId	String	The globally unique identifier for the CMK.
KeyState	String	The state of the CMK. For more information, see Impact of CMK states on API call .
KeyUsage	String	The cryptographic operations for which you can use the CMK. Valid Values: ENCRYPT/DECRYPT.
DeleteDate	Timestamp	The date and time after which KMS deletes the CMK. <ul style="list-style-type: none">· A null value indicates that the CMK is not to be deleted.· This value is present only when <code>KeyState</code> 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 CMK's key material.

MaterialExpireTime	String	The time at which the imported key material expires. If the value is null , the key does not expire.
--------------------	--------	------------------------------------------------------------------------------------------------------

Examples

Request example

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

Response example

JSON format

```
// json response
{
  "KeyMetadata": {
    "CreationDate": "2016-03-25T10:42:40Z",
    "Description": "key description example",
    "KeyId": "08c33a6f-4e0a-4a1b-a3fa-7ddfa1d4fb73",
    "KeyState": "Enabled",
    "KeyUsage": "ENCRYPT/DECRYPT",
    "DeleteDate": "",
    "Creator": "123456",
    "Arn": "acs:kms:cn-hangzhou:123456:key/08c33a6f-4e0a-4a1b-a3fa-7ddfa1d4fb73",
    "Origin": "Aliyun_KMS",
    "MaterialExpireTime": ""
  },
  "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-7ddfa1d4fb73</KeyId>
    <KeyState>Enabled</KeyState>
    <KeyUsage>ENCRYPT/DECRYPT</KeyUsage>
    <DeleteDate></DeleteDate>
    <Creator>123456</Creator>
    <Arn>acs:kms:cn-hangzhou:123456:key/08c33a6f-4e0a-4a1b-a3fa-7ddfa1d4fb73</Arn>
    <Origin>Aliyun_KMS</Origin>
  
```

```
      < MaterialEx  pireTime ></ MaterialEx  pireTime >
    </ KeyMetadat  a >
    < RequestId > 6cb4bf6b - d9c9 - 4660 - af5f - 2328378e72  57 </
    RequestId >
  </ KMS >
```