ALIBABA CLOUD

Alibaba Cloud

Key Management Service

API Reference

Document Version: 20201012

Alibaba Cloud

Legal disclaimer

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

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

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

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

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

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

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

Document conventions

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

Table of Contents

1.List of operations by function 07
2.Impact of CMK status on API operations 11
3.Calling method 14
3.1. Overview 14
3.2. Request structure 14
3.3. Common parameters 16
3.4. Request signatures 18
3.5. Responses 20
4.Key 25
4.1. CreateKey 25
4.2. GetParametersForImport 33
4.3. ImportKeyMaterial 36
4.4. EnableKey 39
4.5. DisableKey 40
4.6. ScheduleKeyDeletion 41
4.7. CancelKeyDeletion 43
4.8. DeleteKeyMaterial 44
4.9. DescribeKey 45
4.10. ListKeys 49
4.11. UpdateKeyDescription 52
4.12. DescribeKeyVersion 53
4.13. ListKeyVersions 55
4.14. UpdateRotationPolicy 59
4.15. CreateKeyVersion 61
4.16. Encrypt 63
4.17. GenerateDataKey 65

4.18. GenerateDataKeyWithoutPlaintext 69
4.19. ExportDataKey 73
4.20. GenerateAndExportDataKey 77
4.21. Decrypt 82
4.22. ReEncrypt 84
4.23. AsymmetricSign 90
4.24. AsymmetricVerify 93
4.25. AsymmetricDecrypt 97
4.26. AsymmetricEncrypt 100
4.27. GetPublicKey 103
4.28. CreateAlias 106
4.29. UpdateAlias 108
4.30. DeleteAlias 110
4.31. ListAliases 111
4.32. ListAliasesByKeyId 113
5.Secrets 117
5.1. CreateSecret 117
5.2. ListSecrets 119
5.3. DeleteSecret 123
5.4. DescribeSecret 125
5.5. GetSecretValue 128
5.6. PutSecretValue 130
5.7. UpdateSecret 133
5.8. UpdateSecretVersionStage 134
5.9. RestoreSecret 136
5.10. ListSecretVersionIds 137
5.11. GetRandomPassword 141
6.Tag 144

6.1. TagResource 144
6.2. ListResourceTags 145
6.3. UntagResource 147

1.List of 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 API operations

- **CMK management**

  CMK management API operations are used to create and modify CMKs and manage their lifecycle.

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

- **Key version management**

Key version management API operations are used for CMK rotation.

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

- **Cryptographic operation**

  Cryptographic API operations are used to perform cryptographic operations such as data encryption and decryption.

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

Operation	Description
AsymmetricVerify	Uses the public key of an asymmetric key pair to verify a digital signature that is generated by using the private key.
AsymmetricDecrypt	Uses the private key of an asymmetric key pair to decrypt the data that is encrypted by using the public key.
AsymmetricEncrypt	Uses the public key of an asymmetric key pair to encrypt data.
GetPublicKey	Obtains the public key of an asymmetric key pair. You can use the public key to encrypt data or verify digital signatures offline.

- **Alias management**

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

Operation	Description
CreateAlias	Creates an alias and binds it to a CMK.
UpdateAlias	Binds an alias to a different CMK.
DeleteAlias	Deletes an alias.
ListAliases	Lists all aliases under the current Alibaba Cloud account in the current region.
ListAliasesByKeyId	Lists all aliases bound to a specified CMK.

Secrets Manager API operations

KMS Secrets Manager hosts, protects, distributes, and rotates secrets.

Operation	Description
CreateSecret	Creates a secret and stores the secret value in the initial version.
ListSecrets	Queries all secrets created by your Alibaba Cloud account in the current region.
DeleteSecret	Deletes a secret.
DescribeSecret	Obtains the metadata of a secret.
GetSecretValue	Obtains a secret value.
PutSecretValue	Stores the secret value of a new version into a secret object.
UpdateSecret	Updates the metadata of a secret.
UpdateSecretVersionStage	Updates the stage label that marks a secret version.

Operation	Description
RestoreSecret	Restores a deleted secret.
ListSecretVersionIds	Queries all versions of a secret.
GetRandomPassword	Obtains a random password string.

Tag management API operations

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

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

Other API operations

Operation	Description
DescribeRegions	Queries available regions under your Alibaba Cloud account.

2.Impact of CMK status on API operations

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

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

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

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

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

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

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

Common API operations

API operation	Enabled	Disabled	PendingDeletion	PendingImport
CreateKey	Success	Success	Success	Success
GenerateDataKey	Success	Rejected.Disabled	Rejected.PendingDeletion	Rejected.PendingImport
GenerateDataKeyWithoutPlaintext	Success	Rejected.Disabled	Rejected.PendingDeletion	Rejected.PendingImport
Encrypt	Success	Rejected.Disabled	Rejected.PendingDeletion	Rejected.PendingImport
Decrypt	Success	Rejected.Disabled	Rejected.PendingDeletion	Rejected.PendingImport

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

Special API operations

UpdateAlias:

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

BYOK-specific API operations

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

3.Calling method

3.1. 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. Request signatures

3.2. Request structure

This topic describes the endpoints, communication protocols, HTTP request methods, and request parameters of KMS API.

Endpoints

The following table lists the endpoints of the KMS API.

Region	RegionId	Public endpoint	VPC endpoint
Japan (Tokyo)	ap-northeast-1	kms.ap-northeast-1.aliyuncs.com	kms-vpc.ap-northeast-1.aliyuncs.com
Singapore	ap-southeast-1	kms.ap-southeast-1.aliyuncs.com	kms-vpc.ap-southeast-1.aliyuncs.com
Australia (Sydney)	ap-southeast-2	kms.ap-southeast-2.aliyuncs.com	kms-vpc.ap-southeast-2.aliyuncs.com
Malaysia (Kuala Lumpur)	ap-southeast-3	kms.ap-southeast-3.aliyuncs.com	kms-vpc.ap-southeast-3.aliyuncs.com
Indonesia (Jakarta)	ap-southeast-5	kms.ap-southeast-5.aliyuncs.com	kms-vpc.ap-southeast-5.aliyuncs.com
India (Mumbai)	ap-south-1	kms.ap-south-1.aliyuncs.com	kms-vpc.ap-south-1.aliyuncs.com
China (Hangzhou)	cn-hangzhou	kms.cn-hangzhou.aliyuncs.com	kms-vpc.cn-hangzhou.aliyuncs.com

Region	RegionId	Public endpoint	VPC endpoint
China (Shanghai)	cn-shanghai	kms.cn-shanghai.aliyuncs.com	kms-vpc.cn-shanghai.aliyuncs.com
China (Qingdao)	cn-qingdao	kms.cn-qingdao.aliyuncs.com	kms-vpc.cn-qingdao.aliyuncs.com
China (Beijing)	cn-beijing	kms.cn-beijing.aliyuncs.com	kms-vpc.cn-beijing.aliyuncs.com
China (Zhangjiakou-Beijing Winter Olympic)	cn-zhangjiakou	kms.cn-zhangjiakou.aliyuncs.com	kms-vpc.cn-zhangjiakou.aliyuncs.com
China (Hohhot)	cn-huhehaote	kms.cn-huhehaote.aliyuncs.com	kms-vpc.cn-huhehaote.aliyuncs.com
China (Shenzhen)	cn-shenzhen	kms.cn-shenzhen.aliyuncs.com	kms-vpc.cn-shenzhen.aliyuncs.com
Germany (Frankfurt)	eu-central-1	kms.eu-central-1.aliyuncs.com	kms-vpc.eu-central-1.aliyuncs.com
UAE (Dubai)	me-east-1	kms.me-east-1.aliyuncs.com	kms-vpc.me-east-1.aliyuncs.com
China (Hong Kong)	cn-hongkong	kms.cn-hongkong.aliyuncs.com	kms-vpc.cn-hongkong.aliyuncs.com
US (Virginia)	us-east-1	kms.us-east-1.aliyuncs.com	kms-vpc.us-east-1.aliyuncs.com
US (Silicon Valley)	us-west-1	kms.us-west-1.aliyuncs.com	kms-vpc.us-west-1.aliyuncs.com
China East 1 Finance	cn-hangzhou-finance	kms.cn-hangzhou-finance.aliyuncs.com	N/A
China East 2 Finance	cn-shanghai-finance-1	kms.cn-shanghai-finance-1.aliyuncs.com	kms-vpc.cn-shanghai-finance-1.aliyuncs.com
China South 1 Finance	cn-shenzhen-finance-1	kms.cn-shenzhen-finance-1.aliyuncs.com	kms-vpc.cn-shenzhen-finance-1.aliyuncs.com
UK (London)	eu-west-1	kms.eu-west-1.aliyuncs.com	kms-vpc.eu-west-1.aliyuncs.com
China (Heyuan)	cn-heyuan	kms.cn-heyuan.aliyuncs.com	kms-vpc.cn-heyuan.aliyuncs.com

Region	RegionId	Public endpoint	VPC endpoint
China (Ulanqab)	cn-wulanchabu	kms.cn-wulanchabu.aliyuncs.com	kms-vpc.cn-wulanchabu.aliyuncs.com

Protocols

You must call KMS API operations by sending HTTPS requests.

KMS supports only TLS1.0 and later.

Methods

You can use the HTTP POST and GET methods to send requests. If you use these methods, the request parameters must be included in the request URL.

Parameters

Each request must specify the operation to be performed. For example, to create a CMK, you must set the `Action` parameter to CreateKey. Request parameters include both common parameters and operation-specific parameters.

For more information, see Common parameters.

Encoding

Requests and responses are encoded using `UTF-8`.

3.3. Common parameters

Common request parameters must be included in all API requests.

Common request parameters

Parameter	Type	Required	Description
Format	String	No	The format in which to return the response. Valid values: JSON and XML. Default value: XML.
Version	String	Yes	The version number of the API. The value is in the format of YYYY-MM-DD. The current version is 2016-01-20.
AccessKeyId	String	Yes	The AccessKey ID provided to you by Alibaba Cloud.

Parameter	Type	Required	Description
Signature	String	Yes	The signature string of the current request. For more information about how signatures are calculated, see Request signatures.
SignatureMethod	String	Yes	The encryption method of the signature string. Set the value to HMAC-SHA1.
Timestamp	String	Yes	The timestamp of the request. Specify the time in the ISO 8601 standard in the yyyy-MM-ddTHH:mm:ssZ format. The time must be in UTC. Example: 2015-12-01T12:00:00Z.
SignatureVersion	String	Yes	The version of the signature encryption algorithm. Set the value to 1.0.

Examples

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

Common response parameters

Every response returns a unique request ID regardless of whether the call is successful.

Examples

`XML` format

```
<KMS>
<RequestId>348d9445-e39a-4d80-907d-298cc6c94447</RequestId>
<!—Return Result Data-->
</KMS>
```

`JSON` format

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

3.4. Request signatures

You must sign all API requests to ensure security. Alibaba Cloud uses the request signature to verify the identity of the API caller. KMS implements symmetric encryption with an AccessKey pair to verify the identity of the request sender. An AccessKey pair consists of an AccessKey ID and an AccessKey secret. You can apply for an AccessKey pair and manage it in the Alibaba Cloud Management Console.

Procedure

1. Compose and encode a string-to-sign.
   - Create a canonicalized query string by arranging the request parameters (including all common and operation-specific parameters except Signature) in alphabetical order. The canonicalized query string is only made up of the parameters and does not include "https://endpoint/?".

     > **Note** If you use the GET method to send a request, the request parameters are included as a part of the request URL. The request parameters in the URL are placed after a question mark (?) and separated with ampersands (&).

   - Encode the canonicalized query string in UTF-8. Encoding rules:
     - Uppercase letters, lowercase letters, digits, and some special characters such as hyphens (-), underscores (_), periods (.), and tildes (~) do not need to be encoded.
     - Other characters must be percent encoded in %XY format. XY represents the ASCII code of the characters in hexadecimal notation. For example, double quotation marks (") are encoded as %22.

- Spaces must be encoded as %20. Do not encode spaces as plus signs (+).

  > **Note** Most libraries that support URL encoding, such as java.net.URLEncoder, comply with the Multipurpose Internet Mail Extensions (MIME) encoding rules of `application/x-www-form-urlencoded`. If this encoding method is used, replace the plus signs (+) in the encoded strings with %20, the asterisks (*) with %2A, and %7E with a tilde (~) to conform to the encoding rules.

- Connect the encoded parameter names and values by using equal signs (=).
- Sort the equal sign-connected strings by their parameter names in alphabetical order and connect them with ampersands (&).

  Create a string-to-sign from the encoded canonicalized query string.

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

  where:

  - HTTPMethod indicates the HTTP method that is used to submit a request, such as GET.
  - percentEncode("/") specifies the encoded value for the forward slash (/) based on the URL encoding rules previously described. The value is %2F.
  - percentEncode(CanonicalizedQueryString) specifies the encoded string of the canonicalized query string constructed in step 1, produced by following the URL encoding rules previously described.

2. Use the previous signature string to calculate the HMAC value of the signature as defined in RFC 2104. For more information about RFC 2104, see RFC 2104.

   > **Notice** The key used for signature calculation is your AccessKey secret. An ampersand (&) is added to the end of the key (ASCII: 38). SHA-1 hashing is used.

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

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

Example

The following code is the request URL without a signature for the `CreateKey` operation:

```
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
```

The following code is the `CanonicalizedQueryString`:

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

The following code is the `StringToSign`:

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

Assume that the AccessKey ID is `testid`, the AccessKey secret is `testsecret`, and the key used for HMAC calculation is `testsecret&`. The following signature string is obtained:

```
41wk2SSX1GJh7fwnc5eqOfiJPF****
```

The following code is the signed request URL 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=41wk2SSX1GJh7fwnc5eqOfiJPF****
```

3.5. 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 sup
plied. </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
Forbidden.InDebt	Current user is indebted.	403

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

Error code	Description	HTTP status code

4.Key

4.1. CreateKey

Creates a CMK.

A CMK can be symmetric or asymmetric.

Symmetric CMKs are used to encrypt data of 6 KB or less and generate data keys to encrypt data larger than 6 KB. For more information, see GenerateDataKey.

Asymmetric CMKs are used to encrypt, decrypt, and sign data, and verify signatures, but cannot be used to generate data keys.

The following table lists the key types and operations supported by symmetric and asymmetric CMKs.

	Key type	Description	Encryption and decryption	Signature and verification
Symmetric CMK	Aliyun_AES_256	AES key with a length of 256 bits	Supported	Unsupported
Symmetric CMK	Aliyun_SM4	SM4 key	Supported	Unsupported
Asymmetric CMK	RSA_2048	RSA key with a length of 2048 bits	Supported	Supported
Asymmetric CMK	EC_P256	NIST-recommended elliptic curve P-256 (secp256r1)	Not supported	Supported
Asymmetric CMK	EC_P256K	SECC elliptic curve secp256k1	Not supported	Supported
Asymmetric CMK	EC_SM2	256-bit elliptic curve in the prime number domain defined by GBT32918	Supported	Supported

> **Note**
>
> - The symmetric key KeySpec is prefixed with the standard key type `Aliyun_` which indicates the cryptographic algorithm that uses the standard key, but generates non-standard ciphertext. Asymmetric keys generate standard ciphertext or signatures.
> - An RSA key supports the ENCRYPT/DECRYPT operations or SIGN/VERIFY operations.
> - SM4 and SM2 are cryptographic algorithms approved by state cryptography Administration of China. KMS supports SM4 and SM2 through managed hardware security module deployed in mainland China.

Debugging

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

Request parameters

Parameter	Scenario	Required	Example	Description
Action	String	Retained	CreateKey	The operation that you want to perform. Set the value to CreateKey.
Description	String	No	key description example	The description of the CMK. The description can be up to 8,192 characters in length.
KeySpec	String	No	Aliyun_AES_256	The type of the CMK. Valid values: • Aliyun_AES_256 • Aliyun_SM4 • RSA_2048 • EC_P256 • EC_P256K • EC_SM2 **Note** If the CMK is created in a managed hardware security module in mainland China, the default value is Aliyun_SM4. In other cases, the default value is Aliyun_AES_256.

Parameter	Scenario	Required	Example	Description
KeyUsage	String	No	ENCRYPT/DECRYPT	The purpose of the CMK. Valid values: • ENCRYPT/DECRYPT: data encryption and decryption. • SIGN/VERIFY: generate and VERIFY a digital signature.
Origin	String	No	Aliyun_KMS	The source of the key material. Valid values: • Aliyun_KMS (default) • EXTERNAL Note • The value of this parameter is case-sensitive. • When KeySpec is an asymmetric key type, the EXTERNAL parameter cannot be selected. • If you select EXTERNAL, you must import key material.

Parameter	Scenario	Required	Example	Description
ProtectionLevel	String	No	SOFTWARE	The protection level of the CMK. Valid values: • SOFTWARE (default) • HSM Note • The value of this parameter is case-sensitive. • When you set this parameter to HSM: If you set the Origin parameter to Aliyun_KMS, the CMK is generated in the managed hardware security module. If you set the Origin parameter to externa, you can import external keys to a managed hardware security module for password calculation.
EnableAutomaticRotation	Boolean	No	false	Indicates whether automatic key rotation is enabled. Valid values: • true • false Note If the Origin parameter is set to EXTERNAL, or the KeySpec parameter is set to an asymmetric CMK type, automatic rotation is unavailable.

Parameter	Scenario	Required	Example	Description
RotationInterval	String	No	365d	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). 7d or 604,800 S indicates a 7-day period. Valid values: 7 to 730 days. Note If EnableAutomaticRotation is set to true, this parameter is required. If not, this parameter is ignored.

Response parameters

Parameter	Scenario	Example	Description
KeyMetadata	Struct		The metadata of the CMK.
Arn	String	acs:kms:cn-hangzhou:123456:key/08c33a6f-4e0a-4a1b-a3fa-7ddf****	The Alibaba Cloud Resource Name (ARN) of the CMK.
AutomaticRotation	String	Enabled	Indicates whether automatic key rotation is enabled. Valid values: • Enabled: Automatic rotation is enabled. • Disabled: Automatic rotation is disabled. • Suspended: KMS suspended the execution of automatic key rotation. For more information, see Automatic key rotation. Note This API is only applicable to symmetric cmks. Asymmetric cmks do not support automatic rotation.

Parameter	Scenario	Example	Description
CreationDate	String	2016-03-25T10:42:40Z	The date and time the CMK was created. The time is displayed in UTC.
Creator	String	123456	The creator of the CMK.
DeleteDate	String	2020-07-06T18:22:03Z	The scheduled deletion time of the CMK. For more information, see ScheduleKeyDeletion. Note This value is only returned when the KeyState value is PendingDeletion.
Description	String	key description example	The description of the CMK.
KeyId	String	08c33a6f-4e0a-4a1b-a3fa-7ddf****	The globally unique ID of the CMK.
KeySpec	String	Aliyun_AES_256	The type of the CMK.
KeyState	String	Enabled	The status of the CMK. For more information, see impact of CMK states on API calls.
KeyUsage	String	ENCRYPT/DECRYPT	The purpose of the CMK.
LastRotationDate	String	2019-06-06T18:22:03Z	The date and time the last rotation was performed. The time is displayed in UTC. For a newly created key, the value of this parameter is the date and time the initial version of the new key was generated.
MaterialExpireTime	String	2020-07-06T18:22:03Z	The date and time 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.

Parameter	Scenario	Example	Description
NextRotationDate	String	2020-07-06T18:22:03Z	The time the next rotation is scheduled for execution. Note This value is only returned when AutomaticRotation is Enabled or Suspended.
Origin	String	Aliyun_KMS	The source of the key material.
PrimaryKeyVersion	String	0ec2d249-9f64-4d8f-9587-1215525e****	The ID of the current primary key version. Note • The primary key version is an active encryption key of a symmetric CMK, and key management uses the primary key version to process encryption requests. • This operation is not applicable to asymmetric cmks.
ProtectionLevel	String	SOFTWARE	The protection level of the CMK.
RotationInterval	String	31536000s	The period of automatic key rotation. Unit: seconds. Format: integer[s] For example, a 7-day rotation cycle is 604800 seconds. This value is only returned when AutomaticRotation is Enabled or Suspended.
RequestId	String	3455b9b4-95c1-419d-b310-db6a53b09a39	The ID of the instance.

Samples

Sample requests

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

Sample success responses

`XML` format

```
<KMS>
  <KeyMetadata>
    <CreationDate>2016-03-25T10:42:40Z</CreationDate>
    <Description>key description example</Description>
    <KeyId>08c33a6f-4e0a-4a1b-a3fa-7ddfa1d4****</KeyId>
    <KeySpec>Aliyun_AES_256</KeySpec>
    <KeyState>Enabled</KeyState>
    <KeyUsage>ENCRYPT/DECRYPT</KeyUsage>
    <PrimaryKeyVersion>0ec2d249-9f64-4d8f-9587-1215525e****</PrimaryKeyVersion>
    <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>SOFTWARE</ProtectionLevel>
    <LastRotationDate>2016-03-25T10:42:40Z</LastRotationDate>
    <AutomaticRotation>Enabled</AutomaticRotation>
    <RotationInterval>31536000s</RotationInterval>
    <NextRotationDate>2017-03-25T10:42:40Z</NextRotationDate>
  </KeyMetadata>
  <RequestId>3455b9b4-95c1-419d-b310-db6a53b09a39</RequestId>
</KMS>
```

`JSON` format

```
{
    "KeyMetadata": {
        "CreationDate": "2016-03-25T10:42:40Z",
        "Description": "key description example",
        "KeyId": "08c33a6f-4e0a-4a1b-a3fa-7ddfa1d4****",
        "KeySpec": "Aliyun_AES_256",
        "KeyState": "Enabled",
        "KeyUsage": "ENCRYPT/DECRYPT",
        "PrimaryKeyVersion": "0ec2d249-9f64-4d8f-9587-1215525e****",
        "DeleteDate": "",
        "Creator":"123456",
        "Arn":"acs:kms:cn-hangzhou:123456:key/08c33a6f-4e0a-4a1b-a3fa-7ddfa1d4****",
        "Origin":"Aliyun_KMS",
        "MaterialExpireTime":"",
        "ProtectionLevel":"SOFTWARE",
        "LastRotationDate":"2016-03-25T10:42:40Z",
        "AutomaticRotation": "Enabled",
        "RotationInterval": "31536000s",
        "NextRotationDate":"2017-03-25T10:42:40Z"
    },
    "RequestId": "3455b9b4-95c1-419d-b310-db6a53b09a39"
}
```

4.2. GetParametersForImport

Queries the GetParametersForImport of CMK materials.

The returned parameters can be used to perform the ImportKeyMaterial.

> **Note**
>
> - The CMK material must be external, that is **Origin** for **EXTERNAL**.
> - The type of the public key used to encrypt the key material must be specified, and the encryption algorithm must be specified. See the following table for details.
> - This operation returns a public key (PublicKey), an import token, and the import token expiration time. The public key is base64 encoded. The token is valid for 24 hours.
> - The public key and STS token can be used only for the CMK specified in this request.
> - The public key and token that are returned 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 call returns a public key that is different from the token.

Types of public keys	Encryption Algorithm	Description
RSA_2048	RSAES_PKCS1_V1_5 RSAES_OAEP_SHA_1 RSAES_OAEP_SHA_256	It supports keys of any protection level in all regions.
EC_SM2	SM2PKE	Only the protection level is **HSM** with the hardware security module detection type **commercial password testing and authentication by State Security Bureau**(For more information, see overview of managed hardware security module).

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	GetParametersForImport	The operation that you want to perform. Set the value to **GetParametersForImport**.
KeyId	String	Yes	1234abcd-12ab-34cd-56ef-12345678****	The globally unique identifier of the CMK. **Note** The key material source must be external (**Origin** for **EXTERNAL**).
WrappingAlgorithm	String	Yes	RSAES_PKCS1_V1_5	The algorithm used to encrypt the key material.
WrappingKeySpec	String	Yes	RSA_2048	The type of the public key used to encrypt the key material.

Response parameters

Prameter	Type	Sample response	Description
ImportToken	String	Base64String	Import token. Subsequent calls ImportKeyMaterial required.
KeyId	String	1234abcd-12ab-34cd-56ef-12345678****	The globally unique identifier of the CMK. Subsequent calls ImportKeyMaterial required.
PublicKey	String	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAlls4uIBxD0GG84C+lGBO6Dhpf1J3XimC6cPmPNaKKJMOzoX4tD+C+r7aZv8lZ3vnPfxuxvy/YwG+whUxTEEFUdqJTOIzhPfYucupqKM92crVHIuG+xtMVeHKjyTr+UrtKCsQikqHT+19yDRN/RMoo2HUx0gmEnRyXd8t3JyUXun9FdoxKA08GrsV7nodb9ZsoBLhnev7tTLcXvLyKW6XG1ZQCQm6dPnbnwLeDXR7uK0Lqn9PM28mBIdaiQUQxj2XbM1CoJA+JiyVX3Ptdb+4rqukb4Rb05B80Bs9xV/cf7FIku08l7xGhrGiQFq+DFXwQWtwihXHZxz3LhldU+4ZPwIDAQAB	The public key used to encrypt the key material.
RequestId	String	8 cdf51 fd-bcd6-d79a-0ef4-e52c9b5466dc	The ID of the request.
TokenExpireTime	String	2018-01-25T00:01:02Z	The time when the import token expires.

Examples

Sample requests

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

Sample success responses

`XML` format

```
<KMS>
  <ImportToken>Base64String</ImportToken>
  <PublicKey>MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAlls4uIBxD0GG84C+lGBO6Dhpf1J3Xim
C6cPmPNaKKJMOzoX4tD+C+r7aZv8lZ3vnPfxuxvy/YwG+whUxTEEFUdqJTOIzhPfYucupqKM92crVHIuG+xtM
VeHKjyTr+UrtKCsQikqHT+19yDRN/RMoo2HUx0gmEnRyXd8t3JyUXun9FdoxKA08GrsV7nodb9ZsoBLhnev7tT
LcXvLyKW6XG1ZQCQm6dPnbnwLeDXR7uK0Lqn9PM28mBIdaiQUQxj2XbM1CoJA+JiyVX3Ptdb+4rqukb4Rb05
B80Bs9xV/cf7FIku08l7xGhrGiQFq+DFXwQWtwihXHZxz3LhldU+4ZPwIDAQAB</PublicKey>
  <KeyId>KeyId</KeyId>
  <TokenExpireTime>2018-01-25T00:01:02Z</TokenExpireTime>
  <RequestId>8cdf51fd-bcd6-d79a-0ef4-e52c9b5466dc</RequestId>
</KMS>
```

`JSON` format

```
{
    "ImportToken":"Base64String",
    "PublicKey":"MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAlls4uIBxD0GG84C+lGBO6Dhpf1J3
XimC6cPmPNaKKJMOzoX4tD+C+r7aZv8lZ3vnPfxuxvy/YwG+whUxTEEFUdqJTOIzhPfYucupqKM92crVHIuG+
xtMVeHKjyTr+UrtKCsQikqHT+19yDRN/RMoo2HUx0gmEnRyXd8t3JyUXun9FdoxKA08GrsV7nodb9ZsoBLhne
v7tTLcXvLyKW6XG1ZQCQm6dPnbnwLeDXR7uK0Lqn9PM28mBIdaiQUQxj2XbM1CoJA+JiyVX3Ptdb+4rqukb4R
b05B80Bs9xV/cf7FIku08l7xGhrGiQFq+DFXwQWtwihXHZxz3LhldU+4ZPwIDAQAB",
    "KeyId":"KeyId",
    "TokenExpireTime":"2018-01-25T00:01:02Z",
    "RequestId":"8cdf51fd-bcd6-d79a-0ef4-e52c9b5466dc"
}
```

4.3. ImportKeyMaterial

Call the ImportKeyMaterial operation to import the key material.

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

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

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

Debugging

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

Request parameters

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

Parameter	Type	Required	Example	Description
EncryptedKeyMaterial	String	Yes	bCPZx7I6v6KXsqEpr2OXKxuj2CCRtKdwp75Bw+BGncYqBdfjFBYRtOE6HRlT0oeiRDWzwnw9OA54OL36smDJrq4Lo9x0CyYDiuKnRkcKtMtlzW0din7Pd7IlZWWRdVueiw2qpzl7PkUWQGTdsdbzpfJJQ+qj/cRIrk/E83UGyeyytSpgnb+lu0xEYcPajRyWNsbi98N3pqqQzHXNNHO2NJqHlnQgglqTiBEjkGeKFhfKmTc3vjulldVa3EaVIN6lwWfgx+UUYSrvbA77WDYKlDsZ4SbK2/T7za9Tp1qU7Ynqba7OKGVVj7PMbiaO80AxWZnjUMYCgEp5w7V+seOXqw==	Use **GetParametersForImport** the Returned public key and the base64-encoded key material.
ImportToken	String	Yes	Base64String	By calling **GetParametersForImport** the import token.
KeyId	String	Yes	1234abcd-12ab-34cd-56ef-12345678****	The ID of the CMK to be imported.
KeyMaterialExpireUnix	Long	Yes	0	The time when the key material expires. If this parameter is not specified or set this parameter to 0, the key material does not expire. **Note** The value cannot be earlier than the time when the API is called (based on the server time).

Response parameters

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

Examples

Sample requests

```
https://[Endpoint]/? Action=ImportKeyMaterial
&EncryptedKeyMaterial=bCPZx7I6v6KXsqEpr2OXKxuj2CCRtKdwp75Bw+BGncYqBdfjFBYRtOE6HRlT0oeiRD
Wzwnw9OA54OL36smDJrq4Lo9x0CyYDiuKnRkcKtMtlzW0din7Pd7IlZWWRdVueiw2qpzl7PkUWQGTdsdbzpfJJ
Q+qj/cRIrk/E83UGyeyytSpgnb+lu0xEYcPajRyWNsbi98N3pqqQzHXNNHO2NJqHlnQgglqTiBEjkGeKFhfKmTc3
vjulIdVa3EaVIN6lwWfgx+UUYSrvbA77WDYKlDsZ4SbK2/T7za9Tp1qU7Ynqba7OKGVVj7PMbiaO80AxWZnjU
MYCgEp5w7V+seOXqw==
&ImportToken=Base64String
&KeyId=1234abcd-12ab-34cd-56ef-12345678****
&KeyMaterialExpireUnix=0
&<Common request parameters>
```

Sample success responses

`XML` format

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

`JSON` format

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

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

Debugging

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

Request parameters

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

Response parameters

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

Examples

Sample requests

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

Sample success responses

`XML` format

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

`JSON` format

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

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 **PendingDeletion**state, 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

Queries details of a specific CMK.

Debugging

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

Request parameters

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

Response parameters

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

Parameter	Type	Example	Description
CreationDate	String	2016-03-25T10:42:40Z	The date and time the CMK was created. The time is displayed in UTC.
Description	String	key description example	The description of the CMK.
KeyId	String	08c33a6f-4e0a-4a1b-a3fa-7ddf****	The globally unique ID of the CMK.
KeyState	String	Enabled	The status of the CMK. For more information, see Effects of CMK states on API operations.
KeyUsage	String	ENCRYPT/DECRYPT	The purpose of the CMK.
DeleteDate	String	2020-07-06T18:22:03Z	The date and time the CMK is scheduled for deletion. For more information, see ScheduleKeyDeletion. This value is only returned if the value of the **KeyState** parameter is **PendingDeletion**.
Creator	String	123456	The creator of the CMK.
Arn	String	acs:kms:cn-hangzhou:123456:key/08c33a6f-4e0a-4a1b-a3fa-7ddf****	The Alibaba Cloud Resource Name (ARN) of the CMK.
Origin	String	Aliyun_KMS	The source of the key material for the CMK.
MaterialExpireTime	String	2020-07-06T18:22:03Z	The time and date 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	SOFTWARE	The protection level of the CMK.

Parameter	Type	Example	Description
PrimaryKeyVersion	String	0ec2d249-9f64-4d8f-9587-1215525e****	The ID of the current primary key version of the symmetric CMK. The primary key version of a CMK is an active encryption key. KMS uses the primary key version of a specified CMK to encrypt data. This parameter is unavailable for asymmetric CMKs.
LastRotationDate	String	2019-06-06T18:22:03Z	The date and time the last rotation was performed. The time is displayed in UTC. For a newly created key, the value of this parameter is the date and time the initial version of the new key was generated.
AutomaticRotation	String	Enabled	Indicates whether automatic key rotation is enabled. • Enabled: Automatic rotation is enabled. • Disabled: Automatic rotation is disabled. • Suspended: KMS suspended the execution of automatic key rotation. For more information, see Automatic key rotation. This parameter is only available for symmetric CMKs.
RotationInterval	String	31536000s	The period of automatic key rotation. Unit: seconds. For example, the seven-day rotation period is 604800s. This value is only returned when the **AutomaticRotation** parameter is set to **Enabled** or **Suspended**.
NextRotationDate	String	2020-07-06T18:22:03Z	The time the next rotation is scheduled for execution. This value is only returned when the **AutomaticRotation** parameter is set to **Enabled** or **Suspended**.
KeySpec	String	Aliyun_AES_256	The type of the CMK.

Examples

Sample requests

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

Sample success responses

`XML` format

```
<KMS>
  <KeyMetadata>
    <CreationDate>2016-03-25T10:42:40Z</CreationDate>
    <Description>key description example</Description>
    <KeyId>08c33a6f-4e0a-4a1b-a3fa-7ddf****</KeyId>
    <KeySpec>Aliyun_AES_256</KeySpec>
    <KeyState>Enabled</KeyState>
    <KeyUsage>ENCRYPT/DECRYPT</KeyUsage>
    <PrimaryKeyVersion>0ec2d249-9f64-4d8f-9587-1215525e****</PrimaryKeyVersion>
    <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>SOFTWARE</ProtectionLevel>
    <LastRotationDate>2019-06-06T18:22:03Z</LastRotationDate>
    <AutomaticRotation>Enabled</AutomaticRotation>
    <RotationInterval>31536000s</RotationInterval>
    <NextRotationDate>2020-07-06T18:22:03Z</NextRotationDate>
  </KeyMetadata>
  <RequestId>3455b9b4-95c1-419d-b310-db6a53b09a39</RequestId>
</KMS>
```

`JSON` format

```
{
    "KeyMetadata": {
        "CreationDate": "2016-03-25T10:42:40Z",
        "Description": "key description example",
        "KeyId": "08c33a6f-4e0a-4a1b-a3fa-7ddf****",
        "KeySpec": "Aliyun_AES_256",
        "KeyState": "Enabled",
        "KeyUsage": "ENCRYPT/DECRYPT",
        "PrimaryKeyVersion": "0ec2d249-9f64-4d8f-9587-1215525e****",
        "DeleteDate": "",
        "Creator":"123456",
        "Arn":"acs:kms:cn-hangzhou:123456:key/08c33a6f-4e0a-4a1b-a3fa-7ddf****",
        "Origin":"Aliyun_KMS",
        "MaterialExpireTime":"",
        "ProtectionLevel":"SOFTWARE",
        "LastRotationDate": "2019-06-06T18:22:03Z",
        "AutomaticRotation": "Enabled",
        "RotationInterval": "31536000s",
        "NextRotationDate": "2020-07-06T18:22:03Z"
    },
    "RequestId": "3455b9b4-95c1-419d-b310-db6a53b09a39"
}
```

Error codes

4.10. ListKeys

Calls the ListKeys operation to query the IDs of all cmks in the region where you call the operation.

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ListKeys	The operation that you want to perform. Value: ListKeys

Parameter	Type	Required	Example	Description
PageNumber	Integer	Optional	1	The number of the page to return. Value range: greater than 0. Default value: 1.
PageSize	Integer	Optional	10	The number of entries returned on each page. Valid values: 1 to 100. Default value: 10.

Response parameters

Prameter	Type	Sample response	Description
TotalCount	Integer	3	The total number of cmks.
PageNumber	Integer	1	The number of the page to return.
PageSize	Integer	10	The number of entries returned on each page.
RequestId	String	1050b8f1-b264-496d-a782-6299cbaf15f8	The ID of the request.
Keys	Array		The CMK.
KeyId	String	08 c33a6 f-4e0a-4a1b-a3fa-7ddfa1d4 function compute instance *	The globally unique ID of the CMK.
KeyArn	String	acs:kms:cn-hangzhou:123456:key/80e9409f-78fa-42ab-84bd-83f40c81****	The ARN of the CMK.

Examples

Sample requests

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

Sample success responses

`XML` format

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

`JSON` format

```
//json response
{
    "Keys": {
        "Key": [
            {
                "KeyId": "80e9409f-78fa-42ab-84bd-83f40c81****",
                "KeyArn": "acs:kms:cn-hangzhou:123456:key/80e9409f-78fa-42ab-84bd-83f40c81****"

            },
            {
                "KeyId": "8fbb1226-a06f-4c57-8887-daa5b627****",
                "KeyArn": "acs:kms:cn-hangzhou:123456:key/8fbb1226-a06f-4c57-8887-daa5b627****
"
            },
              ]
        "TotalCount": 3,
    "PageNumber": 1,
    "PageSize": 10,
    "RequestId": "bc29ec35-3373-48d1-8202-520fd78d****"
}
```

Error codes

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

4.11. UpdateKeyDescription

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

The description of the CMK DescribeKey with the value passed in by the user. You can add, modify, or delete the description of a CMK through this operation.

Request parameters

Parameter	Type	Required or Not	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 success responses

`JSON` format

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

`XML` format

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

4.12. DescribeKeyVersion

Queries detailed information about a specified CMK version.

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeKeyVersion	The operation that you want to perform. Set the value to DescribeKeyVersion.
KeyId	String	Yes	1234abcd-12ab-34cd-56ef-12345678****	The globally unique ID of the CMK. You can also set this parameter to an alias that is bound to the CMK. For more information, see Use aliases.
KeyVersionId	String	Yes	2ab1a983-7072-4bbc-a582-584b5bd8****	The globally unique ID of the CMK version.

Response parameters

Parameter	Type	Example	Description
KeyVersion	Struct		The metadata of the CMK version.
CreationDate	String	2016-03-25T10:42:40Z	The date and time when the CMK version was created. The time is displayed in UTC.
KeyId	String	599fa825-17de-417e-9554-bb032cc6****	The globally unique ID of the CMK. Note If you set the KeyId parameter to the alias of the CMK, the ID of the CMK to which the alias is bound is returned.
KeyVersionId	String	2ab1a983-7072-4bbc-a582-584b5bd8****	The globally unique ID of the CMK version.
RequestId	String	7021b6ec-4be7-4d3c-8a68-1e85d4d515a0	The ID of the request.

Examples

Sample requests

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

Sample success responses

`XML` format

```
<KMS>
    <RequestId>7021b6ec-4be7-4d3c-8a68-1e85d4d515a0</RequestId>
    <KeyVersion>
        <CreationDate>2016-03-25T10:42:40Z</CreationDate>
        <KeyId>599fa825-17de-417e-9554-bb032cc6****</KeyId>
        <KeyVersionId>2ab1a983-7072-4bbc-a582-584b5bd8****</KeyVersionId>
    </KeyVersion>
</KMS>
```

`JSON` format

```
{
  "RequestId":"7021b6ec-4be7-4d3c-8a68-1e85d4d515a0",
  "KeyVersion":{
    "CreationDate":"2016-03-25T10:42:40Z",
    "KeyId":"599fa825-17de-417e-9554-bb032cc6****",
    "KeyVersionId":"2ab1a983-7072-4bbc-a582-584b5bd8****"
    }
}
```

4.13. ListKeyVersions

Queries all versions of a specified CMK.

Debugging

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

Request parameters

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

Response parameters

Parameter	Type	Example	Description
KeyVersions	Array		An array that consists of key versions.
KeyVersion			
CreationDate	String	2016-03-25T10:42:40Z	The date and time when the CMK version was created. The time is displayed in UTC.
KeyId	String	0b30658a-ed1a-4922-b8f7-a673ca9c****	The globally unique ID of the CMK. **Note** If you set the KeyId parameter to the alias of the CMK, the ID of the CMK to which the alias is bound is returned.
KeyVersionId	String	1e3304fd-68ac-4d5b-8886-ae5f01a1****	The globally unique ID of the CMK version.

Parameter	Type	Example	Description
PageNumber	Integer	1	The page number of the returned page.
PageSize	Integer	10	The number of entries returned per page.
RequestId	String	f71204c4-53cd-4eea-b405-653ba2db7e86	The ID of the request.
TotalCount	Integer	3	The total number of returned key versions.

Examples

Sample requests

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

Sample success responses

`XML` format

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

`JSON` format

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


4.14. UpdateRotationPolicy

Updates a key rotation policy.

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

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

Debugging

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

Request parameters

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

Response parameters

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

Examples

Sample requests

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

Sample success responses

`XML` format

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

`JSON` format

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

Error codes

4.15. CreateKeyVersion

Creates a new version for the CMK.

This operation is available only for asymmetric CMKs and only when the CMK is in the Enabled state. The minimum interval at which a key version is created is seven days. If you call this operation within seven days after the creation of the last key version, the error code **Rejected.UnsupportedOperation**is returned. The creation date of the last key version is specified by the **LastRotationDate** parameter. Each user can hold up to 50 asymmetric key versions in each region.

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description

Parameter	Type	Required	Example	Description
Action	String	Yes	CreateKeyVersion	The operation that you want to perform. Set the value to CreateKeyVersion.
KeyId	String	Yes	0b30658a-ed1a-4922-b8f7-a673ca9c****	The globally unique ID of the CMK.

Response parameters

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

Examples

Sample requests

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

Sample success responses

`XML` format

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

`JSON` format

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

Error codes

4.16. Encrypt

Encrypts plaintext by using a symmetric CMK.

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

Debugging

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

Request parameters

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

Response parameters

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

Examples

Sample requests

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

Sample success responses

`XML` format

```
<KMS>
    <RequestId>475f1620-b9d3-4d35-b5c6-3fbdd941423d</RequestId>
    <CiphertextBlob>DZhOWVmZDktM2QxNi00ODk0LWJkNGYtMWZjNDNmM2YyYWJmaaSl+TztSIMe43nb
TH/Z1Wr4XfLftKhAciUmDQXuMRl4WTvKhxjMThjK****</CiphertextBlob>
    <KeyId>1234abcd-12ab-34cd-56ef-12345678****</KeyId>
    <KeyVersionId>86a9efd9-3d16-4894-bd4f-1fc43f3f****</KeyVersionId>
</KMS>
```

`JSON` format

```
{
  "RequestId":"475f1620-b9d3-4d35-b5c6-3fbdd941423d",
  "CiphertextBlob":"DZhOWVmZDktM2QxNi00ODk0LWJkNGYtMWZjNDNmM2YyYWJmaaSl+TztSIMe43nbT
H/Z1Wr4XfLftKhAciUmDQXuMRl4WTvKhxjMThjK****",
  "KeyId":"1234abcd-12ab-34cd-56ef-12345678****",
  "KeyVersionId":"86a9efd9-3d16-4894-bd4f-1fc43f3f****"
}
```

4.17. GenerateDataKey

Call GenerateDataKey to generate a random data key. You can use the data key 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 returned plaintext to encrypt local data in services other than KMS in an offline manner. When storing encrypted data, you also need to store the ciphertext of the data key. 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 specified in the request is only used to encrypt the data key and is not involved in the generation of the data key. KMS does not record or store the generated data key, so you need to implement persistence of the data key cipher.

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

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

Debugging

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

Request parameters

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

Parameter	Type	Required	Example	Description
KeySpec	String	No	AES_256	The length of the generated data key. Valid values: • AES_256: a 256-bit symmetric key. • AES_128: a 128-bit symmetric key. Note We recommend that you use the KeySpec or NumberOfBytes parameter to specify the length of data keys. If neither is specified, KMS generates 256-bit data key. If both are specified, KMS ignores the KeySpec parameter.
NumberOfBytes	Integer	No	256	Specifies the length of the data key to generate. Value range: 1 to 1024 Unit: bytes.
EncryptionContext	Json	No	{"Example":"Example"}	The JSON string of the key-value pair. If you specify this parameter, it is also required when you call the Decrypt API operation. For more information, see EncryptionContext.

Response parameters

Parameter	Type	Example	Description
CiphertextBlob	String	ODZhOWVmZDktM2QxNi00ODk0LWJkNGYtMWZjNDNmM2YyYWJmS7FmDBBQ0BkKsQrtRnidtPwirmDcS0ZuJCU41xxAAWk4Z8qsADfbV0b+i6kQmlvj79dJdGOvtX69Uycs901qOjop4bTSl0oQ	The ciphertext of the data key encrypted by using the primary CMK version.

Parameter	Type	Example	Description
KeyId	String	599 fa825-17 de-417e-9554-bb032cc6 instance account number *	The globally unique ID of the CMK. Note If you set the KeyId parameter to the alias of the CMK, the ID of the CMK to which the alias is bound is returned.
KeyVersionId	String	2ab1a983-7072-4bbc-a582-584b5bd8****	The ID of the key version used to encrypt plaintext. It is the primary key version of the specified CMK.
Plaintext	String	Cost	The plaintext of the data key, which is encoded in Base64.
RequestId	String	7021 b6 ec-4be7-4d3c-8a68-1e85d4d515a0	The ID of the request.

Examples

Sample requests

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

Sample success responses

`XML` format

```
<KMS>
    <CiphertextBlob>ODZhOWVmZDktM2QxNi00ODk0LWJkNGYtMWZjNDNmM2YyYWJmS7FmDBBQ0BkK
sQrtRnidtPwirmDcS0ZuJCU41xxAAWk4Z8qsADfbV0b+i6kQmlvj79dJdGOvtX69Uycs901qOjop4bTSl0oQ</Ci
phertextBlob>
    <KeyId>599fa825-17de-417e-9554-bb032cc6****</KeyId>
    <KeyVersionId>2ab1a983-7072-4bbc-a582-584b5bd8****</KeyVersionId>
    <Plaintext>QmFzZTY0IGVuY29kZWQgcGxhaW50ZXh0</Plaintext>
    <RequestId>7021b6ec-4be7-4d3c-8a68-1e85d4d515a0</RequestId>
</KMS>
```

`JSON` format

```
{
    "CiphertextBlob": "ODZhOWVmZDktM2QxNi00ODk0LWJkNGYtMWZjNDNmM2YyYWJmS7FmDBBQ0BkK
sQrtRnidtPwirmDcS0ZuJCU41xxAAWk4Z8qsADfbV0b+i6kQmlvj79dJdGOvtX69Uycs901qOjop4bTSl0oQ",
    "KeyId": "599fa825-17de-417e-9554-bb032cc6****",
    "KeyVersionId": "2ab1a983-7072-4bbc-a582-584b5bd8****",
    "Plaintext": "QmFzZTY0IGVuY29kZWQgcGxhaW50ZXh0",
    "RequestId": "7021b6ec-4be7-4d3c-8a68-1e85d4d515a0"
}
```

Error codes

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

4.18. GenerateDataKeyWithoutPlaintext

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

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

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

Note

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

Debugging

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

Request parameters

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

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

Response parameters

Parameter	Type	Example	Description
CiphertextBlob	String	ODZhOWVmZDktM2QxNi00ODk0LWJkNGYtMWZjNDNmM2YyYWJmS7FmDBBQ0BkKsQrtRnidtPwirmDcS0ZuJCU41xxAAWk4Z8qsADfbV0b+i6kQmlvj79dJdGOvtX69Uycs901qOjop4bTS****	The ciphertext of the data that is encrypted by using the primary CMK version.

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

Examples

Sample requests

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

Sample success responses

`XML` format

```
<KMS>
    <RequestId>7021b6ec-4be7-4d3c-8a68-1e85d4d515a0</RequestId>
    <CiphertextBlob>ODZhOWVmZDktM2QxNi00ODk0LWJkNGYtMWZjNDNmM2YyYWJmS7FmDBBQ0BkKs
QrtRnidtPwirmDcS0ZuJCU41xxAAWk4Z8qsADfbV0b+i6kQmlvj79dJdGOvtX69Uycs901qOjop4bTS****</Ciph
ertextBlob>
    <KeyId>599fa825-17de-417e-9554-bb032cc6****</KeyId>
    <KeyVersionId>2ab1a983-7072-4bbc-a582-584b5bd8****</KeyVersionId>
</KMS>
```

`JSON` format

```
{
  "RequestId":"7021b6ec-4be7-4d3c-8a68-1e85d4d515a0",
  "CiphertextBlob":"ODZhOWVmZDktM2QxNi00ODk0LWJkNGYtMWZjNDNmM2YyYWJmS7FmDBBQ0BkKsQr
tRnidtPwirmDcS0ZuJCU41xxAAWk4Z8qsADfbV0b+i6kQmlvj79dJdGOvtX69Uycs901qOjop4bTS****",
  "KeyId":"599fa825-17de-417e-9554-bb032cc6****",
  "KeyVersionId":"2ab1a983-7072-4bbc-a582-584b5bd8****"
}
```


4.19. ExportDataKey

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

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

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

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ExportDataKey	The operation that you want to perform. Set the value to ExportDataKey.
CiphertextBlob	String	Yes	ODZhOWVmZDktM2QxNi00ODk0LWJkNGYtMWZjNDNmM2YyYWJmS7FmDBBQ0BkKsQrtRnidtPwirmDcS0ZuJCU41xxAAWk4Z8qsADfbV0b+i6kQmlvj79dJdGOvtX69Uycs901q********	The ciphertext of the data key encrypted by using a CMK.

Parameter	Type	Required	Example	Description
PublicKeyBlob	String	Yes	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAndKfC2ReLL2+y8a0+ZBBeAft/uBYo86GZiYJuflqgUzKxpyuvlo3uQkBv6b+nx+0tz8g8v7GhpPWMSW5L9mNHYsvYFsa7jTxsYdt17yj6GlUHPuMIs8hr5qbwl38IHU1iIa7nYWwE2fb3ePOvLDACRJVgGpU0yxioW80d2QD+9aU4jF5dlAahcfgsNzo2CXzCUc1+xbmNuq7Rp+H9VJB9dyYOwqnW3RhOLBo21FzpORapf0UiRlrHRpk1V6ez+aE1dofaYh/9bh0m6ioxj7j5hpZbWccuEZTMBKd+cbuBkRhJzc6Tti6qwZbDiu4fUwbZS0Tqpuo1UadiyxMW*********	A Base64-encoded public key.
WrappingAlgorithm	String	Yes	RSAES_OAEP_SHA_256	The encryption algorithm based on which you want to use the public key specified by PublicKeyBlob to encrypt the data key. For more information about encryption algorithms, see AsymmetricDecrypt. Valid values: • RSAES_OAEP_SHA_256 • RSAES_OAEP_SHA_1 • SM2PKE

Parameter	Type	Required	Example	Description
WrappingKeySpec	String	Yes	RSA_2048	The key type of the public key specified by PublicKeyBlob. For more information about key types, see Introduction to asymmetric keys. Valid values: • RSA_2048 • EC_SM2
EncryptionContext	Json	No	{"Example":"Example"}	A JSON string that consists of key-value pairs. If you specify this parameter when you use a CMK to encrypt the data key, an equivalent value is required here. For more information, see EncryptionContext.

Response parameters

Parameter	Type	Example	Description
ExportedDataKey	String	BQKP+1zK6+ZEMxTP5qaVzcsgXtWplYBKm0NXdSnB5FzliFxE1bSiu4dnEIlca2JpeH7yz1/S6fed630H+hIH6DoM25fTLNcKj+mFB0Xnh9m2+HN59Mn4qyTfcUeadnfCXSWcGBouhXFwcdd2rJ3n337bzTf4jm659gZu3L0i6PLuxM9p7mqdwO0cKJPfGVfhnfMz+f4alMg79WB/NNyE2lyX7/qxvV49ObNrrJbKSFiz8Djocaf0IESNLMbfYI5bXjWkJlX92DQbKhibtQW8ZOJ//ZC6t0AWcUoKL6QDm/dg5koQalcleRinpB+QadFm894sLbVZ9+N4GVs*******	The data key encrypted by using the public key and then exported.
KeyId	String	202b9877-5a25-46e3-a763-e20791b5****	The ID of the CMK that is used to decrypt the specified ciphertext of the data key. This parameter is the globally unique ID of the CMK.

Parameter	Type	Example	Description
KeyVersionId	String	2ab1a983-7072-4bbc-a582-584b5bd8****	The ID of the CMK version that is used to decrypt the specified ciphertext of the data key.
RequestId	String	4bd560a1-729e-45f1-a3d9-b2a33d61046b	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=ExportDataKey
&CiphertextBlob=ODZhOWVmZDktM2QxNi00ODk0LWJkNGYtMWZjNDNmM2YyYWJmS7FmDBBQ0BkKsQrtR
nidtPwirmDcS0ZuJCU41xxAAWk4Z8qsADfbV0b+i6kQmlvj79dJdGOvtX69Uycs901q********
&PublicKeyBlob=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAndKfC2ReLL2+y8a0+ZBBeAft/uB
Yo86GZiYJuflqgUzKxpyuvlo3uQkBv6b+nx+0tz8g8v7GhpPWMSW5L9mNHYsvYFsa7jTxsYdt17yj6GlUHPuMI
s8hr5qbwl38IHU1iIa7nYWwE2fb3ePOvLDACRJVgGpU0yxioW80d2QD+9aU4jF5dlAahcfgsNzo2CXzCUc1+xb
mNuq7Rp+H9VJB9dyYOwqnW3RhOLBo21FzpORapf0UiRlrHRpk1V6ez+aE1dofaYh/9bh0m6ioxj7j5hpZbWcc
uEZTMBKd+cbuBkRhJzc6Tti6qwZbDiu4fUwbZS0Tqpuo1UadiyxMW********
&WrappingAlgorithm=RSAES_OAEP_SHA_256
&WrappingKeySpec=RSA_2048
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
    <KeyId>202b9877-5a25-46e3-a763-e20791b5****</KeyId>
    <KeyVersionId>2ab1a983-7072-4bbc-a582-584b5bd8****</KeyVersionId>
    <ExportedDataKey>BQKP+1zK6+ZEMxTP5qaVzcsgXtWplYBKm0NXdSnB5FzliFxE1bSiu4dnEIlca2JpeH
7yz1/S6fed630H+hIH6DoM25fTLNcKj+mFB0Xnh9m2+HN59Mn4qyTfcUeadnfCXSWcGBouhXFwcdd2rJ3n337
bzTf4jm659gZu3L0i6PLuxM9p7mqdwO0cKJPfGVfhnfMz+f4alMg79WB/NNyE2lyX7/qxvV49ObNrrJbKSFiz8Dj
ocaf0IESNLMbfYI5bXjWkJlX92DQbKhibtQW8ZOJ//ZC6t0AWcUoKL6QDm/dg5koQalcleRinpB+QadFm894sLb
VZ9+N4GVs*******</ExportedDataKey>
    <RequestId>4bd560a1-729e-45f1-a3d9-b2a33d61046b</RequestId>
</KMS>
```

`JSON` format

```
{
  "KeyId": "202b9877-5a25-46e3-a763-e20791b5****",
  "KeyVersionId": "2ab1a983-7072-4bbc-a582-584b5bd8****",
  "ExportedDataKey": "BQKP+1zK6+ZEMxTP5qaVzcsgXtWplYBKm0NXdSnB5FzliFxE1bSiu4dnEIlca2JpeH7y
z1/S6fed630H+hIH6DoM25fTLNcKj+mFB0Xnh9m2+HN59Mn4qyTfcUeadnfCXSWcGBouhXFwcdd2rJ3n337bz
Tf4jm659gZu3L0i6PLuxM9p7mqdwO0cKJPfGVfhnfMz+f4alMg79WB/NNyE2lyX7/qxvV49ObNrrJbKSFiz8Djoc
af0IESNLMbfYI5bXjWkJlX92DQbKhibtQW8ZOJ//ZC6t0AWcUoKL6QDm/dg5koQalcleRinpB+QadFm894sLbVZ
9+N4GVs*******",
  "RequestId": "4bd560a1-729e-45f1-a3d9-b2a33d61046b"
}
```


Error codes

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

4.20. GenerateAndExportDataKey

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

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

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

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

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	GenerateAndExportDataKey	The operation that you want to perform. Set the value to GenerateAndExportDataKey.
KeyId	String	Yes	1234abcd-12ab-34cd-56ef-12345678****	The globally unique ID of the CMK. You can also set this parameter to an alias that is bound to the CMK. For more information, see Use aliases.
PublicKeyBlob	String	Yes	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAndKfC2ReLL2+y8a0+ZBBeAft/uBYo86GZiYJuflqgUzKxpyuvlo3uQkBv6b+nx+0tz8g8v7GhpPWMSW5L9mNHYsvYFsa7jTxsYdt17yj6GlUHPuMIs8hr5qbwl38IHU1iIa7nYWwE2fb3ePOvLDACRJVgGpU0yxioW80d2QD+9aU4jF5dlAahcfgsNzo2CXzCUc1+xbmNuq7Rp+H9VJB9dyYOwqnW3RhOLBo21FzpORapf0UiRlrHRpk1V6ez+aE1dofaYh/9bh0m6ioxj7j5hpZbWccuEZTMBKd+cbuBkRhJzc6Tti6qwZbDiu4fUwbZS0Tqpuo1UadiyxMW*******	A Base64-encoded public key.

Parameter	Type	Required	Example	Description
WrappingAlgorithm	String	Yes	RSAES_OAEP_SHA_256	The encryption algorithm based on which you want to use the public key specified by PublicKeyBlob to encrypt the data key. For more information about encryption algorithms, see AsymmetricDecrypt. Valid values: • RSAES_OAEP_SHA_256 • RSAES_OAEP_SHA_1 • SM2PKE
WrappingKeySpec	String	Yes	RSA_2048	The key type of the public key specified by PublicKeyBlob. For more information about key types, see Introduction to asymmetric keys. Valid values: • RSA_2048 • EC_SM2
KeySpec	String	No	AES_256	The length of the data key that you want to generate. Valid values: • AES_256: a 256-bit symmetric key • AES_128: a 128-bit symmetric key Note We recommend that you use the KeySpec or NumberOfBytes parameter to specify the length of a data key. If both parameters are not specified, KMS generates a 256-bit data key. If both parameters are specified, KMS ignores the KeySpec parameter.
NumberOfBytes	Integer	No	32	The length of the data key that you want to generate. Valid values: 1 to 1024. Unit: bytes.

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

Response parameters

Parameter	Type	Example	Description
CiphertextBlob	String	ODZhOWVmZDktM2QxNi00ODk0LWJkNGYtMWZjNDNmM2YyYWJmS7FmDBBQ0BkKsQrtRnidtPwirmDcS0ZuJCU41xxAAWk4Z8qsADfbV0b+i6kQmlvj79dJdGOvtX69Uycs901qOjop4bTS****	The ciphertext of the data key encrypted by using the primary CMK version.
ExportedDataKey	String	BQKP+1zK6+ZEMxTP5qaVzcsgXtWplYBKm0NXdSnB5FzliFxE1bSiu4dnEIlca2JpeH7yz1/S6fed630H+hIH6DoM25fTLNcKj+mFB0Xnh9m2+HN59Mn4qyTfcUeadnfCXSWcGBouhXFwcdd2rJ3n337bzTf4jm659gZu3L0i6PLuxM9p7mqdwO0cKJPfGVfhnfMz+f4alMg79WB/NNyE2lyX7/qxvV49ObNrrJbKSFiz8Djocaf0IESNLMbfYI5bXjWkJlX92DQbKhibtQW8ZOJ//ZC6t0AWcUoKL6QDm/dg5koQalcleRinpB+QadFm894sLbVZ9+N4GVs*******	The data key encrypted by using the public key and then exported.

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

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=GenerateAndExportDataKey
&KeyId=1234abcd-12ab-34cd-56ef-12345678****
&PublicKeyBlob=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAndKfC2ReLL2+y8a0+ZBBeAft/uB
Yo86GZiYJuflqgUzKxpyuvlo3uQkBv6b+nx+0tz8g8v7GhpPWMSW5L9mNHYsvYFsa7jTxsYdt17yj6GlUHPuMI
s8hr5qbwl38IHU1iIa7nYWwE2fb3ePOvLDACRJVgGpU0yxioW80d2QD+9aU4jF5dlAahcfgsNzo2CXzCUc1+xb
mNuq7Rp+H9VJB9dyYOwqnW3RhOLBo21FzpORapf0UiRlrHRpk1V6ez+aE1dofaYh/9bh0m6ioxj7j5hpZbWcc
uEZTMBKd+cbuBkRhJzc6Tti6qwZbDiu4fUwbZS0Tqpuo1UadiyxMW********
&WrappingAlgorithm=RSAES_OAEP_SHA_256
&WrappingKeySpec=RSA_2048
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
    <KeyId>202b9877-5a25-46e3-a763-e20791b5****</KeyId>
    <KeyVersionId>2ab1a983-7072-4bbc-a582-584b5bd8****</KeyVersionId>
    <CiphertextBlob>ODZhOWVmZDktM2QxNi00ODk0LWJkNGYtMWZjNDNmM2YyYWJmS7FmDBBQ0BkK
sQrtRnidtPwirmDcS0ZuJCU41xxAAWk4Z8qsADfbV0b+i6kQmlvj79dJdGOvtX69Uycs901qOjop4bTS****</Cip
hertextBlob>
    <ExportedDataKey>BQKP+1zK6+ZEMxTP5qaVzcsgXtWplYBKm0NXdSnB5FzliFxE1bSiu4dnEIlca2JpeH
7yz1/S6fed630H+hIH6DoM25fTLNcKj+mFB0Xnh9m2+HN59Mn4qyTfcUeadnfCXSWcGBouhXFwcdd2rJ3n337
bzTf4jm659gZu3L0i6PLuxM9p7mqdwO0cKJPfGVfhnfMz+f4alMg79WB/NNyE2lyX7/qxvV49ObNrrJbKSFiz8Dj
ocaf0IESNLMbfYI5bXjWkJlX92DQbKhibtQW8ZOJ//ZC6t0AWcUoKL6QDm/dg5koQalcleRinpB+QadFm894sLb
VZ9+N4GVs*******</ExportedDataKey>
    <RequestId>4bd560a1-729e-45f1-a3d9-b2a33d61046b</RequestId>
</KMS>
```

`JSON` format

```
{
  "KeyId": "202b9877-5a25-46e3-a763-e20791b5****",
  "KeyVersionId": "2ab1a983-7072-4bbc-a582-584b5bd8****",
  "CiphertextBlob":"ODZhOWVmZDktM2QxNi00ODk0LWJkNGYtMWZjNDNmM2YyYWJmS7FmDBBQ0BkKsQr
tRnidtPwirmDcS0ZuJCU41xxAAWk4Z8qsADfbV0b+i6kQmlvj79dJdGOvtX69Uycs901qOjop4bTS****",
  "ExportedDataKey": "BQKP+1zK6+ZEMxTP5qaVzcsgXtWplYBKm0NXdSnB5FzliFxE1bSiu4dnEIlca2JpeH7y
z1/S6fed630H+hIH6DoM25fTLNcKj+mFB0Xnh9m2+HN59Mn4qyTfcUeadnfCXSWcGBouhXFwcdd2rJ3n337bz
Tf4jm659gZu3L0i6PLuxM9p7mqdwO0cKJPfGVfhnfMz+f4alMg79WB/NNyE2lyX7/qxvV49ObNrrJbKSFiz8Djoc
af0IESNLMbfYI5bXjWkJlX92DQbKhibtQW8ZOJ//ZC6t0AWcUoKL6QDm/dg5koQalcleRinpB+QadFm894sLbVZ
9+N4GVs*******",
  "RequestId": "207596a2-36d3-4840-b1bd-f87044699bd7"
}
```

Error codes

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

4.21. Decrypt

Decrypts the ciphertext that is specified by the CiphertextBlob parameter.

You can call this operation to decrypt the ciphertext that is generated by using the following operations:

- GenerateDataKey
- Encrypt
- GenerateDataKeyWithoutPlaintext

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	Decrypt	The operation that you want to perform. Set the value to Decrypt.
CiphertextBlob	String	Yes	DZhOWVmZDktM2QxNi00ODk0LWJkNGYtMWZjNDNmM2YyYWJmaaSl+TztSIMe43nbTH/Z1Wr4XfLftKhAciUmDQXuMRl4WTvKhxjMThjK****	The ciphertext that you want to decrypt.
EncryptionContext	Json	No	{"Example":"Example"}	A JSON string that consists of key-value pairs. If you specify this parameter when you encrypt the data or data key, an equivalent value is required here. For more information, see EncryptionContext.

Response parameters

Parameter	Type	Example	Description
KeyId	String	202b9877-5a25-46e3-a763-e20791b5****	The ID of the CMK that is used to decrypt the ciphertext. This parameter is the globally unique ID of the CMK.

Parameter	Type	Example	Description
KeyVersionId	String	2ab1a983-7072-4bbc-a582-584b5bd8****	The ID of the CMK version that is used to decrypt the ciphertext.
Plaintext	String	tRYXuCwgja12xxO1N/gZERDDCLw9doZEQiPDk/Bv****	The decrypted plaintext.
RequestId	String	207596a2-36d3-4840-b1bd-f87044699bd7	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=Decrypt
&CiphertextBlob=DZhOWVmZDktM2QxNi00ODk0LWJkNGYtMWZjNDNmM2YyYWJmaaSl+TztSIMe43nbTH/Z
1Wr4XfLftKhAciUmDQXuMRl4WTvKhxjMThjK****
&<Common request parameters>
```

Sample success responses

`XML` format

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

`JSON` format

```
{
  "KeyId": "202b9877-5a25-46e3-a763-e20791b5****",
  "KeyVersionId": "2ab1a983-7072-4bbc-a582-584b5bd8****",
  "Plaintext": "tRYXuCwgja12xxO1N/gZERDDCLw9doZEQiPDk/Bv****",
  "RequestId": "207596a2-36d3-4840-b1bd-f87044699bd7"
}
```

4.22. ReEncrypt

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

You can call this operation in the following scenarios:

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

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

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

Debugging

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

Request parameters

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

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

Parameter	Type	Required	Example	Description
SourceKeyVersionId	String	No	2ab1a983-7072-4bbc-a582-584b5bd8****	The ID of the CMK version that is used to decrypt the ciphertext. Note If you set CiphertextBlob to the public key-encrypted ciphertext that is returned after an asymmetric encryption operation, specify this parameter.
SourceEncryptionAlgorithm	String	No	RSAES_OAEP_SHA_256	The encryption algorithm based on which the public key is used to encrypt the ciphertext specified by CiphertextBlob. For more information about encryption algorithms, see AsymmetricDecrypt. Valid values: • RSAES_OAEP_SHA_256 • RSAES_OAEP_SHA_1 • SM2PKE Note If you set CiphertextBlob to the public key-encrypted ciphertext that is returned after an asymmetric encryption operation, specify this parameter.

Parameter	Type	Required	Example	Description
SourceEncryptionContext	Json	No	{"Example":"Example"}	A JSON string that consists of key-value pairs. If you specify EncryptionContext when you call the Encrypt, GenerateDataKey, GenerateDataKeyWithoutPlaintext, or GenerateAndExportDataKey operation to encrypt the data or data key, an equivalent value is required here. For more information, see EncryptionContext. Note If you set CiphertextBlob to the ciphertext that is returned after a symmetric encryption operation, specify this parameter.
DestinationEncryptionContext	Json	No	{"Example":"Example"}	A JSON string that consists of key-value pairs. This parameter specifies the EncryptionContext that is used to re-encrypt the decrypted data or data key.

Response parameters

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

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=ReEncrypt
&CiphertextBlob=ODZhOWVmZDktM2QxNi00ODk0LWJkNGYtMWZjNDNmM2YyYWJmS7FmDBBQ0BkKsQrtR
nidtPwirmDcS0ZuJCU41xxAAWk4Z8qsADfbV0b+i6kQmlvj79dJdGOvtX69Uycs901q********
&DestinationKeyId=1234abcd-12ab-34cd-56ef-12345678****
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
        <KeyId>202b9877-5a25-46e3-a763-e20791b5****</KeyId>
        <KeyVersionId>2ab1a983-7072-4bbc-a582-584b5bd8****</KeyVersionId>
        <CiphertextBlob>DZhOWVmZDktM2QxNi00ODk0LWJkNGYtMWZjNDNmM2YyYWJmaaSl+TztSIMe43n
bTH/Z1Wr4XfLftKhAciUmDQXuMRl4WTvKhxjMThjK****</CiphertextBlob>
        <RequestId>4bd560a1-729e-45f1-a3d9-b2a33d61046b</RequestId>
</KMS>
```

`JSON` format

```
{
   "KeyId": "202b9877-5a25-46e3-a763-e20791b5****",
   "KeyVersionId": "2ab1a983-7072-4bbc-a582-584b5bd8****",
   "CiphertextBlob": "DZhOWVmZDktM2QxNi00ODk0LWJkNGYtMWZjNDNmM2YyYWJmaaSl+TztSIMe43nbT
H/Z1Wr4XfLftKhAciUmDQXuMRl4WTvKhxjMThjK****",
   "RequestId": "4bd560a1-729e-45f1-a3d9-b2a33d61046b"
}
```

Error codes

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

4.23. AsymmetricSign

Uses asymmetric keys to sign signatures.

This operation is only supported for asymmetric keys with **Usage** set to **SIGN/VERIFY**. The following table lists the supported signature algorithms.

KeySpec	Algorithm	Description
RSA_2048	RSA_PSS_SHA_256	RSASSA-PSS using SHA-256 and MGF1 with SHA-256
RSA_2048	RSA_PKCS1_SHA_256	RSASSA-PKCS1-v1_5 using SHA-256
EC_P256	ECDSA_SHA_256	ECDSA on the P-256 Curve(secp256r1) with a SHA-256 digest
EC_P256K	ECDSA_SHA_256	ECDSA on the P-256K Curve(secp256k1) with a SHA-256 digest
EC_SM2	SM2DSA	SM2 Elliptic Curve Digital Signature Algorithm

Note According to the national standard GBT32918, when calculating SM2 signature value, **Digest** the parameter is not directly used to calculate the SM3 digest, but for the Z(A) the digest computed based on the mosaic values of and M, where M is the original message to be signed and Z(A) is A hash value for user A as defined in gbt32918.

Debugging

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

Request parameters

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

Parameter	Type	Required	Example	Description
Algorithm	String	Yes	RSA_PSS_SHA_256	The signature algorithm to use.
Digest	String	Yes	ZOyIygCyaOW6GjVnihtTFtIS9PNmskdyMlNKiuyjfzw=	Use **Algorithm**, which is the digest generated for the original message. Note Use Base64 encoding.
KeyId	String	Yes	5c438b18-05be-40ad-b6c2-3be6752c****	The globally unique ID of the CMK. Note This parameter can also be specified as an alias bound to the master key. For more information, see use aliases.
KeyVersionId	String	Yes	2ab1a983-7072-4bbc-a582-584b5bd8****	The globally unique ID of the CMK version.

Response parameters

Parameter	Type	Example	Description
KeyId	String	5c438b18-05be-40ad-b6c2-3be6752c****	The globally unique ID of the CMK. Note If you set the KeyId parameter to the alias of a CMK, the ID of the CMK created by the alias is returned.
KeyVersionId	String	2ab1a983-7072-4bbc-a582-584b5bd8****	The globally unique ID of the CMK version.

Parameter	Type	Example	Description
Value	String	M2CceNZH00ZgL9ED/ZHFp21YRAvYeZHknJUc207OCZ0N9wNn9As4z2bON3FF3je+1Nu+2+/8Zj50HpMTpzYpMp2R93cYmACCmhaYoKydxylbyGzJR8y9likZRCrkD38lRoS40aBBvv/6iRKzQuo9EGYVcel36cMNg00VmYNBy3pa1rwg3gA4l3cy6kjayZja1WGPkVhrVKsrJMdbpl0ApLjXKuD8rw1n1XLCwCUEL5eLPljTZaAveqdOFQOiZnZEGI27qIiZe7I1fN8tcz6anS/gTM7xRKE++5egEvRWlTQQTJeApnPSiUPA+8ZykNdelQsOQh5SrGoyI4A5pq3a/w==	The calculated signature. Note Use Base64 encoding.
RequestId	String	475f1620-b9d3-4d35-b5c6-3fbdd941423d	The ID of the request.

Examples

Sample requests

```
https://[Endpoint]/?Action=AsymmetricSign
&KeyId=5c438b18-05be-40ad-b6c2-3be6752c****
&KeyVersionId=2ab1a983-7072-4bbc-a582-584b5bd8****
&Algorithm=RSA_PSS_SHA_256
&Digest=ZOyIygCyaOW6GjVnihtTFtIS9PNmskdyMlNKiuyjfzw=
&<Common request parameters>
```

Sample success responses

`XML` format

```
<KMS>
  <KeyId>5c438b18-05be-40ad-b6c2-3be6752c****</KeyId>
  <KeyVersionId>2ab1a983-7072-4bbc-a582-584b5bd8****</KeyVersionId>
  <Value>M2CceNZH00ZgL9ED/ZHFp21YRAvYeZHknJUc207OCZ0N9wNn9As4z2bON3FF3je+1Nu+2+/8Zj5
0HpMTpzYpMp2R93cYmACCmhaYoKydxylbyGzJR8y9likZRCrkD38lRoS40aBBvv/6iRKzQuo9EGYVcel36cMNg
00VmYNBy3pa1rwg3gA4l3cy6kjayZja1WGPkVhrVKsrJMdbpl0ApLjXKuD8rw1n1XLCwCUEL5eLPljTZaAveqd
OFQOiZnZEGI27qliZe7I1fN8tcz6anS/gTM7xRKE++5egEvRWlTQQTJeApnPSiUPA+8ZykNdelQsOQh5SrGoyI4
A5pq3a/w==</Value>
  <RequestId>475f1620-b9d3-4d35-b5c6-3fbdd941423d</RequestId>
</KMS>
```

`JSON` format

```
{
 "KeyId": "5c438b18-05be-40ad-b6c2-3be6752c****",
 "KeyVersionId": "2ab1a983-7072-4bbc-a582-584b5bd8****",
 "Value": "M2CceNZH00ZgL9ED/ZHFp21YRAvYeZHknJUc207OCZ0N9wNn9As4z2bON3FF3je+1Nu+2+/8Zj5
0HpMTpzYpMp2R93cYmACCmhaYoKydxylbyGzJR8y9likZRCrkD38lRoS40aBBvv/6iRKzQuo9EGYVcel36cMNg
00VmYNBy3pa1rwg3gA4l3cy6kjayZja1WGPkVhrVKsrJMdbpl0ApLjXKuD8rw1n1XLCwCUEL5eLPljTZaAveqd
OFQOiZnZEGI27qliZe7I1fN8tcz6anS/gTM7xRKE++5egEvRWlTQQTJeApnPSiUPA+8ZykNdelQsOQh5SrGoyI4
A5pq3a/w==",
 "RequestId": "475f1620-b9d3-4d35-b5c6-3fbdd941423d"
}
```

4.24. AsymmetricVerify

Call AsymmetricVerify API to use asymmetric keys for verification.

This operation is only supported for asymmetric keys with **Usage** set to **SIGN/VERIFY**. The following table lists the supported signature algorithms.

KeySpec	Algorithm	Description
RSA_2048	RSA_PSS_SHA_256	RSASSA-PSS using SHA-256 and MGF1 with SHA-256
RSA_2048	RSA_PKCS1_SHA_256	RSASSA-PKCS1-v1_5 using SHA-256

KeySpec	Algorithm	Description
EC_P256	ECDSA_SHA_256	ECDSA on the P-256 Curve(secp256r1) with a SHA-256 digest
EC_P256K	ECDSA_SHA_256	ECDSA on the P-256K Curve(secp256k1) with a SHA-256 digest
EC_SM2	SM2DSA	SM2 Elliptic Curve Digital Signature Algorithm

Note According to the national standard GBT32918, when calculating SM2 signature value, **Digest** the parameter is not directly used to calculate the SM3 digest, but for the Z(A) the digest computed based on the mosaic values of and M, where M is the original message to be signed and Z(A) is A hash value for user A as defined in gbt32918.

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	AsymmetricVerify	The operation that you want to perform. Set the value to **AsymmetricVerify**.
Algorithm	String	Yes	RSA_PSS_SHA_256	The signature algorithm to use.
Digest	String	Yes	ZOyIygCyaOW6GjVnihtTFtIS9PNmskdyMlNKiuyjfzw=	Use **Algorithm**, which is the digest generated for the original message. **Note** Use Base64 encoding.

Parameter	Type	Required	Example	Description
KeyId	String	Yes	5c438b18-05be-40ad-b6c2-3be6752c****	The globally unique ID of the CMK. Note This parameter can also be specified as an alias bound to the master key. For more information, see use aliases.
KeyVersionId	String	Yes	2ab1a983-7072-4bbc-a582-584b5bd8****	The globally unique ID of the CMK version.
Value	String	Yes	M2CceNZH00ZgL9ED/ZHFp21YRAvYeZHknJUc207OCZ0N9wNn9As4z2bON3FF3je+1Nu+2+/8Zj50HpMTpzYpMp2R93cYmACCmhaYoKydxylbyGzJR8y9likZRCrkD38lRoS40aBBvv/6iRKzQuo9EGYVcel36cMNg00VmYNBy3pa1rwg3gA4l3cy6kjayZja1WGPkVhrVKsrJMdbpl0ApLjXKuD8rw1n1XLCwCUEL5eLPljTZaAveqdOFQOiZnZEGI27qIiZe7I1fN8tcz6anS/gTM7xRKE++5egEvRWlTQQTJeApnPSiUPA+8ZykNdelQsOQh5SrGoyI4A5pq3a/w==	The signature value to be verified. Note Use Base64 encoding.

Response parameters

Parameter	Type	Example	Description

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

Examples

Sample requests

```
https://[Endpoint]/?Action=AsymmetricVerify
&KeyId=5c438b18-05be-40ad-b6c2-3be6752c****
&KeyVersionId=2ab1a983-7072-4bbc-a582-584b5bd8****
&Algorithm=RSA_PSS_SHA_256
&Digest=ZOyIygCyaOW6GjVnihtTFtIS9PNmskdyMlNKiuyjfzw=
&Value=M2CceNZH00ZgL9ED/ZHFp21YRAvYeZHknJUc207OCZ0N9wNn9As4z2bON3FF3je+1Nu+2+/8Zj50H
pMTpzYpMp2R93cYmACCmhaYoKydxylbyGzJR8y9likZRCrkD38lRoS40aBBvv/6iRKzQuo9EGYVcel36cMNg00
VmYNBy3pa1rwg3gA4l3cy6kjayZja1WGPkVhrVKsrJMdbpl0ApLjXKuD8rw1n1XLCwCUEL5eLPljTZaAveqdOF
QOiZnZEGI27qIiZe7I1fN8tcz6anS/gTM7xRKE++5egEvRWlTQQTJeApnPSiUPA+8ZykNdelQsOQh5SrGoyI4A5
pq3a/w==
&<Common request parameters>
```

Sample success responses

`XML` format

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

`JSON` format

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

4.25. AsymmetricDecrypt

Call AsymmetricDecrypt API to decrypt data using asymmetric keys.

This operation is only supported for asymmetric keys with **Usage** set to **ENCRYPT/DECRYPT**. The following table lists the supported encryption algorithms.

KeySpec	Algorithm	Description	The length of the ciphertext. Unit: bytes.
RSA_2048	RSAES_OAEP_SHA_256	RSAES-OAEP using SHA-256 and MGF1 with SHA-256	256
RSA_2048	RSAES_OAEP_SHA_1	RSAES-OAEP using SHA1 and MGF1 with SHA1	256
EC_SM2	SM2PKE	SM2 elliptic curve public key encryption algorithm	Maximum 6144

The ciphertext is generated either by calling the **AsymmetricEncrypt** operation or by using one of the two asymmetric decryption algorithms listed above.

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	AsymmetricDecrypt	The operation that you want to perform. Set the value to **AsymmetricDecrypt**.
Algorithm	String	Yes	RSAES_OAEP_SHA_1	The asymmetric decryption algorithm to use.
CiphertextBlob	String	Yes	BQKP+1zK6+ZEMxTP5qaVzcsgXtWplYBKm0NXdSnB5FzliFxE1bSiu4dnEIlca2JpeH7yz1/S6fed630H+hIH6DoM25fTLNcKj+mFB0Xnh9m2+HN59Mn4qyTfcUeadnfCXSWcGBouhXFwcdd2rJ3n337bzTf4jm659gZu3L0i6PLuxM9p7mqdwO0cKJPfGVfhnfMz+f4alMg79WB/NNyE2lyX7/qxvV49ObNrrJbKSFiz8Djocaf0IESNLMbfYI5bXjWkJlX92DQbKhibtQW8ZOJ//ZC6t0AWcUoKL6QDm/dg5koQalcleRinpB+QadFm894sLbVZ9+N4GVsv1Wbjwg==	Decrypt the ciphertext. Note Use Base64 encoding.
KeyId	String	Yes	5c438b18-05be-40ad-b6c2-3be6752c****	The globally unique ID of the CMK. Note This parameter can also be specified as an alias bound to the CMK. For more information, see use aliases.

Parameter	Type	Required	Example	Description
KeyVersionId	String	Yes	2ab1a983-7072-4bbc-a582-584b5bd8****	The globally unique ID of the CMK version.

Response parameters

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

Examples

Sample requests

```
https://[Endpoint]/?Action=AsymmetricDecrypt
&Algorithm=RSAES_OAEP_SHA_1
&CiphertextBlob=BQKP+1zK6+ZEMxTP5qaVzcsgXtWplYBKm0NXdSnB5FzliFxE1bSiu4dnEllca2JpeH7yz1/S6
fed630H+hIH6DoM25fTLNcKj+mFB0Xnh9m2+HN59Mn4qyTfcUeadnfCXSWcGBouhXFwcdd2rJ3n337bzTf4jm
659gZu3L0i6PLuxM9p7mqdwO0cKJPfGVfhnfMz+f4alMg79WB/NNyE2lyX7/qxvV49ObNrrJbKSFiz8Djocaf0IES
NLMbfYI5bXjWkJlX92DQbKhibtQW8ZOJ//ZC6t0AWcUoKL6QDm/dg5koQalcleRinpB+QadFm894sLbVZ9+N4
GVsv1Wbjwg==
&KeyId=5c438b18-05be-40ad-b6c2-3be6752c****
&KeyVersionId=2ab1a983-7072-4bbc-a582-584b5bd8****
&<Common request parameters>
```

Sample success responses

`XML` format

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

`JSON` format

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

4.26. AsymmetricEncrypt

Call the AsymmetricEncrypt operation to encrypt data using asymmetric keys.

This operation is only supported for asymmetric keys with **Usage** set to **ENCRYPT/DECRYPT**. The following table lists the supported encryption algorithms.

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

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	AsymmetricEncrypt	The operation that you want to perform. Set the value to **AsymmetricEncrypt**.
Algorithm	String	Yes	RSAES_OAEP_SHA_1	The asymmetric encryption algorithm to use.
KeyId	String	Yes	5c438b18-05be-40ad-b6c2-3be6752c****	The globally unique ID of the CMK. **Note** This parameter can also be specified as an alias bound to the master key. For more information, see use aliases.
KeyVersionId	String	Yes	2ab1a983-7072-4bbc-a582-584b5bd8****	The globally unique ID of the CMK version.
Plaintext	String	Yes	SGVsbG8gd29ybGQ=	The plaintext to be encrypted, which must be Base64-encoded.

Response parameters

Parameter	Type	Example	Description
KeyId	String	5c438b18-05be-40ad-b6c2-3be6752c****	The globally unique ID of the CMK. **Note** If you set the KeyId parameter to the alias of a CMK, the ID of the CMK created by the alias is returned.

Parameter	Type	Example	Description
KeyVersionId	String	2ab1a983-7072-4bbc-a582-584b5bd8****	The CMK version used to encrypt the plaintext.
CiphertextBlob	String	BQKP+1zK6+ZEMxTP5qaVzcsgXtWplYBKm0NXdSnB5FzliFxE1bSiu4dnEIlca2JpeH7yz1/S6fed630H+hIH6DoM25fTLNcKj+mFB0Xnh9m2+HN59Mn4qyTfcUeadnfCXSWcGBouhXFwcdd2rJ3n337bzTf4jm659gZu3L0i6PLuxM9p7mqdwO0cKJPfGVfhnfMz+f4alMg79WB/NNyE2lyX7/qxvV49ObNrrJbKSFiz8Djocaf0IESNLMbfYI5bXjWkJlX92DQbKhibtQW8ZOJ//ZC6t0AWcUoKL6QDm/dg5koQalcleRinpB+QadFm894sLbVZ9+N4GVsv1Wbjwg==	The encrypted ciphertext. Note Use Base64 encoding.
RequestId	String	475f1620-b9d3-4d35-b5c6-3fbdd941423d	The ID of the request.

Examples

Sample requests

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

Sample success responses

`XML` format

```
<KMS>
  <KeyId>5c438b18-05be-40ad-b6c2-3be6752c****</KeyId>
  <KeyVersionId>2ab1a983-7072-4bbc-a582-584b5bd8****</KeyVersionId>
  <CiphertextBlob>RKF5WeXJtusIrvuPOjpkA/55EKzi8Wmc/eJ2fQUKphvL750jtInSX1wijw/7jGxUaTHTW6tgIJ
l2ReN1aI1/wxqGxdzScwsMHxCBncnzQsZF+Fi4UFpI9pr4A1wc2u5Ngwyx9uA4K/kJ5bkS4NvmanxssAPZfSfb
JSrAWlCP11tS0Cd54tQVGj4XK9tP9bJDKzKis1NClsOXZtNPX88kUqr3LkgFCsD07IwiePAfI2tn2fzeisje1Q7/d6V
kF48c3ZE0DAmnLRujt3yRRGDaKUkI6SUDjuKD4yqBUX15/DKfJtya+JIPQGiO2IEPlhL7+NMT17U0tKtK5ZPNEwx
fZw==</CiphertextBlob>
  <RequestId>475f1620-b9d3-4d35-b5c6-3fbdd941423d</RequestId>
</KMS>
```

`JSON` format

```
{
 "KeyId": "5c438b18-05be-40ad-b6c2-3be6752c****",
 "KeyVersionId": "2ab1a983-7072-4bbc-a582-584b5bd8****",
 "CiphertextBlob": "RKF5WeXJtusIrvuPOjpkA/55EKzi8Wmc/eJ2fQUKphvL750jtInSX1wijw/7jGxUaTHTW6tgI
Jl2ReN1aI1/wxqGxdzScwsMHxCBncnzQsZF+Fi4UFpI9pr4A1wc2u5Ngwyx9uA4K/kJ5bkS4NvmanxssAPZfSf
bJSrAWlCP11tS0Cd54tQVGj4XK9tP9bJDKzKis1NClsOXZtNPX88kUqr3LkgFCsD07IwiePAfI2tn2fzeisje1Q7/d6
VkF48c3ZE0DAmnLRujt3yRRGDaKUkI6SUDjuKD4yqBUX15/DKfJtya+JIPQGiO2IEPlhL7+NMT17U0tKtK5ZPNEw
xfZw==",
 "RequestId": "475f1620-b9d3-4d35-b5c6-3fbdd941423d"
}
```

4.27. GetPublicKey

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

Debugging

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

Request parameters

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

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

Response parameters

Parameter	Type	Example	Description
KeyId	String	5c438b18-05be-40ad-b6c2-3be6752c****	The globally unique ID of the CMK. Note If you set the KeyId parameter to the alias of the CMK, the ID of the CMK to which the alias is bound is returned.
KeyVersionId	String	2ab1a983-7072-4bbc-a582-584b5bd8****	The version of the CMK that is used to encrypt the plaintext.

Parameter	Type	Example	Description
PublicKey	String	-----BEGIN PUBLIC KEY----- \nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAs5Yu9AEgATN2/e3nUz1K\nEy6ng8MSPutcse2/VECG/NUF9C6D4IsJ64ShzY3dcn34WYzTOe916eMJFxyrNrSw\nHtc4UOR5AvaoRrfpgu2uq+i70/ZXrWL+pGb1hgZV8cWheIHMxwrR3IiQlM5qN7EF\n9BdyWtyBfUGsp0Bn1VqlPc5G0x0a9xU2z9YtP994yDenNVIoIQ6Cov1lIEuwXAb2\n7boC41ePXwD0JWt41sP+rgCmpjBx00puIG+IlnoReEgI1ZGYmK98GgA/XzmNjZiD\nyvXJZAcM33Ue85+PkR5iHTtSEbi4QAoqpJabprUzz3Fin2j1dRrcacxGb7p31A9c\nJQIDAQAB\n----- END PUBLIC KEY-----\n	The public key returned in the PEM format.
RequestId	String	475f1620-b9d3-4d35-b5c6-3fbdd941423d	The ID of the request.

Examples

Sample requests

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

Sample success responses

`XML` format

```
<KMS>
  <KeyId>5c438b18-05be-40ad-b6c2-3be6752c****</KeyId>
  <KeyVersionId>2ab1a983-7072-4bbc-a582-584b5bd8****</KeyVersionId>
  <PublicKey>-----BEGIN PUBLIC KEY-----\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAs5Yu9
AEgATN2/e3nUz1K\nEy6ng8MSPutcse2/VECG/NUF9C6D4IsJ64ShzY3dcn34WYzTOe916eMJFxyrNrSw\nHtc
4UOR5AvaoRrfpgu2uq+i70/ZXrWL+pGb1hgZV8cWheIHMxwrR3IiQlM5qN7EF\n9BdyWtyBfUGsp0Bn1VqlPc5
G0x0a9xU2z9YtP994yDenNVIoIQ6Cov1lIEuwXAb2\n7boC41ePXwD0JWt41sP+rgCmpjBx00puIG+IlnoReEgI1
ZGYmK98GgA/XzmNjZiD\nyvXJZAcM33Ue85+PkR5iHTtSEbi4QAoqpJabprUzz3Fin2j1dRrcacxGb7p31A9c\nJ
QIDAQAB\n-----END PUBLIC KEY-----\n</PublicKey>
  <RequestId>475f1620-b9d3-4d35-b5c6-3fbdd941423d</RequestId>
</KMS>
```

`JSON` format

```
{
 "KeyId": "5c438b18-05be-40ad-b6c2-3be6752c****",
 "KeyVersionId": "2ab1a983-7072-4bbc-a582-584b5bd8****",
 "PublicKey": "-----BEGIN PUBLIC KEY-----\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAs5Yu9
AEgATN2/e3nUz1K\nEy6ng8MSPutcse2/VECG/NUF9C6D4IsJ64ShzY3dcn34WYzTOe916eMJFxyrNrSw\nHtc
4UOR5AvaoRrfpgu2uq+i70/ZXrWL+pGb1hgZV8cWheIHMxwrR3IiQlM5qN7EF\n9BdyWtyBfUGsp0Bn1VqlPc5
G0x0a9xU2z9YtP994yDenNVIoIQ6Cov1lIEuwXAb2\n7boC41ePXwD0JWt41sP+rgCmpjBx00puIG+IlnoReEgI1
ZGYmK98GgA/XzmNjZiD\nyvXJZAcM33Ue85+PkR5iHTtSEbi4QAoqpJabprUzz3Fin2j1dRrcacxGb7p31A9c\nJ
QIDAQAB\n-----END PUBLIC KEY-----\n",
 "RequestId": "475f1620-b9d3-4d35-b5c6-3fbdd941423d"
}
```

4.28. CreateAlias

Creates an alias for a CMK.

When you create an alias, take note of the following points:

- Each CMK can have only one alias.
- The aliases of cmks must be unique in a region.

Debugging

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

Request parameters

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

Response parameters

Parameter	Type	Example	Description
RequestId	String	Cost	The ID of the request.

Examples

Sample requests

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

Sample success responses

`XML` format

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

`JSON` format

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

Error codes

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

4.29. UpdateAlias

Associates an existing alias with a different CMK ID.

Debugging

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

Request parameters

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

Response parameters

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

Examples

Sample requests

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

Sample success responses

`XML` format

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

`JSON` format

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

Error codes

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

4.30. DeleteAlias

Deletes an alias.

Debugging

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

Request parameters

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

Response parameters

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

Examples

Sample requests

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

Sample success responses

`XML` format

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

`JSON` format

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

4.31. ListAliases

You can call this operation to query all aliases in the current region.

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
PageNumber	Integer	Optional	1	The number of the page to return. Value range: integers greater than 0. Default value: 1.
PageSize	Integer	Optional	10	The number of entries to return on each page. Valid values: 0 to 101. Default value: 10.

Response parameters

Prameter	Type	Sample response	Description
TotalCount	Integer	1	The total number of returned cmks.
PageNumber	Integer	1	The number of the page to return.
PageSize	Integer	10	The number of entries returned per page.
RequestId	String	1 b57992 c-834b-4811-a889-f8bac1ba0353	The ID of the request.

Prameter	Type	Sample response	Description
Aliases	Array		The alias of the user.
KeyId	String	08 c33a6 f-4e0a-4a1b-a3fa-7ddfa1d function compute instance *	The CMK to which the alias belongs.
AliasName	String	alias/ExampleAlias 1	The unique identifier of the alias.
AliasArn	String	acs:kms:cn-hangzhou:123456: alias/ExampleAlias 1	The ARN of the alias.

Examples

Sample requests

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

Sample success responses

`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>
```

`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"
}
```

Error codes

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

4.32. ListAliasesByKeyId

Queries all aliases bound to a CMK.

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description

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

Response parameters

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

Prameter	Type	Sample response	Description
AliasArn	String	acs:kms:cn-hangzhou:123456:alias/ExampleAlias1	The ARN of the alias.

Examples

Sample requests

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

Sample success responses

`XML` format

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

`JSON` format

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

Error codes

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

5.Secrets

5.1. CreateSecret

Creates a secret and stores the secret value in the initial version.

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

You can specify a symmetric CMK as the encryption key that is used to protect the secret. If you do not specify a CMK, Secrets Manager creates an encryption key to encrypt the secrets that are created by using your Alibaba Cloud account in the current region. Secrets Manager encrypts only the secret value of each version. It does not encrypt the metadata, such as the secret name, version number, and state label.

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

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	CreateSecret	The operation that you want to perform. Set the value to CreateSecret.
SecretData	String	Yes	{"user":"root","passwd":"****"}	The value of the secret that you want to create. Secrets Manager encrypts the secret value and stores it in the initial version.
SecretName	String	Yes	mydbconninfo	The name of the secret.
VersionId	String	Yes	v1	The version number of the initial version. Version numbers are unique in each secret object.

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

Response parameters

Parameter	Type	Example	Description
Arn	String	acs:kms:test-1:127046163668****:secret/seret001	The Alibaba Cloud Resource Name (ARN).
RequestId	String	2c124f6f-4210-499f-b88a-69f54004d2d8	The ID of the request.
SecretName	String	mydbconninfo	The name of the secret.
VersionId	String	v1	The version number of the idempotent operation.

Examples

Sample requests

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

Sample success responses

`XML` format

```
<KMS>
    <Arn>acs:kms:test-1:127046163668****:secret/secret001</Arn>
    <SecretName>mydbconninfo</SecretName>
    <VersionId>v1</VersionId>
    <RequestId>2c124f6f-4210-499f-b88a-69f54004d2d8</RequestId>
</KMS>
```

`JSON` format

```
{
  "Arn": "acs:kms:test-1:127046163668****:secret/secret001",
  "SecretName": "mydbconninfo",
  "VersionId": "v1",
  "RequestId": "2c124f6f-4210-499f-b88a-69f54004d2d8"
}
```

5.2. ListSecrets

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

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

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ListSecrets	The operation that you want to perform. Set the value to **ListSecrets**.
FetchTags	String	No	false	Specifies whether to return the resource tags of the secrets. Default value: **false**
PageNumber	Integer	No	1	The number of the page to return.
PageSize	Integer	No	10	The number of entries to return on each page.

Response parameters

Parameter	Type	Example	Description
PageNumber	Integer	1	The page number of the returned page.
PageSize	Integer	10	The number of entries returned per page.
RequestId	String	e8818e65-5c5b-4a0e-a571-8f50b59920a7	The ID of the request.
SecretList	Array		A list of secrets.
Secret			
CreateTime	String	2020-02-21T01:24:45Z	The time when a secret was created.
PlannedDeleteTime	String	2020-03-21T01:24:45Z	The time when a secret is scheduled to be deleted.
SecretName	String	secret001	The name of a secret.
Tags	Array		The resource tags of secrets. If the request parameter FetchTags is set to false, this parameter is not returned.

Parameter	Type	Example	Description
Tag			
TagKey	String	key1	The key of a resource tag.
TagValue	String	valq	The value of a resource tag.
UpdateTime	String	2020-02-21T15:22:45Z	The time when a secret was updated.
TotalCount	Integer	20	The number of returned secrets.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=ListSecrets
&PageNumber=1
&PageSize=10
&<Common request parameters>
```

Sample success responses

`XML` format

```
<SecretList>
  <Secret>
    <SecretName>secret001</SecretName>
    <CreateTime>2020-02-21T01:24:45Z</CreateTime>
    <UpdateTime>2020-02-21T01:24:45Z</UpdateTime>
    <Tags>
    </Tags>
  </Secret>
  <Secret>
    <SecretName>secret004</SecretName>
    <CreateTime>2020-02-21T15:22:45Z</CreateTime>
    <UpdateTime>2020-02-21T15:22:45Z</UpdateTime>
    <Tags>
      <Tag>
        <TagKey>key1</TagKey>
        <TagValue>val1</TagValue>
      </Tag>
      <Tag>
        <TagKey>key2</TagKey>
        <TagValue>val2</TagValue>
      </Tag>
    </Tags>
  </Secret>
</SecretList>
<RequestId>edbdc10d-3bcb-4690-95cb-3bf5664e1f02</RequestId>
<PageNumber>1</PageNumber>
<PageSize>10</PageSize>
<TotalCount>2</TotalCount>
```

`JSON` format

```
{
  "SecretList": {
    "Secret": [
      {
        "SecretName": "secret001",
        "CreateTime": "2020-02-21T01:24:45Z",
        "UpdateTime": "2020-02-21T01:24:45Z",
        "Tags": {
          "Tag": []
        }
      },
      {
        "SecretName": "secret004",
        "CreateTime": "2020-02-21T15:22:45Z",
        "UpdateTime": "2020-02-21T15:22:45Z",
        "Tags": {
          "Tag": [
            {
              "TagKey": "key1",
              "TagValue": "val1"
            },
            {
              "TagKey": "key2",
              "TagValue": "val2"
            }
          ]
        }
      }
    ]
  },
  "RequestId": "edbdc10d-3bcb-4690-95cb-3bf5664e1f02",
  "PageNumber": 1,
  "PageSize": 10,
  "TotalCount": 2
}
```


5.3. DeleteSecret

Deletes a secret.

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

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

Debugging

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

Request parameters

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

Response parameters

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

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

Examples

Sample requests

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

Sample success responses

`XML` format

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

`JSON` format

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

5.4. DescribeSecret

Obtains the metadata of a secret.

This operation returns the metadata information stored in a secret object and does not return the encrypted secret value.

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeSecret	The operation that you want to perform. Set the value to DescribeSecret.
SecretName	String	Yes	secret001	The name of the secret you want to delete.
FetchTags	String	No	true	Specifies whether to return the resource tags of the secret. Default value: false

Response parameters

Parameter	Type	Example	Description
Arn	String	acs:kms:test-1:1270461636684862:secret/secret001	The Alibaba Cloud Resource Name (ARN).
CreateTime	String	2020-02-21T15:39:26Z	The time when the secret was created.
Description	String	userinfo	The description of the secret.
EncryptionKeyId	String	00 aa68 af-2c02-4f68-95fe-3435d330 instance account number *	The ID of the KMS customer master key (CMK) that is used to encrypt the secret value.
PlannedDeleteTime	String	2020-03-21T15:45:12Z	The time when the secret is scheduled to be deleted.
RequestId	String	93348dfb-3627-4417-8d90-487a76a909c9	The ID of the request.
SecretName	String	secret003	The name of a secret.
Tags	Array		The resource tags of the secret. If the request parameter FetchTags is set to false, this parameter is not returned.
Tag			

Parameter	Type	Example	Description
TagKey	String	key1	The key of a resource tag.
TagValue	String	val1	The value of a resource tag.
UpdateTime	String	2020-02-21T15:39:26Z	The time when the secret was updated.

Examples

Sample requests

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

Sample success responses

`XML` format

```
<Arn>acs:kms:test-1:1270461636684862:secret/secret003</Arn>
<SecretName>secret003</SecretName>
<EncryptionKeyId>00aa68af-2c02-4f68-95fe-3435d330****</EncryptionKeyId>
<Description>data3 description</Description>
<Tags>
</Tags>
<CreateTime>2020-02-21T15:45:12Z</CreateTime>
<UpdateTime>2020-02-21T15:45:12Z</UpdateTime>
<RequestId>da08ec4c-7a55-4e98-9686-fca7114f6696</RequestId>
```

`JSON` format

```
{
 "Arn": "acs:kms:test-1:1270461636684862:secret/secret003",
 "SecretName": "secret003",
 "EncryptionKeyId": "00aa68af-2c02-4f68-95fe-3435d330****",
 "Description": "data3 description",
 "Tags": {
  "Tag": []
 },
 "CreateTime": "2020-02-21T15:45:12Z",
 "UpdateTime": "2020-02-21T15:45:12Z",
 "RequestId": "da08ec4c-7a55-4e98-9686-fca7114f6696"
}
```

5.5. GetSecretValue

Obtains a secret value.

- If you do not specify a version number or stage label, Secrets Manager returns the secret value of the version marked with **ACSCurrent**.
- If a KMS customer master key (CMK) is specified to encrypt the secret value, you must be granted the `kms:Decrypt` permission on the CMK to call this operation.

Debugging

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

Request parameters

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

Parameter	Type	Required	Example	Description
VersionStage	String	No	ACSCurrent	The stage label that marks the secret version. If you specify this parameter, Secrets Manager returns the secret value of the version that is marked with the specified stage label. Default value: **ACSCurrent**
VersionId	String	No	00000000000000000000000000000001	The version number of the secret value. If you specify this parameter, Secrets Manager returns the secret value of the specified version.

Response parameters

Parameter	Type	Example	Description
CreateTime	String	2020-02-21T15:39:26Z	The time when the secret version was created.
RequestId	String	8dde04f4-0d27-431c-a0f2-a89c8af016c6	The ID of the request.
SecretData	String	testdata1	The secret value. Secrets Manager decrypts the stored secret value in ciphertext and returns it.
SecretDataType	String	text	The type of the secret value. Valid values: • **binary** • **text**
SecretName	String	secret001	The name of the secret.
VersionId	String	00000000000000000000000000000001	The version number of the secret value.
VersionStages	List	{ "VersionStage": ["ACSCurrent"] }	Stage labels that mark the secret version.

Examples

Sample requests

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

Sample success responses

`XML` format

```
<SecretName>secret001</SecretName>
<VersionId>00000000000000000000000000000001</VersionId>
<SecretData>testdata1</SecretData>
<SecretDataType>text</SecretDataType>
<VersionStages>
  <VersionStage>ACSCurrent</VersionStage>
</VersionStages>
<CreateTime>2020-02-21T15:39:26Z</CreateTime>
<RequestId>8dde04f4-0d27-431c-a0f2-a89c8af016c6</RequestId>
```

`JSON` format

```
{
  "SecretName": "secret001",
  "VersionId": "00000000000000000000000000000001",
  "SecretData": "testdata1",
  "SecretDataType": "text",
  "VersionStages": {
    "VersionStage": [
      "ACSCurrent"
    ]
  },
  "CreateTime": "2020-02-21T15:39:26Z",
  "RequestId": "8dde04f4-0d27-431c-a0f2-a89c8af016c6"
}
```

5.6. PutSecretValue

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

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

secret value of an existing version.

If you do not specify VersionStage, the newly stored secret value is marked with **ACSCurrent**, and the original version marked with **ACSCurrent** is marked with **ACSPrevious**. If you specify **VersionStage**, the newly stored secret value is marked with the specified stage label.

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

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

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	PutSecretValue	The operation that you want to perform. Set the value to **PutSecretValue**.
SecretData	String	Yes	importantdata	The secret value that you want to store. It is encrypted and then stored in a specified new version.
SecretName	String	Yes	secret001	The name of the secret whose value you want to store.
VersionId	String	Yes	00000000000000000000000000000000000203	The version number of the secret value you want to store. It must be unique in the secret object.

Parameter	Type	Required	Example	Description
SecretDataType	String	No	text	The type of the secret value that you want to store. Valid values: • **text** • **binary** Default value: **text**
VersionStages	String	No	["ACSCurrent", "UStage1","Ustage2"]	The stage labels that mark the new secret version. If you do not specify this parameter, Secrets Manager marks it with **ACSCurrent**.

Response parameters

Parameter	Type	Example	Description
RequestId	String	6d394629-3ae3-4412-bb83-ae95ceb2b5da	The ID of the request.
SecretName	String	secret001	The name of the secret.
VersionId	String	00000000000000000000000000000000203	The version number of the secret value.
VersionStages	List	{ "VersionStage": ["ACSCurrent", "UStage1", "Ustage2"] }	Stage labels that mark the version.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=PutSecretValue
&SecretData=importantdata
&SecretDataType=text
&SecretName=secret001
&VersionId=00000000000000000000000000000000203
&<Common request parameters>
```

Sample success responses

`XML` format

```
<SecretName>secret001</SecretName>
<VersionId>00000000000000000000000000000000203</VersionId>
<VersionStages>
  <VersionStage>ACSCurrent</VersionStage>
  <VersionStage>UStage1</VersionStage>
  <VersionStage>Ustage2</VersionStage>
</VersionStages>
<RequestId>6d394629-3ae3-4412-bb83-ae95ceb2b5da</RequestId>
```

`JSON` format

```
{
  "SecretName": "secret001",
  "VersionId": "00000000000000000000000000000000203",
  "VersionStages": {
    "VersionStage": [
      "ACSCurrent",
      "UStage1",
      "Ustage2"
    ]
  },
  "RequestId": "6d394629-3ae3-4412-bb83-ae95ceb2b5da"
}
```

5.7. UpdateSecret

Updates the metadata of a secret.

Debugging

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

Request parameters

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

Parameter	Type	Required	Example	Description
SecretName	String	Yes	secret001	The name of the secret whose metadata you want to update.
Description	String	No	datainfo	The description of the updated secret.

Response parameters

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

Examples

Sample requests

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

Sample success responses

`XML` format

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

`JSON` format

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

5.8. UpdateSecretVersionStage

Updates the stage label that marks a secret version.

You can use this operation to achieve the following purposes:

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

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	UpdateSecretVersionStage	The operation that you want to perform. Set the value to UpdateSecretVersionStage.
SecretName	String	Yes	secret001	The name of the secret whose stage label you want to update.
VersionStage	String	Yes	ACSCurrent	The stage label you want to update.
RemoveFromVersion	String	No	00000000000000000000000000000001	The version from which you want to remove the specified stage label.
MoveToVersion	String	No	00000000000000000000000000000002	The version to which you want to apply the specified stage label.

Response parameters

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

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=UpdateSecretVersionStage
&SecretName=secret001
&VersionStage=ACSCurrent
&MoveToVersion=vid0001
&<Common request parameters>
```

Sample success responses

`XML` format

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

`JSON` format

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

5.9. RestoreSecret

Restores a deleted secret.

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

Debugging

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

Request parameters

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

Response parameters

Parameter	Type	Example	Description
RequestId	String	e4885adf-548f-4ca5-8075-f540bbd3a55f	The ID of the request.
SecretName	String	secret001	The name of the secret.

Examples

Sample requests

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

Sample success responses

`XML` format

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

`JSON` format

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

5.10. ListSecretVersionIds

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

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

Debugging

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

Request parameters

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

Response parameters

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

Parameter	Type	Example	Description
CreateTime	String	2020-02-21T15:39:26Z	The time when the secret version was created.
VersionId	String	00000000000000000000000000000000203	The version of the secret.
VersionStages	List	{ "VersionStage": ["ACSCurrent", "UStage1", "Ustage2"] }	The stage labels that mark the secret version.

Examples

Sample requests

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

Sample success responses

`XML` format

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

`JSON` format

```
{
  "SecretName": "secret001",
  "VersionIds": {
    "VersionId": [
      {
        "VersionId": "00000000000000000000000000000000203",
        "VersionStages": {
          "VersionStage": [
            "ACSCurrent",
            "UStage1",
            "Ustage2"
          ]
        }
      },
      {
        "VersionId": "00000000000000000000000000000001",
        "VersionStages": {
          "VersionStage": [
            "ACSPrevious"
          ]
        }
      }
    ]
  },
  "RequestId": "5b75d8b1-5b6a-4ec0-8e0c-c08befdfad47",
  "PageNumber": 1,
  "PageSize": 10,
  "TotalCount": 4
}
```


5.11. GetRandomPassword

Obtains a random password string.

Debugging

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

Request parameters

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

Parameter	Type	Required	Example	Description
ExcludePunctuation	String	No	false	Specifies whether to exclude special characters. Valid values: • true • false
RequireEachIncludedType	String	No	true	Specifies whether to include all the preceding character types. Valid values: • true • false

Response parameters

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

Examples

Sample requests

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

Sample success responses

`XML` format

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

`JSON` format

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

6.Tag

6.1. TagResource

Adds tags to a CMK or secret.

A CMK or secret can have multiple tags. Each tag consists of a pair of tag key and tag value. You can add a maximum of 10 tags to a CMK or secret.

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

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	TagResource	The operation that you want to perform. Set the value to TagResource.
Tags	String	Yes	[{\"TagKey\":\"S1key1\",\"TagValue\":\"S1val1\"},{\"TagKey\":\"S1key2\",\"TagValue\":\"S2val2\"}]	One or more tags. Format: tag object array. Tag object attributes: • TagKey: tag key • TagValue: tag value
KeyId	String	No	08c33a6f-4e0a-4a1b-a3fa-7ddf****	The globally unique ID of the CMK. Note Set either KeyId or SecretName.
SecretName	String	No	MyDbC****	The name of the secret. Note Set either KeyId or SecretName.

Response parameters

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

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=TagResource
&KeyId=08c33a6f-4e0a-4a1b-a3fa-7ddf****
&Tags=[{\"TagKey\":\"S1key1\",\"TagValue\":\"S1val1\"},{\"TagKey\":\"S1key2\",\"TagValue\":\"S2val
2\"}]
&<Common request parameters>
```

Sample success responses

`XML` format

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

`JSON` format

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

6.2. ListResourceTags

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

Request format: KeyId="string"

Debugging

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

Request parameters

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

Response parameters

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

Examples

Sample requests

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

Sample success responses

`XML` format

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

`JSON` format

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

Error codes

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

6.3. UntagResource

Removes specified tags from a CMK or secret.

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	UntagResource	The operation that you want to perform. Set the value to UntagResource.
TagKeys	String	Yes	["tagkey1","tagkey2"]	One or more tag keys. You do not need to specify tag values. Each tag key must be 1 to 128 bytes in length.
KeyId	String	No	08c33a6f-4e0a-4a1b-a3fa-7ddf****	The globally unique ID of the CMK. Note Set either this parameter or SecretName.
SecretName	String	No	MyDbC****	The name of the secret. Note Set either this parameter or KeyId.

Response parameters

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

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=UntagResource
&KeyId=08c33a6f-4e0a-4a1b-a3fa-7ddf****
&TagKeys=["tagkey1","tagkey2"]
&<Common request parameters>
```

Sample success responses

`XML` format

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

`JSON` format

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