Data Encryption Workshop

API Reference

Issue 01

Date 2022-09-30

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

1 Before You Start

1.1 Overview

Welcome to the *Data Encryption Workshop API Reference*. DEW is a comprehensive data encryption service in the cloud. It provides Key Management Service (KMS). DEW uses HSMs to protect the security of your keys, and can be integrated with other Huawei cloud services to address data security, key security, and key management issues. Additionally, DEW enables you to develop customized encryption applications.

Before calling DEW APIs, ensure that you have understood the concepts related to DEW. For more information, see **What Is DEW?**

1.2 API Calling

DEW supports Representational State Transfer (REST) APIs, allowing you to call APIs using HTTPS requests. For details about API calling, see **Making an API Request**.

1.3 Constraints

The number of keys that you can create is determined by your quota. For details, see **Service Quota**.

In KMS, TPS (the number of API operations that can be performed by a user per second) is set to **20**.

1.4 Concepts

- Account

  An account is created upon successful registration. The account has full access permissions for all of its cloud services and resources. It can be used to reset user passwords and grant user permissions. The account is a payment entity and should not be used to perform routine management. For security purposes, create IAM users and grant them permissions for routine management.

- User

  An IAM user is created by an account in IAM to use cloud services. Each IAM user has its own identity credentials (password and access keys).

  The account name, username, and password will be required for API authentication.

- Region

  Regions are divided based on geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified as universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides services of the same type only or for specific tenants.

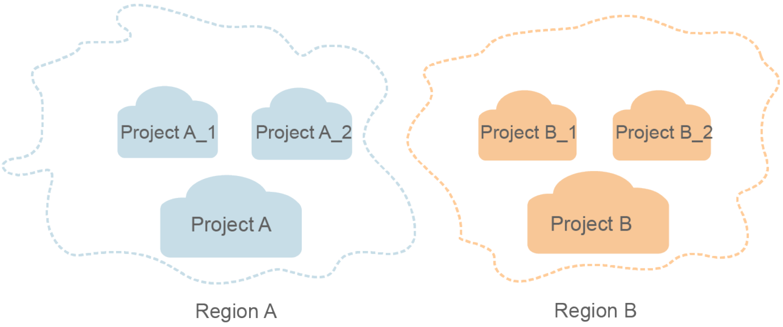
- Availability Zone (AZ)

  An AZ comprises one or multiple physical data centers equipped with independent ventilation, fire, water, and electricity facilities. Compute, network, storage, and other resources in an AZ are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers to support cross-AZ high-availability systems.

- Project

  Projects group and isolate compute, storage, and network resources across physical regions. A default project is provided for each region, and subprojects can be created under each default project. Users can be granted permissions to access all resources in a specific project. For more refined access control, create subprojects under a project and create resources in the subprojects. Users can then be assigned permissions to access only specific resources in the subprojects.

  Figure 1-1 Project isolation model

- Enterprise project

  Enterprise projects group and manage resources across regions. Resources in enterprise projects are logically isolated from each other. An enterprise project can contain resources in multiple regions, and resources can be directly transferred between enterprise projects.

2 Calling APIs

2.1 Making an API Request

This section describes the structure of a REST API request, and uses the IAM API for **obtaining a user token** as an example to demonstrate how to call an API. The obtained token can then be used to authenticate the calling of other APIs.

Request URI

A request URI is in the following format:

{URI-scheme} :// {Endpoint} / {resource-path} ? {query-string}

Although a request URI is included in the request header, most programming languages or frameworks require the request URI to be transmitted separately.

- **URI-scheme**:

  Protocol used to transmit requests. All APIs use HTTPS.
- **Endpoint**:

  Domain name or IP address of the server bearing the REST service. The endpoint varies between services in different regions.

  For example, the endpoint of IAM in region **EU-Dublin** is **iam.eu-west-101.myhuaweicloud.com**.
- **resource-path**:

  Access path of an API for performing a specified operation. Obtain the path from the URI of an API. For example, the **resource-path** of the API used to obtain a user token is **/v3/auth/tokens**.
- **query-string**:

  Query parameter, which is optional. Ensure that a question mark (?) is included before each query parameter that is in the format of "Parameter name=Parameter value". For example, **?limit=10** indicates that a maximum of 10 data records will be displayed.

For example, to obtain an IAM token in region **EU-Dublin**, obtain the endpoint of IAM (**iam.eu-west-101.myhuaweicloud.com**) for this region and the **resource-**

path (**/v3/auth/tokens**) in the URI of the API used to **obtain a user token**. Then, construct the URI as follows:

```
https://iam.eu-west-101.myhuaweicloud.com/v3/auth/tokens
```

NOTE

To simplify the URI display in this document, each API is provided only with a **resource-path** and a request method. The **URI-scheme** of all APIs is **HTTPS**, and the endpoints of all APIs in the same region are identical.

Request Methods

The HTTP protocol defines the following request methods that can be used to send a request to the server:

- **GET**: requests the server to return specified resources.
- **PUT**: requests the server to update specified resources.
- **POST**: requests the server to add resources or perform special operations.
- **DELETE**: requests the server to delete specified resources, for example, an object.
- **HEAD**: same as GET except that the server must return only the response header.
- **PATCH**: requests the server to update partial content of a specified resource. If the resource does not exist, a new resource will be created.

For example, in the case of the API used to **obtain a user token**, the request method is POST. The request is as follows:

```
POST https://iam.eu-west-101.myhuaweicloud.com/v3/auth/tokens
```

Request Header

You can also add additional header fields to a request, such as the fields required by a specified URI or HTTP method. For example, to request for the authentication information, add **Content-Type**, which specifies the request body type.

Common request header fields are as follows:

- **Content-Type**: specifies the request body type or format. This field is mandatory and its default value is **application/json**. Other values of this field will be provided for specific APIs if any.
- **X-Auth-Token**: specifies a user token only for token-based API authentication. The user token is a response to the API used to **obtain a user token**. This API is the only one that does not require authentication.

  NOTE

  In addition to supporting token-based authentication, APIs also support authentication using access key ID/secret access key (AK/SK). During AK/SK-based authentication, an SDK is used to sign the request, and the **Authorization** (signature information) and **X-Sdk-Date** (time when the request is sent) header fields are automatically added to the request.

  For more information, see **AK/SK-based Authentication**.

The API used to **obtain a user token** does not require authentication. Therefore, only the **Content-Type** field needs to be added to requests for calling the API. An example of such requests is as follows:

```
POST https://iam.eu-west-101.myhuaweicloud.com/v3/auth/tokens
Content-Type: application/json
```

Request Body

The body of a request is often sent in a structured format as specified in the **Content-Type** header field. The request body transfers content except the request header.

The request body varies between APIs. Some APIs do not require the request body, such as the APIs requested using the GET and DELETE methods.

In the case of the API used to **obtain a user token**, the request parameters and parameter description can be obtained from the API request. The following provides an example request with a body included. Replace *username*, *domainname*, ******** (login password), and *xxxxxxxxxxxxxxxxxx* (project name) with the actual values.

NOTE

The **scope** parameter specifies where a token takes effect. You can set **scope** to an account or a project under an account. In the following example, the token takes effect only for the resources in a specified project. For more information about this API, see **Obtaining a User Token**.

```
POST https://iam.eu-west-101.myhuaweicloud.com/v3/auth/tokens

Content-Type: application/json

{
    "auth": {
        "identity": {
            "methods": [
                "password"
            ],
            "password": {
                "user": {
                    "name": "username",
                    "password": "********",
                    "domain": {
                        "name": "domainname"
                    }
                }
            }
        },
        "scope": {
            "project": {
                "name": "xxxxxxxxxxxxxxxxxx"
            }
        }
    }
}
```

If all data required for the API request is available, you can send the request to call the API through **curl**, **Postman**, or coding. In the response to the API used to obtain a user token, **x-subject-token** is the desired user token. You can use this token to authenticate the calling of other APIs.

2.2 Authentication

Requests for calling an API can be authenticated using either of the following methods:

- Token-based authentication: Requests are authenticated using a token.
- AK/SK authentication: Requests are encrypted using AK/SK pairs. This method is recommended because it provides higher security than token-based authentication.

Token-based Authentication

NOTE

The validity period of a token is 24 hours. When using a token for authentication, cache it to prevent frequently calling the IAM API used to obtain a user token.

A token specifies temporary permissions in a computer system. During API authentication using a token, the token is added to requests to get permissions for calling the API.

You can **obtain a token** by calling an API. A project-level token is required for calling DEW APIs. When calling an API to obtain a user token, set **project** in **auth.scope** in the request body, as shown in the following example.

```
{
    "auth": {
        "identity": {
            "methods": [
                "password"
            ],
            "password": {
                "user": {
                    "name": "username",
                    "password": "********",
                    "domain": {
                        "name": "domainname"
                    }
                }
            }
        },
      "scope": {
           "project": {
                   "name": "xxxxxxxx",
                      }
                }
    }
}
```

After a token is obtained, the **X-Auth-Token** header field must be added to requests to specify the token when calling other APIs. For example, if the token is **ABCDEFJ....**, **X-Auth-Token: ABCDEFJ....** can be added to a request as follows:

```
POST https://iam.eu-west-101.myhuaweicloud.com/v3/auth/projects
Content-Type: application/json
X-Auth-Token: ABCDEFJ....
```

AK/SK-based Authentication

NOTE

AK/SK-based authentication supports API requests with a body not larger than 12 MB. For API requests with a larger body, token-based authentication is recommended.

In AK/SK-based authentication, AK/SK is used to sign requests and the signature is then added to the requests for authentication.

- AK: access key ID, which is a unique identifier used in conjunction with a secret access key to sign requests cryptographically.
- SK: secret access key used in conjunction with an AK to sign requests cryptographically. It identifies a request sender and prevents the request from being modified.

In AK/SK-based authentication, you can use an AK/SK to sign requests based on the signature algorithm or use the signing SDK to sign requests. For details about how to sign requests and use the signing SDK, see **API Signature Guide**.

NOTICE

The signing SDK is only used for signing requests and is different from the SDKs provided by services.

2.3 Response

Status Codes

After sending a request, you will receive a response, including a status code, response header, and response body.

A status code is a group of digits, ranging from 1xx to 5xx. It indicates the status of a request. For more information, see **Status Codes**.

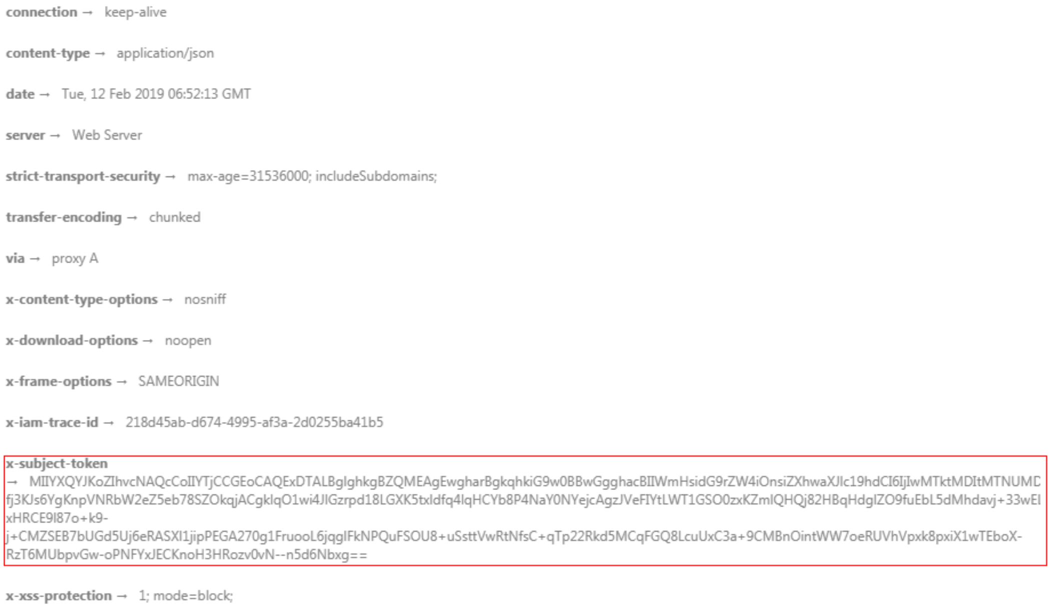
For example, if status code **201** is returned for calling the API used to **obtain a user token**, the request is successful.

Response Header

A response header corresponds to a request header, for example, **Content-Type**.

Figure 2-1 shows the response header for the API of **obtaining a user token**, in which **x-subject-token** is the desired user token. You can use this token to authenticate the calling of other APIs.

Figure 2-1 Header of the response to the request for obtaining a user token



```
connection → keep-alive

content-type → application/json

date → Tue, 12 Feb 2019 06:52:13 GMT

server → Web Server

strict-transport-security → max-age=31536000; includeSubdomains;

transfer-encoding → chunked

via → proxy A

x-content-type-options → nosniff

x-download-options → noopen

x-frame-options → SAMEORIGIN

x-iam-trace-id → 218d45ab-d674-4995-af3a-2d0255ba41b5

x-subject-token
→ MIIYXQYJKoZIhvcNAQcCoIIYTjCCGEoCAQExDTALBglghkgBZQMEAgEwgharBgkqhkiG9w0BBwGgghacBIIWmHsidG9rZW4iOnsiZXhwaXJlc19hdCI6IjIwMTktMDItMTNUMD
fj3KJs6YgKnpVNRbW2eZ5eb78SZOkqjACgklqO1wi4JIGzrpd18LGXK5txldfq4lqHCYb8P4NaY0NYejcAgzJVeFIYtLWT1GSO0zxKZmIQHQj82HBqHdglZO9fuEbL5dMhdavj+33wEl
xHRCE9I87o+k9-
j+CMZSEB7bUGd5Uj6eRASXl1jipPEGA270g1FruooL6jqglFkNPQuFSOU8+uSsttVwRtNfsC+qTp22Rkd5MCqFGQ8LcuUxC3a+9CMBnOintWW7oeRUVhVpxk8pxiX1wTEboX-
RzT6MUbpvGw-oPNFYxJECKnoH3HRozv0vN--n5d6Nbxg==

x-xss-protection → 1; mode=block;
```

(Optional) Response Body

A response body is generally returned in a structured format, corresponding to the **Content-Type** in the response header, and is used to transfer content other than the response header.

The following shows part of the response body for the API to **obtain a user token**. For the sake of space, only part of the content is displayed here.

```
{
    "token": {
        "expires_at": "2019-02-13T06:52:13.855000Z",
        "methods": [
            "password"
        ],
        "catalog": [
            {
                "endpoints": [
                    {
                        "region_id": "xxxxxxxx",
......
```

If an error occurs during API calling, the system returns an error code and a message to you. The following shows the format of an error response body:

```
{
    "error": {
        "message": "The request you have made requires authentication.",
        "title": "Unauthorized"
    }
}
```

In the preceding information, **error_code** is an error code, and **error_msg** describes the error.

3 API Overview

By using the APIs provided by DEW, you can use all the functions of the service.

Type	Description
Key Management APIs	Create, query, modify, and delete keys.
Secret management APIs	Create, query, modify, and delete secrets.
Key Pair Management APIs	(Latest API version) Create, query, modify, and delete key pairs.
Historical APIs	(V2.1 and V2 API versions) Create, query, modify, and delete key pairs.

Historical APIs

Type	Description
Key pair management APIs (V2.1)	Queries the list of key pairs.
	Queries details of a key pair.
	Creates and imports a key pair, and allows you to manage the private key in the cloud.
	Deletes an SSH key pair based on the key pair name.
	Modifies description of a key pair of a specified name.
Key pair management APIs (V2.0)	Queries the list of key pairs.
	Queries a key pair by its name.

Type	Description
	Creates a key pair or import a public key to the cloud to generate a key pair. After an SSH key pair is created, you need to download the private key to a local directory. Then, you can use this private key to log in to an ECS. For ECS security purposes, the private key can be downloaded only once. Keep it secure.
	Deletes an SSH key pair based on the key pair name.
	Copies a user's key pairs to the current user. The two users must belong to the same account.

4 APIs

4.1 Key Management APIs

4.1.1 API Version Querying

4.1.1.1 Querying version list

Function

This API enables you to querying all API versions.

URI

GET /

Request Parameters

None

Response Parameters

Status code: 200

Table 4-1 Response body parameters

Parameter	Type	Description
versions	Array of **ApiVersionDetail** objects	List of all versions.

Table 4-2 ApiVersionDetail

Parameter	Type	Description
id	String	Version number, for example, v1.0.
links	Array of **ApiLink** objects	JSON object.
version	String	If the APIs of this version support microversions, the supported maximum microversion is returned. If microversions are not supported, an empty string is returned.
status	String	Version status. It can be: ● CURRENT: widely used version ● SUPPORTED: earlier version which is still supported ● DEPRECATED: deprecated version which may be deleted later
updated	String	Coordinated Universal time (UTC) time when the version was released. For example, the value is **2014-06-28T12:20:21Z** for v1.
min_version	String	If the APIs of this version support microversions, the supported minimum microversion is returned. If microversions are not supported, an empty string is returned.

Table 4-3 ApiLink

Parameter	Type	Description
href	String	API URL.
rel	String	The default value is self.

Example Requests

None

Example Responses

Status code: 200

Request processing succeeded.

```
[ {
  "min_version" : "",
  "links" : [ {
    "rel" : "self",
    "href" : "https://kms.region_id.domain.com/v1.0/"
  } ],
  "id" : "v1.0",
  "version" : "",
  "updated" : "2016-10-29T02:00:00Z",
  "status" : "CURRENT"
} ]
```

Status Codes

Status Code	Description
200	Request processing succeeded.

Error Codes

See **Error Codes**.

4.1.1.2 Querying a version

Function

This API enables you to query a specified API version.

URI

GET /{version_id}

Table 4-4 Path parameters

Parameter	Mandatory	Type	Description
version_id	Yes	String	API version.

Request Parameters

None

Response Parameters

Status code: 200

Table 4-5 Response body parameters

Parameter	Type	Description
version	Object	List of all versions.

Table 4-6 ApiVersionDetail

Parameter	Type	Description
id	String	Version number, for example, v1.0.
links	Array of **ApiLink** objects	JSON object.
version	String	If the APIs of this version support microversions, the supported maximum microversion is returned. If microversions are not supported, an empty string is returned.
status	String	Version status. It can be: ● CURRENT: widely used version ● SUPPORTED: earlier version which is still supported ● DEPRECATED: deprecated version which may be deleted later
updated	String	Coordinated Universal time (UTC) time when the version was released. For example, the value is **2014-06-28T12:20:21Z** for v1.
min_version	String	If the APIs of this version support microversions, the supported minimum microversion is returned. If microversions are not supported, an empty string is returned.

Table 4-7 ApiLink

Parameter	Type	Description
href	String	API URL.
rel	String	The default value is self.

Example Requests

None

Example Responses

Status code: 200

This API is used to query a specified API version.

```
{
  "min_version" : "",
  "links" : [ {
    "rel" : "self",
    "href" : "https://kms.region_id.domain.com/v1.0/"
  } ],
  "id" : "v1.0",
  "version" : "",
  "updated" : "2016-10-29T02:00:00Z",
  "status" : "CURRENT"
}
```

Status Codes

Status Code	Description
200	This API is used to query a specified API version.

Error Codes

See **Error Codes**.

4.1.2 Lifecycle Management

4.1.2.1 Creating a CMK

Function

This API is used to create customer master keys (CMKs).

- Symmetric CMKs contain a 256-bit symmetric keyIt can be used to encrypt and decrypt small amounts of data or data encryption keys (DEKs).
- Asymmetric CMKs can contain an RSA key pair or an Elliptic Curve (ECC) key pair. It can be used to sign and verify messages

Constraints

Default Master Keys are created by services integrated with KMS. Names of Default Master Keys end with /default. Do not end your CMK names with /default. Enterprise project users' Default Master Keys belong to their default enterprise projects and cannot be moved to other enterprise projects. Default Master Keys provide basic cloud-based encryption functions to meet compliance requirements and can be used by non-default enterprise projects. You can also create and use your own keys as needed.

URI

POST /v1.0/{project_id}/kms/create-key

Table 4-8 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-9 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. The token can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-10 Request body parameters

Parameter	Mandatory	Type	Description
key_alias	Yes	String	Alias of a non-default master key. The value is a string of 1 to 255 characters that match the regular expression ^[a-zA-Z0-9:/_-]{1,255}$ and must be different from the alias of the Default Master Key.
key_description	No	String	Key description. It can contain 0 to 255 characters.
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff

Response Parameters

Status code: 200

Table 4-11 Response body parameters

Parameter	Type	Description
key_info	**KeKInfo** object	Key details.

Table 4-12 KeKInfo

Parameter	Type	Description
key_id	String	CMK ID.
domain_id	String	User domain ID.

Status code: 400

Table 4-13 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-14 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 403

Table 4-15 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-16 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Example Requests

```
{
  "key_alias" : "test"
}
```

Example Responses

Status code: 200

Request processing succeeded.

```
{
  "key_info" : {
    "key_id" : "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
    "domain_id" : "b168fe00ff56492495a7d22974df2d0b"
  }
}
```

Status code: 400

Invalid request parameters.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 403

Authentication failed.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status Codes

Status Code	Description
200	Request processing succeeded.
400	Invalid request parameters.
403	Authentication failed.

Error Codes

See **Error Codes**.

4.1.2.2 Enabling a CMK

Function

This API allows you to enable a CMK.

Constraints

Only a disabled key can be enabled.

URI

POST /v1.0/{project_id}/kms/enable-key

Table 4-17 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-18 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. The token can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-19 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	CMK ID. It should be 36 bytes and match the regular expression ^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$. Example: 0d0466b0-e727-4d9c-b35d-f84bb474a37f
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff

Response Parameters

Status code: 200

Table 4-20 Response body parameters

Parameter	Type	Description
key_info	**KeyStatusInfo** object	Key status.

Table 4-21 KeyStatusInfo

Parameter	Type	Description
key_id	String	CMK ID.
key_state	String	Key state. It can be: ● 2: enabled ● 3: disabled ● 4: pending deletion ● 5: pending import ● 7: frozen

Status code: 400

Table 4-22 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-23 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 403

Table 4-24 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-25 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 404

Table 4-26 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-27 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Example Requests

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f"
}
```

Example Responses

Status code: 200

Request processing succeeded.

```
{
  "key_info" : {
    "key_id" : "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
    "key_state" : "2"
  }
}
```

Status code: 400

Invalid request parameters.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 403

Authentication failed.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 404

The requested resource does not exist or is not found.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status Codes

Status Code	Description
200	Request processing succeeded.
400	Invalid request parameters.
403	Authentication failed.
404	The requested resource does not exist or is not found.

Error Codes

See **Error Codes**.

4.1.2.3 Disabling a CMK

Function

This API allows you to disable a CMK.

Constraints

Only an enabled key can be disabled.

URI

POST /v1.0/{project_id}/kms/disable-key

Table 4-28 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-29 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. The token can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-30 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	CMK ID. It should be 36 bytes and match the regular expression ^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$. Example: 0d0466b0-e727-4d9c-b35d-f84bb474a37f
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff

Response Parameters

Status code: 200

Table 4-31 Response body parameters

Parameter	Type	Description
key_info	**KeyStatusInfo** object	Key status.

Table 4-32 KeyStatusInfo

Parameter	Type	Description
key_id	String	CMK ID.

Parameter	Type	Description
key_state	String	Key state. It can be: ● 2: enabled ● 3: disabled ● 4: pending deletion ● 5: pending import ● 7: frozen

Status code: 400

Table 4-33 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-34 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 403

Table 4-35 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-36 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 404

Table 4-37 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-38 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Example Requests

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f"
}
```

Example Responses

Status code: 200

Request processing succeeded.

```
{
  "key_info" : {
    "key_id" : "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
    "key_state" : "3"
  }
}
```

Status code: 400

Invalid request parameters.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 403

Authentication failed.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 404

The requested resource does not exist or is not found.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status Codes

Status Code	Description
200	Request processing succeeded.
400	Invalid request parameters.
403	Authentication failed.
404	The requested resource does not exist or is not found.

Error Codes

See **Error Codes**.

4.1.2.4 Scheduling the Deletion of a CMK

Function

This API enables you to schedule the deletion of a CMK. A CMK can be scheduled to be deleted after 7 to 1096 days.

URI

POST /v1.0/{project_id}/kms/schedule-key-deletion

Table 4-39 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-40 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. The token can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-41 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	CMK ID. It should be 36 bytes and match the regular expression ^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$. Example: 0d0466b0-e727-4d9c-b35d-f84bb474a37f
pending_days	Yes	String	Number of days after which a CMK is scheduled to be deleted. The value can be from 7 to 1,096 days.
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff

Response Parameters

Status code: 200

Table 4-42 Response body parameters

Parameter	Type	Description
key_id	String	CMK ID.
key_state	String	Key state. It can be: ● 2: enabled ● 3: disabled ● 4: pending deletion ● 5: pending import ● 7: frozen

Status code: 400

Table 4-43 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-44 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 403

Table 4-45 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-46 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 404

Table 4-47 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-48 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Example Requests

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "pending_days" : "7"
}
```

Example Responses

Status code: 200

Request processing succeeded.

```
{
  "key_id" : "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
  "key_state" : "4"
}
```

Status code: 400

Invalid request parameters.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 403

Authentication failed.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 404

The requested resource does not exist or is not found.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status Codes

Status Code	Description
200	Request processing succeeded.
400	Invalid request parameters.
403	Authentication failed.
404	The requested resource does not exist or is not found.

Error Codes

See **Error Codes**.

4.1.2.5 Canceling the Scheduled Deletion of a CMK

Function

This API is used to cancel the scheduled deletion of a CMK.

Constraints

You can cancel the scheduled deletion for a CMK only when the CMK's status is Scheduled deletion.

URI

POST /v1.0/{project_id}/kms/cancel-key-deletion

Table 4-49 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-50 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. The token can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-51 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	CMK ID. It should be 36 bytes and match the regular expression ^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$. Example: 0d0466b0-e727-4d9c-b35d-f84bb474a37f
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff

Response Parameters

Status code: 200

Table 4-52 Response body parameters

Parameter	Type	Description
key_id	String	CMK ID.
key_state	String	Key state. It can be: ● 2: enabled ● 3: disabled ● 4: pending deletion ● 5: pending import ● 7: frozen

Status code: 400

Table 4-53 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-54 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 403

Table 4-55 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-56 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 404

Table 4-57 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-58 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Example Requests

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f"
}
```

Example Responses

Status code: 200

Request processing succeeded.

```
{
  "key_id" : "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
  "key_state" : "3"
}
```

Status code: 400

Invalid request parameters.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 403

Authentication failed.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 404

The requested resource does not exist or is not found.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status Codes

Status Code	Description
200	Request processing succeeded.
400	Invalid request parameters.
403	Authentication failed.
404	The requested resource does not exist or is not found.

Error Codes

See **Error Codes**.

4.1.2.6 Changing the Alias of a CMK

Function

This API enables you to change the alias of a CMK.

Constraints

- A Default Master Key (the alias suffix of which is /default) does not allow alias changes.
- A CMK in Scheduled deletion status does not allow alias changes.

URI

POST /v1.0/{project_id}/kms/update-key-alias

Table 4-59 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-60 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. The token can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-61 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	CMK ID. It should be 36 bytes and match the regular expression ^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$. Example: 0d0466b0-e727-4d9c-b35d-f84bb474a37f
key_alias	Yes	String	Alias of a non-default CMK. The value is a string of 1 to 255 characters and must match the regular expression ^[a-zA-Z0-9:/_-]{1,255}$. The suffix cannot be /default.
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff

Response Parameters

Status code: 200

Table 4-62 Response body parameters

Parameter	Type	Description
key_info	**KeyAliasInfo** object	Key alias.

Table 4-63 KeyAliasInfo

Parameter	Type	Description
key_id	String	CMK ID.
key_alias	String	Key alias.

Status code: 400

Table 4-64 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-65 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 403

Table 4-66 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-67 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error information.

Status code: 404

Table 4-68 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-69 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Example Requests

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "key_alias" : "test"
}
```

Example Responses

Status code: 200

Request processing succeeded.

```
{
  "key_info" : {
    "key_id" : "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
    "key_alias" : "test"
  }
}
```

Status code: 400

Invalid request parameters.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 403

Authentication failed.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 404

The requested resource does not exist or is not found.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status Codes

Status Code	Description
200	Request processing succeeded.
400	Invalid request parameters.
403	Authentication failed.
404	The requested resource does not exist or is not found.

Error Codes

See **Error Codes**.

4.1.2.7 Changing the Description of a CMK

Function

This API enables you to change the description of a CMK.

Constraints

- A Default Master Key (the alias suffix of which is /default) does not allow description changes.
- A CMK in Scheduled deletion status does not allow description changes..

URI

POST /v1.0/{project_id}/kms/update-key-description

Table 4-70 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-71 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. The token can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-72 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	CMK ID. It should be 36 bytes and match the regular expression ^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$. Example: 0d0466b0-e727-4d9c-b35d-f84bb474a37f
key_description	Yes	String	Key description. It can contain 0 to 255 characters.
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff

Response Parameters

Status code: 200

Table 4-73 Response body parameters

Parameter	Type	Description
key_info	**KeyDescriptionInfo** object	Key description.

Table 4-74 KeyDescriptionInfo

Parameter	Type	Description
key_id	String	CMK ID.
key_description	String	Key description.

Status code: 400

Table 4-75 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-76 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 403

Table 4-77 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-78 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 404

Table 4-79 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-80 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Example Requests

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "key_description" : "test"
}
```

Example Responses

Status code: 200

Request processing succeeded.

```
{
  "key_info" : {
    "key_id" : "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
    "key_description" : "test"
  }
}
```

Status code: 400

Invalid request parameters.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 403

Authentication failed.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 404

The requested resource does not exist or is not found.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status Codes

Status Code	Description
200	Request processing succeeded.
400	Invalid request parameters.
403	Authentication failed.
404	The requested resource does not exist or is not found.

Error Codes

See **Error Codes**.

4.1.3 DEK Management

4.1.3.1 Creating a Random Number

Function

This API generates a random number that is 8 bits to 8192 bits long.

URI

POST /v1.0/{project_id}/kms/gen-random

Table 4-81 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-82 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. The token can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-83 Request body parameters

Parameter	Mandatory	Type	Description
random_data_length	Yes	String	Bit length of a random number. The value is a multiple of 8, in the range 8 to 8192.
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff

Response Parameters

Status code: 200

Table 4-84 Response body parameters

Parameter	Type	Description
random_data	String	Random number in hexadecimal format. Two characters represent 1 byte. Its length should match random_data_length.

Status code: 400

Table 4-85 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-86 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 403

Table 4-87 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-88 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Example Requests

```
{
  "random_data_length" : "512"
}
```

Example Responses

Status code: 200

Request processing succeeded.

```
{
  "random_data" : "5791C223E87120BE4B98D168F47A58BB2A88834EEADC"
}
```

Status code: 400

Invalid request parameters.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 403

Authentication failed.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status Codes

Status Code	Description
200	Request processing succeeded.
400	Invalid request parameters.
403	Authentication failed.

Error Codes

See **Error Codes**.

4.1.3.2 Creating a DEK

Function

This API allows you to create a DEK. A returned result includes the plaintext and the ciphertext of a DEK.

URI

POST /v1.0/{project_id}/kms/create-datakey

Table 4-89 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-90 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. The token can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-91 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	CMK ID. It should be 36 bytes and match the regular expression ^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$. Example: 0d0466b0-e727-4d9c-b35d-f84bb474a37f
encryption_context	No	Object	Key-value pairs with a maximum length of 8,192 characters. This parameter is used to record resource context information, excluding sensitive information, to ensure data integrity. If this parameter is specified during encryption, it is also required for decryption. Example: {"Key1":"Value1","Key2":"Value2"}
datakey_length	No	String	Bit length of a key. The value is a multiple of 8, in the range 8 to 8,192. Note: Set either datakey_length or key_spec. ● If neither of them is specified, a 256-bit key is generated by default. ● If both of them are specified, only datakey_length takes effect.
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff

Response Parameters

Status code: 200

Table 4-92 Response body parameters

Parameter	Type	Description
key_id	String	CMK ID.

Parameter	Type	Description
plain_text	String	Plaintext DEK in hexadecimal format. Two characters represent 1 byte.
cipher_text	String	Ciphertext DEK in hexadecimal format. Two characters represent 1 byte.

Status code: 400

Table 4-93 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-94 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 403

Table 4-95 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-96 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 404

Table 4-97 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-98 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Example Requests

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "datakey_length" : "512"
}
```

Example Responses

Status code: 200

Request processing succeeded.

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "plain_text" : "8151014275E426C72EE7D44267XXXXX...",
  "cipher_text" : "020098009EEAFCE122CAA5927D2XXX..."
}
```

Status code: 400

Invalid request parameters.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 403

Authentication failed.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 404

The requested resource does not exist or is not found.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status Codes

Status Code	Description
200	Request processing succeeded.
400	Invalid request parameters.
403	Authentication failed.
404	The requested resource does not exist or is not found.

Error Codes

See **Error Codes**.

4.1.3.3 Creating a Plaintext-Free DEK

Function

This API allows you to create a plaintext-free DEK, that is, the returned result of this API includes only the plaintext of the DEK.

URI

POST /v1.0/{project_id}/kms/create-datakey-without-plaintext

Table 4-99 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-100 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. The token can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-101 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	CMK ID. It should be 36 bytes and match the regular expression ^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$. Example: 0d0466b0-e727-4d9c-b35d-f84bb474a37f
encryption_context	No	Object	Key-value pairs with a maximum length of 8,192 characters. This parameter is used to record resource context information, excluding sensitive information, to ensure data integrity. If this parameter is specified during encryption, it is also required for decryption. Example: {"Key1":"Value1","Key2":"Value2"}
datakey_length	No	String	Bit length of a key. The value is a multiple of 8, in the range 8 to 8,192. Note: Set either datakey_length or key_spec. ● If neither of them is specified, a 256-bit key is generated by default. ● If both of them are specified, only datakey_length takes effect.
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff

Response Parameters

Status code: 200

Table 4-102 Response body parameters

Parameter	Type	Description
key_id	String	CMK ID.

Parameter	Type	Description
cipher_text	String	Ciphertext DEK in hexadecimal format. Two characters represent 1 byte.

Status code: 400

Table 4-103 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-104 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 403

Table 4-105 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-106 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 404

Table 4-107 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-108 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Example Requests

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "datakey_length" : "512"
}
```

Example Responses

Status code: 200

Request processing succeeded.

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "cipher_text" : "020098009EEAFCE122CAA5927D2XXX..."
}
```

Status code: 400

Invalid request parameters.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 403

Authentication failed.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 404

The requested resource does not exist or is not found.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status Codes

Status Code	Description
200	Request processing succeeded.
400	Invalid request parameters.
403	Authentication failed.
404	The requested resource does not exist or is not found.

Error Codes

See **Error Codes**.

4.1.3.4 Encrypting a DEK

Function

This API enables you to encrypt a DEK using a specified CMK.

URI

POST /v1.0/{project_id}/kms/encrypt-datakey

Table 4-109 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-110 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. The token can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-111 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	CMK ID. It should be 36 bytes and match the regular expression ^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$. Example: 0d0466b0-e727-4d9c-b35d-f84bb474a37f
encryption_context	No	Object	Key-value pairs with a maximum length of 8,192 characters. This parameter is used to record resource context information, excluding sensitive information, to ensure data integrity. If this parameter is specified during encryption, it is also required for decryption. Example: {"Key1":"Value1","Key2":"Value2"}
plain_text	Yes	String	Both the plaintext of a DEK and the SHA-256 hash value (32 bytes) of the plaintext are expressed as a hexadecimal string. Both the plaintext (64 bytes) of a DEK and the SHA-256 hash value (32 bytes) of the plaintext are expressed as a hexadecimal string.
datakey_plain_length	Yes	String	Number of bytes of a DEK in plaintext. The value range is 1 to 1024. Number of bytes of a DEK in plaintext. The value is 64.
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff

Response Parameters

Status code: 200

Table 4-112 Response body parameters

Parameter	Type	Description
key_id	String	CMK ID.
cipher_text	String	Ciphertext DEK in hexadecimal format. Two characters represent 1 byte.
datakey_length	String	Length of a DEK, in bytes.

Status code: 400

Table 4-113 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-114 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 403

Table 4-115 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-116 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 404

Table 4-117 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-118 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Example Requests

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "plain_text" :
"7549d9aea901767bf3c0b3e14b10722eaf6f59053bbd82045d04e075e809a0fe6ccab48f8e5efe74e4b18ff0512
525e527b10331100f357bf42125d8d5ced94ffbc8ac72b0785ca7fe33eb6776ce3990b11e32b299d9c0a9ee0305f
b9540f797",
  "datakey_plain_length" : "64"
}
```

Example Responses

Status code: 200

Request processing succeeded.

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "datakey_length" : "64",
  "cipher_text" : "020098009EEAFCE122CAA5927D2XXX..."
}
```

Status code: 400

Invalid request parameters.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 403

Authentication failed.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 404

The requested resource does not exist or is not found.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status Codes

Status Code	Description
200	Request processing succeeded.
400	Invalid request parameters.
403	Authentication failed.
404	The requested resource does not exist or is not found.

Error Codes

See **Error Codes**.

4.1.3.5 Decrypting a DEK

Function

This API enables you to decrypt a DEK using a specified CMK.

Constraints

Decrypted data is the result in the encrypted data.

URI

POST /v1.0/{project_id}/kms/decrypt-datakey

Table 4-119 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-120 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. The token can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-121 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	CMK ID. It should be 36 bytes and match the regular expression ^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$. Example: 0d0466b0-e727-4d9c-b35d-f84bb474a37f
encryption_context	No	Object	Key-value pairs with a maximum length of 8,192 characters. This parameter is used to record resource context information, excluding sensitive information, to ensure data integrity. If this parameter is specified during encryption, it is also required for decryption. Example: {"Key1":"Value1","Key2":"Value2"}
cipher_text	Yes	String	Hexadecimal string of the DEK ciphertext and the metadata. It is the value of cipher_text in the encryption result.
datakey_cipher_length	Yes	String	Number of bytes of a key. The value range is 1 to 1024. Number of bytes of a key. The value is 64.
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff

Response Parameters

Status code: 200

Table 4-122 Response body parameters

Parameter	Type	Description
data_key	String	Hexadecimal string of the plaintext of a DEK
datakey_length	String	Length of a plaintext DEK, in bytes.
datakey_dgst	String	Hexadecimal string corresponding to the SHA-256 hash value of the plaintext of a DEK.

Status code: 400

Table 4-123 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-124 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 403

Table 4-125 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-126 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 404

Table 4-127 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-128 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Example Requests

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "cipher_text" : "020098005273E14E6E8E95F5463BECDC27E80AFxxxxxxxxxx...",
  "datakey_cipher_length" : "64"
}
```

Example Responses

Status code: 200

Request processing succeeded.

```
{
  "data_key" : "000000e724d9cb35df84bb474a37fXXX...",
  "datakey_length" : "64",
  "datakey_dgst" : "F5A5FD42D16A20302798EF6ED3099XXX..."
}
```

Status code: 400

Invalid request parameters.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 403

Authentication failed.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 404

The requested resource does not exist or is not found.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status Codes

Status Code	Description
200	Request processing succeeded.
400	Invalid request parameters.
403	Authentication failed.
404	The requested resource does not exist or is not found.

Error Codes

See **Error Codes**.

4.1.4 CMK Importing Management

4.1.4.1 Obtaining CMK Import Parameters

Function

This API enables you to obtain necessary parameters to import a CMK, including a CMK import token and a CMK encryption public key.

Constraints

- The returned public key type is RSA_2048 by default.

URI

POST /v1.0/{project_id}/kms/get-parameters-for-import

Table 4-129 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-130 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. The token can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-131 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	CMK ID. It should be 36 bytes and match the regular expression ^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$. Example: 0d0466b0-e727-4d9c-b35d-f84bb474a37f
wrapping_algorithm	Yes	String	Encryption algorithm of key materials. It can be: ● RSAES_PKCS1_V1_5 ● RSAES_OAEP_SHA_1 ● RSAES_OAEP_SHA_256
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff

Response Parameters

Status code: 200

Table 4-132 Response body parameters

Parameter	Type	Description
key_id	String	CMK ID.
import_token	String	Key import token.
expiration_time	String	Import parameter expiration time. The timestamp indicates the total seconds past the start of the epoch date (January 1, 1970).

Parameter	Type	Description
public_key	String	Public key of the DEK material, in Base64 format.

Status code: 400

Table 4-133 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-134 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 403

Table 4-135 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-136 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 404

Table 4-137 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-138 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Example Requests

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "wrapping_algorithm" : "RSAES_OAEP_SHA_1"
}
```

Example Responses

Status code: 200

Request processing succeeded.

```
{
  "key_id" : "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
  "import_token" : "AACIBjY2ZTQxYjBmLTY3ZWItNDU4Ny04OTIxLWVhZXXX...",
  "expiration_time" : 1501578672,
  "public_key" : "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCXXX..."
}
```

Status code: 400

Invalid request parameters.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 403

Authentication failed.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 404

The requested resource does not exist or is not found.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status Codes

Status Code	Description
200	Request processing succeeded.
400	Invalid request parameters.
403	Authentication failed.
404	The requested resource does not exist or is not found.

Error Codes

See **Error Codes**.

4.1.4.2 Importing CMK Material

Function

This API allows you to import CMK material.

URI

POST /v1.0/{project_id}/kms/import-key-material

Table 4-139 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-140 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. The token can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-141 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	CMK ID. It should be 36 bytes and match the regular expression ^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$. Example: 0d0466b0-e727-4d9c-b35d-f84bb474a37f
import_token	Yes	String	Key import token in Base64 format, which matches the regular expression ^[0-9a-zA-Z+/=]{200,6144}$.
encrypted_key_material	Yes	String	Encrypted key material, which is in Base64 format and matches the regular expression ^[0-9a-zA-Z+/=]{344,360}$.
expiration_time	No	String	Time when the key material expires. The timestamp indicates the total seconds past the start of the epoch date (January 1, 1970). KMS will delete the key material within 24 hours after its expiration. Example: 1550291833
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff

Response Parameters

Status code: 400

Table 4-142 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-143 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 403

Table 4-144 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-145 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 404

Table 4-146 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-147 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Example Requests

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "import_token" : "AACIBjY2ZTQxYItNDU4Ny04OTIxLWVhZTVhZjg5NDZm....",
  "expiration_time" : 1521578672
}
```

Example Responses

Status code: 400

Invalid request parameters.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 403

Authentication failed.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 404

The requested resource does not exist or is not found.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status Codes

Status Code	Description
200	Request processing succeeded.
400	Invalid request parameters.
403	Authentication failed.
404	The requested resource does not exist or is not found.

Error Codes

See **Error Codes**.

4.1.4.3 Deleting CMK Material

Function

This API allows you to delete CMK material.

URI

POST /v1.0/{project_id}/kms/delete-imported-key-material

Table 4-148 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-149 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. The token can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-150 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	CMK ID. It should be 36 bytes and match the regular expression ^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$. Example: 0d0466b0-e727-4d9c-b35d-f84bb474a37f
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff

Response Parameters

Status code: 400

Table 4-151 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-152 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 403

Table 4-153 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-154 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 404

Table 4-155 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-156 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Example Requests

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f"
}
```

Example Responses

Status code: 400

Invalid request parameters.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 403

Authentication failed.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 404

The requested resource does not exist or is not found.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status Codes

Status Code	Description
200	Request processing succeeded.
400	Invalid request parameters.
403	Authentication failed.
404	The requested resource does not exist or is not found.

Error Codes

See **Error Codes**.

4.1.5 Authorization Management

4.1.5.1 Creating a Grant

Function

This API is used to create a grant. A grantee can perform operations on a granted key.

Constraints

A Default Master Key (the alias suffix of which is /default) does not allow permission granting.

URI

POST /v1.0/{project_id}/kms/create-grant

Table 4-157 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-158 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. The token can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-159 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	CMK ID. It should be 36 bytes and match the regular expression ^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$. Example: 0d0466b0-e727-4d9c-b35d-f84bb474a37f

Parameter	Mandatory	Type	Description
grantee_principal	Yes	String	Grantee ID, which contains 1 to 64 bytes and matches the regular expression ^[a-zA-Z0-9]{1, 64}$. Example: 0d0466b00d0466b00d0466b00d0466b0
operations	Yes	Array of strings	List of granted operations. Values: create-datakey, create-datakey-without-plaintext, encrypt-datakey, decrypt-datakey, describe-key, create-grant, retire-grant, encrypt-data, decrypt-data. A value containing only create-grant is invalid.
name	No	String	Grant name. The value is a string of 1 to 255 characters and matches the regular expression ^[a-zA-Z0-9:/_-]{1,255}$.
retiring_principal	No	String	ID of the user who can retire a grant. It contains 1 to 64 bytes and matches the regular expression ^[a-zA-Z0-9]{1, 64}$. Example: 0d0466b00d0466b00d0466b00d0466b0
grantee_principal_type	No	String	Grant type. Values: user, domain. The default value is user.
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff

Response Parameters

Status code: 200

Table 4-160 Response body parameters

Parameter	Type	Description
grant_id	String	Grant ID, which contains 64 bytes.

Status code: 400

Table 4-161 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-162 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 403

Table 4-163 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-164 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 404

Table 4-165 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-166 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error information.

Example Requests

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "operations" : [ "describe-key", "create-datakey", "encrypt-datakey" ],
  "grantee_principal" : "13gg44z4g2sglzk0egw0u726zoyzvrs8",
  "grantee_principal_type" : "user",
  "retiring_principal" : "13gg44z4g2sglzk0egw0u726zoyzvrs8"
}
```

Example Responses

Status code: 200

Request processing succeeded.

```
{
  "grant_id" : "7c9a3286af4fcca5f0a385ad13e1d21a50e27b6dbcab50f37f30f93b8939827d"
}
```

Status code: 400

Invalid request parameters.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 403

Authentication failed.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 404

The requested resource does not exist or is not found.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status Codes

Status Code	Description
200	Request processing succeeded.
400	Invalid request parameters.
403	Authentication failed.
404	The requested resource does not exist or is not found.

Error Codes

See **Error Codes**.

4.1.5.2 Revoking a Grant

Function

This API allows you to revoke a grant.

Constraints

Only the user who created the CMK can revoke a grant.

URI

POST /v1.0/{project_id}/kms/revoke-grant

Table 4-167 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-168 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. The token can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-169 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	CMK ID. It should be 36 bytes and match the regular expression ^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$. Example: 0d0466b0-e727-4d9c-b35d-f84bb474a37f
grant_id	Yes	String	Grant ID, which contains 64 bytes and matches the regular expression ^[A-Fa-f0-9]{64}$. Example: 7c9a3286af4fcca5f0a385ad13e1d21a50e27b6dbcab50f37f30f93b8939827d
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff

Response Parameters

Status code: 400

Table 4-170 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-171 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 403

Table 4-172 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-173 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 404

Table 4-174 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-175 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Example Requests

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "grant_id" : "7c9a3286af4fcca5f0a385ad13e1d21a50e27b6dbcab50f37f30f93b8939827d"
}
```

Example Responses

Status code: 400

Invalid request parameters.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 403

Authentication failed.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 404

The requested resource does not exist or is not found.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status Codes

Status Code	Description
200	Request processing succeeded.
400	Invalid request parameters.
403	Authentication failed.
404	The requested resource does not exist or is not found.

Error Codes

See **Error Codes**.

4.1.5.3 Retiring a Grant

Function

This API enables users to retire a grant. For example, user A grants operation permissions on CMK A/key to user B and authorizes user C to retire the grant. By doing this, users A, B, and C all can cancel the permissions. After the canceling, user B does not have permissions on CMK A/key any more.

Constraints

The following are allowed to call this API:

- The user who granted the permissions
- The user indicated by parameter retiring_principal
- The user indicated by parameter grantee_principal when retire-grant has been selected

URI

POST /v1.0/{project_id}/kms/retire-grant

Table 4-176 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-177 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. The token can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-178 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	CMK ID. It should be 36 bytes and match the regular expression ^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$. Example: 0d0466b0-e727-4d9c-b35d-f84bb474a37f
grant_id	Yes	String	Grant ID, which contains 64 bytes and matches the regular expression ^[A-Fa-f0-9]{64}$. Example: 7c9a3286af4fcca5f0a385ad13e1d21a50e27b6dbcab50f37f30f93b8939827d
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff

Response Parameters

Status code: 400

Table 4-179 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-180 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 403

Table 4-181 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-182 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 404

Table 4-183 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-184 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Example Requests

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "grant_id" : "7c9a3286af4fcca5f0a385ad13e1d21a50e27b6dbcab50f37f30f93b8939827d"
}
```

Example Responses

Status code: 400

Invalid request parameters.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 403

Authentication failed.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 404

The requested resource does not exist or is not found.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status Codes

Status Code	Description
200	Request processing succeeded.
400	Invalid request parameters.
403	Authentication failed.
404	The requested resource does not exist or is not found.

Error Codes

See **Error Codes**.

4.1.5.4 Querying Grants on a CMK

Function

This API enables you to query grants on a CMK.

URI

POST /v1.0/{project_id}/kms/list-grants

Table 4-185 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-186 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. The token can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-187 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	CMK ID. It should be 36 bytes and match the regular expression ^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$. Example: 0d0466b0-e727-4d9c-b35d-f84bb474a37f

Parameter	Mandatory	Type	Description
limit	No	String	Number of returned grant records. If the number of retrieved results is greater than this value, true is returned for the response parameter truncated, indicating that multiple pages of results are retrieved. The value cannot exceed the maximum number of grants. Example: 100
marker	No	String	Start position of pagination query. If truncated is true in the response, you can send consecutive requests to obtain more records. Set marker to the value of next_marker in the response. Example: 10
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff

Response Parameters

Status code: 200

Table 4-188 Response body parameters

Parameter	Type	Description
grants	Array of **Grants** objects	Grant list.
next_marker	String	Value of marker used for obtaining the next page of results. If truncated is false, next_marker is left blank.
truncated	String	Whether there is a next page of results: ● true: There is a next page. ● false: This is the last page.
total	Integer	Total number of grants.

Table 4-189 Grants

Parameter	Type	Description
key_id	String	CMK ID.
grant_id	String	Grant ID, which contains 64 bytes.
grantee_principal	String	Grantee ID, which contains 1 to 64 bytes and matches the regular expression ^[a-zA-Z0-9]{1, 64}$. Example: 0d0466b00d0466b00d0466b00d0466b0
grantee_principal_type	String	Grant type. Values: user, domain.
operations	Array of strings	List of granted operations. Values: create-datakey, create-datakey-without-plaintext, encrypt-datakey, decrypt-datakey, describe-key, create-grant, retire-grant, encrypt-data, decrypt-data. A value containing only create-grant is invalid.
issuing_principal	String	Grantor ID, which contains 1 to 64 bytes and matches the regular expression ^[a-zA-Z0-9]{1, 64}$. Example: 0d0466b00d0466b00d0466b00d0466b0
creation_date	String	Creation time. The timestamp indicates the total seconds past the start of the epoch date (January 1, 1970). Example: 1497341531000
name	String	Grant name. The value is a string of 1 to 255 characters and matches the regular expression ^[a-zA-Z0-9:/_-]{1,255}$.
retiring_principal	String	ID of the user who can retire a grant. It contains 1 to 64 bytes and matches the regular expression ^[a-zA-Z0-9]{1, 64}$. Example: 0d0466b00d0466b00d0466b00d0466b0

Status code: 400

Table 4-190 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-191 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 403

Table 4-192 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-193 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 404

Table 4-194 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-195 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Example Requests

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f"
}
```

Example Responses

Status code: 200

Request processing succeeded.

```
{
  "grants" : [ {
    "operations" : [ "create-datakey", "describe-key" ],
    "issuing_principal" : "8b961fb414344d59825ba0c8c008c815",
    "key_id" : "737fd52b-36c4-4c91-972e-f6e202de9f6e",
    "grant_id" : "dd3f03e9229a5e47a41be6c27a630e60d5cbdbad2be89465d63109ad034db7d8",
    "grantee_principal" : "13gg44z4g2sglzk0egw0u726zoyzvrs8",
    "name" : "13gg44z4g2sglzk0egw0u726zoyzvrs8",
    "creation_date" : "1597062260000",
    "grantee_principal_type" : "user"
  } ],
  "next_marker" : "",
  "total" : 1,
  "truncated" : "false"
}
```

Status code: 400

Invalid request parameters.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 403

Authentication failed.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 404

The requested resource does not exist or is not found.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status Codes

Status Code	Description
200	Request processing succeeded.
400	Invalid request parameters.
403	Authentication failed.

Status Code	Description
404	The requested resource does not exist or is not found.

Error Codes

See **Error Codes**.

4.1.5.5 Querying Grants That Can Be Retired

Function

This API enables you to query grants that can be retired.

URI

POST /v1.0/{project_id}/kms/list-retirable-grants

Table 4-196 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-197 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. The token can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-198 Request body parameters

Parameter	Mandatory	Type	Description
limit	No	String	Number of returned records of grants that can be retired. If the number of retrieved results is greater than this value, true is returned for the response parameter truncated, indicating that multiple pages of results are retrieved. The value cannot exceed the maximum number of grants. Example: 100
marker	No	String	Start position of pagination query. If truncated is true in the response, you can send consecutive requests to obtain more records. Set marker to the value of next_marker in the response. Example: 10
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff

Response Parameters

Status code: 200

Table 4-199 Response body parameters

Parameter	Type	Description
grants	Array of **Grants** objects	Grant list.
next_marker	String	Value of marker used for obtaining the next page of results. If truncated is false, next_marker is left blank.
truncated	String	Whether there is a next page of results: ● true: There is a next page. ● false: This is the last page.

Table 4-200 Grants

Parameter	Type	Description
key_id	String	CMK ID.
grant_id	String	Grant ID, which contains 64 bytes.
grantee_principal	String	Grantee ID, which contains 1 to 64 bytes and matches the regular expression ^[a-zA-Z0-9]{1, 64}$. Example: 0d0466b00d0466b00d0466b00d0466b0
grantee_principal_type	String	Grant type. Values: user, domain.
operations	Array of strings	List of granted operations. Values: create-datakey, create-datakey-without-plaintext, encrypt-datakey, decrypt-datakey, describe-key, create-grant, retire-grant, encrypt-data, decrypt-data. A value containing only create-grant is invalid.
issuing_principal	String	Grantor ID, which contains 1 to 64 bytes and matches the regular expression ^[a-zA-Z0-9]{1, 64}$. Example: 0d0466b00d0466b00d0466b00d0466b0
creation_date	String	Creation time. The timestamp indicates the total seconds past the start of the epoch date (January 1, 1970). Example: 1497341531000
name	String	Grant name. The value is a string of 1 to 255 characters and matches the regular expression ^[a-zA-Z0-9:/_-]{1,255}$.
retiring_principal	String	ID of the user who can retire a grant. It contains 1 to 64 bytes and matches the regular expression ^[a-zA-Z0-9]{1, 64}$. Example: 0d0466b00d0466b00d0466b00d0466b0

Status code: 400

Table 4-201 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-202 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 403

Table 4-203 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-204 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 404

Table 4-205 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-206 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Example Requests

```
{
  "limit" : "1000"
}
```

Example Responses

Status code: 200

Request processing succeeded.

```
{
  "grants" : [ {
    "operations" : [ "create-datakey", "describe-key" ],
    "issuing_principal" : "8b961fb414344d59825ba0c8c008c815",
    "key_id" : "737fd52b-36c4-4c91-972e-f6e202de9f6e",
    "grant_id" : "dd3f03e9229a5e47a41be6c27a630e60d5cbdbad2be89465d63109ad034db7d8",
    "grantee_principal" : "13gg44z4g2sglzk0egw0u726zoyzvrs8",
    "name" : "13gg44z4g2sglzk0egw0u726zoyzvrs8",
    "creation_date" : "1597062260000",
    "grantee_principal_type" : "user"
  } ],
  "next_marker" : "",
  "total" : 1,
  "truncated" : "false"
}
```

Status code: 400

Invalid request parameters.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 403

Authentication failed.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 404

The requested resource does not exist or is not found.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status Codes

Status Code	Description
200	Request processing succeeded.
400	Invalid request parameters.
403	Authentication failed.

Status Code	Description
404	The requested resource does not exist or is not found.

Error Codes

See **Error Codes**.

4.1.6 Small Data Encryption & Decryption

4.1.6.1 Encrypting Data

Function

This API enables you to encrypt data using a specified CMK.

Constraints

- When using an asymmetric CMK to encrypt data, please record the selected CMK ID and encryption algorithm. When decrypting data, you need to provide the same CMK ID and encryption algorithm. If the specified CMK and encryption algorithm do not match the value used to encrypt the data, the decryption operation will fail.
- When using a symmetric CMK to decrypt data, there is no need to provide the CMK ID and encryption algorithm. KMS will store the information in the ciphertext. KMS cannot store metadata in the ciphertext generated using an asymmetric key. The standard format of the asymmetric key ciphertext does not include configurable fields.

URI

POST /v1.0/{project_id}/kms/encrypt-data

Table 4-207 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-208 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. The token can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-209 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	CMK ID. It should be 36 bytes and match the regular expression ^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$. Example: 0d0466b0-e727-4d9c-b35d-f84bb474a37f
encryption_context	No	Object	Key-value pairs with a maximum length of 8,192 characters. This parameter is used to record resource context information, excluding sensitive information, to ensure data integrity. If this parameter is specified during encryption, it is also required for decryption. Example: {"Key1":"Value1","Key2":"Value2"}
plain_text	Yes	String	Plaintext data. It can be 1 to 4,096 bytes and should match the regular expression ^.{1,4096}$. After it is converted to a byte array, its length should still be 1 to 4096 bytes.
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff

Response Parameters

Status code: 200

Table 4-210 Response body parameters

Parameter	Type	Description
key_id	String	CMK ID.
cipher_text	String	Ciphertext DEK in hexadecimal format. Two characters represent 1 byte.

Status code: 400

Table 4-211 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-212 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 403

Table 4-213 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-214 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 404

Table 4-215 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-216 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Example Requests

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "plain_text" : "hello world"
}
```

Example Responses

Status code: 200

Request processing succeeded.

```
{
  "key_id" : "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
  "cipher_text" : "AgDoAG7EsEc2OHpQxz4gDFDH54CqwaelpTdEl+RFXXX..."
}
```

Status code: 400

Invalid request parameters.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 403

Authentication failed.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 404

The requested resource does not exist or is not found.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status Codes

Status Code	Description
200	Request processing succeeded.
400	Invalid request parameters.
403	Authentication failed.
404	The requested resource does not exist or is not found.

Error Codes

See **Error Codes**.

4.1.6.2 Decrypting Data

Function

This API enables you to decrypt data.

Constraints

- When decrypting data encrypted with an asymmetric CMK, you need to specify the CMK ID and encryption algorithm. If the specified CMK and encryption algorithm do not match the value used to encrypt the data, the decryption operation will fail.

URI

POST /v1.0/{project_id}/kms/decrypt-data

Table 4-217 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-218 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. The token can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-219 Request body parameters

Parameter	Mandatory	Type	Description
cipher_text	Yes	String	Ciphertext of encrypted data. It is the value of cipher_text in the data encryption result and matches the regular expression ^[0-9a-zA-Z+/=]{188,5648}$.
encryption_context	No	Object	Key-value pairs with a maximum length of 8,192 characters. This parameter is used to record resource context information, excluding sensitive information, to ensure data integrity. If this parameter is specified during encryption, it is also required for decryption. Example: {"Key1":"Value1","Key2":"Value2"}
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff

Response Parameters

Status code: 200

Table 4-220 Response body parameters

Parameter	Type	Description
key_id	String	CMK ID.

Parameter	Type	Description
plain_text	String	Plaintext.

Status code: 400

Table 4-221 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-222 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 403

Table 4-223 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-224 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 404

Table 4-225 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-226 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Example Requests

```
{
  "cipher_text" : "AgDoAG7EsEc2OHpQxz4gDFDH54Cqwaelxxxxxxx"
}
```

Example Responses

Status code: 200

Request processing succeeded.

```
{
  "key_id" : "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
  "plain_text" : "hello world"
}
```

Status code: 400

Invalid request parameters.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 403

Authentication failed.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 404

The requested resource does not exist or is not found.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status Codes

Status Code	Description
200	Request processing succeeded.
400	Invalid request parameters.
403	Authentication failed.
404	The requested resource does not exist or is not found.

Error Codes

See **Error Codes**.

4.1.7 Signature & Verification

4.1.7.1 Signing Message

Function

This API enables you to create a digital signature for a message or message digest by using the privatekey in an asymmetric CMK.

Constraints

- Only support asymmetric keys with key_usage of SIGN_VERIFY for signing operation.

URI

POST /v1.0/{project_id}/kms/sign

Table 4-227 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-228 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. The token can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-229 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	Key ID. It should be 36 bytes and match the regular expression ^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$. Example: 0d0466b0-e727-4d9c-b35d-f84bb474a37f
message	Yes	String	Specifies the message or message digest to sign. Messages can be 0-4096 bytes. To sign a larger message, provide the message digest.Using Base64-encoded binary data object.
signing_algorithm	Yes	String	Specifies the signing algorithm to use when signing the message. Choose an algorithm that is compatible with the type of the specified asymmetric CMK.It can be: ● RSASSA_PSS_SHA_256 ● RSASSA_PSS_SHA_384 ● RSASSA_PSS_SHA_512 ● RSASSA_PKCS1_V1_5_SHA_256 ● RSASSA_PKCS1_V1_5_SHA_384 ● RSASSA_PKCS1_V1_5_SHA_512 ● ECDSA_SHA_256 ● ECDSA_SHA_384 ● ECDSA_SHA_512

Parameter	Mandatory	Type	Description
message_type	No	String	Message Type. The default value is "DIGEST" It can be: ● DIGEST : message digest ● RAW : message
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff

Response Parameters

Status code: 200

Table 4-230 Response body parameters

Parameter	Type	Description
key_id	String	CMK ID.
signature	String	The cryptographic signature that was generated for the message.

Status code: 400

Table 4-231 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-232 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 403

Table 4-233 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-234 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 404

Table 4-235 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-236 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Example Requests

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "signing_algorithm" : "RSASSA_PKCS1_V1_5_SHA_256",
  "message" : "MmFiZWE0ZjI3ZGIxYTkzY2RmYmEzM2YwMTA1YmJjYw=="
}
```

Example Responses

Status code: 200

Request processing succeeded.

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "signature" : "jFUqQESGBc0j6k9BozzrP9YL4qk8/W9DZRvK6XXX..."
}
```

Status code: 400

Invalid request parameters.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 403

Authentication failed.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 404

The requested resource does not exist or is not found.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status Codes

Status Code	Description
200	Request processing succeeded.
400	Invalid request parameters.
403	Authentication failed.
404	The requested resource does not exist or is not found.

Error Codes

See **Error Codes**.

4.1.7.2 Verifying Signature

Function

This API enables you to verify a digital signature that was generated by the sign operation.

Constraints

- Only support asymmetric keys with key_usage of SIGN_VERIFY for verifying operation.

URI

POST /v1.0/{project_id}/kms/verify

Table 4-237 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-238 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. The token can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-239 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	Key ID. It should be 36 bytes and match the regular expression ^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$. Example: 0d0466b0-e727-4d9c-b35d-f84bb474a37f
message	Yes	String	Specifies the message or message digest to sign. Messages can be 0-4096 bytes. To sign a larger message, provide the message digest.Using Base64-encoded binary data object.
signature	Yes	String	The signature that the Sign operation generated.

Parameter	Mandatory	Type	Description
signing_algorithm	Yes	String	Specifies the signing algorithm to use when signing the message. Choose an algorithm that is compatible with the type of the specified asymmetric CMK.It can be: ● RSASSA_PSS_SHA_256 ● RSASSA_PSS_SHA_384 ● RSASSA_PSS_SHA_512 ● RSASSA_PKCS1_V1_5_SHA_256 ● RSASSA_PKCS1_V1_5_SHA_384 ● RSASSA_PKCS1_V1_5_SHA_512 ● ECDSA_SHA_256 ● ECDSA_SHA_384 ● ECDSA_SHA_512
message_type	No	String	Message Type. The default value is "DIGEST" It can be: ● DIGEST : message digest ● RAW : message
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff

Response Parameters

Status code: 200

Table 4-240 Response body parameters

Parameter	Type	Description
key_id	String	CMK ID.
signature_vaild	Boolean	A Boolean value that indicates whether the signature was verified.

Status code: 400

Table 4-241 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-242 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 403

Table 4-243 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-244 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 404

Table 4-245 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-246 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Example Requests

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "signing_algorithm" : "RSASSA_PKCS1_V1_5_SHA_256",
  "signature" : "jFUqQESGBc0j6k9BozzrP9YL4qk8/W9DZRvK6XXX...",
  "message" : "MmFiZWE0ZjI3ZGIxYTkzY2RmYmEzM2YwMTA1YmJjYw=="
}
```

Example Responses

Status code: 200

Request processing succeeded.

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "signature_valid" : "true"
}
```

Status code: 400

Invalid request parameters.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 403

Authentication failed.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 404

The requested resource does not exist or is not found.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status Codes

Status Code	Description
200	Request processing succeeded.
400	Invalid request parameters.
403	Authentication failed.
404	The requested resource does not exist or is not found.

Error Codes

See **Error Codes**.

4.1.8 Rotation Management

4.1.8.1 Enabling Rotation for a CMK

Function

This API allows you to enable rotation for a CMK.

Constraints

- The default rotation interval is 365 days.
- CMKs created using imported key materials and Default Master Keys do not support rotation.

URI

POST /v1.0/{project_id}/kms/enable-key-rotation

Table 4-247 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-248 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. The token can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-249 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	CMK ID. It should be 36 bytes and match the regular expression ^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$. Example: 0d0466b0-e727-4d9c-b35d-f84bb474a37f
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff

Response Parameters

Status code: 400

Table 4-250 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-251 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 403

Table 4-252 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-253 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 404

Table 4-254 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-255 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Example Requests

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f"
}
```

Example Responses

Status code: 400

Invalid request parameters.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 403

Authentication failed.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 404

The requested resource does not exist or is not found.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status Codes

Status Code	Description
200	Request processing succeeded.
400	Invalid request parameters.
403	Authentication failed.
404	The requested resource does not exist or is not found.

Error Codes

See **Error Codes**.

4.1.8.2 Changing the Rotation Interval for a CMK

Function

This API enables you to change the rotation interval for a CMK.

URI

POST /v1.0/{project_id}/kms/update-key-rotation-interval

Table 4-256 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-257 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. The token can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-258 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	CMK ID. It should be 36 bytes and match the regular expression ^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$. Example: 0d0466b0-e727-4d9c-b35d-f84bb474a37f
rotation_interval	Yes	Integer	Rotation interval. The value is an integer in the range 30 to 365. Set the interval based on how often a CMK is used. If it is frequently used, set a short interval; otherwise, set a long one.
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff

Response Parameters

Status code: 400

Table 4-259 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-260 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 403

Table 4-261 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-262 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 404

Table 4-263 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-264 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Example Requests

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
  "rotation_interval" : 30
}
```

Example Responses

Status code: 400

Invalid request parameters.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 403

Authentication failed.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 404

The requested resource does not exist or is not found.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status Codes

Status Code	Description
200	Request processing succeeded.
400	Invalid request parameters.
403	Authentication failed.
404	The requested resource does not exist or is not found.

Error Codes

See **Error Codes**.

4.1.8.3 Disabling Rotation for a CMK

Function

This API allows you to disable rotation for a CMK.

URI

POST /v1.0/{project_id}/kms/disable-key-rotation

Table 4-265 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-266 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. The token can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-267 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	CMK ID. It should be 36 bytes and match the regular expression ^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$. Example: 0d0466b0-e727-4d9c-b35d-f84bb474a37f
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff

Response Parameters

Status code: 400

Table 4-268 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-269 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 403

Table 4-270 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-271 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 404

Table 4-272 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-273 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Example Requests

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f"
}
```

Example Responses

Status code: 400

Invalid request parameters.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 403

Authentication failed.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 404

The requested resource does not exist or is not found.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status Codes

Status Code	Description
200	Request processing succeeded.
400	Invalid request parameters.
403	Authentication failed.
404	The requested resource does not exist or is not found.

Error Codes

See **Error Codes**.

4.1.8.4 Querying the Rotation Status of a CMK

Function

This API enables you to query the rotation status of a CMK.

URI

POST /v1.0/{project_id}/kms/get-key-rotation-status

Table 4-274 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-275 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. The token can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-276 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	CMK ID. It should be 36 bytes and match the regular expression ^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$. Example: 0d0466b0-e727-4d9c-b35d-f84bb474a37f
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff

Response Parameters

Status code: 200

Table 4-277 Response body parameters

Parameter	Type	Description
key_rotation_enabled	Boolean	Key rotation status. The default value is false, indicating that key rotation is disabled.

Parameter	Type	Description
rotation_interval	String	Rotation interval. The value is an integer in the range 30 to 365. Set the interval based on how often a CMK is used. If it is frequently used, set a short interval; otherwise, set a long one.
last_rotation_time	String	Last key rotation time. The timestamp indicates the total seconds past the start of the epoch date (January 1, 1970).
number_of_rotations	Integer	Number of key rotations.

Status code: 400

Table 4-278 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-279 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 403

Table 4-280 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-281 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 404

Table 4-282 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-283 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Example Requests

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f"
}
```

Example Responses

Status code: 200

Request processing succeeded.

```
{
  "key_rotation_enabled" : true,
  "rotation_interval" : 30,
  "last_rotation_time" : "1501578672000",
  "number_of_rotations" : 3
}
```

Status code: 400

Invalid request parameters.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 403

Authentication failed.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 404

The requested resource does not exist or is not found.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status Codes

Status Code	Description
200	Request processing succeeded.
400	Invalid request parameters.
403	Authentication failed.
404	The requested resource does not exist or is not found.

Error Codes

See **Error Codes**.

4.1.9 Tag Management

4.1.9.1 Querying CMK Instances

Function

This API allows you to query CMK instances. You can use the tag filtering function to query the detailed information about a specified CMK.

URI

POST /v1.0/{project_id}/kms/resource_instances/action

Table 4-284 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-285 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. The token can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-286 Request body parameters

Parameter	Mandatory	Type	Description
limit	No	String	Number of records in a query. If action is to count, you do not need to set this parameter. If action is filter, the default value of this parameter is 10. The value of limit is in the ranges 1 to 1,000.
offset	No	String	Index location. The query starts from the next resource of the specified location. When data on a page is queried, the value in the response body of the previous page is transferred to this parameter. (If action is to count, you do not need to set this parameter.) If the action value is filter, the default value is 0. The value of offset must be a number and cannot be negative.
action	No	String	Operation type. It can be: ● filter: Filter record. ● count: Count the total number of records.

Parameter	Mandatory	Type	Description
tags	No	Array of **Tag** objects	Tag list, which is a collection of key-value pairs. ● key: Tag key. A CMK can have a maximum of 10 keys, and each of them is unique and cannot be empty. A key cannot have duplicate values. It consists of up to 36 characters. ● value: Tag value. Each tag value can contain a maximum of 43 characters. The values are in the AND relationship.
matches	No	Array of **TagItem** objects	Field to be matched. ● key: The field to be matched, for example, resource_name. ● value: The value to be matched. It contains a maximum of 255 characters and cannot be empty.
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff

Table 4-287 Tag

Parameter	Mandatory	Type	Description
key	No	String	Key. A tag key contains a maximum of 36 Unicode characters. It cannot be left blank. It cannot contain ASCII characters (0–31), asterisks (*), angle brackets (< and >), backslashes (), and equal signs (=).
values	No	Array of strings	Tag value set.

Table 4-288 TagItem

Parameter	Mandatory	Type	Description
key	No	String	Key. A tag key contains a maximum of 36 Unicode characters. It cannot be left blank. It cannot contain ASCII characters (0–31), asterisks (*), angle brackets (< and >), backslashes (), and equal signs (=).
value	No	String	Value. A tag value can contain a maximum of 43 Unicode characters and can be an empty string. It cannot contain ASCII characters (0–31), asterisks (*), angle brackets (< and >), backslashes (), and equal signs (=).

Response Parameters

Status code: 200

Table 4-289 Response body parameters

Parameter	Type	Description
resources	Array of **ActionResources** objects	Resource list.
total_count	Integer	Total number of records.

Table 4-290 ActionResources

Parameter	Type	Description
resource_id	String	Resource ID.
resource_detail	**KeyDetails** object	Key details.
resource_name	String	Specifies the resource name. This parameter is an empty string by default.
tags	Array of **TagItem** objects	Tag list. If there is no tag in the list, an empty array is returned.

Table 4-291 KeyDetails

Parameter	Type	Description
key_id	String	CMK ID.
domain_id	String	User domain ID.
key_alias	String	Key alias.
realm	String	Key realm.
key_usage	String	CMK usage。 ● ENCRYPT_DECRYPT ● SIGN_VERIFY
key_description	String	Key description.
creation_date	String	Time when the key was created. The timestamp indicates the total seconds past the start of the epoch date (January 1, 1970).
scheduled_deletion_date	String	Time when the key was scheduled to be deleted. The timestamp indicates the total seconds past the start of the epoch date (January 1, 1970).
key_state	String	Key status, which matches the regular expression ^[1-5]{1}$. It can be: ● 1: to be activated ● 2: enabled ● 3: disabled ● 4: pending deletion ● 5: pending import
default_key_flag	String	Master key identifier. The value is 1 for Default Master Keys and 0 for non-default master keys.
key_type	String	Key type.
expiration_time	String	Time when the key material expires. The timestamp indicates the total seconds past the start of the epoch date (January 1, 1970).
origin	String	Key source. It can be: ● kms: The key material was generated by KMS. ● external: The key material was imported.
key_rotation_enabled	String	Key rotation status. The default value is false, indicating that key rotation is disabled.

Parameter	Type	Description
sys_enterprise_project_id	String	Enterprise project ID. Its default value is 0. ● For users who have enabled the enterprise project function, this value indicates that resources are in the default enterprise project. ● For users who have not enabled the enterprise project function, this value indicates that resources are not in the default enterprise project.

Table 4-292 TagItem

Parameter	Type	Description
key	String	Key. A tag key contains a maximum of 36 Unicode characters. It cannot be left blank. It cannot contain ASCII characters (0–31), asterisks (*), angle brackets (< and >), backslashes (), and equal signs (=).
value	String	Value. A tag value can contain a maximum of 43 Unicode characters and can be an empty string. It cannot contain ASCII characters (0–31), asterisks (*), angle brackets (< and >), backslashes (), and equal signs (=).

Status code: 400

Table 4-293 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-294 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 403

Table 4-295 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-296 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Example Requests

```
{
  "offset" : "100",
  "limit" : "100",
  "action" : "filter",
  "matches" : [ {
    "key" : "resource_name",
    "value" : "resource1"
  } ],
  "tags" : [ {
    "key" : "key1",
    "values" : [ "value1", "value2" ]
  } ]
}
```

Example Responses

Status code: 200

Request processing succeeded.

```
{
  "resources" : [ {
    "resource_id" : "90c03e67-5534-4ed0-acfa-89780e47a535",
    "resource_detail" : [ {
      "key_id" : "90c03e67-5534-4ed0-acfa-89780e47a535",
      "domain_id" : "4B688Fb77412Aee5570E7ecdbeB5afdc",
      "key_alias" : "tagTest_xmdmi",
      "key_description" : "123",
      "creation_date" : 1521449277000,
      "scheduled_deletion_date" : "",
      "key_state" : 2,
      "default_key_flag" : 0,
      "key_type" : 1,
      "key_rotation_enabled" : false,
      "expiration_time" : "",
      "origin" : "kms",
      "sys_enterprise_project_id" : "0",
      "realm" : "test"
    } ],
    "resource_name" : "tagTest_xmdmi",
    "tags" : [ {
      "key" : "key",
      "value" : "testValue!"
    }, {
      "key" : "haha",
      "value" : "testValue"
    } ]
  } ],
  "total_count" : 1
}
```

Status code: 400

Invalid request parameters.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 403

Authentication failed.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status Codes

Status Code	Description
200	Request processing succeeded.
400	Invalid request parameters.
403	Authentication failed.

Error Codes

See **Error Codes**.

4.1.9.2 Querying CMK Tags

Function

This API allows you to query tags of a specified CMK. TMS may use this API to query all tags of a specified CMK.

URI

GET /v1.0/{project_id}/kms/{key_id}/tags

Table 4-297 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
key_id	Yes	String	CMK ID.

Request Parameters

Table 4-298 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. The token can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-299 Request body parameters

Parameter	Mandatory	Type	Description
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff

Response Parameters

Status code: 200

Table 4-300 Response body parameters

Parameter	Type	Description
tags	Array of **TagItem** objects	Tag list, which is a collection of key-value pairs. ● key: Tag key. A CMK can have a maximum of 10 keys, and each of them is unique and cannot be empty. A key cannot have duplicate values. It consists of up to 36 characters. ● value: Tag value. Each tag value can contain a maximum of 43 characters. The values are in the AND relationship.
existTagsNum	Integer	

Table 4-301 TagItem

Parameter	Type	Description
key	String	Key. A tag key contains a maximum of 36 Unicode characters. It cannot be left blank. It cannot contain ASCII characters (0–31), asterisks (*), angle brackets (< and >), backslashes (), and equal signs (=).
value	String	Value. A tag value can contain a maximum of 43 Unicode characters and can be an empty string. It cannot contain ASCII characters (0–31), asterisks (*), angle brackets (< and >), backslashes (), and equal signs (=).

Status code: 400

Table 4-302 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-303 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 403

Table 4-304 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-305 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 404

Table 4-306 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-307 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Example Requests

None

Example Responses

Status code: 200

Request processing succeeded.

```
{
  "tags" : [ {
    "key" : "key1",
    "value" : "value1"
  }, {
    "key" : "key2",
    "value" : "value2"
  } ],
  "existTagsNum" : 2
}
```

Status code: 400

Invalid request parameters.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 403

Authentication failed.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 404

The requested resource does not exist or is not found.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status Codes

Status Code	Description
200	Request processing succeeded.
400	Invalid request parameters.
403	Authentication failed.
404	The requested resource does not exist or is not found.

Error Codes

See **Error Codes**.

4.1.9.3 Querying Project Tags

Function

This API enables you to query all tag sets of a specified project.

URI

GET /v1.0/{project_id}/kms/tags

Table 4-308 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-309 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. The token can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-310 Request body parameters

Parameter	Mandatory	Type	Description
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff

Response Parameters

Status code: 200

Table 4-311 Response body parameters

Parameter	Type	Description
tags	Array of **Tag** objects	Tag list, which is a collection of key-value pairs. ● key: Tag key. A CMK can have a maximum of 10 keys, and each of them is unique and cannot be empty. A key cannot have duplicate values. It consists of up to 36 characters. ● value: Tag value. Each tag value can contain a maximum of 43 characters. The values are in the AND relationship.

Table 4-312 Tag

Parameter	Type	Description
key	String	Key. A tag key contains a maximum of 36 Unicode characters. It cannot be left blank. It cannot contain ASCII characters (0–31), asterisks (*), angle brackets (< and >), backslashes (), and equal signs (=).

Parameter	Type	Description
values	Array of strings	Tag value set.

Status code: 403

Table 4-313 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-314 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Example Requests

None

Example Responses

Status code: 200

Request processing succeeded.

```
{
  "tags" : [ {
    "key" : "key1",
    "values" : [ "value1", "value2" ]
  }, {
    "key" : "key2",
    "values" : [ "value1", "value2" ]
  } ]
}
```

Status code: 403

Authentication failed.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status Codes

Status Code	Description
200	Request processing succeeded.
403	Authentication failed.

Error Codes

See **Error Codes**.

4.1.9.4 Adding or Deleting CMK Tags in Batches

Function

This API enables you to add or delete CMK tags in batches.

URI

POST /v1.0/{project_id}/kms/{key_id}/tags/action

Table 4-315 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
key_id	Yes	String	CMK ID.

Request Parameters

Table 4-316 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. The token can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-317 Request body parameters

Parameter	Mandatory	Type	Description
tags	No	Array of **TagItem** objects	Tag list, which is a collection of key-value pairs.
action	No	String	Operation type. It can be: create or delete
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff

Table 4-318 TagItem

Parameter	Mandatory	Type	Description
key	No	String	Key. A tag key contains a maximum of 36 Unicode characters. It cannot be left blank. It cannot contain ASCII characters (0–31), asterisks (*), angle brackets (< and >), backslashes (), and equal signs (=).
value	No	String	Value. A tag value can contain a maximum of 43 Unicode characters and can be an empty string. It cannot contain ASCII characters (0–31), asterisks (*), angle brackets (< and >), backslashes (), and equal signs (=).

Response Parameters

Status code: 400

Table 4-319 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-320 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 403

Table 4-321 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-322 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 404

Table 4-323 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-324 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Example Requests

```
{
  "action" : "create",
  "tags" : [ {
    "key" : "key1",
    "value" : "value1"
  }, {
    "key" : "key",
    "value" : "value3"
  } ]
}
```

Example Responses

Status code: 400

Invalid request parameters.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 403

Authentication failed.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 404

The requested resource does not exist or is not found.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status Codes

Status Code	Description
204	No Content
400	Invalid request parameters.
403	Authentication failed.
404	The requested resource does not exist or is not found.

Error Codes

See **Error Codes**.

4.1.9.5 Adding a CMK Tag

Function

This API allows you to add a CMK tag.

URI

POST /v1.0/{project_id}/kms/{key_id}/tags

Table 4-325 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
key_id	Yes	String	CMK ID.

Request Parameters

Table 4-326 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. The token can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-327 Request body parameters

Parameter	Mandatory	Type	Description
tag	No	**TagItem** object	Tag.
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff

Table 4-328 TagItem

Parameter	Mandatory	Type	Description
key	No	String	Key. A tag key contains a maximum of 36 Unicode characters. It cannot be left blank. It cannot contain ASCII characters (0–31), asterisks (*), angle brackets (< and >), backslashes (), and equal signs (=).
value	No	String	Value. A tag value can contain a maximum of 43 Unicode characters and can be an empty string. It cannot contain ASCII characters (0–31), asterisks (*), angle brackets (< and >), backslashes (), and equal signs (=).

Response Parameters

Status code: 400

Table 4-329 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-330 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 403

Table 4-331 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-332 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 404

Table 4-333 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-334 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Example Requests

```
{
  "tag" : {
    "key" : "DEV",
    "value" : "DEV1"
  }
}
```

Example Responses

Status code: 400

Invalid request parameters.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 403

Authentication failed.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 404

The requested resource does not exist or is not found.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status Codes

Status Code	Description
204	No Content
400	Invalid request parameters.
403	Authentication failed.
404	The requested resource does not exist or is not found.

Error Codes

See **Error Codes**.

4.1.9.6 Adding or Deleting CMK Tags in Batches

Function

This API enables you to add or delete CMK tags in batches.

URI

DELETE /v1.0/{project_id}/kms/{key_id}/tags/{key}

Table 4-335 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
key_id	Yes	String	CMK ID.
key	Yes	String	Value of a tag key.

Request Parameters

Table 4-336 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. The token can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-337 Request body parameters

Parameter	Mandatory	Type	Description
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff

Response Parameters

Status code: 400

Table 4-338 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-339 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 403

Table 4-340 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-341 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 404

Table 4-342 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-343 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Example Requests

None

Example Responses

Status code: 400

Invalid request parameters.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 403

Authentication failed.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 404

The requested resource does not exist or is not found.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status Codes

Status Code	Description
204	No Content
400	Invalid request parameters.
403	Authentication failed.
404	The requested resource does not exist or is not found.

Error Codes

See **Error Codes**.

4.1.10 Querying APIs

4.1.10.1 Querying the List of CMKs

Function

This API allows you to query the list of all CMKs.

URI

POST /v1.0/{project_id}/kms/list-keys

Table 4-344 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-345 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. The token can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-346 Request body parameters

Parameter	Mandatory	Type	Description
limit	No	String	Number of returned records. If the number of retrieved results is greater than this value, true is returned for the response parameter truncated, indicating that multiple pages of results are retrieved. The value cannot exceed the maximum number of keys. Example: 100
marker	No	String	Start position of pagination query. If truncated is true in the response, you can send consecutive requests to obtain more records. Set marker to the value of next_marker in the response. Example: 10

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID. ● If the enterprise project function is not enabled, you do not need to set this parameter. ● If the enterprise project function is enabled, you can set this parameter when creating a resource. If this parameter is not specified, the resource you create will be put under the default enterprise project (whose project ID is 0). ● If you do not have the permission to create resources under the default enterprise project, an error will be reported.
key_state	No	String	Key status, which matches the regular expression ^[1-5]{1}$. It can be: ● 1: to be activated ● 2: enabled ● 3: disabled ● 4: pending deletion ● 5: pending import
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff

Response Parameters

Status code: 200

Table 4-347 Response body parameters

Parameter	Type	Description
keys	Array of strings	CMK ID list.

Parameter	Type	Description
key_details	Array of **KeyDetails** objects	Key details list.
next_marker	String	Value of marker used for obtaining the next page of results. If truncated is false, next_marker is left blank.
truncated	String	Whether there is a next page of results: ● true: There is a next page. ● false: This is the last page.
total	Integer	Total number of keys.

Table 4-348 KeyDetails

Parameter	Type	Description
key_id	String	CMK ID.
domain_id	String	User domain ID.
key_alias	String	Key alias.
realm	String	Key realm.
key_usage	String	CMK usage。 ● ENCRYPT_DECRYPT ● SIGN_VERIFY
key_description	String	Key description.
creation_date	String	Time when the key was created. The timestamp indicates the total seconds past the start of the epoch date (January 1, 1970).
scheduled_deletion_date	String	Time when the key was scheduled to be deleted. The timestamp indicates the total seconds past the start of the epoch date (January 1, 1970).
key_state	String	Key status, which matches the regular expression ^[1-5]{1}$. It can be: ● 1: to be activated ● 2: enabled ● 3: disabled ● 4: pending deletion ● 5: pending import

Parameter	Type	Description
default_key_flag	String	Master key identifier. The value is 1 for Default Master Keys and 0 for non-default master keys.
key_type	String	Key type.
expiration_time	String	Time when the key material expires. The timestamp indicates the total seconds past the start of the epoch date (January 1, 1970).
origin	String	Key source. It can be: ● kms: The key material was generated by KMS. ● external: The key material was imported.
key_rotation_enabled	String	Key rotation status. The default value is false, indicating that key rotation is disabled.
sys_enterprise_project_id	String	Enterprise project ID. Its default value is 0. ● For users who have enabled the enterprise project function, this value indicates that resources are in the default enterprise project. ● For users who have not enabled the enterprise project function, this value indicates that resources are not in the default enterprise project.

Status code: 400

Table 4-349 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-350 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 403

Table 4-351 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-352 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Example Requests

```
{
  "limit" : "2",
  "marker" : "1"
}
```

Example Responses

Status code: 200

Request processing succeeded.

```
{
  "keys" : [ "0d0466b0-e727-4d9c-b35d-f84bb474a37f", "2e258389-bb1e-4568-a1d5-e1f50adf70ea" ],
  "key_details" : [ {
    "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
    "domain_id" : "00074811d5c27c4f8d48bb91e4a1dcfd",
    "key_alias" : "test",
    "realm" : "cn-north-7",
    "key_description" : "key_description",
    "creation_date" : "1502799822000",
    "scheduled_deletion_date" : "",
    "key_spec" : "AES_256",
    "key_usage" : "ENCRYPT_DECRYPT",
    "key_state" : "2",
    "default_key_flag" : "0",
    "key_type" : "1",
    "expiration_time" : "1501578672000",
    "origin" : "kms",
    "key_rotation_enabled" : "true",
    "sys_enterprise_project_id" : "0",
    "partition_type" : "1"
  }, {
    "key_id" : "2e258389-bb1e-4568-a1d5-e1f50adf70ea",
    "domain_id" : "00074811d5c27c4f8d48bb91e4a1dcfd",
    "key_alias" : "test",
    "realm" : "realm",
    "key_description" : "key_description",
    "creation_date" : "1502799822000",
    "scheduled_deletion_date" : "",
    "key_spec" : "AES_256",
    "key_usage" : "ENCRYPT_DECRYPT",
    "key_state" : "2",
    "default_key_flag" : "0",
    "key_type" : "1",
    "expiration_time" : "1501578672000",
    "origin" : "kms",
    "key_rotation_enabled" : "true",
    "sys_enterprise_project_id" : "0",
    "partition_type" : "1"
  } ],
  "next_marker" : "",
  "truncated" : "false",
  "total" : "2"
}
```

Status code: 400

Invalid request parameters.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 403

Authentication failed.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status Codes

Status Code	Description
200	Request processing succeeded.
400	Invalid request parameters.
403	Authentication failed.

Error Codes

See **Error Codes**.

4.1.10.2 Querying the Information About a CMK

Function

This API allows you to query the details about a CMK.

URI

POST /v1.0/{project_id}/kms/describe-key

Table 4-353 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-354 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. The token can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-355 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	CMK ID. It should be 36 bytes and match the regular expression ^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$. Example: 0d0466b0-e727-4d9c-b35d-f84bb474a37f
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff

Response Parameters

Status code: 200

Table 4-356 Response body parameters

Parameter	Type	Description
key_info	**KeyDetails** object	Key details.

Table 4-357 KeyDetails

Parameter	Type	Description
key_id	String	CMK ID.
domain_id	String	User domain ID.
key_alias	String	Key alias.
realm	String	Key realm.
key_usage	String	CMK usage。 ● ENCRYPT_DECRYPT ● SIGN_VERIFY
key_description	String	Key description.
creation_date	String	Time when the key was created. The timestamp indicates the total seconds past the start of the epoch date (January 1, 1970).
scheduled_deletion_date	String	Time when the key was scheduled to be deleted. The timestamp indicates the total seconds past the start of the epoch date (January 1, 1970).
key_state	String	Key status, which matches the regular expression ^[1-5]{1}$. It can be: ● 1: to be activated ● 2: enabled ● 3: disabled ● 4: pending deletion ● 5: pending import
default_key_flag	String	Master key identifier. The value is 1 for Default Master Keys and 0 for non-default master keys.
key_type	String	Key type.
expiration_time	String	Time when the key material expires. The timestamp indicates the total seconds past the start of the epoch date (January 1, 1970).
origin	String	Key source. It can be: ● kms: The key material was generated by KMS. ● external: The key material was imported.
key_rotation_enabled	String	Key rotation status. The default value is false, indicating that key rotation is disabled.

Parameter	Type	Description
sys_enterprise_project_id	String	Enterprise project ID. Its default value is 0. ● For users who have enabled the enterprise project function, this value indicates that resources are in the default enterprise project. ● For users who have not enabled the enterprise project function, this value indicates that resources are not in the default enterprise project.

Status code: 400

Table 4-358 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-359 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 403

Table 4-360 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-361 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 404

Table 4-362 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-363 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Example Requests

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f"
}
```

Example Responses

Status code: 200

Request processing succeeded.

```
{
  "key_info" : {
    "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
    "domain_id" : "00074811d5c27c4f8d48bb91e4a1dcfd",
    "key_alias" : "test",
    "realm" : "test",
    "key_description" : "key_description",
    "creation_date" : "1502799822000",
    "scheduled_deletion_date" : "",
    "key_spec" : "AES_256",
    "key_usage" : "ENCRYPT_DECRYPT",
    "key_state" : "2",
    "default_key_flag" : "0",
    "key_type" : "1",
    "expiration_time" : "1501578672000",
    "origin" : "kms",
    "key_rotation_enabled" : "false",
    "sys_enterprise_project_id" : "0",
    "partition_type" : "1"
  }
}
```

Status code: 400

Invalid request parameters.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 403

Authentication failed.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 404

The requested resource does not exist or is not found.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status Codes

Status Code	Description
200	Request processing succeeded.
400	Invalid request parameters.
403	Authentication failed.
404	The requested resource does not exist or is not found.

Error Codes

See **Error Codes**.

4.1.10.3 Querying the Public Key About a CMK

Function

This API allows you to query the public key info of an asymmetric CMK

URI

POST /v1.0/{project_id}/kms/get-publickey

Table 4-364 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-365 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. The token can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-366 Request body parameters

Parameter	Mandatory	Type	Description
key_id	Yes	String	CMK ID. It should be 36 bytes and match the regular expression ^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}$. Example: 0d0466b0-e727-4d9c-b35d-f84bb474a37f
sequence	No	String	36-byte sequence number of a request message. Example: 919c82d4-8046-4722-9094-35c3c6524cff

Response Parameters

Status code: 200

Table 4-367 Response body parameters

Parameter	Type	Description
key_id	String	CMK ID.
public_key	String	Public key info.

Status code: 400

Table 4-368 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-369 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 403

Table 4-370 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-371 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Status code: 404

Table 4-372 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-373 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Example Requests

```
{
  "key_id" : "0d0466b0-e727-4d9c-b35d-f84bb474a37f"
}
```

Example Responses

Status code: 200

Request processing succeeded.

```
{
  "key_id" : "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
  "public_key" : "-----BEGIN PUBLIC KEY-----\r\nMIICCgKCAgEA3RQAXXwya9k4zV1/
Q3AFr37GO8JgFobDKZioAklLQdgElHZ/uxmP\r\n4bveNHpY6OI0Okk/1Ov8oJf+9W10VqVxbzihWa5n/
RMN0720DzLV7KuH4YylCGDb\r\n3JH/+bMbhF2qRArrrKod0kR9rYHrdPkI7O5fYQQprZ3kWnPgrhDoDFC8ja
+OelOg\r\nn4MMOGGYA/DAOb0XyxPnGl26PnUtvvF7aZbMW5x/Yq2yAVFE1cjqLaH7/j1C8KYE\r
\naOSYtl2nOif28WoweFavXpgVsb/iICTfqgC91BtCSFC5pT8vqZCimfoHmJCAkZa5\r
\nZ8QIqkOOf9F6iMqqIz7pGKgQSUmoKKY9j6DK3OwXDOB5gKu0vyuz+gW3b4SZn+Xa\r
\nKkEN8ZpXsdQdEGpe4SwIzSVyUGYNBOCLrsydBcPR7jWgQ6gs56IJrV2pdAtmBwKd\r\n6l33z1tQ7+/
h3IrZxXuuej/fRRUMlbVcmhTS2l6vle7HXgZj/dWzPsLLg9MGHu0+\r\no9PRr+brxTbrf5e2Zdr1ad35X/
b86gx7Grg1sYPkly2aEI4fsnDGPgFrudG+Hzx/\r\nABHejYfJEI6P0SXCzB/oDMkjw6XKhTSojMzuncAP/AM
+0LVYQxQe750qkb3hjBT0\r\nq/HBl/
4zMXA03tMb9QySnLK63uo64JMJiBsEe7wPLhHB3VzBZk9SvvECAwEAAQ==\r\n-----END PUBLIC KEY-----\r\n"
}
```

Status code: 400

Invalid request parameters.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 403

Authentication failed.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status code: 404

The requested resource does not exist or is not found.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status Codes

Status Code	Description
200	Request processing succeeded.
400	Invalid request parameters.
403	Authentication failed.

Status Code	Description
404	The requested resource does not exist or is not found.

Error Codes

See **Error Codes**.

4.1.10.4 Querying the Number of Instances

Function

This API is used to query the number of instances, that is, the number of CMKs created."

Constraints

Default Master Keys are automatically created by services and are not included in this query.

URI

GET /v1.0/{project_id}/kms/user-instances

Table 4-374 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-375 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. The token can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Response Parameters

Status code: 200

Table 4-376 Response body parameters

Parameter	Type	Description
instance_num	Long	Number of non-default CMKs.

Status code: 403

Table 4-377 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-378 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Example Requests

None

Example Responses

Status code: 200

Request processing succeeded.

```
{
  "instance_num" : 15
}
```

Status code: 403

Authentication failed.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status Codes

Status Code	Description
200	Request processing succeeded.
403	Authentication failed.

Error Codes

See **Error Codes**.

4.1.10.5 Querying the Quota of a User

Function

This API is used to query the quota of a user, that is, the allocated total number of CMKs that can be created by a user and the number of CMKs that has been created by the user.

Constraints

The quota does not include Default Master Keys.

URI

GET /v1.0/{project_id}/kms/user-quotas

Table 4-379 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-380 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. The token can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Response Parameters

Status code: 200

Table 4-381 Response body parameters

Parameter	Type	Description
quotas	**Quotas** object	Quota details.

Table 4-382 Quotas

Parameter	Type	Description
resources	Array of **Resources** objects	Resource quota list.

Table 4-383 Resources

Parameter	Type	Description
type	String	Quota type. The value can be: ● CMK ● grant_per_CMK: maximum number of grants that can be created for a CMK
used	Integer	Used quotas.
quota	Integer	Total quotas.

Status code: 403

Table 4-384 Response body parameters

Parameter	Type	Description
error	Object	Error message.

Table 4-385 ErrorDetail

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error information.

Example Requests

None

Example Responses

Status code: 200

Request processing succeeded.

```
{
  "quotas" : {
    "resources" : [ {
      "quota" : 20,
      "used" : 20,
      "type" : "CMK"
    }, {
      "quota" : 100,
      "used" : 0,
      "type" : "grant_per_CMK"
    } ]
  }
}
```

Status code: 403

Authentication failed.

```
{
  "error" : {
    "error_code" : "KMS.XXX",
    "error_msg" : "XXX"
  }
}
```

Status Codes

Status Code	Description
200	Request processing succeeded.
403	Authentication failed.

Error Codes

See **Error Codes**.

5 Application Examples

5.1 Example 1: Encrypting or Decrypting Small Volumes of Data

Scenario

Encrypt or decrypt data not larger than 4 KB, such as passwords, certificates, and phone numbers, by using a tool on the console or calling an API. This section describes how to call a KMS API and use a CMK to encrypt or decrypt data.

Process:

1. Create a CMK in KMS.
2. Call the encrypt-data API of KMS to encrypt plaintext data by using a CMK.
3. Deploy ciphertext certificates on your servers.
4. When your servers need to use a certificate, they call the decrypt-data API of KMS to decrypt the ciphertext data and obtain the ciphertext certificate.

Operations

APIs are called to perform the following operations:

- **Create a CMK**
- **Encrypt a DEK**
- **Decrypt a DEK**

Procedure

Step 1 Create a CMK.

- API information

  URI format: POST /v1.0/*{project_id}*/kms/create-key

  For details, see **Creating a CMK**.

NOTE

Default Master Keys are created by services integrated with KMS. Names of Default Master Keys end with **/default**. Do not end your CMK names with **/default**.

- Example request

  POST: https://*{endpoint}*/v1.0/53d1aefc533f4ce9a59c26b01667cbcf/kms/create-key

  Body:

  ```
  {
     "key_alias": "test"
  }
  ```

- Example response

  ```
  {
     "key_info": {
        "key_id": "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
        "domain_id": "b168fe00ff56492495a7d22974df2d0b"
     }
  }
  ```

Step 2 Encrypt data.

- API information

  URI format: POST /v1.0/*{project_id}*/kms/encrypt-data

  For details, see **Encrypting Data**.

- Example request

  POST https://*{endpoint}*/v1.0/53d1aefc533f4ce9a59c26b01667cbcf/kms/encrypt-data

  You can use the API for **Querying the List of CMKs** to check key information, including key_id.

  Body:

  ```
  {
     "key_id": "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
     "plain_text": "12345678"
  }
  ```

- Example response

  ```
  {     "key_id": "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
      "cipher_text": "AgDoAG7EsEc2OHpQxz4gDFDH54CqwaelpTdEl
  +RFPjbKn5klPTvOywYIeZX60kPbFsYOpXJwkL32HUM50MY22Eb1fOSpZK7WJpYjx66EWOkJvO
  +Ey3r1dLdNAjrZrYzQlxRwNS05CaNKoX5rr3NoDnmv+UNobaiS25muLLiqOt6UrStaWow9AUyOHSzl
  +BrX2Vu0whv74djK
  +3COO6cXT2CBO6WajTJsOgYdxMfv24KWSKw0TqvHe8XDKASQGKdgfI74hzI1YWJlNjlmLWFlMTAtNDRjZ
  C1iYzg3LTFiZGExZGUzYjdkNwAAAACdcfNpLXwDUPH3023MvZK8RPHe129k6VdNIi3zNb0eFQ=="
  }
  ```

Step 3 Decrypt data.

- API information

  URI format: POST /v1.0/*{project_id}*/kms/decrypt-data

  For details, see **Decrypting Data**.

- Example request

  POST https://*{endpoint}*/v1.0/53d1aefc533f4ce9a59c26b01667cbcf/kms/decrypt-data

  You can use the API for **Querying the List of CMKs** to check key information, including key_id.

Body:

```
{      "cipher_text": "AgDoAG7EsEc2OHpQxz4gDFDH54CqwaelpTdEl
+RFPjbKn5klPTvOywYIeZX60kPbFsYOpXJwkL32HUM50MY22Eb1fOSpZK7WJpYjx66EWOkJvO
+Ey3r1dLdNAjrZrYzQlxRwNS05CaNKoX5rr3NoDnmv+UNobaiS25muLLiqOt6UrStaWow9AUyOHSzl
+BrX2Vu0whv74djK
+3COO6cXT2CBO6WajTJsOgYdxMfv24KWSKw0TqvHe8XDKASQGKdgfI74hzI1YWJlNjlmLWFlMTAtNDRjZ
C1iYzg3LTFiZGExZGUzYjdkNwAAAACdcfNpLXwDUPH3023MvZK8RPHe129k6VdNIi3zNb0eFQ=="
 }
```

- Example response

```
{
    "key_id": "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
     "plain_text": "12345678"
 }
```

----End

5.2 Example 2: Encrypting or Decrypting Large Volumes of Data

Scenario

Encrypt or decrypt a large amount of data.

- Encryption process:
  a. Create a CMK in KMS.
  b. Call the create-datakey API of the KMS to create a DEK. A plaintext DEK and a ciphertext DEK will be generated. The ciphertext DEK was generated by using a CMK to encrypt the plaintext DEK.
  c. Use the plaintext DEK to encrypt a plaintext file, generating a ciphertext file.
  d. Store the ciphertext DEK and the ciphertext file together in a permanent storage device or a storage service.
- Decryption process:
  a. Read the ciphertext DEK and the ciphertext file from the permanent storage device or storage service.
  b. Call the decrypt-datakey API and use the encryption CMK to decrypt the ciphertext DEK. The plaintext DEK will be generated.

     If the CMK is deleted, the decryption will fail. Properly keep your CMKs.
  c. Use the plaintext DEK to decrypt the ciphertext file.

Involved APIs

APIs used for the following operations are involved:

- **Create a CMK**
- **Create a DEK**
- **Encrypt a DEK**
- **Decrypt a DEK**

Procedure

Step 1 Create a CMK.

- API information

  URI format: POST /v1.0/*{project_id}*/kms/create-key

  For details, see **Creating a CMK**.

  NOTE

  Default Master Keys are created by services integrated with KMS. Names of Default Master Keys end with **/default**. Do not end your CMK names with **/default**.

- Example request

  POST: https://*{endpoint}*/v1.0/53d1aefc533f4ce9a59c26b01667cbcf/kms/create-key

  Body:

```
{
   "key_alias": "test"
}
```

- Example response

```
{
   "key_info": {
      "key_id": "bb6a3d22-dc93-47ac-b5bd-88df7ad35f1e",
      "domain_id": "b168fe00ff56492495a7d22974df2d0b"
   }
}
```

Step 2 Create a DEK.

- API information

  URI format: POST /v1.0/*{project_id}*/kms/create-datakey

  For details, see **Creating a DEK**.

- Example request

  POST https://*{endpoint}*/v1.0/53d1aefc533f4ce9a59c26b01667cbcf/kms/create-datakey

  You can use the API for **Querying the List of CMKs** to check key information, including key_id.

  Body:

```
{
   "key_id": "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
   "datakey_length": "512"
}
```

- Example response

```
{
   "key_id": "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
   "plain_text": 
"8151014275E426C72EE7D44267EF11590DCE0089E19863BA8CC832187B156A72A5A17F17B5EF0D525
872C59ECEB72948AF85E18427F8BE0D46545C979306C08D",
   "cipher_text": 
"020098009EEAFCE122CAA5927D2E020086F9548BA1675FDB022E4ECC01B96F2189CF4B85E78357E73
E1CEB518DAF7A4960E7C7DE8885ED3FB2F1471ABF400119CC1B20BD3C4A9B80AF590EFD0AEDABFDB
B0E2B689DA7B6C9E7D3C5645FCD9274802586BE63779471F9156F2CDF07CD8412FFBE923064303436
3662302D653732372D346439632D623335642D6638346262343734613376600000000045B05321483B
D9F9561865EE7DFE9BE267A42EB104E98C16589CE46940B18E52"
}
```

Step 3 Encrypt the DEK.

- API information

  URI format: POST /v1.0/*{project_id}*/kms/encrypt-datakey

  For details, see **Creating a DEK**.

- Example request

  POST https://*{endpoint}*/v1.0/53d1aefc533f4ce9a59c26b01667cbcf/kms/encrypt-datakey

  You can use the API for **Querying the List of CMKs** to check key information, including key_id.

  Body:

```
{
    "key_id": "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
    "plain_text": 
"00000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000F5A5FD42D16A20302798EF6ED309979B43003
D2320D9F0E8EA9831A92759FB4B",
    "datakey_plain_length": "64"
}
```

- Example response

```
{
    "key_id": "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
    "cipher_text": 
"020098005273E14E6E8E95F5463BECDC27E80AF820B9FC086CB47861899149F67CF07DAFF2810B7D2
7BDF19AB7632488E0926A48DB2FC85BEA905119411B46244C5E6B8036C60A0B0B4842FFE6994518E89
C19B1C1D688D9043BCD6053EA7BA0652642CE59F2543C80669139F4F71ABB9BD9A243306430343636
62302D653732372D346439632D623335642D663834626234373461333766000000000D34457984F9730
D57F228C210FD22CA6017913964B21D4ECE45D81092BB9112E",
    "datakey_length": "64"
}
```

Step 4 Decrypt the DEK.

- API information

  URI format: POST /v1.0/*{project_id}*/kms/decrypt-datakey

  For details, see **Decrypting a DEK**.

- Example request

  POST https://*{endpoint}*/v1.0/53d1aefc533f4ce9a59c26b01667cbcf/kms/decrypt-datakey

  You can use the API for **Querying the List of CMKs** to check key information, including key_id.

  Body:

```
{
    "key_id": "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
    "datakey_cipher_length": "64",
    "cipher_text": 
"020098005273E14E6E8E95F5463BECDC27E80AF820B9FC086CB47861899149F67CF07DAFF2810B7D2
7BDF19AB7632488E0926A48DB2FC85BEA905119411B46244C5E6B8036C60A0B0B4842FFE6994518E89
C19B1C1D688D9043BCD6053EA7BA0652642CE59F2543C80669139F4F71ABB9BD9A243306430343636
62302D653732372D346439632D623335642D663834626234373461333766000000000D34457984F9730
D57F228C210FD22CA6017913964B21D4ECE45D81092BB9112E"
}
```

- Example response

```
{
    "data_key": 
"00000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000",
    "datakey_length": "64",
   "datakey_dgst": "F5A5FD42D16A20302798EF6ED309979B43003D2320D9F0E8EA9831A92759FB4B"
}
```

----End

5.3 Example 3: Querying Information About Keys

Scenario

Use KMS APIs to obtain the list of keys, key information, key instances, and key tags.

Involved APIs

- **Query key list**
- **Query key information**
- **Query key instance**
- **Query key tags** Tag Management Service (TMS) needs to query all the tags of a specified CMK.

Procedure

Step 1 Query the list of keys.

- API information

  URI format: POST /v1.0/*{project_id}*/kms/list-keys

  For details, see "Querying Key List".

- Example request

  POST: https://*{endpoint}*/v1.0/53d1aefc533f4ce9a59c26b01667cbcf/kms/list-keys

  Body:

```
{
  "limit": "2",
   "marker": "1"
 }
```

- Example response

```
{
   "keys": [
        "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
       "2e258389-bb1e-4568-a1d5-e1f50adf70ea"
    ],
    "key_details": [
    {
     "key_id":"0d0466b0-e727-4d9c-b35d-f84bb474a37f",
      "domain_id":"00074811d5c27c4f8d48bb91e4a1dcfd",
        "key_alias":"caseuirpr",
        "realm":"aaaa",
        "key_description":"123",
       "creation_date":"1502799822000",
        "scheduled_deletion_date":"",
        "key_state":"2",
        "default_key_flag":"0",
        "key_type":"1",
        "expiration_time":"1501578672000",
        "origin":"kms"
 },
       {
     "key_id":"2e258389-bb1e-4568-a1d5-e1f50adf70ea",
      "domain_id":"00074811d5c27c4f8d48bb91e4a1dcfd",
      "key_alias":"casehvniz",
       "realm":"aaaa",
     "key_description":"234",
       "creation_date":"1502799820000",
        "scheduled_deletion_date":"",
        "key_state":"2",
        "default_key_flag":"0",
        "key_type":"1",
       "expiration_time":"1501578673000",
        "origin":"kms"
 }
     ],
    "next_marker": "",
   "truncated": "false",
    "total":2
}
```

Step 2 Query the information about keys.

- API information

  URI format: POST /v1.0/*{project_id}*/kms/describe-key

  For details, see "Querying Key Details".

- Example request

  POST: https://*{endpoint}*/v1.0/53d1aefc533f4ce9a59c26b01667cbcf/kms/describe-key

  You can use the API for **Querying the List of CMKs** to check key information, including key_id.

  Body:

```
{
   "key_id": "0d0466b0-e727-4d9c-b35d-f84bb474a37f"
}
```

- Example response

```
{
    "key_info": {
        "key_id": "0d0466b0-e727-4d9c-b35d-f84bb474a37f",
        "domain_id": "b168fe00ff56492495a7d22974df2d0b",
        "key_alias": "kms_test",
        "realm": "aaa",
         "key_description": "",
       "creation_date": "1472442386000",
        "scheduled_deletion_date": "",
        "key_state": "2",
        "default_key_flag": "0",
        "key_type": "1",
        "expiration_time":"1501578672000",
        "origin":"kms",
        "key_rotation_enabled":"false",
        "sys_enterprise_project_id ": "0",
     }
 }
```

Step 3 Query CMK instances.

- API information

  URI format: POST /v1.0/*{project_id}*/kms/resource_instances/action

  For details, see "Querying Key Instances".

- Example request

  POST: https://*{endpoint}*/v1.0/53d1aefc533f4ce9a59c26b01667cbcf/kms//resource_instances/action

Body:

```
 {
      "offset": "100",
      "limit": "100",
      "action": "filter",
        "matches":[
    {
           "key": "resource_name",
              "value": "resource1"
         }
      ],
      "tags": [
          {
          "key": "key1",
             "values": [
                    "value1",
                      "value2"
             ]
          }
    ]
 }
```

- Example response

```
{
  "resources" : [ {
    "resource_id" : "90c03e67-5534-4ed0-acfa-89780e47a535",
    "resource_detail" : [ {
      "key_id" : "90c03e67-5534-4ed0-acfa-89780e47a535",
      "domain_id" : "4B688Fb77412Aee5570E7ecdbeB5afdc",
      "key_alias" : "tagTest_xmdmi",
      "key_description" : "123",
      "creation_date" : 1521449277000,
      "scheduled_deletion_date" : "",
      "key_state" : 2,
      "default_key_flag" : 0,
      "key_type" : 1,
      "key_rotation_enabled" : false,
      "expiration_time" : "",
      "origin" : "kms",
      "sys_enterprise_project_id" : "0",
      "realm" :  "cn-hongkong-7"
    } ],
    "resource_name" : "tagTest_xmdmi",
    "tags" : [ {
      "key" : "key",
      "value" : "testValue!"
    }, {
      "key" : "haha",
      "value" : "testValue"
    } ]
  } ],
  "total_count" : 1
}
```

Step 4 Query the tags of a key.

- API information

  URI format: GET /v1.0/{project_id}/kms/{key_id}/tags

  For details, see "Querying Key Tags".

- Example request

  GET: https://*{endpoint}*/v1.0/53d1aefc533f4ce9a59c26b01667cbcf/kms/94752282-805e-4032-ada8-34966f70e02f/tags

  Body:

  None

- Example response

```
{
        "tags": [
         {
          "key": "key1",
          "value": "value1"
           },
           {
           "key": "key2",
           "value": "value3"
           }
           ],
           "existTagsNum":2
}
```

----End

6 Permissions Policies and Supported Actions

6.1 Introduction

This chapter describes fine-grained permissions management for your DEW. If your Huawei Cloud account does not need individual IAM users, you may skip over this chapter.

By default, new IAM users do not have permissions assigned. You need to add a user to one or more groups, and attach permissions policies or roles to these groups. Users inherit permissions from the groups to which they are added and can perform specified operations on cloud services based on the permissions.

Permissions are classified into **roles** and **policies** based on the authorization granularity. Roles are a type of coarse-grained authorization mechanism that defines permissions related to user responsibilities. Policies define API-based permissions for operations on specific resources under certain conditions, allowing for more fine-grained, secure access control of cloud resources.

NOTE

Policy-based authorization is useful if you want to allow or deny the access to an API.

An account has all of the permissions required to call all APIs, but IAM users must have the required permissions specifically assigned. The permissions required for calling an API are determined by the actions supported by the API. Only users who have been granted permissions allowing the actions can call the API successfully. For example, if an IAM user wants to use an API to query the SSH keys of account key pairs, the user must be granted permissions that allow the **kps:domainKeypairs:list** action.

Supported Actions

DEW provides system-defined policies that can be directly used in IAM. You can also create custom policies and use them to supplement system-defined policies, implementing more refined access control. Operations supported by policies are specific to APIs. The following are common concepts related to policies:

- Permission: A statement in a policy that allows or denies certain operations.
- APIs: REST APIs that can be called in a custom policy.
- Actions: Added to a custom policy to control permissions for specific operations.
- Dependent actions: When assigning an action to users, you also need to assign dependent permissions for that action to take effect.
- IAM projects or enterprise project: Scope of users a permission is granted to. Policies that contain actions supporting both IAM and enterprise projects can be assigned to user groups and take effect in both IAM and Enterprise Management. Policies that only contain actions supporting IAM projects can be assigned to user groups and only take effect in IAM. Such policies will not take effect if they are assigned to user groups in Enterprise Project.

DEW supports the following actions that can be defined in custom policies:

- **Manage keys**, such as creating keys, querying keys, and creating grants.
- Manage key pairs, such as creating, querying, and deleting key pairs.

6.2 Encryption Key Management

Permission	API	Action	Dependent Permission	IAM Project (Project)	Enterprise Project (Enterprise Project)
Creating a CMK	POST /v1.0/{project_id}/kms/create-key	kms:cmk:create	-	√	√
Enabling a CMK	POST /v1.0/{project_id}/kms/enable-key	kms:cmk:enable	-	√	√
Disabling a CMK	POST /v1.0/{project_id}/kms/disable-key	kms:cmk:disable	-	√	√
Scheduling the deletion of a CMK	POST /v1.0/{project_id}/kms/schedule-key-deletion	kms:cmk:update	-	√	√
Canceling the scheduled deletion of a CMK	POST /v1.0/{project_id}/kms/cancel-key-deletion	kms:cmk:update	-	√	√

Permission	API	Action	Dependent Permission	IAM Project (Project)	Enterprise Project (Enterprise Project)
Querying the list of CMKs	POST /v1.0/{project_id}/kms/list-keys	kms:cmk:list	-	√	√
Queries the CMK information.	POST /v1.0/{project_id}/kms/describe-key	kms:cmk:get	-	√	√
Generating a random number	POST /v1.0/{project_id}/kms/gen-random	kms:cmk:generate	-	√	√
Creating a DEK	POST /v1.0/{project_id}/kms/create-datakey	kms:dek:create	-	√	√
Creating a plaintext-free DEK	POST /v1.0/{project_id}/kms/create-datakey-without-plaintext	kms:dek:create	-	√	√
Encrypting a DEK	POST /v1.0/{project_id}/kms/encrypt-datakey	kms:dek:crypto	-	√	√
Decrypting a DEK	POST /v1.0/{project_id}/kms/decrypt-datakey	kms:dek:crypto	-	√	√
Querying the number of instances	GET /v1.0/{project_id}/kms/user-instances	kms:cmk:getInstance	-	√	√
Querying the user quota	GET /v1.0/{project_id}/kms/user-quotas	kms:cmk:getQuota	-	√	√
Modifying the CMK alias	POST /v1.0/{project_id}/kms/update-key-alias	kms:cmk:update	-	√	√

Permission	API	Action	Dependent Permission	IAM Project (Project)	Enterprise Project (Enterprise Project)
Modifying the description of a CMK	POST /v1.0/{project_id}/kms/update-key-description	kms:cmk:update	-	√	√
Creating a grant	POST /v1.0/{project_id}/kms/create-grant	kms:grant:create	-	√	√
Revoking a grant	POST /v1.0/{project_id}/kms/revoke-grant	kms:grant:revoke	-	√	√
Retiring a grant	POST /v1.0/{project_id}/kms/retire-grant	kms:grant:retire	-	√	√
Querying the grant list of a CMK	POST /v1.0/{project_id}/kms/list-grants	kms:grant:list	-	√	√
Querying the list of grants that can be retired	POST /v1.0/{project_id}/kms/list-retirable-grants	kms:grant:list	-	√	√
Encrypting data	POST /v1.0/{project_id}/kms/encrypt-data	kms:cmk:crypto	-	√	√
Decrypting data	POST /v1.0/{project_id}/kms/decrypt-data	kms:cmk:crypto	-	√	√
Obtaining parameters for importing a key	POST /v1.0/{project_id}/kms/get-parameters-for-import	kms:cmk:getMaterial	-	√	√
Importing key material	POST /v1.0/{project_id}/kms/import-key-material	kms:cmk:importMaterial	-	√	√

Permission	API	Action	Dependent Permission	IAM Project (Project)	Enterprise Project (Enterprise Project)
Deleting key material	POST /v1.0/{project_id}/kms/delete-imported-key-material	kms:cmk:deleteMaterial	-	√	√
Enabling key rotation	POST /v1.0/{project_id}/kms/enable-key-rotation	kms:cmk:enableRotation	-	√	√
Modifying the rotation interval	POST /v1.0/{project_id}/kms/update-key-rotation-interval	kms:cmk:updateRotation	-	√	√
Disabling key rotation	POST /v1.0/{project_id}/kms/disable-key-rotation	kms:cmk:disableRotation	-	√	√
Querying the key rotation status	POST /v1.0/{project_id}/kms/get-key-rotation-status	kms:cmk:getRotation	-	√	√
Querying key resource instances	POST /v1.0/{project_id}/kms/resource_instances/action	kms:cmkTag:listInstance	-	√	√
Querying tags of a key	GET /v1.0/{project_id}/kms/{key_id}/tags	kms:cmkTag:list	-	√	√
Querying the project tags	GET /v1.0/{project_id}/kms/tags	kms:cmkTag:list	-	√	√
Adding or deleting key tags in batches	POST /v1.0/{project_id}/kms/{key_id}/tags/action	kms:cmkTag:batch	-	√	√
Adding tags to a key	POST /v1.0/{project_id}/kms/{key_id}/tags	kms:cmkTag:create	-	√	√

Permission	API	Action	Dependent Permission	IAM Project (Project)	Enterprise Project (Enterprise Project)
Deleting tags of a key	POST /v1.0/{project_id}/kms/{key_id}/tags/{key}	kms:cmkTag:delete	-	√	√

A Appendix

A.1 Status Codes

Status Code	Status	Description
200	OK	Request processed successfully.
202	Accept	The job was successfully delivered. However, it will be postponed because the system is busy currently.
204	No Content	The request is processed successfully and no content is returned.
300	multiple choices	The requested resource has multiple available responses.
400	Bad Request	The request parameter is incorrect.
401	Unauthorized	You need to enter the username and password to access the requested page.
403	Forbidden	The server understood the request, but is refusing to fulfill it.
404	Not Found	The requested resource does not exist or not found.
405	Method Not Allowed	The method specified in the request is not allowed.
406	Not Acceptable	The response generated by the server cannot be accepted by the client.
407	Proxy Authentication Required	You must use the proxy server for authentication. Then, the request can be processed.

Status Code	Status	Description
408	Request Timeout	The request timed out.
409	Conflict	The request cannot be processed due to a conflict.
500	Internal Server Error	Internal service error.
501	Not Implemented	Failed to complete the request. The server does not support the requested function.
502	Bad Gateway	Failed to complete the request, because the server receives an invalid request.
503	Service Unavailable	Failed to complete the request due to system exception.
504	Gateway Timeout	A gateway timeout error occurs.

A.2 Error Code

Status Code	Error Code	Message	Description	Measure
400	KMS.0201	Invalid request URL.	Invalid request URL.	Enter a valid URL.
400	KMS.0202	Invalid JSON format of the request message.	Invalid JSON format of the request message.	Enter a valid message.
400	KMS.0203	Request message too long.	Request message too long.	Enter a valid message.
400	KMS.0204	Parameters missing in the request message.	Parameters missing in the request message.	Enter a valid message.
400	KMS.0205	Invalid key ID.	Invalid key ID.	Enter a valid key ID.
400	KMS.0206	Invalid sequence number.	Invalid sequence number.	Enter a valid sequence number.

Status Code	Error Code	Message	Description	Measure
400	KMS.0208	Invalid value of value encryption_context.	Invalid value of value encryption_context.	Enter a valid value of encryption_context.
400	KMS.0209	The key has been disabled.	The key has been disabled.	Enable the key.
400	KMS.0210	The key is in Scheduled deletion state and cannot be used.	The key is in Scheduled deletion state and cannot be used.	Enable the key.
400	KMS.0211	Cannot perform this operation on Default Master Keys.	Cannot perform this operation on default master keys.	Perform this operation on a common CMK.
400	KMS.0308	Invalid parameter.	Invalid parameter.	Enter valid parameters.
400	KMS.0309	External keys required.	External keys required.	Use an imported key.
400	KMS.0310	The key is not in Pending import state.	The key is not in Pending import state.	Ensure the key is in Pending import state.
400	KMS.0311	Failed to decrypt data using the RSA private key.	Failed to decrypt data using the RSA private key.	Ensure the input ciphertext is correct and try again, or contact customer service.
400	KMS.0312	External keys cannot be rotated.	External keys cannot be rotated.	Use a common CMK.
400	KMS.0313	Key rotation is not enabled.	Key rotation is not enabled.	Enable key rotation.
400	KMS.0319	Rotation not supported in the current KMS version.	Rotation not supported in the current KMS version.	Try again later or contact customer service.
400	KMS.0320	Resource frozen.	Resource frozen.	Renew the service and try again.

Status Code	Error Code	Message	Description	Measure
400	KMS.0323	Failed to obtain the partition of the key.	Failed to obtain the partition of the key.	Try again later or contact customer service.
400	KMS.0324	RSA keys cannot be rotated.	RSA keys cannot be rotated.	Use a common CMK.
400	KMS.0327	Failed to obtain user permissions.	Failed to obtain user permissions.	Contact the administrator to grant required permissions.
400	KMS.0329	Hash algorithm does not match the digest length.	Hash algorithm does not match the digest length.	Enter valid parameters or contact customer service.
400	KMS.0401	Tag list cannot be empty.	Tag list cannot be empty.	Enter valid parameters.
400	KMS.0402	Invalid match value.	Invalid match value.	Enter valid parameters.
400	KMS.0403	Invalid match key.	Invalid match key.	Enter valid parameters.
400	KMS.0201	Invalid request URL.	Invalid request URL.	Enter a valid URL.
400	KMS.0202	Invalid JSON format of the request message.	Invalid JSON format of the request message.	Enter a valid message.
400	KMS.0203	Request message too long.	Request message too long.	Enter a valid message.
400	KMS.0204	Parameters missing in the request message.	Parameters missing in the request message.	Enter a valid message.
400	KMS.0205	Invalid key ID.	Invalid key ID.	Enter a valid key ID.
400	KMS.0206	Invalid sequence number.	Invalid sequence number.	Enter a valid sequence number.

Status Code	Error Code	Message	Description	Measure
400	KMS.0208	Invalid value of value encryption_context.	Invalid value of value encryption_context.	Enter a valid value of encryption_context.
400	KMS.0209	The key has been disabled.	The key has been disabled.	Enable the key.
400	KMS.0210	The key is in Scheduled deletion state and cannot be used.	The key is in Pending deletion state and cannot be used.	Enable the key.
400	KMS.0211	Cannot perform this operation on Default Master Keys.	Cannot perform this operation on default master keys.	Perform this operation on a common CMK.
400	KMS.0308	Invalid parameter.	Invalid parameter.	Enter valid parameters.
400	KMS.0309	External keys required.	External keys required.	Use an imported key.
400	KMS.0310	The key is not in Pending import state.	The key is not in Pending import state.	Ensure the key is in Pending import state.
400	KMS.0311	Failed to decrypt data using the RSA private key.	Failed to decrypt data using the RSA private key.	Ensure the input ciphertext is correct and try again, or contact customer service.
400	KMS.0312	External keys cannot be rotated.	External keys cannot be rotated.	Use a common CMK.
400	KMS.0313	Key rotation is not enabled.	Key rotation is not enabled.	Enable key rotation.
400	KMS.0319	Rotation not supported in the current KMS version.	Rotation not supported in the current KMS version.	Try again later or contact customer service.
400	KMS.0320	Resource frozen.	Resource frozen.	Renew the service and try again.

Status Code	Error Code	Message	Description	Measure
400	KMS.0323	Failed to obtain the partition of the key.	Failed to obtain the partition of the key.	Try again later or contact customer service.
400	KMS.0324	RSA keys cannot be rotated.	RSA keys cannot be rotated.	Use a common CMK.
400	KMS.0327	Failed to obtain user permissions.	Failed to obtain user permissions.	Contact the administrator to grant required permissions.
400	KMS.0329	Hash algorithm does not match the digest length.	Hash algorithm does not match the digest length.	Enter valid parameters or contact customer service.
400	KMS.0401	Tag list cannot be empty.	Tag list cannot be empty.	Enter valid parameters.
400	KMS.0402	Invalid match value.	Invalid match value.	Enter valid parameters.
400	KMS.0403	Invalid match key.	Invalid match key.	Enter valid parameters.
400	KMS.0404	Invalid action.	Invalid action.	Enter valid parameters.
400	KMS.0405	Invalid tag value.	Invalid tag value.	Enter valid parameters.
400	KMS.0406	Invalid tag key.	Invalid tag key.	Enter valid parameters.
400	KMS.0407	Invalid tag list size.	Invalid tag list size.	Enter valid parameters.
400	KMS.0408	Invalid resourceType.	Invalid resourceType.	Enter valid parameters.
400	KMS.0409	Too many tags.	Too many tags.	Delete unnecessary tags and try again.
400	KMS.0410	Invalid tag value length.	Invalid tag value length.	Enter valid parameters.
400	KMS.0411	Invalid tag key length.	Invalid tag key length.	Enter valid parameters.

Status Code	Error Code	Message	Description	Measure
400	KMS.0412	Invalid tag list.	Invalid tag list.	Enter valid parameters.
400	KMS.0413	Too many tag values.	Too many tag values.	Enter valid parameters.
400	KMS.0414	Invalid tags.	Invalid tags.	Enter valid parameters.
400	KMS.0415	Invalid matches.	Invalid matches.	Enter valid parameters.
400	KMS.0417	Invalid offset.	Invalid offset.	Enter valid parameters.
400	KMS.1101	Invalid key_alias.	Invalid key_alias.	Enter valid parameters.
400	KMS.1102	Invalid realm.	Invalid realm.	Enter valid parameters.
400	KMS.1103	Invalid key_description.	Invalid key_description.	Enter valid parameters.
400	KMS.1104	Duplicate key aliases.	Duplicate key aliases.	Use another alias.
400	KMS.1105	Too many keys.	Too many keys.	Increase key quota or delete unnecessary keys.
400	KMS.1108	Failed to create the default partition for the key.	Failed to create the default partition for the key.	Try again later or contact customer service.
400	KMS.1109	Failed to create the route for the key.	Failed to create the route for the key.	Try again later or contact customer service.
400	KMS.1201	The key is not disabled.	The key is not disabled.	Disable the key.
400	KMS.1301	The key is not enabled.	The key is not enabled.	Enable the key.

Status Code	Error Code	Message	Description	Measure
400	KMS.1401	Set the pending deletion period between 7 to 1096 days.	Set the pending deletion period between 7 to 1096 days.	Enter valid parameters.
400	KMS.1402	The key is already in Pending deletion state.	The key is already in Pending deletion state.	No further operation required.
400	KMS.1501	The key is not in Pending deletion state.	The key is not in Pending deletion state.	Schedule deletion the key.
400	KMS.1601	Invalid limit.	Invalid limit.	Enter valid parameters.
400	KMS.1602	marker must be greater than or equals 0.	marker must be greater than or equals 0.	Enter valid parameters.
400	KMS.1801	random_data_length must be 512 bits.	random_data_length must be 512 bits.	Enter valid parameters.
400	KMS.1802	random_data_length must be a multiple of 8.	random_data_length must be a multiple of 8.	Enter valid parameters.
400	KMS.1901	datakey_length must be in the range 8 bits to 8,192 bits.	datakey_length must be in the range 8 bits to 8,192 bits.	Enter valid parameters.
400	KMS.1902	key_spec can only be AES_128 or AES_256.	key_spec can only be AES_128 or AES_256.	Enter valid parameters.
400	KMS.1903	datakey_length must be a multiple of 8.	datakey_length must be a multiple of 8.	Enter valid parameters.
400	KMS.2001	datakey_length must be 512 bits.	datakey_length must be 512 bits.	Enter valid parameters.

Status Code	Error Code	Message	Description	Measure
400	KMS.2101	Invalid plain_text.	Invalid plain_text.	Enter valid parameters.
400	KMS.2102	datakey_plain_length must be 64 bytes.	datakey_plain_length must be 64 bytes.	Enter valid parameters.
400	KMS.2103	Failed to verify the DEK hash.	Failed to verify the DEK hash.	Ensure the DEK is valid and try again, or contact customer service.
400	KMS.2104	The length of plain_text does not match datakey_plain_length.	The length of plain_text does not match datakey_plain_length.	Enter valid parameters.
400	KMS.2201	Invalid cipher_text.	invalid cipher_text.	Enter valid parameters.
400	KMS.2202	datakey_cipher_length must be 64 bytes.	datakey_cipher_length must be 64 bytes.	Enter valid parameters.
400	KMS.2203	Failed to verify the DEK hash.	Failed to verify the DEK hash.	Ensure the DEK is valid and try again, or contact customer service.
400	KMS.2204	The length of cipher_text does not match datakey_cipher_length.	The length of cipher_text does not match datakey_cipher_length.	Enter valid parameters.
400	KMS.2401	Specify an operation in addition to create-grant.	Specify an operation in addition to create-grant.	Enter valid parameters.
400	KMS.2402	Invalid user ID.	Invalid user ID.	Enter valid parameters.
400	KMS.2403	Failed to create the grant.	Failed to create the grant.	Try again later or contact customer service.

Status Code	Error Code	Message	Description	Measure
400	KMS.2404	Too many CMK grants.	Too many CMK grants.	Increase grant quota or delete unnecessary grants.
400	KMS.2405	Too many grants.	Too many grants.	Increase grant quota or delete unnecessary grants.
400	KMS.2501	Invalid grant ID.	Invalid grant ID.	Enter a valid grant ID.
400	KMS.2502	grant_id and key_id do not match.	grant_id and key_id do not match.	Ensure input grant_id matches key_id.
400	KMS.2601	Token expired.	Token expired.	Obtain a new token.
400	KMS.2602	Key expiration time must be later than the current time.	Key expiration time must be later than the current time.	Set a valid key expiration time.
400	KMS.2603	Key IDs in the imported key and token do not match.	Key IDs in the imported key and token do not match.	Ensure the key ID in the imported key matches that in the token.
400	KMS.2604	The external key plaintext length must be 32 bits.	The external key plaintext length must be 32 bits.	Enter valid parameters.
400	KMS.2605	Token verification failed.	Token verification failed.	Obtain a new token.
400	KMS.2606	You are importing a deleted key again. The imported plaintext must be the same as the deleted key plaintext.	You are importing a deleted key again. The imported plaintext must be the same as the deleted key plaintext.	Ensure the plaintext of the imported key is the same as that of the deleted key.

Status Code	Error Code	Message	Description	Measure
400	KMS.2701	Key material is not in Enabled or Disabled state and cannot be deleted.	Key material is not in Enabled or Disabled state and cannot be deleted.	Ensure that the key is in Enabled or Disabled state.
400	KMS.2901	Key rotation is not disabled.	Key rotation is not disabled.	Disable key rotation.
400	KMS.3001	Invalid rotation_interval.	Invalid rotation_interval.	Enter valid parameters.
403	KMS.0301	Invalid or null X-Auth-Token.	Invalid or null X-Auth-Token.	Obtain the token again and ensure the token string is complete.
403	KMS.0302	Invalid X-Auth-Token.	Invalid X-Auth-Token.	Obtain the token again and ensure the token string is complete.
403	KMS.0303	X-Auth-Token expired.	X-Auth-Token expired.	Obtain the token again and ensure the token string is complete.
403	KMS.0304	X-Auth-Token contains the OBT tag and cannot be used to access services.	X-Auth-Token contains the OBT tag and cannot be used to access services.	Obtain the token again and ensure the token string is complete.
403	KMS.0305	Invalid X-Auth-Token project name.	Invalid X-Auth-Token project name.	Obtain the token again and ensure the token string is complete.
403	KMS.0306	No access permissions.	The user has no permission to access the key.	Contact the administrator to grant required permissions.
403	KMS.0307	No access permissions.	No access permissions.	Contact the administrator to grant required permissions.

Status Code	Error Code	Message	Description	Measure
403	KMS.0314	Real-name authentication is required to access the API.	Real-name authentication is required to access the API.	Complete real-name authentication and try again.
403	KMS.0321	URIs in URL and X-Auth-Token do not match.	URIs in URL and X-Auth-Token do not match.	Ensure the URI in the URL matches that in X-Auth-Token.
403	KMS.0326	No access permissions.	No access permissions.	Contact the administrator to grant required permissions.
403	KMS.0328	KMS has been frozen. Renew it and try again.	KMS has been frozen. Renew it and try again.	Renew the service and try again.
404	KMS.0207	The key does not exist.	The key does not exist.	Choose a valid key or create a key.
404	KMS.0416	Invalid tag ID.	Invalid tag ID.	Enter a valid key tag.
500	KMS.0101	KMS error.	KMS error.	Try again later or contact customer service.
500	KMS.0102	Abnormal KMS I/O.	Abnormal KMS I/O.	Try again later or contact customer service.
400	KPS.0001	taskId is illegal.	Invalid task ID.	Use a valid task ID.
400	KPS.0002	parameter error.	Parameter error.	Use correct parameters.
400	KPS.0005	Failed task is not found.	Incorrect task ID.	Enter the correct task ID.
400	KPS.0006	User not found.	Incorrect username.	Enter the correct username.
400	KPS.4016	The key pair is not exist.	Incorrect key pair name.	Enter a correct key pair name.
400	KPS.6004	No Keypair find.	The key pair is not found.	Enter a correct key pair name.

Status Code	Error Code	Message	Description	Measure
400	KPS.6005	No private key managed.	The managed private key is not found.	Check whether the private key is managed in the cloud.
400	KPS.6008	Encrypt private key failed.	Failed to encrypt the private key.	Check whether the KMS key exists and is available.
400	KPS.6010	Save privatekey failed.	Failed to save the private key.	Check whether the KMS key exists and is available.
400	KPS.6011	The imported private key not match public key.	The imported private key does not match the public key.	Check whether the imported public and private key match.
401	KPS.9001	The token of the request is not or failed to be authenticated.	The token is invalid.	Use a valid token.
401	KPS.9002	Public test service denied.	Access failed.	Use a non-OBT account.
403	KPS.6009	Keypair verify failed.	Failed to verify the key pair.	Use the correct management verification code.
403	KPS.9003	No operation permission.	No access permission.	Add the required permissions for the user.
403	KPS.9004	The account is frozen.	The account is frozen.	The account is frozen.
403	KPS.9005	The account is restricted.	The account is restricted.	The account is restricted.
403	KPS.9006	Unknown user type.	The account does not have sufficient permissions.	Add the required permissions for the user.

A.3 Obtaining a Project ID

Obtaining a Project ID by Calling an API

You can obtain the project ID by calling the API used to **query project information**.

The API used to obtain a project ID is GET https://{Endpoint}/v3/projects. **{Endpoint}** is the IAM endpoint For details about API authentication, see **Authentication**.

In the following example, **id** indicates the project ID.

```
{
    "projects": [
        {
            "domain_id": "65382450e8f64ac0870cd180d14e684b",
            "is_domain": false,
            "parent_id": "65382450e8f64ac0870cd180d14e684b",
            "name": "xxxxxxxx",
            "description": "",
            "links": {
                "next": null,
                "previous": null,
                "self": "https://www.example.com/v3/projects/a4a5d4098fb4474fa22cd05f897d6b99"
            },
            "id": "a4a5d4098fb4474fa22cd05f897d6b99",
            "enabled": true
        }
    ],
    "links": {
        "next": null,
        "previous": null,
        "self": "https://www.example.com/v3/projects"
    }
}
```

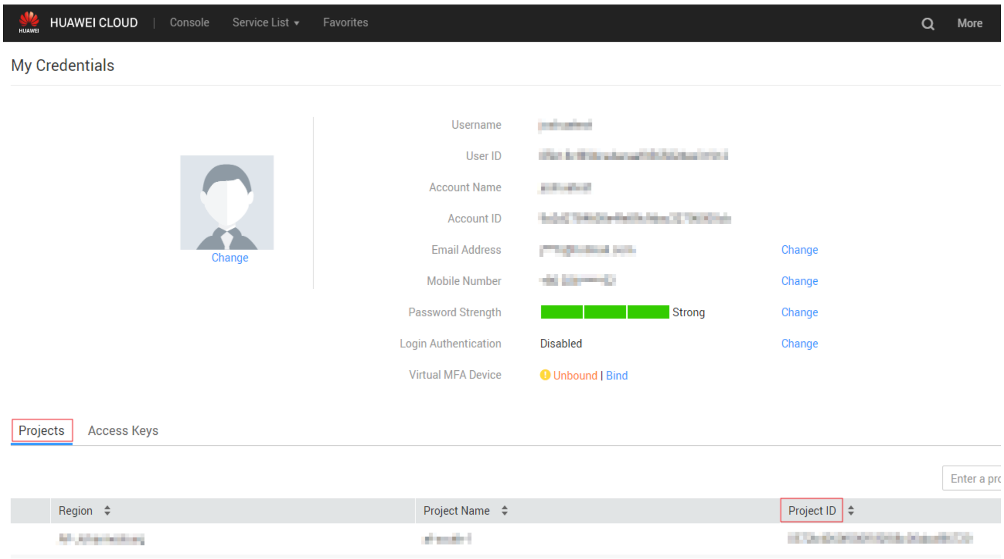
Obtaining a Project ID from the Console

A project ID is required for some URLs when an API is called. To obtain a project ID, perform the following operations:

1. Log in to the management console.
2. Click the username and choose **Basic Information** from the drop-down list.
3. On the **Account Info** page, click **Manage** next to **Security Credentials**.

   On the **My Credentials** page, view project IDs in the project list.

Figure A-1 Viewing project IDs



My Credentials

Username	[redacted]	
User ID	[redacted]	
Account Name	[redacted]	
Account ID	[redacted]	
Email Address	[redacted]	Change
Mobile Number	[redacted]	Change
Password Strength	🟩🟩🟩 Strong	Change
Login Authentication	Disabled	Change
Virtual MFA Device	Unbound | Bind	

Region	Project Name	Project ID
[redacted]	[redacted]	[redacted]

B Change History

Date	Description
2022-09-30	This is the first official release.