

密钥管理系统

API 文档

产品文档



腾讯云

【版权声明】

©2013-2024 腾讯云版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

【商标声明】

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。

【服务声明】

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

文档目录

API 文档

History

Introduction

API Category

Making API Requests

Request Structure

Common Params

Signature v3

Signature

Responses

Key APIs

PostQuantumCryptoEncrypt

PostQuantumCryptoDecrypt

UpdateKeyDescription

UpdateAlias

ReEncrypt

ListKeys

ListKeyDetail

GetServiceStatus

GetKeyRotationStatus

GenerateDataKey

Encrypt

EnableKeys

EnableKeyRotation

EnableKey

DisableKeys

DisableKeyRotation

DisableKey

DescribeKeys

DescribeKey

Decrypt

CreateKey

ScheduleKeyDeletion

CancelKeyDeletion

ImportKeyMaterial

GetParametersForImport
DeleteImportedKeyMaterial
GenerateRandom
ListAlgorithms
UnbindCloudResource
BindCloudResource
GetRegions
CancelKeyArchive
ArchiveKey

Asymmetric Key APIs

PostQuantumCryptoVerify
PostQuantumCryptoSign
GetPublicKey
AsymmetricSm2Decrypt
AsymmetricRsaDecrypt
VerifyByAsymmetricKey
SignByAsymmetricKey

White-Box Key APIs

EncryptByWhiteBox
EnableWhiteBoxKeys
EnableWhiteBoxKey
DisableWhiteBoxKeys
DisableWhiteBoxKey
DescribeWhiteBoxServiceStatus
DescribeWhiteBoxKeyDetails
DescribeWhiteBoxKey
DescribeWhiteBoxDecryptKey
DeleteWhiteBoxKey
CreateWhiteBoxKey
OverwriteWhiteBoxDeviceFingerprints
DescribeWhiteBoxDeviceFingerprints

Data Types

Error Codes

API 文档

History

最近更新时间：2023-08-07 17:45:11

Release 9

Release time: 2023-08-07 17:32:30

Release updates:

Improvement to existing documentation.

New APIs:

- [PostQuantumCryptoDecrypt](#)
- [PostQuantumCryptoEncrypt](#)
- [PostQuantumCryptoSign](#)
- [PostQuantumCryptoVerify](#)

Release 8

Release time: 2023-03-24 15:59:19

Release updates:

Improvement to existing documentation.

Modified APIs:

- [GetServiceStatus](#)
 - New output parameters:SubscriptionInfo

Release 7

Release time: 2023-02-27 16:31:27

Release updates:

Improvement to existing documentation.

Modified APIs:

- [EnableKeyRotation](#)
 - New input parameters:RotateDays

Release 6

Release time: 2022-07-04 10:36:46

Release updates:

Improvement to existing documentation.

Modified APIs:

- [CreateKey](#)
 - New input parameters:HsmClusterId
 - New output parameters:HsmClusterId
- [GetServiceStatus](#)
 - New output parameters:ExclusiveVSMEnabled, ExclusiveHSMEnabled
- [ListKeyDetail](#)
 - New input parameters:HsmClusterId
- [ListKeys](#)
 - New input parameters:HsmClusterId

Modified data structures:

- [KeyMetadata](#)
 - New members:HsmClusterId

Release 5

Release time: 2022-01-18 17:17:48

Release updates:

Improvement to existing documentation.

Modified APIs:

- [Decrypt](#)
 - New input parameters:EncryptionPublicKey, EncryptionAlgorithm

- [GenerateDataKey](#)
 - New input parameters:EncryptionPublicKey, EncryptionAlgorithm

Release 4

Release time: 2021-01-28 20:01:17

Release updates:

Improvement to existing documentation.

New APIs:

- [SignByAsymmetricKey](#)
- [VerifyByAsymmetricKey](#)

Modified APIs:

- [ListAlgorithms](#)
 - New output parameters:AsymmetricSignVerifyAlgorithms

Release 3

Release time: 2020-12-02 11:25:39

Release updates:

Improvement to existing documentation.

Modified APIs:

- [GetServiceStatus](#)
 - New output parameters:UserLevel, ProExpireTime, ProRenewFlag, ProResourceId

Release 2

Release time: 2020-08-06 19:42:05

Release updates:

Improvement to existing documentation.

New APIs:

- [BindCloudResource](#)
- [UnbindCloudResource](#)

Existing Release

Release time: 2020-07-30 19:59:49

Existing APIs/data structures are as follows:

Improvement to existing documentation.

Existing APIs:

- [AsymmetricRsaDecrypt](#)
- [AsymmetricSm2Decrypt](#)
- [CancelKeyDeletion](#)
- [CreateKey](#)
- [CreateWhiteBoxKey](#)
- [Decrypt](#)
- [DeleteImportedKeyMaterial](#)
- [DeleteWhiteBoxKey](#)
- [DescribeKey](#)
- [DescribeKeys](#)
- [DescribeWhiteBoxDecryptKey](#)
- [DescribeWhiteBoxDeviceFingerprints](#)
- [DescribeWhiteBoxKey](#)
- [DescribeWhiteBoxKeyDetails](#)
- [DescribeWhiteBoxServiceStatus](#)
- [DisableKey](#)
- [DisableKeyRotation](#)
- [DisableKeys](#)
- [DisableWhiteBoxKey](#)
- [DisableWhiteBoxKeys](#)
- [EnableKey](#)
- [EnableKeyRotation](#)
- [EnableKeys](#)
- [EnableWhiteBoxKey](#)
- [EnableWhiteBoxKeys](#)
- [Encrypt](#)

- [EncryptByWhiteBox](#)
- [GenerateDataKey](#)
- [GenerateRandom](#)
- [GetKeyRotationStatus](#)
- [GetParametersForImport](#)
- [GetPublicKey](#)
- [GetServiceStatus](#)
- [ImportKeyMaterial](#)
- [ListAlgorithms](#)
- [ListKeyDetail](#)
- [ListKeys](#)
- [OverwriteWhiteBoxDeviceFingerprints](#)
- [ReEncrypt](#)
- [ScheduleKeyDeletion](#)
- [UpdateAlias](#)
- [UpdateKeyDescription](#)

Existing data structures:

- [AlgorithmInfo](#)
- [DeviceFingerprint](#)
- [Key](#)
- [KeyMetadata](#)
- [Tag](#)
- [WhiteboxKeyInfo](#)

Introduction

最近更新时间：2023-02-27 16:39:17

Tencent Cloud Key Management Service (KMS) is a security service that allows you to protect data using keys, delivering high security and availability for your business.

API Category

最近更新时间：2023-08-07 17:45:11

Asymmetric Key APIs

API Name	Feature	Frequency Limit (maximum requests per second)
AsymmetricRsaDecrypt	Decrypts data with an RSA asymmetric key	200
AsymmetricSm2Decrypt	Decrypts data with an SM2 asymmetric key	200
GetPublicKey	Gets the information of the public key that is encrypted with the asymmetric cryptographic algorithm	100
PostQuantumCryptoSign	Signs with PQCDecrypts with PQC	20
PostQuantumCryptoVerify	Verifies a signature with PQC	20
SignByAsymmetricKey	Generates a signature	100
VerifyByAsymmetricKey	Verifies a signature	100

White-Box Key APIs

API Name	Feature	Frequency Limit (maximum requests per second)
CreateWhiteBoxKey	Creates a white-box key	100
DeleteWhiteBoxKey	Deletes a white-box key	200
DescribeWhiteBoxDecryptKey	Gets a white-box decryption key	200
DescribeWhiteBoxDeviceFingerprints	Gets the device fingerprint list of a specified key	100
DescribeWhiteBoxKey	Displays white-box key information	200
DescribeWhiteBoxKeyDetails	Gets the white-box key list	100

DescribeWhiteBoxServiceStatus	Gets the white-box key service status	200
DisableWhiteBoxKey	Disables a white-box key	200
DisableWhiteBoxKeys	Disables white-box keys in batches	200
EnableWhiteBoxKey	Enables a white-box key	200
EnableWhiteBoxKeys	Enables white-box keys in batches	200
EncryptByWhiteBox	Encrypts data with a white-box key	100
OverwriteWhiteBoxDeviceFingerprints	Overwrites the device fingerprint information of a specified key	100

Key APIs

API Name	Feature	Frequency Limit (maximum requests per second)
ArchiveKey	Archives keys	100
BindCloudResource	Binds a key with a Tencent Cloud resource	100
CancelKeyArchive	Unarchives keys	100
CancelKeyDeletion	Cancel CMK plan delete operation	100
CreateKey	Create master key	100
Decrypt	Decrypt	300
DeleteImportedKeyMaterial	Deletes imported key material	100
DescribeKey	Gets CMK attributes	100
DescribeKeys	Gets attributes of multiple CMKs	100
DisableKey	Disable master key	100
DisableKeyRotation	Disable key rotation	100
DisableKeys	Disable master keys in bulk	100

EnableKey	Enable master key	100
EnableKeyRotation	Turn on key rotation	100
EnableKeys	Batch start master key	100
Encrypt	encryption	300
GenerateDataKey	Generate data key	100
GenerateRandom	Generates a random number	150
GetKeyRotationStatus	Query key rotation status	100
GetParametersForImport	Gets the parameters of the material to be imported into a CMK	100
GetRegions	Return all regions support KMS service	100
GetServiceStatus	Query service status	100
ImportKeyMaterial	Imports key material	100
ListAlgorithms	Lists encryption methods supported in the current region	100
ListKeyDetail	Get master key list details	100
ListKeys	Get master key list	100
PostQuantumCryptoDecrypt	Decrypts with PQC	20
PostQuantumCryptoEncrypt	Encrypts with PQC	20
ReEncrypt	Ciphertext refresh	100
ScheduleKeyDeletion	CMK plan delete API	100
UnbindCloudResource	Unbinds a CMK with a Tencent Cloud resource	100
UpdateAlias	Modify alias	100
UpdateKeyDescription	Modify master key description	100

Making API Requests

Request Structure

最近更新时间：2023-02-27 16:37:43

1. Service Address

The API supports access from either a nearby region (at kms.tencentcloudapi.com) or a specified region (at kms.ap-guangzhou.tencentcloudapi.com for Guangzhou, for example).

We recommend using the domain name to access the nearest server. When you call an API, the request is automatically resolved to a server in the region **nearest** to the location where the API is initiated. For example, when you initiate an API request in Guangzhou, this domain name is automatically resolved to a Guangzhou server, the result is the same as that of specifying the region in the domain like "kms.ap-guangzhou.tencentcloudapi.com".

Note: For latency-sensitive businesses, we recommend that you specify the region in the domain name.

Tencent Cloud currently supports the following regions:

Hosted region	Domain name
Local access region (recommended, only for non-financial availability zones)	kms.tencentcloudapi.com
South China (Guangzhou)	kms.ap-guangzhou.tencentcloudapi.com
East China (Shanghai)	kms.ap-shanghai.tencentcloudapi.com
North China (Beijing)	kms.ap-beijing.tencentcloudapi.com
Southwest China (Chengdu)	kms.ap-chengdu.tencentcloudapi.com
Southwest China (Chongqing)	kms.ap-chongqing.tencentcloudapi.com
Hong Kong, Macao, Taiwan (Hong Kong, China)	kms.ap-hongkong.tencentcloudapi.com
Southeast Asia (Singapore)	kms.ap-singapore.tencentcloudapi.com
Southeast Asia (Bangkok)	kms.ap-bangkok.tencentcloudapi.com

South Asia (Mumbai)	kms.ap-mumbai.tencentcloudapi.com
Northeast Asia (Seoul)	kms.ap-seoul.tencentcloudapi.com
Northeast Asia (Tokyo)	kms.ap-tokyo.tencentcloudapi.com
U.S. East Coast (Virginia)	kms.na-ashburn.tencentcloudapi.com
U.S. West Coast (Silicon Valley)	kms.na-siliconvalley.tencentcloudapi.com
North America (Toronto)	kms.na-toronto.tencentcloudapi.com
Europe (Frankfurt)	kms.eu-frankfurt.tencentcloudapi.com

2. Communications Protocol

All the Tencent Cloud APIs communicate via HTTPS, providing highly secure communication tunnels.

3. Request Methods

Supported HTTP request methods:

- POST (recommended)
- GET

The Content-Type types supported by POST requests:

- application/json (recommended). The TC3-HMAC-SHA256 signature algorithm must be used.
- application/x-www-form-urlencoded. The HmacSHA1 or HmacSHA256 signature algorithm must be used.
- multipart/form-data (only supported by certain APIs). You must use TC3-HMAC-SHA256 to calculate the signature.

The size of a GET request packet is up to 32 KB. The size of a POST request is up to 1 MB when the HmacSHA1 or HmacSHA256 signature algorithm is used, and up to 10 MB when TC3-HMAC-SHA256 is used.

4. Character Encoding

Only UTF-8 encoding is used.

Common Params

最近更新时间：2023-02-27 16:37:43

Common parameters are used for all APIs authenticating requestors. Common parameters must be included in all API requests, and they will not be described in individual API documents.

The exact contents of the common parameters will vary depending on the version of the signature method you use.

Common parameters for Signature Algorithm v3

When the TC3-HMAC-SHA256 algorithm is used, the common parameters should be uniformly placed in the HTTP request header, as shown below:

Parameter Name	Type	Required	Description
X-TC-Action	String	Yes	The name of the API for the desired operation. For the specific value, see description of common parameter <code>Action</code> in the input parameters in related API documentation. For example, the API for querying the CVM instance list is <code>DescribeInstances</code> .
X-TC-Region	String	Yes	Region parameter, which is used to identify the region to which the data you work with belongs. For values supported for an API, see the description of common parameter <code>Region</code> in the input parameters in related API documentation. This parameter is not required for some APIs (which will be indicated in related API documentation), and will not take effect even it is passed.
X-TC-Timestamp	Integer	Yes	The current UNIX timestamp that records the time when the API request is sent. For example, 1529223702. Note: If the difference between the UNIX timestamp and server time is greater than 5 minutes, a signature expiration error may occur.
X-TC-Version	String	Yes	API version of the action. For the valid values, see the description of the common parameter <code>Version</code> in the API documentation. For example, the version is 2017-03-12.
Authorization	String	Yes	The HTTP authentication request header, for example: TC3-HMAC-SHA256 Credential=AKIDEXAMPLE/Date/service/tc3_request/Signature=fe5f80f77d5fa3beca038a248ff027d0445342fe2855ddc96317 Here: - TC3-HMAC-SHA256: Signature method, currently fixed as this value; - Credential: Signature credential; AKIDEXAMPLE is the SecretId; Date is the UNIX timestamp in UTC time, and this value must match the value of X-TC-Timestamp (a co

			parameter) in UTC time format; service is the name of the product/service generally a domain name prefix. For example, a domain name cvm.tencent refers to the CVM product and the value would be cvm; - SignedHeaders: The headers that contains the authentication information type and host are the required headers; - Signature: Signature digest.
X-TC-Token	String	No	The token used for a temporary certificate. It must be used with a temporary key to obtain the temporary key and token by calling a CAM API. No token is required for a long-term key.

Assuming you want to query the list of Cloud Virtual Machine instances in the Guangzhou region, the request structure in the form of request URL, request header and request body may be as follows:

Example of an HTTP GET request structure:

```
https://cvm.tencentcloudapi.com/?Limit=10&Offset=0

Authorization: TC3-HMAC-SHA256 Credential=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE/2018-10-09/cvm/tc3_request, SignedHeaders=content-type;host, Signature=5da7a33f6993f0614b047e5df4582db9e9bf4672ba50567dba16c6ccf174c474
Content-Type: application/x-www-form-urlencoded
Host: cvm.tencentcloudapi.com
X-TC-Action: DescribeInstances
X-TC-Version: 2017-03-12
X-TC-Timestamp: 1539084154
X-TC-Region: ap-guangzhou
```

The following example shows you how to structure an HTTP POST (application/json) request:

```
https://cvm.tencentcloudapi.com/

Authorization: TC3-HMAC-SHA256 Credential=AKIDEXAMPLE/2018-05-30/cvm/tc3_request, SignedHeaders=content-type;host, Signature=582c400e06b5924a6f2b5d7d672d79c15b13162d9279b0855cfba6789a8edb4c
Content-Type: application/json
Host: cvm.tencentcloudapi.com
X-TC-Action: DescribeInstances
X-TC-Version: 2017-03-12
X-TC-Timestamp: 1527672334
X-TC-Region: ap-guangzhou

{"Offset":0,"Limit":10}
```

Example of an HTTP POST (multipart/form-data) request structure (only supported by specific APIs):

```
https://cvm.tencentcloudapi.com/
```

```
Authorization: TC3-HMAC-SHA256 Credential=AKIDEXAMPLE/2018-05-30/cvm/tc3_request,
SignedHeaders=content-type;host, Signature=582c400e06b5924a6f2b5d7d672d79c15b1316
2d9279b0855cfba6789a8edb4c
```

```
Content-Type: multipart/form-data; boundary=58731222010402
```

```
Host: cvm.tencentcloudapi.com
```

```
X-TC-Action: DescribeInstances
```

```
X-TC-Version: 2017-03-12
```

```
X-TC-Timestamp: 1527672334
```

```
X-TC-Region: ap-guangzhou
```

```
--58731222010402
```

```
Content-Disposition: form-data; name="Offset"
```

```
0
```

```
--58731222010402
```

```
Content-Disposition: form-data; name="Limit"
```

```
10
```

```
--58731222010402--
```

Common parameters for Signature Algorithm v1

To adopt the HmacSHA1 and HmacSHA256 signature methods, common parameters must be put into the request string, as shown below:

Parameter Name	Type	Required	Description
Action	String	Yes	The name of the API for the desired operation. For the specific value, see the description of common parameter <code>Action</code> in the input parameters in related API documentation. For example, the API for querying the CVM instance list is <code>DescribeInstances</code> .
Region	String	Yes	Region parameter, which is used to identify the region to which the data you want to work with belongs. For values supported for an API, see the description of common parameter <code>Region</code> in the input parameters in related API documentation. Note: This parameter is not required for some APIs (which will be indicated in related API documentation), and will not take effect even if it is passed.

Timestamp	Integer	Yes	The current UNIX timestamp that records the time when the API request was initiated, for example, 1529223702. If the difference between the value and the current system time is too large, a signature expiration error may occur.
Nonce	Integer	Yes	A random positive integer used along with <code>Timestamp</code> to prevent replay attacks.
SecretId	String	Yes	The identifying SecretId obtained on the Cloud API Key page. A SecretId corresponds to a unique SecretKey which is used to generate the request signature (Signature).
Signature	String	Yes	Request signature used to verify the validity of this request. This is calculated based on the actual input parameters. For more information about how this is calculated, see the API authentication documentation.
Version	String	Yes	API version of the action. For the valid values, see the description of the common input parameter <code>Version</code> in the API documentation. For example, the version of CVM is 2017-03-12.
SignatureMethod	String	No	Signature method. Currently, only HmacSHA256 and HmacSHA1 are supported. The HmacSHA256 algorithm is used to verify the signature only when this parameter is specified as HmacSHA256. In other cases, the signature is verified with HmacSHA1.
Token	String	No	The token used for a temporary certificate. It must be used with a temporary key. You can obtain the temporary key and token by calling a CAM API. No token is required for a long-term key.

Assuming you want to query the list of Cloud Virtual Machine instances in the Guangzhou region, the request structure in the form of request URL, request header and request body may be as follows:

Example of an HTTP GET request structure:

```
https://cvm.tencentcloudapi.com/?Action=DescribeInstances&Version=2017-03-12&SignatureMethod=HmacSHA256&Timestamp=1527672334&Signature=37ac2f4fde00b0ac9bd9eadeb459b1bbbe224158d66e7ae5fcadb70b2d181d02&Region=ap-guangzhou&Nonce=23823223&SecretId=AKIDEXAMPLE
```

```
Host: cvm.tencentcloudapi.com
Content-Type: application/x-www-form-urlencoded
```

Example of an HTTP POST request structure:

```
https://cvm.tencentcloudapi.com/
```

```
Host: cvm.tencentcloudapi.com
```

```
Content-Type: application/x-www-form-urlencoded
```

```
Action=DescribeInstances&Version=2017-03-12&SignatureMethod=HmacSHA256&Timestamp=1527672334&Signature=37ac2f4fde00b0ac9bd9eadeb459b1bbec224158d66e7ae5fcadb70b2d181d02&Region=ap-guangzhou&Nonce=23823223&SecretId=AKIDEXAMPLE
```

Signature v3

最近更新时间：2020-10-16 18:20:54

TencentCloud API authenticates every single request, i.e., the request must be signed using the security credentials in the designated steps. Each request has to contain the signature information (Signature) in the common request parameters and be sent in the specified way and format.

Applying for Security Credentials

The security credential used in this document is a key, which includes a SecretId and a SecretKey. Each user can have up to two pairs of keys.

- SecretId: Used to identify the API caller, which is just like a username.
- SecretKey: Used to authenticate the API caller, which is just like a password.
- **You must keep your security credentials private and avoid disclosure; otherwise, your assets may be compromised. If they are disclosed, please disable them as soon as possible.**

You can apply for the security credentials through the following steps:

1. Log in to the [Tencent Cloud Console](#).
2. Go to the [TencentCloud API Key](#) console page.
3. On the [TencentCloud API Key](#) page, click **Create** to create a SecretId/SecretKey pair.

Using the Resources for Developers

TencentCloud API comes with SDKs for seven commonly used programming languages, including [Python](#), [Java](#), [PHP](#), [Go](#), [NodeJS](#) and [.NET](#). In addition, it provides [API Explorer](#) which enables online call, signature verification, and SDK code generation. If you have any troubles calculating a signature, consult these resources.

TC3-HMAC-SHA256 Signature Algorithm

Compatible with the previous HmacSHA1 and HmacSHA256 signature algorithms, the TC3-HMAC-SHA256 signature algorithm is more secure and supports larger requests and JSON format with better performance. We recommend using TC3-HMAC-SHA256 to calculate the signature.

TencentCloud API supports both GET and POST requests. For the GET method, only the Content-Type: application/x-www-form-urlencoded protocol format is supported. For the POST method, two protocol formats,

Content-Type: application/json and Content-Type: multipart/form-data, are supported. The JSON format is supported by default for all business APIs, and the multipart format is supported only for specific business APIs. In this case, the API cannot be called in JSON format. See the specific business API documentation for more information. The POST method is recommended, as there is no difference in the results of both the methods, but the GET method only supports request packets up to 32 KB.

The following uses querying the list of CVM instances in the Guangzhou region as an example to describe the steps of signature splicing. We chose this API because:

1. CVM is activated by default, and this API is often used;
2. It is read-only and does not change the status of existing resources;
3. It covers many types of parameters, which allows it to be used to demonstrate how to use arrays containing data structures.

In the example, we try to choose common parameters and API parameters that are prone to mistakes. When you actually call an API, please use parameters based on the actual conditions. The parameters vary by API. Do not copy the parameters and values in this example.

Assuming that your SecretId and SecretKey are `AKIDz8krbsJ5yKBZQpn74WFkmLPx3*****` and `Gu5t9xGARNpq86cd98joQYCN3*****`, respectively, if you want to view the status of the instance in the Guangzhou region whose CVM instance name is "unnamed" and have only one data entry returned, then the request may be:

```
curl -X POST https://cvm.tencentcloudapi.com \
-H "Authorization: TC3-HMAC-SHA256 Credential=AKIDz8krbsJ5yKBZQpn74WFkmLPx3*****
*/2019-02-25/cvm/tc3_request, SignedHeaders=content-type;host, Signature=c492e8e4
1437e97a620b728c301bb8d17e7dc0c17eeabce80c20cd70fc3a78ff" \
-H "Content-Type: application/json; charset=utf-8" \
-H "Host: cvm.tencentcloudapi.com" \
-H "X-TC-Action: DescribeInstances" \
-H "X-TC-Timestamp: 1551113065" \
-H "X-TC-Version: 2017-03-12" \
-H "X-TC-Region: ap-guangzhou" \
-d '{"Limit": 1, "Filters": [{"Values": ["unnamed"], "Name": "instance-name"}]}'
```

The signature calculation process is explained in detail below.

1. Concatenating the CanonicalRequest String

Concatenate the canonical request string (CanonicalRequest) in the following pseudocode format:

```
CanonicalRequest =
HTTPRequestMethod + '\n' +
CanonicalURI + '\n' +
```

```
CanonicalQueryString + '\n' +  
CanonicalHeaders + '\n' +  
SignedHeaders + '\n' +  
HashedRequestPayload
```

Field Name	Explanation
HTTPRequestMethod	HTTP request method (GET or POST). This example uses <code>POST</code> .
CanonicalURI	URI parameter. Slash ("/") is used for API 3.0.
CanonicalQueryString	The query string in the URL of the originating HTTP request. This is always an empty string for POST requests, and is the string after the question mark (?) for GET requests. For example: <code>Limit=10&Offset=0</code>. Note: <code>CanonicalQueryString</code> must be URL-encoded, referencing RFC3986, the UTF8 character set. We recommend using the programming language library. All special characters must be encoded and capitalized.
CanonicalHeaders	Header information for signature calculation, including at least two headers of <code>host</code> and <code>content-type</code>. Custom headers can be added to participate in the signature process to improve the uniqueness and security of the request. Concatenation rules: - Both the key and value of the header should be converted to lowercase with the leading and trailing spaces removed, so they are concatenated in the format of <code>key:value\n</code> format; - If there are multiple headers, they should be sorted in ASCII ascending order by the header keys (lowercase). The calculation result in this example is <code>content-type:application/json; charset=utf-8\nhost:cvm.tencentcloudapi.com\n</code>. Note: <code>content-type</code> must match the actually sent content. In some programming languages, a charset value would be added even if it is not specified. In this case, the request sent is different from the one signed, and the server will return an error indicating signature verification failed.
SignedHeaders	Header information for signature calculation, indicating which headers of the request participate in the signature process (they must each individually correspond to the headers in CanonicalHeaders). <code>Content-type</code> and <code>host</code> are required headers. Concatenation rules: - Both the key and value of the header should be converted to lowercase; - If there are multiple headers, they should be sorted in ASCII ascending order by the header keys (lowercase) and separated by semicolons (;). The value in this example is <code>content-type;host</code>
HashedRequestPayload	Hash value of the request payload (i.e., the body, such as <code>{"Limit": 1, "Filter</code>

```
[{"Values": ["unnamed"], "Name": "instance-name"}]}
```

 in this example
The pseudocode for calculation is
Lowercase(HexEncode(Hash.SHA256(RequestPayload))) by SHA256 hashing the pay
of the HTTP request, performing hexadecimal encoding, and finally converting the encc
string to lowercase letters. For GET requests, `RequestPayload` is always an empt
string. The calculation result in this example is
`99d58dfbc6745f6747f36bfca17dee5e6881dc0428a0a36f96199342bc5b4907`

According to the rules above, the `CanonicalRequest` string obtained in the example is as follows:

```
POST
/

content-type:application/json; charset=utf-8
host:cvm.tencentcloudapi.com

content-type;host
99d58dfbc6745f6747f36bfca17dee5e6881dc0428a0a36f96199342bc5b4907
```

2. Concatenating the String to Be Signed

The string to sign is concatenated as follows:

```
StringToSign =
Algorithm + \n +
RequestTimestamp + \n +
CredentialScope + \n +
HashedCanonicalRequest
```

Field Name	Explanation
Algorithm	Signature algorithm, which is currently always <code>TC3-HMAC-SHA256</code> .
RequestTimestamp	Request timestamp, i.e., the value of the common parameter <code>X-TC-Timestamp</code> in request header, which is the UNIX timestamp of the current time in seconds, such as <code>1551113065</code> in this example.
CredentialScope	Scope of the credential in the format of <code>Date/service/tc3_request</code> , including date, requested service and termination string (tc3_request). Date is a date in UTC time, whose value should match the UTC date converted by the common parameter X-TC-Timestamp ; service is the product name, which should match the domain name of the product called. The calculation result in this example is <code>2018-05-25/cvm/tc3_request</code> .

HashedCanonicalRequest

Hash value of the CanonicalRequest string concatenated in the steps above. The pseudocode for calculation is Lowercase(HexEncode(Hash.SHA256(CanonicalRequest))). The calculation result in this example is

```
2815843035062fffd6f2a44ea8a34818b0dc46f024b8b3786976a3ad
```

Note:

1. Date has to be calculated from the timestamp "X-TC-Timestamp" and the time zone is UTC+0. If you add the system's local time zone information (such as UTC+8), calls can succeed both day and night but will definitely fail at 00:00. For example, if the timestamp is 1551113065 and the time in UTC+8 is 2019-02-26 00:44:25, the UTC+0 date in the calculated Date value should be 2019-02-25 instead of 2019-02-26.
2. Timestamp must be the same as your current system time, and your system time and standard time must be synced; if the difference between Timestamp and your current system time is larger than five minutes, the request will fail. If your system time is out of sync with the standard time for a while, the request will fail and return a signature expiration error.

According to the preceding rules, the string to be signed obtained in the example is as follows:

```
TC3-HMAC-SHA256
1551113065
2019-02-25/cvm/tc3_request
2815843035062fffd6f2a44ea8a34818b0dc46f024b8b3786976a3adda7a
```

3. Calculating the Signature

1) Calculate the derived signature key with the following pseudocode:

```
SecretKey = "Gu5t9xGARNpq86cd98joQYCN3*****"
SecretDate = HMAC_SHA256("TC3" + SecretKey, Date)
SecretService = HMAC_SHA256(SecretDate, Service)
SecretSigning = HMAC_SHA256(SecretService, "tc3_request")
```

Field Name	Explanation
SecretKey	The original SecretKey, i.e., <code>Gu5t9xGARNpq86cd98joQYCN3*****</code> .
Date	The Date field information in <code>Credential</code> , such as <code>2019-02-25</code> in this example.
Service	Value in the Service field in <code>Credential</code> , such as <code>cvm</code> in this example.

2) Calculate the signature with the following pseudocode:

```
Signature = HexEncode(HMAC_SHA256(SecretSigning, StringToSign))
```

4. Concatenating the Authorization

The Authorization is concatenated as follows:

```
Authorization =  
Algorithm + ' ' +  
'Credential=' + SecretId + '/' + CredentialScope + ', ' +  
'SignedHeaders=' + SignedHeaders + ', ' +  
'Signature=' + Signature
```

Field Name	Explanation
Algorithm	Signature algorithm, which is always <code>TC3-HMAC-SHA256</code> .
SecretId	The SecretId in the key pair, i.e., <code>AKIDz8krbsJ5yKBZQpn74WFkmLPx3*****</code> .
CredentialScope	Credential scope (see above). The calculation result in this example is <code>2019-02-25/cvm/tc3_request</code> .
SignedHeaders	Header information for signature calculation (see above), such as <code>content-type;host</code> in this example.
Signature	Signature value. The calculation result in this example is <code>c492e8e41437e97a620b728c301bb8d17e7dc0c17eeabce80c20cd70fc3a78ff</code> .

According to the rules above, the value obtained in the example is:

```
TC3-HMAC-SHA256 Credential=AKIDz8krbsJ5yKBZQpn74WFkmLPx3*****/2019-02-25/cvm/tc3_request, SignedHeaders=content-type;host, Signature=c492e8e41437e97a620b728c301bb8d17e7dc0c17eeabce80c20cd70fc3a78ff
```

The following example shows a finished authorization header:

```
POST https://cvm.tencentcloudapi.com/  
Authorization: TC3-HMAC-SHA256 Credential=AKIDz8krbsJ5yKBZQpn74WFkmLPx3*****/2019-02-25/cvm/tc3_request, SignedHeaders=content-type;host, Signature=c492e8e41437e97a620b728c301bb8d17e7dc0c17eeabce80c20cd70fc3a78ff  
Content-Type: application/json; charset=utf-8  
Host: cvm.tencentcloudapi.com
```

```
X-TC-Action: DescribeInstances
X-TC-Version: 2017-03-12
X-TC-Timestamp: 1551113065
X-TC-Region: ap-guangzhou

{"Limit": 1, "Filters": [{"Values": ["unnamed"], "Name": "instance-name"}]}
```

5. Signature Demo

When calling API 3.0, you are recommended to use the corresponding Tencent Cloud SDK 3.0 which encapsulates the signature process, enabling you to focus on only the specific APIs provided by the product when developing. See [SDK Center](#) for more information. Currently, the following programming languages are supported:

- [Python](#)
- [Java](#)
- [PHP](#)
- [Go](#)
- [NodeJS](#)
- [.NET](#)

To further explain the signing process, we will use a programming language to implement the process described above. The request domain name, API and parameter values in the sample are used here. This goal of this example is only to provide additional clarification for the signature process, please see the SDK for actual usage.

The final output URL might be: `https://cvm.tencentcloudapi.com/?Action=DescribeInstances&InstanceId=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=ap-guangzhou&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3*****&Signature=EliP9YW3pW28FpsEdkXt%2F%2BWcGel%3D&Timestamp=1465185768&Version=2017-03-12`.

Note: The key in the example is fictitious, and the timestamp is not the current time of the system, so if this URL is opened in the browser or called using commands such as curl, an authentication error will be returned: Signature expired. In order to get a URL that can work properly, you need to replace the SecretId and SecretKey in the example with your real credentials and use the current time of the system as the Timestamp.

Note: In the example below, even if you use the same programming language, the order of the parameters in the URL may be different for each execution. However, the order does not matter, as long as all the parameters are included in the URL and the signature is calculated correctly.

Note: The following code is only applicable to API 3.0. It cannot be directly used in other signature processes. Even with an older API, signature calculation errors may occur due to the differences in details. Please refer to the corresponding documentation.

Java

```
import java.nio.charset.Charset;
import java.nio.charset.StandardCharsets;
import java.security.MessageDigest;
import java.text.SimpleDateFormat;
import java.util.Date;
import java.util.TimeZone;
import java.util.TreeMap;
import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
import javax.xml.bind.DatatypeConverter;

public class TencentCloudAPITC3Demo {
    private final static Charset UTF8 = StandardCharsets.UTF_8;
    private final static String SECRET_ID = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3*****";
    private final static String SECRET_KEY = "Gu5t9xGARNpq86cd98joQYCN3*****";
    private final static String CT_JSON = "application/json; charset=utf-8";

    public static byte[] hmac256(byte[] key, String msg) throws Exception {
        Mac mac = Mac.getInstance("HmacSHA256");
        SecretKeySpec secretKeySpec = new SecretKeySpec(key, mac.getAlgorithm());
        mac.init(secretKeySpec);
        return mac.doFinal(msg.getBytes(UTF8));
    }

    public static String sha256Hex(String s) throws Exception {
        MessageDigest md = MessageDigest.getInstance("SHA-256");
        byte[] d = md.digest(s.getBytes(UTF8));
        return DatatypeConverter.printHexBinary(d).toLowerCase();
    }

    public static void main(String[] args) throws Exception {
        String service = "cvm";
        String host = "cvm.tencentcloudapi.com";
        String region = "ap-guangzhou";
        String action = "DescribeInstances";
        String version = "2017-03-12";
        String algorithm = "TC3-HMAC-SHA256";
        String timestamp = "1551113065";
        //String timestamp = String.valueOf(System.currentTimeMillis() / 1000);
        SimpleDateFormat sdf = new SimpleDateFormat("yyyy-MM-dd");
        // Pay attention to the time zone; otherwise, errors may occur
        sdf.setTimeZone(TimeZone.getTimeZone("UTC"));
        String date = sdf.format(new Date(Long.valueOf(timestamp + "000")));

        // ***** Step 1: Concatenate the CanonicalRequest string *****
        String httpRequestMethod = "POST";
```

```
String canonicalUri = "/";
String canonicalQueryString = "";
String canonicalHeaders = "content-type:application/json; charset=utf-8\n" + "host:" + host + "\n";
String signedHeaders = "content-type;host";

String payload = "{\"Limit\": 1, \"Filters\": [{\"Values\": [\"unnamed\"], \"Name\": \"instance-name\"}]}";
String hashedRequestPayload = sha256Hex(payload);
String canonicalRequest = httpRequestMethod + "\n" + canonicalUri + "\n" + canonicalQueryString + "\n"
+ canonicalHeaders + "\n" + signedHeaders + "\n" + hashedRequestPayload;
System.out.println(canonicalRequest);

// ***** Step 2: Concatenate the string to sign *****
String credentialScope = date + "/" + service + "/" + "tc3_request";
String hashedCanonicalRequest = sha256Hex(canonicalRequest);
String stringToSign = algorithm + "\n" + timestamp + "\n" + credentialScope + "\n" + hashedCanonicalRequest;
System.out.println(stringToSign);

// ***** Step 3: Calculate the signature *****
byte[] secretDate = hmac256(("TC3" + SECRET_KEY).getBytes(UTF8), date);
byte[] secretService = hmac256(secretDate, service);
byte[] secretSigning = hmac256(secretService, "tc3_request");
String signature = DatatypeConverter.printHexBinary(hmac256(secretSigning, stringToSign)).toLowerCase();
System.out.println(signature);

// ***** Step 4: Concatenate the Authorization *****
String authorization = algorithm + " " + "Credential=" + SECRET_ID + "/" + credentialScope + ", "
+ "SignedHeaders=" + signedHeaders + ", " + "Signature=" + signature;
System.out.println(authorization);

TreeMap<String, String> headers = new TreeMap<String, String>();
headers.put("Authorization", authorization);
headers.put("Content-Type", CT_JSON);
headers.put("Host", host);
headers.put("X-TC-Action", action);
headers.put("X-TC-Timestamp", timestamp);
headers.put("X-TC-Version", version);
headers.put("X-TC-Region", region);

StringBuilder sb = new StringBuilder();
sb.append("curl -X POST https://").append(host)
.append(" -H \"Authorization: ").append(authorization).append("\")")
```

```
.append(" -H \"Content-Type: application/json; charset=utf-8\"")
.append(" -H \"Host: ").append(host).append("\"")
.append(" -H \"X-TC-Action: ").append(action).append("\"")
.append(" -H \"X-TC-Timestamp: ").append(timestamp).append("\"")
.append(" -H \"X-TC-Version: ").append(version).append("\"")
.append(" -H \"X-TC-Region: ").append(region).append("\"")
.append(" -d '").append(payload).append("'");
System.out.println(sb.toString());
}
}
```

Python

```
# -*- coding: utf-8 -*-
import hashlib, hmac, json, os, sys, time
from datetime import datetime

# Key Parameters
secret_id = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3*****"
secret_key = "Gu5t9xGARNpq86cd98joQYCN3*****"

service = "cvm"
host = "cvm.tencentcloudapi.com"
endpoint = "https://" + host
region = "ap-guangzhou"
action = "DescribeInstances"
version = "2017-03-12"
algorithm = "TC3-HMAC-SHA256"
#timestamp = int(time.time())
timestamp = 1551113065
date = datetime.utcfromtimestamp(timestamp).strftime("%Y-%m-%d")
params = {"Limit": 1, "Filters": [{"Name": "instance-name", "Values": ["unnamed"]}]}

# ***** Step 1: Concatenate the CanonicalRequest string *****
http_request_method = "POST"
canonical_uri = "/"
canonical_querystring = ""
ct = "application/json; charset=utf-8"
payload = json.dumps(params)
canonical_headers = "content-type:%s\nhost:%s\n" % (ct, host)
signed_headers = "content-type;host"
hashed_request_payload = hashlib.sha256(payload.encode("utf-8")).hexdigest()
canonical_request = (http_request_method + "\n" +
canonical_uri + "\n" +
canonical_querystring + "\n" +
```

```
canonical_headers + "\n" +
signed_headers + "\n" +
hashed_request_payload)
print(canonical_request)

# ***** Step 2: Concatenate the string to sign *****
credential_scope = date + "/" + service + "/" + "tc3_request"
hashed_canonical_request = hashlib.sha256(canonical_request.encode("utf-8")).hexdigest()
string_to_sign = (algorithm + "\n" +
str(timestamp) + "\n" +
credential_scope + "\n" +
hashed_canonical_request)
print(string_to_sign)

# ***** Step 3: Calculate the Signature *****
# Function for computing signature digest
def sign(key, msg):
return hmac.new(key, msg.encode("utf-8"), hashlib.sha256).digest()
secret_date = sign(("TC3" + secret_key).encode("utf-8"), date)
secret_service = sign(secret_date, service)
secret_signing = sign(secret_service, "tc3_request")
signature = hmac.new(secret_signing, string_to_sign.encode("utf-8"), hashlib.sha256).hexdigest()
print(signature)

# ***** Step 4: Concatenate the Authorization *****
authorization = (algorithm + " " +
"Credential=" + secret_id + "/" + credential_scope + ", " +
"SignedHeaders=" + signed_headers + ", " +
"Signature=" + signature)
print(authorization)

print('curl -X POST ' + endpoint
+ ' -H "Authorization: ' + authorization + '" '
+ ' -H "Content-Type: application/json; charset=utf-8" '
+ ' -H "Host: ' + host + '" '
+ ' -H "X-TC-Action: ' + action + '" '
+ ' -H "X-TC-Timestamp: ' + str(timestamp) + '" '
+ ' -H "X-TC-Version: ' + version + '" '
+ ' -H "X-TC-Region: ' + region + '" '
+ " -d '" + payload + "'")
```

Golang

```
package main

import (
    "crypto/hmac"
    "crypto/sha256"
    "encoding/hex"
    "fmt"
    "time"
)

func sha256hex(s string) string {
    b := sha256.Sum256([]byte(s))
    return hex.EncodeToString(b[:])
}

func hmacsha256(s, key string) string {
    hashed := hmac.New(sha256.New, []byte(key))
    hashed.Write([]byte(s))
    return string(hashed.Sum(nil))
}

func main() {
    secretId := "AKIDz8krbsJ5yKBZQpn74WFkmLPx3*****"
    secretKey := "Gu5t9xGARNpq86cd98joQYCN3*****"
    host := "cvm.tencentcloudapi.com"
    algorithm := "TC3-HMAC-SHA256"
    service := "cvm"
    version := "2017-03-12"
    action := "DescribeInstances"
    region := "ap-guangzhou"
    //var timestamp int64 = time.Now().Unix()
    var timestamp int64 = 1551113065

    // step 1: build canonical request string
    httpRequestMethod := "POST"
    canonicalURI := "/"
    canonicalQueryString := ""
    canonicalHeaders := "content-type:application/json; charset=utf-8\n" + "host:" +
        host + "\n"
    signedHeaders := "content-type;host"
    payload := `{"Limit": 1, "Filters": [{"Values": ["unnamed"], "Name": "instance-na
me"}]}`
    hashedRequestPayload := sha256hex(payload)
    canonicalRequest := fmt.Sprintf("%s\n%s\n%s\n%s\n%s\n%s",
        httpRequestMethod,
        canonicalURI,
```

```
canonicalQueryString,
canonicalHeaders,
signedHeaders,
hashedRequestPayload)
fmt.Println(canonicalRequest)

// step 2: build string to sign
date := time.Unix(timestamp, 0).UTC().Format("2006-01-02")
credentialScope := fmt.Sprintf("%s/%s/tc3_request", date, service)
hashedCanonicalRequest := sha256hex(canonicalRequest)
string2sign := fmt.Sprintf("%s\n%d\n%s\n%s",
algorithm,
timestamp,
credentialScope,
hashedCanonicalRequest)
fmt.Println(string2sign)

// step 3: sign string
secretDate := hmacsha256(date, "TC3"+secretKey)
secretService := hmacsha256(service, secretDate)
secretSigning := hmacsha256("tc3_request", secretService)
signature := hex.EncodeToString([]byte(hmacsha256(string2sign, secretSigning)))
fmt.Println(signature)

// step 4: build authorization
authorization := fmt.Sprintf("%s Credential=%s/%s, SignedHeaders=%s, Signature=%s",
algorithm,
secretId,
credentialScope,
signedHeaders,
signature)
fmt.Println(authorization)

curl := fmt.Sprintf(`curl -X POST https://%s\
-H "Authorization: %s"\
-H "Content-Type: application/json; charset=utf-8"\
-H "Host: %s" -H "X-TC-Action: %s"\
-H "X-TC-Timestamp: %d"\
-H "X-TC-Version: %s"\
-H "X-TC-Region: %s"\
-d '%s'`, host, authorization, host, action, timestamp, version, region, payload)
fmt.Println(curl)
}
```

```
<?php
$secretId = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3*****";
$secretKey = "Gu5t9xGARNpq86cd98joQYCN3*****";
$host = "cvm.tencentcloudapi.com";
$service = "cvm";
$version = "2017-03-12";
$action = "DescribeInstances";
$region = "ap-guangzhou";
// $timestamp = time();
$timestamp = 1551113065;
$algorithm = "TC3-HMAC-SHA256";

// step 1: build canonical request string
$httpRequestMethod = "POST";
$canonicalUri = "/";
$canonicalQueryString = "";
$canonicalHeaders = "content-type:application/json; charset=utf-8\n"."host:". $host. "\n";
$signedHeaders = "content-type;host";
$payload = '{"Limit": 1, "Filters": [{"Values": ["unnamed"], "Name": "instance-name"}]}';
$hashedRequestPayload = hash("SHA256", $payload);
$canonicalRequest = $httpRequestMethod. "\n"
.$canonicalUri. "\n"
.$canonicalQueryString. "\n"
.$canonicalHeaders. "\n"
.$signedHeaders. "\n"
.$hashedRequestPayload;
echo $canonicalRequest.PHP_EOL;

// step 2: build string to sign
$date = gmdate("Y-m-d", $timestamp);
$credentialScope = $date. "/" . $service. "/tc3_request";
$hashedCanonicalRequest = hash("SHA256", $canonicalRequest);
$stringToSign = $algorithm. "\n"
.$timestamp. "\n"
.$credentialScope. "\n"
.$hashedCanonicalRequest;
echo $stringToSign.PHP_EOL;

// step 3: sign string
$secretDate = hash_hmac("SHA256", $date, "TC3". $secretKey, true);
$secretService = hash_hmac("SHA256", $service, $secretDate, true);
$secretSigning = hash_hmac("SHA256", "tc3_request", $secretService, true);
$signature = hash_hmac("SHA256", $stringToSign, $secretSigning);
echo $signature.PHP_EOL;
```

```
// step 4: build authorization
$authorization = $algorithm
." Credential=".$secretId."/".$credentialScope
.", SignedHeaders=content-type;host, Signature=".$signature;
echo $authorization.PHP_EOL;

$curl = "curl -X POST https://".$host
.' -H "Authorization: '.$authorization.'"
.' -H "Content-Type: application/json; charset=utf-8"
.' -H "Host: '.$host.'"
.' -H "X-TC-Action: '.$action.'"
.' -H "X-TC-Timestamp: '.$timestamp.'"
.' -H "X-TC-Version: '.$version.'"
.' -H "X-TC-Region: '.$region.'"
." -d ".$payload."";
echo $curl.PHP_EOL;
```

Ruby

```
# -*- coding: UTF-8 -*-
# require ruby>=2.3.0
require 'digest'
require 'json'
require 'time'
require 'openssl'

# Key Parameters
secret_id = 'AKIDz8krbsJ5yKBZQpn74WFkmLPx3*****'
secret_key = 'Gu5t9xGARNpq86cd98joQYCN3*****'

service = 'cvm'
host = 'cvm.tencentcloudapi.com'
endpoint = 'https://' + host
region = 'ap-guangzhou'
action = 'DescribeInstances'
version = '2017-03-12'
algorithm = 'TC3-HMAC-SHA256'
# timestamp = Time.now.to_i
timestamp = 1551113065
date = Time.at(timestamp).utc.strftime('%Y-%m-%d')

# ***** Step 1: Concatenate the CanonicalRequest string *****
http_request_method = 'POST'
canonical_uri = '/'
canonical_querystring = ''
```

```
canonical_headers = "content-type:application/json; charset=utf-8\nhost:#{host}\n"
signed_headers = 'content-type;host'
# params = { 'Limit' => 1, 'Filters' => [{ 'Name' => 'instance-name', 'Values' =>
['unnamed'] }] }
# payload = JSON.generate(params, { 'ascii_only' => true, 'space' => ' ' })
# json will generate in random order, to get specified result in example, we hard
-code it here.
payload = '{"Limit": 1, "Filters": [{"Values": ["unnamed"], "Name": "instance-nam
e"}]}'
hashed_request_payload = Digest::SHA256.hexdigest(payload)
canonical_request = [
http_request_method,
canonical_uri,
canonical_querystring,
canonical_headers,
signed_headers,
hashed_request_payload,
].join("\n")

puts canonical_request

# ***** Step 2: Concatenate the string to sign *****
credential_scope = date + '/' + service + '/' + 'tc3_request'
hashed_request_payload = Digest::SHA256.hexdigest(canonical_request)
string_to_sign = [
algorithm,
timestamp.to_s,
credential_scope,
hashed_request_payload,
].join("\n")
puts string_to_sign

# ***** Step 3: Calculate the Signature *****
digest = OpenSSL::Digest.new('sha256')
secret_date = OpenSSL::HMAC.digest(digest, 'TC3' + secret_key, date)
secret_service = OpenSSL::HMAC.digest(digest, secret_date, service)
secret_signing = OpenSSL::HMAC.digest(digest, secret_service, 'tc3_request')
signature = OpenSSL::HMAC.hexdigest(digest, secret_signing, string_to_sign)
puts signature

# ***** Step 4: Concatenate the Authorization *****
authorization = "#{algorithm} Credential=#{secret_id}/#{credential_scope}, Signed
Headers=#{signed_headers}, Signature=#{signature}"
puts authorization

puts 'curl -X POST ' + endpoint \
```

```
+ ' -H "Authorization: ' + authorization + "' \n\n+ ' -H "Content-Type: application/json; charset=utf-8"' \n\n+ ' -H "Host: ' + host + "' \n\n+ ' -H "X-TC-Action: ' + action + "' \n\n+ ' -H "X-TC-Timestamp: ' + timestamp.to_s + "' \n\n+ ' -H "X-TC-Version: ' + version + "' \n\n+ ' -H "X-TC-Region: ' + region + "' \n\n+ " -d '" + payload + "'"
```

DotNet

```
using System;\nusing System.Collections.Generic;\nusing System.Security.Cryptography;\nusing System.Text;\n\npublic class Application\n{\n    public static string SHA256Hex(string s)\n    {\n        using (SHA256 algo = SHA256.Create())\n        {\n            byte[] hashbytes = algo.ComputeHash(Encoding.UTF8.GetBytes(s));\n            StringBuilder builder = new StringBuilder();\n            for (int i = 0; i < hashbytes.Length; ++i)\n            {\n                builder.Append(hashbytes[i].ToString("x2"));\n            }\n            return builder.ToString();\n        }\n    }\n\n    public static byte[] HmacSHA256(byte[] key, byte[] msg)\n    {\n        using (HMACSHA256 mac = new HMACSHA256(key))\n        {\n            return mac.ComputeHash(msg);\n        }\n    }\n\n    public static Dictionary<String, String> BuildHeaders(string secretid,\n        string secretkey, string service, string endpoint, string region,\n        string action, string version, DateTime date, string requestPayload)\n    {\n        string datestr = date.ToString("yyyy-MM-dd");\n        DateTime startTime = new DateTime(1970, 1, 1, 0, 0, 0, 0, DateTimeKind.Utc);\n        long requestTimestamp = (long)Math.Round((date - startTime).TotalMilliseconds, Mi
```

```
dpointRounding.AwayFromZero) / 1000;
// ***** Step 1: Concatenate the CanonicalRequest string *****
string algorithm = "TC3-HMAC-SHA256";
string httpRequestMethod = "POST";
string canonicalUri = "/";
string canonicalQueryString = "";
string contentType = "application/json";
string canonicalHeaders = "content-type:" + contentType + "; charset=utf-8\n" +
"host:" + endpoint + "\n";
string signedHeaders = "content-type;host";
string hashedRequestPayload = SHA256Hex(requestPayload);
string canonicalRequest = httpRequestMethod + "\n"
+ canonicalUri + "\n"
+ canonicalQueryString + "\n"
+ canonicalHeaders + "\n"
+ signedHeaders + "\n"
+ hashedRequestPayload;
Console.WriteLine(canonicalRequest);
Console.WriteLine("-----");

// ***** Step 2: Concatenate the string to sign *****
string credentialScope = datestr + "/" + service + "/" + "tc3_request";
string hashedCanonicalRequest = SHA256Hex(canonicalRequest);
string stringToSign = algorithm + "\n" + requestTimestamp.ToString() + "\n" + cre
dentialScope + "\n" + hashedCanonicalRequest;
Console.WriteLine(stringToSign);
Console.WriteLine("-----");

// ***** Step 3: Calculate the signature *****
byte[] tc3SecretKey = Encoding.UTF8.GetBytes("TC3" + secretkey);
byte[] secretDate = HmacSHA256(tc3SecretKey, Encoding.UTF8.GetBytes(datestr));
byte[] secretService = HmacSHA256(secretDate, Encoding.UTF8.GetBytes(service));
byte[] secretSigning = HmacSHA256(secretService, Encoding.UTF8.GetBytes("tc3_requ
est"));
byte[] signatureBytes = HmacSHA256(secretSigning, Encoding.UTF8.GetBytes(stringTo
Sign));
string signature = BitConverter.ToString(signatureBytes).Replace("-", "").ToLower
();
Console.WriteLine(signature);
Console.WriteLine("-----");

// ***** Step 4: Concatenate the Authorization *****
string authorization = algorithm + " "
+ "Credential=" + secretid + "/" + credentialScope + ", "
+ "SignedHeaders=" + signedHeaders + ", "
+ "Signature=" + signature;
Console.WriteLine(authorization);
```

```
Console.WriteLine("-----");

Dictionary<string, string> headers = new Dictionary<string, string>();
headers.Add("Authorization", authorization);
headers.Add("Host", endpoint);
headers.Add("Content-Type", contentType + "; charset=utf-8");
headers.Add("X-TC-Timestamp", requestTimestamp.ToString());
headers.Add("X-TC-Version", version);
headers.Add("X-TC-Action", action);
headers.Add("X-TC-Region", region);
return headers;
}

public static void Main(string[] args)
{
    // SecretID and SecretKey
    string SECRET_ID = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3*****";
    string SECRET_KEY = "Gu5t9xGARNpq86cd98joQYCN3*****";

    string service = "cvm";
    string endpoint = "cvm.tencentcloudapi.com";
    string region = "ap-guangzhou";
    string action = "DescribeInstances";
    string version = "2017-03-12";

    // The timestamp `2019-02-26 00:44:25` used here is only for reference. In a project, use the following parameter:
    // DateTime date = DateTime.UtcNow;
    // Enter the correct time zone. We recommend using UTC timestamp to avoid errors.
    DateTime date = new DateTime(1970, 1, 1, 0, 0, 0, 0, DateTimeKind.Utc).AddSeconds(1551113065);
    string requestPayload = "{\"Limit\": 1, \"Filters\": [{\"Values\": [\"\\u672a\\u547d\\u540d\"], \"Name\": \"instance-name\"}]}";

    Dictionary<string, string> headers = BuildHeaders(SECRET_ID, SECRET_KEY, service, endpoint, region, action, version, date, requestPayload);

    Console.WriteLine("POST https://cvm.tencentcloudapi.com");
    foreach (KeyValuePair<string, string> kv in headers)
    {
        Console.WriteLine(kv.Key + ": " + kv.Value);
    }
    Console.WriteLine();
    Console.WriteLine(requestPayload);
}
```

NodeJS

```
const crypto = require('crypto');

function sha256(message, secret = '', encoding) {
  const hmac = crypto.createHmac('sha256', secret)
  return hmac.update(message).digest(encoding)
}

function getHash(message, encoding = 'hex') {
  const hash = crypto.createHash('sha256')
  return hash.update(message).digest(encoding)
}

function getDate(timestamp) {
  const date = new Date(timestamp * 1000)
  const year = date.getUTCFullYear()
  const month = ('0' + (date.getUTCMonth() + 1)).slice(-2)
  const day = ('0' + date.getUTCDate()).slice(-2)
  return `${year}-${month}-${day}`
}

function main() {

  const SECRET_ID = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3*****"
  const SECRET_KEY = "Gu5t9xGARNpq86cd98joQYCN3*****"

  const endpoint = "cvm.tencentcloudapi.com"
  const service = "cvm"
  const region = "ap-guangzhou"
  const action = "DescribeInstances"
  const version = "2017-03-12"
  //const timestamp = getTime()
  const timestamp = 1551113065
  const date = getDate(timestamp)

  // ***** Step 1: Concatenate the CanonicalRequest string *****
  const signedHeaders = "content-type;host"

  const payload = "{\"Limit\": 1, \"Filters\": [{\"Values\": [\"unnamed\"], \"Name\": \"instance-name\"}]}"

  const hashedRequestPayload = getHash(payload);
  const httpRequestMethod = "POST"
  const canonicalUri = "/"
  const canonicalQueryString = ""
  const canonicalHeaders = "content-type:application/json; charset=utf-8\n" + "host:" + endpoint + "\n"

  const canonicalRequest = httpRequestMethod + "\n"
```

```
+ canonicalUri + "\n"
+ canonicalQueryString + "\n"
+ canonicalHeaders + "\n"
+ signedHeaders + "\n"
+ hashedRequestPayload
console.log(canonicalRequest)
console.log("-----")

// ***** Step 2: Concatenate the string to sign *****
const algorithm = "TC3-HMAC-SHA256"
const hashedCanonicalRequest = getHash(canonicalRequest);
const credentialScope = date + "/" + service + "/" + "tc3_request"
const stringToSign = algorithm + "\n" +
timestamp + "\n" +
credentialScope + "\n" +
hashedCanonicalRequest
console.log(stringToSign)
console.log("-----")

// ***** Step 3: Calculate the signature *****
const kDate = sha256(date, 'TC3' + SECRET_KEY)
const kService = sha256(service, kDate)
const kSigning = sha256('tc3_request', kService)
const signature = sha256(stringToSign, kSigning, 'hex')
console.log(signature)
console.log("-----")

// ***** Step 4: Concatenate the Authorization *****
const authorization = algorithm + " " +
"Credential=" + SECRET_ID + "/" + credentialScope + ", " +
"SignedHeaders=" + signedHeaders + ", " +
"Signature=" + signature
console.log(authorization)
console.log("-----")

const Call_Information = 'curl -X POST ' + "https://" + endpoint
+ ' -H "Authorization: ' + authorization + '"'
+ ' -H "Content-Type: application/json; charset=utf-8"'
+ ' -H "Host: ' + endpoint + '"'
+ ' -H "X-TC-Action: ' + action + '"'
+ ' -H "X-TC-Timestamp: ' + timestamp.toString() + '"'
+ ' -H "X-TC-Version: ' + version + '"'
+ ' -H "X-TC-Region: ' + region + '"'
+ " -d '" + payload + '"'
console.log(Call_Information)
}
main()
```

C++

```
#include <iostream>
#include <iomanip>
#include <sstream>
#include <string>
#include <stdio.h>
#include <time.h>
#include <openssl/sha.h>
#include <openssl/hmac.h>

using namespace std;

string get_data(int64_t &timestamp)
{
    string utcDate;
    char buff[20] = {0};
    // time_t timenow;
    struct tm sttime;
    sttime = *gmtime(&timestamp);
    strftime(buff, sizeof(buff), "%Y-%m-%d", &sttime);
    utcDate = string(buff);
    return utcDate;
}

string int2str(int64_t n)
{
    std::stringstream ss;
    ss << n;
    return ss.str();
}

string sha256Hex(const string &str)
{
    char buf[3];
    unsigned char hash[SHA256_DIGEST_LENGTH];
    SHA256_CTX sha256;
    SHA256_Init(&sha256);
    SHA256_Update(&sha256, str.c_str(), str.size());
    SHA256_Final(hash, &sha256);
    std::string NewString = "";
    for(int i = 0; i < SHA256_DIGEST_LENGTH; i++)
    {
        sprintf(buf, sizeof(buf), "%02x", hash[i]);
        NewString = NewString + buf;
    }
    return NewString;
}
```

```
}  
  
string HmacSha256(const string &key, const string &input)  
{  
    unsigned char hash[32];  
  
    HMAC_CTX *h;  
    #if OPENSSL_VERSION_NUMBER < 0x10100000L  
    HMAC_CTX hmac;  
    HMAC_CTX_init(&hmac);  
    h = &hmac;  
    #else  
    h = HMAC_CTX_new();  
    #endif  
  
    HMAC_Init_ex(h, &key[0], key.length(), EVP_sha256(), NULL);  
    HMAC_Update(h, ( unsigned char* )&input[0], input.length());  
    unsigned int len = 32;  
    HMAC_Final(h, hash, &len);  
  
    #if OPENSSL_VERSION_NUMBER < 0x10100000L  
    HMAC_CTX_cleanup(h);  
    #else  
    HMAC_CTX_free(h);  
    #endif  
  
    std::stringstream ss;  
    ss << std::setfill('0');  
    for (int i = 0; i < len; i++)  
    {  
        ss << hash[i];  
    }  
  
    return (ss.str());  
}  
  
string HexEncode(const string &input)  
{  
    static const char* lut = "0123456789abcdef";  
    size_t len = input.length();  
  
    string output;  
    output.reserve(2 * len);  
    for (size_t i = 0; i < len; ++i)  
    {  
        const unsigned char c = input[i];  
        output.push_back(lut[c >> 4]);  
        output.push_back(lut[c & 15]);  
    }  
}
```

```
return output;
}

int main()
{
    string SECRET_ID = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3*****";
    string SECRET_KEY = "Gu5t9xGARNpq86cd98joQYCN3*****";

    string service = "cvm";
    string host = "cvm.tencentcloudapi.com";
    string region = "ap-guangzhou";
    string action = "DescribeInstances";
    string version = "2017-03-12";
    int64_t timestamp = 1551113065;
    string date = get_data(timestamp);

    // ***** Step 1: Concatenate the CanonicalRequest string *****
    string httpRequestMethod = "POST";
    string canonicalUri = "/";
    string canonicalQueryString = "";
    string canonicalHeaders = "content-type:application/json; charset=utf-8\nhost:" +
    host + "\n";
    string signedHeaders = "content-type;host";
    string payload = "{\"Limit\": 1, \"Filters\": [{\"Values\": [\"unnamed\"], \"Name\": \"instance-name\"}] }";
    string hashedRequestPayload = sha256Hex(payload);
    string canonicalRequest = httpRequestMethod + "\n" + canonicalUri + "\n" + canonicalQueryString + "\n"
    + canonicalHeaders + "\n" + signedHeaders + "\n" + hashedRequestPayload;
    cout << canonicalRequest << endl;
    cout << "-----" << endl;

    // ***** Step 2: Concatenate the string to sign *****
    string algorithm = "TC3-HMAC-SHA256";
    string RequestTimestamp = int2str(timestamp);
    string credentialScope = date + "/" + service + "/" + "tc3_request";
    string hashedCanonicalRequest = sha256Hex(canonicalRequest);
    string stringToSign = algorithm + "\n" + RequestTimestamp + "\n" + credentialScope + "\n" + hashedCanonicalRequest;
    cout << stringToSign << endl;
    cout << "-----" << endl;

    // ***** Step 3: Calculate the signature *****
    string kKey = "TC3" + SECRET_KEY;
    string kDate = HmacSha256(kKey, date);
    string kService = HmacSha256(kDate, service);
    string kSigning = HmacSha256(kService, "tc3_request");
```

```
string signature = HexEncode(HmacSha256(kSigning, stringToSign));
cout << signature << endl;
cout << "-----" << endl;

// ***** Step 4: Concatenate the Authorization *****
string authorization = algorithm + " " + "Credential=" + SECRET_ID + "/" + creden
tialScope + ", "
+ "SignedHeaders=" + signedHeaders + ", " + "Signature=" + signature;
cout << authorization << endl;
cout << "-----" << endl;

string headers = "curl -X POST https://" + host + "\n"
+ " -H \"Authorization: \" + authorization + "\n"
+ " -H \"Content-Type: application/json; charset=utf-8\"" + "\n"
+ " -H \"Host: \" + host + "\n"
+ " -H \"X-TC-Action: \" + action + "\n"
+ " -H \"X-TC-Timestamp: \" + RequestTimestamp + "\n"
+ " -H \"X-TC-Version: \" + version + "\n"
+ " -H \"X-TC-Region: \" + region + "\n"
+ " -d '" + payload;
cout << headers << endl;
return 0;
};
```

Signature Failure

The following situational error codes for signature failure may occur. Please resolve the errors accordingly.

Error Code	Description
AuthFailure.SignatureExpire	Signature expired. Timestamp and server time cannot differ by more than five minutes.
AuthFailure.SecretIdNotFound	The key does not exist. Please go to the console to check whether it is disabled or you copied fewer or more characters.
AuthFailure.SignatureFailure	Signature error. It is possible that the signature was calculated incorrectly, the signature does not match the content actually sent, or the SecretKey is incorrect.
AuthFailure.TokenFailure	Temporary certificate token error.
AuthFailure.InvalidSecretId	Invalid key (not a TencentCloud API key type).

Signature

最近更新时间：2021-10-13 15:26:06

Tencent Cloud API authenticates each access request, i.e. each request needs to include authentication information (Signature) in the common parameters to verify the identity of the requester.

The Signature is generated by the security credentials which include SecretId and SecretKey. If you don't have the security credentials yet, go to the [TencentCloud API Key](#) page to apply for them; otherwise, you cannot invoke the TencentCloud API.

1. Applying for Security Credentials

Before using the TencentCloud API for the first time, go to the [TencentCloud API Key](#) page to apply for security credentials.

Security credentials consist of SecretId and SecretKey:

- SecretId is used to identify the API requester.
- SecretKey is used to encrypt the signature string and verify it on the server.
- **You must keep your security credentials private and avoid disclosure.**

You can apply for the security credentials through the following steps:

1. Log in to the [Tencent Cloud Console](#).
2. Go to the [TencentCloud API Key](#) page.
3. On the [API Key Management](#) page, click **Create Key** to create a SecretId/SecretKey pair.

Note: Each account can have up to two pairs of SecretId/SecretKey.

2. Generating a Signature

With the SecretId and SecretKey, a signature can be generated. The following describes how to generate a signature:

Assume that the SecretId and SecretKey are:

- SecretId: AKIDz8krbsJ5yKBZQpn74WFkmLPx3*****
- SecretKey: Gu5t9xGARNpq86cd98joQYCN3*****

Note: This is just an example. For actual operations, please use your own SecretId and SecretKey.

Take the Cloud Virtual Machine's request to view the instance list (DescribeInstances) as an example. When you invoke this API, the request parameters may be as follows:

Parameter name	Description	Parameter value
Action	Method name	DescribeInstances
SecretId	Key ID	AKIDz8krbsJ5yKBZQpn74WFkmLPx3*****
Timestamp	Current timestamp	1465185768
Nonce	Random positive integer	11886
Region	Region where the instance is located	ap-guangzhou
InstanceIds.0	ID of the instance to query	ins-09dx96dg
Offset	Offset	0
Limit	Allowed maximum output	20
Version	API version number	2017-03-12

2.1. Sorting Parameters

First, sort all the request parameters in an ascending lexicographical order (ASCII code) by their names. Notes: (1) Parameters are sorted by their names instead of their values; (2) The parameters are sorted based on ASCII code, not in an alphabetical order or by values. For example, InstanceIds.2 should be arranged after InstanceIds.12. You can complete the sorting process using a sorting function in a programming language, such as the ksort function in PHP. The parameters in the example are sorted as follows:

```
{
  'Action' : 'DescribeInstances',
  'InstanceIds.0' : 'ins-09dx96dg',
  'Limit' : 20,
  'Nonce' : 11886,
  'Offset' : 0,
  'Region' : 'ap-guangzhou',
  'SecretId' : 'AKIDz8krbsJ5yKBZQpn74WFkmLPx3*****',
  'Timestamp' : 1465185768,
  'Version': '2017-03-12',
}
```

When developing in another programming language, you can sort these sample parameters and it will work as long as you obtain the same results.

2.2. Concatenating a Request String

This step generates a request string.

Format the request parameters sorted in the previous step into the form of "parameter name"="parameter value". For example, for the Action parameter, its parameter name is "Action" and its parameter value is "DescribeInstances", so it will become Action=DescribeInstances after formatted.

Note: The "parameter value" is the original value but not the value after URL encoding.

Then, concatenate the formatted parameters with "&". The resulting request string is as follows:

```
Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0
&Region=ap-guangzhou&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3*****&Timestamp=1465
185768&Version=2017-03-12
```

2.3. Concatenating the Signature Original String

This step generates a signature original string.

The signature original string consists of the following parameters:

1. HTTP method: POST and GET modes are supported, and GET is used here for the request. Please note that the method name should be in all capital letters.
2. Request server: the domain name of the request to view the list of instances (DescribeInstances) is cvm.tencentcloudapi.com. The actual request domain name varies by the module to which the API belongs. For more information, see the instructions of the specific API.
3. Request path: The request path in the current version of TencentCloud API is fixed to /.
4. Request string: the request string generated in the previous step.

The concatenation rule of the signature original string is: Request method + request host + request path + ? + request string

The concatenation result of the example is:

```
GETcvm.tencentcloudapi.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&L
imit=20&Nonce=11886&Offset=0&Region=ap-guangzhou&SecretId=AKIDz8krbsJ5yKBZQpn74WF
kmLPx3*****&Timestamp=1465185768&Version=2017-03-12
```

2.4. Generating a Signature String

This step generates a signature string.

First, use the HMAC-SHA1 algorithm to sign the **signature original string** obtained in the previous step, and then

encode the generated signature using Base64 to obtain the final signature.

The specific code is as follows with the PHP language being used as an example:

```
$secretKey = 'Gu5t9xGARNpq86cd98joQYCN3*****';  
$srcStr = 'GETcvm.tencentcloudapi.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=ap-guangzhou&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3*****&Timestamp=1465185768&Version=2017-03-12';  
$signStr = base64_encode(hash_hmac('sha1', $srcStr, $secretKey, true));  
echo $signStr;
```

The final signature is:

```
zmmjn35mikh6pM3V7sUEuX4wyYM=
```

When developing in another programming language, you can sign and verify the original in the example above and it works as long as you get the same results.

3. Encoding a Signature String

The generated signature string cannot be directly used as a request parameter and must be URL encoded.

For example, if the signature string generated in the previous step is zmmjn35mikh6pM3V7sUEuX4wyYM=, the final signature string request parameter (Signature) is zmmjn35mikh6pM3V7sUEuX4wyYM%3D, which will be used to generate the final request URL.

Note: If your request method is GET, or the request method is POST and the Content-Type is application/x-www-form-urlencoded, then all the request parameter values need to be URL encoded (except the parameter key and the symbol of =) when sending the request. Non-ASCII characters need to be encoded with UTF-8 before URL encoding.

Note: The network libraries of some programming languages automatically URL encode all parameters, in which case there is no need to URL encode the signature string; otherwise, two rounds of URL encoding will cause the signature to fail.

Note: Other parameter values also need to be encoded using [RFC 3986](#). Use %XY in percent-encoding for special characters such as Chinese characters, where "X" and "Y" are hexadecimal characters (0-9 and uppercase A-F), and using lowercase will cause an error.

4. Signature Failure

The following situational error codes for signature failure may occur. Please resolve the errors accordingly.

Error code	Error description
AuthFailure.SignatureExpire	The signature is expired
AuthFailure.SecretIdNotFound	The key does not exist
AuthFailure.SignatureFailure	Signature error
AuthFailure.TokenFailure	Token error
AuthFailure.InvalidSecretId	Invalid key (not a TencentCloud API key type)

5. Signature Demo

When calling API 3.0, you are recommended to use the corresponding Tencent Cloud SDK 3.0 which encapsulates the signature process, enabling you to focus on only the specific APIs provided by the product when developing. See [SDK Center](#) for more information. Currently, the following programming languages are supported:

- [Python](#)
- [Java](#)
- [PHP](#)
- [Go](#)
- [NodeJS](#)
- [.NET](#)

To further explain the signing process, we will use a programming language to implement the process described above. The request domain name, API and parameter values in the sample are used here. This goal of this example is only to provide additional clarification for the signature process, please see the SDK for actual usage.

The final output URL might be:

```
https://cvm.tencentcloudapi.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=ap-guangzhou&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3*****&Signature=zmmjn35mikh6pM3V7sUEuX4wyYM%3D&Timestamp=1465185768&Version=2017-03-12
```

Note: The key in the example is fictitious, and the timestamp is not the current time of the system, so if this URL is opened in the browser or called using commands such as curl, an authentication error will be returned: Signature expired. In order to get a URL that can work properly, you need to replace the SecretId and SecretKey in the example with your real credentials and use the current time of the system as the Timestamp.

Note: In the example below, even if you use the same programming language, the order of the parameters in the URL may be different for each execution. However, the order does not matter, as long as all the parameters are included in the URL and the signature is calculated correctly.

Note: The following code is only applicable to API 3.0. It cannot be directly used in other signature processes. Even with an older API, signature calculation errors may occur due to the differences in details. Please refer to the corresponding documentation.

Java

```
import java.io.UnsupportedEncodingException;
import java.net.URLEncoder;
import java.util.Random;
import java.util.TreeMap;
import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
import javax.xml.bind.DatatypeConverter;

public class TencentCloudAPIDemo {
    private final static String CHARSET = "UTF-8";

    public static String sign(String s, String key, String method) throws Exception {
        Mac mac = Mac.getInstance(method);
        SecretKeySpec secretKeySpec = new SecretKeySpec(key.getBytes(CHARSET), mac.getAlgorithm());
        mac.init(secretKeySpec);
        byte[] hash = mac.doFinal(s.getBytes(CHARSET));
        return DatatypeConverter.printBase64Binary(hash);
    }

    public static String getStringToSign(TreeMap<String, Object> params) {
        StringBuilder s2s = new StringBuilder("GETcvm.tencentcloudapi.com/?");
        // When signing, the parameters need to be sorted in lexicographical order. TreeMap is used here to guarantee the correct order.
        for (String k : params.keySet()) {
            s2s.append(k).append("=").append(params.get(k).toString()).append("&");
        }
        return s2s.toString().substring(0, s2s.length() - 1);
    }

    public static String getUrl(TreeMap<String, Object> params) throws UnsupportedEncodingException {
        StringBuilder url = new StringBuilder("https://cvm.tencentcloudapi.com/?");
        // There is no requirement for the order of the parameters in the actual request URL.
        for (String k : params.keySet()) {
            // The request string needs to be URL encoded. As the Key is all in English letters, only the value is URL encoded here.
            url.append(k).append("=").append(URLEncoder.encode(params.get(k).toString(), CHARSET)).append("&");
        }
    }
}
```

```
}
return url.toString().substring(0, url.length() - 1);
}
public static void main(String[] args) throws Exception {
    TreeMap<String, Object> params = new TreeMap<String, Object>(); // TreeMap enables automatic sorting
    // A random number should be used when actually calling, for example: params.put("Nonce", new Random().nextInt(Integer.MAX_VALUE));
    params.put("Nonce", 11886); // Common parameter
    // The current time of the system should be used when actually calling, for example: params.put("Timestamp", System.currentTimeMillis() / 1000);
    params.put("Timestamp", 1465185768); // Common parameter
    params.put("SecretId", "AKIDz8krbsJ5yKBZQpn74WFkmLPx3*****"); // Common parameter
    params.put("Action", "DescribeInstances"); // Common parameter
    params.put("Version", "2017-03-12"); // Common parameter
    params.put("Region", "ap-guangzhou"); // Common parameter
    params.put("Limit", 20); // Business parameter
    params.put("Offset", 0); // Business parameter
    params.put("InstanceIds.0", "ins-09dx96dg"); // Business parameter
    params.put("Signature", sign(getStringToSign(params), "Gu5t9xGARNpq86cd98joQYCN3*****", "HmacSHA1")); // Common parameter
    System.out.println(getUrl(params));
}
}
```

Python

Note: If running in a Python 2 environment, the following requests dependency package must be installed first: `pip install requests`.

```
# -*- coding: utf8 -*-
import base64
import hashlib
import hmac
import time
import requests

secret_id = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3*****"
secret_key = "Gu5t9xGARNpq86cd98joQYCN3*****"

def get_string_to_sign(method, endpoint, params):
    s = method + endpoint + "?"
    query_str = "&".join("%s=%s" % (k, params[k]) for k in sorted(params))
    return s + query_str

def sign_str(key, s, method):
    hmac_str = hmac.new(key.encode("utf8"), s.encode("utf8"), method).digest()
    return base64.b64encode(hmac_str)
```

```
if __name__ == '__main__':
    endpoint = "cvm.tencentcloudapi.com"
    data = {
        'Action': 'DescribeInstances',
        'InstanceIds.0': 'ins-09dx96dg',
        'Limit': 20,
        'Nonce': 11886,
        'Offset': 0,
        'Region': 'ap-guangzhou',
        'SecretId': secret_id,
        'Timestamp': 1465185768, # int(time.time())
        'Version': '2017-03-12'
    }
    s = get_string_to_sign("GET", endpoint, data)
    data["Signature"] = sign_str(secret_key, s, hashlib.sha1)
    print(data["Signature"])
    # An actual invocation would occur here, which may incur fees after success
    # resp = requests.get("https://" + endpoint, params=data)
    # print(resp.url)
```

Golang

```
package main
import (
    "bytes"
    "crypto/hmac"
    "crypto/sha1"
    "encoding/base64"
    "fmt"
    "sort"
)
func main() {
    secretId := "AKIDz8krbsJ5yKBZQpn74WFkmLPx3*****"
    secretKey := "Gu5t9xGARNpq86cd98joQYCN3*****"
    params := map[string]string{
        "Nonce": "11886",
        "Timestamp": "1465185768",
        "Region": "ap-guangzhou",
        "SecretId": secretId,
        "Version": "2017-03-12",
        "Action": "DescribeInstances",
        "InstanceIds.0": "ins-09dx96dg",
        "Limit": "20",
        "Offset": "0",
    }
    var buf bytes.Buffer
```

```
buf.WriteString("GET")
buf.WriteString("cvm.tencentcloudapi.com")
buf.WriteString("/")
buf.WriteString("?")
// sort keys by ascii asc order
keys := make([]string, 0, len(params))
for k, _ := range params {
    keys = append(keys, k)
}
sort.Strings(keys)
for i := range keys {
    k := keys[i]
    buf.WriteString(k)
    buf.WriteString("=")
    buf.WriteString(params[k])
    buf.WriteString("&")
}
buf.Truncate(buf.Len() - 1)
hashed := hmac.New(sha1.New, []byte(secretKey))
hashed.Write(buf.Bytes())
fmt.Println(base64.StdEncoding.EncodeToString(hashed.Sum(nil)))
}
```

PHP

```
<?php
$secretId = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3*****";
$secretKey = "Gu5t9xGARNpq86cd98joQYCN3*****";
$params["Nonce"] = 11886;//rand();
$params["Timestamp"] = 1465185768;//time();
$params["Region"] = "ap-guangzhou";
$params["SecretId"] = $secretId;
$params["Version"] = "2017-03-12";
$params["Action"] = "DescribeInstances";
$params["InstanceIds.0"] = "ins-09dx96dg";
$params["Limit"] = 20;
$params["Offset"] = 0;
ksort($params);
$signStr = "GETcvm.tencentcloudapi.com/?";
foreach ( $params as $key => $value ) {
    $signStr = $signStr . $key . "=" . $value . "&";
}
$signStr = substr($signStr, 0, -1);
$signature = base64_encode(hash_hmac("sha1", $signStr, $secretKey, true));
echo $signature.PHP_EOL;
// need to install and enable curl extension in php.ini
```

```
// $param["Signature"] = $signature;
// $url = "https://cvm.tencentcloudapi.com/?".http_build_query($param);
// echo $url.PHP_EOL;
// $ch = curl_init();
// curl_setopt($ch, CURLOPT_URL, $url);
// $output = curl_exec($ch);
// curl_close($ch);
// echo json_decode($output);
```

Ruby

```
# -*- coding: UTF-8 -*-
# require ruby>=2.3.0
require 'time'
require 'openssl'
require 'base64'
secret_id = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3*****"
secret_key = "Gu5t9xGARNpq86cd98joQYCN3*****"
method = 'GET'
endpoint = 'cvm.tencentcloudapi.com'
data = {
  'Action' => 'DescribeInstances',
  'InstanceIds.0' => 'ins-09dx96dg',
  'Limit' => 20,
  'Nonce' => 11886,
  'Offset' => 0,
  'Region' => 'ap-guangzhou',
  'SecretId' => secret_id,
  'Timestamp' => 1465185768, # Time.now.to_i
  'Version' => '2017-03-12',
}
sign = method + endpoint + '/*?'
params = []
data.sort.each do |item|
  params << "#{item[0]}=#{item[1]}"
end
sign += params.join('&')
digest = OpenSSL::Digest.new('sha1')
data['Signature'] = Base64.encode64(OpenSSL::HMAC.digest(digest, secret_key, sign))
puts data['Signature']
# require 'net/http'
# uri = URI('https://' + endpoint)
# uri.query = URI.encode_www_form(data)
# p uri
```

```
# res = Net::HTTP.get_response(uri)
# puts res.body
```

DotNet

```
using System;
using System.Collections.Generic;
using System.Net;
using System.Security.Cryptography;
using System.Text;
public class Application {
public static string Sign(string signKey, string secret)
{
string signRet = string.Empty;
using (HMACSHA1 mac = new HMACSHA1(Encoding.UTF8.GetBytes(signKey)))
{
byte[] hash = mac.ComputeHash(Encoding.UTF8.GetBytes(secret));
signRet = Convert.ToBase64String(hash);
}
return signRet;
}
public static string MakeSignPlainText(SortedDictionary<string, string> requestParams, string requestMethod, string requestHost, string requestPath)
{
string retStr = "";
retStr += requestMethod;
retStr += requestHost;
retStr += requestPath;
retStr += "?";
string v = "";
foreach (string key in requestParams.Keys)
{
v += string.Format("{0}={1}&", key, requestParams[key]);
}
retStr += v.TrimEnd('&');
return retStr;
}
public static void Main(string[] args)
{
string SECRET_ID = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3*****";
string SECRET_KEY = "Gu5t9xGARNpq86cd98joQYCN3*****";
string endpoint = "cvm.tencentcloudapi.com";
string region = "ap-guangzhou";
string action = "DescribeInstances";
string version = "2017-03-12";
double RequestTimestamp = 1465185768;
```

```
// long timestamp = ToTimestamp() / 1000;
// string requestTimestamp = timestamp.ToString();
Dictionary<string, string> param = new Dictionary<string, string>();
param.Add("Limit", "20");
param.Add("Offset", "0");
param.Add("InstanceIds.0", "ins-09dx96dg");
param.Add("Action", action);
param.Add("Nonce", "11886");
// param.Add("Nonce", Math.Abs(new Random().Next()).ToString());
param.Add("Timestamp", RequestTimestamp.ToString());
param.Add("Version", version);
param.Add("SecretId", SECRET_ID);
param.Add("Region", region);
SortedDictionary<string, string> headers = new SortedDictionary<string, string>(p
aram, StringComparer.Ordinal);
string sigInParam = MakeSignPlainText(headers, "GET", endpoint, "/");
Console.WriteLine(sigInParam);
string sigOutParam = Sign(SECRET_KEY, sigInParam);
Console.WriteLine("GET https://cvm.tencentcloudapi.com");
foreach (KeyValuePair<string, string> kv in headers)
{
    Console.WriteLine(kv.Key + ": " + kv.Value);
}
Console.WriteLine("Signature" + ": " + WebUtility.UrlEncode(sigOutParam));
Console.WriteLine();
string result = "https://cvm.tencentcloudapi.com/?";
foreach (KeyValuePair<string, string> kv in headers)
{
    result += WebUtility.UrlEncode(kv.Key) + "=" + WebUtility.UrlEncode(kv.Value) +
"&";
}
result += WebUtility.UrlEncode("Signature") + "=" + WebUtility.UrlEncode(sigOutPa
ram);
Console.WriteLine("GET " + result);
}
}
```

NodeJS

```
const crypto = require('crypto');
function get_req_url(params, endpoint){
    params['Signature'] = escape(params['Signature']);
    const url_strParam = sort_params(params)
    return "https://" + endpoint + "/" + url_strParam.slice(1);
}
function formatSignString(reqMethod, endpoint, path, strParam){
```

```
let strSign = reqMethod + endpoint + path + "?" + strParam.slice(1);
return strSign;
}
function sha1(secretKey, strsign){
let signMethodMap = {'HmacSHA1': "sha1"};
let hmac = crypto.createHmac(signMethodMap['HmacSHA1'], secretKey || "");
return hmac.update(Buffer.from(strsign, 'utf8')).digest('base64')
}
function sort_params(params) {
let strParam = "";
let keys = Object.keys(params);
keys.sort();
for (let k in keys) {
//k = k.replace(/_/g, '.');
strParam += ("&" + keys[k] + "=" + params[keys[k]]);
}
return strParam
}
function main() {
const SECRET_ID = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3*****"
const SECRET_KEY = "Gu5t9xGARNpq86cd98joQYCN3*****"
const endpoint = "cvm.tencentcloudapi.com"
const Region = "ap-guangzhou"
const Version = "2017-03-12"
const Action = "DescribeInstances"
const Timestamp = 1465185768
// const Timestamp = Math.round(Date.now() / 1000)
const Nonce = 11886
//const nonce = Math.round(Math.random() * 65535)
let params = {};
params['Action'] = Action;
params['InstanceIds.0'] = 'ins-09dx96dg';
params['Limit'] = 20;
params['Offset'] = 0;
params['Nonce'] = Nonce;
params['Region'] = Region;
params['SecretId'] = SECRET_ID;
params['Timestamp'] = Timestamp;
params['Version'] = Version;
strParam = sort_params(params)
const reqMethod = "GET";
const path = "/";
strSign = formatSignString(reqMethod, endpoint, path, strParam)
console.log(strSign)
console.log("-----")
params['Signature'] = sha1(SECRET_KEY, strSign)
console.log(params['Signature'])
```

```
console.log("-----")
const req_url = get_req_url(params, endpoint)
console.log(params['Signature'])
console.log("-----")
console.log(req_url)
}
main()
```

Responses

最近更新时间：2020-02-10 14:30:47

Response for Successful Requests

For example, when calling CAM API (version: 2017-03-12) to view the status of instances (DescribeInstancesStatus), if the request has succeeded, you may see the response as shown below:

```
{
  "Response": {
    "TotalCount": 0,
    "InstanceStatusSet": [],
    "RequestId": "b5b41468-520d-4192-b42f-595cc34b6c1c"
  }
}
```

- The API will return `Response`, which contains `RequestId`, as long as it processes the request. It does not matter if the request is successful or not.
- RequestId is the unique ID of an API request. Contact us with this ID when an exception occurs.
- Except for the fixed fields, all fields are action-specified. For the definitions of action-specified fields, see the corresponding API documentation. In this example, `TotalCount` and `InstanceStatusSet` are the fields specified by the API `DescribeInstancesStatus`. `0` `TotalCount` means that the requester owns 0 CVM instance so the `InstanceStatusSet` is empty.

Response for Failed Requests

If the request has failed, you may see the response as shown below:

```
{
  "Response": {
    "Error": {
      "Code": "AuthFailure.SignatureFailure",
      "Message": "The provided credentials could not be validated. Please ensure your signature is correct."
    },
    "RequestId": "ed93f3cb-f35e-473f-b9f3-0d451b8b79c6"
  }
}
```

- The presence of the `Error` field indicates that the request has failed. A response for a failed request will include `Error`, `Code` and `Message` fields.
- `Code` is the code of the error that helps you identify the cause and solution. There are two types of error codes so you may find the code in either common error codes or API-specified error codes.
- Message explains the cause of the error. Note that the returned messages are subject to service updates. The information the messages provide may not be up-to-date and should not be the only source of reference.
- RequestId is the unique ID of an API request. Contact us with this ID when an exception occurs.

Common Error Codes

If there is an Error field in the response, it means that the API call failed. The Code field in Error indicates the error code. The following table lists the common error codes that all actions can return.

Error Code	Description
AuthFailure.InvalidSecretId	Invalid key (not a TencentCloud API key type).
AuthFailure.MFAFailure	MFA failed.
AuthFailure.SecretIdNotFound	The key does not exist.
AuthFailure.SignatureExpire	Signature expired.
AuthFailure.SignatureFailure	Signature error.
AuthFailure.TokenFailure	Token error.
AuthFailure.UnauthorizedOperation	The request does not have CAM authorization.
DryRunOperation	DryRun Operation. It means that the request would have succeeded, but the DryRun parameter was used.
FailedOperation	Operation failed.
InternalError	Internal error.
InvalidAction	The API does not exist.
InvalidParameter	Incorrect parameter.
InvalidParameterValue	Invalid parameter value.
LimitExceeded	Quota limit exceeded.

Error Code	Description
MissingParameter	A parameter is missing.
NoSuchVersion	The API version does not exist.
RequestLimitExceeded	The number of requests exceeds the frequency limit.
ResourceInUse	Resource is in use.
ResourceInsufficient	Insufficient resource.
ResourceNotFound	The resource does not exist.
ResourceUnavailable	Resource is unavailable.
UnauthorizedOperation	Unauthorized operation.
UnknownParameter	Unknown parameter.
UnsupportedOperation	Unsupported operation.
UnsupportedProtocol	HTTPS request method error. Only GET and POST requests are supported.
UnsupportedRegion	API does not support the requested region.

Key APIs

PostQuantumCryptoEncrypt

最近更新时间：2023-08-07 17:45:14

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to encrypt using PQC. It supports up to 4 KB of data. It is applicable for encryption of database passwords, RSA keys, or other sensitive information. You can also apply `DataKey` generated by API `GenerateDataKey` to encrypt or decrypt your local data.

A maximum of 20 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: PostQuantumCryptoEncrypt.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
KeyId	Yes	String	Globally unique ID of the CMK generated by calling the <code>CreateKey</code> API
PlainText	Yes	String	Encrypted plaintext data. This field must be Base64-encoded. The maximum size of the original data is 4 KB.

3. Output Parameters

Parameter Name	Type	Description
CiphertextBlob	String	Base64-encoded ciphertext after encryption. This field contains the information of ciphertext and keys. It is not the result of encrypting the plaintext. To get the plaintext, you need to pass in this field to the PostQuantumCryptoDecrypt API.
KeyId	String	Globally unique ID of the CMK used for encryption
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.

4. Example

Example1 Encrypting with PQC

This example shows you how to encrypt using PQC.

Input Example

```
POST / HTTP/1.1
Host: kms.tencentcloudapi.com
Content-Type: application/json
X-TC-Action: PostQuantumCryptoEncrypt
<Common request parameters>

{
  "KeyId": "abc",
  "PlainText": "abc"
}
```

Output Example

```
{
  "Response": {
    "CiphertextBlob": "abc",
    "KeyId": "abc",
    "RequestId": "abc"
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
InternalServerError	Internal error.
InvalidParameter	Invalid parameter.
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
InvalidParameterValue.InvalidPlaintext	Invalid <code>Plaintext</code> .
ResourceUnavailable.CmkArchived	The CMK has been archived.
ResourceUnavailable.CmkDisabled	The CMK has been disabled.
ResourceUnavailable.CmkNotFound	The CMK does not exist.
UnauthorizedOperation	Unauthorized operation.

PostQuantumCryptoDecrypt

最近更新时间：2023-08-07 17:45:14

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

u200dThis API u200dis used to decrypt ciphertext using post-quantum cryptography (PQC) algorithm, and return the plaintext.

A maximum of 20 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: PostQuantumCryptoDecrypt.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
CiphertextBlob	Yes	String	The ciphertext data to be decrypted.
EncryptionPublicKey	No	String	PEM-encoded public key (2048-bit RSA/SM2 key), which can be used to encrypt the <code>Plaintext</code> returned. If this field is left empty, the <code>Plaintext</code> will not be encrypted.
EncryptionAlgorithm	No	String	Asymmetric encryption algorithm. It is used in combination with <code>EncryptionPublicKey</code> to encrypt the returned data. u200dValues: <code>SM2</code> u200d(Return the ciphertext in the format of "C1C3C2"), <code>SM2_C1C3C2_ASN1</code> (Return the ciphertext in

the format of "C1C3C2 ASN1"), `RSAES_PKCS1_V1_5` , `RSAES_OAEP_SHA_1` , `RSAES_OAEP_SHA_256` . It defaults to `SM2` if it's not specified.

3. Output Parameters

Parameter Name	Type	Description
KeyId	String	Globally unique CMK ID
PlainText	String	If <code>EncryptionPublicKey</code> is left empty, a Base64-encoded ciphertext will be returned. To get the plaintext, you need to decode the ciphertext first. If <code>EncryptionPublicKey</code> is passed in, this field contains the Base64-encoded ciphertext after asymmetric encryption by using the public key in <code>EncryptionPublicKey</code> . To get the plaintext, you need to first decode the Base64 format, and then decrypt with the private key corresponding with the public key. The private key is uploaded by the user.
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.

4. Example

Example1 Decrypting with PQC

This example shows you how to decrypt using PQC.

Input Example

```
POST / HTTP/1.1
Host: kms.tencentcloudapi.com
Content-Type: application/json
X-TC-Action: PostQuantumCryptoDecrypt
<Common request parameters>

{
  "CiphertextBlob": "abc",
  "EncryptionPublicKey": "abc",
  "EncryptionAlgorithm": "abc"
}
```

Output Example

```
{
  "Response": {
    "KeyId": "abc",
    "PlainText": "abc",
    "RequestId": "abc"
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
FailedOperation.EncryptionError	Encryption failed.
InternalError	Internal error.
InvalidParameter	Invalid parameter.

InvalidParameterValue.InvalidCiphertext	Incorrect ciphertext format
ResourceUnavailable.CmkDisabled	The CMK has been disabled.
ResourceUnavailable.CmkNotFound	The CMK does not exist.
UnauthorizedOperation	Unauthorized operation.

UpdateKeyDescription

最近更新时间：2023-03-24 16:02:36

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to modify the description of the specified CMK. CMKs in `PendingDelete` status cannot be modified.

A maximum of 100 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: UpdateKeyDescription.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
Description	Yes	String	New description of up to 1,024 bytes in length
KeyId	Yes	String	ID of the CMK for which to modify the description

3. Output Parameters

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

Name		
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.

4. Example

Example1 Modifying the description of a specified CMK

Modify the description of the specified CMK.

Input Example

```
https://kms.tencentcloudapi.com/?Action=UpdateKeyDescription
&KeyId=23e80852-1e38-11e9-b129-5cb9019b4b01
&Description=NewDescription
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "RequestId": "1b580852-1e38-11e9-b129-5cb9019b4b00"
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
ResourceUnavailable.CmkNotFound	The CMK does not exist.
UnauthorizedOperation	Unauthorized operation.
UnsupportedOperation.ServiceTemporaryUnavailable	The service is temporarily unavailable.

UpdateAlias

最近更新时间：2023-03-24 16:02:36

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to modify the alias of a CMK. CMKs in `PendingDelete` status cannot be modified.

A maximum of 100 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: UpdateAlias.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
Alias	Yes	String	New alias containing 1-60 characters or digits
KeyId	Yes	String	Globally unique CMK ID

3. Output Parameters

Parameter Name	Type	Description
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for

		locating a problem.
--	--	---------------------

4. Example

Example1 Modifying alias

Modify the alias of the specified CMK.

Input Example

```
https://kms.tencentcloudapi.com/?Action=UpdateAlias
&KeyId=23e80852-1e38-11e9-b129-5cb9019b4b01
&Alias=NewAlias
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "RequestId": "1b580852-1e38-11e9-b129-5cb9019b4b00"
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.
InvalidParameterValue.AliasAlreadyExists	The alias already exists.
InvalidParameterValue.InvalidAlias	Incorrect alias format
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
ResourceUnavailable.CmkNotFound	The CMK does not exist.
UnauthorizedOperation	Unauthorized operation.
UnsupportedOperation.ServiceTemporaryUnavailable	The service is temporarily unavailable.

ReEncrypt

最近更新时间：2023-03-24 16:02:37

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

Re-encrypt the ciphertext using the specified CMK.

A maximum of 100 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: ReEncrypt.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
CiphertextBlob	Yes	String	Ciphertext to be re-encrypted
DestinationKeyId	No	String	CMK used for re-encryption. If this parameter is empty, the ciphertext will be re-encrypted by using the original CMK (as long as the key is not rotated, the ciphertext will not be refreshed)
SourceEncryptionContext	No	String	JSON string of the key-value pair used during ciphertext encryption by <code>CiphertextBlob</code> . If not used during encryption, this parameter will be empty

DestinationEncryptionContext	No	String	JSON string of the key-value pair used during re-encryption. If this field is used, the same string should be entered when the returned new ciphertext is decrypted
------------------------------	----	--------	---

3. Output Parameters

Parameter Name	Type	Description
CiphertextBlob	String	Re-encrypted ciphertext
KeyId	String	CMK used for re-encryption
SourceKeyId	String	CMK used by ciphertext before re-encryption
ReEncrypted	Boolean	<code>true</code> indicates that the ciphertext has been re-encrypted. When re-encryption is initiated by using the same CMK, as long as the CMK is not rotated, no actual re-encryption will be performed, and the original ciphertext will be returned
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.

4. Example

Example1 Re-encrypting

Re-encrypt the ciphertext

Input Example

```
https://kms.tencentcloudapi.com/?Action=ReEncrypt
&DestinationKeyId=23e80852-1e38-11e9-b129-5cb9019b4b01
&CiphertextBlob=Ade234dasdeEwdGVzdCUyMHBSYWlJlIHL
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "CiphertextBlob": "g2F8eQk44QrTbfj09TL17AZyFPgs8BTtZe2j27Wuw1YzTBCxnd0T/gwFQsasmt"
```

```
zxZi6mmvD7DCjCE+LxJmdhXQ==--k-zJshb0kBH7C2J5I3XXbbEg==--k-o1O+7H9HFAzWbCkftO2ZtPKew
S3diSB4zGKOJhMn7LcKRhYr",
"KeyId": "23e80852-1e38-11e9-b129-5cb9019b4b01",
"SourceKeyId": "23e80852-1e38-11e9-b129-5cb9019b0000",
"ReEncrypted": true,
"RequestId": "1b580852-1e38-11e9-b129-5cb9019b4b00"
}
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.
InvalidParameterValue.InvalidCiphertext	Incorrect ciphertext format
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .

ResourceUnavailable.CmkDisabled	The CMK has been disabled.
ResourceUnavailable.CmkNotFound	The CMK does not exist.
UnauthorizedOperation	Unauthorized operation.

ListKeys

最近更新时间：2023-03-24 16:02:37

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to list the KeyIds of CMKs in `Enabled`, `Disabled`, and `PendingImport` status under the account.

A maximum of 100 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: ListKeys.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
Offset	No	Integer	This parameter has the same meaning of the <code>Offset</code> in an SQL query, indicating that this acquisition starts from the "No. Offset value" element of the array arranged in a certain order. The default value is 0
Limit	No	Integer	This parameter has the same meaning of the <code>Limit</code> in an SQL query, indicating that up to <code>Limit</code> value elements can be obtained in this request. The default value is 10 and the maximum value is 200
Role	No	Integer	Filter by creator role. 0 (default value): the CMK is created by the user; 1: the CMK is created automatically by an authorized Tencent

			Cloud service
HsmClusterId	No	String	ID of the HSM cluster. This field is only valid for Exclusive and Managed KMS instances.

3. Output Parameters

Parameter Name	Type	Description
Keys	Array of Key	CMK list array
TotalCount	Integer	Total number of CMKs
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.

4. Example

Example1 Getting CMK list

This example shows you how to get the list of CMKs.

Input Example

```
https://kms.tencentcloudapi.com/?Action=ListKeys
&Offset=0
&Limit=2
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "RequestId": "1b580852-1e38-11e9-b129-5cb9019b4b00",
    "Keys": [
      {
        "KeyId": "23e80852-1e38-11e9-b129-5cb9019b4b01"
      },
      {
        "KeyId": "23e80852-1e38-11e9-b129-5cb9019b4b02"
      }
    ]
  }
}
```

```
}  
],  
"TotalCount": 100  
}  
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.
InvalidParameterValue.InvalidHsmClusterId	Invalid HSM cluster ID.
UnauthorizedOperation	Unauthorized operation.

ListKeyDetail

最近更新时间：2023-08-07 17:45:14

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

Get the master key list details according to the specified Offset and Limit.

A maximum of 100 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: ListKeyDetail.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
Offset	No	Integer	This parameter has the same meaning of the <code>Offset</code> in an SQL query, indicating that this acquisition starts from the "No. Offset value" element of the array arranged in a certain order. The default value is 0.
Limit	No	Integer	This parameter has the same meaning of the <code>Limit</code> in an SQL query, indicating that up to <code>Limit</code> value elements can be obtained in this request. The default value is 10 and the maximum value is 200.
Role	No	Integer	Filters by creator role. 0 (default value): the CMK is created by the user; 1: the CMK is created automatically by an authorized

			Tencent Cloud service.
OrderType	No	Integer	Sorts by CMK creation time. 0: descending; 1: ascending
KeyState	No	Integer	Filters by CMK status. 0: all CMKs; 1: CMKs in <code>Enabled</code> status only; 2: CMKs in <code>Disabled</code> status only; 3: CMKs in <code>PendingDelete</code> status only (i.e., keys with schedule deletion enabled); 4: CMKs in <code>PendingImport</code> status only; 5: CMKs in <code>Archived</code> status only.
SearchKeyAlias	No	String	Performs a fuzzy query by <code>KeyId</code> or <code>Alias</code>
Origin	No	String	Filters by CMK type. "TENCENT_KMS" indicates to filter CMKs whose key materials are created by KMS; "EXTERNAL" indicates to filter CMKs of <code>EXTERNAL</code> type whose key materials are imported by users; "ALL" or empty indicates to filter CMKs of both types. This value is case-sensitive.
KeyUsage	No	String	Filters by the <code>KeyUsage</code> field value. Valid values: <code>ALL</code> (all CMKs), <code>ENCRYPT_DECRYPT</code> (used when this field is left empty), <code>ASYMMETRIC_DECRYPT_RSA_2048</code> , <code>ASYMMETRIC_DECRYPT_SM2</code> , <code>ASYMMETRIC_SIGN_VERIFY_SM2</code> , <code>ASYMMETRIC_SIGN_VERIFY_RSA_2048</code> , and <code>ASYMMETRIC_SIGN_VERIFY_ECC</code> .
TagFilters.N	No	Array of TagFilter	Tag filter condition
HsmClusterId	No	String	ID of the HSM cluster. This field is only valid for Exclusive and Managed KMS instances.

3. Output Parameters

Parameter Name	Type	Description
TotalCount	Integer	Total number of CMKs
KeyMetadatas	Array of KeyMetadata	List of returned attribute information. Note: this field may return null, indicating that no valid values can be obtained.
RequestId	String	The unique request ID, which is returned for each request. RequestId is

required for locating a problem.

4. Example

Example1 Getting CMK list details

Input Example

```
https://kms.tencentcloudapi.com/?Action=ListKeyDetail
&Offset=0
&Limit=3
&Role=0
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "RequestId": "1b580852-1e38-11e9-b129-5cb9019b4b00",
    "KeyMetadatas": [
      {
        "KeyId": "23e80852-1e38-11e9-b129-5cb9019b4b01",
        "Alias": "myalias",
        "CreateTime": 1548210729,
        "Description": "test cmk",
        "KeyState": "Enabled",
        "KeyUsage": "ENCRYPT_DECRYPT",
        "Type": 1,
        "CreatorUin": 1001,
        "KeyRotationEnabled": true,
        "Owner": "user",
        "NextRotateTime": 1553151489,
        "DeletionDate": 0,
        "Origin": "TENCENT_KMS",
        "ValidTo": 0
      },
      {
        "KeyId": "23e80852-1e38-11e9-b129-5cb9019b4b02",
        "Alias": "testalias",
        "CreateTime": 1548210730,
        "Description": "test cmk",
        "KeyState": "Disabled",
        "KeyUsage": "ENCRYPT_DECRYPT",
        "Type": 1,
```

```
"CreatorUin": 1001,
"KeyRotationEnabled": true,
"Owner": "user",
"NextRotateTime": 1553151489,
"DeletionDate": 0,
"Origin": "TENCENT_KMS",
"ValidTo": 0
},
{
  "KeyId": "23e80852-1e38-11e9-b129-5cb9019b4b03",
  "Alias": "testalias2",
  "CreateTime": 1548210730,
  "Description": "test cmk",
  "KeyState": "PendingDelete",
  "KeyUsage": "ENCRYPT_DECRYPT",
  "Type": 1,
  "CreatorUin": 1001,
  "KeyRotationEnabled": true,
  "Owner": "user",
  "NextRotateTime": 1553151489,
  "DeletionDate": 1560580015,
  "Origin": "TENCENT_KMS",
  "ValidTo": 0
}
],
"TotalCount": 100
}
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.
InvalidParameterValue.InvalidHsmClusterId	Invalid HSM cluster ID.
UnauthorizedOperation	Unauthorized operation.

GetServiceStatus

最近更新时间：2023-03-24 16:02:38

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

Used to query whether the user has activated the KMS service.

A maximum of 100 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: GetServiceStatus.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.

3. Output Parameters

Parameter Name	Type	Description
ServiceEnabled	Boolean	Whether the KMS service has been activated. true: activated
InvalidType	Integer	Service unavailability type. 0: not purchased; 1: normal; 2: suspended due to arrears; 3: resource released
UserLevel	Integer	0: Basic Edition, 1: Ultimate Edition

ProExpireTime	Integer	Expiration time of the KMS Ultimate edition. It's represented in a Unix Epoch timestamp. Note: This field may return null, indicating that no valid values can be obtained.
ProRenewFlag	Integer	Whether to automatically renew Ultimate Edition. 0: no, 1: yes Note: this field may return null, indicating that no valid values can be obtained.
ProResourceId	String	Unique ID of the Ultimate Edition purchase record. If the Ultimate Edition is not activated, the returned value will be null. Note: this field may return null, indicating that no valid values can be obtained.
ExclusiveVSMEnabled	Boolean	Whether to activate Managed KMS Note: This field may return <code>null</code> , indicating that no valid value can be obtained.
ExclusiveHSMEnabled	Boolean	Whether to activate Exclusive KMS Note: This field may return <code>null</code> , indicating that no valid value can be obtained.
SubscriptionInfo	String	KMS subscription information. Note: This field may return null, indicating that no valid values can be obtained.
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.

4. Example

Example1 Querying the service status

This example shows you how to query service status.

Input Example

```
POST / HTTP/1.1
Host: kms.tencentcloudapi.com
Content-Type: application/json
X-TC-Action: GetServiceStatus
<Common request parameters>

{ }
```

Output Example

```
{
  "Response": {
    "ServiceEnabled": true,
    "InvalidType": 1,
    "UserLevel": 0,
    "ProResourceId": "kms_pro_12345",
    "ProRenewFlag": 1,
    "ProExpireTime": 1603701385,
    "RequestId": "1b580852-1e38-11e9-b129-5cb9019b4b00",
    "ExclusiveHSMEnabled": false,
    "ExclusiveVSMEnabled": false,
    "SubscriptionInfo": "Prepaid_KMS"
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
InternalError	Internal error.
UnauthorizedOperation	Unauthorized operation.
UnsupportedOperation	Unsupported operation.

GetKeyRotationStatus

最近更新时间：2023-03-24 16:02:38

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

Query whether the specified CMK has the key rotation function.

A maximum of 100 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: GetKeyRotationStatus.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
KeyId	Yes	String	Unique CMK ID

3. Output Parameters

Parameter Name	Type	Description
KeyRotationEnabled	Boolean	Whether key rotation is enabled

RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.
-----------	--------	--

4. Example

Example1 Querying key rotation status

Query whether key rotation is enabled for the specified CMK.

Input Example

```
https://kms.tencentcloudapi.com/?Action=GetKeyRotationStatus
&KeyId=23e80852-1e38-11e9-b129-5cb9019b4b01
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "KeyRotationEnabled": false,
    "RequestId": "1b580852-1e38-11e9-b129-5cb9019b4b00"
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
ResourceUnavailable.CmkNotFound	The CMK does not exist.
UnauthorizedOperation	Unauthorized operation.

GenerateDataKey

最近更新时间：2023-03-24 16:02:39

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API generates a data key, which you can use to encrypt local data.

A maximum of 100 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: GenerateDataKey.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
KeyId	Yes	String	Globally unique CMK ID
KeySpec	No	String	Specifies the encryption algorithm and size of the <code>DataKey</code> . Valid values: AES_128, AES_256. Either <code>KeySpec</code> or <code>NumberOfBytes</code> must be specified.
NumberOfBytes	No	Integer	Length of the <code>DataKey</code> . If both <code>NumberOfBytes</code> and <code>KeySpec</code> are specified, <code>NumberOfBytes</code> will prevail. Minimum value: 1; maximum value: 1024. Either <code>KeySpec</code> or <code>NumberOfBytes</code> must be specified.
EncryptionContext	No	String	JSON string of key-value pair. If this field is used, the same

			string should be entered when the returned <code>DataKey</code> is decrypted.
EncryptionPublicKey	No	String	PEM-encoded public key (2048-bit RSA/SM2 key), which can be used to encrypt the <code>Plaintext</code> returned. If this field is left empty, the <code>Plaintext</code> will not be encrypted.
EncryptionAlgorithm	No	String	Asymmetric encryption algorithm. Valid values: <code>SM2</code> (C1C3C2 ciphertext is returned) , <code>SM2_C1C3C2_ASN1</code> (C1C3C2 ASN1 ciphertext is returned), <code>RSAES_PKCS1_V1_5</code> , <code>RSAES_OAEP_SHA_1</code> , and <code>RSAES_OAEP_SHA_256</code> . This field is used in combination with <code>EncryptionPublicKey</code> for encryption. If it is left empty, an SM2 public key will be used by default.

3. Output Parameters

Parameter Name	Type	Description
KeyId	String	Globally unique CMK ID
Plaintext	String	If <code>EncryptionPublicKey</code> is left empty, a Base64-encoded ciphertext will be returned. To get the plaintext, you need to decode the ciphertext first. If <code>EncryptionPublicKey</code> is specified, this field will return the Base64-encoded ciphertext encrypted with the specified public key. To get the plaintext, you need to decode the ciphertext and upload the corresponding private key.
CiphertextBlob	String	Ciphertext of the data key, which should be kept by yourself. KMS does not host user data keys. You can call the <code>Decrypt</code> API to get the plaintext of the data key from <code>CiphertextBlob</code> .
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.

4. Example

Example1 Generating a DEK

This example shows you how to generate a DEK using the specified CMK.

Input Example

```
https://kms.tencentcloudapi.com/?Action=GenerateDataKey
&KeyId=23e80852-1e38-11e9-b129-5cb9019b4b01
&KeySpec=AES_256
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "RequestId": "fe11aa29-0cc2-4204-bfea-6ebb30cc00d7",
    "KeyId": "23e80852-1e38-11e9-b129-5cb9019b4b01",
    "Plaintext": "uW9wqntw+FAgnfsIrxOpOA==",
    "CiphertextBlob": "g2F8eQk44QrTbfj09TL17AZyFPgs8BTtZe2j27Wuw1YzTBCxnd0T/gwFQSasmt
zxZi6mmvD7DCjCE+LxJmdhXQ==k-fKVP3WI1Gpg8m9LMW4jEkQ==k-h/nUfRbaTUY7/KWXwuSK1Py+Z
FRTK5WQiUz6yQE5XBFUN3UwPOUbl8P3A3caow2rlqTjUw=="
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
FailedOperation.EncryptionError	Encryption failed.
InternalError	Internal error.
InvalidParameter	Invalid parameter.
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
ResourceUnavailable.CmkDisabled	The CMK has been disabled.
ResourceUnavailable.CmkNotFound	The CMK does not exist.
ResourceUnavailable.KeyPendingDelete	The key is not available as it's pending deleted.
UnauthorizedOperation	Unauthorized operation.

Encrypt

最近更新时间：2023-03-24 16:02:39

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to encrypt any data up to 4KB. It can be used to encrypt database passwords, RSA Key, or other small sensitive information. For application data encryption, use the DataKey generated by GenerateDataKey to perform local data encryption and decryption operations

A maximum of 300 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: Encrypt.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
KeyId	Yes	String	Globally unique ID of the CMK generated by calling the <code>CreateKey</code> API
Plaintext	Yes	String	Encrypted plaintext data. This field must be Base64-encoded. The maximum size of the original data is 4 KB
EncryptionContext	No	String	JSON string of key-value pair. If this parameter is specified, the same parameter needs to be provided when the <code>Decrypt</code> API is called. It is up to 1,024 characters

3. Output Parameters

Parameter Name	Type	Description
CiphertextBlob	String	Base64-encoded ciphertext, which is the encrypted information of the ciphertext and key. To get the plaintext, you need to pass in this field to the Decrypt API.
KeyId	String	Globally unique ID of the CMK used for encryption
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.

4. Example

Example1 Encrypting data

This example shows you how to use a CMK to encrypt data up to 4 KB.

Input Example

```
https://kms.tencentcloudapi.com/?Action=Encrypt
&KeyId=23e80852-1e38-11e9-b129-5cb9019b4b01
&Plaintext=dGVzdCUyMHBSYWluJTlwdGV4dA==
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "RequestId": "816c6886-2147-4ee7-86f0-9400a7a398a5",
    "KeyId": "9999aed0-4956-11e9-bc70-5254005e86b4",
    "CiphertextBlob": "g2F8eQk44QrTbfj09TL17AZyFPgs8BTtZe2j27Wuw1YzTBCxnd0T/gwFQsasmt
zxZi6mmvD7DCjCE+LxJmdhXQ==k-zJshb0kBH7C2J5I3XXbbEg==k-o1o+7H9HFAzWbCkftO2ZtPKew
S3diSB4zGKOJhMn7LcKRhYr"
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
InternalServerError	Internal error.
InvalidParameter	Invalid parameter.
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
InvalidParameterValue.InvalidPlaintext	Invalid <code>Plaintext</code> .
ResourceUnavailable.CmkArchived	The CMK has been archived.
ResourceUnavailable.CmkDisabled	The CMK has been disabled.
ResourceUnavailable.CmkNotFound	The CMK does not exist.
UnauthorizedOperation	Unauthorized operation.

EnableKeys

最近更新时间：2023-03-24 16:02:39

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to enable CMK in batches.

A maximum of 100 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: EnableKeys.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
KeyIds.N	Yes	Array of String	List of IDs of the CMKs to be enabled in batches. Up to 100 CMKs are supported at a time

3. Output Parameters

Parameter Name	Type	Description
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for

		locating a problem.
--	--	---------------------

4. Example

Example1 Enabling CMKs in batches

This example shows you how to enable the CMKs on a specified list in batches.

Input Example

```
https://kms.tencentcloudapi.com/?Action=EnableKeys
&KeyIds.0=23e80852-1e38-11e9-b129-5cb9019b4b01
&KeyIds.1=23e80852-1e38-11e9-b129-5cb9019b4b02
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "RequestId": "1b580852-1e38-11e9-b129-5cb9019b4b00"
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.
InvalidParameterValue.DuplicatedKeyId	Duplicate <code>KeyId</code> .
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
ResourceUnavailable.CmkNotFound	The CMK does not exist.
ResourceUnavailable.CmkStateNotSupport	This operation cannot be performed under the current CMK status.
UnauthorizedOperation	Unauthorized operation.
UnsupportedOperation.ServiceTemporaryUnavailable	The service is temporarily unavailable.

EnableKeyRotation

最近更新时间：2023-03-24 16:02:39

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

Turn on the key rotation function for the specified CMK.

A maximum of 100 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: EnableKeyRotation.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
KeyId	Yes	String	Unique CMK ID
RotateDays	No	Integer	The interval between each key rotation in days. Value range: 7 - 365 (default).

3. Output Parameters

Parameter Name	Type	Description

RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.
-----------	--------	--

4. Example

Example1 Enabling key rotation

This example shows you how to enable key rotation for a specified CMK.

Input Example

```
POST / HTTP/1.1
Host: kms.tencentcloudapi.com
Content-Type: application/json
X-TC-Action: EnableKeyRotation
<Common request parameters>

{
  "KeyId": "23e80852-1e38-11e9-b129-5cb9019b4b01"
}
```

Output Example

```
{
  "Response": {
    "RequestId": "1b580852-1e38-11e9-b129-5cb9019b4b00"
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)

- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
InternalServerError	Internal error.
InvalidParameter	Invalid parameter.
InvalidParameterValue	Incorrect parameter value.
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
ResourceUnavailable.CmkNotFound	The CMK does not exist.
ResourceUnavailable.CmkStateNotSupport	This operation cannot be performed under the current CMK status.
UnauthorizedOperation	Unauthorized operation.
UnsupportedOperation.ExternalCmkCanNotRotate	External CMKs cannot be rotated.
UnsupportedOperation.ServiceTemporaryUnavailable	The service is temporarily unavailable.

EnableKey

最近更新时间：2023-03-24 16:02:40

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

Enable a specified CMK.

A maximum of 100 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: EnableKey.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
KeyId	Yes	String	Unique CMK ID

3. Output Parameters

Parameter Name	Type	Description
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.

4. Example

Example1 Enabling a CMK

Enable a CMK for use.

Input Example

```
https://kms.tencentcloudapi.com/?Action=EnableKey
&KeyId=23e80852-1e38-11e9-b129-5cb9019b4b01
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "RequestId": "1b580852-1e38-11e9-b129-5cb9019b4b00"
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
ResourceUnavailable.CmkNotFound	The CMK does not exist.
ResourceUnavailable.CmkStateNotSupport	This operation cannot be performed under the current CMK status.
UnauthorizedOperation	Unauthorized operation.
UnsupportedOperation.ServiceTemporaryUnavailable	The service is temporarily unavailable.

DisableKeys

最近更新时间：2023-03-24 16:02:40

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to batch prohibit the use of CMK.

A maximum of 100 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: DisableKeys.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
KeyIds.N	Yes	Array of String	List of IDs of the CMKs to be disabled in batches. Up to 100 CMKs are supported at a time

3. Output Parameters

Parameter Name	Type	Description
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for

		locating a problem.
--	--	---------------------

4. Example

Example1 Disabling CMKs in batches

This example shows you how to disable the CMKs on a specified list in batches.

Input Example

```
https://kms.tencentcloudapi.com/?Action=DisableKeys
&KeyIds.0=23e80852-1e38-11e9-b129-5cb9019b4b01
&KeyIds.1=23e80852-1e38-11e9-b129-5cb9019b4b02
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "RequestId": "1b580852-1e38-11e9-b129-5cb9019b4b00"
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

• [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
FailedOperation.CmkUsedByCloudProduct	The CMK is being used by a Tencent Cloud product.
InternalError	Internal error.
InvalidParameter	Invalid parameter.
InvalidParameterValue.DuplicatedKeyId	Duplicate <code>KeyId</code> .
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
ResourceUnavailable.CmkNotFound	The CMK does not exist.
ResourceUnavailable.CmkStateNotSupport	This operation cannot be performed under the current CMK status.
UnauthorizedOperation	Unauthorized operation.
UnsupportedOperation.ServiceTemporaryUnavailable	The service is temporarily unavailable.

DisableKeyRotation

最近更新时间：2023-03-24 16:02:40

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

Disabled key rotation for the specified CMK.

A maximum of 100 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: DisableKeyRotation.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
KeyId	Yes	String	Unique CMK ID

3. Output Parameters

Parameter Name	Type	Description
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for

		locating a problem.
--	--	---------------------

4. Example

Example1 Disabling key rotation

Disable key rotation for the specified CMK.

Input Example

```
https://kms.tencentcloudapi.com/?Action=DisableKeyRotation
&KeyId=23e80852-1e38-11e9-b129-5cb9019b4b01
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "RequestId": "1b580852-1e38-11e9-b129-5cb9019b4b00"
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
ResourceUnavailable.CmkNotFound	The CMK does not exist.
UnauthorizedOperation	Unauthorized operation.

DisableKey

最近更新时间：2023-03-24 16:02:40

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to disable a master key. The disabled key cannot be used for encryption and decryption operations.

A maximum of 100 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: DisableKey.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
KeyId	Yes	String	Unique CMK ID

3. Output Parameters

Parameter Name	Type	Description
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.

4. Example

Example1 Disabling a CMK

Disable the specified CMK.

Input Example

```
https://kms.tencentcloudapi.com/?Action=DisableKey
&KeyId=23e80852-1e38-11e9-b129-5cb9019b4b01
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "RequestId": "1b580852-1e38-11e9-b129-5cb9019b4b00"
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
FailedOperation.CmkUsedByCloudProduct	The CMK is being used by a Tencent Cloud product.
InternalError	Internal error.
InvalidParameter	Invalid parameter.
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
ResourceUnavailable.CmkNotFound	The CMK does not exist.
ResourceUnavailable.CmkStateNotSupport	This operation cannot be performed under the current CMK status.
UnauthorizedOperation	Unauthorized operation.
UnsupportedOperation.ServiceTemporaryUnavailable	The service is temporarily unavailable.

DescribeKeys

最近更新时间：2023-03-24 16:02:40

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to get the attribute information of CMKs in batches.

A maximum of 100 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: DescribeKeys.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
KeyIds.N	Yes	Array of String	List of IDs of the CMKs to be queried in batches. Up to 100 <code>KeyId</code> values are supported in one query.

3. Output Parameters

Parameter Name	Type	Description
KeyMetadatas	Array of	List of returned attribute information

	KeyMetadata	Note: this field may return null, indicating that no valid values can be obtained.
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.

4. Example

Example1 Getting attributes of multiple CMKs

Get attributes of multiple CMKs.

Input Example

```
https://kms.tencentcloudapi.com/?Action=DescribeKeys
&KeyIds.0=23e80852-1e38-11e9-b129-5cb9019b4b01
&KeyIds.1=23e80852-1e38-11e9-b129-5cb9019b4b02
&KeyIds.2=23e80852-1e38-11e9-b129-5cb9019b4b03
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "KeyMetadatas": [
      {
        "KeyId": "23e80852-1e38-11e9-b129-5cb9019b4b01",
        "Alias": "myalias",
        "CreateTime": 1548210729,
        "Description": "test cmk",
        "KeyState": "Enabled",
        "KeyUsage": "ENCRYPT_DECRYPT",
        "Type": 1,
        "CreatorUin": 1001,
        "KeyRotationEnabled": true,
        "Owner": "user",
        "NextRotateTime": 1553151489,
        "DeletionDate": 0,
        "Origin": "TENCENT_KMS",
        "ValidTo": 0
      },
      {
        "KeyId": "23e80852-1e38-11e9-b129-5cb9019b4b02",
        "Alias": "testalias",
```

```
"CreateTime": 1548210730,
"Description": "test cmk",
"KeyState": "Disabled",
"KeyUsage": "ENCRYPT_DECRYPT",
"Type": 1,
"CreatorUin": 1001,
"KeyRotationEnabled": true,
"Owner": "user",
"NextRotateTime": 1553151489,
"DeletionDate": 0,
"Origin": "TENCENT_KMS",
"ValidTo": 0
},
{
  "KeyId": "23e80852-1e38-11e9-b129-5cb9019b4b03",
  "Alias": "testalias3",
  "CreateTime": 1548210730,
  "Description": "test cmk",
  "KeyState": "PendingDelete",
  "KeyUsage": "ENCRYPT_DECRYPT",
  "Type": 1,
  "CreatorUin": 1001,
  "KeyRotationEnabled": true,
  "Owner": "user",
  "NextRotateTime": 1553151489,
  "DeletionDate": 1560580015,
  "Origin": "TENCENT_KMS",
  "ValidTo": 0
}
],
"RequestId": "1b580852-1e38-11e9-b129-5cb9019b4b00"
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)

- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
InternalServerError	Internal error.
InvalidParameter	Invalid parameter.
InvalidParameterValue.DuplicatedKeyId	Duplicate <code>KeyId</code> .
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
ResourceUnavailable.CmkNotFound	The CMK does not exist.
UnauthorizedOperation	Unauthorized operation.

DescribeKey

最近更新时间：2023-03-24 16:02:41

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to get the attribute details of the CMK with a specified `KeyId`.

A maximum of 100 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: DescribeKey.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
KeyId	Yes	String	Globally unique CMK ID

3. Output Parameters

Parameter Name	Type	Description
KeyMetadata	KeyMetadata	Key attribute information Note: this field may return null, indicating that no valid values can be obtained.

RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.
-----------	--------	--

4. Example

Example1 Getting CMK attributes

Get the attribute details of the specified CMK.

Input Example

```
https://kms.tencentcloudapi.com/?Action=DescribeKey
&KeyId=23e80852-1e38-11e9-b129-5cb9019b4b01
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "KeyMetadata": {
      "KeyId": "23e80852-1e38-11e9-b129-5cb9019b4b01",
      "Alias": "myalias",
      "CreateTime": 1548210729,
      "Description": "test cmk",
      "KeyState": "Enabled",
      "KeyUsage": "ENCRYPT_DECRYPT",
      "Type": 1,
      "CreatorUin": 1001,
      "KeyRotationEnabled": true,
      "Owner": "user",
      "NextRotateTime": 1553151489,
      "DeletionDate": 0,
      "Origin": "TENCENT_KMS",
      "ValidTo": 0
    },
    "RequestId": "1b580852-1e38-11e9-b129-5cb9019b4b00"
  }
}
```

Example2 Getting the attributes of a CMK scheduled for deletion

This example shows you how to get the attributes of a CMK scheduled for deletion.

Input Example

```
https://kms.tencentcloudapi.com/?Action=DescribeKey
&KeyId=23e80852-1e38-11e9-b129-5cb9019b4b02
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "KeyMetadata": {
      "KeyId": "23e80852-1e38-11e9-b129-5cb9019b4b02",
      "Alias": "myalias",
      "CreateTime": 1548210729,
      "Description": "test cmk",
      "KeyState": "PendingDelete",
      "KeyUsage": "ENCRYPT_DECRYPT",
      "Type": 1,
      "CreatorUin": 1001,
      "KeyRotationEnabled": true,
      "Owner": "user",
      "NextRotateTime": 1553151489,
      "DeletionDate": 1560580015,
      "Origin": "TENCENT_KMS",
      "ValidTo": 0
    },
    "RequestId": "1b580852-1e38-11e9-b129-5cb9019b4b00"
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
ResourceUnavailable.CmkNotFound	The CMK does not exist.
UnauthorizedOperation	Unauthorized operation.

Decrypt

最近更新时间：2023-03-24 16:02:41

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to decrypt the ciphertext and obtain the plaintext data.

A maximum of 300 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: Decrypt.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
CiphertextBlob	Yes	String	The ciphertext data to be decrypted.
EncryptionContext	No	String	JSON string of key-value pair. If this parameter is specified for <code>Encrypt</code> , the same parameter needs to be provided when the <code>Decrypt</code> API is called. The maximum length is 1,024 bytes.
EncryptionPublicKey	No	String	PEM-encoded public key (2048-bit RSA/SM2 key), which can be used to encrypt the <code>Plaintext</code> returned. If this field is left empty, the <code>Plaintext</code> will not be encrypted.
EncryptionAlgorithm	No	String	Asymmetric encryption algorithm. Valid values: <code>SM2</code> (C1C3C2 ciphertext is returned), <code>SM2_C1C3C2_ASN1</code>

(C1C3C2 ASN1 ciphertext is returned),
RSAES_PKCS1_V1_5 , RSAES_OAEP_SHA_1 , and
RSAES_OAEP_SHA_256 . This field is used in combination
with EncryptionPublicKey for encryption. If it is left
empty, an SM2 public key will be used by default.

3. Output Parameters

Parameter Name	Type	Description
KeyId	String	Globally unique CMK ID
Plaintext	String	If EncryptionPublicKey is left empty, a Base64-encoded ciphertext will be returned. To get the plaintext, you need to decode the ciphertext first. If EncryptionPublicKey is specified, this field will return the Base64-encoded ciphertext encrypted with the specified public key. To get the plaintext, you need to decode the ciphertext and upload the corresponding private key.
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.

4. Example

Example1 Decrypting

Decrypt ciphertext.

Input Example

```
https://kms.tencentcloudapi.com/?Action=Decrypt
&CiphertextBlob=Ade234dasdeEWdGVzdCUyMHBsYWlJlIHL
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "KeyId": "23e80852-1e38-11e9-b129-5cb9019b4b01",
    "Plaintext": "dGVzdCUyMHBsYWlJlIwdGV4dA==",
    "RequestId": "1b580852-1e38-11e9-b129-5cb9019b4b00"
```

```
}  
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
FailedOperation.EncryptionError	Encryption failed.
InternalError	Internal error.
InvalidParameter	Invalid parameter.
InvalidParameterValue.InvalidCiphertext	Incorrect ciphertext format
ResourceUnavailable.CmkDisabled	The CMK has been disabled.
ResourceUnavailable.CmkNotFound	The CMK does not exist.
UnauthorizedOperation	Unauthorized operation.

CreateKey

最近更新时间：2023-03-24 16:02:41

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

Create a master key CMK (Custom Master Key) for user management data keys

A maximum of 100 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: CreateKey.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
Alias	Yes	String	Unique alias that makes a key more recognizable and understandable. This parameter cannot be empty, can contain 1-60 letters, digits, <code>-</code> , and <code>_</code> , and must begin with a letter or digit. The <code>kms-</code> prefix is used for Tencent Cloud products.
Description	No	String	CMK description of up to 1,024 bytes in length
KeyUsage	No	String	Defines the purpose of the key. The valid values are as follows: <code>ENCRYPT_DECRYPT</code> (default): creates a symmetric encryption/decryption key; <code>ASYMMETRIC_DECRYPT_RSA_2048</code> : creates an asymmetric encryption/decryption 2048-bit RSA key; <code>ASYMMETRIC_DECRYPT_SM2</code> : creates an asymmetric

			encryption/decryption SM2 key; <code>ASYMMETRIC_SIGN_VERIFY_SM2</code> : creates an asymmetric SM2 key for signature verification; <code>ASYMMETRIC_SIGN_VERIFY_ECC</code> : creates an asymmetric 2048-bit RSA key for signature verification; <code>ASYMMETRIC_SIGN_VERIFY_ECDSA384</code> : creates an asymmetric ECDSA384 key for signature verification. You can get a full list of supported key purposes and algorithms using the <code>ListAlgorithms</code> API.
Type	No	Integer	Specifies the key type. Default value: 1. Valid value: 1 - default type, indicating that the CMK is created by KMS; 2 - EXTERNAL type, indicating that you need to import key material. For more information, please see the <code>GetParametersForImport</code> and <code>ImportKeyMaterial</code> API documents.
Tags.N	No	Array of Tag	Tag list
HsmClusterId	No	String	ID of the HSM cluster. This field is only valid for Exclusive and Managed KMS instances.

3. Output Parameters

Parameter Name	Type	Description
KeyId	String	Globally unique CMK ID
Alias	String	Alias that makes a key more recognizable and understandable
CreateTime	Integer	Key creation time in UNIX timestamp format
Description	String	CMK description
KeyState	String	CMK status
KeyUsage	String	CMK usage
TagCode	Integer	Tag operation return code. 0: success; 1: internal error; 2: business processing error
TagMsg	String	Tag operation return information
HsmClusterId	String	ID of the HSM cluster. This field is only valid for Exclusive and Managed KMS instances.

		Note: This field may return <code>null</code> , indicating that no valid value can be obtained.
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.

4. Example

Example1 Creating a CMK

This example shows you how to create a Custom Master Key (CMK) for data encryption key management. The CMK is required for creating data encryption keys, encryption and decryption, and more.

Input Example

```
https://kms.tencentcloudapi.com/?Action=CreateKey
&Alias=mykey
&KeyUsage=ENCRYPT_DECRYPT
&Description=test
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "KeyId": "9999aed0-4956-11e9-bc70-5254005e86b4",
    "Alias": "alias-0001",
    "CreateTime": 1552897190,
    "Description": "test cmk",
    "TagMsg": "Success",
    "TagCode": 0,
    "KeyState": "Enabled",
    "KeyUsage": "ENCRYPT_DECRYPT",
    "RequestId": "850bf779-2249-4995-8c55-b3966daf0a8c",
    "HsmClusterId": ""
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
FailedOperation.TaggingError	Tagging error.
InternalError	Internal error.
InvalidParameter	Invalid parameter.
InvalidParameterValue.AliasAlreadyExists	The alias already exists.
InvalidParameterValue.InvalidAlias	Incorrect alias format
InvalidParameterValue.InvalidHsmClusterId	Invalid HSM cluster ID.
InvalidParameterValue.InvalidKeyUsage	Incorrect <code>KeyUsage</code> parameter.
InvalidParameterValue.InvalidType	Incorrect <code>Type</code> parameter.
InvalidParameterValue.TagKeysDuplicated	Duplicate tag key.
InvalidParameterValue.TagsNotExisted	The tag key or tag value does not exist.
LimitExceeded.CmkLimitExceeded	The number of CMKs has reached the upper limit.

UnauthorizedOperation	Unauthorized operation.
UnsupportedOperation.ServiceTemporaryUnavailable	The service is temporarily unavailable.
UnsupportedOperation.UnsupportedKeyUsageInCurrentRegion	The encryption method is not supported in the current region.

ScheduleKeyDeletion

最近更新时间：2023-03-24 16:02:37

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

CMK planned deletion API, used to specify the time of CMK deletion, the optional time interval is [7,30] days

A maximum of 100 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: ScheduleKeyDeletion.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
KeyId	Yes	String	Unique CMK ID
PendingWindowInDays	Yes	Integer	Schedule deletion time range. Value range: [7,30]

3. Output Parameters

Parameter Name	Type	Description

DeletionDate	Integer	Schedule deletion execution time
KeyId	String	Unique ID of the CMK scheduled for deletion
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.

4. Example

Example1 Scheduling deletion

This example shows you how to delete a specified CMK on the 7th day upon schedule deletion.

Input Example

```
POST / HTTP/1.1
Host: kms.tencentcloudapi.com
Content-Type: application/json
X-TC-Action: ScheduleKeyDeletion
<Common request parameters>

{
  "PendingWindowInDays": "7",
  "KeyId": "\"23e80852-1e38-11e9-b129-5cb9019b4b01\""
}
```

Output Example

```
{
  "Response": {
    "RequestId": "8e8f23a7-50b2-4c8e-bd23-0a98cb643f88",
    "DeletionDate": 1559318399,
    "KeyId": "23e80852-1e38-11e9-b129-5cb9019b4b01"
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
FailedOperation.CmkUsedByCloudProduct	The CMK is being used by a Tencent Cloud product.
InternalError	Internal error.
InvalidParameter.InvalidPendingWindowInDays	The schedule deletion time parameter is invalid.
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
ResourceUnavailable.CmkNotFound	The CMK does not exist.
ResourceUnavailable.CmkShouldBeDisabled	An enabled CMK cannot be scheduled for deletion.
ResourceUnavailable.CmkStateNotSupport	This operation cannot be performed under the current CMK status.
UnauthorizedOperation	Unauthorized operation.
UnsupportedOperation.ServiceTemporaryUnavailable	The service is temporarily unavailable.

CancelKeyDeletion

最近更新时间：2023-03-24 16:02:41

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

Cancel the scheduled deletion of CMK

A maximum of 100 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: CancelKeyDeletion.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
KeyId	Yes	String	Unique ID of the CMK for which to cancel schedule deletion

3. Output Parameters

Parameter Name	Type	Description
KeyId	String	Unique ID of the CMK for which the schedule deletion is canceled
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for

		locating a problem.
--	--	---------------------

4. Example

Example1 Canceling a scheduled deletion task

This example shows you how to cancel a scheduled deletion task of a CMK.

Input Example

```
POST / HTTP/1.1
Host: kms.tencentcloudapi.com
Content-Type: application/json
X-TC-Action: CancelKeyDeletion
<Common request parameters>

{
  "KeyId": "23e80852-1e38-11e9-b129-5cb9019b4b01"
}
```

Output Example

```
{
  "Response": {
    "RequestId": "8e8f23a7-50b2-4c8e-bd23-0a98cb643f88",
    "KeyId": "23e80852-1e38-11e9-b129-5cb9019b4b01"
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)

- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
InternalError	Internal error.
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
ResourceUnavailable.CmkNotFound	The CMK does not exist.
ResourceUnavailable.CmkNotPendingDelete	As the CMK is not scheduled for deletion, you cannot cancel the schedule deletion.
UnauthorizedOperation	Unauthorized operation.
UnsupportedOperation.ServiceTemporaryUnavailable	The service is temporarily unavailable.

ImportKeyMaterial

最近更新时间：2023-08-07 17:45:15

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to import key material into an EXTERNAL CMK. The key obtained through the `GetParametersForImport` API is used to encrypt the key material. You can only reimport the same key material into the specified CMK and set a new expiration time. After the CMK key material is imported, it cannot be replaced. After the key material is expired or deleted, the CMK will remain unavailable until the same key material is reimported. CMKs are independent, which means that the same key material can be imported into different CMKs, but data encrypted by one CMK cannot be decrypted by another one.

Key material can only be imported into CMKs in `Enabled` and `PendingImport` status.

A maximum of 100 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: ImportKeyMaterial.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
EncryptedKeyMaterial	Yes	String	Base64-encoded key material that encrypted with the <code>PublicKey</code> returned by <code>GetParametersForImport</code> . For the KMS of SM-CRYPTO version, the length of the key material should be

			128 bits, while for KMS of FIPS-compliant version, the length should be 256 bits.
ImportToken	Yes	String	Import token obtained by calling <code>GetParametersForImport</code> .
KeyId	Yes	String	Specifies the CMK into which to import key material, which must be the same as the one specified by <code>GetParametersForImport</code> .
ValidTo	No	Integer	Unix timestamp of the key material's expiration time. If this value is empty or 0, the key material will never expire. To specify the expiration time, it should be later than the current time. Maximum value: 2147443200.

3. Output Parameters

Parameter Name	Type	Description
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.

4. Example

Example1 Importing key material

Input Example

```
POST / HTTP/1.1
Host: kms.tencentcloudapi.com
Content-Type: application/json
X-TC-Action: ImportKeyMaterial
<Common request parameters>

{
  "ValidTo": "0",
  "KeyId": "23e80852-1e38-11e9-b129-5cb9019b4b01",
  "ImportToken": "Sy+GF4f+XxUan1sfSBfqWQmyJeVO30wcqLEMoW4REpxBApJqYG9zc37OM0Z3qT/mvLofzM3hwVJSTzIITcAo6ew3LidOJ3nwNoVNOM2wnrL+g9puwP0GpbbSwTd16X9E",
  "EncryptedKeyMaterial": "dgqtAzLde+xsR5q3kwOsWu4bst7FaE4sbhhf1OHCmujhjTJTnFGEubKowVFnFC96e2vUvO5fwGvfNcPIDkg6q7iuFviM0BepCmF9Fyk3tluJVRf/Nv8FCccANXmsZDPxtSHdcD00/
```

```
dQg1i2BIaLMP3/VFBDVEK7AzRh1TkrNiout4pavGSCAF+uBl2Vmnq6fF4DT37B0Q0WQ4NyfUwDCSR0VSF
9vwqommhudJUHV4+21xHMgUCdbFvVoOmZP/Md5Sb4rbMbWi5qRpLusi8W3KKTyJ8onp7UC+0qi6DTw4XC
q4UPniFNJXIxUOSVXpZHQKFCJXr6/cxNAci8eMTTwfA=="
}
```

Output Example

```
{
  "Response": {
    "RequestId": "1b580852-1e38-11e9-b129-5cb9019b4b00"
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
InternalError	Internal error.

InvalidParameter	Invalid parameter.
InvalidParameter.DecryptMaterialError	Decryption of <code>EncryptedKeyMaterial</code> failed.
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
InvalidParameterValue.MaterialNotMatch	The key material is different from the one previously imported.
ResourceUnavailable.CmkNotFound	The CMK does not exist.
ResourceUnavailable.CmkStateNotSupport	This operation cannot be performed under the current CMK status.
ResourceUnavailable.TokenExpired	Token has expired.
UnsupportedOperation.NotExternalCmk	Incorrect CMK type. Only <code>External</code> CMKs are supported.
UnsupportedOperation.ServiceTemporaryUnavailable	The service is temporarily unavailable.

GetParametersForImport

最近更新时间：2023-08-07 17:45:15

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to obtain the parameters of the material to be imported into a CMK. The returned `Token` is used as one of the parameters to execute `ImportKeyMaterial`, and the returned `PublicKey` is used to encrypt the key material. The `Token` and `PublicKey` are valid for 24 hours. If they are expired, you will need to call the API again to get a new `Token` and `PublicKey`.

A maximum of 100 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: GetParametersForImport.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
KeyId	Yes	String	Unique ID of a CMK. The CMK for which to get the key parameters must be of the <code>EXTERNAL</code> type, i.e., Type = 2 when the CMK is created by the <code>CreateKey</code> API.
WrappingAlgorithm	Yes	String	Specifies the algorithm for key material encryption. Currently, <code>RSAES_PKCS1_V1_5</code> , <code>RSAES_OAEP_SHA_1</code> , and <code>RSAES_OAEP_SHA_256</code> are supported.

WrappingKeySpec	Yes	String	Specifies the type of wrapping key. Currently, only <code>RSA_2048</code> is supported.
-----------------	-----	--------	---

3. Output Parameters

Parameter Name	Type	Description
KeyId	String	Unique ID of a CMK, which is used to specify the CMK into which to import key material.
ImportToken	String	The token required for importing key material, which is used as a parameter for <code>ImportKeyMaterial</code> .
PublicKey	String	The Base64-encoded RSA public key used to encrypt key material before importing it with <code>ImportKeyMaterial</code> .
ParametersValidTo	Integer	Validity period of the token and public key. A token and public key can only be imported when they are valid. If they are expired, you will need to call the <code>GetParametersForImport</code> API again to get a new token and public key.
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.

4. Example

Example1 Getting the parameters of the key material imported to a CMK

Input Example

```
https://kms.tencentcloudapi.com/?Action=GetParametersForImport
&KeyId=1ff78c0d-c54b-11e9-9cc9-5254006d0810
&WrappingAlgorithm=RSAES_OAEP_SHA_1
&WrappingKeySpec=RSA_2048
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "KeyId": "1ff78c0d-c54b-11e9-9cc9-5254006d0810",
```

```
"ImportToken": "Sy+GF4f+XxUan1sfSBfqWQmyJeVO30wcqLEMoW4REpw3adjEFXyCP2yqzV8xdD5GM
Y4gIZoDfJ33SnnbxDMRND8lzh4mZjzFNM8PsjhYrgVSxIiJOCHupZvD4QcoGco8",
"PublicKey": "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1IjpYRubNKn97lPU0/eR8UB
aV11glfQLNqlub+YspXwBsvVqcnSvu5c8GoLTEYGSTVbvsREDCq6VfFoSeoIqbv8aWukxbPGWgI1nu55o
cvWwthzROFA5UPGC8LOuH0ftZ5Z7cIaigEenS3ngfo4MYTJtg6/B11jJVWvjnKzgsWsZeFclSURedSXUc
MxfSI344s6I17DTNAQ/vQqyjFGIyo2+JctaxVlY2XuBZf7tPimNdoxAoJ14QxAl1gQGu959xnRJ4rwZbx
sklJnEivQqTBeFiiv3KTzFJS6bkz2eqRJ1p4jTBDWbHEWTVt6tdXPj4+4D21RFGAt3706vf4PIrwIDAQA
B",
"ParametersValidTo": 1566614716,
"RequestId": "5e137679-519f-409f-9a99-579a034cc320"
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
InternalError	Internal error.

InvalidParameter	Invalid parameter.
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
ResourceUnavailable.CmkNotFound	The CMK does not exist.
UnsupportedOperation.NotExternalCmk	Incorrect CMK type. Only <code>External</code> CMKs are supported.
UnsupportedOperation.ServiceTemporaryUnavailable	The service is temporarily unavailable.

DeleteImportedKeyMaterial

最近更新时间：2023-08-07 17:45:15

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to delete the imported key material. It is only valid for EXTERNAL CMKs. Specifically, it puts a CMK into `PendingImport` status instead of deleting the CMK, so that the CMK can be used again after key material is reimported. To delete the CMK completely, please call the `ScheduleKeyDeletion` API.

A maximum of 100 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: DeleteImportedKeyMaterial.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
KeyId	Yes	String	Specifies the EXTERNAL CMK for which to delete the key material.

3. Output Parameters

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

RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.
-----------	--------	--

4. Example

Example1 Deleting the imported key material

Input Example

```
https://kms.tencentcloudapi.com/?Action=DeleteImportedKeyMaterial
&KeyId=23e80852-1e38-11e9-b129-5cb9019b4b01
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "RequestId": "1b580852-1e38-11e9-b129-5cb9019b4b00"
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
FailedOperation.CmkUsedByCloudProduct	The CMK is being used by a Tencent Cloud product.
InternalError	Internal error.
InvalidParameter	Invalid parameter.
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
ResourceUnavailable.CmkNotFound	The CMK does not exist.
ResourceUnavailable.CmkStateNotSupport	This operation cannot be performed under the current CMK status.
UnsupportedOperation.NotExternalCmk	Incorrect CMK type. Only <code>External</code> CMKs are supported.
UnsupportedOperation.ServiceTemporaryUnavailable	The service is temporarily unavailable.

GenerateRandom

最近更新时间：2023-03-24 16:02:39

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to generate a random number.

A maximum of 150 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: GenerateRandom.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
NumberOfBytes	Yes	Integer	Length of the random number. Minimum value: 1. Maximum value: 1024

3. Output Parameters

Parameter Name	Type	Description
Plaintext	String	Base64-encoded plaintext of the randomly generated number. You need to Base64-

		decode it to get the plaintext.
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.

4. Example

Example1 Generating a random number

This example shows you how to generate a random number.

Input Example

```
https://kms.tencentcloudapi.com/?Action=GenerateRandom
&NumberOfBytes=16
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "Plaintext": "17mvQgM10sbM70AJ7fpLsA==",
    "RequestId": "6010cd3d-a85a-4e00-b37b-22606d017420"
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.
UnauthorizedOperation	Unauthorized operation.

ListAlgorithms

最近更新时间：2023-08-07 17:45:15

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to list the encryption methods supported in the current region.

A maximum of 100 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: ListAlgorithms.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.

3. Output Parameters

Parameter Name	Type	Description
SymmetricAlgorithms	Array of AlgorithmInfo	Symmetric encryption algorithms supported in this region
AsymmetricAlgorithms	Array of AlgorithmInfo	Asymmetric encryption algorithms supported in this region

AsymmetricSignVerifyAlgorithms	Array of AlgorithmInfo	Asymmetric signature verification algorithms supported in the current region
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.

4. Example

Example1 Listing encryption methods supported in the current region

Input Example

```
https://kms.tencentcloudapi.com/?Action=ListAlgorithms
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "RequestId": "460fe7ff-f4db-4509-9b20-208badcfb915",
    "SymmetricAlgorithms": [
      {
        "KeyUsage": "ENCRYPT_DECRYPT",
        "Algorithm": "SM4"
      }
    ],
    "AsymmetricAlgorithms": [
      {
        "KeyUsage": "ASYMMETRIC_DECRYPT_SM2",
        "Algorithm": "SM2"
      },
      {
        "KeyUsage": "ASYMMETRIC_DECRYPT_RSA_2048",
        "Algorithm": "RSA_2048"
      }
    ]
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
InternalError	Internal error.
UnauthorizedOperation	Unauthorized operation.

UnbindCloudResource

最近更新时间：2023-08-07 17:45:14

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to unbind a key with a Tencent Cloud resource, indicating that the Tencent Cloud resource will not use the key any longer.

A maximum of 100 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: UnbindCloudResource.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
KeyId	Yes	String	CMK ID
ProductId	Yes	String	Unique ID of a Tencent Cloud service
ResourceId	Yes	String	Resource/instance ID, which is stored as a string and defined by the caller based on the Tencent Cloud service's features.

3. Output Parameters

Parameter Name	Type	Description
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.

4. Example

Example1 Unbinding a CMK with a Tencent Cloud resource

Input Example

```
https://kms.tencentcloudapi.com/?Action=UnbindCloudResource
&KeyId=23e80852-1e38-11e9-b129-5cb9019b4b01
&ProductId=ssm
&ResourceId=resourceId
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "RequestId": "fe11aa29-0cc2-4204-bfea-6ebb30cc00d7"
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
ResourceUnavailable.CloudResourceBindingNotFound	The CMK is not bound with the Tencent Cloud resource
ResourceUnavailable.CmkNotFound	The CMK does not exist.
UnauthorizedOperation	Unauthorized operation.
UnsupportedOperation.ServiceTemporaryUnavailable	The service is temporarily unavailable.

BindCloudResource

最近更新时间：2023-03-24 16:02:42

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to bind a key with a Tencent Cloud resource. If the key has been set to be expired automatically, the setting will be canceled to ensure that the key will not be invalid automatically. If the key and the resource has already been bound, the call will still be successful.

A maximum of 100 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: BindCloudResource.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
KeyId	Yes	String	CMK ID
ProductId	Yes	String	Unique ID of a Tencent Cloud service
ResourceId	Yes	String	Resource/instance ID, which is stored as a string and defined by the caller based on the Tencent Cloud service's features.

3. Output Parameters

Parameter Name	Type	Description
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.

4. Example

Example1 Binding a key with a Tencent Cloud resource

This example shows you how to bind a key with a Tencent Cloud resource.

Input Example

```
https://kms.tencentcloudapi.com/?Action=BindCloudResource
&KeyId=23e80852-1e38-11e9-b129-5cb9019b4b01
&ProductId=ssm
&ResourceId=resourceId
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "RequestId": "fe11aa29-0cc2-4204-bfea-6ebb30cc00d7"
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)

- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
FailedOperation.CmkUsedByCloudProduct	The CMK is being used by a Tencent Cloud product.
InternalError	Internal error.
InvalidParameter	Invalid parameter.
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
ResourceUnavailable.CmkNotFound	The CMK does not exist.
ResourceUnavailable.CmkStateNotSupport	This operation cannot be performed under the current CMK status.
UnsupportedOperation.ServiceTemporaryUnavailable	The service is temporarily unavailable.

GetRegions

最近更新时间：2023-08-07 17:45:15

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to return all regions support KMS service.

A maximum of 100 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: GetRegions.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.

3. Output Parameters

Parameter Name	Type	Description
Regions	Array of String	The list of supported regions Note: this field may return null, indicating that no valid values can be obtained.
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.

4. Example

Example1 Querying the list of supported regions

Input Example

```
https://kms.tencentcloudapi.com/?Action=GetRegions
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "Regions": [
      "ap-hongkong",
      "ap-guangzhou"
    ],
    "RequestId": "1b580852-1e38-11e9-b129-5cb9019b4b00"
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
InternalError	Internal error.

CancelKeyArchive

最近更新时间：2023-08-07 17:45:16

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to unarchive keys. If a key is unarchived, its status will be `Enabled`.

A maximum of 100 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: CancelKeyArchive.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
KeyId	Yes	String	Unique CMK ID

3. Output Parameters

Parameter Name	Type	Description
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.

4. Example

Example1 Unarchiving keys

Input Example

```
https://kms.tencentcloudapi.com/?Action=CancelKeyArchive
&KeyId=23e80852-1e38-11e9-b129-5cb9019b4b01
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "RequestId": "1b580852-1e38-11e9-b129-5cb9019b4b00"
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
ResourceUnavailable.CmkNotFound	The CMK does not exist.
ResourceUnavailable.CmkStateNotSupport	This operation cannot be performed under the current CMK status.
UnauthorizedOperation	Unauthorized operation.
UnsupportedOperation.NotUserCreatedCmk	You can only update the CMKs created by you.
UnsupportedOperation.ServiceTemporaryUnavailable	The service is temporarily unavailable.

ArchiveKey

最近更新时间：2023-08-07 17:45:16

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to archive keys. The archived keys can only be used for decryption but not encryption.

A maximum of 100 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: ArchiveKey.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
KeyId	Yes	String	Unique CMK ID

3. Output Parameters

Parameter Name	Type	Description
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.

4. Example

Example1 Archiving keys

Input Example

```
https://kms.tencentcloudapi.com/?Action=ArchiveKey
&KeyId=23e80852-1e38-11e9-b129-5cb9019b4b01
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "RequestId": "1b580852-1e38-11e9-b129-5cb9019b4b00"
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
FailedOperation.CmkUsedByCloudProduct	The CMK is being used by a Tencent Cloud product.
InternalError	Internal error.
InvalidParameter	Invalid parameter.
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
ResourceUnavailable.CmkNotFound	The CMK does not exist.
ResourceUnavailable.CmkStateNotSupport	This operation cannot be performed under the current CMK status.
UnauthorizedOperation	Unauthorized operation.
UnsupportedOperation.NotUserCreatedCmk	You can only update the CMKs created by you.
UnsupportedOperation.ServiceTemporaryUnavailable	The service is temporarily unavailable.

Asymmetric Key APIs

PostQuantumCryptoVerify

最近更新时间：2023-08-07 17:45:17

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to verify a signature using PQC.

A maximum of 20 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: PostQuantumCryptoVerify.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
KeyId	Yes	String	Unique ID of a key
SignatureValue	Yes	String	Signature value, which is generated by calling the <code>PostQuantumCryptoSign</code> API.
Message	Yes	String	Original message text before Base64 encoding. It cannot exceed 4096 bytes.

3. Output Parameters

Parameter Name	Type	Description
SignatureValid	Boolean	Verify whether the signature is valid. <code>true</code> : The signature is valid. <code>false</code> : The signature is invalid.
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.

4. Example

Example1 Verifying a signature with PQC

This example shows you how to verify a signature using PQC.

Input Example

```
POST / HTTP/1.1
Host: kms.tencentcloudapi.com
Content-Type: application/json
X-TC-Action: PostQuantumCryptoVerify
<Common request parameters>

{
  "KeyId": "abc",
  "SignatureValue": "abc",
  "Message": "abc"
}
```

Output Example

```
{
  "Response": {
    "SignatureValid": true,
    "RequestId": "abc"
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.
InvalidParameterValue	Incorrect parameter value.
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
ResourceUnavailable.CmkNotFound	The CMK does not exist.
ResourceUnavailable.CmkStateNotSupport	This operation cannot be performed under the current CMK status.

PostQuantumCryptoSign

最近更新时间：2023-08-07 17:45:17

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to sign u200dusing PQC.

A maximum of 20 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: PostQuantumCryptoSign.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
Message	Yes	String	Original message text before Base64 encoding. It cannot exceed 4096 bytes.
KeyId	Yes	String	Unique ID of a key

3. Output Parameters

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

Name		
Signature	String	Base64-encoded signature You can use PostQuantumCryptoVerify to verify the signature value.
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.

4. Example

Example1 Generating a signature using PQC

This example shows you how to generate a signature using PQC.

Input Example

```
POST / HTTP/1.1
Host: kms.tencentcloudapi.com
Content-Type: application/json
X-TC-Action: PostQuantumCryptoSign
<Common request parameters>

{
  "Message": "abc",
  "KeyId": "abc"
}
```

Output Example

```
{
  "Response": {
    "Signature": "abc",
    "RequestId": "abc"
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
AuthFailure	CAM signature/authentication error
InternalError	Internal error.
InvalidParameter	Invalid parameter.
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
MissingParameter	Missing parameters. Please check and try again.
ResourceUnavailable.CmkNotFound	The CMK does not exist.
ResourceUnavailable.CmkStateNotSupport	This operation cannot be performed under the current CMK status.

GetPublicKey

最近更新时间：2023-08-07 17:45:17

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to get the public key of an asymmetric KMS key (which must be enabled). With the public key, you can encrypt messages and verify signatures.

A maximum of 100 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: GetPublicKey.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
KeyId	Yes	String	Unique CMK ID.

3. Output Parameters

Parameter Name	Type	Description
KeyId	String	Unique CMK ID.

PublicKey	String	Base64-encoded public key content.
PublicKeyPem	String	Public key content in PEM format.
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.

4. Example

Example1 Getting the public key of an asymmetric key

Input Example

```
https://kms.tencentcloudapi.com/?Action=GetPublicKey
&KeyId=554ef4b3-3071-11ea-a86a-5254006d0810
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "RequestId": "8918bd5b-e189-4e2d-b718-01c9f99acd45",
    "KeyId": "554ef4b3-3071-11ea-a86a-5254006d0810",
    "PublicKey": "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAz00TVMh28VCjOE5DM1BM8a2
qIjgipYByb7WE/GyTRLUiIGDUq44VIM5fNI9nVeIf2D+4pIiU0s4LUYnLxkGcFKUVWkz3nubUzbNdSHRb
NjKhbFyyRGT6YYxqMfvCmNXMA3OE56EmvsWU9VwVXqRPOFTaODCx8bRd+R6O+Aho9GaRfwLKHt1X7doch
dDs9SWC6iybRISgpLEh4tvzcSlBemEuyx5U/X/BoL+sVnSsC/XT8J9w0EvJVHZAaBW7OhIbBOolhzWTF8T
pL/7ncZZUbtFP4SrAkVkgOEIEfRhv5vh5LfSxiS2zQzIShrT6JYqh5IgDIHTdCcPiYmTsk/lmM2wIDAQA
B",
    "PublicKeyPem": "-----BEGIN PUBLIC KEY-----\nTUlJQklqQU5CZ2txaGtpRzl3MEJBUUVGQUFP
Q0FROEFNSUlcQ2dLQ0FRRUF6ME9U\nVkl0MjhWQ2pPRTVETWxCTThhMnFJamdpclCeWI3V0UvR3lUUXkx
VaUlHRFVxNDRW\nSU01Zk5JOW5WZUlmMkQrNHBjaVUwczRMVWluTHhrR2NGS1VWV2t6M251Y1V6Yk5k\n
U0hSYk5qS2hiRnl5UkdUN1lZeHFNZnZDbU5YTUEzT0U1NkVtdnNXVTlWd1ZyYVJQ\nT0ZUYU9EQ3g4Y1J
kK1I2TytBaG85R2FSZndMS0h0bFg3ZG9jaGREczlTV0M2aXli\nUkl1Tz3BMRWg0dHZ6Y1NsQmVtRXV5eD
VVL1gvQm9MK3NWblNzQy9YVDhKOXcwRXZK\nVkhayUJXN09oSWJCT29saHpXVEY4VHBMLzduY1paVWJ0Z
1A0U3JBa3ZLZ29FSUVm\nUmh2NXZoNUxmU3hpUzJ6UXpJU2hyVDZKWXFoNUlnRELIVGRDY1BpWW1Uc2sv
bG1N\nMndJREFRQUI=\n-----END PUBLIC KEY-----\n"
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
ResourceUnavailable.CmkNotFound	The CMK does not exist.
ResourceUnavailable.CmkStateNotSupport	This operation cannot be performed under the current CMK status.
UnauthorizedOperation	Unauthorized operation.

AsymmetricSm2Decrypt

最近更新时间：2023-08-07 17:45:17

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to decrypt data with the specified private key that is encrypted with SM2 asymmetric cryptographic algorithm. The ciphertext must be encrypted with the corresponding public key. The asymmetric key must be in `Enabled` state for decryption. The length of the ciphertext passed in cannot exceed 256 bytes.

A maximum of 200 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: AsymmetricSm2Decrypt.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
KeyId	Yes	String	Unique CMK ID
Ciphertext	Yes	String	Base64-encoded ciphertext encrypted with <code>PublicKey</code> , whose length cannot exceed 256 bytes.

3. Output Parameters

--	--	--

Parameter Name	Type	Description
KeyId	String	Unique CMK ID
Plaintext	String	Base64-encoded plaintext after decryption
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.

4. Example

Example1 Decrypting data with an SM2 asymmetric key

Input Example

```
https://kms.tencentcloudapi.com/?Action=AsymmetricSm2Decrypt
&KeyId=554ef4b3-3071-11ea-a86a-5254006d0810
&Ciphertext=Fb0UICocErQgNEkYKJagtoKNed7DLeo5UkZzPJMyI94CfWh6yKHGgb/0PBHrCve2Avo4g
JI5pJMWP3Aq5ggX0aunLv87UX+sgO1/3HXW+q4ARaiwZ9Q73RQuPg6qJ2Eg33uZ2Xjey3l+5yHiOdZYmC
VePtKAsuhxzKw/sALTbGTYYnbJXnGKr3Yu7Hs0hCC1bOz0sNqd1IXdUyMtQtbDOV8NWg2ecdZPIodbnrC
KIQ4rpMUghjSFv3rSHo5VbpuOGPXqEZT4goou42psIXb03li3TXxFZMTAdxVMzpqEuTfRximPEqyPEHe6
xG92vJX0FZfWU8Y5SxlfXp+mvBbAmw==
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "RequestId": "7c076c83-1402-41d8-8ce6-73a350a9eaf6",
    "KeyId": "554ef4b3-3071-11ea-a86a-5254006d0810",
    "Plaintext": "dGVzdA=="
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
FailedOperation.DecryptError	Decryption failed.
InternalError	Internal error.
InvalidParameter	Invalid parameter.
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
InvalidParameterValue.InvalidKeyUsage	Incorrect <code>KeyUsage</code> parameter.
ResourceUnavailable.CmkNotFound	The CMK does not exist.
ResourceUnavailable.CmkStateNotSupport	This operation cannot be performed under the current CMK status.
UnauthorizedOperation	Unauthorized operation.
UnsupportedOperation.UnsupportedKeyUsageInCurrentRegion	The encryption method is not supported in the current region.

AsymmetricRsaDecrypt

最近更新时间：2023-08-07 17:45:17

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to decrypt data with the specified private key that is encrypted with RSA asymmetric cryptographic algorithm. The ciphertext must be encrypted with the corresponding public key. The asymmetric key must be in `Enabled` state for decryption.

A maximum of 200 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: AsymmetricRsaDecrypt.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
KeyId	Yes	String	Unique CMK ID
Ciphertext	Yes	String	Base64-encoded ciphertext encrypted with <code>PublicKey</code>
Algorithm	Yes	String	Corresponding algorithm when a public key is used for encryption. Valid values: RSAES_PKCS1_V1_5, RSAES_OAEP_SHA_1, RSAES_OAEP_SHA_256

3. Output Parameters

Parameter Name	Type	Description
KeyId	String	Unique CMK ID
Plaintext	String	Base64-encoded plaintext after decryption
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.

4. Example

Example1 Decrypting data with an RSA asymmetric key

Input Example

```
https://kms.tencentcloudapi.com/?Action=AsymmetricRsaDecrypt
&KeyId=554ef4b3-3071-11ea-a86a-5254006d0810
&Ciphertext=Fb0UICocErQgNEkYKJagtoKNed7DLeo5UkZzPJMyI94CfWh6yKHGgb/0PBHrCve2Avo4g
JI5pJMWp3Aq5ggX0aunLv87UX+sgO1/3HXW+q4ARaiwZ9Q73RQuPg6qJ2Eg33uZ2Xjey3l+5yHiOdZYmC
VePtKAsuhxzKw/sALTbGTYYnbJXnGKr3Yu7Hs0hCC1bOz0sNqd1IXdUyMtQtbDOV8NWg2ecdZPIOdbnrC
KIQ4rpMUghjSFv3rSHo5VbpuOGPXqEZT4goou42psIXb03li3TXxFZMTAdxVMzpqEuTfRxIMPEqyPEHe6
xG92vJX0FZfWU8Y5SxlfXp+mvBbAmw==
&Algorithm=RSAES_OAEP_SHA_1
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "RequestId": "7c076c83-1402-41d8-8ce6-73a350a9eaf6",
    "KeyId": "554ef4b3-3071-11ea-a86a-5254006d0810",
    "Plaintext": "dGVzdA=="
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
FailedOperation.DecryptError	Decryption failed.
InternalError	Internal error.
InvalidParameter	Invalid parameter.
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
InvalidParameterValue.InvalidKeyUsage	Incorrect <code>KeyUsage</code> parameter.
ResourceUnavailable.CmkNotFound	The CMK does not exist.
ResourceUnavailable.CmkStateNotSupport	This operation cannot be performed under the current CMK status.
UnauthorizedOperation	Unauthorized operation.

VerifyByAsymmetricKey

最近更新时间：2023-08-07 17:45:16

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to verify a signature with an asymmetric key.

A maximum of 100 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: VerifyByAsymmetricKey.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
KeyId	Yes	String	Unique ID of a key
SignatureValue	Yes	String	Signature value, which is generated by calling the KMS signature API.
Message	Yes	String	Full message or message abstract. Before Base64 encoding, an original message can contain up to 4,096 bytes while a message abstract must be 32 bytes.
Algorithm	Yes	String	Signature algorithm. The valid values include <code>SM2DSA</code> , <code>ECC_P256_R1</code> , <code>RSA_PSS_SHA_256</code> , and

			RSA_PKCS1_SHA_256 , etc. You can get a full list of supported algorithms using the ListAlgorithms API.
MessageType	No	String	Message type. Valid values: RAW (indicating an original message; used by default if the parameter is not passed in) and DIGEST .

3. Output Parameters

Parameter Name	Type	Description
SignatureValid	Boolean	Whether the signature is valid. true : the signature is valid; false : the signature is invalid.
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.

4. Example

Example1 Verifying a signature with an asymmetric key

Input Example

```
https://kms.tencentcloudapi.com/?Action=VerifyByAsymmetricKey
&Algorithm=SM2DSA
&Message=Zsfw9GLu7dnR8tRr3BDk4kFnxIdc8veiKX2gK49LqOA%3D
&KeyId=6cdf26d1-44ff-11eb-841c-5254006d0810
&MessageType=DIGEST
&SignatureValue=MEUCIQDeO1wB%2F5dEfprulvh9Zw06UJylDt9R8MQY5qRMjzhXJgIgPKO2kKicFKe
mwOf8SgniUA692ORrqVEabS3kcbPL8U%3D
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "RequestId": "3e634985-c311-4790-953a-44990f7bec6b",
    "SignatureValid": true
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
InternalServerError	Internal error.
InvalidParameter	Invalid parameter.
InvalidParameterValue	Incorrect parameter value.
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
ResourceUnavailable.CmkNotFound	The CMK does not exist.
ResourceUnavailable.CmkStateNotSupport	This operation cannot be performed under the current CMK status.

SignByAsymmetricKey

最近更新时间：2023-08-07 17:45:16

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to generate a signature with an asymmetric key.

Note that only when KeyUsage is `ASYMMETRIC_SIGN_VERIFY_${ALGORITHM}` (e.g., `ASYMMETRIC_SIGN_VERIFY_SM2` and `ASYMMETRIC_SIGN_VERIFY_ECC`), the key can be used for signing.

A maximum of 100 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: SignByAsymmetricKey.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
Algorithm	Yes	String	Signature algorithm. The valid values include <code>SM2DSA</code> , <code>ECC_P256_R1</code> , <code>RSA_PSS_SHA_256</code> , and <code>RSA_PKCS1_SHA_256</code> , etc. You can get a full list of supported algorithms using the ListAlgorithms API.
Message	Yes	String	Full message or message abstract. Before Base64 encoding, an original message can contain up to 4,096 bytes while a message abstract must be 32 bytes.

KeyId	Yes	String	Unique ID of a key
MessageType	No	String	Message type. Valid values: <code>RAW</code> (indicating an original message; used by default if the parameter is not passed in) and <code>DIGEST</code> .

3. Output Parameters

Parameter Name	Type	Description
Signature	String	Base64-encoded signature
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.

4. Example

Example1 Generating a signature with an asymmetric key

Input Example

```
https://kms.tencentcloudapi.com/?Action=SignByAsymmetricKey
&Algorithm=SM2DSA
&Message=Zsfw9GLu7dnR8tRr3BDk4kFnXIdc8veiKX2gK49LqOA%3D
&KeyId=6cdf26d1-44ff-11eb-841c-5254006d0810
&MessageType=DIGEST
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "RequestId": "e86d6131-2830-4e1c-9d03-d421affd646c",
    "Signature": "MEUCICr/JCV52BqGvI0iYxdZ1eL8zzJjx39mWNv2ZWdLOMvRAiEApO6os3Wj0Tg302fbTBr02IxHO1aCr0Zr41t4hi6yTG8="
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
AuthFailure	CAM signature/authentication error
InternalError	Internal error.
InvalidParameter	Invalid parameter.
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
MissingParameter	Missing parameters. Please check and try again.
ResourceUnavailable.CmkNotFound	The CMK does not exist.
ResourceUnavailable.CmkStateNotSupport	This operation cannot be performed under the current CMK status.

White-Box Key APIs

EncryptByWhiteBox

最近更新时间：2023-08-07 17:45:11

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to encrypt data with a white-box key.

A maximum of 100 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: EncryptByWhiteBox.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
KeyId	Yes	String	Globally unique white-box key ID
PlainText	Yes	String	Base64-encoded text to be encrypted. The size of the original text cannot exceed 4 KB.
InitializationVector	No	String	Base64-encoded initialization vector of 16 bytes, which will be used by the encryption algorithm. If this parameter is not passed in, the backend service will generate a random one. You should save this value as a parameter for decryption.

3. Output Parameters

Parameter Name	Type	Description
InitializationVector	String	Base64-encoded initialization vector, which will be used by the encryption algorithm. If this parameter is passed in by the caller, it will be returned as-is; otherwise, the backend service will generate a random one and return it.
CipherText	String	Base64-encoded ciphertext after encryption
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.

4. Example

Example1 Encrypting data with a white-box key

Input Example

```
https://kms.tencentcloudapi.com/?Action=EncryptByWhiteBox
&KeyId=244dab8c-6dad-11ea-80c6-5254006d0810
&PlainText=UGxhaW5UZXBh0
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "RequestId": "4b3be01e-117a-43f5-aa34-dd5034efe3dd",
    "InitializationVector": "BQbVImt3p_xr8VQebZaXGQ==",
    "CipherText": "ZKHH21a4DpwlkwjANQ5hgw=="
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
InternalServerError	Internal error.
InvalidParameterValue	Incorrect parameter value.
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
ResourceNotFound	The resource does not exist.
ResourceUnavailable.KeyDisabled	The key has been disabled.
ResourceUnavailable.NotPurchased	The white-box key service has not been activated.
UnauthorizedOperation	Unauthorized operation.

EnableWhiteBoxKeys

最近更新时间：2023-08-07 17:45:11

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to enable white-box keys in batches.

A maximum of 200 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: EnableWhiteBoxKeys.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
KeyIds.N	Yes	Array of String	List of globally unique white-box key IDs. Note: you should make sure that all provided <code>KeyId</code> values are in valid format, unique, and actually exist. Up to 50 ones are allowed.

3. Output Parameters

Parameter Name	Type	Description

RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.
-----------	--------	--

4. Example

Example1 Batch enabling white-box keys

Input Example

```
https://kms.tencentcloudapi.com/?Action=EnableWhiteBoxKeys
&KeyIds.0=23e80852-1e38-11e9-b129-5cb9019b4b01
&KeyIds.1=23e80852-1e38-11e9-b129-5cb9019b4b02
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "RequestId": "850bf779-2249-4995-8c55-b3966daf0a8c"
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.
InvalidParameterValue.DuplicatedKeyId	Duplicate <code>KeyId</code> .
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
ResourceNotFound	The resource does not exist.
ResourceUnavailable.NotPurchased	The white-box key service has not been activated.
UnauthorizedOperation	Unauthorized operation.

EnableWhiteBoxKey

最近更新时间：2023-08-07 17:45:12

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to enable a white-box key.

A maximum of 200 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: EnableWhiteBoxKey.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
KeyId	Yes	String	Globally unique white-box key ID

3. Output Parameters

Parameter Name	Type	Description
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for

		locating a problem.
--	--	---------------------

4. Example

Example1 Enabling a white-box key

Input Example

```
https://kms.tencentcloudapi.com/?Action=EnableWhiteBoxKey
&KeyId=23e80852-1e38-11e9-b129-5cb9019b4b01
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "RequestId": "850bf779-2249-4995-8c55-b3966daf0a8c"
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
InternalError	Internal error.
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
ResourceNotFound	The resource does not exist.
ResourceUnavailable.NotPurchased	The white-box key service has not been activated.
UnauthorizedOperation	Unauthorized operation.

DisableWhiteBoxKeys

最近更新时间：2023-08-07 17:45:12

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to disable white-box keys in batches.

A maximum of 200 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: DisableWhiteBoxKeys.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
KeyIds.N	Yes	Array of String	List of globally unique white-box key IDs. Note: you should make sure that all provided <code>KeyId</code> values are in valid format, unique, and actually exist. Up to 50 ones are allowed.

3. Output Parameters

Parameter Name	Type	Description

RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.
-----------	--------	--

4. Example

Example1 Batching disabling white-box keys

Input Example

```
POST / HTTP/1.1
Host: kms.tencentcloudapi.com
Content-Type: application/json
X-TC-Action: DisableWhiteBoxKeys
<Common request parameters>

{
  "KeyIds": [
    "23e80852-1e38-11e9-b129-5cb9019b4b02",
    "23e80852-1e38-11e9-b129-5cb9019b4b01"
  ]
}
```

Output Example

```
{
  "Response": {
    "RequestId": "1b580852-1e38-11e9-b129-5cb9019b4b00"
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)

- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
InternalServerError	Internal error.
InvalidParameter	Invalid parameter.
InvalidParameterValue.DuplicatedKeyId	Duplicate <code>KeyId</code> .
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
ResourceNotFound	The resource does not exist.
ResourceUnavailable.NotPurchased	The white-box key service has not been activated.
UnauthorizedOperation	Unauthorized operation.

DisableWhiteBoxKey

最近更新时间：2023-08-07 17:45:12

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to disable a white-box key.

A maximum of 200 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: DisableWhiteBoxKey.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
KeyId	Yes	String	Globally unique white-box key ID

3. Output Parameters

Parameter Name	Type	Description
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for

		locating a problem.
--	--	---------------------

4. Example

Example1 Disabling a white-box key

Input Example

```
https://kms.tencentcloudapi.com/?Action=DisableWhiteBoxKey
&KeyId=244dab8c-6dad-11ea-80c6-5254006d0810
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "RequestId": "850bf779-2249-4995-8c55-b3966daf0a8c"
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
InternalError	Internal error.
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
ResourceNotFound	The resource does not exist.
ResourceUnavailable.NotPurchased	The white-box key service has not been activated.
UnauthorizedOperation	Unauthorized operation.

DescribeWhiteBoxServiceStatus

最近更新时间：2023-08-07 17:45:12

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to get the white-box key service status.

A maximum of 200 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: DescribeWhiteBoxServiceStatus.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.

3. Output Parameters

Parameter Name	Type	Description
ServiceEnabled	Boolean	Whether the user's white-box key service is available
RequestId	String	The unique request ID, which is returned for each request. RequestId is

		required for locating a problem.
--	--	----------------------------------

4. Example

Example1 Querying the white-box key service status

Input Example

```
https://kms.tencentcloudapi.com/?Action=DescribeWhiteBoxServiceStatus
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "RequestId": "8a5ab931-bb22-4d55-9042-e1ef1a36c941",
    "ServiceEnabled": true
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
InternalError	Internal error.
ResourceUnavailable.NotPurchased	The white-box key service has not been activated.
UnauthorizedOperation	Unauthorized operation.

DescribeWhiteBoxKeyDetails

最近更新时间：2023-08-07 17:45:12

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to get the white-box key list.

A maximum of 100 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: DescribeWhiteBoxKeyDetails.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
KeyStatus	No	Integer	Filter: key status. 0: disabled, 1: enabled
Offset	No	Integer	This parameter has the same meaning of the <code>Offset</code> in an SQL query, indicating that this acquisition starts from the "No. Offset value" element of the array arranged in a certain order. The default value is 0.
Limit	No	Integer	This parameter has the same meaning of the <code>Limit</code> in an SQL query, indicating that up to <code>Limit</code> value elements can be obtained in this request. The default value is 0, indicating not to paginate.

TagFilters.N	No	Array of TagFilter	Tag filter condition
--------------	----	------------------------------------	----------------------

3. Output Parameters

Parameter Name	Type	Description
KeyInfos	Array of WhiteboxKeyInfo	White-box key information list
TotalCount	Integer	Total white-box keys. Note: This field may return null, indicating that no valid values can be obtained.
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.

4. Example

Example1 Getting the white-box key list

Input Example

```
POST / HTTP/1.1
Host: kms.tencentcloudapi.com
Content-Type: application/json
X-TC-Action: DescribeWhiteBoxKeyDetails
<Common request parameters>

{ }
```

Output Example

```
{
  "Response": {
    "KeyInfos": [
      {
        "Status": "xx",
        "DecryptKey": "xx",
        "KeyId": "xx",
```

```
"Description": "xx",
"CreatorUin": 1,
"ResourceId": "xx",
"OwnerUin": 1,
"Algorithm": "xx",
"Alias": "xx",
"EncryptKey": "xx",
"CreateTime": 1,
"DeviceFingerprintBind": true
},
{
  "Status": "xx",
  "DecryptKey": "xx",
  "KeyId": "xx",
  "Description": "xx",
  "CreatorUin": 1,
  "ResourceId": "xx",
  "OwnerUin": 1,
  "Algorithm": "xx",
  "Alias": "xx",
  "EncryptKey": "xx",
  "CreateTime": 1,
  "DeviceFingerprintBind": true
}
],
"TotalCount": 2,
"RequestId": "xx"
}
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)

- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
InternalError	Internal error.
InvalidParameterValue	Incorrect parameter value.
ResourceUnavailable.NotPurchased	The white-box key service has not been activated.
UnauthorizedOperation	Unauthorized operation.

DescribeWhiteBoxKey

最近更新时间：2023-08-07 17:45:13

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to display white-box key information.

A maximum of 200 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: DescribeWhiteBoxKey.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
KeyId	Yes	String	Globally unique white-box key ID

3. Output Parameters

Parameter Name	Type	Description
KeyInfo	WhiteboxKeyInfo	White-box key information

RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.
-----------	--------	--

4. Example

Example1 Displaying white-box key information

Input Example

```
https://kms.tencentcloudapi.com/?Action=DescribeWhiteBoxKey
&KeyId=244dab8c-6dad-11ea-80c6-5254006d0810
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "RequestId": "395989ef-4e4a-4f16-856d-3bb5a86ba99c",
    "KeyInfo": {
      "KeyId": "244dab8c-6dad-11ea-80c6-5254006d0810",
      "Alias": "xx",
      "CreateTime": 1585040099,
      "Description": "xx",
      "CreatorUin": 0,
      "OwnerUin": 0,
      "Status": "Disabled",
      "Algorithm": "SM4",
      "EncryptKey": "AAAAACL4R9T1M3r3/S9XpMbUbW HJUKbq/tl10Bop7LG90lHpj+DKmOiEE0Rs5rRrMN
aCYIWzWJyU0SNQoX1Wnn06QB2qrhDCXEPdwMwgJHx+YfJHUH/eSF5/LUEv27ltidqJyUk3HF5CZgjkN90
1hFEPf9ZCJCeo5XrORpopW7Ur6svPAjDtIPN3kUDCTqgTPC+FBX0cO/zEZFeMMAU2BPwe6f501x5BTrCB
Ef4qJDpZqT/WxXvSid8pFQ8uSxMqaf0ot57NzfuWG92oAe9HQ7bDCcfuBN7nXX+QipQIBxD/LVWk7zrHt
LD/TJfAAoTue7QKc/lSTOpI1xkTxJq/AFLd5K9EaBN7kpAkAsponZc20Tpk+KlyWE3NHdQrION9fsxtUB
15tz/l6T1j49SR5J2axZ2nnkA3o7L1WIGiv7r3tkd+",
      "DecryptKey": "AAAAACL4R9T1M3r3/S9XpMbUbW HJUKbq/tl10Bop7LG90lHpj+DKmOiEE0Rs5rRrMN
aCYIWzWJyU0SNQoX1Wnn06QB2qrhDCXEPdwMwgJHx+YfJHUH/eSF5/LUEv27ltidqJyUk3HF5CZgjkN90
1hFEPf9ZCJCeo5XrORpopW7Ur6svPAjDtIPN3kUDCTqgTPC+FBX0cO/zEZFeMMAU2BPwe6f501x5BTrCB
Ef4qJDpZqT/WxXvSid8pFQ8uSxMqaf0ot57NzfuWG92oAe9HQ7bDCcfuBN7nXX+QipQIBxD/LVWk7zrHt
LD/TJfAAoTue7QKc/lSTOpI1xkTxJq/AFLd5K9EaBN7kpAkAsponZc20Tpk+KlyWE3NHdQrION9fsxtUB
15tz/l6T1j49SR5J2axZ2nnkA3o7L1WIGiv7r3tkd+",
      "DeviceFingerprintBind": true,
      "ResourceId": "xx"
    }
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
InternalError	Internal error.
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
ResourceNotFound	The resource does not exist.
ResourceUnavailable.NotPurchased	The white-box key service has not been activated.
UnauthorizedOperation	Unauthorized operation.

DescribeWhiteBoxDecryptKey

最近更新时间：2023-08-07 17:45:13

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to get a white-box decryption key.

A maximum of 200 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: DescribeWhiteBoxDecryptKey.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
KeyId	Yes	String	Globally unique white-box key ID

3. Output Parameters

Parameter Name	Type	Description
DecryptKey	String	Base64-encoded white-box decryption key

RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.
-----------	--------	--

4. Example

Example1 Getting a white-box decryption key

Input Example

```
https://kms.tencentcloudapi.com/?Action=DescribeWhiteBoxDecryptKey
&KeyId=244dab8c-6dad-11ea-80c6-5254006d0810
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "RequestId": "8788b5f3-8eaa-48a8-915a-b7c52f57065e",
    "DecryptKey": "AAAAACL4R9T1M3r3/S9XpMbUbwHJUKbq/tl10Bop7LG90lHpj+DKmOiEE0Rs5rRrMN
aCYIWzWJyU0SNQoX1WNn06QB2qrhDCXEPdwMwgJHx+YfJHUh/eSF5/LUEv27ltidqJyUk3HF5CZgjkN90
1hFEPf9ZCJcEo5XrORpopW7Ur6svPAjDtIPN3kUDCTqgTPC+FBX0cO/zEZFeMMAU2BPwe6f501x5BTrCB
Ef4qJdpZqT/WxXvSid8pFQ8uSxMqaf0ot57NzfuWG92oAe9HQ7bDCcfuBN7nXX+QipQIBxD/LVWk7zrHt
LD/TJfAAoTuE7QKc/lSTOpI1xkTxJq/AFLd5K9EaBN7kpAkAsponZc20Tpk+KlyWE3NHdQrION9fsxtUB
15tz/l6T1j49SR5J2axZ2nnkA3o7L1WIGiv7r3tkd+"
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)

- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
InternalError	Internal error.
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
ResourceNotFound	The resource does not exist.
ResourceUnavailable.NotPurchased	The white-box key service has not been activated.
UnauthorizedOperation	Unauthorized operation.

DeleteWhiteBoxKey

最近更新时间：2023-08-07 17:45:13

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to delete a white-box key. Note: only disabled white-box keys can be deleted.

A maximum of 200 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: DeleteWhiteBoxKey.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
KeyId	Yes	String	Globally unique white-box key ID

3. Output Parameters

Parameter Name	Type	Description
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for

		locating a problem.
--	--	---------------------

4. Example

Example1 Deleting a white-box key

Input Example

```
https://kms.tencentcloudapi.com/?Action=DeleteWhiteBoxKey
&KeyId=244dab8c-6dad-11ea-80c6-5254006d0810
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "RequestId": "850bf779-2249-4995-8c55-b3966daf0a8c"
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
FailedOperation	Operation failed.
InternalError	Internal error.
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
ResourceNotFound	The resource does not exist.
ResourceUnavailable.NotPurchased	The white-box key service has not been activated.
UnauthorizedOperation	Unauthorized operation.

CreateWhiteBoxKey

最近更新时间：2023-08-07 17:45:13

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to create a white-box key. Up to 50 ones can be created.

A maximum of 100 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: CreateWhiteBoxKey.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
Alias	Yes	String	Unique alias that makes a key more recognizable and understandable. This parameter should be 1 to 60 letters, digits, <code>-</code> , and <code>_</code> ; it must begin with a letter or digit and cannot be left empty.
Algorithm	Yes	String	All algorithm types for creating keys. Valid values: AES_256, SM4
Description	No	String	Key description of up to 1024 bytes
Tags.N	No	Array of Tag	Tag list

3. Output Parameters

Parameter Name	Type	Description
EncryptKey	String	Base64-encoded encryption key
DecryptKey	String	Base64-encoded decryption key
KeyId	String	Globally unique white-box key ID
TagCode	Integer	Tag operation return code. 0: success; 1: internal error; 2: business processing error
TagMsg	String	Tag operation return message
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.

4. Example

Example1 Creating a white-box key

Input Example

```
https://kms.tencentcloudapi.com/?Action=CreateWhiteBoxKey
&Alias=test_alias
&Description=test_description
&Algorithm=SM4
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "RequestId": "3691b76c-1ba5-4f93-88ad-858d23ba6c8a",
    "EncryptKey": "AAAAAHP6lsgUa4mYE/cT5LGkquR3xKzUG+cB6oWJ7exbmFR37G6QCB2dEjpdq6+JvmC7cbiDXUFaExxSHQTj1JAzTh/T4p6BZy31uiPXogOnsDEm/vGnh3AJQBopXreiUYe54ZlpJPd/yZocQhsFhiNw2Bmqy6bkb4LrzT2FvzHh5YhwNLRuJnou3G5OecuvaNQoz2L9hkCSc4s7iUaiCMzzDgCnfCYhggKP+HtaqOMv0LKRzTjSYKxdmzWjPT1vMUxv2Mtk+fF/5gEI6z++eybnWsyJHTx03YnF52sVw5RNs3axXRmOQWUOIoswKmb8M/urWdUio6ZZeE2fMPBg2H2GJvf5wbtCsHLFwdUZBQJ/VcgLXHj0VQxUdUffL/yZfvIOXAzACvkiZmUEIRP422s5EXIJffLzA5S+aJgl1Kwp7XI",
    "DecryptKey": "AAAAAHP6lsgUa4mYE/cT5LGkquR3xKzUG+cB6oWJ7exbmFR37G6QCB2dEjpdq6+Jvm
```

```
C7cbiDXUFaExxSHQTjlJAzTh/T4p6BZy31uiPXogOnsDEm/vGnh3AJQBopXreiUYe54ZlpJPd/yZocQhs
FhiNw2Bmqy6bqp4LrzT2FvzHh5YhwNLRuJnou3G5OecuvaNQoz2L9hkCSc4s7iUaiCMzzDgCnfCYhggKP
+HtaqOMv0LKRzTjSYKxdmzWjPT1vMUxv2Mtk+fF/5gEI6z++eybnWsyJHTx03YnF52sVw5RNs3axXRmOQ
WUOIoswKmb8M/urWdUio6ZZeE2fMPBg2H2GJvf5wbtCsHLFwdUZBQJ/VcgLXHj0VQxUdUffL/yZfvIOX
AzACvkiZmUEIRP422s5EXIJffLzA5S+aJgl1Kwp7XI",
"KeyId": "3235f222-6e40-11ea-8f2f-5254006d0810",
"TagMsg": "xx",
"TagCode": 1
}
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
InternalError	Internal error.
InvalidParameterValue	Incorrect parameter value.
InvalidParameterValue.AliasAlreadyExists	The alias already exists.

InvalidParameterValue.InvalidAlias	Incorrect alias format
InvalidParameterValue.TagKeysDuplicated	Duplicate tag key.
InvalidParameterValue.TagsNotExisted	The tag key or tag value does not exist.
LimitExceeded.KeyLimitExceeded	The number of created keys exceeded the limit.
ResourceUnavailable.NotPurchased	The white-box key service has not been activated.
UnauthorizedOperation	Unauthorized operation.

OverwriteWhiteBoxDeviceFingerprints

最近更新时间：2023-08-07 17:45:11

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to overwrite the device fingerprint information of a specified key.

A maximum of 100 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: OverwriteWhiteBoxDeviceFingerprints.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
KeyId	Yes	String	White-box key ID
DeviceFingerprints.N	No	Array of DeviceFingerprint	Device fingerprint list. If the list is empty, it means to delete all fingerprint information corresponding to the key. There can be up to 200 entries in the list.

3. Output Parameters

Parameter Name	Type	Description
RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.

4. Example

Example1 Overwriting the device fingerprint information of a specified key

Input Example

```
https://kms.tencentcloudapi.com/?Action=OverwriteWhiteBoxDeviceFingerprints
&KeyId=cd850a3d-9b1b-11ea-a96a-5254006d0810
&DeviceFingerprints.0.Identity=c19c024c-2ba1-11b2-a85c-96f970f4a8e1
&DeviceFingerprints.0.Description=desc1
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "RequestId": "c8d1f1b9-632a-4c0b-b369-9bcf8e7e6ef9"
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
InternalError	Internal error.
InvalidParameterValue	Incorrect parameter value.
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
LimitExceeded.FingerprintsLimitExceeded	The number of device fingerprints exceeded the limit.
ResourceNotFound	The resource does not exist.
ResourceUnavailable.NotPurchased	The white-box key service has not been activated.
UnauthorizedOperation	Unauthorized operation.

DescribeWhiteBoxDeviceFingerprints

最近更新时间：2023-08-07 17:45:13

1. API Description

Domain name for API request: kms.tencentcloudapi.com.

This API is used to get the device fingerprint list of a specified key.

A maximum of 100 requests can be initiated per second for this API.

We recommend you to use API Explorer

[Try it](#)

API Explorer provides a range of capabilities, including online call, signature authentication, SDK code generation, and API quick search. It enables you to view the request, response, and auto-generated examples.

2. Input Parameters

The following request parameter list only provides API request parameters and some common parameters. For the complete common parameter list, see [Common Request Parameters](#).

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params . The value used for this API: DescribeWhiteBoxDeviceFingerprints.
Version	Yes	String	Common Params . The value used for this API: 2019-01-18.
Region	No	String	Common Params . This parameter is not required for this API.
KeyId	Yes	String	White-box key ID

3. Output Parameters

Parameter Name	Type	Description
DeviceFingerprints	Array of DeviceFingerprint	Device fingerprint list

RequestId	String	The unique request ID, which is returned for each request. RequestId is required for locating a problem.
-----------	--------	--

4. Example

Example1 Getting the device fingerprint list of a specified key

Input Example

```
https://kms.tencentcloudapi.com/?Action=DescribeWhiteBoxDeviceFingerprints
&KeyId=cd850a3d-9b1b-11ea-a96a-5254006d0810
&<Common request parameters>
```

Output Example

```
{
  "Response": {
    "RequestId": "f643be96-3ea8-4abe-b148-0cc74436b2c1",
    "DeviceFingerprints": [
      {
        "Identity": "c19c024c-2ba1-11b2-a85c-96f970f4a8e1",
        "Description": "desc"
      }
    ]
  }
}
```

5. Developer Resources

SDK

TencentCloud API 3.0 integrates SDKs that support various programming languages to make it easier for you to call APIs.

- [Tencent Cloud SDK 3.0 for Python](#)
- [Tencent Cloud SDK 3.0 for Java](#)
- [Tencent Cloud SDK 3.0 for PHP](#)
- [Tencent Cloud SDK 3.0 for Go](#)
- [Tencent Cloud SDK 3.0 for NodeJS](#)
- [Tencent Cloud SDK 3.0 for .NET](#)

- [Tencent Cloud SDK 3.0 for C++](#)

Command Line Interface

- [Tencent Cloud CLI 3.0](#)

6. Error Code

The following only lists the error codes related to the API business logic. For other error codes, see [Common Error Codes](#).

Error Code	Description
InternalError	Internal error.
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
ResourceNotFound	The resource does not exist.
ResourceUnavailable.NotPurchased	The white-box key service has not been activated.
UnauthorizedOperation	Unauthorized operation.

Data Types

最近更新时间：2022-07-04 10:38:55

AlgorithmInfo

Algorithm name and ID

Used by actions: ListAlgorithms.

Name	Type	Description
KeyUsage	String	Algorithm ID
Algorithm	String	Algorithm name

DeviceFingerprint

Device fingerprint

Used by actions: DescribeWhiteBoxDeviceFingerprints, OverwriteWhiteBoxDeviceFingerprints.

Name	Type	Required	Description
Identity	String	Yes	Fingerprint information collected by device fingerprint collector. Its format must be in the following regular expression: <code>^[0-9a-f]{8}[-][0-9a-f]{14}[-][0-9a-f]{14}[-][0-9a-f]{14}[-][0-9a-f]{16}\$</code>
Description	String	No	Description, such as IP and device name. Length limit: 1,024 bytes Note: this field may return null, indicating that no valid values can be obtained.

Key

Returned CMK list information

Used by actions: ListKeys.

Name	Type	Description
KeyId	String	Globally unique CMK ID.

KeyMetadata

CMK attribute information

Used by actions: DescribeKey, DescribeKeys, ListKeyDetail.

Name	Type	Description
KeyId	String	Globally unique CMK ID
Alias	String	Alias that makes a key more recognizable and understandable
CreateTime	Integer	Key creation time
Description	String	CMK description
KeyState	String	CMK status. Valid values: Enabled, Disabled, PendingDelete, PendingImport, Archived.
KeyUsage	String	CMK purpose. Valid values: <code>ENCRYPT_DECRYPT</code> , <code>ASYMMETRIC_DECRYPT_RSA_2048</code> , <code>ASYMMETRIC_DECRYPT_SM2</code> , <code>ASYMMETRIC_SIGN_VERIFY_SM2</code> , <code>ASYMMETRIC_SIGN_VERIFY_RSA_2048</code> , and <code>ASYMMETRIC_SIGN_VERIFY_ECC</code> .
Type	Integer	CMK type. 2: FIPS-compliant; 4: SM-CRYPTO
CreatorUin	Integer	Creator
KeyRotationEnabled	Boolean	Whether key rotation is enabled
Owner	String	CMK creator. The value of this parameter is <code>user</code> if the CMK is created by the user, or the corresponding service name if it is created automatically by an authorized Tencent Cloud service.
NextRotateTime	Integer	Time of next rotation if key rotation is enabled
DeletionDate	Integer	Scheduled deletion time
Origin	String	CMK key material type. <code>TENCENT_KMS</code> : created by KMS; <code>EXTERNAL</code> : imported by user. Note: This field may return null, indicating that no valid values can be obtained.
ValidTo	Integer	It's valid when <code>Origin</code> is <code>EXTERNAL</code> , indicating the expiration date of key material. 0 means valid forever.

		Note: This field may return null, indicating that no valid values can be obtained.
ResourceId	String	Resource ID in the format of <code>creatorUin/\$creatorUin/\$keyId</code> .
HsmClusterId	String	ID of the HSM cluster. This field is only valid for Exclusive and Managed KMS instances. Note: This field may return <code>null</code> , indicating that no valid value can be obtained.

Tag

Tag key and tag value

Used by actions: CreateKey, CreateWhiteBoxKey.

Name	Type	Required	Description
TagKey	String	Yes	Tag key
TagValue	String	Yes	Tag value

TagFilter

Tag filter

Used by actions: DescribeWhiteBoxKeyDetails, ListKeyDetail.

Name	Type	Required	Description
TagKey	String	Yes	Tag key
TagValue	Array of String	No	Tag value

WhiteboxKeyInfo

White-box key information

Used by actions: DescribeWhiteBoxKey, DescribeWhiteBoxKeyDetails.

Name	Type	Description

KeyId	String	Globally unique white-box key ID
Alias	String	Unique alias that makes a key more recognizable and understandable. This parameter cannot be empty, can contain 1 to 60 letters, digits, hyphens (-), and underscores (_), and must begin with a letter or digit.
CreatorUin	Integer	Creator
Description	String	Key description information
CreateTime	Integer	Key creation time in Unix timestamp
Status	String	White-box key status. Valid values: Enabled, Disabled
OwnerUin	Integer	Creator
Algorithm	String	Key algorithm type
EncryptKey	String	Base64-encoded white-box encryption key
DecryptKey	String	Base64-encoded white-box decryption key
ResourceId	String	Resource ID in the format of <code>creatorUin/\$creatorUin/\$keyId</code>
DeviceFingerprintBind	Boolean	Whether there is a device fingerprint bound to the current key Note: this field may return null, indicating that no valid values can be obtained.

Error Codes

最近更新时间：2023-02-27 16:37:55

Feature Description

If there is an Error field in the response, it means that the API call failed. For example:

```
{
  "Response": {
    "Error": {
      "Code": "AuthFailure.SignatureFailure",
      "Message": "The provided credentials could not be validated. Please check your signature is correct."
    },
    "RequestId": "ed93f3cb-f35e-473f-b9f3-0d451b8b79c6"
  }
}
```

Code in Error indicates the error code, and Message indicates the specific information of the error.

Error Code List

Common Error Codes

Error Code	Description
ActionOffline	This API has been deprecated.
AuthFailure.InvalidAuthorization	<code>Authorization</code> in the request header is invalid.
AuthFailure.InvalidSecretId	Invalid key (not a TencentCloud API key type).
AuthFailure.MFAFailure	MFA failed.
AuthFailure.SecretIdNotFound	Key does not exist. Check if the key has been deleted or disabled in the console, and if not, check if the key is correctly entered. Note that whitespaces should not exist before or after the key.
AuthFailure.SignatureExpire	Signature expired. Timestamp and server time cannot differ by more than five minutes. Please

	ensure your current local time matches the standard time.
AuthFailure.SignatureFailure	Invalid signature. Signature calculation error. Please ensure you've followed the signature calculation process described in the Signature API documentation.
AuthFailure.TokenFailure	Token error.
AuthFailure.UnauthorizedOperation	The request is not authorized. For more information, see the CAM documentation.
DryRunOperation	DryRun Operation. It means that the request would have succeeded, but the DryRun parameter was used.
FailedOperation	Operation failed.
InternalServerError	Internal error.
InvalidAction	The API does not exist.
InvalidParameter	Incorrect parameter.
InvalidParameterValue	Invalid parameter value.
InvalidRequest	The multipart format of the request body is incorrect.
IpInBlacklist	Your IP is in uin IP blacklist.
IpNotInWhitelist	Your IP is not in uin IP whitelist.
LimitExceeded	Quota limit exceeded.
MissingParameter	A parameter is missing.
NoSuchProduct	The product does not exist.
NoSuchVersion	The API version does not exist.
RequestLimitExceeded	The number of requests exceeds the frequency limit.
RequestLimitExceeded.GlobalRegionUinLimitExceeded	Uin exceeds the frequency limit.
RequestLimitExceeded.IPLimitExceeded	The number of ip requests exceeds the frequency limit.
RequestLimitExceeded.UinLimitExceeded	The number of uin requests exceeds the frequency

	limit.
RequestSizeLimitExceeded	The request size exceeds the upper limit.
ResourceInUse	Resource is in use.
ResourceInsufficient	Insufficient resource.
ResourceNotFound	The resource does not exist.
ResourceUnavailable	Resource is unavailable.
ResponseSizeLimitExceeded	The response size exceeds the upper limit.
ServiceUnavailable	Service is unavailable now.
UnauthorizedOperation	Unauthorized operation.
UnknownParameter	Unknown parameter.
UnsupportedOperation	Unsupported operation.
UnsupportedProtocol	HTTP(S) request protocol error; only GET and POST requests are supported.
UnsupportedRegion	API does not support the requested region.

Service Error Codes

Error Code	Description
AuthFailure	CAM signature/authentication error
FailedOperation.CmkUsedByCloudProduct	The CMK is being used by a Tencent Cloud product.
FailedOperation.DecryptError	Decryption failed.
FailedOperation.EncryptionError	Encryption failed.
FailedOperation.TaggingError	Tagging error.
InvalidParameter.DecryptMaterialError	Decryption of <code>EncryptedKeyMaterial</code> failed.
InvalidParameter.InvalidPendingWindowInDays	The schedule deletion time parameter is invalid.
InvalidParameterValue.AliasAlreadyExists	The alias already exists.

InvalidParameterValue.DuplicatedKeyId	Duplicate <code>KeyId</code> .
InvalidParameterValue.InvalidAlias	Incorrect alias format
InvalidParameterValue.InvalidCiphertext	Incorrect ciphertext format
InvalidParameterValue.InvalidHsmClusterId	Invalid HSM cluster ID.
InvalidParameterValue.InvalidKeyId	Invalid <code>KeyId</code> .
InvalidParameterValue.InvalidKeyUsage	Incorrect <code>KeyUsage</code> parameter.
InvalidParameterValue.InvalidPlaintext	Invalid <code>Plaintext</code> .
InvalidParameterValue.InvalidType	Incorrect <code>Type</code> parameter.
InvalidParameterValue.MaterialNotMatch	The key material is different from the one previously imported.
InvalidParameterValue.TagKeysDuplicated	Duplicate tag key.
InvalidParameterValue.TagsNotExisted	The tag key or tag value does not exist.
LimitExceeded.CmkLimitExceeded	The number of CMKs has reached the upper limit.
LimitExceeded.FingerprintsLimitExceeded	The number of device fingerprints exceeded the limit.
LimitExceeded.KeyLimitExceeded	The number of created keys exceeded the limit.
ResourceUnavailable.CloudResourceBindingNotFound	The CMK is not bound with the Tencent Cloud resource
ResourceUnavailable.CmkArchived	The CMK has been archived.
ResourceUnavailable.CmkDisabled	The CMK has been disabled.
ResourceUnavailable.CmkNotFound	The CMK does not exist.
ResourceUnavailable.CmkNotPendingDelete	As the CMK is not scheduled for deletion, you cannot cancel the schedule deletion.
ResourceUnavailable.CmkShouldBeDisabled	An enabled CMK cannot be scheduled for deletion.
ResourceUnavailable.CmkStateNotSupport	This operation cannot be performed under

	the current CMK status.
ResourceUnavailable.KeyDisabled	The key has been disabled.
ResourceUnavailable.KeyPendingDelete	The key is not available as it's pending deleted.
ResourceUnavailable.NotPurchased	The white-box key service has not been activated.
ResourceUnavailable.TokenExpired	Token has expired.
UnsupportedOperation.ExternalCmkCanNotRotate	External CMKs cannot be rotated.
UnsupportedOperation.NotExternalCmk	Incorrect CMK type. Only <code>External</code> CMKs are supported.
UnsupportedOperation.NotUserCreatedCmk	You can only update the CMKs created by you.
UnsupportedOperation.ServiceTemporaryUnavailable	The service is temporarily unavailable.
UnsupportedOperation.UnsupportedKeyUsageInCurrentRegion	The encryption method is not supported in the current region.