

密钥管理服务

API文档

产品文档

【版权声明】

©2013-2018 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模式的承诺或保证。

文档目录

API文档

加解密相关接口

加密

解密

密钥管理相关接口

修改主密钥属性

创建主密钥

启用主密钥

生成数据密钥

禁用主密钥

获取主密钥列表

获取主密钥属性

API概览

简介

更新历史

调用方式

请求结构

公共请求参数

最终请求形式

请求结构简介

返回结果

错误返回结果

正确返回结果

错误码

签名方法

地域说明

API文档

加解密相关接口

加密

最近更新时间：2017-12-21 17:26:25

1. 接口描述

本接口 (Encrypt) 用于加密最多为4KB任意数据，诸如RSA密钥，数据库密钥，或者其他敏感的客户信息。

kms请求域名接口和说明可参考[地域和域名说明](#)。

任何时候，包括内测期间，如果使用外网域名产生公网下行流量，都会收取流量费用。所以强烈建议服务在腾讯云上的用户使用内网域名，内网不会产生流量费用。

- 输入参数有些是可选的，不填取默认值。
- 输出参数在成功情况下所有出参都会返回给用户；失败情况下，至少会有code, message, requestId返回。

2. 输入参数

以下请求参数列表仅列出了接口请求参数，其它参数见[公共请求参数](#)页面。

参数名称	是否必选	类型	描述
keyId	是	String	调用CreateKey生成的CMK全局唯一标识符。
plaintext	是	String	被加密的明文数据，该字符串必须使用base64编码。KMS SDK 加密接口已经封装了base64编码操作。用户若使用SDK则不需要调用base64操作。
encryptionContext	否	json 格式 字符串	key/value对的json字符串，如果指定了该参数，则在调用Decrypt API时需要提供同样的参数。

3. 输出参数

参数名称	类型	描述
code	Int	0：表示成功，others：错误，详细错误见下表。
message	String	错误提示信息。
requestId	String	服务器生成的请求 Id，出现服务器内部错误时，用户可提交此 Id 给后台定位问题。
keyId	String	CMK的全局唯一标识。
ciphertextBlob	String	加密后的密文。

错误代码	模块错误代码	英文提示	描述
4560	10660	encryption failed, please check input parameters	加密失败，请检查加密参数。
4540	10640	illegal encryptionContext	encryptionContext 非法，该字段必须为json格式字符串。
4590	10690	plaintext is not encoded with base64	plaintext 必须使用base64编码。

注意：上表所列错误码是接口特有错误码，如果您要查找的错误码不在其中，可能在[公共错误码](#)中。

4. 示例

输入：

```
https://kms-gz.api.tencentyun.com/v2/index.php?Action=Encrypt
&keyId=kms-30slkdf
&plaintext=databasepassword
&<公共请求参数>
```

输出：

```
{
  "code": 0,
  "message": "",
  "requestId": "14534664555",
  "msgId": "123345346",
```

```
"keyId": "kms-30slkdf",  
"ciphertextBlob": "string"  
  
}
```

解密

最近更新时间：2017-12-21 17:26:38

1. 接口描述

本接口 (Decrypt) 用于解密密文，得到明文数据。**此接口不需要keyId作为入参，因为加密接口得到的密文已经包含了keyId。解密接口会获取密文中携带的keyId，并验证权限。**

本接口会检查

kms请求域名接口和说明可参考[地域和域名说明](#)。

任何时候，包括内测期间，如果使用外网域名产生公网下行流量，都会收取流量费用。所以强烈建议服务在腾讯云上的用户使用**内网**域名，内网不会产生流量费用。

- 输入参数有些是可选的，不填取默认值。
- 输出参数在成功情况下所有出参都会返回给用户；失败情况下，至少会有code, message, requestId返回。

2. 输入参数

以下请求参数列表仅列出了接口请求参数，其它参数见[公共请求参数](#)页面。

参数名称	是否必选	类型	描述
ciphertextBlob	是	String	被加密的密文数据。
encryptionContext	否	json 格式字符串	key/value对的json字符串，应输入跟Encrypt接口相同的值。

3. 输出参数

参数名称	类型	描述
code	Int	0：表示成功，others：错误，详细错误见下表。
message	String	错误提示信息。
requestId	String	服务器生成的请求 Id，出现服务器内部错误时，用户可提交此 Id 给后台定位问题。
keyId	String	CMK的全局唯一标识。

参数名称	类型	描述
plaintext	String	解密后的明文。api返回的plaintext是base64编码的，为了得到原始明文，应调用相应的base64解码。KMS SDK解密接口已经封装了base64解密操作，若使用SDK不需要额外进行base64解密操作。

错误代码	模块错误代码	英文提示	描述
4560	10670	decryption failed, please check input parameters	解密失败，请检查输入参数。
4580	10680	invalid ciphertextBlob	ciphertextBlob非法。

注意：上表所列错误码是接口特有错误码，如果您要查找的错误码不在其中，可能在[公共错误码](#)中。

4. 示例

输入：

```
https://kms-gz.api.tencentyun.com/v2/index.php?Action=Decrypt
&ciphertextBlob=
&<公共请求参数>
```

输出：

```
{
  "code": 0,
  "message": "",
  "requestId": "14534664555",
  "keyId": "kms-30slkdf",
  "plaintext": "string"
}
```

密钥管理相关接口

修改主密钥属性

最近更新时间：2017-12-21 17:26:55

1. 接口描述

本接口 (SetKeyAttributes) 用于修改KeyId的属性信息。

kms请求域名接口和说明可参考[地域和域名说明](#)。

任何时候，包括内测期间，如果使用外网域名产生公网下行流量，都会收取流量费用。所以强烈建议服务在腾讯云上的用户使用内网域名，内网不会产生流量费用。

- 输入参数有些是可选的，不填取默认值。
- 输出参数在成功情况下所有出参都会返回给用户；失败情况下，至少会有code, message, requestId返回。

2. 输入参数

以下请求参数列表仅列出了接口请求参数，其它参数见[公共请求参数](#)页面。

参数名称	是否必选	类型	描述
keyId	是	String	调用CreateKey生成的CMK的全局唯一标识符。
alias	否	String	作为密钥更容易辨识，更容易被人看懂的别名。可为空。0-32个字符。

3. 输出参数

参数名称	类型	描述
code	Int	0：表示成功，其他返回值的含义可以参考 错误码 。
message	String	错误提示信息。
requestId	String	服务器生成的请求 Id。出现服务器内部错误时，用户可提交此 Id 给后台定位问题。

4. 示例

输入：

```
https://kms-sh.api.tencentyun.com/v2/index.php?Action=SetKeyAttributes
&keyId=kms-345sdfk
&alias=kms-test-1
&<公共请求参数>
```

输出：

```
{
  "code": 0,
  "message": "",
  "requestId": "14534664555",
}
```

创建主密钥

最近更新时间：2018-06-13 15:38:16

1. 接口描述

本接口 (CreateKey) 用于创建用户管理数据密钥的主密钥CMK (Custom Master Key)，通过CMK后续可以调用其他接口诸如创建数据密钥、加解密等操作。

每个用户，在每个地区，最多可以创建1000个用户主密钥。

如果用户有提高数量限制的需求，可以通过工单系统向我们提交申请。

kms请求域名接口和说明可参考[地域和域名说明](#)。

任何时候，包括内测期间，如果使用外网域名产生公网下行流量，都会收取流量费用。所以强烈建议服务在腾讯云上的用户使用内网域名，内网不会产生流量费用。

- 输入参数有些是可选的，不填取默认值。
- 输出参数在成功情况下所有出参都会返回给用户；失败情况下，至少会有code, message, requestId返回。

2. 输入参数

以下请求参数列表仅列出了接口请求参数，其它参数见[公共请求参数](#)页面。

参数名称	是否必选	类型	描述
description	否	String	key的描述。
alias	是	String	作为密钥更容易辨识，更容易被人看懂的别名。不可为空，1-32个字符。
keyUsage	否	String	指定key的用途。目前，默认为 'ENCRYPT/DECRYPT'，即key用于加密和解密。
type	否	Int	指定key类型，1为普通类型，2为量子类型，默认为普通类型

3. 输出参数

参数名称	类型	描述
------	----	----

参数名称	类型	描述
code	Int	0：表示成功，others：错误，详细错误见下表。
message	String	错误提示信息。
requestId	String	服务器生成的请求Id。出现服务器内部错误时，用户可提交此 Id 给后台定位问题。
keyMetadata	Struct	密钥信息。

keyMetadata定义如下:

参数名称	类型	描述
keyId	String	key的全局唯一标识符。
alias	String	作为密钥更容易辨识，更容易被人看懂的别名。
createTime	UInt32	密钥创建时间，unix时间戳。
description	String	key的描述。
keyState	String	key的状态。
keyUsage	String	key的用途。

错误代码	模块错误代码	英文提示	描述
4490	10470	string of KeyUsage must be ENCRYPT/DECRYPT	KeyUsage参数错误，目前只能是ENCRYPT或者是DECRYPT。
4500	10480	alias is already existed in your account, please input another unique one	别名已经存在，请换一个别名。
4510	10610	number of CMK in your account has reached the limit	CMK数量达到最大值。一个账户的CMK数量是有限(200)的，达到最大值后，就不能创建新的CMK了。
4520	10620	keySpec value error	keySpec错误。

注意：上表所列错误码是接口特有错误码，如果您要查找的错误码不在其中，可能在[公共错误码](#)中。

4. 示例

输入：

```
https://kms-sh.api.tencentyun.com/v2/index.php?Action=CreateKey
&alias=kms-test-1
&description=this key is for kms test, and don't delete it
&keyUsage=ENCRYPT/DECRYPT
&type=1
&<公共请求参数>
```

输出：

```
{
  "code": 0,
  "message": "",
  "requestId": "14534664555",
  "keyMetadata": {
    "keyId": "kms-94kalsdf",
    "alias": "kms-test-1",
    "createTime": 1483945424,
    "description": "this key is for kms test, and don't delete it",
    "keyState": "Enabled",
    "keyUsage": "ENCRYPT/DECRYPT"
  }
}
```

启用主密钥

最近更新时间：2017-12-21 17:27:44

1. 接口描述

本接口 (EnableKey) 用于启用一个主密钥,允许该Key被使用。

kms请求域名接口和说明可参考[地域和域名说明](#)。

任何时候，包括内测期间，如果使用外网域名产生公网下行流量，都会收取流量费用。所以强烈建议服务在腾讯云上的用户使用**内网**域名，内网不会产生流量费用。

- 输入参数有些是可选的，不填取默认值。
- 输出参数在成功情况下所有出参都会返回给用户；失败情况下，至少会有code, message, requestId返回。

2. 输入参数

以下请求参数列表仅列出了接口请求参数，其它参数见[公共请求参数](#)页面。

参数名称	是否必选	类型	描述
keyId	是	String	调用CreateKey生成的CMK全局唯一标识符。

3. 输出参数

参数名称	类型	描述
code	Int	0：表示成功，其他返回值的含义可以参考 错误码 。
message	String	错误提示信息。
requestId	String	服务器生成的请求 Id。出现服务器内部错误时，用户可提交此 Id 给后台定位问题。

4. 示例

输入：

```
https://kms-gz.api.tencentyun.com/v2/index.php?Action=EnableKey
&keyId=kms-13f32s3fr
&<公共请求参数>
```

输出：

```
{
  "code": 0,
  "message": "",
  "requestId": "14534664555",
}
```

生成数据密钥

最近更新时间：2018-06-13 15:39:48

1. 接口描述

本接口 (GenerateDataKey) 生成一个密钥，您可以用这个密钥进行本地数据的加密。

kms请求域名接口和说明可参考[地域和域名说明](#)。

任何时候，包括内测期间，如果使用外网域名产生公网下行流量，都会收取流量费用。所以强烈建议服务在腾讯云上的用户使用**内网**域名，内网不会产生流量费用。

- 输入参数有些是可选的，不填取默认值。
- 输出参数在成功情况下所有出参都会返回给用户；失败情况下，至少会有code, message, requestId返回。

2. 输入参数

以下请求参数列表仅列出了接口请求参数，其它参数见[公共请求参数](#)页面。

参数名称	是否必选	类型	描述
keyId	是	String	调用CreateKey生成的CMK全局唯一标识符。
keySpec	否	String	指定生成Datakey的加密算法以及Datakey大小，AES_128或者AES_256。
numberOfBytes	否	Int	生成的DataKey的长度，同时指定NumberOfBytes和KeySpec时，以NumberOfBytes为准。
encryptionContext	否	json字符串	key/value对的json字符串，如果指定了该参数，则在调用Decrypt API时需要提供同样的参数。

3. 输出参数

参数名称	类型	描述
code	Int	0：表示成功，others：错误，详细错误见下表。

参数名称	类型	描述
message	String	错误提示信息。
requestId	String	服务器生成的请求Id。出现服务器内部错误时，用户可提交此 Id 给后台定位问题。
keyId	String	CMK的全局唯一标识。
plaintext	String	生成的DataKey的明文，该密文使用base64编码，用户需要使用base64解码得到明文。 KMS SDK 生成数据密钥接口已经封装了base64解码操作，用户若使用SDK则不需要调用base64解码操作。
ciphertextBlob	String	DataKey加密后的密文。

4. 示例

输入：

```
https://kms-bj.api.tencentyun.com/v2/index.php?Action=GenerateDataKey
&keyId=kms-345sdfk
&keySpec=AES_256
&<公共请求参数>
```

输出：

```
{
  "code": 0,
  "message": "",
  "requestId": "14534664555",
  "keyId": "kms-345sdfk",
  "plaintext": "string",
  "ciphertextBlob": "string"
}
```

禁用主密钥

最近更新时间：2017-12-21 17:46:01

1. 接口描述

本接口 (DisableKey) 用于禁用一个主密钥,处于禁用状态的Key无法用于加密、解密操作。直到Key恢复到启用状态之前,原来使用该Key加密的密文也无法解密。。

kms请求域名接口和说明可参考[地域和域名说明](#)。

任何时候,包括内测期间,如果使用外网域名产生公网下行流量,都会收取流量费用。所以强烈建议服务在腾讯云上的用户使用内网域名,内网不会产生流量费用。

- 输入参数有些是可选的,不填取默认值。
- 输出参数在成功情况下所有出参都会返回给用户;失败情况下,至少会有code, message, requestId返回。

2. 输入参数

以下请求参数列表仅列出了接口请求参数,其它参数见[公共请求参数](#)页面。

参数名称	是否必选	类型	描述
keyId	是	String	调用CreateKey生成的CMK全局唯一标识符。

3. 输出参数

参数名称	类型	描述
code	Int	
message	String	错误提示信息。
requestId	String	服务器生成的请求 Id。出现服务器内部错误时,用户可提交此 Id 给后台定位问题。

4. 示例

输入：

```
https://kms-gz.api.tencentyun.com/v2/index.php?Action=DisableKey
&keyId=kms-345sdfk
&<公共请求参数>
```

输出：

```
{
  "code": 0,
  "message": "",
  "requestId": "14534664555"
}
```

获取主密钥列表

最近更新时间：2017-12-21 17:45:48

1. 接口描述

本接口 (ListKey)，用于列出账号下面的密钥列表。

kms请求域名接口和说明可参考[地域和域名说明](#)。

任何时候，包括内测期间，如果使用外网域名产生公网下行流量，都会收取流量费用。所以强烈建议服务在腾讯云上的用户使用内网域名，内网不会产生流量费用。

- 输入参数有些是可选的，不填取默认值。
- 输出参数在成功情况下所有出参都会返回给用户；失败情况下，至少会有code, message, requestId返回。

2. 输入参数

以下请求参数列表仅列出了接口请求参数，其它参数见[公共请求参数](#)页面。

参数名称	是否必选	类型	描述
offset	否	Int	含义跟SQL查询的Offset一致，表示本次获取从按一定顺序排列数组的第Offset个元素开始。缺省为0。
limit	否	Int	含义跟SQL查询的Limit一致，表示本次获最多获取Limit个元素。缺省值为10。

3. 输出参数

参数名称	类型	描述
code	Int	0：表示成功，其他返回值的含义可以参考 错误码 。
message	String	错误提示信息。
requestId	String	服务器生成的请求 Id。出现服务器内部错误时，用户可提交此 Id 给后台定位问题。
keys	Array	key数组。

参数名称	类型	描述
totalCount	Int	key的总数。

Keys的每个元素定义如下：

参数名称	类型	描述
keyId	String	CMK的全局唯一标识。

4. 示例

输入：

```
https://kms-bj.api.tencentyun.com/v2/index.php?Action=ListKey
&offset=20
&limit=10
&<公共请求参数>
```

输出：

```
{
  "code": 0,
  "message": "",
  "requestId": "14534664555",
  "keys": [
    {"keyId": "kms-984ksdl"},
    {"keyId": "kms-84sjkla"}
  ],
  "totalCount": 100,
}
```

获取主密钥属性

最近更新时间：2017-12-21 17:45:23

1. 接口描述

本接口 (GetKeyAttributes) 用于返回指定KeyId的属性信息。

kms请求域名接口和说明可参考[地域和域名说明](#)。

任何时候，包括内测期间，如果使用外网域名产生公网下行流量，都会收取流量费用。所以强烈建议服务在腾讯云上的用户使用内网域名，内网不会产生流量费用。

- 输入参数有些是可选的，不填取默认值。
- 输出参数在成功情况下所有出参都会返回给用户；失败情况下，至少会有code, message, requestId返回。

2. 输入参数

以下请求参数列表仅列出了接口请求参数，其它参数见[公共请求参数](#)页面。

参数名称	是否必选	类型	描述
keyId	是	String	调用CreateKey生成的CMK全局唯一标识符。

3. 输出参数

参数名称	类型	描述
code	Int	请参考 错误码
message	String	错误提示信息。
requestId	String	服务器生成的请求Id。出现服务器内部错误时，用户可提交此 Id 给后台定位问题。
keyMetadata	Struct	密钥信息。

keyMetadata定义如下：

参数名称	类型	描述	取值	备注
keyId	String	key的全局唯一标识符		
alias	否	String	作为密钥更容易辨识，更容易被人看懂的别名。	可为空。0-32个字符。
createTime	UInt32	密钥创建时间	时间戳	
description	String	key的描述	key的描述	
keyState	String	key的状态	Enabled 或者Disabled	
keyUsage	String	key的用途	ENCRYPT/DECRYPT	
type	Int	指定key类型，1为普通类型，2为量子类型。		

4. 示例

输入：

```
https://kms-gz.api.tencentyun.com/v2/index.php?Action=GetKeyAttributes
&keyId=kms-345sdfk
&<公共请求参数>
```

输出：

```
{
  "code": 0,
  "message": "",
  "requestId": "14534664555",
  "keyMetadata": {
    "keyId": "kms-345sdfk",
    "createTime": 1483945424,
    "description": "test",
    "keyState": "Enabled",
    "keyUsage": "ENCRYPT/DECRYPT",
    "type": 1
  }
}
```

API概览

最近更新时间：2018-06-13 15:41:50

密钥管理服务

加解密相关接口

接口功能	Action ID	功能描述
加密	Encrypt	用于加密最多为4KB任意数据，诸如RSA密钥，数据库密钥，或者其他敏感的客户信息。
解密	Decrypt	用于解密密文数据，得到明文数据。

密钥管理相关接口

接口功能	Action ID	功能描述
创建主密钥	CreateKey	创建用户管理数据密钥的主密钥CMK (Custom Master Key)。
获取主密钥列表	ListKey	用于获取用户所有的keyId。
获取主密钥属性	GetKeyAttributes	用于获取指定keyId的属性信息。
禁用主密钥	DisableKey	用于禁用一个指定的keyId。
启用主密钥	EnableKey	用于启用一个指定的keyId。
生成数据密钥	GenerateDataKey	用于生成一个密钥，用户可以使用该密钥用于本地数据的加密。
修改主密钥属性	SetKeyAttributes	用于修改指定keyId的属性信息。

简介

最近更新时间：2018-06-13 15:43:08

欢迎使用密钥管理服务KMS。

KMS产品介绍请参考[产品介绍](#)

支持的全部操作可参见[API概览页](#)。

注意：协助者帐号目前不能用于kms的操作。

密码学术语表

本文档涉及的一些常用术语如下：

术语	中文直译	含义	备注
DataKey	数据密钥	实际用于加密业务数据的密钥	
CMK	customer master key：用户主密钥	用户创建的，用于加密小包数据（最多4KB）或者DataKey的密钥	
KeyId	密钥id	CMK返回给用户的全局唯一标识，注意这不是CMK本身，只是一个索引而已	
CiphertextBlob	密文结构体	用户调加密或者GenerateDataKey接口返回的结构体，其中包含了明文的KeyId和密文的数据密钥或者加密后数据	
根密钥		用于加密CMKs的密钥	

KMS术语

术语	中文直译	含义
KMS	Key Management Service:密钥管理服务	PAAS层密钥服务, 提供密钥安全管理和小包数据加解密服务
HSA	Harden Security Appliance:加固的安全模块	一个软件或硬件实现的安全模块，是KMS实现密钥管理，加密解密的核心部件

术语	中文直译	含义
qps throttling	QPS Throttling	qps 限制

输入参数与返回参数释义

- limit 和 offset

用来控制分页的参数；当相应结果是列表形式时，如果数量超过了 limit 所限定的值，那么只返回limit个值。用户可以通过 limit 和 offset 两个参数来控制分页：limit 为单次返回的最多条目数量，offset 为偏移量。

举例来说，参数 offset=0&limit=20 返回第0到20项，offset=20&limit=20 返回第20到40项，offset=40&limit=20 返回第40到60项；以此类推。

- id.n

同时输入多个参数的格式。当遇到形如这样的格式时，那么该输入参数可以同时传多个。例如：

id.0="10.12.243.21"&id.1="10.12.243.21"&id.2="10.12.243.21"&id.3="10.12.243.21"...

以此类推（以下标0开始）。

API快速入门

用户可以通过[KMS SDK](#)（推荐，目前提供多个语言版本），或直接调用云API（较为麻烦，建议SDK语言之外的用户使用）使用KMS的服务：

选择地域和内外网。与其他云产品不同，KMS API 的请求域名随地域不同而变化，需选择地域对应的域名，请求域名的构成规则形如 kms-region.api.cloud.tencent.com/v2/index.php，其中 region 字段需用具体地域替换：gz（广州），sh（上海），bj（北京）。如果是用户使用的机器是腾讯云服务器，则应优先选择内网域名，否则选外网域名。

接口功能	接口名	功能描述
加密	Encrypt	用于加密最多为4KB任意数据，诸如RSA密钥，数据库密钥，或者其他敏感的客户信息。
解密	Decrypt	用于解密密文数据，得到明文数据。
创建主密钥	CreateKey	创建用户管理数据密钥的主密钥CMK（Custom Master Key）。

接口功能	接口名	功能描述
获取主密钥列表	ListKey	用于获取用户所有的keyId。
获取主密钥属性	GetKeyAttributes	用于获取指定keyId的属性信息。
禁用主密钥	DisableKey	用于禁用一个指定的keyId。
启用主密钥	EnableKey	用于启用一个指定的keyId。
生成数据密钥	GenerateDataKey	用于生成一个密钥，用户可以使用该密钥用于本地数据的加密。
修改主密钥属性	SetKeyAttributes	用于修改指定keyId的属性信息。

更新历史

最近更新时间：2017-11-30 20:45:53

时间	更新内容
2017-2-24	创建密钥SDK，API文档。

调用方式

请求结构

公共请求参数

最近更新时间：2017-11-30 20:46:50

公共请求参数是每个接口都需要使用到的请求参数，如非必要，在各个接口单独的文档中不再对这些参数进行说明，但**每次请求均需要携带这些参数，才能正常发起请求**。公共请求参数的首字母均为大写，以此区分于接口请求参数。

公共请求参数具体列表如下：

名称	类型	描述	是否必选
Action	String	具体操作的指令接口名称，例如想要调用 查询实例列表 接口，则 Action 参数即为 DescribeInstances。	是
Region	String	区域参数，用来标识希望操作哪个区域的实例。各区域的参数值为：北京:bj，广州:gz，上海:sh，香港:hk，北美:ca。、 注意：正常情况下此参数是必须的，如无需传入，则会在相应接口中进行说明。	否
Timestamp	UInt	当前UNIX时间戳，可记录发起API请求的时间。	是
Nonce	UInt	随机正整数，与 Timestamp 联合起来，用于防止重放攻击。	是
SecretId	String	在 云API密钥 上申请的标识身份的 SecretId，一个 SecretId 对应唯一的 SecretKey，而 SecretKey 会用来生成请求签名 Signature。具体可参考 签名方法 页面。	是
Signature	String	请求签名，用来验证此次请求的合法性，由系统根据输入参数自动生成。具体可参考 签名方法 页面。	是

假设用户想要查询广州地域的云服务器实例列表，则其请求链接的形式可能如下：

<https://cvm.api.qcloud.com/v2/index.php?>

Action=DescribeInstances
&SecretId=xxxxxxx
&Region=gz
&Timestamp=1465055529
&Nonce=59485
&Signature=mysignature
&<接口请求参数>

一个完整的请求需要两类请求参数：公共请求参数和接口请求参数。这里只列出了上述6个公共请求参数，并未列出接口请求参数，有关接口请求参数的说明可见[接口请求参数](#)小节。

最终请求形式

最近更新时间：2017-11-30 20:47:40

最终的请求URL由以下几部分组成：

- 1) 请求域名: [查询实例列表](#) (DescribeInstances) 的请求域名为：cvm.api.qcloud.com。实际的请求域名根据接口所属模块的不同而不同, 详见各接口说明。
- 2) 请求路径: 云API的请求路径固定为/v2/index.php。
- 3) 最终请求参数串: 包括公共请求参数和接口请求参数。

最终的请求 URL 的拼接规则为:

```
https:// + 请求域名 + 请求路径 + ? + 最终请求参数串
```

因此，我们得到最终的请求 URL 如下，其中前6个参数为公共请求参数，后6个参数为接口请求参数。

```
https://cvm.api.qcloud.com/v2/index.php?  
Action=DescribeInstances  
&SecretId=xxxxxxx  
&Region=gz  
&Timestamp=1465055529  
&Nonce=59485  
&Signature=mysignature  
&instanceIds.0=ins-0hm4gvho  
&instanceIds.1=ins-8oby8q00  
&offset=0  
&limit=20  
&status=2  
&zoned=100003
```

请求结构简介

最近更新时间：2017-11-30 20:48:33

对腾讯云的 API 接口调用是通过向腾讯云 API 的服务端地址发送请求，并按照接口说明在请求中加入相应请求参数来完成的。腾讯云 API 的请求结构由以下几部分组成：

1. 服务地址

腾讯云 API 的服务接入地址与具体模块相关，详见各接口描述。

2. 通信协议

腾讯云 API 的大部分接口都通过HTTPS进行通信，提供高安全性的通信通道。

KMS API 只支持 https协议，目前支持TLSv1 TLSv1.1 TLSv1.2

3. 请求方法

腾讯云API同时支持 POST 和 GET 请求。

注意：

- 1、不能混合使用这两种请求方式，即如果使用 GET 方式，则参数均从 Querystring 取得；如果使用 POST 方式，则参数均从 Request Body 中取得，而Querystring 中的参数将忽略。两种方式参数格式规则相同，一般情况下推荐使用POST，因为GET可能会因为长度过长碰到不可预料的问题。
- 2、无论用户的请求方法是GET或者POST，都需要对参数编码。

4. 请求参数

腾讯云API的每个请求都需要指定两类参数：即公共请求参数以及接口请求参数。其中公共请求参数是每个接口都要用到的请求参数，具体可参见 [公共请求参数](#) 小节，而接口请求参数是各个接口所特有的，具体见各个接口的“请求参数”描述。

5. 字符编码

腾讯云API的请求及返回结果均使用UTF-8字符集进行编码。

返回结果

错误返回结果

最近更新时间：2018-06-04 21:05:57

若API调用失败，则最终返回结果中的错误码code不为0，message字段会显示详细错误信息。您可以根据code和message在 [错误码](#) 页面查询具体的错误信息。

错误返回示例如下：

```
{
  "code": 5100,
  "message": "(100004)projectId不正确",
}
```

正确返回结果

最近更新时间：2017-11-30 20:50:59

若API调用成功，则最终返回结果中的错误码code为0，错误信息message为空，并且会显示返回的结果数据。

示例如下：

```
{  
  "code": 0,  
  "message": "",  
  <返回结果数据>  
}
```

错误码

最近更新时间：2017-11-30 20:51:59

错误码

message字段表示与模块相关的错误。

其示例如下：

"message": "(100004)projectId不正确"

它由两部分组成，()内的为模块错误代码，()后的为具体的错误描述。

不同模块可能产生的错误情况是不一样的，用户可以根据具体的错误描述确定错误所在。**下面的表都是公共错误码，如果您要查找的错误码不在其中，请到接口文档中具体接口说明处查找。**

公共错误码

错误代码	模块错误代码	英文提示	描述
4000	10000	invalid request parameters	无效（非法）请求参数。通常是参数没有按照KMS云API的接口说明导致的错误。
4000	10010	lacked of required parameters	缺少必填参数。应参照KMS云API接口的说明看缺少哪些必填参数。
4100	10030	authentication failed	鉴权失败。可能的原因有 1) 生成签名算法的secret key错误；2) 签名算法有误（没用官方sdk，自己实现签名算法）。
4300	10040	charge overdue	账户欠费。
6000	10050	server internal error	服务器内部错误。一般会有requestId返回给用户，用户可根据requestId提工单给技术支持人员定位问题。
4100	10080	secret id status error	secret id状态错误。secret id可能处于禁用状态。
4000	10110	request parameters error	请求参数错误。通常是参数没有按照KMS云API的接口说明导致的错误。
4420	10250	qps throttling	qps达到最大值，因此被限制。为了保证后台的稳定性和调用时延，目前实际的限制是每秒的消息数最大5k。对于有特殊要求的客户，可以提工单申请。

4100	10270	secret id is not existed	secret id 不存在。
4000	10280	action is not existed	参数Action不存在。
4000	10310	error: parameter key format error"	参数格式错误。
4000	10320	no such parameter	不存在这样的参数。
4000	10330	parameter is NOT a repeatable parameter	参数不是一个可以重复的参数。
4000	10350	parameter value or length is out of range	参数取值或参数长度超过了范围限制。通常对于整型而言，是取值错误。对String类型参数而言，是长度错误。
4000	10360	parameter error type	参数类型错误。例如把整型填成了字符串类型。
4000	10370	batch size of parameter is too large	批量接口的批量值超过了最大值。
4000	10380	index of parameter is not consequent	可重复参数的下标不连续。
4000	10390	lacked of required parameter	缺少必填的参数。
4000	10400	cannot find parameter in uri	uri中找不到参数。
4000	10410	unexpected http method, only GET or POST is supported	不支持的http方法。目前只支持GET和POST方法。由于GET有长度的限制，建议使用POST。
4000	10420	cannot parse	无法解析参数。
4000	10430	action name is not existed	Action所指定的接口名不存在。
4000	10440	account illegal, it	帐号不合法。请检查是不是协助者帐号，目前KMS不

		may be an assistant account	支持协助者帐号的操作。
4000	10450	secret id dosen't begin with AKID account	secret id不是以AKID开头。
4480	10460	exceed interface frequency limit, please slow down	为保护后端系统，控制类接口（例如 ListKey等）的允许调用频率比 QPS 要低很多，所以看到该错误时，请减少控制类接口调用频率。
4530	10630	key is not existed	key不存在，表明用户没有该CMK,请检查该key是否存在。
4550	10650	key is disabled	该key被禁用了，请检查该key的状态是否为启用。

签名方法

最近更新时间：2017-11-30 20:52:56

腾讯云 API 会对每个访问的请求进行身份验证，即每个请求都需要在公共请求参数中包含签名信息（Signature）以验证用户身份。签名信息由用户所执有的安全凭证生成，安全凭证包括 SecretId 和 SecretKey，若用户还没有安全凭证，则需要在腾讯云官网上自主申请，否则就无法调用云API接口。

1. 申请安全凭证

在第一次使用云API之前，用户需要在腾讯云控制台上申请安全凭证。安全凭证包括 SecretId 和 SecretKey，其中 SecretId 是用于标识 API 调用者身份的，而SecretKey是用于加密签名字符串和服务器端验证签名字符串的密钥。用户应严格保管其SecretKey，避免泄露。

申请安全凭证的具体步骤如下：

- 1) 登录[腾讯云管理中心控制台](#)。
- 2) 点击【云产品】，选择【监控与管理】栏下的【云API密钥】，进入云API密钥管理页面。
- 3) 在[云API访问密钥管理](#)页面，点击【新建】即可以创建一对SecretId/SecretKey，每个帐号最多可以拥有两对 SecretId/SecretKey。

2. 生成签名串

有了安全凭证SecretId 和 SecretKey后，就可以生成签名串了。下面给出了一个生成签名串的详细过程。

假设用户的 SecretId 和 SecretKey 分别是：

```
SecretId: AKIDz8krbsJ5yKBZQpn74WFkmLPx3gnPhESA  
SecretKey: Gu5t9xGARNpq86cd98joQYCN3Cozk1qA
```

注意：这里只是示例，请用户根据自己实际的SecretId和SecretKey进行后续操作！

以[查看实例列表](#)(DescribeInstances)请求为例，当用户调用这一接口时，其请求参数可能如下：

参数名称	中文	参数值
Action	方法名	DescribeInstances

参数名称	中文	参数值
SecretId	密钥Id	AKIDz8krbsJ5yKBZQpn74WFkmLPx3gnPhESA
Timestamp	当前时间戳	1465185768
Nonce	随机正整数	11886
Region	实例所在区域	gz
instanceIds.0	待查询的实例ID	ins-09dx96dg
offset	偏移量	0
limit	最大允许输出	20

由上表可以看出，请求参数中的公共请求参数只有5个：Action、SecretId、Timestamp、Nonce和Region，而不是在“公共请求参数”中所述的6个，事实上，第6个参数Signature（签名串）正是由其他参数（包括指令请求参数）共同生成的，具体步骤如下：

2.1. 对参数排序

首先对所有请求参数按参数名做字典序升序排列，所谓字典序升序排列，直观上就如同在字典中排列单词一样排序，按照字母表或数字表里递增顺序的排列次序，即先考虑第一个“字母”，在相同的情况下考虑第二个“字母”，依此类推。您可以借助编程语言中的相关排序函数来实现这一功能，如php中的ksort函数。上述示例参数的排序结果如下：

```
{
  'Action': 'DescribeInstances',
  'Nonce': 11886,
  'Region': 'gz',
  'SecretId': 'AKIDz8krbsJ5yKBZQpn74WFkmLPx3gnPhESA',
  'Timestamp': 1465185768,
  'instanceIds.0': 'ins-09dx96dg',
  'limit': 20,
  'offset': 0,
}
```

使用其它程序设计语言开发时，可对上面示例中的参数进行排序，得到的结果一致即可。

2.2. 拼接请求字符串

此步骤生成请求字符串。

将把上一步排序好的请求参数格式化“参数名称”=“参数值”的形式，如对Action参数，其参数名称为“Action”，参

数值为"DescribeInstances"，因此格式化后就为Action=DescribeInstances。

注意：1、“参数值”为原始值而非url编码后的值。2、若输入参数中包含下划线，则需要将其转换为“.”。

然后将格式化后的各个参数用"&"拼接在一起，最终生成的请求字符串为：

```
Action=DescribeInstances&Nonce=11886&Region=gz&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3gI
```

2.3. 拼接签名原文字符串

此步骤生成签名原文字符串。

签名原文字符串由以下几个参数构成：

- 1) 请求方法: 支持 POST 和 GET 方式, 这里使用 GET 请求, 注意方法为全大写。
- 2) 请求主机: [查看实例列表](#)(DescribeInstances)的请求域名为：cvm.api.qcloud.com。实际的请求域名根据接口所属模块的不同而不同, 详见各接口说明。
- 3) 请求路径: 云API的请求路径固定为/v2/index.php。
- 4) 请求字符串: 即上一步生成的请求字符串。

签名原文串的拼接规则为：

请求方法 + 请求主机 + 请求路径 + ? + 请求字符串

示例的拼接结果为：

```
GETcvm.api.qcloud.com/v2/index.php?Action=DescribeInstances&Nonce=11886&Region=gz&SecretId=
```

2.4. 生成签名串

此步骤生成签名串。

首先使用 HMAC-SHA1 算法对上一步中获得的**签名原文字符串**进行签，然后将生成的签名串使用 Base64 进行编码，即可获得最终的签名串。

具体代码如下，以 PHP 语言为例：

```
$secretKey = 'Gu5t9xGARNpq86cd98joQYCN3Cozk1qA';  
$srcStr = 'GETcvm.api.qcloud.com/v2/index.php?Action=DescribeInstances&Nonce=11886&Region=gz&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3gI';  
$signStr = base64_encode(hash_hmac('sha1', $srcStr, $secretKey, true));  
echo $signStr;
```

最终得到的签名串为：

```
NSI3UqqD99b/UJb4tbG/xZpRW64=
```

使用其它程序设计语言开发时, 可用上面示例中的原文进行签名验证, 得到的签名串与例子中的一致即可。

3. 签名串编码

生成的签名串并不能直接作为请求参数，需要对其进行 URL 编码。

注意：如果用户的请求方法是GET，则对所有请求参数值均需要做URL编码。

如上一步生成的签名串为NSI3UqqD99b/UJb4tbG/xZpRW64=，则其编码后为

NSI3UqqD99b/UJb4tbG/xZpRW64=。因此，最终得到的签名串请求参数(Signature)为：

NSI3UqqD99b/UJb4tbG/xZpRW64=，它将用于生成最终的请求URL。

地域说明

最近更新时间：2017-11-30 20:53:55

请求域名说明

外网接口请求域名：**kms-region.api.qcloud.com**

内网接口请求域名：**kms-region.api.tencentyun.com**

任何时候，包括内测期间，如果使用外网域名产生公网下行流量，都会收取流量费用。所以强烈建议服务在腾讯云上的用户使用**内网**域名，内网不会产生流量费用。

只支持https协议。

地域说明

接口请求域名中 region 需用具体地域替换，如下表所示：

区域	替换值	外网请求域名	内网请求域名
北京	bj	kms-bj.api.qcloud.com	kms-bj.api.tencentyun.com
上海	sh	kms-sh.api.qcloud.com	kms-sh.api.tencentyun.com
广州	gz	kms-gz.api.qcloud.com	kms-gz.api.tencentyun.com