

密钥管理服务

入门指南

产品文档



腾讯云

【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

入门指南

快速开始

创建密钥

管理密钥

加密解密

入门指南

快速开始

最近更新时间：2017-12-21 17:46:34

简介

以一个简单的证书加解密例子来介绍KMS 最常见的使用场景，对主机硬盘上的证书、密钥、配置文件等信息直接进行加密保护。

1. 创建密钥

打开 [控制台](#)，为了和后续Demo的代码对应，区域最好选择广州，

点击上方【新建】按钮，然后输入密钥名称，用途可以留空，点击【确定】。

界面在点击【确定】后会返回【密钥列表】，此时新创建的密钥已经展示在列表最上方，可以通过密钥名称来确认它。

2. 使用控制台工具加密一个SSL证书

在【密钥列表】上点击你刚才创建的密钥的【密钥ID/密钥名称】列，进入该密钥【详情页】，滚动到【在线工具】部分，选择【加密】

腾讯云已经为你提供了测试用证书文件，[Demo证书（明文）>>](#)

以文本的方式打开证书，然后将内容复制到左侧明文输入栏，并点击【执行】按钮

```
1 -----BEGIN CERTIFICATE-----
2 MIICGjCCAeugAwIBAgIJAJqEg8+4pyq/MA0GCSqGSIb3DQEBCwUAMHoxCzAJBgNV
3 BAYTAlVTMQswCQYDVQQLDAJ0OTELMAkGA1UEBwwCU0YxZDZANBghNDAwMkpvewUu
4 dDEQMA4GA1UECwwHT9kZS5qc2EwMA0GA1UEAw0Y2EzMSAwMkpvewUuMkpvewUu
5 FhFyeUB8aW55Y2xvdWRzLn9yZzAeFw0dH0OTABMTGpxZiNDFAFa08MjA5MDx0ZzI4
6 NDFAHoxCzAJBgNVBAYTAlVTMQswCQYDVQQLDAJ0OTELMAkGA1UEBwwCU0YxZDZAN
7 BAYTAlVTMQswCQYDVQQLDAJ0OTELMAkGA1UEBwwCU0YxZDZANBghNDAwMkpvewUu
8 HgYKozThvcMA0KBHFyeUJ8aW55Y2xvdWRzLn9yZzCBnzANBgkqhkiG9w0BAQEF
9 AAOBjQAwgYkCgYEAs4MKn9saUII/9Efh0PouC3kL9Mo5sd1WR6R8BesD8cqeFzXW
10 EwEq/P8hUeAH1sY08RF0cc3m5Jg8KTYRgc+VZwImopz17nTu0Y4HPM4bFzqm0m
11 75TfJz5eHzynBTU8jK5om18hjbNRA38j0m4D7rN/vqtB+RG+vEhx0Nng4DMCAwEA
12 AaMQMA4wDAYDR8TBAUwAwEB/zANBgkqhkiG9w0BAQsFAA0BgQBo8rX1uZMhVKhG
13 gwW+LXrY24Pk9NdRmfqEvyuaR4GoG0XCqLVaFa6x+4/eq0UzHoC9uGfPtjrvW
14 BYQ1o/10J2M4KZYuXoVuMUSj+seL82mf9zLDeq5WYTPecqJDMfgVpx0mhHfyezn
15 SKUTX7XJ0ohjET+X5BqTFqRT/rFIw==
16 -----END CERTIFICATE-----
```

在线工具

加密 解密

-----BEGIN CERTIFICATE-----
MIICGjCCAeugAwIBAgIJAJqEg8+4pyq/MA0GCSqGSIb3DQEBCwUAMHoxCzAJBgNV
xCzAJBgNV
BAYTAlVTMQswCQYDVQQLDAJ0OTELMAkGA1UEBwwCU0YxZDZANBghNDAwMkpvewUu
VBAoMBkpvewUu
dDEQMA4GA1UECwwHT9kZS5qc2EwMA0GA1UEAw0Y2EzMSAwMkpvewUuMkpvewUu

执行

下载

生成的密文会出现在右侧密文结果栏，请保存好它以便下一步解密环节使用，最简单的方法就是点击【下载】按钮

在线工具

加密 解密

```
-----BEGIN CERTIFICATE-----
MIIICgICC AeuG AwI BAgl JAJgEq8+4pyg/MA0GCSqGSIb3DQEBCwUAMHo
xCzAJBgNV
BAYTAiVTMQswCQYDVQQIDAJDQTElMAkGA1UEBwwCU0YxZzANBgN
VBAoMBkpvWVU
dDEQMA4GA1UECwwHTm9kZS5qc2EMMAoGA1UEAwwDY2ExMSAwHg
```

执行

```
a21zL TE2aWRwcWg1AAAAAAAAA=7CMaRdcZS8RBrtsS/IvRgCkOJsm
CVaucsfyBxTlJ2SYN5quwkvjeXQ9DLuECdsCplEUDuzftj4G3uBCqdU1jo
nAZVJg6NK7ygvBq5xB817UZCi987kd7Roop5rkZjivMD0S4GFS/Ltldu3D5
r26tvAwYDOorZg74ciZMET/Ug03inOZOBKOrfP+s6wkulDyibYCczvO/yyl
NyWbSVKo2/5JIBDbvMycmlpTd7YZAUlthLZdqzSvTIRSE20dprKB/sY
CsrN4knbfwNXpaSYck4C7P8aQPWDxyOhblxF2ipDDdEmsKMnDlk7U0Q
```

下载

3. 使用KMS SDK解密证书密文文件

Python环境检查

运行测试代码需要Python运行环境，运行下面的命令可以检查你的主机是否已经支持

```
$ Python -V
Python 2.7.10
```

正常返回版本信息则代表支持，如果没有请参照 [Python安装指引](#)>>

运行Demo

Demo核心代码见下，可以通过链接 [快速开始Demo](#)>> 下载完整Demo

```
#!/usr/bin/env python
# coding=utf8

from kms.kms_account import KMSAccount
from kms.kms_exception import *

# 1.初始化KMS SDK
# 请填写你的云API密钥
secretId = "your secret id"
secretKey = "your secret key"

# 请根据你创建密钥的区域填写正确的endpoint URL
endpoint = "https://kms-gz.api.qcloud.com"
kms_account = KMSAccount(endpoint, secretId, secretKey)
```

2. 调用解密接口

```
CiphertextBlob = "your ciphertextblob";
Plaintext = kms_account.decrypt(CiphertextBlob)
print "the decrypted data is :\n%s\n" % Plaintext
```

- secretId和secretKey需要使用你创建密钥的帐号所绑定的云API密钥，你可以在这里找到你的 [云API密钥](#)
- endpoint需要和密钥创建时选择的区域对应，☑Demo使用的是广州区域对应的URL，详情见 [地域说明](#)
- CiphertextBlob即上一步通过控制台工具产生的证书密文，你也可以通过链接 [Demo证书（密文）>>](#) 下载后再复制对应文本到代码中，Demo压缩包中的kms_start_demo.py文件中已经为你替换好

Demo执行命令和运行结果如下，明文证书以字符串的形式解密在Demo程序的内存空间中

```
$ python kms_start_demo.py
```

```
the decrypted data is :
```

```
-----BEGIN CERTIFICATE-----
```

```
MIIICgjCCAeugAwIBAgIJAJqEq8+4pyq/MA0GCSqGSIb3DQEBCwUAMHoxCzAJBgNV
BAYTAIVTMQswCQYDVQQIDAJDQTElMAkGA1UEBwwCU0YxZDZANBgNVBAoMBkpveWVu
dDEQMA4GA1UECwwHTm9kZS5qc2EMMAoGA1UEAwwDY2ExMSAwHgYJKoZIhvcNAQkB
FhFyeUB0aW55Y2xvdWRzLm9yZzAeFw0xNTA0MTgxMzI4NDFaFw00MjA5MDIxMzI4
NDFaMHoxCzAJBgNVBAYTAIVTMQswCQYDVQQIDAJDQTElMAkGA1UEBwwCU0YxZDZAN
BgNVBAoMBkpveWVuDEQMA4GA1UECwwHTm9kZS5qc2EMMAoGA1UEAwwDY2EzMSAw
HgYJKoZIhvcNAQkBFhFyeUB0aW55Y2xvdWRzLm9yZzCBnzANBkgqhkiG9w0BAQEF
AAOBjQAwgYkCgYEAqs4MKn9saUlu/9EfHQpouC3kL9Mo5sd1WR6RBeSd8cqeFxXW
EWEq/P0hUeAH1sY0u8RFOccJmSJg8KTyRGc+VZzWimopz17mTuQY4hPW4bFzqmQm
7STfJz5eHzynBTU8jk5omi8hjbNRA38jOm4D7rN/vqtB+RG+vEhxONnq4DMCAwEA
AaMQMA4wDAYDVR0TBAUwAwEB/zANBkgqhkiG9w0BAQsFAAObgQBo8rX1uZWHvKHG
gWw+LXrY24Pk8NdDRmfqEVyuaR4GoGGOXcQlVaFa6x+4/eqOUzHoC9uGfPtjrW
BYQ1o/I0JZWW4KZYuXoVuMUSj+sel82mf9zLDeq5WYTPECgJDMfgVpXOmHfyezn
SkUTX7XJUohjET+X5BqTFlqRT/Rflw==
```

```
-----END CERTIFICATE-----
```

你可以将类似的代码结合到你的应用程序中，只需要☑一点点额外工作即可显著的提高安全性。

4. 在这个例子中，证书的安全性得到了怎样的提升？

- ☑ **静态存储安全**：主机上 不再有明文的证书文件，黑客以前直接以文本方式查看文件甚至通过后缀名即可判断是否是一个证书文件，而现在保存在磁盘的是一段 无法识别的密文文件。
- ☑ **流程安全**：对于大型开发商，密文证书由证书管理人员生成，开发人员负责开发解密和使用的程序，运维人员负责部署密文证书文件，流程中，开发和运维人员 都无法单独获取 到明文证书。而对于独立开发者，证书☑经常☑会“意外”的随代码一起被上传到Git，若是加密后的证书，即使意外上传也无安全风险。

5. 下一步可以做什么？

1. 通过控制台创建其他更多新的密钥，并管理它们，比如启用、禁用、修改昵称和用途描述。

1) [创建密钥](#)

2) [管理密钥](#)

2. 尝试更多的使用KMS提供能力去加密、解密文件，为你在实际业务中使用KMS 做准备。

1) [加密解密](#)

2) [敏感信息加密](#)

3. 如果你有对海量静态数据加密或通信加密的需求，可以去学习和尝试基于KMS 的信封加密方案。

1) [信封加密](#)

创建密钥

最近更新时间：2018-06-13 15:24:25

- 1.访问控制台页面 [控制台](#)
- 2.选择需要创建密钥的区域，单击『新建』。注意：目前量子密钥类型只有广州区域支持，其他区域暂未支持。
- 3.输入【密钥名称】，【密钥类型】和【密钥用途】，【密钥名称】必填且在区域内唯一，密钥名称只能为字母、数字及字符 "_" 和 "-"，且不能以 "KMS-" 开头，【密钥用途】部分选填
- 4.单击【确定】后返回密钥列表，新创建的密钥会出现在密钥列表首位，也可以通过密钥名称来识别新创建的密钥

管理密钥

最近更新时间：2018-06-13 15:26:43

查看密钥

访问[控制台](#)，注意主密钥是区分区域的，通过切换上方区域可以查看其他区域主密钥列表

启用、禁用密钥

单个操作

密钥信息的右侧操作区域可以对该密钥进行启用、禁用操作。

批量操作

支持勾选多个密钥，然后单击列表上方的操作按钮进行批量操作，单击后会弹出【操作确认框】，继续单击【确认】则对所有选中密钥进行对应操作。

如果同时选择了不同可用状态的密钥，则会在单击批量【启用】、【禁用】按钮后弹出的【操作确认框】里进行相应提示，单击【确定】后只会对状态符合要求的密钥进行操作，不符合的密钥保持原有可用状态

禁用密钥会导致所有依赖该密钥的加解密操作被同时禁用，所以在禁用密钥前，请确认没有运行中业务依赖该密钥。

查看密钥详情

单击任一密钥的【密钥ID/密钥名称】即可进入该密钥的【详情页】，可以查看和修改该密钥的信息，【在线工具】也在详情页。

修改名称、用途

在密钥【详情页】可以修改密钥的名称、用途，在单击【密钥名称】、【密钥用途】后方的按钮后弹出的对话框内输入需要新的内容。注意密钥名称只能为字母、数字及字符"_"和"-",且不能以“KMS-”开头

加密解密

最近更新时间：2018-06-13 15:28:01

腾讯云提供了对于小型数据（ < 4 KB ）加密、解密的API、SDK以及在线工具，您可以根据自己的需要以及不同的场景选择合适的使用方式。

API、SDK


在绝大多数情况下，开发者使用云API、SDK来对证书或密钥进行加解密操作，详细使用请参考

- [API概览](#)
- [C++ SDK](#)
- [JAVA SDK](#)
- [Python SDK](#)
- [PHP SDK](#)

在线可视化工具

在线工具适合处理单次或者非批量的加解密操作，比如首次生成密钥密文，开发者无需为非批量的加解密操作而去开发额外的工具，将精力集中在实现核心业务能力上，使用步骤如下。

1. 选择操作类型

在线工具 


加密 解密

请输入明文或选择文件

执行

下载

2. 输入待处理数据

在线工具 

加密 解密

Test for encryption

执行

下载

3. 执行操作，单击【执行】按钮

4. 获取处理后结果

在线工具 

加密 解密

Test for encryption

a21zLWFsdDB4eGZ6AAAAAAAAAAAA=84D3sP/toCDdxOEdXnoHEcuzg5
DFmXVfzAEq6cVFdQZhVqAQ==

执行

下载