

数字版权管理

开发指南

产品文档



腾讯云

【 版权声明 】

©2013–2021 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【 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。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【 服务声明 】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。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。

【 联系我们 】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100。

文档目录

开发指南

点播 DRM 加密工具

直播 DRM 推拉流

相关参考

开发指南

点播 DRM 加密工具

最近更新时间：2020-11-26 15:38:49

key、keyid、iv、content id 等数据可通过 DescribeKeys 接口获取。

Widevine 加密

- 推荐加密工具：[shaka packager](#)
- 加密命令：

```
$ ./packager-linux in={input filename},stream=audio,output={output filename} in={input filename},stream=video,output={output filename} --enable_raw_key_encryption --keys label={label}:key_id={key_id}:key={key},label={label}:key_id={key_id}:key={key} --pssh {pssh} --mpd_output {output mpd name}
```

🔗 说明：

Widevine 方案，音频和视频需使用不同的加密 key。

更多用法，请参考 [shaka packager 文档](#)。

准备 Fairplay 材料

以下四项材料需用户使用自己的 Apple 开发者帐户从 Apple 官方处获取，**材料不可复用**。

- 获取 FPS_Deployment_Package.zip 文件。
- 参照解压的 FPS_Deployment_Package 文档生成公私钥对。
- 提交生成的公钥给 Apple，获取 Apple 返回的公钥证书。
- 提交 Apple 返回的公钥证书后，获取网页显示的 Ask。

Fairplay 加密

- 推荐加密工具：[bento4 mp42hls](#)
- 加密命令：

```
$ ./mp42hls --encryption-mode SAMPLE-AES --encryption-key {key+iv} --encryption-iv  
-mode fps --output-single-file --encryption-key-uri skd://{content id} --encryptio  
n-key-format com.apple.streamingkeydelivery --encryption-key-format-versions 1 --i  
ndex-filename {output m3u8 filename} --segment-duration 10 {input filename}
```

更多用法，请参考 [bento4 文档](#)。

直播 DRM 推拉流

最近更新时间：2020-07-20 16:20:50

推流

直播使用 DRM，在推流参数中添加 txDRMInfo 参数即可，示例如下：

```
rtmp://xxx.livepush.myqcloud.com/live/test?bizid=1234&txDRMInfo=hls:fairplay,dash:widevine
```

Widevine 对应参数为 dash，Fairplay 对应参数为 hls，同一条直播流可同时使用多种 DRM 方案。

拉流

在流 ID 后添加 .mpd（Widevine 方案）或 .m3u8（Fairplay 方案）即可拉取加密流，示例如下：

```
http://xxx.liveplay.myqcloud.com/test/test.mpd?bizid=1234
```

相关参考

最近更新时间：2020-11-26 15:37:38

加密结果回调

```
{
  "DrmEncryptInfo": {
    "CosEndPoint": "cos.ap-hongkong.myqcloud.com",
    "DrmType": "fairplay",
    "OutputObjects": [
      {
        "BucketName": "drm-encrypt-1251697373",
        "ObjectName": "out.m3u8",
        "Para": {
          "Type": "m3u8"
        }
      },
      {
        "BucketName": "drm-encrypt-1251697373",
        "ObjectName": "out.ts",
        "Para": {
          "Type": "video"
        }
      }
    ],
    "CosSecretId": "xxx",
    "CosSecretKey": "xxx",
    "SourceObject": {
      "BucketName": "drm-unencrypt-1251697373",
      "ObjectName": "in.mp4"
    }
  },
  "Code": -26,
  "Message": "encrypt failed",
  "RequestId": "3fcd0191-2668-43e0-932f-26891d425540"
}
```

业务鉴权服务器参考

依赖云图 API Python sdk

[demo_fp_live_proxy.py](#)

[demo_fp_vod_proxy.py](#)

[demo_wv_vod_proxy.py](#)

[demo_wv_live_proxy.py](#)

🔗 说明:

相关操作均需在 Linux 下完成。

DescribeKeys 接口 rsa 公、私钥生成方法

生成私钥

```
$ genrsa -out rsa_private_key.pem 1024
```

生成公钥

```
$ rsa -in rsa_private_key.pem -pubout -out rsa_public_key.pem
```

Base64 加密公钥

```
$ base64 rsa_public_key.pem
```

解密 session key

```
$ echo { session_key } | base64 -d > session_key.en  
$ openssl rsautl -decrypt -in session_key.en -inkey rsa_private_key.pem -out session_key.de
```

解密 key

```
$ echo {key} | base64 -d > key.en  
$ openssl enc -aes-128-ecb -in key.en -out key.de -K { session_key } -d
```

Widevine 腾讯云服务证书

[腾讯云 Widevine 服务证书](#)

App 和 Web Demo 下载

[Android apk](#)

[web 页面](#)