

视频 实施指南 产品文档



腾讯云

【版权声明】

©2013-2020 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

实施指南

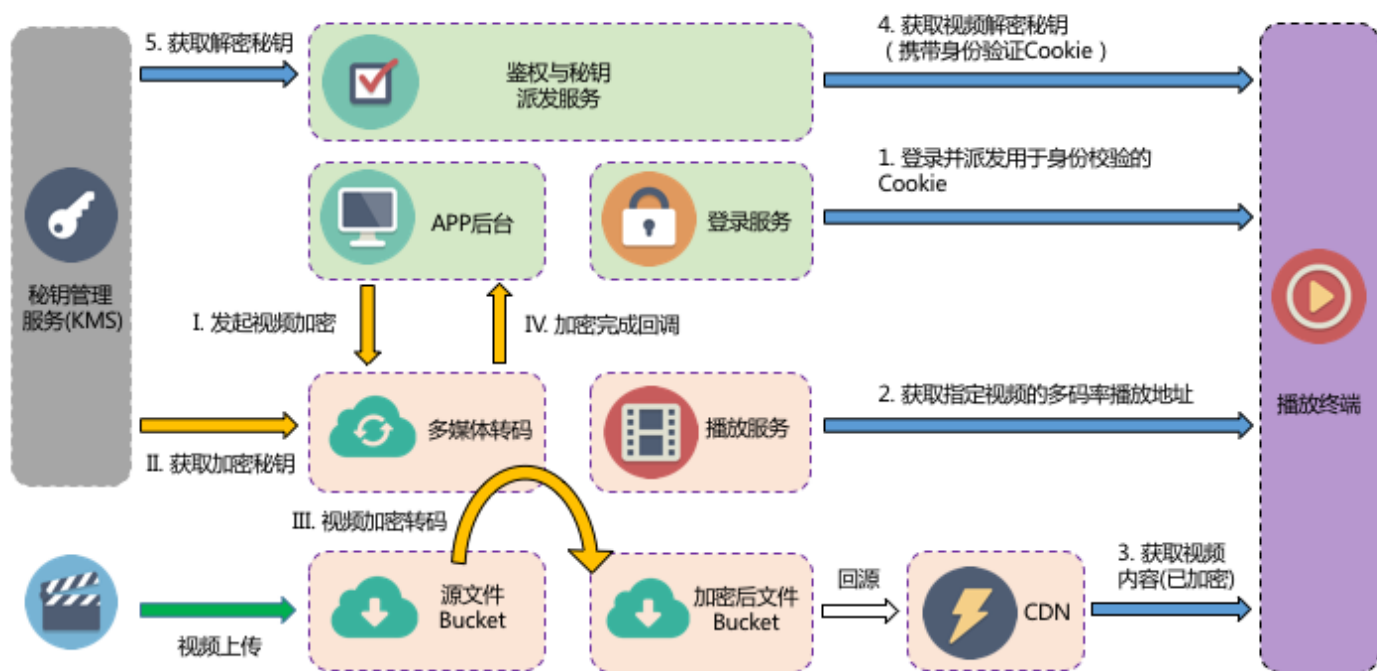
视频加密

实施指南

视频加密

最近更新时间：2020-07-28 14:56:02

整体架构



初步实施

建立密钥管理服务（KMS）

密钥管理服务主要用于管理视频密钥。视频加密过程需要与 KMS 系统进行交互，步骤如下：

1. 生成用于视频加密的数据密钥，即架构图中第II步。这一步将返回数据密钥（DK）和加密后的数据密钥（EDK）。在后续环节中，能够接触到 DK 的角色包括：点播转码服务、App 后台、经过合法身份校验的最终用户。EDK 可以分发给任意用户，但通过 EDK 获取 DK 这一步，必须由 App 后台进行身份校验。
2. 根据 EDK 获取 DK 来进行数据播放，即架构图中的第4步。App 后台在通过用户的身份验证后，需要调用 KMS 相关接口，使用 EDK 去获取 DK，即架构图中的第5步。

搭建鉴权与密钥派发服务

对于已加密的视频，只有经过 App 后台认证过的客户端才能得到 DK。因此，最终客户获取密钥的行为必须要有 App 后台参与鉴权。该服务的主要业务逻辑是：

1. 对于客户端携带 EDK 换取 DK 的请求（即架构图中第4步），对请求方进行身份认证。
2. 如果身份认证通过，则去 KMS 系统获取对应的 DK（即架构图中第5步），并返回给客户端。

配置视频加密模板

为确保点播后台能够进行正确的加密操作，您需要配置视频加密模板。详情请参见 [视频加密参数模板](#)。

完整实施

视频上传

可以通过服务端上传、客户端上传、控制台上传、录制上传、URL 转拉上传等方式来将已有视频文件上传到点播平台。

视频加密

视频加密主要分为以下四个步骤：

1. App 后台发起视频加密
目前您可以通过 [ProcessFile](#) 接口发起视频加密，目前只支持对 HLS 文件进行加密。
2. 点播平台获取加密密钥
点播平台根据调用方指定的加密参数模板，读取密钥获取方式、最终用户获取解密密钥的 URL（假定为 [https://getkey.example.com](#)），然后从指定 KMS 系统中获取视频加密密钥 DK、EDK。
3. 点播平台发起视频加密转码
点播转码平台在进行视频加密时，不仅会依照指定的加密算法和密钥对目标输出文件进行加密，而且会将获取解密密钥的 URL 写入视频文件中。
4. 点播平台发起加密完成回调
包含加密操作的任务流状态发生变化（或者执行完毕）后，点播平台将发起 [任务流状态变更通知](#)。

媒资管理

视频加密操作完成后，可通过 [GetVideoInfo](#) 接口获取视频的加密信息。

[GetVideoInfo](#) 接口会返回该视频所有转码规格的视频播放地址，包括源文件的播放地址，由于源文件是没有加密处理的，App 服务端可以过滤掉源文件的播放地址，只提供加密视频的播放地址给客户端。[GetVideoInfo](#) 获取到的源文件 definition 参数是0，可以根据这个值来过滤源文件的视频播放地址。

视频播放

只有经过合法身份认证的用户才应当得到视频解密密钥。因此在播放过程中，如何对用户的身份信息校验就成为关键因素。

播放过程中，播放器会访问 m3u8 文件中 EXT-X-KEY 标签所标识的 URI 以获取密钥，播放器需要在这一步中携带观看者的身份认证信息。此时有两种方式可以将这一信息传递给 App 鉴权服务：

1. 将用户身份信息通过参数的方式追加到 URI 中，带给 App 的鉴权服务；该方案适用于所有的 HLS 播放器。具体方案参见 [视频播放方案1：通过 QueryString 传递身份认证信息](#)。
2. 将用户身份信息通过 Cookie 带给 App 的鉴权服务；该方案安全性更高，但其仅适用于在访问 EXT-X-KEY 标签所标识的 URI 时会携带 Cookie 的播放器。具体方案参见 [视频播放方案2：通过 Cookie 传递身份认证信息](#)。