

视频加密

域名黑白名单、授权播放等安全机制主要用于控制视频播放请求来源的合法性，能够有效保障用户的合法访问。但这些机制不会对视频数据本身进行加密，对于付费观看视频的业务场景，用户只需通过一次付费行为拿到视频资源URL便可将视频下载到本地并进行二次分发，因此，这些机制对于视频版权保护是不够的。

保利威视频加密采用私有的加密算法，提供包括加密转码、安全传输、解密播放等一体化的视频安全方案。通过对视频数据本身进行高强度的加密，视频文件即使被下载到本地也无法直接播放和传播，可有效防止视频泄露和盗版问题。

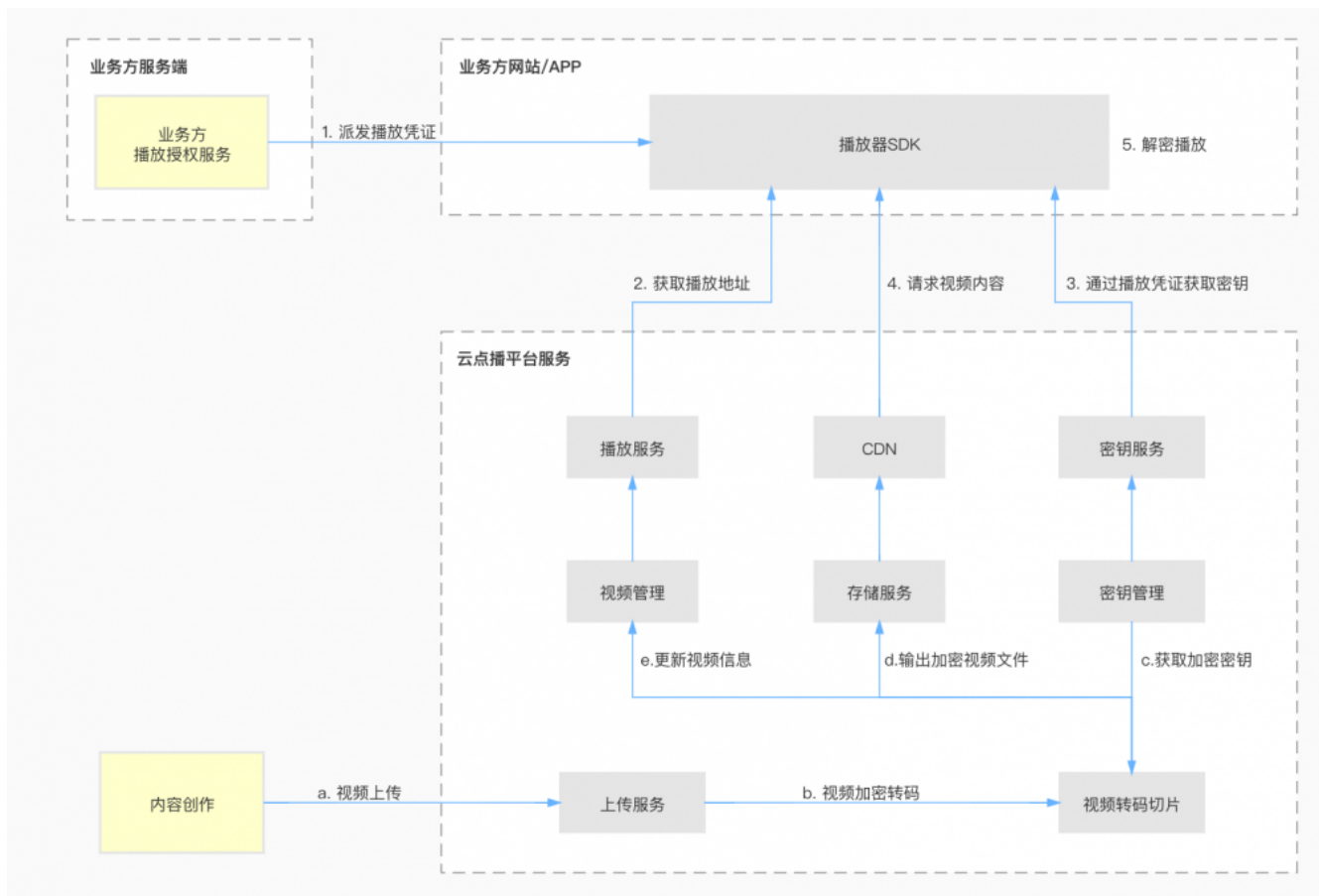
核心优势

保利威视频加密的核心优势有：

- 保利威视频加密功能采用自有知识产权的专利技术，视频的加密转码、传输、解密播放全部受私有算法保护，破解难度极高。
- 每个视频文件都有独立的私钥，能有效避免一个密钥的泄露引起大范围的安全问题。播放器和服务端使用加密协议进行密文传输，有效防止密钥被窃取。
- 提供多套不同安全级别的加密方案，可根据自身业务场景选择。
- 提供安全的播放器SDK，覆盖H5、Flash、iOS、Android、小程序、桌面客户端等多平台，且加密视频必须使用保利威安全播放器才能播放。
- 云点播平台提供了完整的加密视频播放授权体系，开发者只需获取播放凭证并传入Polyv播放器即可实现加密播放，免去了凭证和密钥的管理、验证、分发等开发工作。
- Polyv播放器提供的授权播放和防录屏跑马灯功能，进一步加强了版权保护能力。
- 保利威服务于上千家在线教育客户，视频版权保护技术不断更新迭代，始终处于行业领先水平。

流程架构

点播视频加密和解密播放的整体架构流程如下：



使用说明

一、后台配置

在云点播管理后台，支持针对整个账号或某个视频分类进行加密设置，操作流程如下：

1、登录云点播管理后台，点击 **【设置】** → **【加密设置】**，进入加密设置页面。



- 视频加密设置：打开后，**新上传**的视频都会经过加密转码。

- 加密视频授权设置：播放加密视频有四种授权方式，分别为：非加密授权、Web授权、App授权和小程序授权。这四种授权方式的安全级别不同，支持播放的终端也不同，您可以根据自身业务场景选择合适的授权方式。详见下表：

授权方式/支持终端	PC Web	手机H5	手机APP	PC 客户端	微信小程序
非加密授权	✓	✓	✓	✓	✓
WEB授权	✓	✓	✓	✓	✓
APP授权	✓	✗	✓	✓	✗
小程序授权	✓	✗	✓	✓	✓

- 安全级别从高到低排序为：APP授权 > 小程序授权 > WEB授权 > 非加密授权。
- 如果您的业务场景只有手机APP播放，建议选择“APP授权”，如果有手机H5播放视频的需求，建议选择“WEB授权”，但Web授权的安全级别低于APP授权。
- 加密视频只能通过保利威提供的安全播放器SDK才能播放。

2、开启加密设置后，所有新上传的视频都会经过加密转码。管理后台还支持只对某一视频分类进行单独设置。操作方式为：点击【视频列表】→【视频分类管理】，选中某个分类，点击【分类属性设置】，进行分类下的加密设置。



二、播放加密视频

加密视频必须使用保利威提供的播放器才能播放，云点播提供Web端、iOS、Android、小程序、桌面客户端等多平台的播放器SDK，以便您快速在自身应用或网站中集成。

- Web播放器（PC/手机 H5、Flash）：通过引入Polyv Web播放器代码，可在自己的Web页面嵌入播放器并实现播放，详见：[Web端播放加密视频](#)。
- 移动端播放器（iOS、Android SDK）：用户可以通过SDK快速集成视频播放能力到自己的应用中，详见：[iOS SDK](#)，[Android SDK](#)。