



技术开启新“视”界  
Technology Bring New Vision

## 视频加密和DRM的实施实践

周源

LiveVideoStack  
— 音视频技术社区 —

CSDN

1

数据加密

2

全链路保护

3

数字版权管理 ( DRM )

4

内容识别



- 对称

优点：计算量小，速度快、效率高。

缺点：密钥的管理和分发非常困难，不够安全。

常见算法：AES，DES

- 非对称

优点：算法公开，安全性高，公钥是公开的，私钥不需要公开。

缺点：加密和解密花费时间长、速度慢，只适合少量数据加密。

常见算法：RSA，ECC

- 视频特点
  - 数据量大 – 速度
    - 文本：KB，图片：MB，视频：GB
    - DVD 480P 4.7GB，蓝光 1080P 50GB
  - 各种软件平台 – 标准化
    - Linux、Windows、Mac
    - Android、iOS
  - 各种硬件芯片 – 功耗
    - 海思、瑞芯微...

- AES算法
  - 密码学：数学可证明的安全
  - 安全：2104亿年
  - 实现：均衡了时-空占用
  - 标准化：硬件芯片，软件平台
  - 风险：旁路攻击（攻击实现技术，不是算法。有解决方案）
- 速度

名称	密钥长度	运算速度	安全性	资源消耗
DES	56位	较快	低	中
3DES	112或168位	慢	中	高
AES	128、192、256位	快	高	低

- M3U8例子

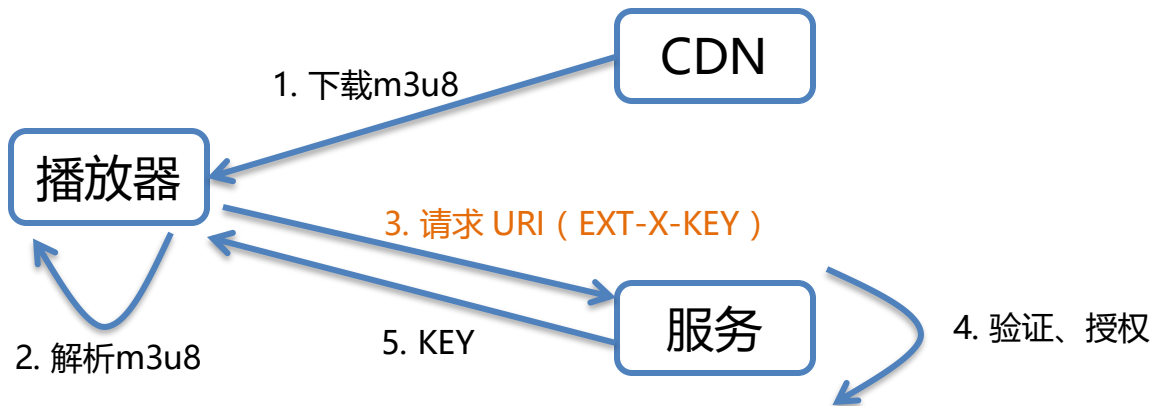
#EXT-X-KEY:METHOD=AES-128,URI="http://priv.example.com/key.php?r=52"

#EXTINF:2.833,

http://media.example.com/fileSequence52-A.ts


#EXTINF:15.0,

http://media.example.com/fileSequence52-B.ts





- CURL “<http://priv.example.com/key.php?r=52>”
- 16个字节的密钥



## 数据加密-问题？

---

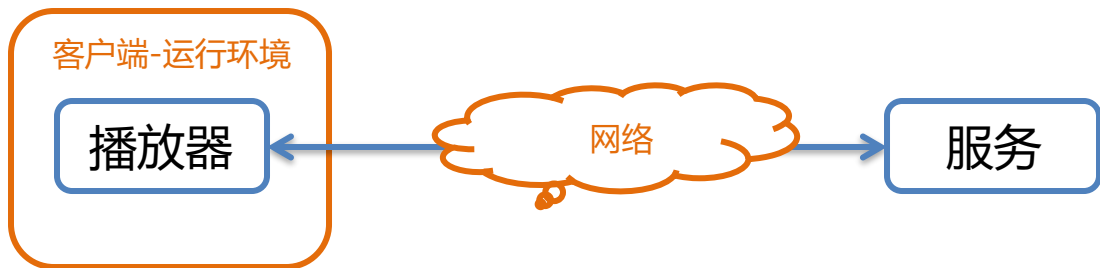


- 网络传输的安全（中间人攻击）X
- 客户端的安全（标准协议）X
- 解法：全链路保护





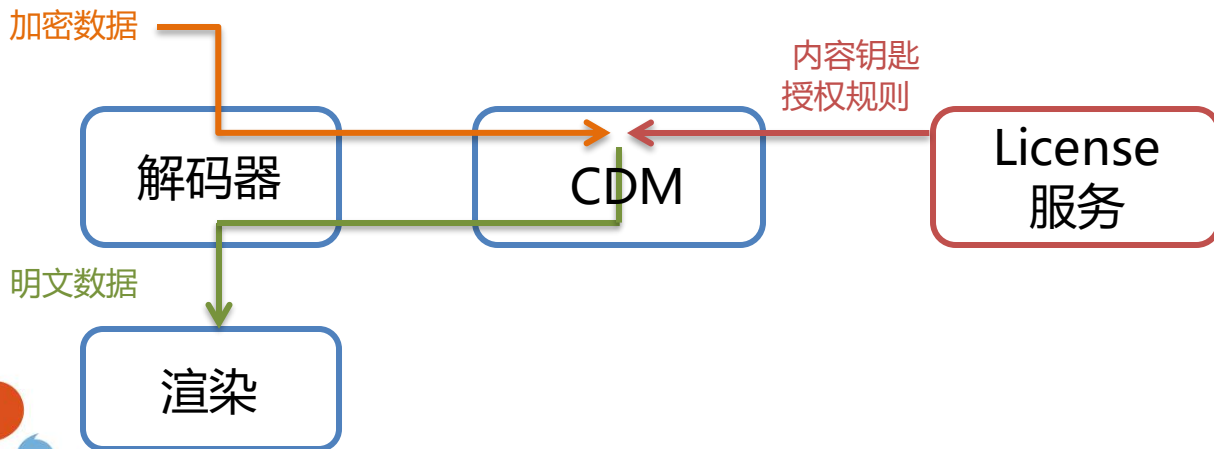
- 中间网络不可信
- 客户端不可信



- 经典方案：HTTPS
  - 融合非对称算法(RSA)和对称算法(AES)
  - 权衡安全和效率
  - 解决中间人攻击



- H5
  - IE、Chrome、Firefox、Safari
  - 标准：媒体源扩展（Media Source Extensions, MSE）  
+ 加密媒体扩展（Encrypted Media Extensions）
  - 非标准：内容解码模块（Content Decryption Module）  
授权的发放、格式、存储、使用规则和权限映射等细节，  
都由 DRM 提供商负责。






- 移动端
  - Web
    - 各种定制WebKit引擎不支持内容解码模块 ( Content Decryption Module )
    - 标准：JavaScript
    - 缺点：安全性差（明文代码），定制，私有
    - 安全改进：WebAssembly
  - App
    - 标准：无
    - 缺点：定制、私有



- 恶意用户
  - 开发者工具，模拟器，定制软件
  - 真正的不可信
  - 自动化：破坏力强，损失大



## 全链路保护-问题？

---



- 网络传输的安全（HTTPS）✓
- 客户端的安全（标准协议）✗
- 解法：数字版权管理（DRM）

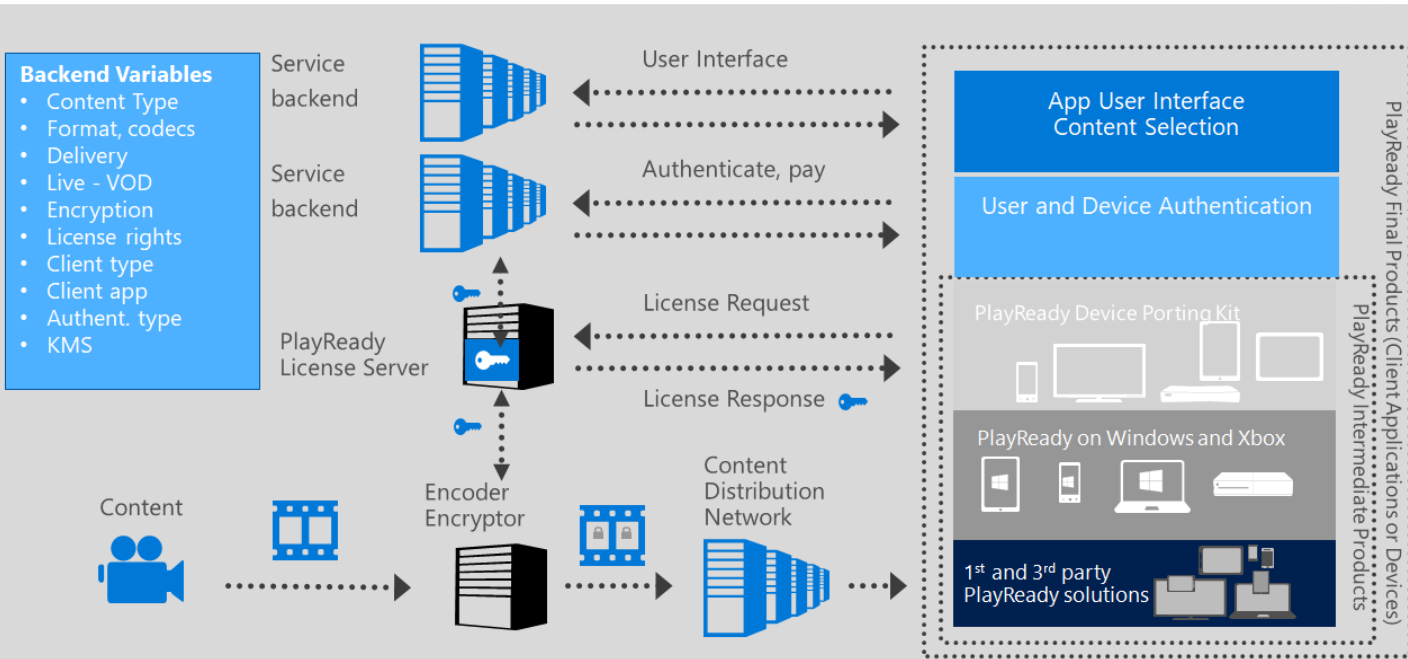




- 平台之争
  - 厂商：微软的PlayReady，谷歌的Widevine，苹果的FairPlay
  - 操作系统：Microsoft，Mac
  - 浏览器：IE/Edge，Chrome，Safari
  - 移动平台：Android，iOS

# 数字版权管理 ( DRM ) - 如何跨平台 ?

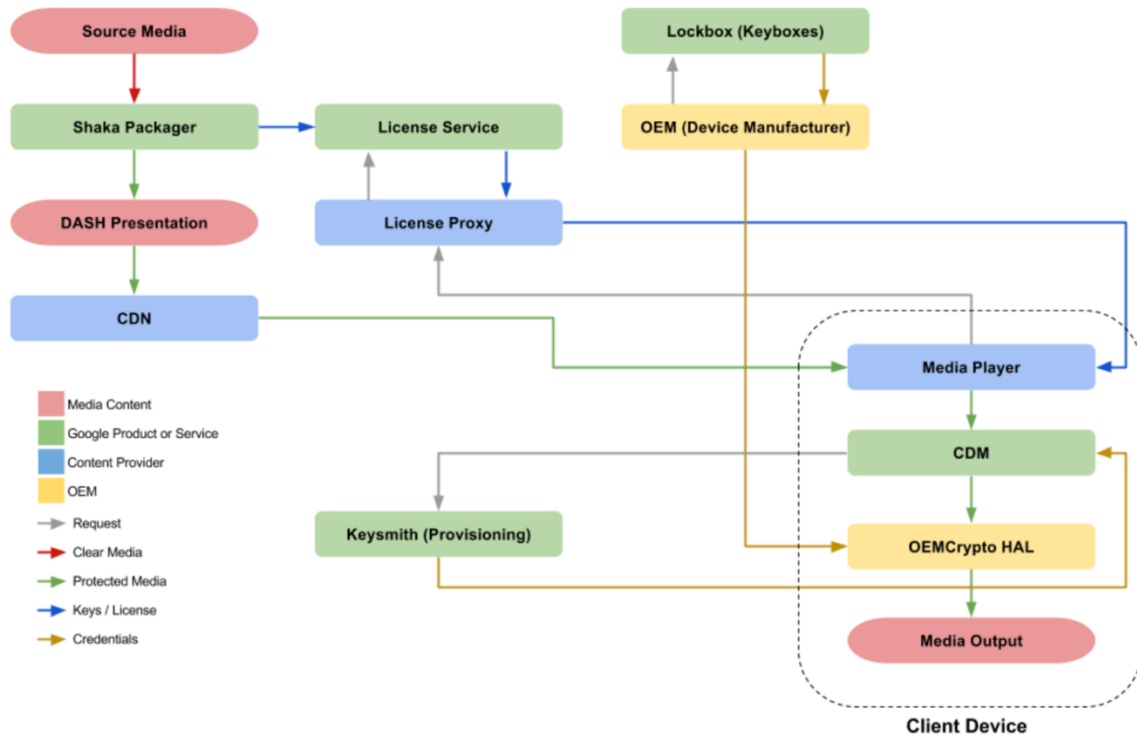
- PlayReady





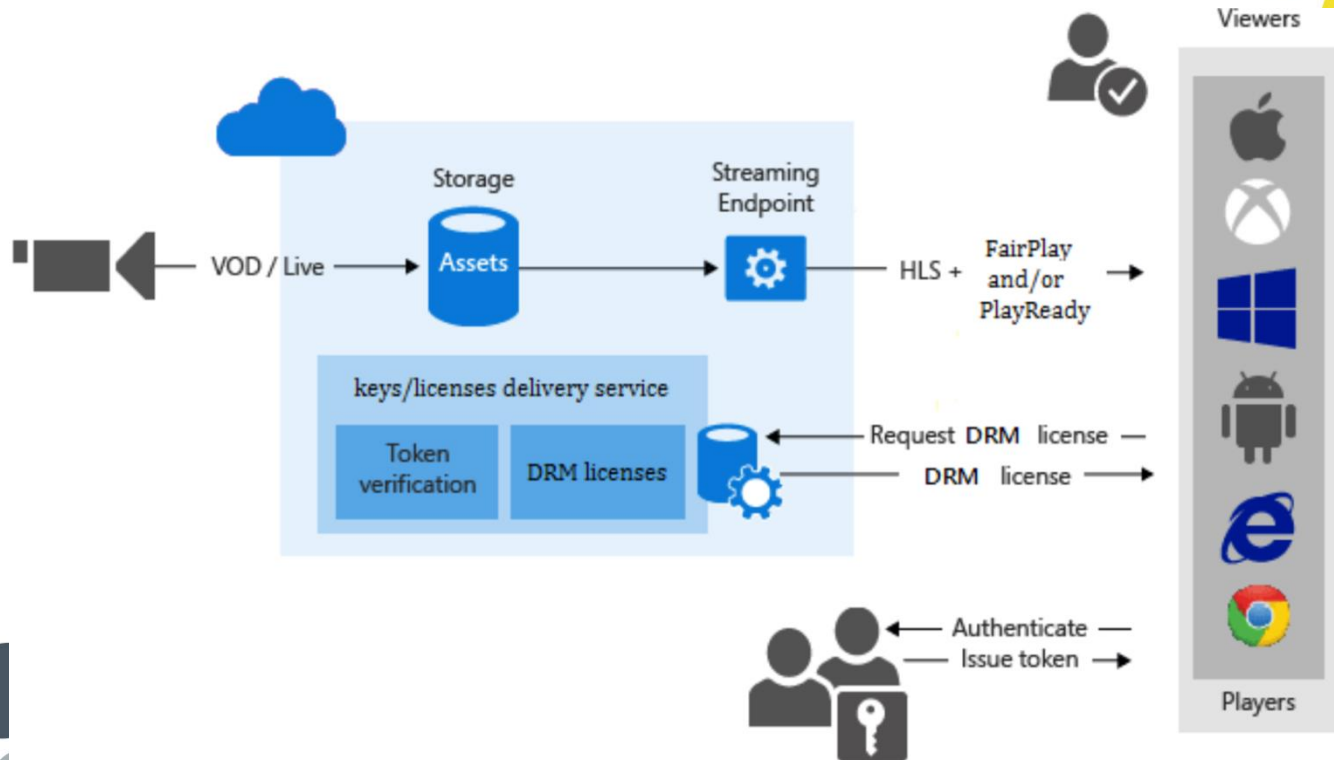
# 数字版权管理 ( DRM ) - 如何跨平台？

- Widevine



## 数字版权管理 ( DRM ) - 如何跨平台？

- FairPlay



# 数字版权管理 ( DRM ) - 多重DRM

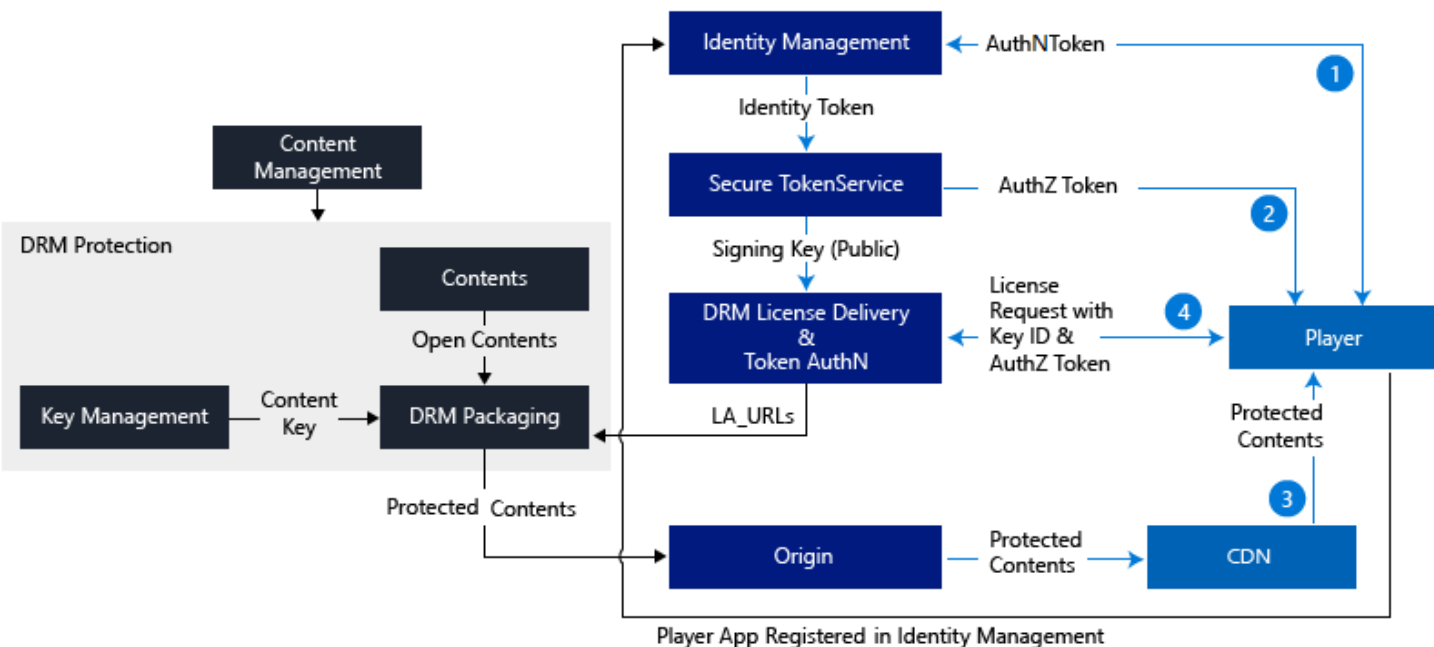


## Logical Diagram of a Generic DRM Subsystem with CENC

Back-Office/Setup Time

DMZ/Public Facing Endpoints

Public/Runtime



- 多重DRM
  - 降低加密成本：对于不同平台使用其原生 DRM 进行单一加密处理。
  - 降低管理成本：只需要一份加密资产。
  - 消除客户端许可成本：因为原生 DRM 客户端在其原生平台上通常是免费提供的。
- 技术方案：通用加密格式(CENC)+DASH
  - AES-128 Counter (CTR )
  - 支持H5 , App
- 现实
  - FairPlay : AES-128 Cipher Block Chaining CBC ( CBC )
  - 两份加密资产



- 破解
  - HDCP主密钥泄露
  - **4K**视频版权保护技术被破解
  - Netflix 4K版权保护恐被攻破 《绝命毒师》第一季现身PT网站
- 被动保护
- 解法：内容识别




重混

“对已有事物的重新排列和再利用，而对传统的财产观念和所有权概念产生巨大的影响。”

《必然》

凯文·凯利



- 是否对原有素材做了一定的转化，还是仅仅复制了原作？
  - 禁止还是开放？
  - 每个人都可以是导演，把自己录制的或者网上收集的素材重混起来就是一部新的作品
  - 例子
    - Youtube：克里斯 布朗的歌曲 “Forever”
    - 《JK婚礼入场舞蹈》 背景音乐 4000万次播放
    - 18个月后，重回iTunes榜单第四名
    - 版权方双重获利（广告、iTunes）
- 

- 视频指纹
  - 一种识别、提取、压缩视频的技术，可以产生唯一“指纹”代表视频文件进行视频查找



提取指纹



检索指纹





- 版权保护


新增视频与版权库做比对，对存在版权风险的视频进行播放控制，降低侵权风险;对自有版权的视频资源，从公网抓取视频数据鉴别，防止自有版权内容被侵权。

- 原创识别

识别视频是否是原创视频、剪辑后视频、自媒体再创造视频。

- 广告分成

判断新上传的视频原创性，检索分成库召回认领视频，支撑广告分成业务生态。



- 数据加密
  - 安全的基础，但是没有解决问题
- 全链路保护
  - 整体保护的方案，但是无法落地
- 数字版权管理（DRM）
  - 完善的保护，但是依旧存在风险
- 内容识别
  - 改变思路，被动变主动，开拓更广阔空间

# Thank you

