GY

中华人民共和国广播电视和网络视听行业标准

GY/T XXX—XXXX

视音频内容分发数字版权管理　互联网电视 DRM 系统集成

Digital rights management of video audio content distribution—
OTT TV DRM system integration

（报批稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

国家广播电视总局　　发 布

目　　次

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件发布机构不承担识别这些专利的责任。

本标准由全国广播电影电视标准化技术委员会（SAC/TC 239）归口。

本标准起草单位：国家广播电视总局广播电视科学研究院、中央广播电视总台、广东南方新媒体股份有限公司、华数数字电视传媒集团有限公司、阿里巴巴（中国）有限公司、百视通网络电视技术发展有限责任公司、湖南快乐阳光互动娱乐传媒有限公司、北京爱奇艺科技有限公司、上海海思技术有限公司、北京数码视讯科技有限公司、北京江南天安科技有限公司、北京数字太和科技有限责任公司、北京永新视博数字电视技术有限公司、北京安视网信息技术有限公司、中国传媒大学、英特尔（中国）有限公司、深圳创维-RGB电子有限公司。

本标准主要起草人：丁文华、郭沛宇、王兵、王磊、罗泽文、冉大为、张智骞、陈靓、邵淇锋、赵鹏、姜堑、汤毅、刘广宾、陈赫、陈钢、梁志坚、吴迪、郑黎方、赵云辉、马吉伟、刘琦、汪沛、张晶、田雪冰、刘好伟、张鹏、林卫国、隋爱娜、尚文倩、周菁、曹建香、梅雪莲、张智军、沈阳、王佳敏、姜涛。

视音频内容分发数字版权管理　互联网电视DRM系统集成

1　范围

本标准规定了互联网电视数字版权管理系统集成框架、系统功能和接口协议。

本标准适用于互联网电视数字版权管理系统集成部署与实施。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GY/T 277—2019　视音频内容分发数字版权管理技术规范

GY/T XXX—XXXX　视音频内容分发数字版权管理　有线数字电视DRM系统集成

3　术语和定义

下列术语和定义适用于本文件。

3.1

许可证　license

对数字媒体内容访问权限、使用规则和密钥等控制信息的描述。

[GY/T 277—2019，定义3.2]

3.2

DRM客户端　DRM client

设备中的可信实体，负责执行与DRM内容相关的许可和限制。

[GY/T 277—2019，定义3.4]

3.3

设备　device

安装有DRM客户端的消费内容的实体。

[GY/T 277—2019，定义3.3]

3.4

DRM内容　DRM content

采用DRM技术管理的数字媒体内容。

[GY/T 277—2019，定义3.6]

3.5

密文 ciphertext
已加密的信息。
[GY/T 277—2019，定义3.7]

3.6

加密 encryption
为了产生密文，即隐藏数据的信息内容，由密码算法对数据进行（可逆）变换。
[GY/T 277—2019，定义3.8]

3.7

解密 decryption
与加密过程相对应的逆过程。即由密码算法对密文数据进行逆变换。
[GY/T 277—2019，定义3.9]

3.8

密钥 key
控制密码变换操作（例如：加密、解密、密码校验函数计算、签名生成或签名验证）的符号序列。
[GY/T 277—2019，定义3.10]

4 缩略语

下列缩略语适用于本文件。
CRL 证书吊销列表（Certificate Revocation List）
DRM 数字版权管理（Digital Rights Management）
EPG 电子节目指南（Electronic Program Guide）
OCSP 在线证书状态协议（Online Certificate Status Protocol）
TEE 可信执行环境（Trusted Execution Environment）
URL 统一资源定位符（Uniform Resource Locator）

5 集成框架

互联网电视数字版权管理系统包括内容加密、密钥管理、密钥网关、内容授权以及DRM客户端等核心功能。互联网电视数字版权管理系统集成框架如图1所示。

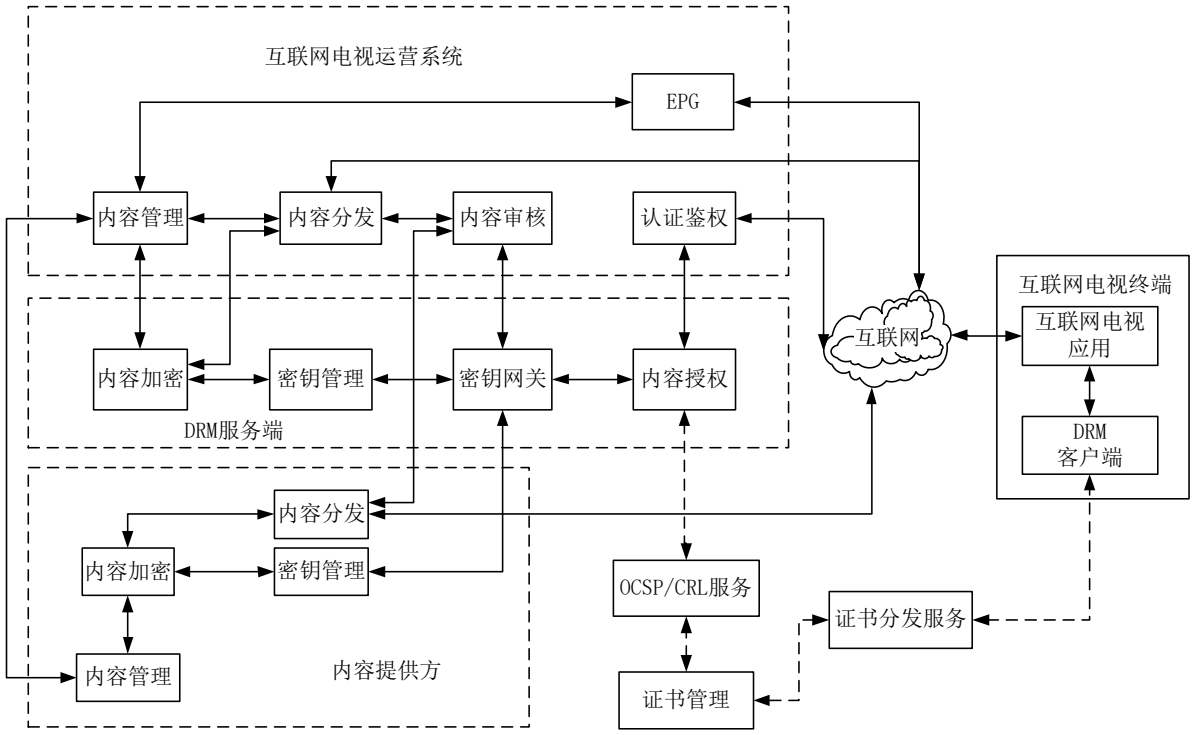

图1　互联网电视数字版权管理系统集成框架

互联网电视运营系统和内容提供方的内容管理负责维护内容提供方的版权要求，如客户端安全等级要求、输出保护要求等；该要求将通过密钥同步消息同步到密钥网关，在内容授权从密钥网关请求内容加密密钥时将该内容版权要求发送给内容授权，由内容授权作为内容加密密钥的密钥使用规则封装在内容授权许可证中发送给互联网电视终端。互联网电视运营系统的鉴权模块负责内容的按次、按时间段等付费和播放模式，内容授权只负责客户端安全等级要求、输出保护要求等版权方使用规则。

内容可在互联网电视运营系统加密，也可在内容提供方系统加密，所有的内容加密密钥均由密钥管理产生，并同步到互联网电视运营系统的密钥网关；如果内容在内容提供方系统加密，则内容提供方的内容管理应与互联网电视运营系统的内容管理进行交互，同步内容唯一标识、加密内容地址等相关信息；所有内容在通过内容分发注入到内容分发网络之前应经过互联网电视运营系统审核；互联网电视运营系统的内容审核通过密钥网关请求内容加密密钥，对内容进行解密播放审核。

互联网电视终端内的DRM客户端和DRM客户端证书及私钥应采用产线烧写或在线分发的方式进行置入。互联网电视终端应用在播放鉴权时从DRM客户端请求许可证获取请求消息，通过播放鉴权消息发送到互联网电视运营系统的鉴权模块，由鉴权模块判断是否为该互联网电视终端应用提供内容授权；如需提供内容授权，则鉴权模块将许可证获取请求消息发送到内容授权，从内容授权请求内容授权许可证，并将内容授权返回的许可证获取响应消息通过播放鉴权返回给互联网电视终端应用，由互联网电视终端应用调用DRM客户端实现许可证获取响应消息的解析、许可证的解析处理、以及内容的解密播放。

6　内容加密

内容可在互联网电视运营系统的内容加密系统加密后注入到内容分发网络，也可在内容提供方的内容加密系统加密后注入到内容分发网络。

内容管理系统向内容加密系统下达内容加密任务，内容加密系统接收到内容加密任务后，从密钥管理系统申请内容加密密钥按照规定的加密算法和加密模式进行内容加密，内容加密完成后，将内容存放到内容加密任务指定的位置，并通知密钥管理系统可将密钥同步到密钥网关系统。

内容管理系统应维护内容加密模式、内容唯一标识、内容使用规则等，在下达内容加密任务时，应携带内容唯一标识和必要的内容使用规则。内容加密完成后，在内容发布之前，内容分发应能从内容管理获得内容加密模式、内容唯一标识、内容编码格式等信息，用于封装M3U8等索引文件。

内容如果在内容提供方进行加密，内容提供方应将内容唯一标识、加密内容地址等同步至互联网电视运营方的内容管理系统，以便于互联网电视运营方进行加密内容的审核。

内容管理系统应将内容是否加密、内容唯一标识等信息同步到EPG系统，互联网电视终端应用应能够通过该信息判断在播放鉴权时是否需要初始化DRM客户端实例，从DRM客户端请求许可证获取请求消息。

内容加密封装应符合GY/T XXX—XXXX《视音频内容分发数字版权管理　有线数字电视DRM系统集成》中6.1的规定；内容管理与内容加密之间的接口协议应符合GY/T XXX—XXXX《视音频内容分发数字版权管理　有线数字电视DRM系统集成》中6.3的规定。

7　密钥管理

密钥管理系统为内容加密系统生成内容加密密钥，并负责将内容加密密钥同步到密钥网关。

内容加密与密钥管理之间的接口、密钥管理与密钥网关之间的密钥同步接口应符合GY/T XXX—XXXX《视音频内容分发数字版权管理　有线数字电视DRM系统集成》中7.2的规定。

8　内容授权

8.1　内容授权机制

内容管理系统负责管理内容唯一标识、内容使用规则、内容加密模式、加密内容URL等信息，通过向内容加密系统下达加密任务实现内容加密。内容加密完成后，内容加密密钥同步到互联网电视运营系统的密钥网关系统，加密后的内容通过内容分发网络进行分发。

互联网电视运营系统的内容授权系统通过鉴权系统统一为互联网电视终端应用提供内容授权许可证。

密钥网关系统与内容授权系统之间的密钥查询接口应符合GY/T 277—2019中9.3的规定。内容授权系统与鉴权系统之间的许可证获取接口应符合GY/T 277—2019中第8章的规定。

8.2　内容审核机制

互联网电视内容加密后，在内容分发系统将内容注入到内容分发网络之前，应对加密内容进行审核。

内容审核系统应从证书管理系统申请内容审核专用客户端证书和私钥，配置密钥网关系统URL和证书链等信息，从互联网电视运营系统的内容管理系统获取待审核内容的唯一标识、内容地址等，按照GY/T 277—2019中9.3的接口从密钥网关申请内容加密密钥，采用内容加密密钥解密播放内容进行审核。

9　客户端集成

9.1　互联网电视终端播放流程

互联网电视终端应用播放加密内容的流程如图2所示。

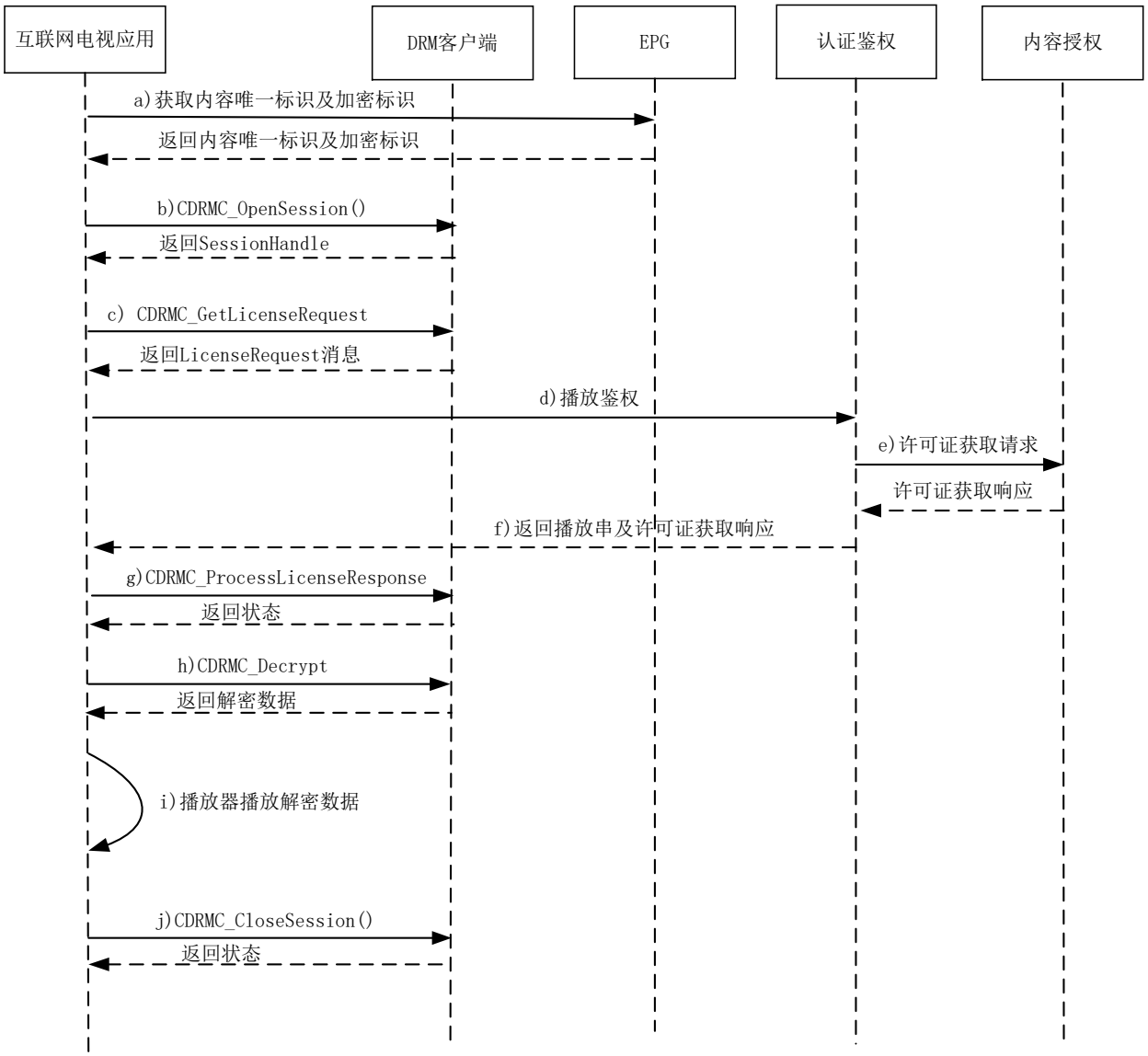

图2　互联网电视终端应用播放加密内容流程

互联网电视终端应用播放加密内容的流程说明如下：

a) 用户通过互联网电视终端应用浏览 EPG。用户选定内容后，互联网电视终端应用通过 EPG 信息中的内容加密标识、加密内容唯一标识判断是否为加密内容；如果是加密内容，则执行后续步骤。

b) 互联网电视终端应用通过调用 CDRMC_OpenSession 接口初始化 DRM 客户端，创建 DRM 会话，CDRMC_OpenSession 接口见 GY/T 277—2019 中的 C.3.1。

c) 互联网电视终端应用调用 DRM 客户端 CDRMC_GetLicenseRequest 接口，得到许可证获取请求消息，CDRMC_GetLicenseRequest 接口见 GY/T 277—2019 中的 C.3.3。

d) 互联网电视终端应用将许可证获取请求消息封装到播放鉴权消息中，发送到互联网电视运营平台的鉴权系统进行播放鉴权。如果鉴权失败，则互联网电视终端应用跳到 j）。如果鉴权成功，执行后续步骤。

e) 鉴权系统将许可证获取请求消息发送到 DRM 内容授权系统申请内容授权许可证。DRM 内容授权系统封装内容授权许可证到许可证获取响应中，返回给鉴权系统。

f） 鉴权系统将接收到的许可证获取响应和播放串封装到播放鉴权响应中，返回给互联网电视终端应用。

g） 互联网电视终端应用通过调用 CDRMC_ProcessLicenseResponse 接口，将许可证获取响应发送给 DRM 客户端实例，如果 DRM 客户端实例返回失败则跳转到 j）；返回成功则执行后续步骤。CDRMC_ProcessLicenseResponse 接口见 GY/T 277—2019 中的 C.3.4。

h） 播放器实例通过调用 CDRMC_Decrypt 接口将视频密文数据传给 DRM 客户端实例解密，DRM 客户端实例解密视频密文，将视频明文返回给播放器实例。CDRMC_Decrypt 接口见 GY/T 277—2019 中的 C.3.8。

i） 互联网电视终端应用启动播放器实例，将 DRM 客户端实例传入播放器，进行点播内容的下载、解密和播放。

j） 播放结束或异常退出时，互联网电视终端应用通过调用 CDRMC_CloseSession 接口关闭 DRM 会话，退出播放。CDRMC_CloseSession 接口见 GY/T 277—2019 中的 C.3.2。

9.2 DRM 客户端初始化机制

DRM客户端初始化主要是指DRM客户端密钥和证书的置入。DRM客户端密钥和证书置入分为离线分发和在线分发两种方式。离线分发是指互联网电视终端在出厂前预置DRM客户端证书和私钥，应符合GY/T XXX—XXXX《视音频内容分发数字版权管理　有线数字电视DRM系统集成》中9.2的规定；在线分发方式是指互联网电视应用在第一次启动时从服务端申请DRM客户端证书和私钥，流程如图3所示。

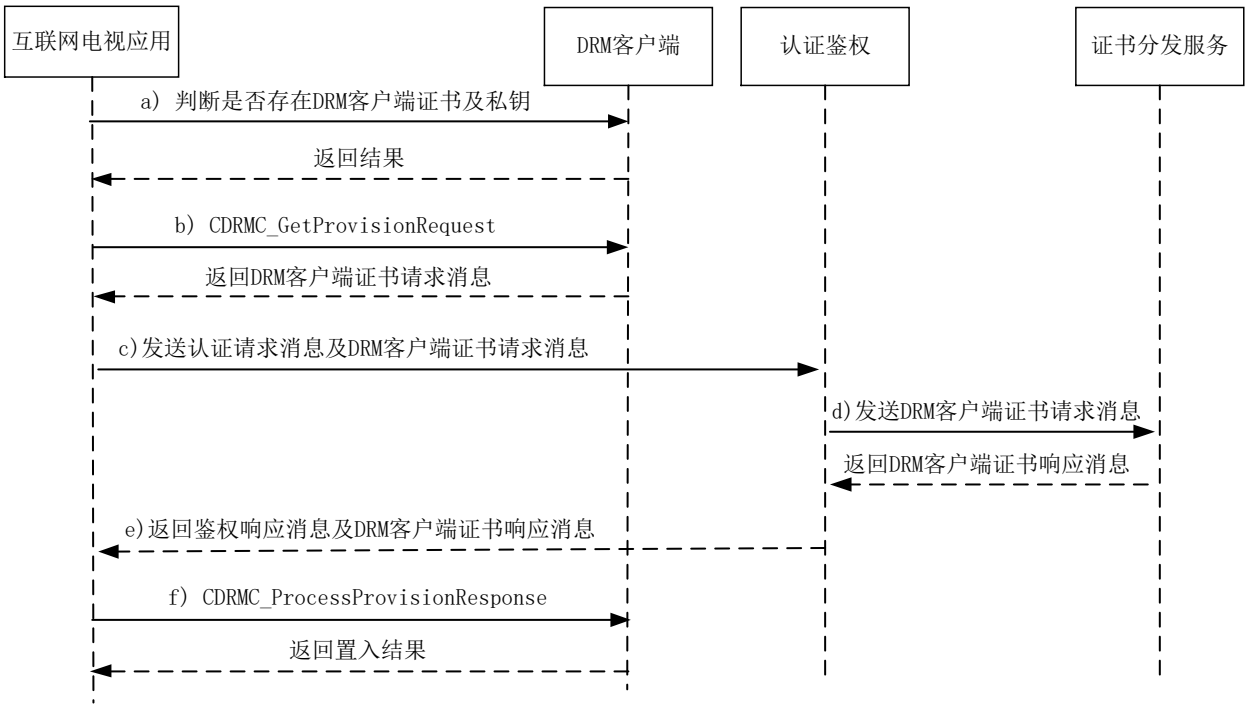

图3　DRM 客户端证书在线置入流程

互联网电视应用启动时，应调用DRM客户端接口判断是否存在DRM客户端证书和私钥；如果不存在，则在启动鉴权阶段，请求DRM客户端证书请求消息，将该消息封装在鉴权请求消息中发送给鉴权系统；鉴权系统将该消息转发给DRM客户端证书分发系统，由该系统封装DRM客户端证书响应消息发送给鉴权系统；鉴权系统将该消息封装在鉴权响应消息中发送给互联网电视应用，由互联网电视应用调用DRM客户端接口进行DRM客户端证书和私钥的置入。

DRM客户端证书在线置入流程说明如下：

a) 互联网电视应用启动时，应调用DRM客户端接口判断是否存在DRM客户端证书和私钥；
b) 如果DRM客户端证书不存在，则调用CDRMC_GetProvisionRequest接口获得证书请求消息，CDRMC_GetProvisionRequest接口见GY/T 277—2019中的C.3.5；
c) 互联网电视应用将证书请求消息封闭到认证请求消息中，发送到认证鉴权系统；
d) 认证鉴权系统将请求中的DRM客户端证书请求转发到证书分发服务；
e) 认证鉴权系统将证书分发服务返回的证书信息及认证消息合并后返回给互联网电视终端；
f) 互联网电视应用调用CDRMC_ProcessProvisionResponse接口完成证书的置入，DRMC_ProcessProvisionResponse接口见GY/T 277—2019中的C.3.6。

9.3 DRM客户端集成机制

互联网电视终端具备可信硬件执行环境的情况下，互联网电视终端应在出厂时预置DRM客户端证书和私钥到设备TEE中，互联网电视终端应提供基于TEE的DRM客户端给互联网电视应用调用。

互联网电视终端不具备可信硬件执行环境的情况下，互联网电视终端应在出厂时预置DRM客户端证书和私钥到设备的软件安全执行环境中（如：基于白盒密码的软件安全执行环境），互联网电视终端应提供统一的基于软件安全执行环境的DRM客户端给互联网电视应用调用。

已有的互联网电视终端应支持在应用中包含DRM客户端，该DRM客户端应运行在软件安全执行环境中，基于该软件安全执行环境运行DRM客户端。