GY

中华人民共和国广播电视和网络视听行业标准

GY/T 246—2020
代替 GY/T 246—2011

视音频内容分发数字版权管理　IPTV 数字版权管理系统集成

Digital rights management for video audio content distribution—
Digital rights management system integration for IPTV

2020－11－09 发布　　2020－11－09 实施

国家广播电视总局　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件代替GY/T 246—2011《数字版权管理系统与IPTV集成播控平台接口技术规范》，与GY/T 246—2011相比，主要技术变化如下：

——修改了范围，明确了适用于IPTV数字版权管理系统集成部署实施（见第1章，2011年版的第1章）；

——修改了规范性引用文件（见第2章，2011年版的第2章）；

——删除了术语和定义（2011年版的第3章）；

——删除了系统功能和架构（2011年版的第5章）；

——增加了集成框架（见第4章）；

——删除了A类接口（2011年版的第6章）；

——增加了直播内容加密与授权（见第5章）；

——删除了B类接口（2011年版的第7章）；

——增加了点播内容加密与授权（见第6章）；

——删除了C类接口（2011年版的第8章）；

——增加了DRM客户端集成（见第7章）。

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。

本文件由全国广播电影电视标准化技术委员会（SAC/TC 239）归口。

本文件起草单位：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、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、阿里巴巴（中国）有限公司、北京爱奇艺科技有限公司、华数数字电视传媒集团有限公司、上海海思技术有限公司、北京数字太和科技有限责任公司、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。

本文件主要起草人：丁文华、郭沛宇、王兵、王磊、张智骞、罗泽文、陈志业、汤毅、刘广宾、赵鹏、陈赫、陈钢、陈靓、戴金晶、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、姜涛。

本文件于2011年7月首次发布。

视音频内容分发数字版权管理　IPTV数字版权管理系统集成

1　范围

本文件规定了IPTV数字版权管理系统集成框架、直播内容加密与授权、点播内容加密与授权以及DRM客户端集成。

本文件适用于IPTV数字版权管理系统集成部署与实施。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 333—2020　视音频内容分发数字版权管理　有线数字电视数字版权管理系统集成

ISO/IEC 23000-19:2018　信息技术　多媒体应用格式（MPEG-A）　第19部分：分片媒体的通用媒体应用格式（CMAF）（Information technology — Multimedia application format (MPEG-A)—Part 19:Common media application format (CMAF) for segmented media）

3　缩略语

下列缩略语适用于本文件。

CBC　密码分组链接（Cipher Block Chain）

CEI　内容加密信息（Content Encryption Information）

ChinaDRM　中国数字版权管理（China Digital Rights Management）

CRL　证书撤销列表（Certification Revocation List）

DRM　数字版权管理（Digital Rights Management）

EPG　电子节目指南（Electronic Program Guide）

HLS　基于HTTP的实时流媒体协议（Http Live Streaming）

MPD　媒体展现描述（Media Presentation Description）

OCSP　在线证书状态协议（Online Certificate Status Protocol）

PMT　节目映射表（Program Mapping Table）

TS　传送流（Transport Stream）

URI　通用资源标识符（Uniform Resource Identifier）

URL　统一资源定位符（Uniform Resource Locator）

4　集成框架

IPTV DRM系统包括IPTV集成播控总平台DRM系统和IPTV集成播控分平台DRM系统。IPTV集成播控总平台DRM系统应包括：直播内容加密、点播内容加密、密钥管理等子系统；IPTV集成播控分平台DRM系统应包括：直播内容加密、点播内容加密、密钥管理、密钥网关、内容授权等子系统。

IPTV DRM系统集成框架如图1所示。

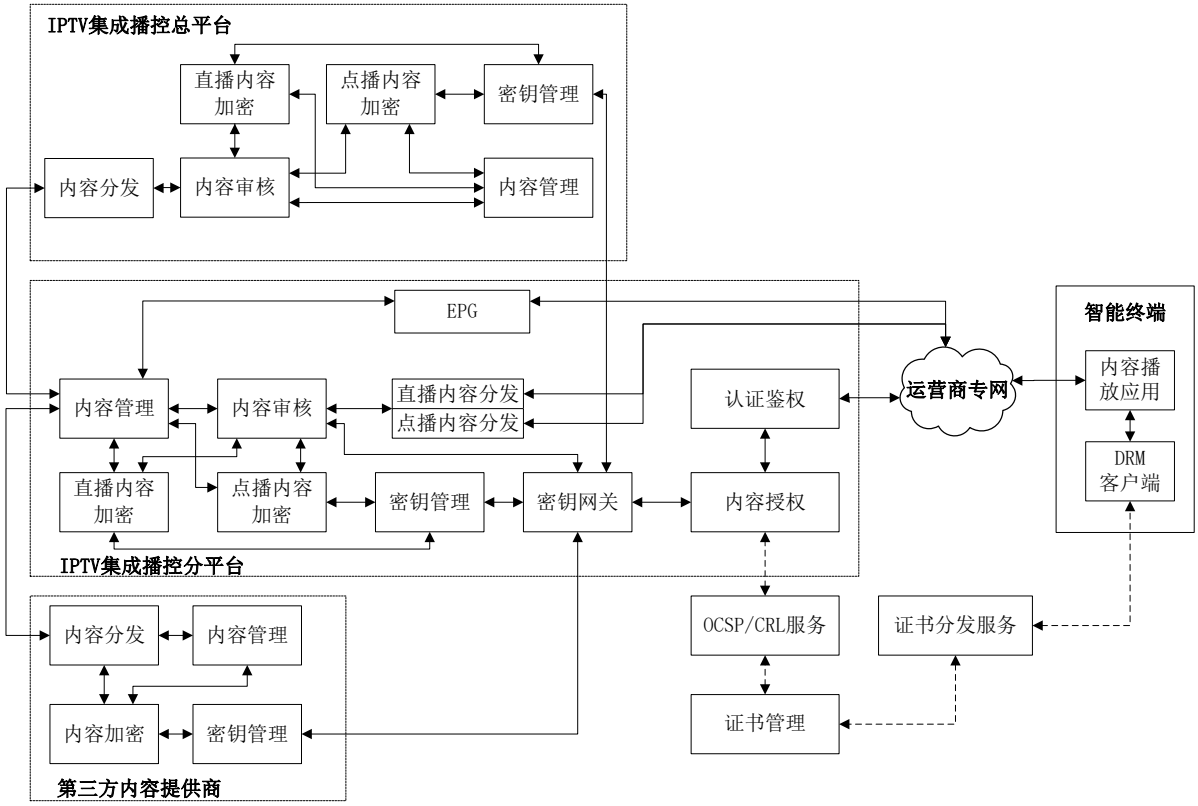

图1　IPTV DRM系统集成框架

受保护视音频内容可由内容提供方系统加密，或由IPTV集成播控总平台、分平台系统进行加密。内容加密密钥应同步至播控平台密钥网关。如果内容在第三方内容提供方或IPTV集成播控总平台加密，则内容提供方或总平台的内容管理应与IPTV集成播控分平台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；IPTV集成播控总平台和各IPTV集成播控分平台的内容管理系统管理各自平台内容唯一标识、内容使用规则、内容加密模式、加密内容URL等信息，通过向内容加密子系统下达加密任务实现内容加密。加密后的内容通过IPTV专网分发至IPTV集成播控分平台。IPTV集成播控分平台内容授权子系统通过认证鉴权系统统一为IPTV智能终端提供直播和点播内容授权许可证。

IPTV集成播控总分平台在完成直播和点播内容审核后，进行IPTV直播和点播内容加密。IPTV集成播控总分平台如需对加密内容进行再次审核，则内容审核系统应从证书中心申请内容审核专用客户端证书和私钥，配置密钥网关子系统URL和证书链等信息，从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规定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。

5　直播内容加密与授权

5.1　直播内容加密方法

直播内容加密应按照GY/T 277—2019中6.2的方法对直播内容基本码流进行加密，在基本码流的扩展数据中增加内容加密信息CEI，在传输流的PMT表中增加ChinaDRM描述子。CEI语法见GY/T 277—2019中的表1，ChinaDRM描述子见GY/T 277—2019中的表3，ChinaDRM描述子中的DRM_data_bytes应包含直播频道标识。

5.2 直播内容授权机制

直播加密应配置直播频道标识、直播加密模式、直播密钥更新频率、密钥管理URL等配置信息，按照配置的加密模式和密钥更新频率从密钥管理请求直播内容加密密钥进行直播内容加密，直播加密从密钥管理申请直播加密密钥的接口见GY/T 333—2020中的7.1.2。

密钥管理每次应将当前加密密钥、下一加密密钥发送给直播加密，并同步直播加密密钥到密钥网关，直播加密密钥同步到密钥网关的接口见GY/T 277—2019中的9.2。

当前内容加密密钥到期时，直播加密应切换到下一内容加密密钥，并从密钥管理申请新的内容加密密钥。

IPTV智能终端设备通过IPTV集成播控分平台认证鉴权系统从内容授权子系统申请直播内容授权许可证，内容授权子系统接收到直播内容授权许可证申请后从密钥网关子系统查询内容加密密钥，封装成内容授权许可证通过认证鉴权系统发送到IPTV智能终端设备。密钥网关子系统与内容授权子系统之间的密钥查询接口见GY/T 277—2019中的9.3。内容授权子系统与认证鉴权系统之间的许可证获取接口见GY/T 277—2019中的第8章。

IPTV智能终端设备根据内容授权许可证进行直播内容解密播放，在直播播放过程中发现CEI信息中发生密钥更新时，应检查本地是否存储有相应的内容加密密钥，如未发现本地有相应密钥，则启动新的直播内容授权许可申请。

6 点播内容加密与授权

6.1 点播内容加密方法

IPTV点播采用DASH分发内容时，MPD文件的规定见GY/T 277—2019中的6.3.2，内容加密应遵循GY/T 277—2019中6.3.3的规定。

IPTV点播采用ISO/IEC 23000-19分发内容时，内容加密应遵循GY/T 277—2019中6.3.3的规定，索引文件的规定见GY/T 277—2019中的6.3.2和6.3.4。

IPTV点播采用HLS分发内容时，内容加密封装采用TS文件格式，支持H.264、H.265、AVS+、AVS2等视频编码。内容加密可采用全加密模式或部分加密模式，内容加密算法应采用SM4算法，加密模式应采用CBC模式。加密内容的基本码流中包含CEI数据，CEI数据中包含内容加密密钥唯一标识和初始向量。M3U8文件中包含#EXT-X-KEY，其METHOD属性应为SM4-CBC或SAMPLE-SM4，VIDEOFORMAT应为实际的编码内容格式，URI中包含获取内容授权许可证的URL。

6.2 点播内容授权机制

点播内容管理对点播内容加密模式、加密内容唯一标识、加密内容URL等信息进行管理，通过向内容加密系统下达加密任务实现内容的加密，内容管理与点播内容加密子系统之间的接口见GY/T 333—2020中的6.3。

点播内容加密接收到内容加密任务后，从密钥管理申请点播内容加密密钥进行内容加密，内容加密完成后，通过点播内容分发系统进行分发。点播内容加密密钥申请接口见GY/T 333—2020中的7.2.2。

密钥管理按照GY/T 277—2019中9.2规定的密钥同步接口将内容加密密钥同步到IPTV集成播控分平台密钥网关，IPTV集成播控分平台内容授权在接收到IPTV智能终端点播内容授权许可证请求后，按照GY/T 277—2019中9.2规定的密钥查询接口从密钥网关查询内容加密密钥，封装成内容授权许可证发给IPTV智能终端，许可证获取接口见GY/T 277—2019中的第8章。

IPTV智能终端设备的DRM客户端通过内容授权许可证按照密钥使用规则进行内容的解密播放。

7 DRM客户端集成

7.1 DRM客户端集成机制

如IPTV智能终端具备可信硬件执行环境，应为其上安装的应用程序提供基于可信硬件执行环境的DRM客户端进行调用，应在出厂时烧写DRM客户端证书和私钥到设备可信硬件执行环境中。

如IPTV智能终端不具备可信硬件执行环境,应为其上安装的应用程序提供统一的基于软件安全执行环境的的DRM客户端进行调用,应置入DRM客户端证书和私钥到IPTV智能终端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）。

如IPTV智能终端不具备DRM客户端功能，视音频播放应用中应包含DRM客户端，该DRM客户端通常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。

7.2 IPTV智能终端播放流程

IPTV智能终端播放加密内容的流程如图2所示。

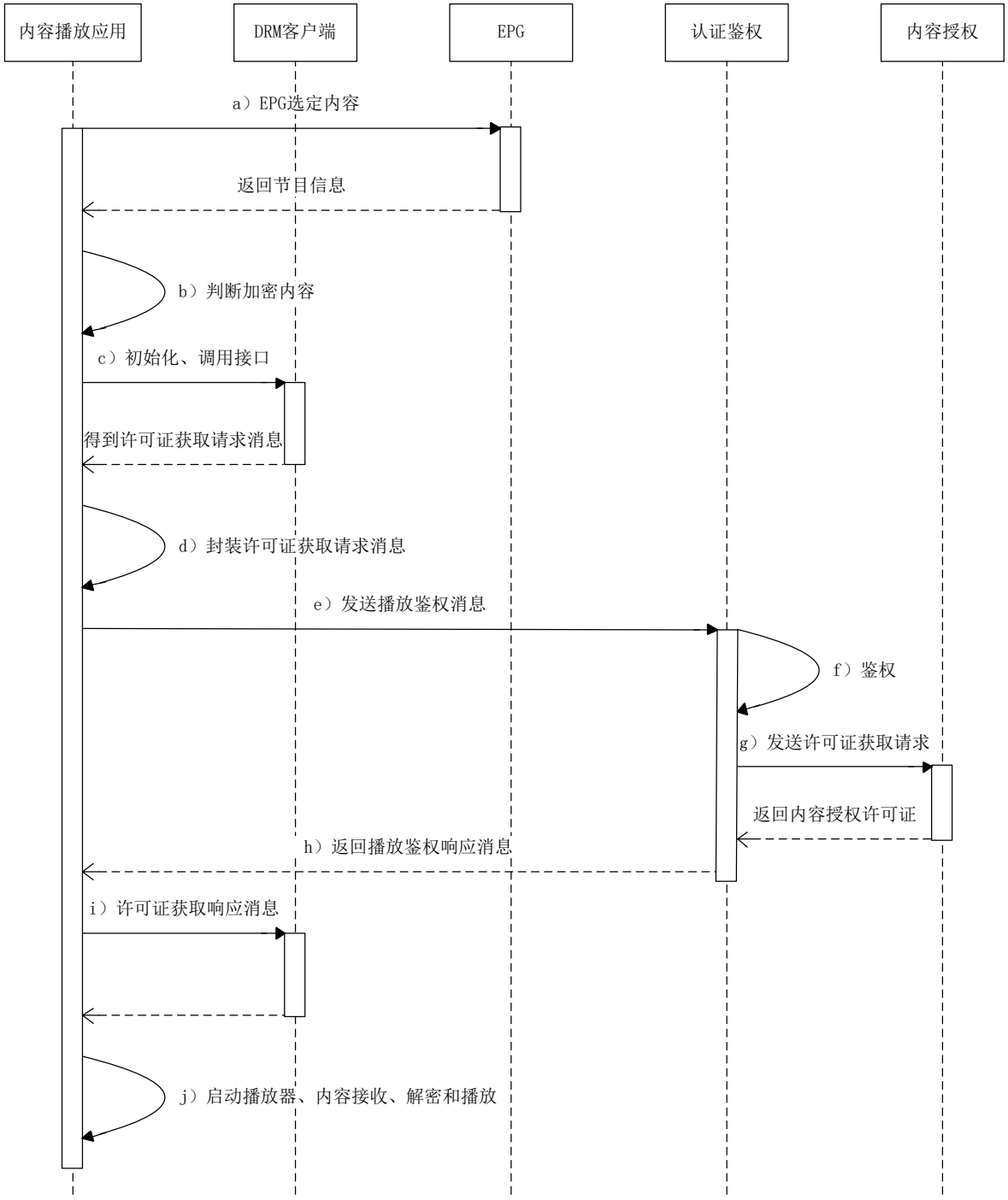

图2　IPTV 智能终端播放加密内容流程

IPTV智能终端播放加密内容的流程说明如下：

a)　内容播放应用通过 EPG 选定节目内容，获取节目信息；

b)　内容播放应用通过节目信息中的内容加密标识判断是否为加密内容；

c） 如判断为加密内容，则内容播放应用初始化 DRM 客户端，调用 DRM 客户端许可证获取请求消息接口，得到许可证获取请求消息；
d） 内容播放应用将许可证获取请求消息封装到播放鉴权消息中；
e） 内容播放应用将合并后的播放鉴权消息发送到 IPTV 认证鉴权系统；
f） 认证鉴权系统进行播放鉴权后，如果鉴权失败，则内容播放应用注销 DRM 客户端，退出播放；
g） 如果鉴权成功，则认证鉴权系统将许可证获取请求消息发送到内容授权系统申请内容授权许可证，内容授权系统接收到许可证获取请求消息后封装内容授权许可证返回给认证鉴权系统；
h） 认证鉴权系统合并授权许可证及鉴权结果信息返回给内容播放应用；
i） 内容播放应用将接收到的许可证获取响应消息传递给 DRM 客户端；
j） 如果 DRM 客户端接收内容授权响应消息成功，则启动播放器并调用 DRM 客户端进行解密，进行直播或点播内容的接收、解密和播放。