附件

视音频内容分发数字版权管理（DRM）技术应用实施指南（2023 版）

国家广播电视总局

2023 年 12 月

前　言

为贯彻落实党中央关于建设文化强国、知识产权强国的战略部署，鼓励广播电视和网络视听内容创作，保护内容服务提供者知识产权权益，创新服务模式，国家广播电视总局积极推进视音频内容版权保护工作，组织建立视音频内容分发数字版权管理（DRM，Digital Rights Management）标准体系，发布《视音频内容分发数字版权管理技术规范》（GY/T 277—2019）等6项行业标准，促进视音频内容分发数字版权管理系统标准化建设和规范化运行。

视音频内容分发数字版权管理涉及视音频内容提供、服务提供和终端播放等多个环节。目前，部分互联网电视、互联网视频服务、IPTV、有线数字电视等机构开展了视音频内容分发DRM技术标准应用部署，集成DRM功能的智能电视机、智能机顶盒、移动终端、车载娱乐设备等达1亿台以上，为DRM技术标准大规模产业化应用打下了基础。

为指导视音频内容提供与服务提供等环节行业机构、智能终端设备和芯片制造商、DRM技术提供商，加快DRM技术标准的应用实施，强化视听内容版权保护，特制定本实施指南。

指导单位：国家广播电视总局科技司。

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、上海海思技术有限公司、寰宇信任（北京）有限公司、华为技术有限公司、北京江南天安科技有限公司、北京数码视讯科技股份有限公司、广东南方新媒体股份有限公司、华数传媒网络股份有限公司、吉视传媒股份有限公司。

起草人：王磊、潘晓菲、梁志坚、沈阳、郑黎方、汪润华、赵云辉、刘利华、吴迪、陈志业、戴金晶、刘师蕾、张智军、宫铭豪、王荣、陈维玮。

目 录

1　范围

本实施指南适用于视音频内容分发数字版权管理的系统规划、设计、研发、生产、集成、建设和运行。

本实施指南为视音频内容提供方和服务提供方实现视音频内容的加密分发和安全授权，以及智能终端设备和芯片制造商集成研发符合行业标准的DRM客户端功能提供指导。

2　规范性引用文件

GB/T 32907—2016　信息安全技术　SM4分组密码算法（本文称：SM4标准）

GB/T 35276—2017　信息安全技术　SM2密码算法使用规范

GB/T 37092—2018　信息安全技术　密码模块安全要求

GB/T 39786—2021　信息安全技术　信息系统密码应用基本要求

GY/T 246—2020　视音频内容分发数字版权管理　IPTV数字版权管理系统集成

GY/T 257.1—2012　广播电视先进音视频编解码　第1部分：视频（本文称：AVS+标准）

GY/T 277—2019　视音频内容分发数字版权管理技术规范

GY/T 299.1—2016　高效音视频编码　第1部分：视频（本文称：AVS2标准）

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

GY/T 334—2020　视音频内容分发数字版权管理　互联网电视数字版权管理系统集成

GY/T 335—2020　视音频内容分发数字版权管理　标准符合性测试

GY/T 336—2020　视音频内容分发数字版权管理　系统合规性要求

GY/T 368—2023　先进高效视频编码（本文称：AVS3标准）

ISO/IEC 13818-1:2022　信息技术　运动图像及其伴音信息的通用编码　第1部分：系统（Information technology—Generic coding of moving pictures and associated audio information — Part 1: Systems）（本文称：TS）

ISO/IEC 14496-12:2022　信息技术　音视频对象编码　第12部分：ISO基础媒体文件格式（Information technology—Coding of audio-visual objects - Part 12: ISO base media file format）（本文称：ISO基础媒体文件格式）

ISO/IEC 23000-19:2020　信息技术　多媒体应用格式（MPEG-A）　第19部分：分段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）（本文称：CMAF）

ISO/IEC 23009-4:2018 信息技术 基于HTTP的动态自适应流媒体（DASH） 第4部分：分段加密与认证（Information technology - Dynamic adaptive streaming over HTTP (DASH)- Part 4:Segment encryption and authentication）（本文称：DASH）

3 概述

3.1 技术简介

视音频内容分发DRM技术以密码技术、PKI技术和授权技术为基础，实现视音频内容的加密分发和安全授权，只有可信的DRM客户端才能按照内容授权许可规则解密和播放内容，防止视音频内容在分发过程中被非法获取。

视音频内容分发DRM系统从逻辑上分为DRM服务端和DRM客户端两个部分，逻辑架构见图1。

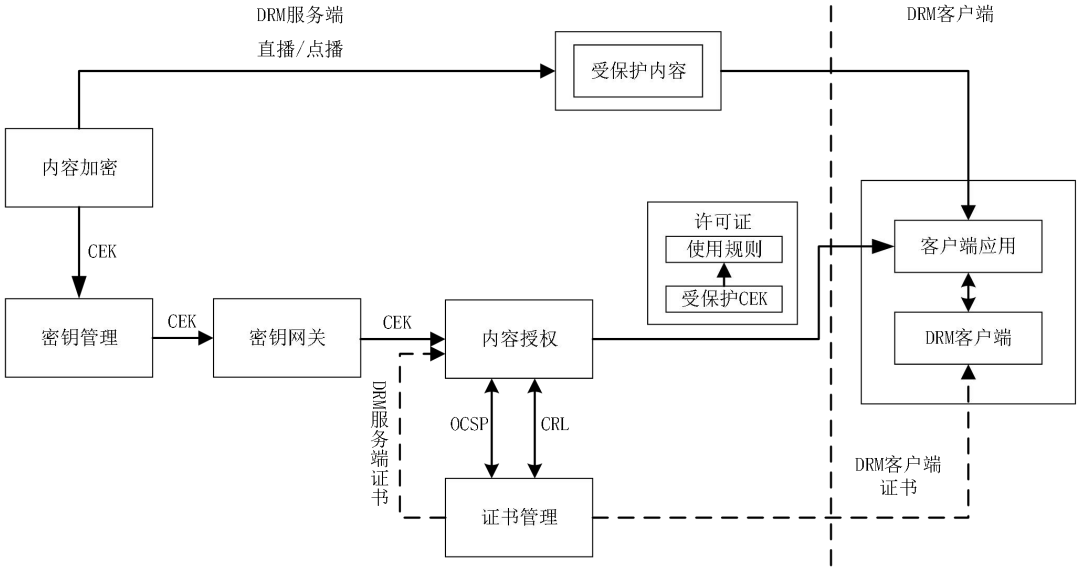


图 1 视音频内容分发 DRM 系统逻辑架构

DRM服务端包括内容加密、密钥管理、密钥网关、内容授权、证书管理等核心模块。内容加密模块负责对视音频内容进行加密保护；密钥管理模块负责管理内容加密密钥并将内容加密密钥同步给密钥网关；密钥网关模块安全存储从密钥管理模块接收到的内容加密密钥，并接收内容授权模块的密钥查询；内容授权模块接收DRM客户端的请求，从密钥网关模块查询内容加密密钥，将包含有内容加密密钥和密钥使用规则的内容授权许可证安全发送到可信的DRM客户端；证书管理模块负责为内容加密、密钥管理、密钥网关、内容授权等模块以及DRM客户端签发数字证书，建立图2所示的信任链，保障彼此之间的安全通信。

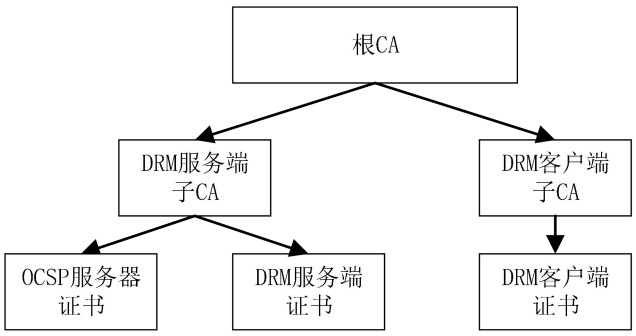


图 2　视音频内容分发 DRM 系统信任链

DRM客户端集成在视音频播放终端中（本文简称：终端，包括但不限于智能机顶盒、智能电视机、移动终端、个人电脑、车载娱乐系统、智能投影仪等）。视音频播放终端客户端应用在播放受保护内容时调用DRM客户端，从DRM服务端申请内容授权许可证，接收到内容授权许可证后，DRM客户端按照内容授权许可证规定的规则解密内容加密密钥，用内容加密密钥解密内容并进行播放。

3.2　标准体系

为规范视音频内容分发DRM技术应用部署，国家广播电视总局于2021年发布《视音频内容分发数字版权管理标准体系》（广电办发〔2021〕45号），其中6项标准已正式发布，视音频内容分发数字版权管理标准体系见图3。

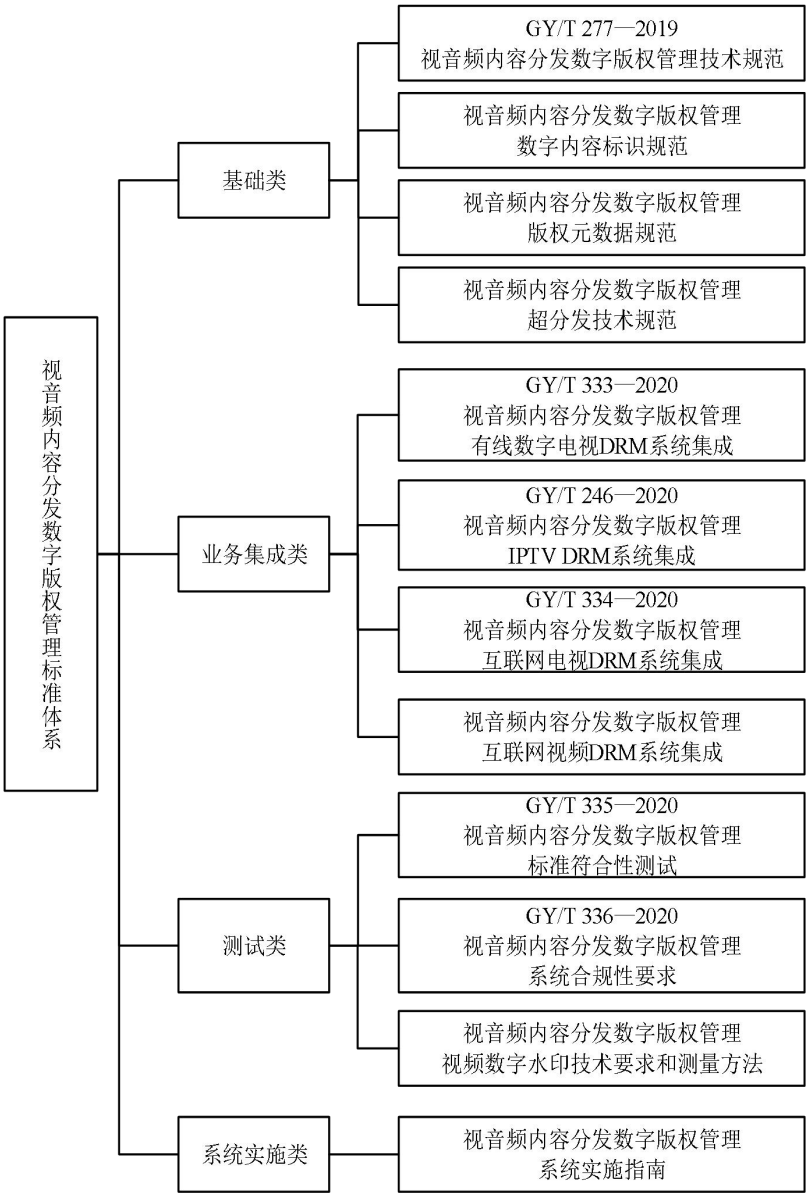


图 3　视音频内容分发数字版权管理标准体系

GY/T 277—2019规定了视音频内容分发数字版权管理的逻辑架构、技术机制、内容加密、许可证格式、许可证获取协议，以及DRM服务端和DRM客户端的相关技术要求。

GY/T 333—2020规定了有线数字电视DRM系统集成框架、内容加密、密钥管理、内容授权及终端集成等核心机制与接口协议。

GY/T 246—2020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。

GY/T 334—2020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。

GY/T 335—2020规定了GY/T 277—2019的符合性测试内容和测试方法。

GY/T 336—2020规定了视音频内容分发数字版权管理系统功能、性能、标准符合性测试要求，以及系统集成和运行维护的安全管理测评要求。

3.3　应用模式

视音频内容分发 DRM 技术支持服务提供方加密授权和内容提供方加密授权两种模式，实现频道播出和点播场景下的版权保护，具体实施应符合广播电视和网络视听行业相关管理规定。

3.3.1　服务提供方技术模式

服务提供方技术模式是指服务提供方以安全的方式接收频道播出和点播内容，并对内容进行加密；视音频播放终端从服务提供方获取频道播出和点播内容以及内容的授权。服务提供方技术模式见图4。

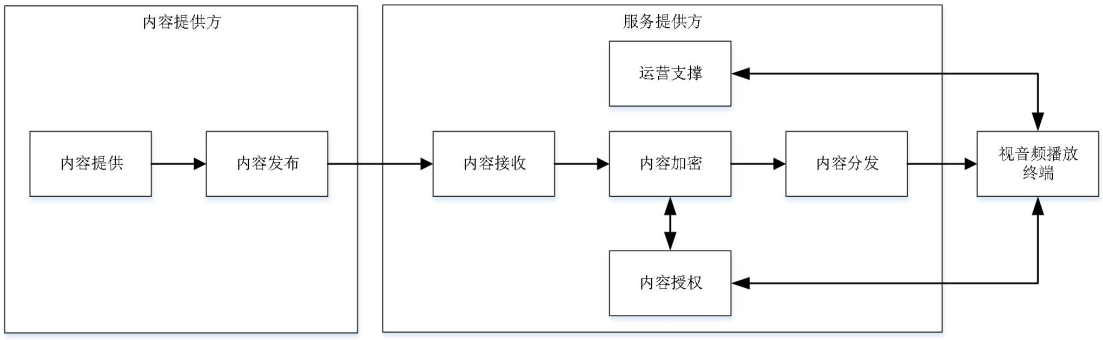


图 4　服务提供方技术模式

3.3.2　内容提供方技术模式

内容提供方技术模式是指内容提供方对频道播出和点播内容进行加密，视音频播放终端从服务提供方获取频道播出和点播内容，从内容提供方获取频道播出和点播内容的授权。内容提供方技术模式见图5。

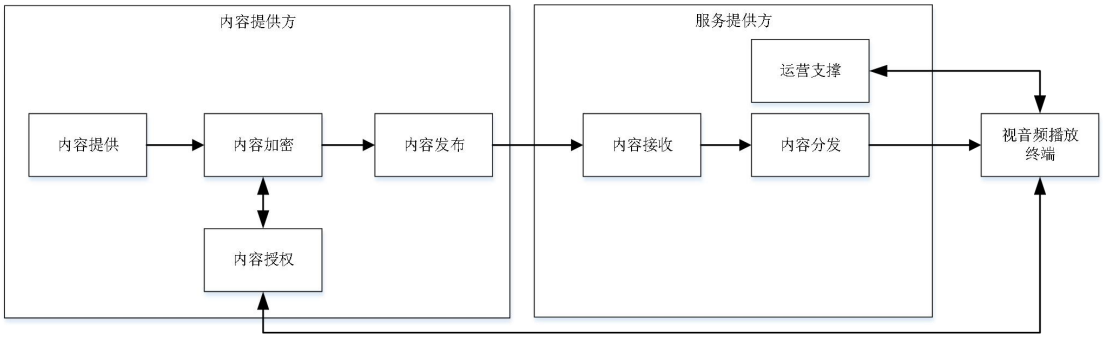


图 5　内容提供方技术模式

4　DRM 技术应用框架

4.1　总体框架

视音频内容分发DRM技术的应用部署需要视音频内容提供方、服务提供方、智能终端设备制造商、芯片制造商、DRM客户端软件开发包提供方、证书管理机构以及评估认证机构等的有机协同，总体框架见图6。

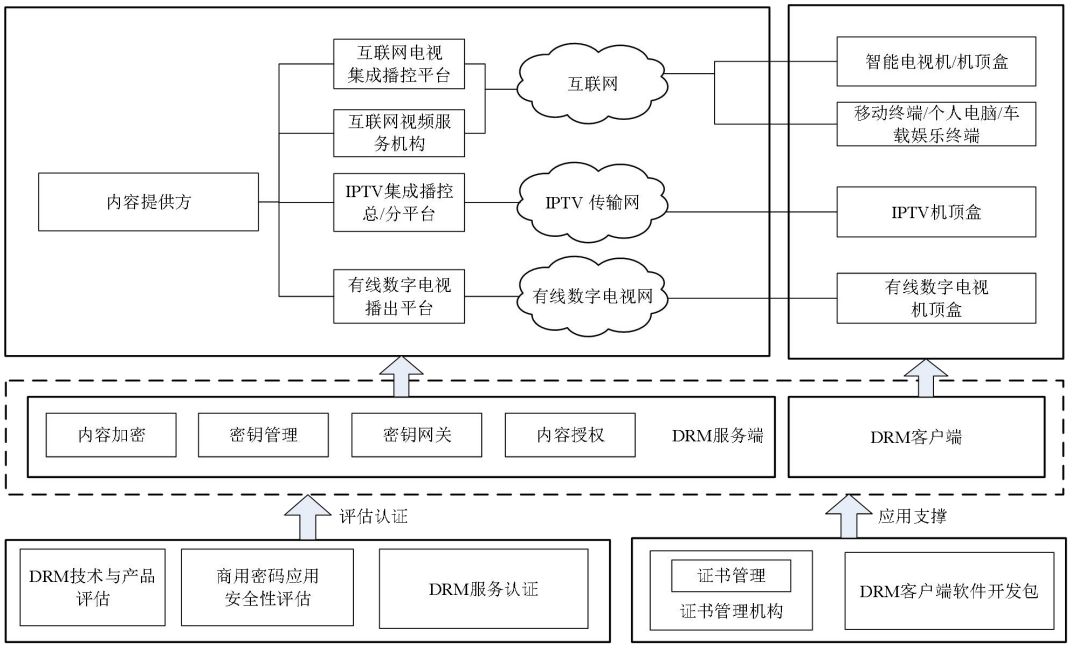


图 6　总体框架

4.2　DRM 服务端

DRM服务端的内容加密、密钥管理、密钥网关、内容授权等核心功能，部署在各级广播电视台等视音频内容提供方，以及互联网电视、互联网视频服务、IPTV、有线数字电视等视音频内容服务提供方，实现对频道播出和点播内容的加密授权。视音频内容提供方与服务提供方应协同开展内容加密、密钥管理、密钥网关、内容授权等DRM服务端功能的集成部署，以支持不同的技术应用模式。

4.2.1　内容加密

视音频内容分发DRM技术支持对AVS+、AVS2、AVS3等标准视频编码格式编码内容的加密，支持采用TS、HLS、DASH、CMAF等视音频内容封装格式进行加密内容封装传输，以实现频道播出和点播内容的加密保护，内容加密技术要求见表1。

表 1　内容加密技术要求

应用场景	格式	格式规范	加密方法
频道播出	TS	PMT 表中应包含 ChinaDRM 描述子，描述子中 video_format 使用 0101b（0x05）表示 AVS3 编码；在基本码流的扩展数据中增加内容加密信息（Content Encryption Information，CEI，语	对基本码流的每帧编码数据进行加密，内容加密采用 SM4 加密算

应用场景	格式	格式规范	加密方法
		法格式见 GY/T 277—2019 表 1）。	法，具体规定见 GY/T 277—2019 第 6 章。
视频点播	HLS	m3u8 文件的#EXT-X-KEY 字段描述加密的基本信息，其中 KEYFORMAT 固定为“urn:uuid:3d5e6d35-9b9a-41e8-b843-dd3c6e72c42c”，其他要求见 A.1。TS 切片加密方法与频道播出的 TS 加密方法一致。	
	DASH	MPD 文件中包含 ContentProtection 字段，描述加密的基本信息，其中 cenc:pssh 中 ContentProtection 的 schemeIdUri 属性定义为“3d5e6d35-9b9a-41e8-b843-dd3c6e72c42c”，其他要求见 A.2。	切片采用 SM4 算法加密，具体规定见 GY/T 277—2019 第 6 章。
	CMAF	m3u8 文件的#EXT-X-KEY 字段描述加密的基本信息，其中 KEYFORMAT 固定为“urn:uuid:3d5e6d35-9b9a-41e8-b843-dd3c6e72c42c”，其他要求见 A.3。	
	TS 文件	PMT 表中应包含 ChinaDRM 描述子，描述子中 video_format 使用 0101b（0x05）表示 AVS3 编码；在基本码流的扩展数据中增加内容加密信息。	对基本码流的每帧编码数据进行加密，内容加密采用 SM4 加密算法，具体规定见 GY/T 277—2019 第 6 章。
	ISO 基础媒体文件	基于 ISO 23001-7:2016 对视音频内容加密，对 TrackEncryptionBox、SampleGroupDescriptionBox 的规定见 A.2。在 PSSH 将 SystemID 设置为“3d5e6d35-9b9a-41e8-b843-dd3c6e72c42c”，格式见表 A.1。	具体规定见 GY/T 277—2019 6.3.3 节。

频道播出内容加密功能要求如下：

（1）支持实时 TS、HLS、DASH、CMAF 等频道播出内容封装中的一种或多种；

（2）支持 AVS+、AVS2、AVS3 等视频编码格式；

（3）支持通过密钥管理申请频道内容加密密钥，内容加密密钥申请应符合 GY/T 333—2020 中 7.1 节的规定；

（4）加密延时应不高于 500ms；

（5）支持内容加密密钥按照可配置的频率更新，至少支持秒级密钥更新频率；

（6）内容加密应符合 GY/T 333—2020 6.1.1 和 6.2 节的规定；

（7）内容加密后的编码数据应避免出现 00 00 00、00 00 01、00 00 02、00 00 03。可通过变换初始向量的方式避免起始码二义冲突，同时将 GY/T 277—2019 中表 1 规定的内容加密信息的第 3 个比特（从 0 比特开始计算）置为 1，表示码流中不含二义转换的编码数据；

（8）内容加密公私钥对在硬件密码模块中生成，私钥安全存储在硬件密码模块中；

（9）加解密、签名等密码运算功能在硬件密码模块中实现；

（10）内容加密私钥、内容加密密钥、会话密钥、临时密钥等不将明文暴露在硬件密码模块之外；

（11）硬件密码模块应符合 GB/T 37092—2018 规定的二级或更高安全级别，且具备商用密码产品认证证书；

（12）具备硬件密码模块识别机制，硬件密码模块移除时停止服务；

（13）具备软件组件完整性校验机制，软件组件被篡改后停止服务；

（14）支持安全日志记录和日志审查，任何操作包括软件升级、软件组件修改、非法篡改、硬件密码模块移除等安全记录；

（15）具备安全升级机制，在出现新的安全风险或安全漏洞时能及时进行安全修复。

点播内容加密功能要求如下：

（1）支持TS、HLS、DASH、CMAF等点播内容封装中的一种或多种；

（2）支持AVS+、AVS2、AVS3等视频编码格式，点播内容加密密钥申请应符合GY/T 333—2020中7.2的规定；

（3）支持通过密钥管理申请内容加密密钥；

（4）点播内容加密应符合GY/T 333—2020中6.1.2和6.2的规定；

（5）点播内容加密任务管理应符合GY/T 333—2020中6.3的规定；

（6）内容加密后的编码数据应避免出现00 00 00、00 00 01、00 00 02、00 00 03。可通过变换初始向量的方式避免起始码二义冲突，同时将GY/T 277—2019中表1规定的内容加密信息的第3个比特（从0比特开始计算）置为1，表示码流中不含二义转换的编码数据；

（7）点播内容加密的公私钥对在硬件密码模块中生成，私钥安全存储在硬件密码模块中；

（8）加解密、签名等密码运算功能在硬件密码模块中实现；

（9）点播内容加密私钥、内容加密密钥、会话密钥、临时密钥等不将明文暴露在硬件密码模块之外；

（10）硬件密码模块应符合GB/T 37092—2018规定的二级或更高安全级别，且具备商用密码产品认证证书；

（11）具备硬件密码模块识别机制，硬件密码模块移除时停止服务；

（12）具备软件组件完整性校验机制，软件组件被篡改后停止服务；

（13）支持安全日志记录和日志审查，任何操作包括软件升级、软件组件修改、非法篡改、硬件密码模块移除等安全记录；

（14）具备安全升级机制，在出现新的安全风险或安全漏洞时能及时进行安全修复。

4.2.2 密钥管理

密钥管理功能要求如下：

（1）支持接收处理内容加密密钥申请；

（2）支持安全存储管理内容加密密钥；

（3）支持同步内容加密密钥到密钥网关；

（4）频道播出内容加密密钥管理应符合 GY/T 333—2020 中 7.1 的规定；

（5）点播内容加密密钥管理应符合 GY/T 333—2020 中 7.2 的规定；

（6）密钥管理的公私钥对在硬件密码模块中生成和运算，私钥安全存储；

（7）加解密、签名等密码运算功能在硬件密码模块中实现；

（8）密钥管理组件私钥、内容加密密钥、会话密钥、临时密钥等不将明文暴露在硬件密码模块之外；

（9）具备内容加密密钥库，实现内容加密密钥的安全存储、备份和导入/导出；

（10）硬件密码模块应符合 GB/T 37092—2018 规定的二级或更高安全级别，且具备商用密码产品认证证书；

（11）具备硬件密码模块识别机制，硬件密码模块移除时停止服务；

（12）具备软件组件完整性校验机制，软件组件被篡改后停止服务；

（13）支持安全日志记录和日志审查，任何操作包括软件升级、软件组件修改、非法篡改、硬件密码模块移除等安全记录；

（14）具备安全升级机制，在出现新的安全风险或安全漏洞时能及时进行安全修复。

4.2.3 密钥网关

密钥网关功能要求如下：

（1）支持接收处理密钥管理模块的内容加密密钥请求；

（2）支持安全存储管理内容加密密钥；

（3）支持接收处理内容授权发出的内容加密密钥请求；

（4）密钥同步应符合 GY/T 277—2019 中 9.2 的规定；

（5）密钥查询应符合 GY/T 277—2019 中 9.3 的规定；

（6）密钥网关的公私钥对在硬件密码模块中生成和运算，私钥安全存储；

（7）加解密、签名等密码运算功能在硬件密码模块中实现；

（8）密钥网关私钥、内容加密密钥、会话密钥、临时密钥等不将明文暴露在硬件密码模块之外；

（9）具备内容加密密钥库，实现内容加密密钥的安全存储、备份和导入/导出；

（10）硬件密码模块应符合 GB/T 37092—2018 规定的二级或更高安全级别，且具备商用密码产品认证证书；

（11）具备硬件密码模块识别机制，硬件密码模块移除时停止服务；

（12）具备软件组件完整性校验机制，软件组件被篡改后停止服务；

（13）支持安全日志记录和日志审查，任何操作包括软件升级、软件组件修改、非法篡改、硬件密码模块移除等安全记录；

（14）具备安全升级机制，在出现新的安全风险或安全漏洞时能及时进行安全修复。

4.2.4 内容授权

内容授权功能要求如下：

（1）支持接收处理 DRM 客户端发出的内容授权许可证请求；

（2）支持从密钥网关请求内容加密密钥；

（3）内容授权许可证请求/响应应符合 GY/T 277—2019 中第 8 章的规定；

（4）密钥查询应符合 GY/T 277—2019 中 9.3 的规定；

（5）内容授权的公私钥对在硬件密码模块中生成和运算，私钥安全存储；

（6）加解密、签名等密码运算功能在硬件密码模块中实现；

（7）内容授权的私钥、内容加密密钥、会话密钥、临时密钥等不将明文暴露在硬件密码模块之外；

（8）硬件密码模块应符合 GB/T 37092—2018 规定的二级或更高安全级别，且具备商用密码产品认证证书；

（9）具备硬件密码模块识别机制，硬件密码模块移除时停止服务；

（10）具备软件组件完整性校验机制，软件组件被篡改后停止服务；

（11）支持安全日志记录和日志审查任何操作包括软件升级、软件组件修改、非法篡改、硬件密码模块移除等安全记录；

（12）具备安全升级机制，在出现新的安全风险或安全漏洞时能及时进行安全修复。

4.3 DRM 客户端

DRM 客户端集成在视音频播放终端中，负责接收 DRM 服务端发送的内容授权许可消息，按照内容授权许可消息中规定的播放规则解密内容，确保视音频内容在解码、解密、播放过程中的安全。DRM 客户端应符合 GY/T 336—2020 第 7 章规定的 DRM 客户端合规性要求。

DRM 客户端安全等级按照由低到高的顺序分为软件安全级别、硬件安全级别、增强硬件安全级别三个安全等级，各安全等级 DRM 客户端的安全要求见表 2，详细的 DRM 客户端安全要求见 GY/T 336—2020 7.3 节。

表 2 DRM 客户端安全等级要求

序号	DRM 客户端安全等级	安全要求
1	软件安全级别	部分或全部 DRM 客户端运行环境基于软件安全机制实现。
2	硬件安全级别	DRM 客户端运行环境全部基于硬件安全机制实现。
3	增强硬件安全级别	在硬件安全级别的基础上，DRM 客户端安全运行环境应具备侧信道攻击防御、取证水印等功能。

一般情况下，按照DRM客户端安全等级进行视音频内容的分级授权，DRM客户端安全等级越高可解密播放视音频内容的质量或商业价值越高，4K及以上内容一般只授权给增强硬件安全级别DRM客户端解密播放，1080P内容授权给硬件安全级别以上的DRM客户端解密播放，软件安全级别DRM客户端只能解密播放720P及以下的内容。

4.4 评估认证

评估认证是视音频内容分发 DRM 技术在研发生产、规划设计、集成部署、运行维护等环节标准化规范化的重要保障，包括：DRM 技术与产品安全评估、商用密码应用安全性评估，以及 DRM 服务认证。

DRM 技术与产品安全评估依据 GY/T 335—2020、GY/T 336—2020 进行，为 DRM 系统建设提供符合要求的产品目录。

商用密码应用安全性评估依照国家关于商用密码应用法律法规相关要求进行，用于确保各机构集成部署的 DRM 系统正确、合规、有效地实施密码应用。

DRM 服务认证按照国家服务认证相关要求、认证认可标准以及视音频内容分发 DRM 技术标准进行。

4.5 应用支撑

证书管理应符合 GY/T 277-2019 的规定，由第三方证书管理机构建设并运行，提供 DRM 服务端证书签发、DRM 客户端密钥生成和证书签发服务。

DRM 客户端应符合 GY/T 336-2020 的规定，“数字媒体内容保护技术研究国家广播电视总局重点实验室”以免费许可的方式为行业提供 DRM 客户端软件开发包。

5 DRM 技术实施流程

视音频内容分发 DRM 系统实施过程包括：规划设计、系统集成、系统验收、运行维护等。

5.1 规划设计

按照 GY/T 277—2019、GY/T 333—2020、GY/T 246—2020、GY/T 334—2020、GY/T 335—2020、GY/T 336—2020 等标准进行视音频内容分发 DRM 系统规划设计；根据版权方要求和版权内容运营业务规划，确定拟覆盖的视音频播放终端设备范围和 DRM 客户端安全等级，参照 5.1.1 和 5.1.2 设计视音频内容分发 DRM 系统方案。

5.1.1 DRM 服务端集成

DRM 服务端集成方式分为独立部署、云服务集成部署等。

独立部署是指拟建设 DRM 系统的机构在其运营系统内部部署内容加密、密钥管理、密钥网关、内容授权等 DRM 服务端核心功能，由第三方证书管理机构签发 DRM 服务端数字证书，以确保建立完备的 DRM 端到端信任管理机制。

云服务集成部署是指以云服务方式提供内容加密、密钥管理、密钥网关、内容授权等DRM服务端核心功能，拟使用DRM系统的机构以购买服务的方式实现视音频内容分发DRM相关功能与其运营系统的集成；在该模式下，拟使用DRM系统的机构在购买服务的同时，将第三方证书管理机构签发的DRM服务端数字证书托管到其购买的DRM服务端云服务中，以确保建立完备的DRM端到端信任管理机制。云服务集成部署要求见附录C。

为确保视音频内容分发DRM系统持续、稳定运行，内容加密、密钥管理、密钥网关、内容授权等核心DRM服务端功能应采用双机热备、负载均衡或云服务等方式部署。为保障播出安全，在频道播出场景下，频道播出内容加密、密钥管理、内容授权等模块应具备应急处置机制，以确保DRM技术保护的频道播出安全，频道播出DRM技术应用应急技术要求见表3。

表3 频道播出DRM技术应用应急技术要求

DRM技术环节	技术要求
频道内容加密	应在紧急情况下切换清流模式。
密钥管理	可在紧急情况下设置不同的内容加密密钥更新频率。
内容授权	应能够生成具有有效期的、支持在DRM客户端缓存的内容授权许可证。
DRM客户端	应具备在本地存储频道授权许可证的能力；支持首次开机获取携带有应急授权许可证的内容授权许可证响应消息。

此外，DRM系统建设和运行维护机构在做好日常运行维护、定期评估和认证监督的前提下，还应结合以上部署要求和应急机制制定并完善应急处置预案。

5.1.2 DRM客户端集成

根据DRM客户端所在终端设备的能力，DRM客户端集成方式分为硬件可信执行环境内置、操作系统内置、应用内置等。不同集成方式下，DRM客户端密钥的预置模式不同。

（1）硬件可信执行环境内置方式

在终端设备具备硬件可信执行环境的情况下，由终端设备的硬件可信执行环境提供符合GY/T 277—2019要求的DRM客户端运行环境，并在其中集成DRM客户端功能。终端设备上的应用软件通过操作系统媒体框架调用DRM客户端功能。

该方式下，DRM客户端密钥和证书一般在终端设备产线预置，也可基于终端设备硬件可信执行环境提供的硬件安全能力在线置入。

（2）操作系统内置方式

在终端设备不具备硬件可信执行环境的情况下，通常采用白盒密码等技术实现符合GY/T 277—2019要求的软件安全级别DRM客户端运行环境，并在其中集成DRM客户端功能。应用软件通过操作系统的媒体框架调用DRM客户端功能。

该方式下，DRM客户端密钥和证书一般在终端设备产线预置，也可基于终端设备操作系统提供的安全能力在线置入。

（3）应用内置方式

在终端设备不提供DRM客户端功能的情况下，一般在应用程序内部集成独立的DRM客户端功能。在该方式下，通常采用白盒密码等技术实现符合GY/T 277—2019要求的软件安全级别DRM客户端运行环境，并在其中集成DRM客户端功能。DRM客户端功能仅供当前应用软件使用。

该方式下，如果应用为终端出厂预置，建议在终端设备出厂前在产线预置DRM客户端密钥和证书；其他情况下，采用在线分发的方式进行预置。

针对市场上已经部署的存量终端，应根据终端能力按照硬件可信执行环境内置、操作系统内置、应用内置的优先级顺序选择升级方式。市场存量终端升级后，采用在线分发的方式预置DRM客户端密钥和证书。

5.2 系统集成

DRM系统建设方根据其视音频内容分发数字版权管理系统规划设计，组织开展DRM服务端研发或招标采购、DRM客户端集成调试、DRM服务端安装部署以及端到端系统联调。

DRM客户端集成调试包括终端设备上的DRM客户端功能集成调试、应用程序调用DRM客户端的集成调试。终端设备上的DRM客户端功能集成调试是指在终端设备中集成DRM客户端功能，通常由终端芯片制造商、操作系统提供商、终端制造商共同完成。应用程序调用DRM客户端的集成调试是指在终端设备中实现视音频内容播放应用程序对DRM客户端功能的调用，通常由视音频内容播放应用程序开发商完成，必要时需由终端设备操作系统提供商配合提供必要的技术支持。

在该阶段，DRM系统建设方部署DRM服务端数字证书；终端设备制造商通过产线预置或在线分发方式在终端设备中预置DRM客户端密钥和DRM客户端数字证书；在5.1.2给出的应用内置方式中，视音频内容播放应用程序提供方通过在线分发方式在视音频内容播放应用程序中的DRM客户端预置DRM客户端密钥和DRM客户端数字证书，确保DRM客户端与DRM服务端互信。

5.3 系统验收

DRM系统建设方完成视音频内容分发DRM系统集成建设后，按照GY/T 335—2020、GY/T 336—2020的要求进行系统上线前的标准符合性测试和系统合规性评估，包括：DRM服务端功能和标准符合性评估、DRM客户端功能和标准符合性评估，确保上线系统正确、合规、有效。

DRM系统试运行后，DRM系统建设方可通过DRM服务认证持续提升视音频内容数字版权管理能力。

5.4 运行维护

DRM系统建设方应制定视音频内容分发DRM系统运行维护方案、应急处置预案等，确保

上线后的 DRM 系统持续有效运行。

6　互联网电视 DRM 技术应用

6.1　技术应用框架

互联网电视内容服务平台和集成服务平台应按照 GY/T 334—2020 等标准，建设部署 DRM 系统，通过互联网电视内容服务平台与集成服务平台的协同合作，部署符合 GY/T 277—2019 规定的内容加密、密钥管理、密钥网关等 DRM 服务端核心功能，实现高质量视听内容的全链条保护。互联网电视数字版权管理系统集成框架见图 7。

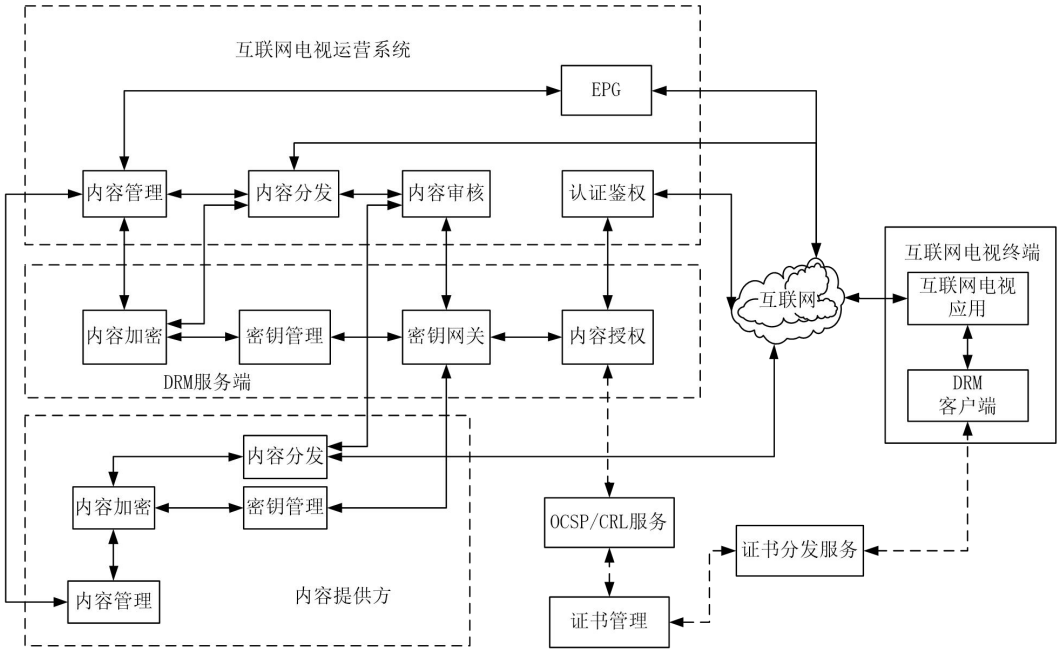


图 7 互联网电视数字版权管理系统集成框架

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，由内容授权将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，内容授权负责客户端安全等级要求、输出保护要求等版权方要求的使用规则，内容授权将所有规则以密钥使用规则的方式封装到内容授权许可证中。

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。

6.2 技术应用要求

互联网电视内容分发各环节 DRM 技术应用要求见表 4。

表 4 互联网电视 DRM 技术应用要求

内容分发环节	基本要求	标准规范
互联网电视内容服务平台	应部署内容加密、密钥管理功能；支持向互联网电视集成服务平台的密钥网关同步内容加密密钥。	GY/T 277—2019 GY/T 334—2020 GY/T 335—2020 GY/T 336—2020
互联网电视集成服务平台	应部署内容加密、密钥管理、密钥网关、内容授权功能；应支持从互联网电视内容服务平台接收内容加密密钥。	
传输网络	CDN 网络应保留 TS 封装格式 PMT 表中的 ChinaDRM 描述子，m3u8、MPD 等索引文件中的 DRM 信息。	
互联网电视终端	具备硬件可信执行环境的，应在硬件可信执行环境中集成 DRM 客户端；不具备硬件可信执行环境的，应在操作系统中集成软件安全级别 DRM 客户端。	

7 互联网视频 DRM 技术应用

互联网/移动互联网视听节目服务机构建设的互联网视频 DRM 系统应符合 GY/T 277—2019 的规定，包括内容加密、密钥管理、内容授权以及 DRM 客户端等核心功能。

互联网/移动互联网视听节目服务DRM技术应用要求见表5。

表 5 互联网/移动互联网视听节目服务 DRM 技术应用要求

内容分发环节	基本要求	标准规范
互联网/移动互联网视听节目服务系统	应部署内容加密、密钥管理、内容授权功能；可通过部署密钥网关功能支持基于 DRM 技术的创新服务，如点播分账等。	GY/T 277—2019 GY/T 335—2020 GY/T 336—2020
传输网络	CDN 网络应保留 TS 封装格式 PMT 表中的 ChinaDRM 描述子，m3u8、MPD 等索引文件中的 DRM 信息。	
互联网/移动互联网视听节目播放终端	具备硬件可信执行环境的，应在硬件可信执行环境中集成 DRM 客户端；不具备硬件可信执行环境的，应在操作系统中集成软件安全级别 DRM 客户端。	
互联网/移动互联网视听节目服务应用	应优先采用互联网视频终端设备内置的硬件安全级别以上 DRM 客户端；在未内置 DRM 客户端的设备中应在应用程序中集成软件安全级别 DRM 客户端。	

各级融媒体平台可参照互联网/移动互联网视听节目服务 DRM 技术应用方式，开展视听内容版权保护，采用 DRM 技术开展创新业务。

8 IPTV DRM 技术应用

8.1 技术应用框架

IPTV DRM 系统应符合 GY/T 277—2019、GY/T 246—2020 的规定，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 系统集成框架见图 8。

注 1：本文中的“直播”是指频道播出。

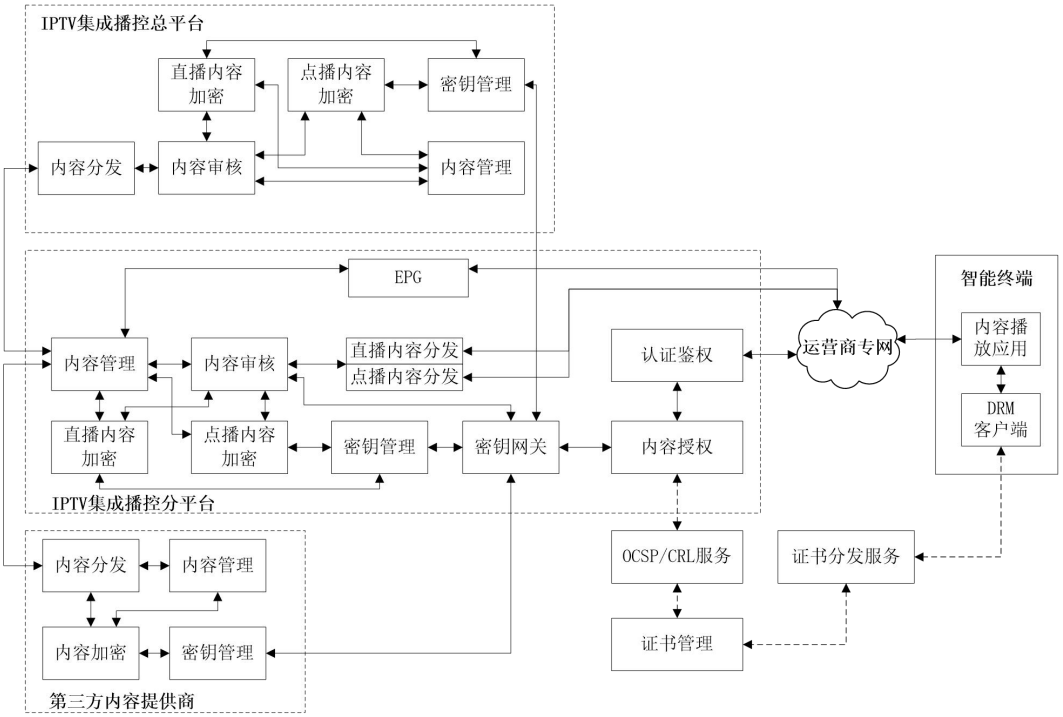


图 8 IPTV DRM 系统集成框架

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第三方证书管理机构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。

直播 DRM 系统设计见附录 B。

8.2 技术应用要求

IPTV内容分发DRM技术应用要求见表6。

表 6 IPTV DRM 技术应用要求

内容分发环节	基本要求	标准规范
IPTV 集成播控总平台	应部署内容加密、密钥管理功能；支持向 IPTV 集成播控分平台的密钥网关同步内容加密密钥。	GY/T 277—2019 GY/T 246—2020 GY/T 335—2020 GY/T 336—2020
IPTV 集成播控分平台	应部署内容加密、密钥管理、密钥网关、内容授权功能；应支持从 IPTV 集成播控总平台接收内容加密密钥。	
IPTV 传输网络	CDN 网络应保留 TS 封装格式 PMT 表中的 ChinaDRM 描述子。	
IPTV 智能机顶盒	应具备硬件可信执行环境，应在硬件可信执行环境中集成 DRM 客户端。	

IPTV 集成播控总、分平台应加强 DRM 技术在超高清频道和高质量视听内容点播服务方面的应用，支持在具备硬件以上安全级别 DRM 客户端功能的 IPTV 机顶盒播出超高清视听内容，逐步提升 IPTV 超高清内容保护力度。支持 IPTV 集成播控总、分平台采用密钥网关等 DRM 技术功能实现中央和省级节目的加密授权，创新 DRM 技术应用模式。IPTV 传输服务机构应加强 CDN 网络升级改造，支持采用 DRM 技术加密保护的 IPTV 直播和点播内容传输分发；加快研发生产和部署具备硬件安全级别以上 DRM 客户端功能的 IPTV 机顶盒。

9 有线数字电视 DRM 技术应用

9.1 技术应用框架

有线数字电视 DRM 系统用于保护双向有线数字电视直播和点播内容版权，确保数字电视内容通过双向有线网络分发到终端播放、输出全流程的安全。有线数字电视 DRM 系统应符合 GY/T 277—2019、GY/T 333—2020 的规定。DRM 服务端包括：直播加密、点播加密、直播密钥管理、点播密钥管理、密钥网关、内容授权等核心子系统，通过直播加密、点播加密、内容授权与有线数字电视运营系统的协同实现有线数字电视 DRM 系统的服务端集成，直播加密后的直播内容通过直播内容分发发送到机顶盒等智能终端，点播加密后的内容通过点播内容分发发送到机顶盒等智能终端，通过在机顶盒等终端中集成 DRM 客户端功能，实现双向有线数字电视直播和点播内容版权的端到端保护。有线数字电视 DRM 系统集成框架见图 9。

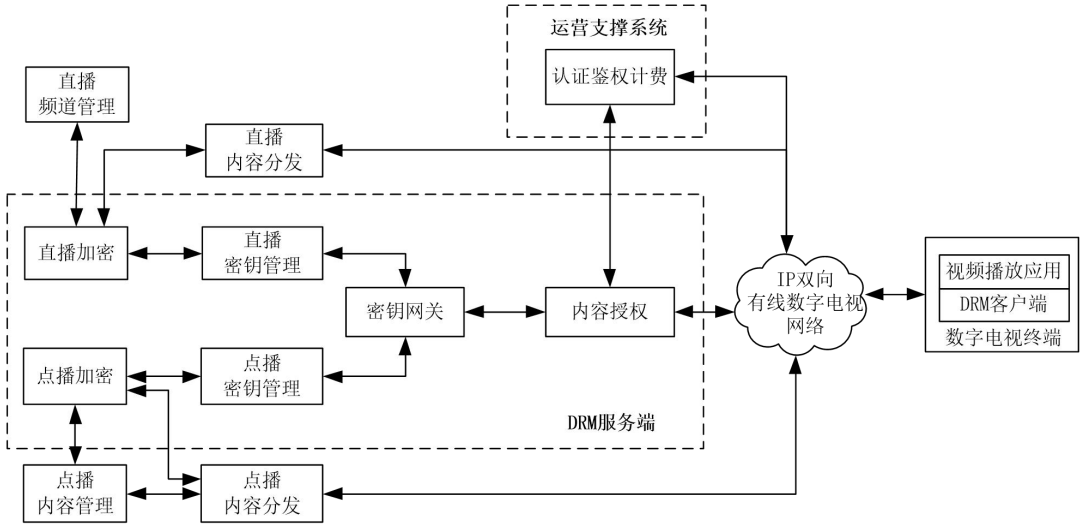


图 9 有线数字电视 DRM 系统集成框架

直播加密和点播加密从对应的直播密钥管理和点播密钥管理请求内容加密密钥进行内容加密；直播密钥管理和点播密钥管理将内容加密密钥同步到密钥网关；密钥网关为内容授权提供全部直播频道和点播内容的内容加密密钥查询。

终端视频播放应用调用 DRM 客户端生成内容授权许可证请求，从内容授权申请内容授权许可证，根据获得的内容授权许可证进行内容的解密播放。

运营系统的频道管理实现对直播加密的配置，点播内容管理实现对点播加密的配置。内容授权接收到内容授权申请时，从运营系统查询该申请的认证鉴权计费结果，依据认证鉴权计费返回的结果判断是否生成内容授权许可证给终端。

在采用广播方式进行数字电视传输流分发且具备 IP 通信链路的场景下，直播 DRM 系统设计见附录 B。

9.2 技术应用要求

有线数字电视 DRM 技术应用要求见表 7。

表 7 有线数字电视 DRM 技术应用要求

内容分发环节	基本功能要求	标准规范
频道播出	应在直播编码环节增加内容加密功能以支持频道节目加密播出；应部署密钥网关功能，支持从频道播出方接收频道节目加密密钥。	GY/T 277—2019 GY/T 333—2020 GY/T 335—2020 GY/T 336—2020
点播服务	应部署点播内容加密和密钥管理功能，支持点播内容加密；应部署密钥网关功能，支持第三方加密内容接入。	
传输网络	双向分发网络应保留 PMT 表中的 ChinaDRM 描述子。	

内容分发环节	基本功能要求	标准规范
双向有线数字电视智能机顶盒	应具备硬件可信执行环境的，应在硬件可信执行环境中集成 DRM 客户端。	

具备双向化传输分发能力的有线数字电视运营机构应按照GY/T 333—2020等行业标准，实现对超高清频道的版权保护，加快研发生产和部署具备硬件安全级别以上 DRM 客户端功能的智能机顶盒等有线数字电视终端。

附录 A 视音频内容加密封装

A.1 基于 HLS 的视音频内容加密封装

采用 HLS 协议的视音频内容点播 DRM 系统按照 GY/T 277—2019 6.2 节的规定对数字电视传输流基本码流进行加密，加密媒体分块的内容加密密钥信息通过 m3u8 文件中#EXT-X-KEY 的 URI 属性指定。

#EXT-X-KEY 的 URI 属性定义了获取许可证的 URI 字符串和内容保护信息，格式为：“data:text/plain;base64”；其中 base64 字符串部分包含了表 A.1 定义的 PSSH 数据。

表 A.1 PSSH 定义

字段	长度 bit	类型	描述
Size	32	uimsbf	PSSH 长度
Type	32	uimsbf	0x70 73 73 68
Version	8	uimsbf	0x00 或 0x01
Flags	24	uimsbf	0x00 00 00
SystemId	128	uimsbf	0x3d5e6d359b9a41e8b843dd3c6e72c42c
KID_Count	32	uimsbf	可选
KID	KID_Count×16×8	uimsbf	可选
DataSize	32	uimsbf	数据长度
Data	DataSize×8	uimsbf	数据

Size：包含 Size 字段在内的 PSSH 长度。

Type：类型，即“pssh”。

Version：Version 为 0 时 PSSH 中不包含 KID_Count 和 KID，Version 为 1 时 PSSH 中包含 KID_Count 和 KID。

Flags：固定为 0。

SystemId：固定为“0x3d5e6d359b9a41e8b843dd3c6e72c42c”。

KID_Count：密钥标识数量。

KID：密钥标识。

DataSize：数据长度，单位为字节。

Data：内容保护描述信息，包括：版本、内容标识、密钥标识、加密方式等信息，采用 JSON编码格式封装，定义应符合表A.2的规定。

表 A.2 内容保护描述信息定义

JSON 键	值类型	规定
version	string	必选
contentID	string	必选
kids	string 数组	必选
enschema	string	必选
playIndex	integer	可选
drmServer	string	可选
exts	string	可选

version：版本号，当前版本为“V1.0”。

contentID：内容标识，base64 编码。

kids：密钥标识数组，base64 编码。

enschema：加密模式，取值包括“sm4t”、“sm4r”、“sm4c”、“sm4s”等，“sm4t”表示采用SM4-CTR加密，“sm4r”表示采用SAMPLE-SM4-CTR加密，“sm4c”表示采用SM4-CBC加密，“sm4s”表示采用SAMPLE-SM4加密。

playIndex：当前播放的位置的索引，无符号整型。

drmServer：获取许可证的 URL。

exts：扩展字段。

内容保护描述信息格式如下：

```
{
    "version": "V1.0",
    "contentID": "base64_string",
    "kids": ["base64_string", "base64_string" , …],
    "enschema": "string",
    "playIndex": integer,
    "drmServer": "base64_string",
    "exts": "string"
}
```

内容保护描述信息格式样例：

{"version":"V1.0","contentID":"c2Zhc1JBZXV5SEpGU0pB","kids":["u76mh6/tuJCJzYiJvcu8dw=="],"enschema":"sm4c"}

表 A.1 定义的 PSSH 数据示例如下：

0000008b70737368000000003d5e6d359b9a41e8b843dd3c6e72c42c0000006b7b2276657273696f6e223a2256312e30222c22636f6e74656e744944223a2263325a6863314a425a5856355345704755307042222c226b696473223a5b227537366d68362f74754a434a7a59694a7663753864773

d3d225d2c22656e736368656d61223a22736d3463227d

示例数据的 base64 编码如下：

AAAAi3Bzc2gAAAAAPV5tNZuaQei4Q908bnLELAAAAGt7InZlcnNpb24iOiJWMS4wIiwiY29udGVudElEIjoiYzJaaGMxSkJaWFY1UOVwR1UwcEIiLCJraWRzIjpbInU3Nm1oNi90dUpDSnpZaUp2Y3U4ZHc9PSJdLCJlbnNjaGVtYSI6InNtNGMifQ==

A.2 基于 DASH 的视音频内容加密

在实际应用过程中，基于DASH的视音频内容加密在符合GY/T 277—2019中6.3.2节和6.3.3节规定的基础上，建议增加SM4-CTR、SAMPLE-SM4-CTR两种模式，即：

保护模式信息盒(‘sinf’)中的模式类型盒(‘schm’)中的模式类型scheme_type=‘sm4t’时表示采用SM4-CTR加密；保护模式信息盒(‘sinf’)中的模式类型盒(‘schm’)中的模式类型 scheme_type=‘sm4r’时，表示采用SAMPLE-SM4-CTR加密。

内容授权许可证获取信息在DASH的MPD文件的<ContentProtection>中，定义如下。

a) ContentProtection的value属性为本节定义的scheme_type字符串，schemeIdUri为“urn:mpeg:dash:mp4protection:2011”，cenc:default_KID为内容加密密钥标识KID，使用UUID格式的字符串，cenc:default_KID可选。

示例1:<ContentProtection value="sm4c" schemeIdUri="urn:mpeg:dash:mp4protection:2011" cenc:default_KID="bbbea687-afed-b890-89cd-8889bdcbbc77"/>

b) ContentProtection的schemeIdUri属性定义为“3d5e6d35-9b9a-41e8-b843-dd3c6e72c42c”，对应的cenc:pssh为表A.1定义的PSSH数据base64编码后得到的字符串。

示例2：<ContentProtection schemeIdUri="urn:uuid:3d5e6d35-9b9a-41e8-b843-dd3c6e72c42c"><cenc:pssh>AAAAi3Bzc2gAAAAAPV5tNZuaQei4Q908bnLELAAAAGt7InZlcnNpb24iOiJWMS4wIiwiY29udGVudElEIjoiYzJaaGMxSkJaWFY1UOVwR1UwcEIiLCJraWRzIjpbInU3Nm1oNi90dUpDSnpZaUp2Y3U4ZHc9PSJdLCJlbnNjaGVtYSI6InNtNGMifQ==</cenc:pssh></ContentProtection>

A.3 基于 CMAF 的视音频内容加密

基于CMAF的视音频内容加密模式采用CTR或CBC模式，具体定义见A.2。加密媒体分块的内容加密密钥信息在m3u8文件中的#EXT-X-KEY的URI属性中定义，具体定义见A.1。

附录 B 直播视音频内容分发 DRM 系统设计

B.1 概述

本附录给出了具备IP通信链路情况下的直播视音频内容分发DRM系统设计参考。具备IP通信链路的直播视音频内容分发DRM系统，内容加密密钥由密钥管理模块生成，每次都生成当前和下一密钥，内容加密模块采用密钥管理模块生成的密钥进行直播内容的加密。采用广播方式进行数字电视传输流分发、具备IP回传链路的场景下，直播视音频内容分发DRM系统设计见B.2；采用UDP组播方式进行数字电视传输流分发场景下，直播视音频内容分发DRM系统设计见B.3；采用HLS、DASH、CMAF等流媒体协议进行频道播出场景下，直播视音频内容分发DRM系统的内容加密封装见附录A。

B.2 采用广播方式进行数字电视传输流分发

采用广播方式进行数字电视传输流分发的情况下，视音频内容加密是对数字电视传输流基本码流进行加密，在基本码流的扩展数据中增加内容加密信息指明随后的视频帧加密方法和加密密钥；在下一个内容加密信息出现之前，所有的视频数据采用当前内容加密信息规定的方式和密钥进行加密，每个视频帧中需要加密的数据均采用当前内容加密信息中的初始向量。

数字电视传输流的PMT表中包含ChinaDRM描述子，该描述子规定DRM客户端获取内容授权许可的相关信息，DRM客户端按照许可证获取协议封装许可证请求消息从系统配置的URL通过IP通信链路申请内容授权许可证，并按照内容授权许可证进行内容的解密播放；当下一个内容加密信息中的当前密钥ID发生改变时，DRM客户端应发起新的内容授权许可证请求，及时更新内容授权许可证。

智能终端设备开机时，DRM客户端从系统配置的URL申请全部授权频道的内容授权许可证响应消息。需要更新许可证时，为避免出现大并发的情形，DRM客户端在一个随机的时间段后进行内容授权许可证的申请。为确保频道播出正常，该场景还应满足表3规定的技术要求。可根据频道播出的内容质量设置不同的内容加密密钥更新频率，针对高价值视音频内容可24小时内更新一次内容加密密钥，其他内容可7至15天更新一次内容加密密钥。

B.3 采用 UDP 组播方式进行数字电视传输流分发

采用UDP组播方式进行数字电视传输流分发的情况下，视音频内容加密是对数字电视传输流基本码流进行加密，在基本码流的扩展数据中增加内容加密信息指明随后的视频帧加密方法和加密密钥；在下一个内容加密信息出现之前，所有的视频数据采用当前内容加密信息规定的方式和密钥进行加密，每个视频帧中需要加密的数据均采用当前内容加密信息中的初始向量。

该场景下，电子节目单或传输流PMT表中包含ChinaDRM描述子，该描述子规定DRM客户端获取内容授权许可的相关信息，DRM客户端按照许可证获取协议封装许可证请求消息从系统配置的URL申请内容授权许可证，并按照内容授权许可证进行内容的解密播放；当下一个内容加密信息中的当前密钥ID发生改变时，DRM客户端应发起新的内容授权许可证请求，及时更新内容授权许可证。

智能终端设备开机时,DRM客户端从系统配置的URL申请全部授权频道的内容授权许可证响应消息。需要更新许可证时，为避免出现大并发的情形，DRM客户端在一个随机的时间段后进行内容授权许可证的申请；为确保频道播出正常，该场景还应满足表3规定的技术要求。可根据频道播出的内容质量设置不同的内容加密密钥更新频率,针对高价值视音频内容可24小时内更新一次内容加密密钥，其他内容可7至15天更新一次内容加密密钥。

附录 C DRM 云服务集成要求

DRM云服务集成部署是指以云服务方式提供直播/点播加密、密钥管理、密钥网关、内容授权等一种或多种核心DRM服务端组件功能，拟使用DRM系统的机构以购买服务的方式实现视音频内容分发数字版权管理能力与其运营系统的集成。

DRM云服务应具备以下能力：

1.以云服务方式提供的 DRM 服务端核心组件应符合 GY/T 335—2020 规定的标准符合性要求以及 GY/T 336—2020 规定的系统合规性要求；

2.应具备以云服务方式提供直播/点播加密、密钥管理、密钥网关、内容授权等一种或多种 DRM 服务端核心组件的服务能力；

3.应支持为不同客户提供直播/点播加密、密钥管理、密钥网关、内容授权等组件的物理或逻辑隔离；

4.应支持将使用 DRM 系统的机构的 DRM 服务端组件数字证书托管到 DRM 服务端组件云服务中。

附录 D DRM 客户端集成

D.1 概述

按照终端安全能力及应用场景的不同，DRM 客户端集成方式包括：硬件可信执行环境内置、操作系统内置、应用内置三种。

D.2 硬件可信执行环境内置

硬件可信执行环境内置 DRM 客户端的集成方式见图 D.1。DRM 客户端由部署于操作系统富执行环境（REE）侧的 DRM 插件和部署于可信执行环境（TEE）侧的 DRM 可信应用（TA）两部分组成。

DRM 插件部署于操作系统的 DRM 框架中。DRM 框架由 DRM 应用编程接口、DRM 应用框架、DRM 服务组成。DRM 应用编程接口为 DRM 播放应用提供证书管理、许可证获取等功能；DRM 应用框架对接 DRM 服务，实现 DRM 应用编程接口功能；DRM 服务通过 DRM 插件接口调用 DRM 插件提供的 DRM 功能，同时对接媒体服务，实现视音频内容的解密。DRM 插件调用 DRM 客户端功能接口，适配 DRM 服务的 DRM 插件接口。在硬件可信执行环境中，DRM 客户端软件开发包集成在 DRM 可信应用中，DRM 插件通过 TEE 客户端应用编程接口以命令的方式调用 DRM 可信应用中的 DRM 客户端功能。在 TVOS 中，DRM 应用注册到 DRM 服务中，替代 DRM 插件完成相关功能。

DRM 可信应用由 TEE 内部应用编程接口适配层、DRM 客户端软件开发包、DRM 客户端运行环境接口适配层组成。TEE 内部应用编程接口适配层实现 DRM 插件发送的命令的解析，并转换成对 DRM 功能接口的调用。DRM 客户端软件开发包调用底层提供的 DRM 客户端运行环境接口，向上提供 DRM 客户端功能接口。DRM 客户端功能接口定义见 GY/T 277—2019 附录 C。DRM 客户端运行环境接口适配层提供密码算法、随机数、安全内存、安全时间、安全存储、输出控制等安全能力。DRM 客户端运行环境接口定义见 GY/T 277—2019 附录 D。硬件安全级别 DRM 客户端应支持安全视频通路，DRM 客户端运行环境接口适配层应支持安全解密及输出控制。

操作系统的 DRM 应用编程接口一般提供证书下载接口，终端可在产线内置硬件安全信任根密钥及其证书，在 DRM 客户端功能启用前通过证书下载接口将 DRM 客户端私钥及 DRM 客户端证书烧写到安全存储中；也可在产线使用 DRM 客户端证书置入接口将 DRM 客户端私钥及 DRM 客户端证书烧写到安全存储中。DRM 客户端证书置入接口定义见 GY/T 333—2020 附录 A。

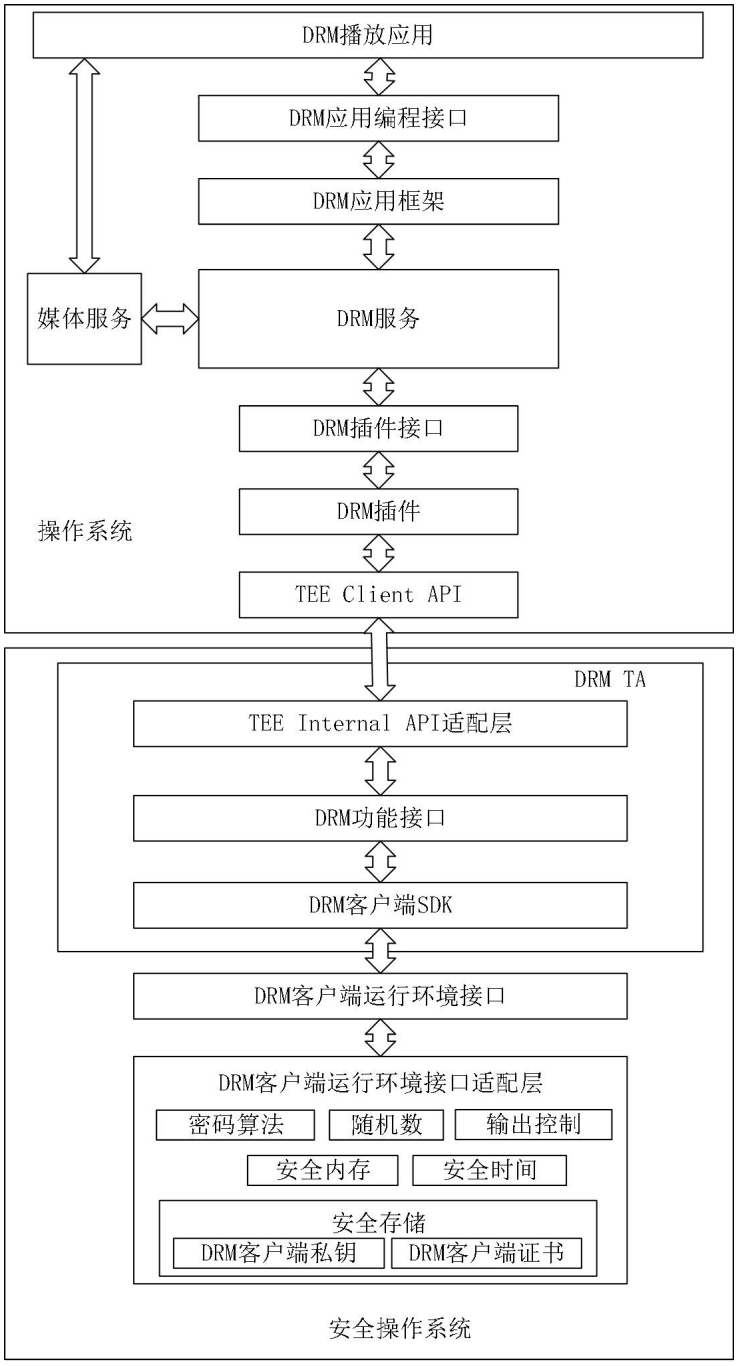
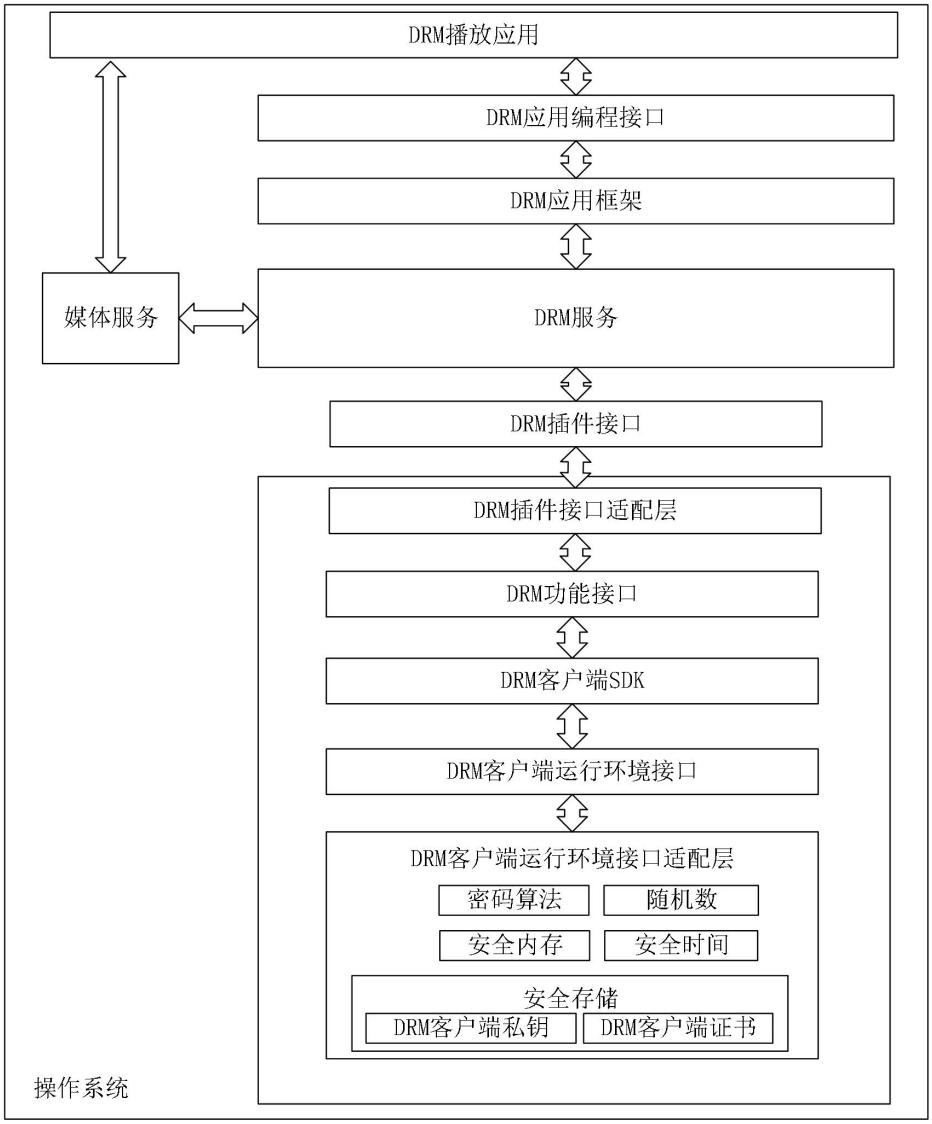


图 D.1 硬件可信执行环境内置方式集成 DRM 客户端

D.3 操作系统内置

操作系统内置 DRM 客户端的集成方式见图 D.2。DRM 插件部署于操作系统的 DRM 框架中。DRM 框架由 DRM 应用编程接口、DRM 应用框架、DRM 服务组成。DRM 应用编程接口为 DRM 播放应用提供证书管理、许可证获取等功能；DRM 应用框架对接 DRM 服务，实现 DRM 应用编程接口功能；DRM 服务调用 DRM 插件提供的 DRM 客户端功能，通过与媒体服务的对接，实现视音频内容的解密。DRM 插件由 DRM 插件接口适配层、DRM 客户端软件开发包、DRM 客户端运行环境接口适配层组成。DRM 客户端软件开发包调用底层提供的 DRM 客户端运行环境接口，以

DRM客户端功能接口的方式提供DRM客户端功能。DRM客户端功能接口定义见GY/T 277—2019附录C。DRM客户端运行环境提供密码算法、随机数、安全内存、安全时间、安全存储等安全能力。DRM客户端运行环境接口定义见GY/T 277—2019附录D。



图D.2 操作系统内置方式集成DRM客户端

操作系统的DRM应用编程接口一般提供证书下载接口，DRM插件应内置证书下载信任根密钥及其证书，在DRM客户端功能启用前通过证书下载接口将DRM客户端私钥及DRM客户端证书写入到DRM客户端运行环境接口适配层实现的安全存储中。

为满足软件安全级别DRM客户端安全要求，DRM插件应采用完整性保护、防破解、防调试、防注入、代码混淆等软件安全机制以确保证书下载信任根密钥和证书、安全存储及其运行的安全。

D.4 应用内置

应用内置DRM客户端的集成方式见图D.3。DRM客户端以库的方式集成到DRM播放应用中。DRM播放应用调用DRM库提供的DRM应用编程接口实现DRM功能。DRM库包括DRM应用

编程接口适配层、DRM 客户端软件开发包、DRM 客户端运行环境接口适配层等。DRM 应用编程接口适配层调用 DRM 客户端功能接口实现 DRM 客户端功能。DRM 客户端软件开发包调用底层提供的 DRM 客户端运行环境接口，向上提供 DRM 客户端功能接口。DRM 客户端功能接口定义见 GY/T 277—2019 附录 C。DRM 客户端运行环境接口适配层提供密码算法、随机数、安全内存、安全时间、安全存储等安全能力。DRM 客户端运行环境接口定义见 GY/T 277—2019 附录 D。

图 D.3 应用内置方式集成 DRM 客户端

DRM 应用编程接口应提供证书下载接口。DRM 播放应用应内置证书下载信任根密钥及其证书，在 DRM 功能启用前通过证书下载接口将 DRM 客户端私钥及 DRM 客户端证书写入到 DRM 客户端运行环境接口适配层实现的安全存储中。

为满足软件安全级别 DRM 客户端安全要求，DRM 播放应用及 DRM 库应采用完整性保护、防破解、防调试、防注入、代码混淆等软件安全机制以确保证书下载信任根密钥和证书、安全存储及应用运行的安全。

参考文件

1. 国家广播电视总局办公厅关于发布视音频内容分发数字版权管理标准体系的通知（广电办发〔2021〕45号）
2. IETF RFC 8216 HTTP实时流媒体（HTTP Live Streaming）（本文称：HLS）

缩略语

下列缩略语适用于本文件。

CA　证书认证中心（Certification Authority）

[来源：GB/T 21053-2023 信息安全技术 公钥基础设施 PKI 系统安全技术要求]

CBC　密文分组链接（Cipher Block Chaining）

[来源：GB/T 17964-2021 信息安全技术 分组密码算法的工作模式]

CDN　内容分发网络（Content Delivery Network）

CEI　内容加密信息（Content Encryption Information）

CEK　内容加密密钥（Content Encryption Key）

CMAF　通用媒体应用格式（Common Media Application Format）

CRL　证书撤销列表（Certificate Revocation List）

[来源：GB/T 21053-2023 信息安全技术 公钥基础设施 PKI 系统安全技术要求]

CTR　计数器（Counter）

[来源：GB/T 17964-2021 信息安全技术 分组密码算法的工作模式]

DASH　基于 HTTP 的动态自适应流媒体（Dynamic Adaptive Streaming over HTTP）

DRM　数字版权管理（Digital Rights Management）

HLS　HTTP 实时流媒体（HTTP Live Streaming）

IP　网际互联协议（Internet Protocol）

ISO　国际标准化组织（International Organization for Standardization）

MPD　媒体展现描述（Media Presentation Description）

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

[来源：GB/T 21053-2023 信息安全技术 公钥基础设施 PKI 系统安全技术要求]

PC　个人计算机（Personal Computer）

PKI　公钥基础设施（Public Key Infrastructure）

[来源：GB/T 21053-2023 信息安全技术 公钥基础设施 PKI 系统安全技术要求]

PMT　节目映射表（Program Mapping Table）

REE　富执行环境（Rich Execution Environment）

TA　可信应用（Trusted Application）

TEE　可信执行环境（Trusted Execution Environment）

TS　传送流（Transport Stream）

UDP　用户数据报协议（User Datagram Protocol）

URL　统一资源定位符（Uniform Resource Locator）