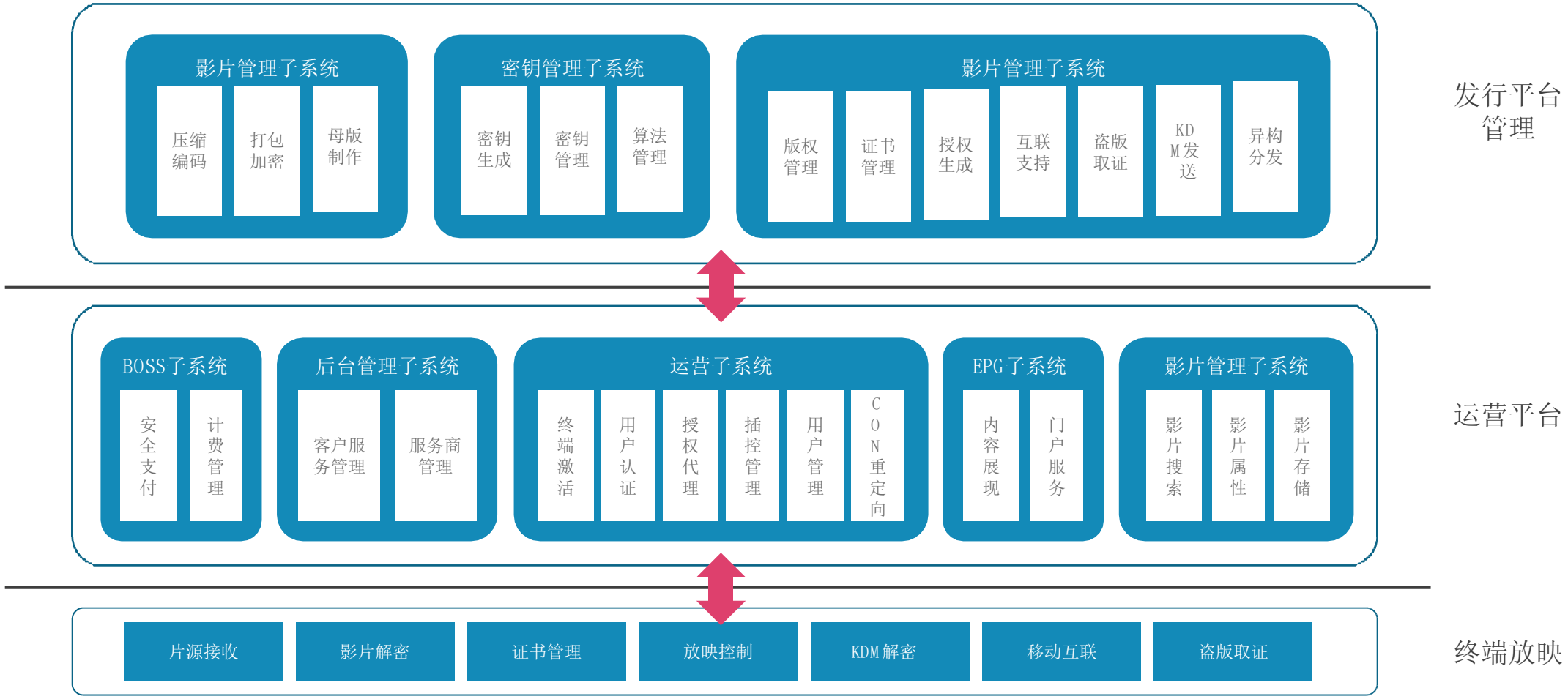
DRAGON VEIN

龙脉数字影视DRM系统介绍

数字点播系统功能描述

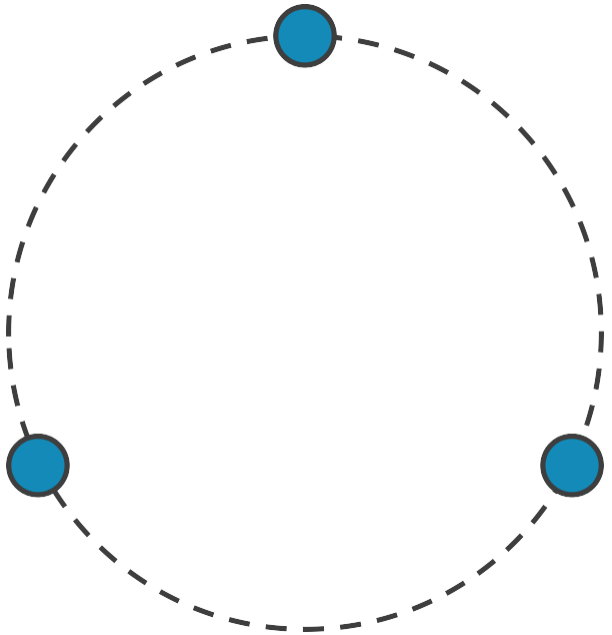
数字点播系统功能示意图如下：



发行管理平台

影片管理子系统

实现对数字电影影片的编码压缩，影片内容的存储和管理，包括影片的导入导出、DRM加密、影片信息（资产信息、供片方等）。



密钥管理子系统

实现对影片密钥的动态生成等功能，家庭影院采取按次授权放映的方式发放密钥。

发行子系统

包括发行版电影的存储、版权管理、授权生成和失效管理、异构分发、盗版取证、KDM发送功能，实现对全国内容的分发,中心影片库向边缘分发节点的内容同步、边缘节点影片的强制下线等。

运营平台

影片管理子系统

对从集中发行管理平台接收的影片进行存储和管理；为用户提供影片搜索功能；影片统计属性管理，包括影片播放排行、热门影片统计等。

运营子系统

运营子系统的作用包括以下内容：

- 放映终端的首次开机上网激活、设置，包括终端所在区域、注册码管理等。
- 用户上线的身份认证、设备认证，用户在线管理、下线管理，并对用户上线、下线相关信息（如上线时间、上线时长等）进行统计。
- 作为用户终端的授权代理，在接收到用户放映影片的请求后，代理用户向发行管理平台申请授权，并进而向用户转发授权。同时对用户的授权、数字证书等权限信息进行保存和管理。
- 在用户获取影片授权后，将用户重定向到相应的CDN节点。
- 为用户提供播控管理服务，如暂停、选时播放等，支持断点续播功能。
- 实现用户管理功能：

① 实现对用户信息、会员资格、会员积分、点播记录等的管理。

② 实现设备管理功能，包括设备类型、厂商信息、所属区域、软件版本的管理与更新等。

③ 对用户点播行为进行统计，如观看影片名、观看时间点等，并对统计数据进行分析，作为用户管理、市场策略、营销策略的依据。

运营平台

BOSS子系统（定价计费和资金账务管理系统）

对用户和设备的认证、开户、销户等进行管理，对影片定价，对用户点播行为进行计费、收费等等。资金账务系统既管理用户的资金账户，也管理与上下游的分账和对账等。BOSS系统需可支持线下预支付、在线支付，以及第三方支付（如支付宝、微信）等多种方式

EPG子系统（门户和服务导航系统）

是用户浏览和检索影片，选择影片并请求播放的系统，可包括本地导航页面和APP导航页面，需根据用户类型显示影片定价信息，支持用户查询点播和消费记录，支持根据用户的兴趣推荐影片，支持多屏互动功能。

后台管理子系统

包括两个模块，分别为服务商管理模块、客户服务管理模块。服务商管理模块：实现对服务商的管理，包括资格管理、签约管理、考核管理、分账管理、授权管理等。客户服务管理模块：包括呼叫中心、网站、APP下载等功能，支持用户的业务咨询、投诉反馈、故障报修、账单投递等。

传输分发网络

IP传输网络

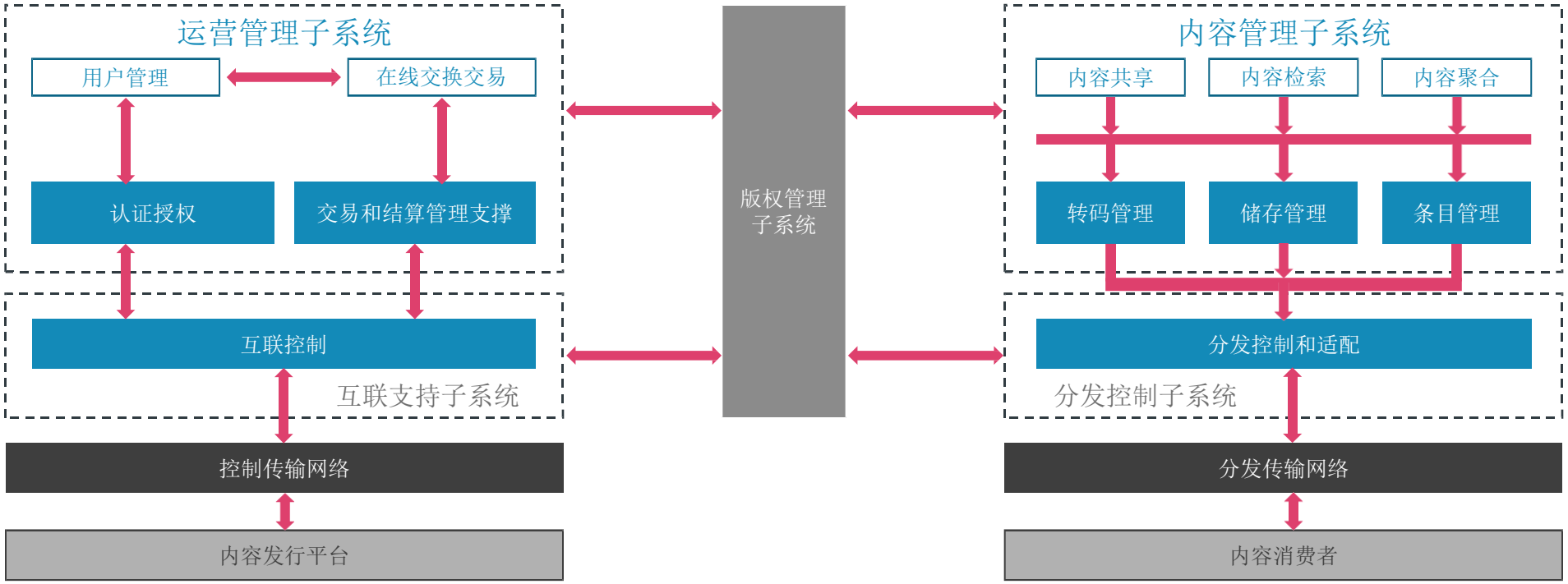
包括运营商的IP城域网和IP接入网，负责用户接入网络的畅通、影片内容的高速安全分发。

CDN网络

运营商的CDN网络，负责运营商已获取授权的影片内容的分布式存储，并就近向获取授权的终端用户分发影片内容。

数字点播内容分发及运营系统开发

数字点播内容分发及运营系统从功能层次上可分为内容管理子系统、异构分发子系统、互联支撑子系统三部分。作为运营支撑，运营管理子系统负责对运营平台服务的用户进行管理，版权管理子系统服务于影片发行和内容监管。平台体系总体结构如下图所示：



其中内容管理子系统实现内容共享、内容检索、内容聚合、转码管理、存储管理、条目管理等与内容管理相关的功能；异构分发子系统实现媒体内容的传送控制和适配，以满足不同分发策略和不同传输网络及不同传输途径的需要；互联支撑子系统实现交易结算等控制信息的安全、可靠传送，并实现各媒体内容集成分发平台间的互通；运营管理子系统实现用户管理、认证授权、在线交换交易和交易结算管理支撑功能；版权管理子系统实现对分发内容的版权管理，控制内容的使用权限。

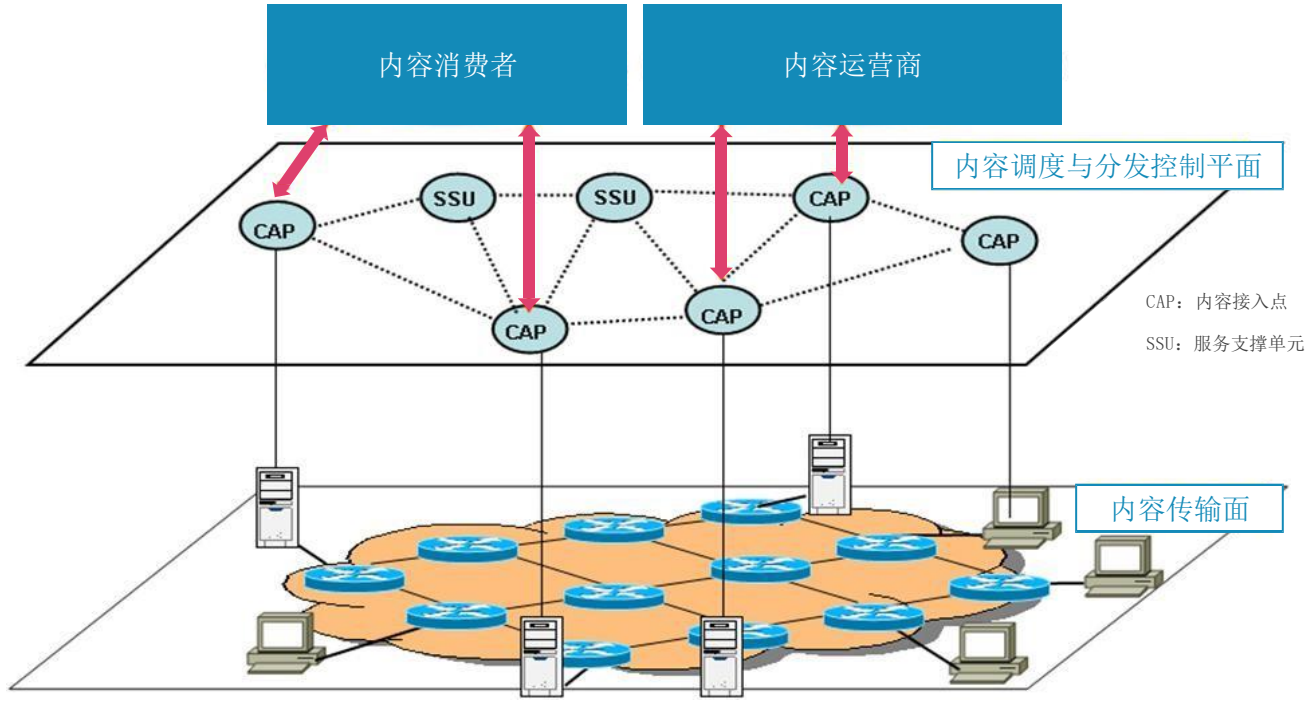
数字点播内容分发及运营系统开发

内容管理子系统

内容管理子系统实现对数字点播内容的管理服务，包括存储管理、条目管理和转码管理。并提供内容共享、内容检索和内容聚合服务。需要对不同来源、不同格式、不同种类的内容资源进行集成整合，实现对数字点播内容的聚合、检索和共享。

数字点播内容分发及运营系统开发

异构分发子系统



本子系统主要解决内容提供商、运营商、用户之间数字点播内容的分发调度控制和传送问题。在数字点播内容统一、多层次、多维结构化描述与操作接口的基础上，对异构的网络和数据传输模式进行分析和综合，抽象出一层可扩展的网络应用架构，并提供统一的访问界面，以解决内容的互连和交换问题。

作为一个服务支撑平台，数字点播内容分发及运营系统屏蔽异构网络在拓扑结构、协议规范和物理特性方面的多样性，透明地向用户提供统一的内容接入服务。根据数字影院媒体内容在内容分发及运营系统内的递送特征，抽象出如下图所示的层级结构。

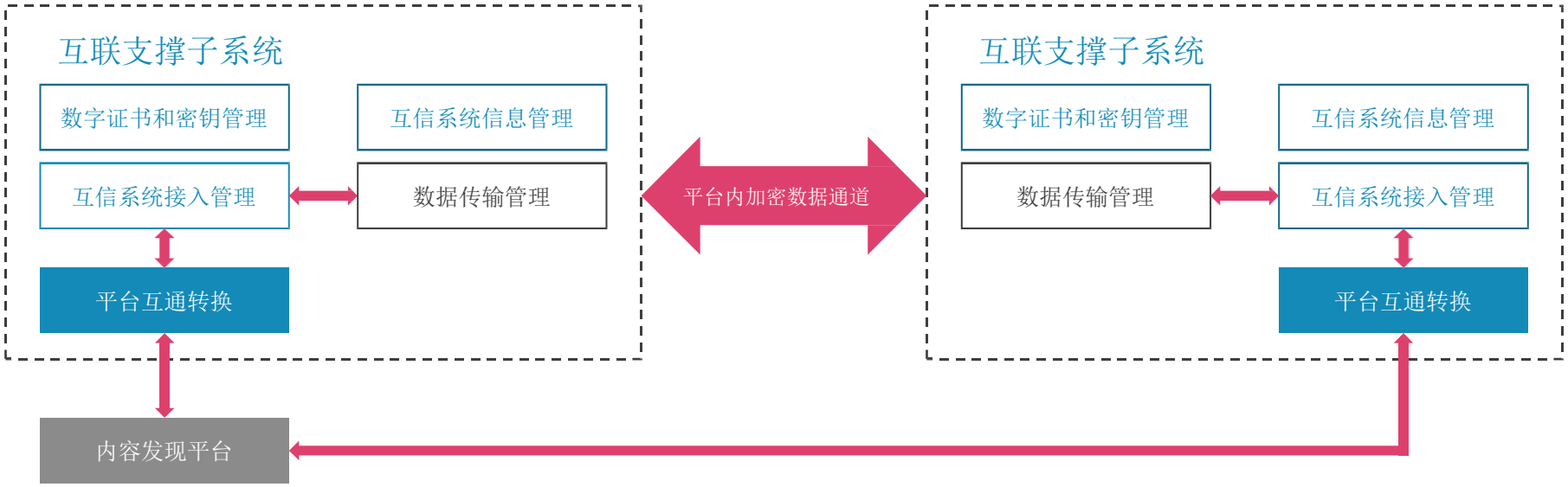
异构分发子系统被分为内容调度与分发控制平面和内容传输平面。内容调度与分发控制平面主要解决不同网络体系、接入方式和运营机制内容分发的优化调度和分发策略选择；内容传输平面要解决内容分发传送的高效和可靠，优化传输资源的配置。

数字点播内容分发及运营系统开发

互联支撑子系统

互联支撑子系统定位在控制平面的中间支撑层，位于控制传输网络之上和运营管理子系统之下。其作用有两个：一是为运营管理子系统屏蔽底层网络的细节，实现运营管理子系统数据安全、可靠的传输。二是为实现与内容发行平台互通而实现的接口和转换功能。

互联支撑子系统将研究实现不同实体在异构网络中的安全加密互联问题。



数字点播内容分发及运营系统开发

互联支撑子系统

互联支撑子系统由数字证书和密钥管理、互信系统信息管理、互信系统接入管理、数据传输管理、平台互通转换五部分组成。

- 数字证书和密钥管理：主要作用是建立互连支撑子系统之间的互信关系所需要的凭证和密钥，以便能够在互相访问的时候根据证书和密钥进行身份认证和安全交易。将针对不同互联支撑子系统生成数字证书和密钥，并对数字证书和密钥信息进行管理；客户端密钥分别分发到不同运营子系统。

- 互信系统信息管理：要保证系统的统一互连和交易视图，需要对各互通的子系统信息进行统一的信息管理。要管理对等实体互联支撑子系统的相关信息（网络特征信息、系统特征信息、密钥特征等），建立信赖关系，向对方系统发起互信请求，交互后建立互信关系。收到在其它实体互联支撑子系统发起的互信请求时，进行系统审核并回复系统应答信息。

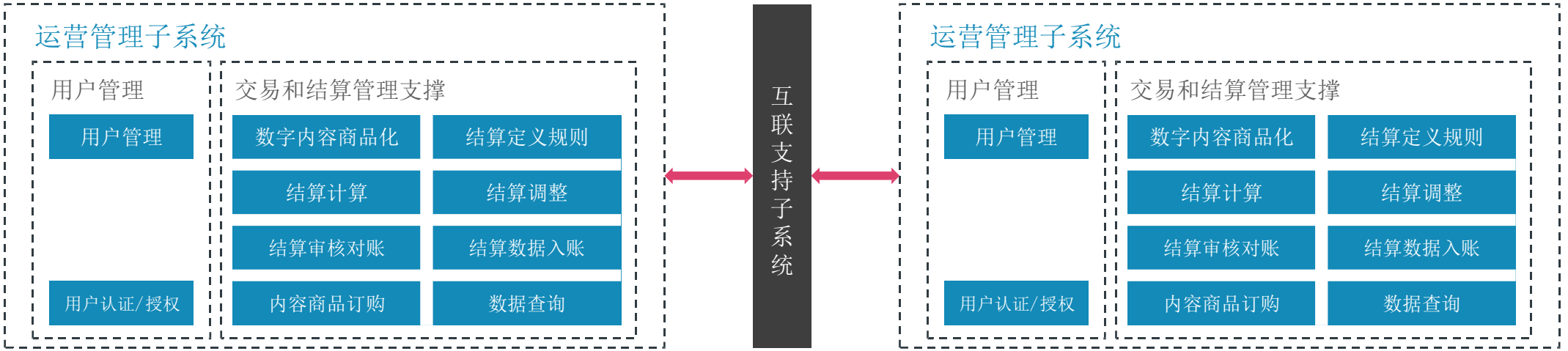
- 互信系统接入管理：一个实体可能基于不同的网络环境、以不同的方式、在不同的时段向其他实体发起的互连请求。需对系统接入进行统一管理，设定指定系统的接入方式、接入时限、接入范围、服务响应范围，访问数据范围等规则；系统被访问时，根据设定规则进行接入层面限制，并根据规则强制中断规则外连接。

- 数据传输管理：不同实体间系统进行访问时，为避免传输过程中数据被拦截和窃取，需要对数据的传输进行两方面的处理：一方面，不同实体系统进行数据交互，使用针对特定系统的数字证书和密钥，建立交互加密安全通道。另外一方面，通过加密通道进行数据交互前，指定加密方式，对数据进行加密，收到数据后对数据进行解密处理。为防止数据丢失，还需对传输数据进行校验和纠错处理。

- 平台互通转换：当本系统与内容发行平台互联时，需要由互联支撑子系统实现两个系统在传输层面的互通。不同的平台可能采用了不同的网络适配方式、协议交互流程、数据加密方式、可靠传输手段，要实现和其它系统的互通，必须在互联支撑子系统处进行协议的转换处理，以确保传输层面的互联互通。

运营平台的用户管理内容

运营平台的用户管理主要由运营管理子系统来实现。运营管理子系统主要有用户管理和在线交易管理。用户管理实现用户注册、用户资料信息管理、用户认证、授权管理。在线交易管理主要实现数字内容商品化、结算规则设定、数字商品定购、交易结算、对帐等。通过不同种类数字点播内容、不同定价策略、不同销售策略、不同使用限制等相关信息组成的多维数字点播内容视图的研究，实现数字点播内容标准商品化。设计出适合我国数字点播内容管理体制、数字点播内容交易模式、不同地方法规下的数字点播内容交易结算模型，并运用相关模型建设交易结算管理系统。



运营平台的用户管理内容

运营平台的用户管理

互联支撑子系统由数字证书和密钥管理、互信系统信息管理、互信系统接入管理、数据传输管理、平台互通转换五部分组成。

- 用户管理：不同实体之间的互相访问，都需要统一标识。互信系统通过统一用户注册报文，进行用户注册，并使用约定报文实现用户信息、用户帐户信息等信息管理维护功能。
- 用户认证/授权：实体间访问系统，需要通过对方系统的认证，并在对方系统授权范围内访问功能、服务、数据。注册用户进行访问，使用被访问系统 发放数字证书，用认证报文进行认证。认证通过后，被访问系统对认证通过用户进行授权，授权可访问系统资源。
- 交易和结算管理支撑：包括数字点播内容商品化、结算规则定义、数字点播内容商品定购、数据查询、结算计算、结算审核对帐、结算调整、结算数据入帐等模块。

运营平台的用户管理内容

运营平台的用户管理

交易和结算管理支撑包括数字点播内容商品化、结算规则定义、数字点播内容商品定购、数据查询、结算计算、结算审核对帐、结算调整、结算数据入帐等模块。

- 数字点播内容商品化：不同实体的数字点播内容格式多种多样，又具有不同的属性描述和使用限制。在数字点播内容进行交易时，可以交易数字点播内容本身、交易某期限范围内的版权、交易信用证等等，可以交易单项数字点播内容又可以打包相关数字点播内容进行交易。要实现数字媒体及其涉及的相关内容的交易，需要对数字点播内容进行商品化处理，使数字点播内容形成可货币化的商品。根据不同的数字点播内容的相关信息，进行商品化处理，定义该数字点播内容的各项分项价格，并指定服务条款、适用条款、商品说明、价格策略（支付方式、费用定义）、商品期限、使用范围等等数字点播内容各项信息抽象内容商品模型，进行数字点播内容商品化处理，最终形成可交易、交换，可货币衡量的数字点播内容商品。
- 结算规则定义：不同实体、内容供应商、运营商之间进行数字点播内容交易，可以采用货币化方式交易，也可能采用物物交换模式等；在交易时，可以买断、可以按使用时间购买；在结算付费时，可以采用即时付费方式，也可采用周期结算方式；在选择付费方式时，可以传统支付方式，也可采用电子支付方式等等，这些都需要灵活的结算规则设定。需针对内容商品的内容信息、版权信息、交易时间信息、交易用户信息、合同协议信息、定购数量信息、使用范围信息等等因素设定结算规则，设定结算周期、结算方法、支付方式、支付周期等。
- 数字点播内容商品定购：数字点播内容商品可以采用货币定购方式进行内容定购。根据约定报文，获取可定购内容列表、价格、结算定义，并进行数字点播内容定购。为保证定购信息的一致性，双方约定既定流程，进行产品定购和定购确认，并形成内容定购记录。内容定购信息通过MAIL、短信等形式发送到内容定购双方，并进行结果确认。
- 数据查询：不同实体之间需要获取其他实体数字点播内容、费用相关信息，需要进行数据查询。使用约定数据格式，发起结算数据、定购数据等查询，并根据约定格式返回查询结果。
- 结算计算： 根据产品定购记录和结算规则设定帐期进行结算计算，并最终出结算结果和结算帐单。
- 结算审核对帐：不同实体间根据各自的交易记录进行结算计算，结算出的结果需要进行互相核对和审核。双方根据结算结果进行自动对帐，发起对帐报文并返回结果，并根据对帐结果对结算结果进行结算数据确认，生成双方认可结算帐单。
- 结算调整：对帐有差距数据，发起调整报文，并针对系统设定进行结算数据调整。
- 结算数据入帐：结算数据双方确认之后，根据用户结算帐单和用户帐户信息、支付方式，进行帐务结转，支持银行自动划帐、帐期结转等。结算入帐后，发出入帐确认信息。

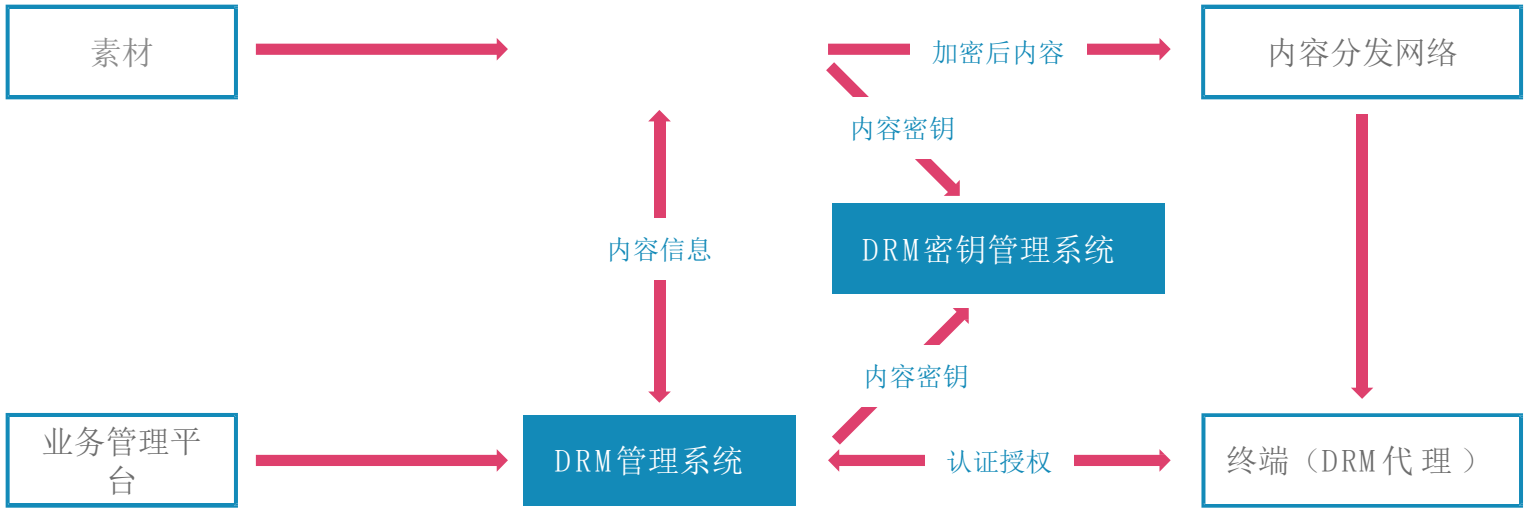
DRM系统技术方案

在片源制作与用户终端环节利用DRM技术进行控制内容的消费和使用。

DRM系统技术框架如图所示，DRM系统作为IP视频能力平台的核心功能部件，对节目内容提供端到端全生命周期的安全保护。

在IP视频能力平台业务系统中，DRM系统提供以下两方面功能：

内容加密，DRM加密系统对节目内容进行加密；终端在播放DRM加密节目时，机顶盒中的DRM代理库发起获得内容许可证请求，DRM系统响应机顶盒请求并将DRM内容许可证安全发送给终端，DRM代理库根据授权情况，对内容进行解密，提供给机顶盒解码芯片播放。

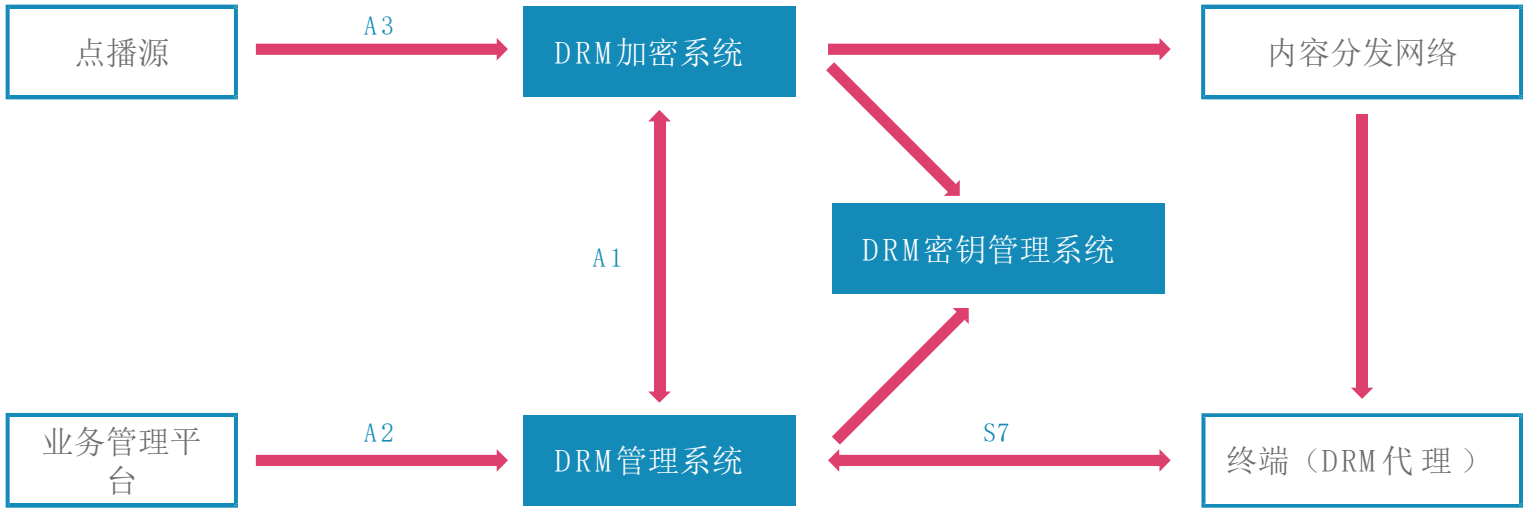


如左图所示，DRM系统由前端系统和终端DRM代理组成。前端系统主要包括DRM加密系统、DRM密钥管理系统、DRM管理系统等子系统组成。

DRM系统技术方案

DRM加密系统负责节目内容加密功能，支持直播内容加密、对点播内容加密等功能；DRM密钥管理系统负责对内容密钥统一管理，支持与DRM加密系统对接；DRM管理系统负责设备管理功能，支持与业务管理平台对接，负责设备号导入/导出、开户/停户、查询等设备管理功能；负责终端机顶盒证书颁发、撤销、更新等功能；负责对终端机顶盒认证并对内容授权等功能；终端DRM代理负责终端DRM管理功能，支持终端认证、内容授权及内容解密功能等。

DRM系统接口如图所示：



图：系统架构

DRM系统与业务系统间的接口，及DRM各子系统之间接口如左图所示。其中：

- A1接口为DRM管理系统与DRM加密系统间接口，负责将内容标识、内容密钥等信息注册到DRM密钥管理系统；
- A2接口为业务管理平台与DRM管理系统接口，负责终端合法性认证及授权；
- A3接口为点播源与DRM加密系统接口，负责点播加密调度及内容提供；
- S7接口为终端与DRM管理系统接口，负责认证、授权等。

DRM系统技术方案

前端DRM 对接方案

DRM平台既支持点播内容离线加密，也可支持直播节目的实时加密。终端播放DRM加密节目时通过DRM代理经网络从DRM平台获取播放授权。

终端DRM 集成方案

对于IP视频能力平台的业务形态，终端类型智能电视一体机，为满足内容保护的要求，终端DRM集成方案为智能电视一体机方案。

对于电视一体机产品，需要主芯片带有TEE功能，集成DRMTA集成到TEE区域，并在组件层集成DRM插件，支持DRM硬件及以上安全级别，以满足内容商对内容DRM保护的要求。

DRM系统技术方案

影片内容格式

参考ISO 26429系列标准的DCP打包格式，图像编码可采用H.264、HEVC等，音频编码AC3 、DTS等。

内容加密

AES-128-CBC （加密长度可调）

认证与授权

参考ISO 26430系列标准的KDM密钥格式进行认证与授权，RSA采用2048位密钥长度，设备私钥应通过安全硬件方式存放保护，KDM证书链签名防篡改。

安全硬件

参考GM/T0039-2015密码模块安全检测要求 ，GM/T 0003.1-5 SM2标准。

场次控制

KDM（Key Delivery Message）档期与场次控制。