GY

中华人民共和国广播电影电视行业标准

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

Technical specification of interface between the DRM system and the integrated IPTV broadcast and control platform

2011-07- 20 发布　　2011－07－20 实施

国家广播电影电视总局　发布

目　　次

前　言

本标准按照GB/T 1.1-2009《标准化工作导则 第1部分：标准的结构和编写》给出的规则编制。

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。

请注意本标准的某些内容可能涉及专利。本标准的发布机构不承担识别这些专利的责任。

本标准起草单位：中国广播影视数字版权管理论坛标准起草委员会IPTV集成播控平台DRM接口特别工作组，包括中央电视台、清华大学、飞利浦上海研发中心、UT斯达康（中国）有限公司、中国国际电视总公司、英特尔（中国）有限公司、中国网络电视台、中央数字电视传媒有限公司、北京数字太和科技有限责任公司、北京捷成世纪科技发展有限公司、北京安视网信息技术有限公司、北京中科大洋科技发展股份有限公司、新奥特（北京）视频技术有限公司、索尼(中国)有限公司、成都索贝数码科技股份有限公司、耐格如信（上海）软件技术服务有限公司、北京永新视博数字电视技术有限公司、天柏宽带网络科技（北京）有限公司、爱迪德技术（北京）有限公司。

本标准主要起草人：丁文华、李晖、文奇、宿为民、马缚龙、邢彩虹、王博维、孙剑、钟宏、赵黎、王兴军、田忠、刘璐、魏启任、徐磊、孔德宇、权晓忠、梅红兵、栾旭涛、汪城、陈晓明、赵于平、王希菊、王付生、张大勇、中山、何峰、薛滨、张晶、孔维良、赵志超、谷晓军。

数字版权管理系统与 IPTV 集成播控平台接口技术规范

1 范围

本标准规定了数字版权管理系统与IPTV集成播控平台的接口。

本标准适用于数字版权管理与IPTV集成播控平台的前端系统及终端的集成。

2 规范性引用文件

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

中国广播影视数字版权管理（DRM）技术白皮书

IEC 62455-2008 互联网协议(IP)和基于服务访问的传输流(TS)(Internet protocol (IP) and transport stream (TS) based service access)

RFC 2396 统一资源标识符：通用句法（Uniform resource identifiers (URI):generic syntax）

ETSI ETR 289 数字视频广播：数字广播系统中对使用加扰和条件接收的支持（Digital video broadcasting (DVB); Support for use of scrambling and conditional access (CA) within digital broadcasting systems）

3 术语和定义

下列术语和定义适用于本标准。

3.1

用户 user

使用数字媒体内容的组织或个人。可通过用户标识（ID）来识别。

3.2

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。

3.3

域 domain

在用户环境中合法使用受保护内容的一组设备，该组设备的范围可由若干参数（比如设备数量、时间、令牌、设备ID等）界定，同时这些参数不应被用户轻易规避（本标准中的“域”即中国广播影视数字版权管理（DRM）技术白皮书中的“用户环境内容保护系统边界”）。

3.4

设备 device

安装有DRM代理的消费内容的实体。

3.5

DRM代理 DRM agent

设备中的可信实体，负责管理对设备上内容的许可。

3.6

DRM保护内容 DRM protected content

根据许可证中的一整套许可而被使用的数字媒体内容。

3.7

集成播控平台 integrated platform of broadcast and control

IPTV内容播出的控制和管理平台，包括内容管理、鉴权管理、计费、用户管理等功能。

3.8

DRM管理系统 DRM management system

DRM管理系统完成数字版权保护所需的各项服务和功能，包括许可证下发、内容加密、域管理等功能。

3.9

DRM 信令 DRM token

DRM信令规定了获取相关内容的对应许可证所需执行的操作序列。

4 缩略语

下列缩略语适用于本标准。

AES Advanced Encryption Standard 高级加密标准
DRM Digital Rights Management 数字版权管理
HTTP Hyper Text Transport Protocol 超文本传输协议
IPTV Internet Protocol Television IP电视
KSM Key Stream Message 密钥流消息
RTP Realtime Transport Protocol 实时传输协议
URI Uniform Resource Indicator 统一资源指示器

5 系统功能和构架

5.1 概述

本标准定义了IPTV集成播控平台中DRM管理系统与其它部分的接口。

IPTV集成播控平台和DRM管理系统的接口可分为以下三部分：

——A 类：中央加密到中央播控平台的接口和地方加密到地方播控平台的接口；

——B 类：DRM 管理服务器和鉴权管理模块的接口；

——C 类：DRM 终端引擎和终端界面应用程序的接口。

DRM管理系统与IPTV集成播控平台及终端接口系统构架见图1。

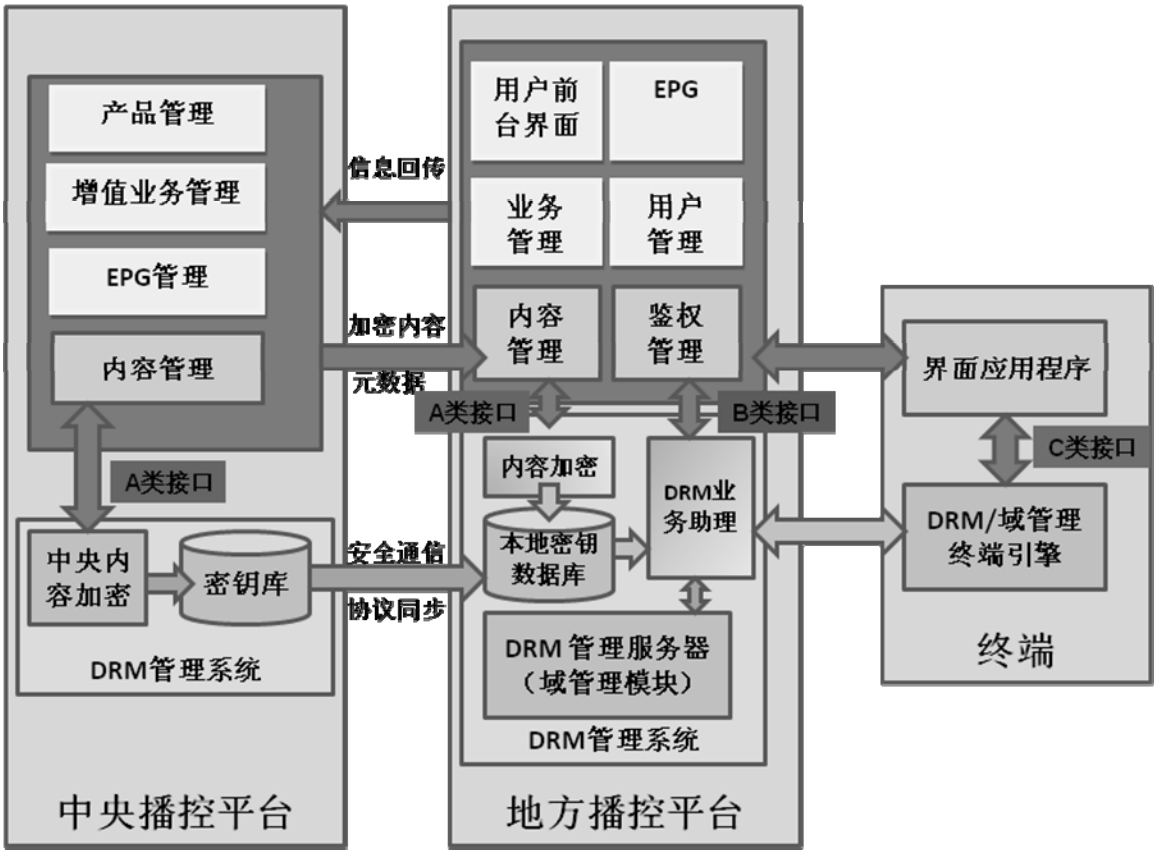

图1　DRM 管理系统与 IPTV 集成播控平台及终端接口系统构架

本标准主要规定的是DRM管理系统和鉴权管理之间的接口，以及地方或者中央播控平台和内容加密之间的接口。

5.2　DRM 管理系统基本构架

DRM管理系统包括内容加密模块、密钥数据库、DRM业务助理模块以及DRM管理服务器等模块。内容由集成播控平台中的内容加密模块加密，内容加密密钥保存在平台的密钥库中。业务助理模块实现了商业模型的需求，DRM管理服务器负责对终端播放的受DRM保护的内容发放许可证。

5.3　基本流程

DRM管理系统部署在中央播控平台和地方播控平台中，由中央播控平台控制。中央内容加密部署在中央播控平台。对于从中央获得的内容，由中央使用A类接口进行内容加密，并将密钥从中央同步到地方DRM管理系统的数据库。对于地方自办内容，直接在DRM管理系统中通过A类接口调用加密模块进行加密，把密钥存储在地方DRM管理系统的密钥数据库。

DRM业务助理从地方播控平台的鉴权管理获得客户的购买信息。集成播控平台业务管理模块或DRM业务助理可以根据业务需求生成相应的DRM业务信令。终端应用程序通过门户导航/EPG或者一个预设的URL获得DRM信令，通过C类接口将信令传递给DRM终端引擎，DRM终端引擎根据信令的要求向DRM管理系统申请内容许可证及相关信息。DRM管理服务器获得从DRM终端发来的请求后，通过DRM业务助理调用B类接口获得授权信息和密钥发放许可证给终端，终端获得合法的许可证后就可以播放所获得的受保护的内容。

当DRM管理服务器接收到从终端DRM引擎发来加入域的申请，DRM业务助理向鉴权管理模块查询是否允许加入域，如果得到授权，DRM业务助理将获得如7.3条所述的用于域注册的必要的信息，并授权终端加入域。

6 A类接口——中央加密到中央播控平台的接口和地方加密到地方播控平台的接口

6.1 概述

本章定义了DRM模块和内容管理模块的数据接口。集成播控平台的内容管理模块将欲加密的内容及相关信息传递给DRM管理系统中的加密模块，由加密模块随机生成加密密钥并对内容进行加密。

6.2 内容信息获取

DRM管理系统在运行中需要向内容管理模块获取所管理的内容的相关信息用以加密。内容管理模块发起一个加密请求、响应的握手协议。

6.2.1 内容加密请求（CEncryptReq）

消息参数如下：

a) DCID：被加密内容的ID；

b) MetaData：被加密内容的元数据，元数据元素及格式定义见表1。

表1 元数据元素及格式定义

元素名称	英文标识	解释	数据类型
数字内容标识符	DCID	唯一标识某个数字内容	字符型
内容名称	Title	内容所有者认可的名称	字符型
时长	Duration	内容的实际时间长度	时间型
内容简介	Description	对内容的概括性描述	字符型

6.2.2 内容加密响应（CEncryptResponse）

消息参数：

a) Result：如果加密成功返回1，否则返回0；

b) KeyIndex：内容加密密钥的索引号。

7 B类接口——DRM管理服务器和鉴权管理模块的接口

7.1 概述

本章定义了DRM管理系统的业务助理模块和鉴权管理模块接口的通用规范。

7.2 传输模式

DRM传输可以使用但是不限于使用基于HTTP协议进行通信。

本标准的接口模式中，由鉴权管理模块把DRM相关信息传递给DRM管理服务器或者DRM管理系统。

7.3 命令要素

最基本的命令要素是DRMCommand，包含了用户和域注册，获取、更新和许可证获取（即交易通知）。

7.4 用户注册

典型的应用场景要求对用户注册，此时DRM管理服务器需要获得用户信息。鉴权管理模块通过用户管理模块获取系统中用户注册的必要数据，并提供给DRM管理服务器。终端应用程序通过门户导航/EPG或者一个预设的URL获得DRM信令，将该信令传送给DRM管理服务器以获取注册信息。

鉴权管理模块提供给DRM管理服务器以下三个参数：

——UserID: 必选项。这是一个用户对象 ID，在用户层该对象应唯一。类型是：“user”。

——ObjectAttribute: 可选项。对象的属性。对于用户对象，有如下属性：

- urn:cdrm:core:node:attribute:friendly-name string;
- urn:cdrm:core:node:attribute:expiration-date int。

——LinkControl: 可选项。用户注册控制，可包含如下控制：

- TimeValidityCondition: 时间控制;
- DeviceTypeCondition: 设备类型控制;
- DeviceCapabilityCondition: 设备能力控制;
- FreshnessCondition: 更新条件。

7.5 域注册

典型的应用场景中内容消费者可以将其设备或用户账户加入域，用户从设备向DRM管理服务器发起加入域的申请，当DRM管理服务器接到终端设备发来的请求后，DRM管理服务器需要从鉴权服务模块获得注册域信息。鉴权服务模块提供系统中注册域的必要数据给DRM管理服务器。

鉴权服务模块提供给DRM管理服务器以下三个参数：

——TargetID: 必选项。这是一个域关联目标对象 ID，根据域注册对象类型不同，其类型是string，值可以是： “user”或者“Domain”。

——ObjectAttribute: 可选项。对象的属性。对于用户对象，有如下属性：

- urn:cdrm:core:node:attribute:friendly-name string;
- urn:cdrm:core:node:attribute:expiration-date int;
- urn:cdrm:core:node:attribute:contextTag string。

——LinkControl: 可选项。域注册控制，可包含如下控制：

- TimeValidityCondition: 时间控制;
- DeviceTypeCondition: 设备类型控制;
- DeviceCapabilityCondition: 设备能力控制;
- FreshnessCondition: 更新条件。

7.6 获取、更新订阅

典型的应用场景中可能要求内容消费者进行内容订阅。此时鉴权服务模块向DRM管理服务器提供订阅信息。终端通过门户导航/EPG或者一个预设的URL获得DRM信令，将该信令传送给DRM管理服务器以获得必要的订阅信息。

鉴权服务模块提供给DRM管理服务器以下三个参数：

——SubscriptionID: 必选项。这是一个订阅对象 ID，在订阅层对象中，该对象应唯一。类型是：“string”，其值为“subscription”。

——ObjectAttribute: 可选项。对象的属性。对于对象，有如下属性：

- urn:cdrm:core:node:attribute:friendly-name string;
- urn:cdrm:core:node:attribute:expiration-date int。

——LinkControl: 可选项。订阅控制，可包含如下控制：

- TimeValidityCondition: 时间控制;
- DeviceTypeCondition: 设备类型控制;
- DeviceCapabilityCondition: 设备能力控制;
- FreshnessCondition: 更新条件。

7.7 许可证获取

典型的应用场景中，用户购买或者订阅DRM保护内容时，鉴权管理模块把客户的购买和订阅信息提供给DRM管理服务器。终端通过门户导航/EPG或者一个预设的URL获得DRM信令后，和DRM管理服务器进行通信，用于获得绑定到某个特定的对象的许可证。DRM管理服务器利用必要的订阅和购买信息，从密钥数据库中获得内容密钥，生成相应的许可证，并通过安全协议发放给终端。

鉴权服务模块需要如下二个可选参数和二个必选参数：

a) TargetObjectID: 可选项。如果指定的话，此 ID 应该和请求中的 TargetNodeID 相同。

b) ObjectAttribute: 可选项。许可证的属性。当前唯一可以指定的是许可证的失效日期。一般不和许可证播放控制的失效日期一起使用。其属性为：

urn:cdrm:core:node:attribute:expiration-date int。

c) ContentID: 必选项。内容的 ID，应唯一。可以包含多个内容 ID，对应不同的内容。

d) LicenseRights：必选项。PlaybackControl 和 ControlData 为 LicenseRights 所包含的可选子元素，描述如下：

——LicenseRights 包含子元素 ControlData，它是一段用于控制内容使用的代码，可与 PlaybackControl 元素搭配使用完成对内容的控制。

——PlaybackControl 所支持的回放控制：

- ActionCountCondition: 消费内容次数要求;
- TimeValidityCondition: 时间要求;
- ValidityAfterFirstUseCondition：从第一次使用后多长时间可用;
- DeviceTypeCondition：设备类型要求;
- DeviceCapabilityCondition: 设备兼容性和能力要求;
- FreshnessCondition:更新要求;
- CDRMSpecificationCondition: 对所支持的 DRM 系统的版本的要求;
- ReachableObjectCondition:要求可达的前提，具体是指的除了绑定的对象，还可达的对象 ID，可以是设备、用户、订阅之一;
- ReachableObjectID 要求可达的对象 ID;
- LicenseSuspensionCondition: 许可证撤销前提;
- MeteringObligationCondition: 播放信息反馈要求。

——ControlData 控制数据：为一段控制伪代码，用以实现自定义控制权限。

7.8 用户行为统计信息反馈

终端向DRM管理服务器端发送用户行为统计信息。DRM管理服务器就会把获得的用户行为统计信息提供给鉴权管理服务模块。客户信息反馈包含了一个衍生元素MeteringData。MeteringData元素包含了原始的用户行为统计信息。DRM管理服务器并不会处理这些信息。只是把这些原始的反馈信息作为XML数据直接提交给鉴权管理模块。

7.9 HTTP 传输错误

当DRM管理服务器无法和鉴权模块进行HTTP通信的时候，会得到HTTP错误信息，见表2。

表2 HTTP 错误信息

HTTP 错误代码	异常情况	错误原因
404	资源无法获得	后台鉴权服务 URL 不存在或者后台鉴权服务暂时不可用
503	服务不可用	后台鉴权服务暂时忙、不可用或者未开启
500	内部服务错误	鉴权服务当前已经崩溃或者遇到未定义错误
不等于 200	传输异常	任何其他不等于 200 的未定义错误码（200 代表 http 通信正常）

8 C 类接口——DRM 终端引擎和终端界面应用程序的接口

8.1 定义

终端应用与DRM终端代理之间采用标准计算机编程语言接口。具体包括：引擎初始化、处理行动信令、获取引擎状态信息、评估许可证、安全更新以及引擎终止。终端应至少具有8MB存储用于支持DRM终端存储信息。

C类接口的具体定义见表3。

表3 C 类接口具体定义

名称	输入	输出	描述
GetSdkInfo		代理软件版本信息	获得代理软件版本信息
EngineInitialize	初始化设置	初始化结果	启动终端代理引擎
EnginePersonalize	初始化信令	个性化结果	初始化DRM终端（获得设备证书）
ProcessToken	行动信令	行动结果（注册、注销、订阅、或者获取许可证）	执行行动信令，进行注册、注销、订阅、或者获取许可证等等一切DRM相关操作
LienseAction	许可证文件和需要解密的content ID	评估许可证结果，如果成功，输出内容密钥。如果失败，输出失败原因。	评估许可证
SecurityUpdate	安全更新的设置	安全更新结果	终端安全更新
GetClientInfo		终端状态，比如设备证书，注册、订阅等等。	获得DRM终端状态。
EngineTerminate		关闭结果	关闭终端DRM代理引擎

8.2 文件格式和内容加密算法

文件编码采用MPEG-4和TS格式。内容加密采用AES方法。

对于TS流，采用基于TS净载荷的加扰，而不采用基于PES及ES净载荷的加密。

Content ID在节目映射表（PMT）中的CA_descriptor中关联视/音频表和ECM。不要求EMM和CAT表。PAT表也是必需的。如果有CAT表，也可以在CAT中描述CA_descriptor，定义见表4。

表4 TS流PMT表中CA_descriptor定义

语法	比特占位数	数据类型	值
CA_descriptor(){			
descriptor_tag	8	Uimsbf	9
descriptor_length	9	Uimsbf	
CA_system_ID	16	Uimsbf	
MPEG2_Reserved	3	Bslbf	
CA_PID	13	Uimsbf	
for (i=0;i<N;i++) {			
Private_data_byte	8	Uimsbf	
}			
}			

表中参数解释如下：

——descriptor_tag，使用标准的MPEG标识值9；

——descriptor_length：描述子的长度；

——CA_system_ID：系统ID；

——CA_PID：TS流中的ECM表的PID。

ECM的格式应符合ETSI ETR 289的有关规定。

ECM表变换间隔为1s至120s之间，以整数为单位。ECM中KSM的格式，应符合IEC 62455-2008。

TS音视频加扰应采用密钥128比特的AES算法。加扰密钥为128比特。加扰算法为AES CBC。加扰密钥经过128比特加密后，存储在ECM中。解密加扰密钥的内容密钥从许可证获得，为16个从00～ff的字符串代表的16进制数（0x00～0xff）。

Content ID应符合RFC 2396的有关规定。Content ID在同一频道的切换，需要同时更新必要的PMT。Content ID不宜频繁切换。最小单位应该是一个节目。

为了支持具体IPTV业务中的时移、回看等业务，视频的帧信息，同步信息等数据在加密同时提取出来提供给IPTV平台。这些相关信息封装在RTP数据包中以供IPTV平台的后续处理。

视频压缩采用MPEG-2、H.264或AVS格式。音频压缩采用MPEG、AAC或者DRA格式。

中 华 人 民 共 和 国
广播电影电视行业标准

数字版权管理系统与IPTV集成播控平台接口技术规范

GY/T 246－2011
*
国家广播电影电视总局广播电视规划院出版发行
责任编辑：王佳梅
查询网址：www.abp.gov.cn
北京复兴门外大街二号
联系电话：（010）86093424　　86092923
邮政编码：100866