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　系统合规性要求

Digital rights management of video audio content distribution—
System compliant requirements

（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、中国传媒大学、英特尔（中国）有限公司、上海海思技术有限公司、阿里巴巴（中国）有限公司、华数数字电视传媒集团有限公司、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、北京爱奇艺科技有限公司、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、北京数码视讯科技有限公司、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、上海国茂数字技术有限公司、辽宁广播电视台、上海文化广播影视集团有限公司。

本标准主要起草人：丁文华、郭沛宇、潘晓菲、王磊、林卫国、梅雪莲、梁志坚、王兵、吴迪、隋爱娜、尚文倩、周菁、曹建香、张智军、沈阳、薛子育、姜涛、冯汉文、张玉娟、张杰开、刘梦雨、王媛媛、蒋鹏飞、赵鹏、陈靓、冉大为、邵淇锋、汤毅、刘广宾、陈志业、姜堑、陈赫、陈钢、赵云辉、马吉伟、刘琦、汪沛、郑黎方、张晶、田雪冰、刘好伟、张鹏、范涛、高宏鹏、吴南山。

视音频内容分发数字版权管理　系统合规性要求

1　范围

本标准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。

本标准适用于视音频内容分发数字版权管理系统研发、集成、建设及运行维护。

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。

GB/T 37092—2018　信息安全技术　密码模块安全要求

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

ISO/IEC 27002　信息技术　安全技术　信息安全控制实用守则（Information Technology—Security Techniques—Code of practice for information security controls）

3　术语和定义

下列术语和定义适用于本文件。

3.1

硬件信任根　hardware root of trust

由硬件构成的安全基元，负责提供一组可信的、关键的安全功能。其被设计为始终以预期的方式运行且不可变。

3.2

安全引导加载　secure bootloader

硬件或软件中所包含的指令、数据在被执行之前为其建立一个初始信任状态的过程。通常硬件和增强硬件安全级别的安全引导加载功能被根植于硬件当中。

3.3

硬件执行环境　hardware execution environment；HEE

用于为DRM应用程序强制实施一个安全硬件边界的硬件信任根，可以是一个硬件信任根、一个安全引导加载程序、一个安全操作系统、一个安全处理器或单个处理器的安全运行模式的组合。

3.4

根检测　root detection

当发现设备已遭到破坏，在检测到该设备或设备上的软件区域可被访问的同时，对该设备/软件或其他软件进行隐藏。

3.5

软件执行环境 software execution environment；SEE

用于隔离或保护软件在执行过程中执行环境的一种基于软件的机制。

3.6

专用工具 special tool

被广泛使用的专用电子或软件工具，包含但不限于内存管理器、调试器（例如，基于软件的总线分析器、交互式反汇编器）或反编译器、集成开发环境、编译器、JTAG带探针读写器和类似的软件开发产品。

3.7

用户可访问总线 user accessible bus

为最终用户设计和提供的，允许最终用户升级或访问智能卡、PCMCIA、Cardbus、USB或PCI等有标准插槽或其他即插即用设施的数据总线。

注：用户可访问总线不包括存储总线、CPU总线以及设备内部架构中不允许最终用户访问的类似部分。

4 缩略语

下列缩略语适用于本文件。

CA 认证中心（Certification Authority）

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

CPU 中央处理器（central processing unit）

DASH 用HTTP协议传输的动态自适应流媒体协议（Dynamic Adaptive Streaming over HTTP）

DRM 数字版权管理（Digital Rights Management）

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

HMAC 散列消息验证码（Hashed Message Authentication Code）

JTAG 联合测试工作组（Joint Test Action Group）

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

PC 个人计算机（Personal Computer）

PCI 定义局部总线的标准（Peripheral Component Interconnect）

PCMCIA 个人计算机卡（Personal Computer Memory Card International Association）

TS 传送流（transport stream）

USB 通用串行总线（Universal Serial Bus）

5 概述

视音频内容分发数字版权管理系统合规性要求包括DRM产品合规性要求和DRM系统实施合规性要求。

DRM产品合规性要求用于指导DRM服务端产品研发集成，以及DRM客户端在终端设备中的集成，主要包括：功能要求、标准符合性要求和安全要求。

DRM系统实施合规性要求用于指导DRM系统集成建设和运行维护，主要指实施中的安全要求。

6 DRM服务端产品合规性要求

6.1 功能要求

DRM服务端产品的功能应包括直播内容加密、点播内容加密、密钥管理、密钥网关和内容授权等五个方面，具体要求如下：

a) 直播内容加密：
   1) 应支持实时 TS、HLS、DASH、CMAF 等直播内容加密封装中的一种或多种；
   2) 应支持 AVS+、AVS2、H.264、H.265 等视频编码格式；
   3) 应支持通过密钥管理申请直播内容加密密钥；
   4) 应支持直播加密密钥按照可配置的频率更新；
   5) 直播加密延时应不高于 500ms；
   6) 应支持秒级内容加密密钥更新频率。
b) 点播内容加密：
   1) 应支持 TS 文件、HLS、DASH、CMAF 等内容加密封装中的一种或多种；
   2) 应支持 AVS+、AVS2、H.264、H.265 等视频编码格式；
   3) 应支持通过密钥管理申请点播内容加密密钥。
c) 密钥管理：
   1) 应支持接收处理内容加密密钥申请；
   2) 应支持安全存储管理内容加密密钥；
   3) 应支持同步内容加密密钥到密钥网关。
d) 密钥网关：
   1) 应支持接收处理密钥管理的直播/点播内容加密密钥请求；
   2) 应支持安全存储管理直播/点播内容加密密钥；
   3) 应支持接收处理内容授权直播/点播内容加密密钥请求。
e) 内容授权：
   1) 应支持接收处理 DRM 客户端直播/点播内容授权许可证请求；
   2) 应支持从密钥网关请求直播/点播内容加密密钥。

6.2 标准符合性要求

DRM服务端产品的标准符合性要求包括直播内容加密、点播内容加密、密钥管理、密钥网关和内容授权等五个方面，具体要求如下：

a) 直播内容加密：
   1) 直播内容加密应符合 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 7.1.1 和 7.2 的规定；
   2) 直播内容加密密钥申请应符合 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 8.1 的规定。
b) 点播内容加密：
   1) 点播内容加密应符合 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 7.1.2 和 7.2 的规定；
   2) 点播内容加密任务管理应符合 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 7.3 的规定；

3) 点播内容加密密钥申请应符合 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 8.2 的规定。

c) 密钥管理：
1) 直播密钥管理应符合 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 8.1 的规定；
2) 点播密钥管理应符合 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 8.2 的规定。

d) 密钥网关：
1) 密钥同步应符合 GY/T 277—2019 中 9.2 的规定；
2) 密钥查询应符合 GY/T 277—2019 中 9.3 的规定。

e) 内容授权：
1) 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；
2) 密钥查询应符合 GY/T 277—2019 中 9.3 的规定。

6.3 安全要求

6.3.1 基本安全要求

DRM服务端产品基本安全要求如下：

a) 应安全保护附录 A 中规定的有保密性要求和完整性要求的值；
b) 应支持基于设备公私钥对生成和存储；
c) 加解密、签名等密码运算功能应在硬件密码模块中实现；
d) 设备私钥、内容加密密钥、会话密钥、临时密钥等不应将明文暴露在硬件密码模块之外；
e) 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，且具备商用密码型号证书。

6.3.2 软件安全要求

DRM服务端产品软件安全要求如下：

a) DRM 服务端软件应具备硬件密码模块识别机制，硬件密码模块移除时应停止服务；
b) DRM 服务端软件应具备软件组件完整性校验机制，软件组件被篡改后应停止服务；
c) DRM 服务端软件应支持安全日志记录和日志审查，DRM 服务端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均应安全记录；
d) DRM 服务端应具备安全升级机制，在出现新的安全风险或安全漏洞时应能及时进行安全修复。

6.3.3 安全威胁应对要求

DRM服务端产品至少应能处理以下安全威胁：

a) 物理威胁：
1) 通过意外事件或设计破坏部分或所有的系统组件；
2) 通过物理断开或其他物理干预损害可用性；
3) 中断电源和网络连接；
4) 使用协议分析器等对本地网络进行窃听。

b) 逻辑威胁：
1) 通过控制台或网络终端进行未经授权的访问；
2) 中间人攻击；

3） 破坏密钥信息；
4） 在系统组件上安装窃听设施；
5） 不正确或未经授权地创建、修改或删除用户账户；
6） 不正确或未经授权地创建、修改或删除数据库内容；
7） 不正确或未经授权地创建、修改或删除数据库访问控制；
8） 操作系统或应用程序中的故障；
9） 软件的错误配置。

c） 运行威胁：
1） 利用输入控制（缓冲区溢出）破坏可用性和升级权限；
2） 未经授权获取密码和明文；
3） 未经授权修改运行日志文件；
4） 通过虚假身份获得未经授权的访问。

7 DRM客户端产品合规性要求

7.1 功能要求

DRM客户端产品功能要求如下：

a） 应支持直播/点播内容授权许可证申请；
b） 应支持直播/点播内容授权许可证解析；
c） 应支持直播/点播内容安全解密、解码、播放和输出。

7.2 标准符合性要求

DRM客户端产品标准符合性要求如下：

a） 直播内容解密应符合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7.1.1和7.2的规定；
b） 点播内容解密应符合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7.1.2和7.2的规定；
c） 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；
d） DRM客户端应符合GY/T 277—2019中第10章的规定；
e） DRM客户端功能接口应符合GY/T 277—2019中附录C的规定；
f） DRM客户端运行环境接口应符合GY/T 277—2019中附录D的规定。

7.3 安全要求

7.3.1 基本安全要求

DRM客户端产品基本安全要求如下：

a） DRM客户端功能模块应安全运行在DRM客户端运行环境中，DRM客户端运行环境应具备保护DRM客户端功能模块完整性的能力，DRM客户端功能模块被篡改后，应能停止其工作；
b） DRM客户端运行环境应安全保护附录A中有保密要求的值和有完整性要求的值,有完整性要求的值被篡改后应停止DRM客户端功能模块；
c） 受保护内容应在DRM客户端执行环境中按照内容授权许可证的要求安全解密、解码、播放和输出；
d） 针对有DRM保护要求的内容，终端设备不应绕过DRM客户端功能；

e） 终端设备应具备DRM客户端安全升级能力，当出现新的安全漏洞时应能及时升级DRM客户端，不应存在官方所公布的6个月之内的漏洞。

7.3.2 软件执行环境（SEE）安全要求

当DRM客户端运行环境为软件执行环境时，安全要求如下：

a） 对已解密的内容数据和有保密要求的值应进行安全保护以抵御未经授权的泄露（例如，在任何用户可访问总线上对解密的内容数据进行加密、在系统内存中对解密的内容数据和有保密要求的值进行加密、通过访问控制对驻留在内存中的已解密的内容数据和有保密要求的参数值进行隔离）。

b） 将与特定设备相关有保密要求的值与该设备进行有效且唯一的关联（例如，使用一个设备里独有的密钥对值进行加密）。

c） 未加密内容数据或有保密要求的值在从SEE输出前，应确保存储它们的内存或缓冲区被清除。

d） 设备应能确保解密后的视音频数据及后续数据内容通过视频链路进行视频处理。视频链路中可能包括非混淆处理的硬件加速器，在视频链路中可使用基于软件的安全保护技术进行保护，从而使不受SEE控制的系统软件和硬件组件无法对已解密的视频数据进行访问。基于软件的安全保护技术包括混淆技术、根检测、调试检测等。解密后的压缩数据应仅能存储在SEE控制下的内存当中，且只能由SEE控制下的功能对其进行访问。

e） SEE应实施软件强制执行机制，对DRM客户端中执行核心功能的部分进行完整性验证，并采取其他可确保该部分完整性的措施来保护DRM客户端中执行核心功能的部分不会遭受到未经授权的修改。软件强制执行机制在设计时还应能确保，一旦发生未经授权的修改，核心功能将不可被执行，企图删除、置换或重新编程软件的行为也将失败，否则这些行为将严重危及DRM客户端的安全保护要求，使DRM客户端无法接收、解密、解码、播放视音频内容。

f） 当DRM客户端运行环境为软件环境时，在安全引导加载程序内应对可更新固件进行签名校验，检查调试器，检查SEE功能的接口的系统权限控制（如根检测），以及采用混淆技术和白盒加密技术，有效防范逆向工程攻击。

g） 当DRM客户端运行环境为软件执行环境时，DRM客户端运行环境可能会存在被具备相关专业技能的人员恶意破解的风险，但通过常用工具或专用工具应无法破解DRM客户端运行环境。

7.3.3 硬件执行环境（HEE）安全要求

当DRM客户端运行环境为硬件执行环境时，安全要求如下：

a） 对解密后的内容数据和有保密要求的值应进行安全保护以防止未经授权的暴露（例如，在任何用户可访问总线或缓存上对解密后的内容数据进行加密、在系统存储器和缓存中对解密后的内容数据和有保密要求的值进行加密、通过访问控制对驻留在内存中的已解密的内容数据或有保密要求的值进行隔离、仅在一个安全处理器内或运行于安全模式下的处理器内使用有保密要求的值、对特定设备有保密要求的值嵌入到该设备的硅电路或固件当中以防止对其的读取）；应防止运行在HEE之外程序对未加密且有保密要求的值进行访问，除进行解密操作外，有保密要求的值应保存在HEE内，且不应在HEE内存驻留。

b） 应确保有保密要求的值具备有效性、唯一性，且与设备关联（例如，通过使用某个单个设备的唯一密钥对值进行加密的方式完成关联）。

c） 未加密的内容数据或有保密要求的值在从硬件执行环境输出前，要确保存储它们的内存或缓冲区被清空。

d） 设备应能确保解密后的视音频数据及后续数据内容通过视频链路进行视频处理。视频链路中可能包括非混淆处理的硬件加速器，在视频链路中可使用基于硬件的安全保护技术进行保护，从

而使不受HEE控制的系统软件和硬件组件无法对已解密的视频数据进行访问。解密后的压缩数据应仅能存储在HEE控制下的内存当中，只能由HEE控制下的解码器功能对其进行访问。解密后的解压缩数据应只能存储在HEE控制下的内存当中，只能由HEE控制下的功能访问。

e) 安全引导加载要求如下：
   1) 任何在 HEE 中执行的代码应通过硬件信任根予以验证。设备应始终被引导至一个被定义好的安全启动流程当中并永远不会引导至一个调试流程；
   2) 所有 HEE 及与安全性相关的代码应只能通过 HEE 的私有资产予以执行；
   3) 应防止高级别或一般用途的操作系统对任何与安全性相关的资产（包括任何密钥、安全元素或受保护的内容）进行访问；
   4) 任何用于验证安全性相关的资产是否被授权的密钥数据（例如，公钥和与公钥相关的数据）应予以保护，防止其被设备上执行的软件修改、置换或重定向；
   5) 维持保密性，即调试模式无法对任何与安全性相关的数据进行访问。调试工具应不能损害安全性数据。
f) HEE通过根植于硬件信任根当中的硬件强制执行机制，对DRM客户端中执行核心功能的部分进行完整性验证，并采取其他可确保该部分完整性的措施来保护DRM客户端中执行核心功能的部分不会遭受到未经授权的修改。硬件强制执行机制应包括对执行核心功能的部分的安全引导加载，并在设计时还应能确保一旦发生未经授权的修改，核心功能将不可被执行，企图删除、置换或重新编程硬件的行为也将失败，否则这类行为将严重危及DRM客户端的内容安全保护要求，从而导致DRM客户端无法接收、解密、解码、播放或复制内容数据。在安全引导加载程序内对可更新固件进行签名校验就是实现上述要求很好的例证。任何在硬件执行环境中使用的未加密的内存数据在被不可信代码或其他不可信的应用程序读取之前应予以清空。
g) 当DRM客户端运行环境为硬件执行环境时，DRM客户端运行环境可能存在被具备相关专业技能的人员恶意破解的风险，但通过使用常见工具、专用工具、软件工具（如反编译程序、加载程序、补丁或其他软件工具）应无法破解DRM客户端运行环境。

7.3.4 DRM 时间

DRM客户端可使用任何可用的时间同步机制，但应保证时间源和同步机制合理准确，且能够抵御最终用户的恶意修改。DRM客户端应能够保持时钟的之前状态并能够检测到丢失DRM时间的记录，例如电源故障等原因导致的DRM时间的丢失。

为了使用户能够合法地消费受时间约束的内容，在没有其他的同步机制可用时，DRM客户端应能够基于任何时间源（包括用户可控时钟）设置其自己的DRM时间且DRM客户端应尝试尽快将其DRM时间与一个已授权的时间源进行同步，在未实现时间同步之前，基于时间的内容授权许可证应处在不可用状态。DRM客户端在设计时应能够对DRM时间予以保护以防止未经授权的修改。

7.3.5 现场升级

如果DRM的使用者同意，其所有的DRM客户端（不包括PC）均应能进行现场升级。为此，应部署一个适用于任何现场升级所需的基础构架，使现场升级能够通过在线分发方式或其他与在线分发具有相同功效的方式部署到DRM客户端当中。当一个DRM客户端在软件中实现核心功能时，该软件应具备现场升级的能力以修改此核心功能的实现。现场升级应能够有效抵御未经授权的修改或置换企图，且应能够提供安全更新流程。

用于现场升级的验证机制应达到128位对称安全性级别，或至少达到与2048位RSA非对称安全性级别相当的级别（例如RSA）。如果当前设备无法达到1024位RSA非对称安全级别，则此条要求可豁免，但2048位的要求仍保持不变。对下载固件的完整性保护应贯穿固件的整个生命周期，从设计到创建、从签名到

下载并最终安装到设备上。在不限制前述规定的前提下，设备应能够检测和防止所存储信息的回滚。如果检测到回滚，代码的执行应能够阻止安全的DRM兼容软件、固件进行升级。

7.3.6 取证水印

如果被许可的内容包含取证水印，则DRM客户端不应干扰该标记。如果设备具备向内容中嵌入取证水印的功能，则这些功能应在HEE的控制下被执行。

7.3.7 侧信道防御

侧信道防御是指能够抵抗加密密钥、有安全需求的资产等保密信息泄露给外部观察者的加密计算方法或算法及其硬件、固件或软件实现，这些外部观察者可以使用的侧信道攻击手段包括：

a) 功耗变量攻击；
b) 电磁攻击；
c) 时间攻击；
d) 噪声干扰；
e) 故障/功耗干扰；
f) 时钟干扰；
g) 电磁/激光干扰；
h) 差分故障分析；
i) 数据残留攻击；
j) Row Hammer漏洞攻击。

加密算法的实现需要考虑针对侧信道攻击的防御对策，使攻击者难以进行商业上可行的侧信道攻击以提取机密信息。一般来说，需防护的侧信道攻击包括但不限于简单功耗分析（SPA）、差分功耗分析（DPA）、简单电磁分析（SEMA）、差分电磁分析（DEMA）、模板分析（TA）和使用标准或特定的设备对一定数量的能量迹进行跟踪的时间攻击。

7.3.8 DRM 客户端安全等级划分规则

基于DRM客户端安全要求，DRM客户端分为三个安全级别：软件安全级别、硬件安全级别和增强硬件安全级别。

软件安全级别：DRM客户端功能模块的功能应在SEE中实现，未在SEE中实现的功能应在HEE中实现。

硬件安全级别：DRM客户端功能模块的功能均应在HEE中实现。

增强硬件安全级别：DRM客户端功能模块的功能均应在HEE中实现，同时还应具备侧信道防御、取证水印等功能。

DRM客户端安全等级划分规则见表1。

表1 DRM 客户端安全等级划分规则

安全要求	类别		
	软件安全级别	硬件安全级别	增强硬件安全级别
基本要求	适用	适用	适用
软件执行环境（SEE）安全要求	适用	不适用	不适用
硬件执行环境（HEE）安全要求	可选	适用	适用
DRM时间	不适用	适用	适用
现场升级	适用	适用	适用

表 1（续）

安全要求	类别		
	软件安全级别	硬件安全级别	增强硬件安全级别
取证水印	可选	可选	适用
侧信道防御	可选	可选	适用

8 DRM 系统实施合规性要求

8.1 概述

DRM系统实施应采用符合第6章和第7章规定的DRM服务端和DRM客户端，同时应满足8.2中的规定。

8.2 DRM 系统实施安全要求

8.2.1 DRM 服务端私钥的复制

在DRM系统实施过程中，出于性能原因的考虑，DRM服务端可在特定的物理设备或模块中生成DRM服务端私钥的副本，并可为安全脱机存储创建DRM服务端私钥的备份副本。DRM服务端私钥的这些副本应符合本章的要求，即，这些副本的安全性应与在DRM服务端设施内安全生成的原始DRM服务端私钥相同。当不再需要这些DRM服务端私钥的副本时，DRM服务端应立即安全地销毁它们。

8.2.2 责任

DRM服务端设备对所有驻留有私钥的系统的访问,特别是对DRM服务端私钥自身的所有访问都应记录在案。此外，DRM服务端私钥副本的所有复制和销毁也应记录在案。

DRM服务端或其他检查机构应能通过对日志文件的检查获知在此前任一时刻有多少个DRM服务端私钥的副本存在于何处，且应有审计工具用于对日志文件进行取证检查，也应采取有效措施确保日志文件的完整性。

8.2.3 控制

DRM服务端应具备控制功能以降低风险。DRM服务端应根据其安全功能对系统组件进行定义，并相应地控制这些组件间的交互。

8.2.4 策略

DRM服务端应创建、实施和维护关于安全目标和方法的策略，此策略应与ISO/IEC 27002保持一致。

8.2.5 标准和流程

DRM系统应创建、实施和维护一套安全标准和流程，详细说明上述策略是如何实施的。这些标准和流程应与ISO/IEC 27002保持一致。

8.2.6 风险登记

DRM系统应维护一个风险登记册，列出超出DRM服务端所实施的控制范围之外的风险。DRM服务端应确保风险登记册保持最新的状态。

8.2.7 运行

DRM系统的实施方应能够生成定期的审计报告以评估其对安全技术要求的符合性。在评定DRM系统是否满足这一要求时，应考虑到DRM系统的物理安全性、运行策略、标准和流程，按要求对相关文件进行查阅。

附 录 A
（规范性附录）
DRM 系统有保密性要求的值和有完整性要求的值

A.1 DRM服务端有保密性要求的值

DRM服务端有保密性要求的值如下：

a) DRM服务端私钥；
b) 内容加密密钥；
c) 会话密钥等密钥加密密钥；
d) 许可证加密密钥；
e) HMAC密钥。

A.2 DRM服务端有完整性要求的值

DRM服务端有完整性要求的值如下：

a) 设备详细信息；
b) GY/T 277—2019中定义的根CA证书、DRM服务端子CA证书、DRM服务端证书、DRM客户端子CA证书、DRM客户端证书、OCSP证书；
c) DRM服务端与DRM客户端之间达成的协议参数、协议版本；
d) OCSP响应；
e) 内容授权许可证对象；
f) 内容授权许可证对象状态元素。

A.3 DRM客户端有保密性要求的值

DRM客户端有保密性要求的值如下：

a) DRM客户端私钥；
b) 内容加密密钥；
c) 会话密钥等密钥加密密钥；
d) 许可证加密密钥；
e) HMAC密钥；
f) 用于随机数生成器的任何种子值；
g) 随机数生成器的输出值。

A.4 DRM客户端有完整性要求的值

DRM客户端有完整性要求的值如下：

a) 设备详细信息；
b) GY/T 277—2019中定义的根CA证书、DRM服务端子CA证书、DRM服务端证书、DRM客户端子CA证书、DRM客户端证书、OCSP证书；

c） DRM服务端与DRM客户端之间达成的协议参数、协议版本；
d） DRM服务端唯一标识；
e） OCSP响应；
f） 内容授权许可证对象；
g） 内容授权许可证对象状态元素；
h） 撤销数据；
i） 序号；
j） DRM时间状态。