GY

中华人民共和国广播电视和网络视听行业标准

GY/T 335—2020

视音频内容分发数字版权管理　标准符合性测试

Digital rights management for video audio content distribution — Standard compliance test

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。

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、中国传媒大学、上海海思技术有限公司、英特尔（中国）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。

本文件主要起草人：丁文华、郭沛宇、林卫国、王磊、王兵、隋爱娜、尚文倩、周菁、曹建香、梁志坚、梅雪莲、吴迪、沈阳、张智军、薛子育、张杰开、刘梦雨、王慧琴、冯汉文、姜涛、王媛媛、蒋鹏飞、张玉娟、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　标准符合性测试

1　范围

本文件规定了GY/T 277—2019的符合性测试内容和测试方法。

本文件适用于GY/T 277—2019的符合性测试。

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

3　术语和定义

GY/T 277—2019界定的以及下列术语和定义适用于本文件。

3.1

内容加密服务器　content encryption server

DRM服务端中加密数字媒体内容的实体，实现形式包括但不限于专用设备、软件服务等。

3.2

内容授权服务器　content authorization server

DRM服务端中从密钥网关查询内容加密密钥并封装成许可证发送给DRM客户端的实体，实现形式包括但不限于专用设备、软件服务等。

3.3

密钥管理服务器　key management server

DRM服务端中负责接收内容加密服务器的内容加密密钥信息并进行安全存储和发布的实体，实现形式包括但不限于专用设备、软件服务等。

3.4

密钥网关服务器　key gateway server

DRM服务端中负责接收密钥管理服务器同步的内容加密密钥，并接收内容授权服务器的密钥查询的实体，实现形式包括但不限于专用设备、软件服务等。

3.5

OCSP服务器　OCSP server

向DRM服务端提供OCSP响应的实体，实现形式包括但不限于专用设备、软件服务等。

3.6

测试平台 testing platform

对视音频内容分发数字版权管理系统进行标准符合性测试的平台。

4 缩略语

下列缩略语适用于本文件。

CA 认证中心(Certification Authority)

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）

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）

HTTP 超文本传输协议（Hyper Text Transport Protocol）

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

ID 唯一标识（Identifier）

MPD 媒体展现描述（Media Presentation Description）

MPEG 动态图像专家组（Moving Picture Experts Group）

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）

5 概述

视音频内容分发数字版权管理系统标准符合性测试包括：内容加密方法和格式封装测试、内容授权服务器测试、密钥管理服务器测试、密钥网关服务器测试、DRM客户端测试五部分。视音频内容分发数字版权管理系统标准符合性测试框架如图1所示。

内容加密方法和格式封装测试主要测试内容加密服务器加密功能以及封装格式的标准符合性；内容授权服务器测试主要测试内容授权服务器从密钥网关查询内容加密密钥的消息协议标准符合性，以及封装许可证发送给DRM客户端的许可证获取协议标准符合性；密钥管理服务器测试主要测试密钥管理服务器向密钥网关服务器同步密钥的消息协议标准符合性；密钥网关服务器测试主要测试密钥网关服务器接收密钥管理服务器的同步内容加密密钥的消息协议标准符合性，以及接收内容授权服务器的密钥查询消息协议的标准符合性；DRM客户端测试主要测试DRM客户端的许可证获取协议标准符合性以及功能测试。

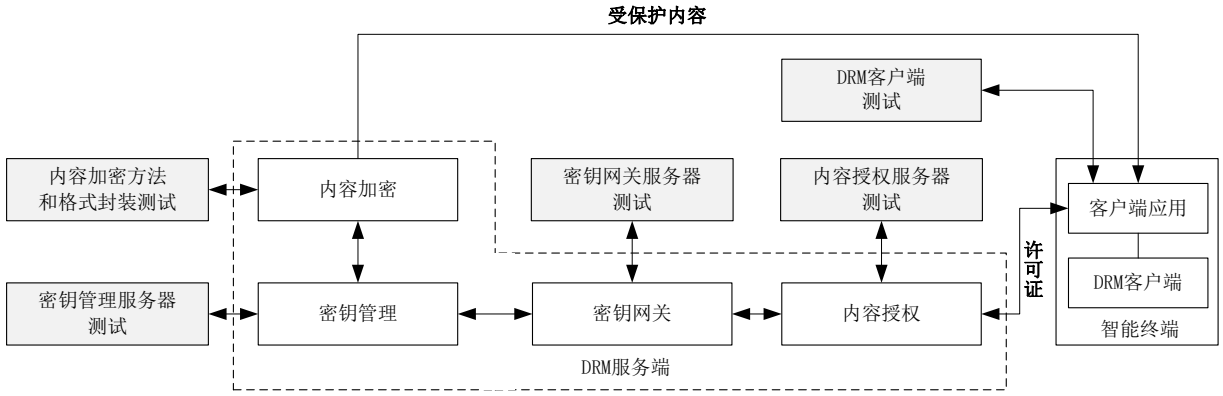

图1　视音频内容分发数字版权管理系统标准符合性测试框架

6　标准符合性测试内容

6.1　内容加密方法

6.1.1　概述

系统中受保护的数字内容应符合GY/T 277—2019第6章规定的内容加密封装要求，加密后的内容流或媒体描述文件中应包含内容标识及获取许可证的信息。加密后的内容基本码流的扩展数据中应含有内容加密信息CEI用来指明随后的视频是如何被加密的。CEI中应包括加密标识符、当前内容加密密钥标识符、下一个内容加密密钥标识符、以及当前内容加密密钥对应的初始向量等。具体CEI语法要求应符合GY/T 277—2019中表1的语法格式。CEI_DATA、加密后的编码数据为防止起始码二义冲突，需要进行转换，转换规则须符合GY/T 277—2019中6.2.5的要求。

6.1.2　TS 封装方式

采用MPEG-TS封装格式传输时，应在PMT表中设置DRM描述子结构，描述子中应指明加密内容格式、加密方式、许可证获取URI等信息。具体DRM描述子语法格式应符合GY/T 277—2019中表3的规定，其中加密内容的视频编码格式字段取值范围应符合GY/T 277—2019中表4的规定；视频内容加密的方式应符合GY/T 277—2019中表5的规定。

对于AVS/AVS2编码的内容，内容加密方法应符合GY/T 277—2019中6.2.1和6.2.2的要求，内容封装格式应符合GY/T 277—2019中6.3.1的要求。

对于H.264编码的内容，内容加密方法应符合GY/T 277—2019中6.2.1和6.2.3的要求，内容封装格式应符合GY/T 277—2019中6.3.1的要求。

对于H.265编码的内容，内容加密方法应该符合GY/T 277—2019中6.2.1和6.2.4的要求，内容封装格式应符合GY/T 277—2019中6.3.1的要求。

6.1.3　MPEG-DASH

对于采用DASH协议分发的内容，内容封装格式应符合GY/T 277—2019中6.3.2的要求，内容加密格式应符合GY/T 277—2019中6.3.3的要求。

对于H.264编码的内容，加密方法应符合GY/T 277—2019中6.2.1和6.2.3要求；对于H.265编码的内容，加密方法应符合GY/T 277—2019中6.2.1和6.2.4要求。

6.1.4 HLS

对于采用HLS协议分发的内容，内容封装格式应符合GY/T 277—2019中6.3.4要求。

对于H.264编码的内容，加密方法应符合GY/T 277—2019中6.2.1和6.2.3要求；对于H.265编码的内容，加密方法应符合GY/T 277—2019中6.2.1和6.2.4要求。

6.2 许可证格式

许可证格式应符合GY/T 277—2019中7.1的规定。

许可证编码应符合GY/T 277—2019中7.2的规定。

6.3 许可证获取协议

6.3.1 许可证获取请求

DRM客户端发送给内容授权服务器的许可证获取请求消息格式应符合GY/T 277—2019中8.2的规定。

当DRM客户端发送非法请求时，内容授权服务器应具备异常容错机制，可能的状态信息应符合GY/T 277—2019中8.4的规定。

6.3.2 许可证获取响应

内容授权服务器发送给DRM客户端的许可证获取响应消息格式应符合GY/T 277—2019中8.3的规定。

当内容授权服务器发送非法响应时，DRM客户端应具备异常容错机制，可能的状态信息应符合GY/T 277—2019中8.4的规定。

6.3.3 消息签名机制

DRM客户端与内容授权服务器之间的许可证获取协议中,DRM客户端发送的许可证获取请求以及内容授权服务器发送的许可证获取响应均需要采用消息签名机制，该消息签名机制应符合GY/T 277—2019中8.5的要求。

6.4 DRM 服务端

6.4.1 密钥同步协议

密钥同步是指密钥管理服务器将直播或点播内容加密密钥同步到密钥网关服务器。密钥同步应包括密钥同步请求和密钥同步响应两条消息。

密钥同步请求消息格式、编码应符合GY/T 277—2019中9.2.2的规定。

密钥同步响应消息格式、编码应符合GY/T 277—2019中9.2.3的规定。

6.4.2 密钥查询协议

密钥查询是指内容授权服务器从密钥网关服务器查询获取DRM客户端需要的内容加密密钥。密钥查询协议应包括密钥查询请求和密钥查询响应两条消息。

密钥查询请求消息格式、编码应符合GY/T 277—2019中9.3.2的规定。

密钥查询响应消息格式、编码应符合GY/T 277—2019中9.3.3的规定。

6.5 DRM 客户端

DRM客户端是设备中的可信实体，负责执行与DRM内容相关的许可和使用。

DRM客户端应按照许可证中密钥使用规则的规定正确使用内容，许可证获取请求消息格式应符合GY/T 277—2019中8.2的规定，许可证获取响应消息应符合GY/T 277—2019中8.3的规定。

7 标准符合性测试

7.1 概述

标准符合性测试分为产品功能标准符合性测试和系统运行标准符合性测试。

产品功能标准符合性测试指采用仿真某一个实体对与其交互的另一个实体进行测试，如：在许可证获取协议中仿真内容授权服务器对DRM客户端进行测试。

系统运行标准符合性测试指在系统运行过程中采用捕获系统中进行交互的两个实体间的通信消息进行测试。系统运行标准符合性测试适用于产品部署后对DRM系统部分或全部进行测试。

7.2 产品功能标准符合性测试

7.2.1 内容加密方法和封装格式测试

内容加密方法和封装格式测试由直播场景测试和点播场景测试两个部分组成，其中直播场景测试是在电视直播和流媒体直播等形式下进行的测试，点播场景测试是在流媒体点播等形式下进行的测试，测试内容均包括对视音频内容的加密方法和封装格式的符合性测试。

直播场景和点播场景测试按封装方式可分为MPEG-TS、DASH和HLS三种封装格式，每种封装格式可封装不同的编码方式，MPEG-TS可封装AVS+、AVS2、H.264和H.265四种编码方式的视频内容，DASH、HLS可封装H.264和H.265两种编码方式的视频内容，每种编码方式又采用两种不同的加密方式SM4-CBC和SM4-SAMPLE加密。

内容加密方法和封装格式标准符合性测试方法见附录A中的A.1。

7.2.2 许可证格式和获取协议测试

许可证格式和获取协议测试主要针对内容授权服务器与DRM客户端之间许可证获取以及许可证格式进行测试。该部分方法主要分为两部分，包括内容授权服务器测试和DRM客户端测试，分别对正确和各种错误情况下的许可证获取以及各种许可证格式进行测试。

许可证格式和获取协议标准符合性测试方法见A.2。

7.2.3 密钥同步与密钥查询协议测试

密钥同步测试主要针对密钥管理服务器与密钥网关服务器之间的密钥同步进行测试，密钥查询测试主要针对内容授权服务器和密钥网关服务器之间的密钥查询进行测试。该部分测试方法在实验室测试环境下针对DRM服务端的密钥网关服务器、密钥管理服务器、内容授权服务器进行测试，分别对正确和各种错误情况下的密钥同步和密钥查询进行测试。

密钥同步与密钥查询协议标准符合性测试方法见 A.3。

7.3 系统运行标准符合性测试

系统运行标准符合性测试采用捕获系统中进行交互的两个实体间的通信消息进行测试，用于产品部署后对系统（此处系统既可是DRM完整系统也可是完成特定功能的DRM子系统）进行测试，测试过程中执行附录B中所有测试方法，标准符合性测试平台将记录测试过程中的相关消息，通过对测试平台记录的消息的分析，实现对内容加密方法和封装格式、许可证获取、密钥同步与密钥查询的标准符合性测试。

系统运行标准符合性测试方法见附录B。

附 录 A
（规范性）
产品功能标准符合性测试方法

A.1 内容加密方法和封装格式测试

A.1.1 直播场景测试

A.1.1.1 对采用MPEG-TS协议封装的AVS+编码的直播流使用SM4-CBC加密的测试方法如下：

测试编号	Content_001	项目属性	必选
测试对象	内容加密服务器		
测试描述	测试内容加密服务器对采用MPEG-TS协议封装的AVS+编码的TS直播流采用SM4-CBC加密方式的加密功能。		
预置条件	设备： a) 内容加密服务器； b) DRM客户端（测试平台）。 状态： a) 已存在待测未加密AVS+编码的TS直播流； b) 已知待测TS直播流的URL； c) 已获得加密TS直播流对应的密钥。		
测试步骤	a) 内容加密服务器采用SM4-CBC加密方式和对应密钥加密待测未加密AVS+编码的TS直播流，生成AVS+编码SM4-CBC加密的TS直播流并上传到URL； b) DRM客户端从URL接收加密TS直播流； c) 解析该TS直播流，从ChinaDRM描述子和CEI字段分别提取出视频序列的加密方法（SM4-CBC）、编码方法（AVS+）等字段信息，以及被加密的视音频内容； d) 结合加密密钥调用对应的解密算法（SM4-CBC）解密被加密的视音频内容并播放。		
符合性判定	a) 通过解析结果显示，TS直播流中加密方法符合GY/T 277—2019中6.2.1和6.2.2的规定，封装格式符合GY/T 277—2019中6.3.1的规定； b) 通过使用对应加密的密钥解密成功播放表明，加密算法符合GY/T 277—2019中6.2.2 CBC模式语法的规定。		

A.1.1.2 对采用MPEG-TS协议封装的AVS+编码直播流使用SM4-SAMPLE加密的测试方法如下：

测试编号	Content_002	项目属性	必选
测试对象	内容加密服务器		
测试描述	测试内容加密服务器对采用MPEG-TS协议封装的AVS+编码TS直播流采用SM4-SAMPLE加密方式的加密功能。		

预置条件	设备： a) 内容加密服务器； b) DRM客户端（测试平台）。 状态： a) 已存在待测未加密AVS+编码的TS直播流； b) 已知待测TS直播流的URL； c) 已获得加密TS直播流对应的密钥。
测试步骤	a) 内容加密服务器采用SM4-SAMPLE加密方式和对应密钥加密待测未加密AVS+编码的TS直播流，生成AVS+编码SM4-SAMPLE加密的TS直播流并上传到URL； b) DRM客户端从URL接收加密TS直播流； c) 解析该TS直播流，从ChinaDRM描述子和CEI字段分别提取出视频序列的加密方法（SM4-SAMPLE）、编码方法（AVS+）等字段信息，以及被加密的视音频内容； d) 结合加密密钥调用对应的解密算法（SM4-SAMPLE）解密被加密的视音频内容并播放。
符合性判定	a) 通过解析结果显示，TS直播流中加密方法符合GY/T 277—2019中6.2.1和6.2.2的规定，封装格式符合GY/T 277—2019中6.3.1的规定； b) 通过使用对应加密的密钥解密成功播放表明，加密算法符合GY/T 277—2019中6.2.2 SAMPLE模式语法的规定。

A.1.1.3 对采用MPEG-TS协议封装的AVS2编码直播流使用SM4-CBC加密的测试方法如下：

测试编号	Content_003	项目属性	必选
测试对象	内容加密服务器		
测试描述	测试内容加密服务器对采用MPEG-TS协议封装的AVS2编码TS直播流采用SM4-CBC加密方式的加密功能。		
预置条件	设备： a) 内容加密服务器； b) DRM客户端（测试平台）。 状态： a) 已存在待测未加密AVS2编码的TS直播流； b) 已知待测TS直播流的URL； c) 已获得加密TS直播流对应的密钥。		
测试步骤	a) 内容加密服务器采用SM4-CBC加密方式和对应密钥加密待测未加密AVS2编码的TS直播流，生成AVS2编码SM4-CBC加密的TS直播流并上传到URL； b) DRM客户端从URL接收加密TS直播流； c) 解析该TS直播流，从ChinaDRM描述子和CEI字段分别提取出视频序列的加密方法（SM4-CBC）、编码方法（AVS2）等字段信息，以及被加密的视音频内容； d) 结合加密密钥调用对应的解密算法（SM4-CBC）解密被加密的视音频内容并播放。		
符合性判定	a) 通过解析结果显示，TS直播流中加密方法符合GY/T 277—2019中6.2.1和6.2.2的规定，封装格式符合GY/T 277—2019中6.3.1的规定； b) 通过使用对应加密的密钥解密成功播放表明，加密算法符合GY/T 277—2019中6.2.2 CBC模式语法的规定。		

A.1.1.4 对采用MPEG-TS协议封装的AVS2编码直播流使用SM4-SAMPLE加密的测试方法如下：

测试编号	Content_004	项目属性	必选
测试对象	内容加密服务器		
测试描述	测试内容加密服务器对采用MPEG-TS协议封装的AVS2编码TS直播流采用SM4-SAMPLE加密方式的加密功能。		
预置条件	设备： a) 内容加密服务器； b) DRM客户端（测试平台）。 状态： a) 已存在待测未加密AVS2编码的TS直播流； b) 已知待测TS直播流的URL； c) 已获得加密TS直播流对应的密钥。		
测试步骤	a) 内容加密服务器采用SM4-SAMPLE加密方式和对应密钥加密待测未加密AVS2编码的TS直播流，生成AVS2编码SM4-SAMPLE加密的TS直播流并上传到URL； b) DRM客户端从URL接收加密TS直播流； c) 解析该TS直播流，从ChinaDRM描述子和CEI字段分别提取出视频序列的加密方法（SM4-SAMPLE）、编码方法（AVS2）等字段信息，以及被加密的视音频内容； d) 结合加密密钥调用对应的解密算法（SM4-SAMPLE）解密被加密的视音频内容并播放。		
符合性判定	a) 通过解析结果显示，TS直播流中加密方法符合GY/T 277—2019中6.2.1和6.2.2的规定，封装格式符合GY/T 277—2019中6.3.1的规定； b) 通过使用对应加密的密钥解密成功播放表明，加密算法符合GY/T 277—2019中6.2.2 SAMPLE模式语法的规定。		

A.1.1.5 对采用MPEG-TS协议封装的H.264编码直播流使用SM4-CBC加密的测试方法如下：

测试编号	Content_005	项目属性	必选
测试对象	内容加密服务器		
测试描述	测试内容加密服务器对采用MPEG-TS协议封装的H.264编码TS直播流采用SM4-CBC加密方式的加密功能。		
预置条件	设备： a) 内容加密服务器； b) DRM客户端（测试平台）。 状态： a) 已存在待测未加密H.264编码的TS直播流； b) 已知待测TS直播流的URL； c) 已获得加密TS直播流对应的密钥。		
测试步骤	a) 内容加密服务器采用SM4-CBC加密方式和对应密钥加密待测未加密H.264编码的TS直播流，生成H.264编码SM4-CBC加密的TS直播流并上传到URL； b) DRM客户端从URL接收加密TS直播流； c) 解析该TS直播流，从ChinaDRM描述子和CEI字段分别提取出视频序列的加密方法（SM4-CBC）、编码方法（H.264）等字段信息，以及被加密的视音频内容； d) 结合加密密钥调用对应的解密算法（SM4-CBC）解密被加密的视音频内容并播放。		

符合性判定	a) 通过解析结果显示，TS直播流中加密方法符合GY/T 277—2019中6.2.1和6.2.2的规定，封装格式符合GY/T 277—2019中6.3.1的的规定； b) 通过使用对应加密的密钥解密成功播放表明，加密算法符合GY/T 277—2019中6.2.2 CBC模式语法的规定。

A.1.1.6 对采用MPEG-TS协议封装的H.264编码直播流使用SM4-SAMPLE加密的测试方法如下：

测试编号	Content_006	项目属性	必选
测试对象	内容加密服务器		
测试描述	测试内容加密服务器对采用MPEG-TS协议封装的H.264编码TS直播流采用SM4-SAMPLE加密方式的加密功能。		
预置条件	设备： a) 内容加密服务器； b) DRM客户端（测试平台）。 状态： a) 已存在待测未加密H.264编码的TS直播流； b) 已知待测TS直播流的URL； c) 已获得加密TS直播流对应的密钥。		
测试步骤	a) 内容加密服务器采用SM4-SAMPLE加密方式和对应密钥加密待测未加密H.264编码的TS直播流，生成H.264编码SM4-SAMPLE加密的TS直播流并上传到URL； b) DRM客户端从URL接收加密TS直播流； c) 解析该TS直播流，从ChinaDRM描述子和CEI字段分别提取出视频序列的加密方法（SM4-SAMPLE）、编码方法（H.264）等字段信息，以及被加密的视音频内容； d) 结合加密密钥调用对应的解密算法（SM4-SAMPLE）解密被加密的视音频内容并播放。		
符合性判定	a) 通过解析结果显示，TS直播流中加密方法符合GY/T 277—2019中6.2.1和6.2.2的规定，封装格式符合GY/T 277—2019中6.3.1的规定； b) 通过使用对应加密的密钥解密成功播放表明，加密算法符合GY/T 277—2019中6.2.2 SAMPLE模式语法的规定。		

A.1.1.7 对采用MPEG-TS协议封装的H.265编码直播流使用SM4-CBC加密的测试方法如下：

测试编号	Content_007	项目属性	必选
测试对象	内容加密服务器		
测试描述	测试内容加密服务器对采用MPEG-TS协议封装的H.265编码TS直播流采用SM4-CBC加密方式的加密功能。		
预置条件	设备： a) 内容加密服务器； b) DRM客户端（测试平台）。 状态： a) 已存在待测未加密H.265编码的TS直播流； b) 已知待测TS直播流的URL； c) 已获得加密TS直播流对应的密钥。		

测试步骤	a) 内容加密服务器采用SM4-CBC加密方式和对应密钥加密待测未加密H.265编码的TS直播流，生成H.265编码SM4-CBC加密的TS直播流并上传到URL； b) DRM客户端从URL接收加密TS直播流； c) 解析该TS直播流，从ChinaDRM描述子和CEI字段分别提取出视频序列的加密方法（SM4-CBC）、编码方法（H.265）等字段信息，以及被加密的视音频内容； d) 结合加密密钥调用对应的解密算法（SM4-CBC）解密被加密的视音频内容并播放。
符合性判定	a) 通过解析结果显示，TS直播流中加密方法符合GY/T 277—2019中6.2.1和6.2.2的规定，封装格式符合GY/T 277—2019中6.3.1的规定； b) 通过使用对应加密的密钥解密成功播放表明，加密算法符合GY/T 277—2019中6.2.2 CBC模式语法的规定。

A.1.1.8 对采用MPEG-TS协议封装的H.265编码直播流使用SM4-SAMPLE加密的测试方法如下：

测试编号	Content_008	项目属性	必选
测试对象	内容加密服务器		
测试描述	测试内容加密服务器对采用MPEG-TS协议封装的H.265编码TS直播流采用SM4-SAMPLE加密方式的加密功能。		
预置条件	设备： a) 内容加密服务器； b) DRM客户端（测试平台）。 状态： a) 已存在待测未加密H.265编码的TS直播流； b) 已知待测TS直播流的URL； c) 已获得加密TS直播流对应的密钥。		
测试步骤	a) 内容加密服务器采用SM4-SAMPLE加密方式和对应密钥加密待测未加密H.265编码的TS直播流，生成H.265编码SM4-SAMPLE加密的TS直播流并上传到URL； b) DRM客户端从URL接收加密TS直播流； c) 解析该TS直播流，从ChinaDRM描述子和CEI字段分别提取出视频序列的加密方法（SM4-SAMPLE）、编码方法（H.265）等字段信息，以及被加密的视音频内容； d) 结合加密密钥调用对应的解密算法（SM4-SAMPLE）解密被加密的视音频内容并播放。		
符合性判定	a) 通过解析结果显示，TS直播流中加密方法符合GY/T 277—2019中6.2.1和6.2.2的规定，封装格式符合GY/T 277—2019中6.3.1的规定； b) 通过使用对应加密的密钥解密成功播放表明，加密算法符合GY/T 277—2019中6.2.2 SAMPLE模式语法的规定。		

A.1.1.9 对采用DASH协议封装的H.264编码直播流使用SM4-CBC加密的测试方法如下：

测试编号	Content_009	项目属性	必选
测试对象	内容加密服务器		
测试描述	测试内容加密服务器对采用DASH协议封装的H.264编码直播流采用SM4-CBC加密方式的加密功能。		

预置条件	设备： a) 内容加密服务器； b) DRM客户端（测试平台）； 状态： a) 已存在待测未加密H.264编码的直播流； b) 已知待测直播流的URL； c) 已获得采用SM4-CBC加密方法加密该直播流的密钥。
测试步骤	a) 内容加密服务器采用SM4-CBC加密方式和对应密钥加密待测未加密H.264编码的直播流，生成H.264编码SM4-CBC加密的直播流并上传到URL； b) DRM客户端周期性地从URL请求、接收并解析MPD文件，提取出视频序列的加密方法（SM4-CBC）、编码方法（H.264）和获取分片MP4文件的地址等字段信息； c) 根据分片MP4文件的地址请求、接收并解析MP4文件，提取出被加密的视音频内容； d) 结合加密密钥调用对应的解密算法（SM4-CBC）解密被加密的视音频内容并播放。
符合性判定	a) 通过解析结果显示，直播流中加密方法符合GY/T 277—2019中6.2.3和6.3.3的规定，封装格式符合GY/T 277—2019中6.3.2的规定； b) 通过使用对应加密的密钥解密成功播放表明，加密算法符合GY/T 277—2019中6.2.3 CBC模式语法的规定。

A.1.1.10 对采用DASH协议封装的H.264编码直播流使用SM4-SAMPLE加密的测试方法如下：

测试编号	Content_010	项目属性	必选
测试对象	内容加密服务器		
测试描述	测试内容加密服务器对采用DASH协议封装的H.264编码直播流采用SM4-SAMPLE加密方式的加密功能。		
预置条件	设备： a) 内容加密服务器； b) DRM客户端（测试平台）。 状态： a) 已存在待测未加密H.264编码的直播流； b) 已知待测直播流的URL； c) 已获得采用SM4-SAMPLE加密方法加密该直播流的密钥。		
测试步骤	a) 内容加密服务器采用SM4-SAMPLE加密方式和对应密钥加密待测未加密H.264编码的直播流，生成H.264编码SM4-SAMPLE加密的直播流并上传到URL； b) DRM客户端周期性地从URL请求、接收并解析MPD文件，提取出视频序列的加密方法（SM4-SAMPLE）、编码方法（H.264）和获取分片MP4文件的地址等字段信息； c) 根据分片MP4文件的地址请求、接收并解析MP4文件，提取出被加密的视音频内容； d) 结合加密密钥调用对应的解密算法（SM4-SAMPLE）解密被加密的视音频内容并播放。		
符合性判定	a) 通过解析结果显示，直播流中加密方法符合GY/T 277—2019中6.2.3和6.3.3的规定，封装格式符合GY/T 277—2019中6.3.2的规定； b) 通过使用对应加密的密钥解密成功播放表明，加密算法符合GY/T 277—2019中6.2.3 SAMPLE模式语法的规定。		

A.1.1.11 对采用DASH协议封装的H.265编码直播流使用SM4-CBC加密的测试方法如下：

测试编号	Content_011	项目属性	必选
测试对象	内容加密服务器		
测试描述	测试内容加密服务器对采用DASH协议封装的H.265编码直播流采用SM4-CBC加密方式的加密功能。		
预置条件	设备： a) 内容加密服务器； b) DRM客户端（测试平台）。 状态： a) 已存在待测未加密H.265编码的直播流； b) 已知待测直播流的URL； c) 已获得采用SM4-CBC加密方法加密该直播流的密钥。		
测试步骤	a) 内容加密服务器采用SM4-CBC加密方式和对应密钥加密待测未加密H.264编码的直播流，生成H.265编码SM4-CBC加密的直播流并上传到URL； b) DRM客户端周期性地从URL请求、接收并解析MPD文件，提取出视频序列的加密方法（SM4-CBC）、编码方法（H.265）和获取分片MP4文件的地址等字段信息； c) 根据分片MP4文件的地址请求、接收并解析MP4文件，提取出被加密的视音频内容； d) 结合加密密钥调用对应的解密算法（SM4-CBC）解密被加密的视音频内容并播放。		
符合性判定	a) 通过解析结果显示，直播流中加密方法符合GY/T 277—2019中6.2.3和6.3.3的规定，封装格式符合GY/T 277—2019中6.3.2的规定； b) 通过使用对应加密的密钥解密成功播放表明，加密算法符合GY/T 277—2019中6.2.3 CBC模式语法的规定。		

A.1.1.12 对采用DASH协议封装的H.265编码直播流使用SM4-SAMPLE加密的测试方法如下：

测试编号	Content_012	项目属性	必选
测试对象	内容加密服务器		
测试描述	测试内容加密服务器对采用DASH协议封装的H.265编码直播流采用SM4-SAMPLE加密方式的加密功能。		
预置条件	设备： a) 内容加密服务器； b) DRM客户端（测试平台）。 状态： a) 已存在待测未加密H.265编码的直播流； b) 已知待测直播流的URL； c) 已获得采用SM4-SAMPLE加密方法加密该直播流的密钥。		
测试步骤	a) 内容加密服务器采用SM4-SAMPLE加密方式和对应密钥加密待测未加密H.264编码的直播流，生成H.265编码SM4-SAMPLE加密的直播流并上传到URL； b) DRM客户端周期性地从URL请求、接收并解析MPD文件，提取出视频序列的加密方法（SM4-SAMPLE）、编码方法（H.265）和获取分片MP4文件的地址等字段信息； c) 根据分片MP4文件的地址请求、接收并解析MP4文件，提取出被加密的视音频内容； d) 结合加密密钥调用对应的解密算法（SM4-SAMPLE）解密被加密的视音频内容并播放。		
符合性判定	a) 通过解析结果显示，直播流中加密方法符合GY/T 277—2019中6.2.3和6.3.3的规定，封装格式符合GY/T 277—2019中6.3.2的规定； b) 通过使用对应加密的密钥解密成功播放表明，加密算法符合GY/T 277—2019中6.2.3 SAMPLE模式语法的规定。		

A.1.1.13 对采用HLS协议封装的H.264编码直播流使用SM4-CBC加密的测试方法如下：

测试编号	Content_013	项目属性	必选
测试对象	内容加密服务器		
测试描述	测试内容加密服务器对采用HLS协议封装的H.264编码直播流采用SM4-CBC加密方式的加密功能		
预置条件	设备： a) 内容加密服务器； b) DRM客户端（测试平台）。 状态： a) 已存在待测未加密H.264编码的直播流； b) 已知待测直播流的URL； c) 已获得采用SM4-CBC加密方法加密该直播流的密钥。		
测试步骤	a) 内容加密服务器采用SM4-CBC加密方式和对应密钥加密待测未加密H.264编码的直播流，生成H.264编码SM4-CBC加密的直播流并上传到URL； b) DRM客户端周期性地从URL请求、接收并解析M3U8文件，提取出视频序列的加密方法（SM4-CBC）、编码方法（H.264）和获取分片TS文件的地址等字段信息； c) 根据分片TS文件的地址请求、接收并解析TS文件，提取出被加密的视音频内容； d) 结合加密密钥调用对应的解密算法（SM4-CBC）解密被加密的视音频内容并播放。		
符合性判定	a) 通过解析结果显示，直播流中加密方法符合GY/T 277—2019中6.2.3和6.3.3的规定，封装格式符合GY/T 277—2019中6.3.2的规定； b) 通过使用对应加密的密钥解密成功播放表明，加密算法符合GY/T 277—2019中6.2.3 CBC模式语法的规定。		

A.1.1.14 对采用HLS协议封装的H.264编码直播流使用SM4-SAMPLE加密的测试方法如下：

测试编号	Content_014	项目属性	必选
测试对象	内容加密服务器		
测试描述	测试内容加密服务器对采用HLS协议封装的H.264编码直播流采用SM4-SAMPLE加密方式的加密功能。		
预置条件	设备： a) 内容加密服务器； b) DRM客户端（测试平台）。 状态： a) 已存在待测未加密H.264编码的直播流； b) 已知待测直播流的URL； c) 已获得采用SM4-SAMPLE加密方法加密该直播流的密钥。		
测试步骤	a) 内容加密服务器采用SM4-SAMPLE加密方式和对应密钥加密待测未加密H.264编码的直播流，生成H.264编码SM4-SAMPLE加密的直播流并上传到URL； b) DRM客户端周期性地从URL请求、接收并解析M3U8文件，提取出视频序列的加密方法（SM4-SAMPLE）、编码方法（H.264）和获取分片TS文件的地址等字段信息； c) 根据分片TS文件的地址请求、接收并解析TS文件，提取出被加密的视音频内容； d) 结合加密密钥调用对应的解密算法（SM4-SAMPLE）解密被加密的视音频内容并播放。		

符合性判定	a) 通过解析结果显示，直播流中加密方法符合GY/T 277—2019中6.2.3和6.3.3的规定，封装格式符合GY/T 277—2019中6.3.2的规定； b) 通过使用对应加密的密钥解密成功播放表明，加密算法符合GY/T 277—2019中6.2.3 SAMPLE模式语法的规定。

A.1.1.15 对采用HLS协议封装的H.265编码直播流使用SM4-CBC加密的测试方法如下：

测试编号	Content_015	项目属性	必选
测试对象	内容加密服务器		
测试描述	测试内容加密服务器对采用HLS协议封装的H.265编码直播流采用SM4-CBC加密方式的加密功能。		
预置条件	设备： a) 内容加密服务器； b) DRM客户端（测试平台）。 状态： a) 已存在待测未加密H.265编码的直播流； b) 已知待测直播流的URL； c) 已获得采用SM4-CBC加密方法加密该直播流的密钥。		
测试步骤	a) 内容加密服务器采用SM4-CBC加密方式和对应密钥加密待测未加密H.264编码的直播流，生成H.265编码SM4-CBC加密的直播流并上传到URL； b) DRM客户端周期性地从URL请求、接收并解析M3U8文件，提取出视频序列的加密方法（SM4-CBC）、编码方法（H.265）和获取分片TS文件的地址等字段信息； c) 根据分片TS文件的地址请求、接收并解析TS文件，提取出被加密的视音频内容； d) 结合加密密钥调用对应的解密算法（SM4-CBC）解密被加密的视音频内容并播放。		
符合性判定	a) 通过解析结果显示，直播流中加密方法符合GY/T 277—2019中6.2.3和6.3.3的规定，封装格式符合GY/T 277—2019中6.3.2的规定； b) 通过使用对应加密的密钥解密成功播放表明，加密算法符合GY/T 277—2019中6.2.3 CBC模式语法的规定。		

A.1.1.16 对采用HLS协议封装的H.265编码直播流使用SM4-SAMPLE加密的测试方法如下：

测试编号	Content_016	项目属性	必选
测试对象	内容加密服务器		
测试描述	测试内容加密服务器对采用HLS协议封装的H.265编码直播流采用SM4-SAMPLE加密方式的加密功能。		
预置条件	设备： a) 内容加密服务器； b) DRM客户端（测试平台）。 状态： a) 已存在待测未加密H.265编码的直播流； b) 已知待测直播流的URL； c) 已获得采用SM4-SAMPLE加密方法加密该直播流的密钥。		

测试步骤	a) 内容加密服务器采用SM4-SAMPLE加密方式和对应密钥加密待测未加密H.264编码的直播流，生成H.265编码SM4-SAMPLE加密的直播流并上传到URL； b) DRM客户端周期性地从URL请求、接收并解析M3U8文件，提取出视频序列的加密方法（SM4-SAMPLE）、编码方法（H.265）和获取分片TS文件的地址等字段信息； c) 根据分片TS文件的地址请求、接收并解析TS文件，提取出被加密的视音频内容； d) 结合加密密钥调用对应的解密算法（SM4-SAMPLE）解密被加密的视音频内容并播放。
符合性判定	a) 通过解析结果显示，直播流中加密方法符合GY/T 277—2019中6.2.3和6.3.3的规定，封装格式符合GY/T 277—2019中6.3.2的规定； b) 通过使用对应加密的密钥解密成功播放表明，加密算法符合GY/T 277—2019中6.2.3 SAMPLE模式语法的规定。

A.1.2 点播场景测试

A.1.2.1 对采用MPEG-TS协议封装的AVS+编码点播流使用SM4-CBC加密的测试方法如下：

测试编号	Content_017	项目属性	必选
测试对象	内容加密服务器		
测试描述	测试内容加密服务器对AVS+编码点播流采用SM4-CBC加密方式的加密功能。		
预置条件	设备： a) 内容加密服务器； b) DRM客户端（测试平台）。 状态： a) 已存在待测试未加密AVS+编码的TS点播流文件； b) 已存在采用SM4-CBC加密方法加密该TS点播流文件的密钥。		
测试步骤	a) 内容加密服务器采用SM4-CBC加密方式和对应密钥加密该待测试未加密AVS+编码的TS点播流文件，生成加密后的TS点播流文件； b) DRM客户端解析该加密TS点播流文件得到所承载视频序列的编码方法（AVS+）、加密方法（SM4-CBC）等信息，并提取出被加密的视音频内容； c) 结合内容解密密钥调用解密算法（SM4-CBC）解密被加密的视音频内容并播放。		
符合性判定	a) 通过解析结果显示，TS点播流文件中加密方法符合GY/T 277—2019中6.2.1和6.2.2的规定，封装格式符合GY/T 277—2019中6.3.1的规定； b) 通过使用对应加密的密钥解密成功播放表明，加密算法符合GY/T 277—2019中6.2.2 CBC模式语法的规定。		

A.1.2.2 对采用MPEG-TS协议封装的AVS+编码点播流使用SM4-SAMPLE加密的测试方法如下：

测试编号	Content_018	项目属性	必选
测试对象	内容加密服务器		
测试描述	测试内容加密服务器对AVS+编码点播流采用SM4-SAMPLE加密方式的加密功能。		
预置条件	设备： a) 内容加密服务器； b) DRM客户端（测试平台）。 状态： a) 已存在待测试未加密AVS+编码的TS点播流文件； b) 已存在采用SM4-SAMPLE加密方法加密该TS点播流文件的密钥。		

测试步骤	a) 内容加密服务器采用SM4-SAMPLE加密方式和对应密钥加密该待测试未加密AVS+编码的TS点播流文件，生成加密后的TS点播流文件； b) DRM客户端解析该加密TS点播流文件得到所承载视频序列的编码方法（AVS+）、加密方法（SM4-SAMPLE）等信息，并提取出被加密的视音频内容； c) 结合内容解密密钥调用解密算法（SM4-SAMPLE）解密被加密的视音频内容并播放。
符合性判定	a) 通过解析结果显示，TS点播流文件中加密方法符合GY/T 277—2019中6.2.1和6.2.2的规定，封装格式符合GY/T 277—2019中6.3.1的规定； b) 通过使用对应加密的密钥解密成功播放表明，加密算法符合GY/T 277—2019中6.2.2 SAMPLE模式语法的规定。

A.1.2.3 对采用MPEG-TS协议封装的AVS2编码点播流使用SM4-CBC加密的测试方法如下：

测试编号	Content_019	项目属性	必选
测试对象	内容加密服务器		
测试描述	测试内容加密服务器对AVS2编码点播流采用SM4-CBC加密方式的加密功能。		
预置条件	设备： a) 内容加密服务器； b) DRM客户端（测试平台）。 状态： a) 已存在待测试未加密AVS2编码的TS点播流文件； b) 已存在采用SM4-CBC加密方法加密该TS点播流文件的密钥。		
测试步骤	a) 内容加密服务器采用SM4-CBC加密方式和对应密钥加密该待测试未加密AVS2编码的TS点播流文件，生成加密后的TS点播流文件； b) DRM客户端解析该加密TS点播流文件得到所承载视频序列的编码方法（AVS2）、加密方法（SM4-CBC）等信息，并提取出被加密的视音频内容； c) 结合内容解密密钥调用解密算法（SM4-CBC）解密被加密的视音频内容并播放。		
符合性判定	a) 通过解析结果显示，TS点播流文件中加密方法符合GY/T 277—2019中6.2.1和6.2.2的规定，封装格式符合GY/T 277—2019中6.3.1的规定； b) 通过使用对应加密的密钥解密成功播放表明，加密算法符合GY/T 277—2019中6.2.2 CBC模式语法的规定。		

A.1.2.4 对采用MPEG-TS协议封装的AVS2编码点播流使用SM4-SAMPLE加密的测试方法如下：

测试编号	Content_020	项目属性	必选
测试对象	内容加密服务器		
测试描述	测试内容加密服务器对AVS2编码点播流采用SM4-SAMPLE加密方式的加密功能。		
预置条件	设备： a) 内容加密服务器； b) DRM客户端（测试平台）。 状态： a) 已存在待测试未加密AVS2编码的TS点播流文件； b) 已存在采用SM4-SAMPLE加密方法加密该TS点播流文件的密钥。		

测试步骤	a) 内容加密服务器采用SM4-SAMPLE加密方式和对应密钥加密该待测试未加密AVS2编码的TS点播流文件，生成加密后的TS点播流文件； b) DRM客户端解析该加密TS点播流文件得到所承载视频序列的编码方法（AVS2）、加密方法（SM4-SAMPLE）等信息，并提取出被加密的视音频内容； c) 结合内容解密密钥调用解密算法（SM4-SAMPLE）解密被加密的视音频内容并播放。
符合性判定	a) 通过解析结果显示，TS点播流文件中加密方法符合GY/T 277—2019中6.2.1和6.2.2的规定，封装格式符合GY/T 277—2019中6.3.1的规定； b) 通过使用对应加密的密钥解密成功播放表明，加密算法符合GY/T 277—2019中6.2.2 SAMPLE模式语法的规定。

A.1.2.5 对采用MPEG-TS协议封装的H.264编码点播流使用SM4-CBC加密的测试方法如下：

测试编号	Content_021	项目属性	必选
测试对象	内容加密服务器		
测试描述	测试内容加密服务器对H.264编码点播流采用SM4-CBC加密方式的加密功能。		
预置条件	设备： a) 内容加密服务器； b) DRM客户端（测试平台）。 状态： a) 已存在待测试未加密H.264编码的TS点播流文件； b) 已存在采用SM4-CBC加密方法加密该TS点播流文件的密钥。		
测试步骤	a) 内容加密服务器采用SM4-CBC加密方式和对应密钥加密该待测试未加密H.264编码的TS点播流文件，生成加密后的TS点播流文件； b) DRM客户端解析该加密TS点播流文件得到所承载视频序列的编码方法（H.264）、加密方法（SM4-CBC）等信息，并提取出被加密的视音频内容； c) 结合内容解密密钥调用解密算法（SM4-CBC）解密被加密的视音频内容并播放。		
符合性判定	a) 通过解析结果显示，TS点播流文件中加密方法符合GY/T 277—2019中6.2.1和6.2.2的规定，封装格式符合GY/T 277—2019中6.3.1的规定； b) 通过使用对应加密的密钥解密成功播放表明，加密算法符合GY/T 277—2019中6.2.2 CBC模式语法的规定。		

A.1.2.6 对采用MPEG-TS协议封装的H.264编码点播流使用SM4-SAMPLE加密的测试方法如下：

测试编号	Content_022	项目属性	必选
测试对象	内容加密服务器		
测试描述	测试内容加密服务器对H.264编码点播流采用SM4-SAMPLE加密方式的加密功能。		
预置条件	设备： a) 内容加密服务器； b) DRM客户端（测试平台）。 状态： a) 已存在待测试未加密H.264编码的TS点播流文件； b) 已存在采用SM4-SAMPLE加密方法加密该TS点播流文件的密钥。		

测试步骤	a) 内容加密服务器采用SM4-SAMPLE加密方式和对应密钥加密该待测试未加密H.264编码的TS点播流文件，生成加密后的TS点播流文件； b) DRM客户端解析该加密TS点播流文件得到所承载视频序列的编码方法（H.264）、加密方法（SM4-SAMPLE）等信息，并提取出被加密的视音频内容； c) 结合内容解密密钥调用解密算法（SM4-SAMPLE）解密被加密的视音频内容并播放。
符合性判定	a) 通过解析结果显示，TS点播流文件中加密方法符合GY/T 277—2019中6.2.1和6.2.2的规定，封装格式符合GY/T 277—2019中6.3.1的规定； b) 通过使用对应加密的密钥解密成功播放表明，加密算法符合GY/T 277—2019中6.2.2 SAMPLE模式语法的规定。

A.1.2.7 对采用MPEG-TS协议封装的H.265编码点播流使用SM4-CBC加密的测试方法如下：

测试编号	Content_023	项目属性	必选
测试对象	内容加密服务器		
测试描述	测试内容加密服务器对H.265编码点播流采用SM4-CBC加密方式的加密功能。		
预置条件	设备： a) 内容加密服务器； b) DRM客户端（测试平台）。 状态： a) 已存在待测试未加密H.265编码的TS点播流文件； b) 已存在采用SM4-CBC加密方法加密该TS点播流文件的密钥。		
测试步骤	a) 内容加密服务器采用SM4-CBC加密方式和对应密钥加密该待测试未加密H.265编码的TS点播流文件，生成加密后的TS点播流文件； b) DRM客户端解析该加密TS点播流文件得到所承载视频序列的编码方法（H.265）、加密方法（SM4-CBC）等信息，并提取出被加密的视音频内容； c) 结合内容解密密钥调用解密算法（SM4-CBC）解密被加密的视音频内容并播放。		
符合性判定	a) 通过解析结果显示，TS点播流文件中加密方法符合GY/T 277—2019中6.2.1和6.2.2的规定，封装格式符合GY/T 277—2019中6.3.1的规定； b) 通过使用对应加密的密钥解密成功播放表明，加密算法符合GY/T 277—2019中6.2.2 CBC模式语法的规定。		

A.1.2.8 对采用MPEG-TS协议封装的H.265编码点播流使用SM4-SAMPLE加密的测试方法如下：

测试编号	Content_024	项目属性	必选
测试对象	内容加密服务器		
测试描述	测试内容加密服务器对H.265编码点播流采用SM4-SAMPLE加密方式的加密功能。		
预置条件	设备： a) 内容加密服务器； b) DRM客户端（测试平台）。 状态： a) 已存在待测试未加密H.265编码的TS点播流文件； b) 已存在采用SM4-SAMPLE加密方法加密该TS点播流文件的密钥。		

测试步骤	a) 内容加密服务器采用SM4-SAMPLE加密方式和对应密钥加密该待测试未加密H.265编码的TS点播流文件，生成加密后的TS点播流文件； b) DRM客户端解析该加密TS点播流文件得到所承载视频序列的编码方法（H.265）、加密方法（SM4-SAMPLE）等信息，并提取出被加密的视音频内容； c) 结合内容解密密钥调用解密算法（SM4-SAMPLE）解密被加密的视音频内容并播放。
符合性判定	a) 通过解析结果显示，TS点播流文件中加密方法符合GY/T 277—2019中6.2.1和6.2.2的规定，封装格式符合GY/T 277—2019中6.3.1的规定； b) 通过使用对应加密的密钥解密成功播放表明，加密算法符合GY/T 277—2019中6.2.2 SAMPLE模式语法的规定。

A.1.2.9 对采用DASH协议封装的H.264编码点播流使用SM4-CBC加密的测试方法如下：

测试编号	Content_025	项目属性	必选
测试对象	内容加密服务器		
测试描述	测试内容加密服务器对H.264编码点播流采用SM4-CBC加密方式的加密功能。		
预置条件	设备： a) 内容加密服务器； b) DRM客户端（测试平台）。 状态： a) 已存在待测未加密H.264编码的MP4点播流文件； b) 已获得采用SM4-CBC加密方法加密该MP4点播流文件的密钥。		
测试步骤	a) 内容加密服务器采用SM4-CBC加密方式和对应密钥加密待测未加密H.264编码的MP4点播流文件，生成加密后的MP4点播流文件，并得到MPD文件； b) DRM客户端解析MPD文件，提取出视频序列的加密方法（SM4-CBC）、编码方法（H.264）等字段信息； c) 解析加密MP4点播流文件，提取出被加密的视音频内容； d) 结合加密密钥调用对应的解密算法（SM4-CBC）解密被加密的视音频内容并播放。		
符合性判定	a) 通过解析结果显示，MP4点播流文件中加密方法符合GY/T 277—2019中6.2.3和6.3.3的规定，封装格式符合GY/T 277—2019中6.3.2的规定； b) 通过使用对应加密的密钥解密成功播放表明，加密算法符合GY/T 277—2019中6.2.3 CBC模式语法的规定。		

A.1.2.10 对采用DASH协议封装的H.264编码点播流使用SM4-SAMPLE加密的测试方法如下：

测试编号	Content_026	项目属性	必选
测试对象	内容加密服务器		
测试描述	测试内容加密服务器对H.264编码点播流采用SM4-SAMPLE加密方式的加密功能。		
预置条件	设备： a) 内容加密服务器； b) DRM客户端（测试平台）。 状态： a) 已存在待测未加密H.264编码的MP4点播流文件； b) 已获得采用SM4-SAMPLE加密方法加密该MP4点播流文件的密钥。		

测试步骤	a) 内容加密服务器采用SM4-SAMPLE加密方式和对应密钥加密待测未加密H.264编码的MP4点播流文件，生成加密后的MP4点播流文件，并得到MPD文件； b) DRM客户端解析MPD文件，提取出视频序列的加密方法（SM4-SAMPLE）、编码方法（H.264）等字段信息； c) 解析加密MP4点播流文件，提取出被加密的视音频内容； d) 结合加密密钥调用对应的解密算法（SM4-SAMPLE）解密被加密的视音频内容并播放。
符合性判定	a) 通过解析结果显示，点播MP4文件中加密方法符合GY/T 277—2019中6.2.3和6.3.3的规定，封装格式符合GY/T 277—2019中6.3.2的规定； b) 通过使用对应加密的密钥解密成功播放表明，加密算法符合GY/T 277—2019中6.2.3 SAMPLE模式语法的规定。

A.1.2.11 对采用DASH协议封装的H.265编码点播流使用SM4-CBC加密的测试方法如下：

测试编号	Content_027	项目属性	必选
测试对象	内容加密服务器		
测试描述	测试内容加密服务器对H.265编码点播流采用SM4-CBC加密方式的加密功能。		
预置条件	设备： a) 内容加密服务器； b) DRM客户端（测试平台）。 状态： a) 已存在待测未加密H.265编码的MP4点播流文件； b) 已获得采用SM4-CBC加密方法加密该MP4点播流文件的密钥。		
测试步骤	a) 内容加密服务器采用SM4-CBC加密方式和对应密钥加密待测未加密H.265编码的MP4点播流文件，生成加密后的MP4点播流文件，并得到MPD文件； b) DRM客户端解析MPD文件，提取出视频序列的加密方法（SM4-CBC）、编码方法（H.265）等字段信息； c) 解析加密MP4点播流文件，提取出被加密的视音频内容； d) 结合加密密钥调用对应的解密算法（SM4-CBC）解密被加密的视音频内容并播放。		
符合性判定	a) 通过解析结果显示，MP4点播流文件中加密方法符合GY/T 277—2019中6.2.3和6.3.3的规定，封装格式符合GY/T 277—2019中6.3.2的规定； b) 通过使用对应加密的密钥解密成功播放表明，加密算法符合GY/T 277—2019中6.2.3 CBC模式语法的规定。		

A.1.2.12 对采用DASH协议封装的H.265编码点播流使用SM4-SAMPLE加密的测试方法如下：

测试编号	Content_028	项目属性	必选
测试对象	内容加密服务器		
测试描述	测试内容加密服务器对H.265编码点播流采用SM4-SAMPLE加密方式的加密功能。		
预置条件	设备： a) 内容加密服务器； b) DRM客户端（测试平台）。 状态： a) 已存在待测未加密H.265编码的MP4点播流文件； b) 已获得采用SM4-SAMPLE加密方法加密该MP4点播流文件的密钥。		

测试步骤	a) 内容加密服务器采用SM4-SAMPLE加密方式和对应密钥加密待测未加密H.265编码的MP4点播流文件，生成加密后的MP4点播流文件，并得到MPD文件； b) DRM客户端解析MPD文件，提取出视频序列的加密方法（SM4-SAMPLE）、编码方法（H.265）等字段信息； c) 解析加密MP4点播流文件，提取出被加密的视音频内容； d) 结合加密密钥调用对应的解密算法（SM4-SAMPLE）解密被加密的视音频内容并播放。
符合性判定	a) 通过解析结果显示，点播MP4文件中加密方法符合GY/T 277—2019中6.2.3和6.3.3的规定，封装格式符合GY/T 277—2019中6.3.2的规定； b) 通过使用对应加密的密钥解密成功播放表明，加密算法符合GY/T 277—2019中6.2.3 SAMPLE模式语法的规定。

A.1.2.13 对采用HLS协议封装的H.264编码点播流使用SM4-CBC加密的测试方法如下：

测试编号	Content_029	项目属性	必选
测试对象	内容加密服务器		
测试描述	测试内容加密服务器对H.264编码点播流采用SM4-CBC加密方式的加密功能。		
预置条件	设备： a) 内容加密服务器； b) DRM客户端（测试平台）。 状态： a) 已存在待测未加密H.264编码的TS点播流文件； b) 已获得采用SM4-CBC加密方法加密该TS点播流文件的密钥。		
测试步骤	a) 内容加密服务器采用SM4-CBC加密方式和对应密钥加密待测未加密H.264编码的TS点播流文件，生成加密后的TS点播流文件，并得到相应的M3U8文件； b) DRM客户端解析M3U8文件，提取出视频序列的加密方法（SM4-CBC）、编码方法（H.264）等字段信息； c) 解析加密TS点播流文件，提取出被加密的视音频内容； d) 结合加密密钥调用对应的解密算法（SM4-CBC）解密被加密的视音频内容并播放。		
符合性判定	a) 通过解析结果显示，TS点播流文件中加密方法符合GY/T 277—2019中6.2.3和6.3.3的规定，封装格式符合GY/T 277—2019中6.3.2的规定； b) 通过使用对应加密的密钥解密成功播放表明，加密算法符合GY/T 277—2019中6.2.3 CBC模式语法的规定。		

A.1.2.14 对采用HLS协议封装的H.264编码点播流采用SM4-SAMPLE加密的测试方法如下：

测试编号	Content_030	项目属性	必选
测试对象	内容加密服务器		
测试描述	测试内容加密服务器对H.264编码点播流采用SM4-SAMPLE加密方式的加密功能。		
预置条件	设备： a) 内容加密服务器； b) DRM客户端（测试平台）。 状态： a) 已存在待测未加密H. 264编码的TS点播流文件； b) 已获得采用SM4-SAMPLE加密方法加密该TS点播流文件的密钥。		

测试步骤	a) 内容加密服务器采用SM4-SAMPLE加密方式和对应密钥加密待测未加密H.264编码的TS点播流文件，生成加密后的TS点播流文件，并得到相应的M3U8文件； b) DRM客户端解析M3U8文件，提取出视频序列的加密方法（SM4-SAMPLE）、编码方法（H.264）等字段信息； c) 解析加密TS点播流文件，提取出被加密的视音频内容； d) 结合加密密钥调用对应的解密算法（SM4-SAMPLE）解密被加密的视音频内容并播放。
符合性判定	a) 通过解析结果显示，TS点播流文件中加密方法符合GY/T 277—2019中6.2.3和6.3.3的规定，封装格式符合GY/T 277—2019中6.3.2的规定； b) 通过使用对应加密的密钥解密成功播放表明，加密算法符合GY/T 277—2019中6.2.3 SAMPLE模式语法的规定。

A.1.2.15 对采用HLS协议封装的H.265编码点播流采用SM4-CBC加密的测试方法如下：

测试编号	Content_031	项目属性	必选
测试对象	内容加密服务器		
测试描述	测试内容加密服务器对H.265编码点播流采用SM4-CBC加密方式的加密功能。		
预置条件	设备： a) 内容加密服务器； b) DRM客户端（测试平台）。 状态： a) 已存在待测未加密H. 265编码的TS点播流文件； b) 已获得采用SM4-CBC加密方法加密该TS点播流文件的密钥。		
测试步骤	a) 内容加密服务器采用SM4-CBC加密方式和对应密钥加密待测未加密H.265编码的TS点播流文件，生成加密后的TS点播流文件，并得到相应的M3U8文件； b) DRM客户端解析M3U8文件，提取出视频序列的加密方法（SM4-CBC）、编码方法（H.265）等字段信息； c) 解析加密TS点播流文件，提取出被加密的视音频内容； d) 结合加密密钥调用对应的解密算法（SM4-CBC）解密被加密的视音频内容并播放。		
符合性判定	a) 通过解析结果显示，TS点播流文件中加密方法符合GY/T 277—2019中6.2.3和6.3.3的规定，封装格式符合GY/T 277—2019中6.3.2的规定； b) 通过使用对应加密的密钥解密成功播放表明，加密算法符合GY/T 277—2019中6.2.3 CBC模式语法的规定。		

A.1.2.16 对采用HLS协议封装的H.265编码点播流采用SM4-SAMPLE加密的测试方法如下：

测试编号	Content_032	项目属性	必选
测试对象	内容加密服务器		
测试描述	测试内容加密服务器对H.265编码点播流采用SM4-SAMPLE加密方式的加密功能。		
预置条件	设备： a) 内容加密服务器； b) DRM客户端（测试平台）。 状态： a) 已存在待测未加密H. 265编码的TS点播流文件； b) 已获得采用SM4-SAMPLE加密方法加密该TS点播流文件的密钥。		

测试步骤	a) 内容加密服务器采用SM4-SAMPLE加密方式和对应密钥加密待测未加密H.265编码的TS点播流文件，生成加密后的TS点播流文件，并得到相应的M3U8文件； b) DRM客户端解析M3U8文件，提取出视频序列的加密方法（SM4-SAMPLE）、编码方法（H.265）等字段信息； c) 解析加密TS点播流文件，提取出被加密的视音频内容； d) 结合加密密钥调用对应的解密算法（SM4-SAMPLE）解密被加密的视音频内容并播放。
符合性判定	a) 通过解析结果显示，TS点播流文件中加密方法符合GY/T 277—2019中6.2.3和6.3.3的规定，封装格式符合GY/T 277—2019中6.3.2的规定； b) 通过使用对应加密的密钥解密成功播放表明，加密算法符合GY/T 277—2019中6.2.3 SAMPLE模式语法的规定。

A.2 许可证格式和获取协议测试

A.2.1 内容授权服务器测试

A.2.1.1 对许可证获取请求的处理功能的测试方法如下：

测试编号	License_001	项目属性	必选
测试对象	内容授权服务器		
测试描述	测试内容授权服务器对DRM客户端的许可证获取请求的处理功能。		
预置条件	设备： a) DRM客户端（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器处理请求消息，并发送包含DRM客户端请求的许可证的响应消息； c) DRM客户端解析许可证获取响应消息。		
符合性判定	a) 内容授权服务器向客户端发送的许可证响应消息格式、内容均正确，符合GY/T 277—2019中8.3的规定； b) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.1.2 对许可证请求包含多个内容标识授权的处理功能的测试方法如下：

测试编号	License_002	项目属性	必选
测试对象	内容授权服务器		
测试描述	测试内容授权服务器对DRM客户端的包含多个内容标识许可证请求的处理功能。		

预置条件	设备： a) DRM客户端（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确，并带有多个内容标识； b) 内容授权服务器处理请求消息，并发送包含DRM客户端请求的多许可证的响应消息； c) DRM客户端解析许可证获取响应消息。
符合性判定	a) 内容授权服务器向客户端发送的许可证响应消息格式、内容均正确，符合GY/T 277—2019中8.3的规定； b) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定； c) DRM客户端能解析出多个内容标识的授权信息。

A.2.1.3 对许可证请求缺少数字签名的处理功能的测试方法如下：

测试编号	License_003	项目属性	必选
测试对象	内容授权服务器		
测试描述	测试内容授权服务器对客户端许可证请求中缺少数字签名的处理功能。		
预置条件	设备： a) DRM客户端（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。		
测试步骤	a) DRM客户端向内容授权服务器发送许可证请求，请求中缺少signature参数或signature值为空； b) 内容授权服务器识别许可证请求消息，并向客户端发送响应消息； c) 客户端解析内容授权服务器发送的响应消息，终止当前协议。		
符合性判定	a) 内容授权服务器向客户端发送“malformedReques”状态，且许可证响应消息格式、内容均符合GY/T 277—2019中8.3的规定； b) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.1.4 对许可证请求数字签名错误的处理功能的测试方法如下：

测试编号	License_004	项目属性	必选
测试对象	内容授权服务器		
测试描述	测试内容授权服务器对客户端许可证请求中包含错误的数字签名的处理功能。		

预置条件	设备： a) DRM客户端（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。
测试步骤	a) DRM客户端向内容授权服务器发送许可证请求，请求中signature参数错误； b) 内容授权服务器识别许可证请求消息，并向客户端发送响应消息； c) 客户端解析内容授权服务器发送的响应消息，终止当前协议。
符合性判定	a) 内容授权服务器向客户端发送“signatureError”状态，且许可证响应消息格式、内容均符合GY/T 277—2019中8.3的规定； b) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。

A.2.1.5 对许可证请求DRM客户端CA证书没有签名的处理功能的测试方法如下：

测试编号	License_005	项目属性	必选
测试对象	内容授权服务器		
测试描述	测试内容授权服务器对客户端许可证请求中包含没有签名的DRM客户端CA证书证书的处理功能。		
预置条件	设备： a) DRM客户端（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成数字证书的置入，其中DRM客户端CA证书证书没有签名。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，请求中包含缺少签名的DRM客户端CA证书证书； b) 内容授权服务器识别许可证请求消息，并向客户端发送响应消息； c) 客户端解析内容授权服务器返回的响应消息，并终止当前协议。		
符合性判定	a) 内容授权服务器向客户端发送“invalidCertificateChain”状态，且许可证获取响应消息格式、内容均符合GY/T 277—2019中8.3的规定； b) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.1.6 对许可证请求DRM客户端CA证书签名错误的处理功能的测试方法如下：

测试编号	License_006	项目属性	必选
测试对象	内容授权服务器		
测试描述	测试内容授权服务器对客户端许可证请求中包含错误签名的DRM客户端CA证书证书的处理功能。		
预置条件	设备： a) DRM客户端（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成数字证书的置入，其中DRM客户端CA证书证书签名错误。		

测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，请求中DRM客户端CA证书签名错误； b) 内容授权服务器识别许可证请求消息，并向客户端发送响应消息； c) 客户端解析内容授权服务器返回的响应消息，并终止当前协议。
符合性判定	a) 内容授权服务器向客户端发送“invalidCertificateChain”状态，且许可证获取响应消息格式、内容均符合GY/T 277—2019中8.3的规定； b) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。

A.2.1.7 对许可证请求DRM客户端 CA证书有效期-UTC Time-NotBefore的处理功能的测试方法如下：

测试编号	License_007	项目属性	必选
测试对象	内容授权服务器		
测试描述	测试内容授权服务器对客户端许可证请求中包含DRM客户端CA证书证书有效期-UTC Time-NotBefore的处理功能。		
预置条件	设备： a) DRM客户端（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成数字证书的置入，其中DRM客户端CA证书证书有效期-UTC Time-NotBefore不满足。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息中DRM客户端CA证书证书有效期-UTC Time-NotBefore不满足； b) 内容授权服务器识别许可证请求消息，并向客户端发送响应消息； c) 客户端解析内容授权服务器发送的响应消息，并终止当前协议。		
符合性判定	a) 内容授权服务器向客户端发送“invalidCertificateChain”状态，且许可证获取响应消息格式、内容均符合GY/T 277—2019中8.3的规定； b) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.1.8 对许可证请求DRM客户端CA证书有效期-UTC Time-NotAfter的处理功能的测试方法如下：

测试编号	License_008	项目属性	必选
测试对象	内容授权服务器		
测试描述	测试内容授权服务器对客户端许可证请求中包含DRM客户端CA证书有效期-UTC Time-NotAfter的处理功能。		
预置条件	设备： a) DRM客户端（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成数字证书的置入，其中DRM客户端CA证书有效期-UTC Time-NotAfter不满足。		

测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息中DRM客户端CA证书有效期-UTC Time-NotAfter不满足； b) 内容授权服务器识别许可证请求消息，并向客户端发送响应消息； c) 客户端解析内容授权服务器返回的响应消息，并终止当前协议。
符合性判定	a) 内容授权服务器向客户端发送“invalidCertificateChain”状态，且许可证获取响应消息格式、内容均符合GY/T 277—2019中8.3的规定； b) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。

A.2.1.9 对许可证请求DRM客户端证书没有签名的处理功能的测试方法如下：

测试编号	License_009	项目属性	必选
测试对象	内容授权服务器		
测试描述	测试内容授权服务器对客户端许可证请求中包含没有签名的DRM客户端证书的处理功能。		
预置条件	设备： a) DRM客户端（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成数字证书的置入，其中DRM客户端证书没有签名。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息中DRM客户端证书没有签名； b) 内容授权服务器识别许可证请求消息，并向客户端发送响应消息； c) 客户端解析内容授权服务器发送的响应消息，并终止当前协议。		
符合性判定	a) 内容授权服务器向客户端发送“invalidCertificateChain”状态，且许可证获取响应消息格式、内容均符合GY/T 277—2019中8.3的规定； b) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.1.10 对许可证请求DRM客户端证书签名错误的处理功能的测试方法如下：

测试编号	License_010	项目属性	必选
测试对象	内容授权服务器		
测试描述	测试内容授权服务器对客户端许可证请求中包含错误签名的DRM客户端证书的处理功能。		
预置条件	设备： a) DRM客户端（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成数字证书的置入，其中DRM客户端证书签名错误。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息中DRM客户端证书签名错误； b) 内容授权服务器识别许可证请求消息，并向客户端发送响应消息； c) 客户端解析内容授权服务器返回的响应消息，并终止当前协议。		
符合性判定	a) 内容授权服务器向客户端发送“invalidCertificateChain”状态，且许可证获取响应消息格式、内容均符合GY/T 277—2019中8.3的规定； b) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.1.11 对许可证请求DRM客户端证书有效期-UTC Time-NotBefore的处理功能的测试方法如下：

测试编号	License_011	项目属性	必选
测试对象	内容授权服务器		
测试描述	测试内容授权服务器对客户端许可证请求中包含DRM客户端证书有效期-UTC Time-NotBefore的处理功能。		
预置条件	设备： a) DRM客户端（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成数字证书的置入，其中DRM客户端证书有效期-UTC Time-NotBefore不满足。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息中DRM客户端证书有效期-UTC Time-NotBefore不满足； b) 内容授权服务器识别许可证请求消息，并向客户端发送响应消息； c) 客户端解析内容授权服务器发送的响应消息，并终止当前协议。		
符合性判定	a) 内容授权服务器向客户端发送“invalidCertificateChain”状态，且许可证获取响应消息格式、内容均符合GY/T 277—2019中8.3的规定； b) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.1.12 对许可证请求DRM客户端证书有效期-UTC Time-NotAfter的处理功能的测试方法如下：

测试编号	License_012	项目属性	必选
测试对象	内容授权服务器		
测试描述	测试内容授权服务器对客户端许可证请求中包含DRM客户端证书有效期-UTC Time-NotAfter的处理功能。		
预置条件	设备： a) DRM客户端（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成数字证书的置入，其中DRM客户端证书有效期-UTC Time-NotAfter不满足。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息中DRM客户端CA证书有效期-UTC Time-NotAfter不满足； b) 内容授权服务器识别许可证请求消息，并向客户端发送响应消息； c) 客户端解析内容授权服务器返回的响应消息，并终止当前协议。		
符合性判定	a) 内容授权服务器向客户端发送“invalidCertificateChain”状态，且许可证获取响应消息格式、内容均符合GY/T 277—2019中8.3的规定； b) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.1.13 对许可证请求Revoked DRM客户端证书的处理功能的测试方法如下：

测试编号	License_013	项目属性	必选
测试对象	内容授权服务器		
测试描述	测试内容授权服务器对客户端许可证请求中包含被注销掉的DRM客户端证书的处理功能。		
预置条件	设备： a) DRM客户端（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成数字证书的置入，其中DRM客户端证书被注销。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息中DRM客户端证书被注销； b) 内容授权服务器识别许可证请求消息，并向客户端发送响应消息； c) 客户端解析内容授权服务器返回的响应消息，并终止当前协议。		
符合性判定	a) 内容授权服务器向客户端发送“invalidCertificateChain”状态，且许可证获取响应消息格式、内容均符合GY/T 277—2019中8.3的规定； b) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.1.14 对许可证请求缺少协议版本参数内容授权服务器的处理功能的测试方法如下：

测试编号	License_014	项目属性	必选
测试对象	内容授权服务器		
测试描述	测试内容授权服务器对客户端许可证请求中缺少协议版本参数的处理。		
预置条件	设备： a) DRM客户端（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入；		
测试步骤	a) DRM客户端向内容授权服务器发送许可证请求，其中缺少version参数或version值为空； b) 内容授权服务器识别许可证请求消息，并向客户端发送响应消息； c) DRM客户端解析许可证获取响应消息消息，并终止当前协议。		
符合性判定	a) 内容授权服务器向客户端发送“malformedRequest”状态，且许可证获取响应消息格式、内容均符合GY/T 277—2019中8.3的规定； b) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.1.15 对内容授权服务器不支持许可证请求的协议版本的处理功能的测试方法如下：

测试编号	License_015	项目属性	必选
测试对象	内容授权服务器		
测试描述	测试内容授权服务器对客户端所使用的协议版本请求不支持的处理功能。		

预置条件	设备： a) DRM客户端（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。
测试步骤	a) DRM客户端向内容授权服务器发送许可证请求，请求中Version不被内容授权服务器支持； b) 内容授权服务器识别许可证请求消息，并向客户端发送响应消息； c) DRM客户端解析许可证获取响应消息消息，并终止当前协议。
符合性判定	a) 内容授权服务器向客户端发送“versionNotSupported”状态，且许可证获取响应消息格式、内容均符合GY/T 277—2019中8.3的规定； b) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。

A.2.1.16 对许可证请求缺少请求时间的处理功能的测试方法如下：

测试编号	License_016	项目属性	必选
测试对象	内容授权服务器		
测试描述	测试内容授权服务器对客户端许可证请求中缺少请求时间参数的处理。		
预置条件	设备： a) DRM客户端（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。		
测试步骤	a) DRM客户端向内容授权服务器发送许可证请求，请求中缺少requestTime参数或requestTime值为空； b) 内容授权服务器识别许可证请求消息，并向客户端发送响应消息； c) DRM客户端解析许可证获取响应消息消息，并终止当前协议。		
符合性判定	a) 内容授权服务器向客户端发送“malformedReques”状态，且许可证获取响应消息格式、内容均符合GY/T 277—2019中8.3的规定； b) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.1.17 对DRM客户端与内容授权服务器时间不一致的许可证请求的处理功能的测试方法如下：

测试编号	License_017	项目属性	必选
测试对象	内容授权服务器		
测试描述	测试内容授权服务器对客户端许可证请求中DRM客户端时间错误的处理功能。		
预置条件	设备： a) DRM客户端（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。		

测试步骤	a) DRM客户端向内容授权服务器发送许可证请求，请求中包含错误的RequestTime参数； b) 内容授权服务器识别许可证请求消息，并向客户端发送响应消息； c) DRM客户端解析许可证获取响应消息消息，并终止当前协议。
符合性判定	a) 内容授权服务器向客户端发送“deviceTimeError”状态，且许可证获取响应消息格式、内容均符合GY/T 277—2019中8.3的规定； b) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。

A.2.1.18 对许可证请求缺少客户端随机数的处理功能的测试方法如下：

测试编号	License_018	项目属性	必选
测试对象	内容授权服务器		
测试描述	测试内容授权服务器对客户端许可证请求中缺少客户端随机数参数的处理。		
预置条件	设备： a) DRM客户端（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。		
测试步骤	a) DRM客户端向内容授权服务器发送许可证请求，请求中缺少DeviceNonce参数或DeviceNonce值为空； b) 内容授权服务器识别许可证请求消息，并向客户端发送响应消息； c) DRM客户端解析许可证获取响应消息消息，并终止当前协议。		
符合性判定	a) 内容授权服务器向客户端发送“malformedReques”状态，且许可证获取响应消息格式、内容均符合GY/T 277—2019中8.3的规定； b) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.1.19 对许可证请求DeviceNonce每次不一样内容授权服务器的处理功能的测试方法如下：

测试编号	License_019	项目属性	必选
测试对象	内容授权服务器		
测试描述	测试内容授权服务器对客户端许可证每次请求中包含客户端随机数不同的处理。		
预置条件	设备： a) DRM客户端（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。		
测试步骤	a) DRM客户端向内容授权服务器发送许可证请求，请求中deviceNonce参数每次不同； b) 内容授权服务器识别许可证请求消息，并向客户端发送响应消息； c) DRM客户端解析许可证获取响应消息。		
符合性判定	a) 内容授权服务器向客户端发送正确响应，且许可证获取响应消息格式、内容均符合GY/T 277—2019中8.3的规定； b) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.1.20 对许可证请求缺少支持算法的处理功能的测试方法如下：

测试编号	License_020	项目属性	必选
测试对象	内容授权服务器		
测试描述	测试内容授权服务器对客户端许可证请求中缺少支持算法参数的处理。		
预置条件	设备： a) DRM客户端（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。		
测试步骤	a) DRM客户端向内容授权服务器发送许可证请求，求中缺少supportedAlgorithms参数或supportedAlgorithms值为空 ； b) 内容授权服务器识别许可证请求消息，并向客户端发送响应消息； c) DRM客户端解析许可证获取响应消息消息，并终止当前协议。		
符合性判定	a) 内容授权服务器向客户端发送“malformedReques”状态，且许可证获取响应消息格式、内容均符合GY/T 277—2019中8.3的规定； b) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.1.21 对许可证请求支持算法错误内容授权服务器的处理功能的测试方法如下：

测试编号	License_021	项目属性	必选
测试对象	内容授权服务器		
测试描述	测试内容授权服务器对客户端许可证请求中包含错误的支持算法参数的处理。		
预置条件	设备： a) DRM客户端（测试平台）； b) 内容授权服务器； c) OCSP服务器； 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。		
测试步骤	a) DRM客户端向内容授权服务器发送许可证请求，请求中supportedAlgorithms参数错误； b) 内容授权服务器识别许可证请求消息，并向客户端发送响应消息； c) DRM客户端解析许可证获取响应消息消息，并终止当前协议。		
符合性判定	a) 内容授权服务器向客户端发送“abort”状态，且许可证获取响应消息格式、内容均符合GY/T 277—2019中8.3的规定； b) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.1.22 对许可证请求缺少客户端标识的处理功能的测试方法如下：

测试编号	License_022	项目属性	必选
测试对象	内容授权服务器		
测试描述	测试内容授权服务器对客户端许可证请求中缺少客户端标识参数的处理。		

预置条件	设备： a) DRM客户端（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。
测试步骤	a) DRM客户端向内容授权服务器发送许可证请求，求中缺少DeviceID参数或DeviceID值为空； b) 内容授权服务器识别许可证请求消息，并向客户端发送响应消息； c) DRM客户端解析许可证获取响应消息消息，并终止当前协议。
符合性判定	a) 内容授权服务器向客户端发送“malformedReques”状态，且许可证获取响应消息格式、内容均符合GY/T 277—2019中8.3的规定； b) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。

A.2.1.23 对许可证请求客户端标识错误内容授权服务器的处理功能的测试方法如下：

测试编号	License_023	项目属性	必选
测试对象	内容授权服务器		
测试描述	测试内容授权服务器对客户端许可证请求中包含错误的客户端标识参数的处理。		
预置条件	设备： a) DRM客户端（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。		
测试步骤	a) DRM客户端向内容授权服务器发送许可证请求，请求中DeviceID参数错误； b) 内容授权服务器识别许可证请求消息，并向客户端发送响应消息； c) DRM客户端解析许可证获取响应消息消息，并终止当前协议。		
符合性判定	a) 内容授权服务器向客户端发送“abort”状态，且许可证获取响应消息格式、内容均符合GY/T 277—2019中8.3的规定； b) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.1.24 对无法找到DRM客户端许可证对象的请求的处理功能的测试方法如下：

测试编号	License_024	项目属性	必选
测试对象	内容授权服务器		
测试描述	测试内容授权服务器无法找到客户端许可证请求的许可证内容标识信息授权的处理功能。		
预置条件	设备： a) DRM客户端（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。		

测试步骤	a) DRM客户端向内容授权服务器发送许可证请求； b) 内容授权服务器识别许可证请求消息，并向客户端发送响应消息； c) DRM客户端解析许可证获取响应消息消息，并终止当前协议。
符合性判定	a) 内容授权服务器向客户端发送“contentIDNotFound”状态，且许可证获取响应消息格式、内容均符合GY/T 277—2019中8.3的规定； b) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。

A.2.1.25 对许可证请求缺少内容标识的处理功能的测试方法如下：

测试编号	License_025	项目属性	必选
测试对象	内容授权服务器		
测试描述	测试内容授权服务器对客户端许可证请求中缺少内容标识参数的处理。		
预置条件	设备： a) DRM客户端（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。		
测试步骤	a) DRM客户端向内容授权服务器发送许可证请求，求中缺少ContentID参数或ContentID值为空； b) 内容授权服务器识别许可证请求消息，并向客户端发送响应消息； c) DRM客户端解析许可证获取响应消息消息，并终止当前协议。		
符合性判定	a) 内容授权服务器向客户端发送“malformedReques”状态，且许可证获取响应消息格式、内容均符合GY/T 277—2019中8.3的规定； b) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.1.26 对许可证请求缺少证书链的处理功能的测试方法如下：

测试编号	License_026	项目属性	必选
测试对象	内容授权服务器		
测试描述	测试内容授权服务器对客户端许可证请求中缺少客户端证书链参数的处理。		
预置条件	设备： a) DRM客户端（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。		
测试步骤	a) DRM客户端向内容授权服务器发送许可证请求，请求中缺少certificateChain参数或certificateChain值为空； b) 内容授权服务器识别许可证请求消息，并向客户端发送响应消息； c) DRM客户端解析许可证获取响应消息消息，并终止当前协议。		
符合性判定	a) 内容授权服务器向客户端发送“malformedReques”状态，且许可证获取响应消息格式、内容均符合GY/T 277—2019中8.3的规定； b) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.1.27 对许可证请求证书链不对应内容授权服务器的处理功能的测试方法如下：

测试编号	License_027	项目属性	必选
测试对象	内容授权服务器		
测试描述	测试内容授权服务器对客户端许可证请求中客户端证书链不能验证的处理。		
预置条件	设备： a) DRM客户端（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。		
测试步骤	a) DRM客户端向内容授权服务器发送许可证请求，客户端证书不是由DRM客户端CA签发的； b) 内容授权服务器识别许可证请求消息，并向客户端发送响应消息； c) DRM客户端解析许可证获取响应消息消息，并终止当前协议。		
符合性判定	a) 内容授权服务器向客户端发送“invalidCertificateChain”状态，且许可证获取响应消息格式、内容均符合GY/T 277—2019中8.3的规定； b) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.1.28 对获取无限制播放授权的处理功能的测试方法如下：

测试编号	License_028	项目属性	可选
测试对象	内容授权服务器		
测试描述	测试许可证中密钥使用规则为无限制播放授权时在客户端的播放权限功能。		
预置条件	设备： a) DRM客户端（测试平台） b) 内容授权服务器； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入； c) 内容授权服务器存在且仅存在1条该客户端的业务授权数据，授权规则为无限制播放授权。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送许可证响应消息，发送许可证响应消息，许可证中密钥使用规则为无限制播放； c) DRM客户端解析内容授权服务器发送的许可证格式； d) 查看DRM客户端播放权限。		
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果显示许可证响应消息格式、内容均正确，符合GY/T 277—2019中8.3的规定； c) DRM客户端解析许可证的密钥使用规则单元keyRulesNum为0，播放权限为无限制播放，许可证中的授权仅包括且严格遵循业务授权，符合GY/T 277—2019中7.2.6的规定； d) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.1.29 对获取按时间段播放授权的处理功能的测试方法如下：

测试编号	License_029	项目属性	可选
测试对象	内容授权服务器		
测试描述	测试许可证中密钥使用规则为按时间段授权播放时在客户端的播放权限功能。		
预置条件	设备： a) DRM客户端（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入； c) 内容授权服务器存在且仅存在1条该客户端的业务授权数据，授权规则为按时间段授权。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送许可证响应消息； c) DRM客户端解析内容授权服务器发送的许可证格式； d) 查看DRM客户端播放权限。		
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果显示许可证响应消息格式、内容均正确，符合GY/T 277—2019中8.3的规定； c) DRM客户端解析许可证的密钥使用规则单元keyRulesNum为1，keyRuleType为时间段，播放权限为按时间段授权播放，许可证中的授权仅包括且严格遵循业务授权数据，符合GY/T 277—2019中7.2.6的规定； d) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.1.30 对获取按次数播放授权的处理功能的测试方法如下：

测试编号	License_030	项目属性	可选
测试对象	内容授权服务器		
测试描述	测试许可证中密钥使用规则为按次数授权播放时在客户端的播放权限功能。		
预置条件	设备： a) DRM客户端（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入； c) 内容授权服务器存在且仅存在1条该客户端的业务授权数据，授权规则为按次数授权。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送许可证响应消息； c) DRM客户端解析内容授权服务器发送的许可证格式； d) 查看DRM客户端播放权限。		

符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果显示许可证响应消息格式、内容均正确，符合GY/T 277—2019中8.3的规定； c) DRM客户端解析许可证的密钥使用规则单元keyRulesNum为1，keyRuleType为次数，播放权限为按次数授权播放，许可证中的授权仅包括且严格遵循业务授权数据，符合GY/T 277—2019中7.2.6的规定； d) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。

A.2.1.31 对获取按时长播放授权的处理功能的测试方法如下：

测试编号	License_031	项目属性	可选
测试对象	内容授权服务器		
测试描述	测试许可证中密钥使用规则为按时长授权播放时在客户端的播放权限功能。		
预置条件	设备： a) DRM客户端（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入； c) 内容授权服务器存在且仅存在1条该客户端的业务授权数据，授权规则为按时长授权。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送许可证响应消息； c) DRM客户端解析内容授权服务器发送的许可证格式； d) 查看DRM客户端播放权限。		
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果显示许可证响应消息格式、内容均正确，符合GY/T 277—2019中8.3的规定； c) DRM客户端解析许可证的密钥使用规则单元keyRulesNum为2，keyRuleType分别为起始时间和截止时间，播放权限为按时长授权播放，许可证中的授权仅包括且严格遵循业务授权数据，符合GY/T 277—2019中7.2.6的规定； d) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.1.32 对按累计时间段播放授权的处理功能的测试方法如下：

测试编号	License_032	项目属性	可选
测试对象	内容授权服务器		
测试描述	测试许可证中密钥使用规则为按累计时间段授权播放时在客户端的播放权限功能。		
预置条件	设备： a) DRM客户端（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入； c) 内容授权服务器存在且仅存在1条该客户端的业务授权数据，授权规则为按累计时间段授权。		

测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送许可证响应消息； c) DRM客户端解析内容授权服务器发送的许可证格式； d) 查看DRM客户端播放权限。
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果显示许可证响应消息格式、内容均正确，符合GY/T 277—2019中8.3的规定； c) DRM客户端解析许可证的密钥使用规则单元keyRulesNum为1，keyRuleType为累计时间段，播放权限为按累计时间段授权播放，许可证中的授权仅包括且严格遵循业务授权数据，符合GY/T 277—2019中7.2.6的规定； d) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。

A.2.1.33 对按输出规则无限制播放授权的处理功能的测试方法如下：

测试编号	License_033	项目属性	可选
测试对象	内容授权服务器		
测试描述	测试许可证中密钥使用规则为按输出规则没有限制授权播放时在客户端的播放权限功能。		
预置条件	设备： a) DRM客户端（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入； c) 内容授权服务器存在且仅存在1条该客户端的业务授权数据，授权规则为按输出规则没有限制授权。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送许可证响应消息； c) DRM客户端解析内容授权服务器发送的许可证格式； d) 查看DRM客户端播放权限。		
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果显示许可证响应消息格式、内容均正确，符合GY/T 277—2019中8.3的规定； c) DRM客户端解析许可证的密钥使用规则单元keyRulesNum为1，keyRuleType为输出规则，播放权限为无输出规则限制授权播放，许可证中的授权仅包括且严格遵循业务授权数据，符合GY/T 277—2019中7.2.6的规定； d) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.1.34 对按输出规则为HDCP1.4播放授权的处理功能的测试方法如下：

测试编号	License_034	项目属性	可选
测试对象	内容授权服务器		
测试描述	测试许可证中密钥使用规则为输出规则为支持HDCP1.4授权播放时在客户端的播放权限功能。		

预置条件	设备： a) DRM客户端（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入； c) 内容授权服务器存在且仅存在1条该客户端的业务授权数据，授权规则为按测试许可证中密钥使用规则为输出规则为支持HDCP1.4授权。
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送许可证响应消息； c) DRM客户端解析内容授权服务器发送的许可证格式； d) 查看DRM客户端播放权限。
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果显示许可证响应消息格式、内容均正确，符合GY/T 277—2019中8.3的规定； c) DRM客户端解析许可证的密钥使用规则单元keyRulesNum为1，keyRuleType为输出规则，播放权限为按输出规则为HDCP1.4授权播放，许可证中的授权仅包括且严格遵循业务授权数据，符合GY/T 277—2019中7.2.6的规定； d) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。

A.2.1.35 对按输出规则为HDCP2.2播放授权的处理功能的测试方法如下：

测试编号	License_035	项目属性	可选
测试对象	内容授权服务器		
测试描述	测试许可证中密钥使用规则为按测试许可证中密钥使用规则为输出规则为支持HDCP2.2授权播放时在客户端的播放权限功能。		
预置条件	设备： a) DRM客户端（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入； c) 内容授权服务器存在且仅存在1条该客户端的业务授权数据，授权规则为输出规则为HDCP2.2授权。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送许可证响应消息； c) DRM客户端解析内容授权服务器发送的许可证格式； d) 查看DRM客户端播放权限。		

符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果显示许可证响应消息格式、内容均正确，符合GY/T 277—2019中8.3的规定； c) DRM客户端解析许可证的密钥使用规则单元keyRulesNum为1，keyRuleType为输出规则，播放权限为按输出规则为HDCP2.2授权播放，许可证中的授权仅包括且严格遵循业务授权数据，符合GY/T 277—2019中7.2.6的规定； d) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。

A.2.1.36 对按输出规则不允许播放授权的处理功能的测试方法如下：

测试编号	License_036	项目属性	可选
测试对象	内容授权服务器		
测试描述	测试许可证中密钥使用规则为按测试许可证中密钥使用规则为输出规则不允许授权播放时在客户端的播放权限功能。		
预置条件	设备： a) DRM客户端（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入； c) 内容授权服务器存在且仅存在1条该客户端的业务授权数据，授权规则为按输出规则不允许授权。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送许可证响应消息； c) DRM客户端解析内容授权服务器发送的许可证格式； d) 查看DRM客户端播放权限。		
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果显示许可证响应消息格式、内容均正确，符合GY/T 277—2019中8.3的规定； c) DRM客户端解析许可证的密钥使用规则单元keyRulesNum为1，keyRuleType为输出规则，播放权限为按输出规则不允许授权播放，许可证中的授权仅包括且严格遵循业务授权数据，符合GY/T 277—2019中7.2.6的规定； d) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.1.37 测试对按软件安全级别播放授权的处理功能的测试方法如下：

测试编号	License_037	项目属性	可选
测试对象	内容授权服务器		
测试描述	测试许可证中密钥使用规则为软件安全级别授权播放时在客户端的播放权限功能。		

预置条件	设备： a) DRM客户端（测试平台）； b) 内容授权服务器； c) OCSP服务器； 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入； c) 内容授权服务器存在且仅存在1条该客户端的业务授权数据，授权规则为软件安全级别授权。
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送许可证响应消息； c) DRM客户端解析内容授权服务器发送的许可证格式； d) 查看DRM客户端播放权限。
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果显示许可证响应消息格式、内容均正确，符合GY/T 277—2019中8.3的规定； c) DRM客户端解析许可证的密钥使用规则单元keyRulesNum为1，keyRuleType为客户端安全等级要求，播放权限为按软件安全等级授权播放，许可证中的授权仅包括且严格遵循业务授权数据，符合GY/T 277—2019中7.2.6的规定； d) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。

A.2.1.38 对按硬件安全级别播放授权的处理功能的测试方法如下：

测试编号	License_038	项目属性	可选
测试对象	内容授权服务器		
测试描述	测试许可证中密钥使用规则为硬件安全级别授权播放时在客户端的播放权限功能。		
预置条件	设备： a) DRM客户端（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入； c) 内容授权服务器存在且仅存在1条该客户端的业务授权数据，授权规则为硬件安全级别授权。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送许可证响应消息； c) DRM客户端解析内容授权服务器发送的许可证格式； d) 查看DRM客户端播放权限。		
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果显示许可证响应消息格式、内容均正确，符合GY/T 277—2019中8.3的规定； c) DRM客户端解析许可证的密钥使用规则单元keyRulesNum为1，keyRuleType为客户端安全等级要求，播放权限为按硬件安全等级授权播放，许可证中的授权仅包括且严格遵循业务授权数据，符合GY/T 277—2019中7.2.6的规定； d) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.1.39 对按增强安全级别播放授权的处理功能的测试方法如下：

测试编号	License_039	项目属性	可选
测试对象	内容授权服务器		
测试描述	测试许可证中密钥使用规则为增强硬件安全级别授权播放时在客户端的播放权限功能。		
预置条件	设备： a) DRM客户端（测试平台）； b) 内容授权服务器； c) OCSP服务器； 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入； c) 内容授权服务器存在且仅存在1条该客户端的业务授权数据，授权规则为增强硬件安全级别授权。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送许可证响应消息； c) DRM客户端解析内容授权服务器发送的许可证格式； d) 查看DRM客户端播放权限。		
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果显示许可证响应消息格式、内容均正确，符合GY/T 277—2019中8.3的规定； c) DRM客户端解析许可证的密钥使用规则单元keyRulesNum为1，keyRuleType为客户端安全等级要求，播放权限为按增强硬件安全级别授权播放，许可证中的授权仅包括且严格遵循业务授权数据，符合GY/T 277—2019中7.2.6的规定； d) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.2 DRM客户端测试

A.2.2.1 对许可证获取响应的处理功能的测试方法如下：

测试编号	License_040	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器的许可证获取响应的处理功能。		
预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器处理请求消息，并发送许可证的响应消息； c) DRM客户端解析许可证获取响应消息。		

符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) 客户端解析结果显示许可证响应消息格式、内容均正确，符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。

A.2.2.2 对许可证包含多个内容标识授权的响应的处理功能的测试方法如下：

测试编号	License_041	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器许可证响应中包含多个内容标识的授权信息的处理功能。		
预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送许可证响应中包含多个内容标识的授权信息； c) 客户端解析内容授权服务器发送的响应。		
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析出多个内容标识的授权信息，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.2.3 对许可证响应缺少状态的处理功能的测试方法如下：

测试编号	License_042	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器许可证响应中缺少状态参数的处理功能。		
预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送中缺少status参数或status值为空的许可证响应消息； c) 客户端解析内容授权服务器发送的响应消息，并终止当前协议。		
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果缺少status字段，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.2.4 对许可证响应状态≠success的处理功能的测试方法如下：

测试编号	License_043	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器许可证响应中status≠success的处理功能。		
预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送status参数不等于success的响应消息； c) 客户端解析内容授权服务器发送的响应消息，并终止当前协议。		
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果status≠success，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.2.5 对许可证响应缺少数字签名的处理功能的测试方法如下：

测试编号	License_044	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器许可证响应中缺少数字签名参数的处理功能。		
预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送发送缺少数字签名参数许可证响应消息； c) 客户端解析内容授权服务器返回的响应消息，并终止当前协议。		
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果缺少数字签名参数，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.2.6 对许可证响应数字签名错误的处理功能的测试方法如下：

测试编号	License_045	项目属性	必选
测试对象	DRM客户端		

测试描述	测试DRM客户端对内容授权服务器许可证响应中数字签名错误的处理功能。
预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送signature参数错误的响应消息； c) 客户端解析内容授权服务器发送的响应消息，并终止当前协议。
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果数字签名字段错误，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。

A.2.2.7 对许可证响应DRM服务端CA证书没有签名的处理功能的测试方法如下：

测试编号	License_046	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器许可证响应中包含没有签名的DRM服务端CA证书的处理功能。		
预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成数字证书的置入，其中DRM服务端CA证书没有签名； b) DRM客户端已完成合法数字证书的置入。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送包含没有签名的DRM Server CA证书的许可证响应消息； c) 客户端解析内容授权服务器返回的响应消息，并终止当前协议。		
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果DRM服务端CA证书格式错误，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.2.8 测试对许可证响应DRM服务端CA证书签名错误的处理功能的测试方法如下：

测试编号	License_047	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器许可证响应中包含错误有签名的DRM服务端CA证书的处理功能。		

预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成数字证书的置入，其中DRM服务端CA证书签名错误； b) DRM客户端已完成合法数字证书的置入。
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送包含错误签名的DRM服务端CA证书的响应消息； c) 客户端解析内容授权服务器返回的响应消息，并终止当前协议。
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果DRM客户端DRM服务端CA证书验证失败，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。

A.2.2.9 对许可证响应DRM服务端CA证书有效期-UTC Time-NotBefore的处理功能的测试方法如下：

测试编号	License_048	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器许可证响应中包含DRM服务端CA证书有效期-UTC Time-NotBefore不满足的处理功能。		
预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成数字证书的置入，其中其中DRM服务端CA证书有效期-UTC Time-NotBefore不满足； b) DRM客户端已完成合法数字证书的置入。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送DRM服务端CA证书有效期-UTC Time-NotBefore不满足的响应消息； c) 客户端解析内容授权服务器发送的响应消息，并终止当前协议。		
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果DRM服务端CA证书验证失败，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.2.10 对许可证响应DRM服务端CA证书有效期-UTC Time-NotAfter的处理功能的测试方法如下：

测试编号	License_049	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器许可证响应中DRM服务端CA证书有效期-UTC Time-NotAfter不满足的		

	处理功能。
预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成数字证书的置入，其中其中DRM服务端CA证书有效期-UTC Time-NotAfter不满； b) DRM客户端已完成合法数字证书的置入。
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送发送DRM服务端CA证书有效期-UTC Time-NotAfter不满足的许可证响应消息； c) 客户端解析内容授权服务器返回的响应消息，并终止当前协议。
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果DRM服务端CA证书验证失败，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。

A.2.2.11 对许可证响应DRM 服务端证书没有签名的处理功能的测试方法如下：

测试编号	License_050	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器许可证响应中包含没有签名的DRM 服务端证书的处理功能。		
预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成数字证书的置入，其中DRM服务端证书没有数字签名； b) DRM客户端已完成合法数字证书的置入。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送包含没有签名的DRM服务端证书的响应消息； c) 客户端解析内容授权服务器发送的响应消息，并终止当前协议。		
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果DRM 服务端证书格式错误，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.2.12 对许可证响应DRM 服务端证书签名错误的处理功能的测试方法如下：

测试编号	License_051	项目属性	必选
测试对象	DRM客户端		

测试描述	测试DRM客户端对内容授权服务器许可证响应中包含签名错误的DRM 服务端证书的处理功能。
预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成数字证书的置入，其中DRM 服务端证书数字签名错误； b) DRM客户端已完成合法数字证书的置入。
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送发送包含签名错误的DRM 服务端证书的许可证响应消息； c) 客户端解析内容授权服务器返回的响应消息，并终止当前协议。
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果其中DRM 服务端证书验证失败，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。

A.2.2.13 对许可证响应DRM 服务端证书有效期-UTC Time-NotBefore的处理功能的测试方法如下：

测试编号	License_052	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器许可证响应中DRM 服务端证书有效期-UTC Time-NotBefore不满足的处理功能。		
预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成数字证书的置入，其中DRM 服务端证书证书有效期-UTC Time-NotBefore不满足； b) DRM客户端已完成合法数字证书的置入。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送DRM 服务端证书有效期-UTC Time-NotBefore不满足的响应消息； c) 客户端解析内容授权服务器发送的响应消息，并终止当前协议。		
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果DRM 服务端证书验证失败，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.2.14 对许可证响应DRM 服务端证书有效期-UTC Time-NotAfter的处理功能的测试方法如下：

测试编号	License_016	项目属性	必选

测试对象	DRM客户端
测试描述	测试DRM客户端对内容授权服务器许可证响应中DRM 服务端证书有效期-UTC Time-NotAfter不满足的处理功能。
预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成数字证书的置入，其中DRM 服务端证书有效期-UTC Time-NotAfter不满足； b) DRM客户端已完成合法数字证书的置入。
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送发送DRM 服务端证书有效期-UTC Time-NotAfter不满足的许可证响应消息； c) 客户端解析内容授权服务器返回的响应消息，并终止当前协议。
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果DRM 服务端证书验证失败，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。

A.2.2.15 对许可证响应缺少OCSP响应的处理功能的测试方法如下：

测试编号	License_054	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器许可证响应中缺少OCSP响应的处理功能。		
预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送发送缺少OCSP响应的许可证响应消息； c) 客户端解析内容授权服务器返回的响应消息，并终止当前协议。		
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果缺少OCSP响应参数，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.2.16 对许可证响应中OCSP响应缺少数字签名的处理功能的测试方法如下：

测试编号	License_055	项目属性	必选

测试对象	DRM客户端
测试描述	测试DRM客户端对内容授权服务器许可证响应中OCSP响应缺少数字签名的处理功能。
预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送缺少数字签名的OCSP响应的许可证响应消息； c) 客户端解析内容授权服务器返回的响应消息，并终止当前协议。
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果OCSP响应格式错误，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。

A.2.2.17 对许可证响应中OCSP响应数字签名错误的处理功能的测试方法如下：

测试编号	License_056	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器许可证响应中OCSP响应数字签名错误的处理功能。		
预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送OCSP响应数字签名错误的响应消息； c) 客户端解析内容授权服务器发送的响应消息，并终止当前协议。		
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果OCSP响应数字签名错误，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.2.18 对许可证响应中OCSP Response状态不等于success的处理功能的测试方法如下：

测试编号	License_057	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器许可证响应中OCSP响应status≠success的处理功能。		

预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送OCSP响应状态不等于success的响应消息； c) 客户端解析内容授权服务器发送的响应消息，并终止当前协议。
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果OCSP响应状态不成功，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。

A.2.2.19 对许可证响应中OCSP响应的有效期-thisUpdate的处理功能的测试方法如下：

测试编号	License_058	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器许可证响应中OCSP响应的有效期-thisUpdate不满足的处理功能。		
预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送OCSP响应的有效期-thisUpdate不满足许可证响应消息； c) 客户端解析内容授权服务器返回的响应消息，并终止当前协议。		
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果OCSP响应验证失败，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.2.20 对许可证响应中OCSP响应有效期-nextUpdate的处理功能的测试方法如下：

测试编号	License_059	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器许可证响应中OCSP响应的有效期-nextUpdate不满足的处理功能。		

预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送OCSP响应的有效期-nextUpdate不满足的响应消息； c) 客户端解析内容授权服务器发送的响应消息，并终止当前协议。
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果OCSP响应验证失败，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。

A.2.2.21 对许可证响应OCSP响应中的CertID不正确的处理功能的测试方法如下：

测试编号	License_060	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器许可证响应中OCSP响应中的CertID不正确的处理功能。		
预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送OCSP响应中的CertID不正确的许可证响应消息； c) 客户端解析内容授权服务器返回的响应消息，并终止当前协议。		
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果OCSP响应中的CertID不正确，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.2.22 对许可证响应OCSP响应中的Revocation Status=‘REVOKED’的处理功能的测试方法如下：

测试编号	License_061	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器许可证响应中OCSP响应中的Revocation Status=‘REVOKED’的处理功能。		

预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送OCSP响应中的Revocation Status=‘REVOKED’的响应消息； c) 客户端解析内容授权服务器发送的响应消息，并终止当前协议。
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果OCSP响应中的Revocation Status=‘REVOKED’，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。

A.2.2.23 对许可证响应OCSP响应中的Revocation Status=‘UNKNOWN’的处理功能的测试方法如下：

测试编号	License_062	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器许可证响应中OCSP响应中的Revocation Status=‘UNKNOWN’的处理功能。		
预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送OCSP响应中的Revocation Status=‘UNKNOWN’的许可证响应消息； c) 客户端解析内容授权服务器返回的响应消息，并终止当前协议。		
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果OCSP响应中的Revocation Status=‘UNKNOWN’，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.2.24 对许可证响应缺少OCSP Responder的证书的数字签名的处理功能的测试方法如下：

测试编号	License_063	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器许可证响应中OCSP Responder的证书缺少数字签名的处理功能。		

预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送OCSP Responder的证书缺少数字签名的响应消息； c) 客户端解析内容授权服务器发送的响应消息，并终止当前协议。
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果OCSP Responder格式错误，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。

A.2.2.25 对许可证响应OCSP Responder的证书的数字签名错误的处理功能的测试方法如下：

测试编号	License_064	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器许可证响应中OCSP Responder的证书的数字签名错误的处理功能。		
预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送OCSP Responder错误数字签名证书的许可证响应消息； c) 客户端解析内容授权服务器返回的响应消息，并终止当前协议。		
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果OCSP Responder的证书验证失败，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.2.26 对许可证响应OCSP响应的证书有效性-NotBefore的处理功能的测试方法如下：

测试编号	License_065	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器许可证响应中OCSP响应的证书有效性-NotBefore不满足的处理功能。		

预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送OCSP响应的证书有效性-NotBefore不满足的许可证响应消息； c) 客户端解析内容授权服务器返回的响应消息，并终止当前协议。
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果OCSP响应验证失败，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。

A.2.2.27 对许可证响应OCSP Responder的证书有效性-NotAfter的处理功能的测试方法如下：

测试编号	License_066	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器许可证响应中OCSP响应的证书有效性-NotAfter的处理功能。		
预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送OCSP响应的证书有效性-NotBefore不满足的响应消息； c) 客户端解析内容授权服务器发送的响应消息，并终止当前协议。		
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果OCSP响应验证失败，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.2.28 对许可证响应缺少协议版本的处理功能的测试方法如下：

测试编号	License_067	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器许可证响应中缺少协议版本参数的处理功能。		

预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送发送缺少version参数许可证响应消息； c) 客户端解析内容授权服务器返回的响应消息，并终止当前协议。
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果缺少协议版本参数，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。

A.2.2.29 对内容授权服务器不支持许可证响应的协议版本的处理功能的测试方法如下：

测试编号	License_068	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器不支持协议版本响应的处理功能。		
预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送不支持协议版本的许可证响应消息； c) 客户端解析内容授权服务器返回的响应消息，并终止当前协议。		
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果许可证响应不支持协议版本，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.2.30 对许可证响应缺少ResponseTime的处理功能的测试方法如下：

测试编号	License_069	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器许可证响应中缺少响应时间参数的处理功能。		

预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送发送缺少ResponseTime参数许可证响应消息； c) 客户端解析内容授权服务器返回的响应消息，并终止当前协议；
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果缺少响应时间参数，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。

A.2.2.31 对DRM客户端与内容授权服务器时间不一致的许可证响应的处理功能的测试方法如下：

测试编号	License_070	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器许可证响应中时间不一致的处理功能。		
预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送包含错误内容授权服务器时间的响应消息； c) 客户端解析内容授权服务器返回的响应消息，并终止当前协议。		
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果响应时间错误，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.2.32 对许可证响应没有ProtectedLicense的处理功能的测试方法如下：

测试编号	License_071	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器许可证响应中没有ProtectedLicense的处理功能。		

预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送没有ProtectedLicense的许可证响应消息； c) 客户端解析内容授权服务器返回的响应消息，并终止当前协议。
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果许可证响应没有ProtectedLicense，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。

A.2.2.33 对许可证响应ProtectedLicense错误的处理功能的测试方法如下：

测试编号	License_072	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器许可证响应中ProtectedLicense错误的处理功能。		
预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送ProtectedLicense参数错误的响应消息； c) 客户端解析内容授权服务器发送的响应消息，并终止当前协议。		
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果ProtectedLicense字段错误，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.2.34 对许可证响应缺少客户端标识的处理功能的测试方法如下：

测试编号	License_073	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器许可证响应中缺少客户端标识参数的处理功能。		

预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送发送缺少DeviceID参数许可证响应消息； c) 客户端解析内容授权服务器返回的响应消息，并终止当前协议。
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果缺少客户端标识参数，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。

A.2.2.35 对许可证响应客户端标识错误的处理功能的测试方法如下：

测试编号	License_074	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器许可证响应中客户端标识错误的处理功能。		
预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送客户端标识参数错误的响应消息； c) 客户端解析内容授权服务器发送的响应消息，并终止当前协。		
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果客户端标识字段错误，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.2.36 对许可证响应缺少内容授权服务器标识的处理功能的测试方法如下：

测试编号	License_075	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器许可证响应中缺少内容授权服务器标识参数的处理功能。		

预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送发送缺少DRMServerID参数许可证响应消息； c) 客户端解析内容授权服务器返回的响应消息，并终止当前协议。
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果缺少内容授权服务器标识参数，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。

A.2.2.37 对许可证响应内容授权服务器标识错误的处理功能的测试方法如下：

测试编号	License_076	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器许可证响应中内容授权服务器标识错误的处理功能。		
预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送内容授权服务器标识错误的响应消息； c) 客户端解析内容授权服务器发送的响应消息，并终止当前协议。		
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果内容授权服务器标识字段错误，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.2.38 对许可证响应缺少设备随机数的处理功能的测试方法如下：

测试编号	License_077	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器许可证响应中缺少设备随机数参数的处理功能。		

预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送发送缺少DeviceNonce参数许可证响应消息； c) 客户端解析内容授权服务器返回的响应消息，并终止当前协议。
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果缺少设备随机数参数，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。

A.2.2.39 对许可证响应设备随机数错误的处理功能的测试方法如下：

测试编号	License_078	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器许可证响应中设备随机数错误的处理功能。		
预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送设备随机数错误的响应消息； c) 客户端解析内容授权服务器发送的响应消息，并终止当前协议。		
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果设备随机数错误，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.2.40 对许可证响应缺少SelectedAlgorithm的处理功能的测试方法如下：

测试编号	License_079	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器许可证响应中缺少选择算法参数的处理功能。		

预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送缺少SelectedAlgorithm参数的许可证响应消息； c) 客户端解析内容授权服务器返回的响应消息，并终止当前协议。
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果缺少选择算法参数，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。

A.2.2.41 对许可证响应SelectedAlgorithm错误的处理功能的测试方法如下：

测试编号	License_080	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器许可证响应中选择算法错误的处理功能。		
预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送选择算法错误的响应消息； c) 客户端解析内容授权服务器发送的响应消息，并终止当前协议。		
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果选择算法错误，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.2.42 对许可证响应内容授权服务器证书链不对应的处理功能的测试方法如下：

测试编号	License_081	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器无法验证服务器使用的证书链响应的处理功能。		

预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成数字证书的置入，其中LI证书不是LICA签发的； b) DRM客户端已完成合法数字证书的置入。
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送许可证响应消息； c) 客户端解析内容授权服务器返回的响应消息，并终止当前协议。
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果证书链无法验证，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。

A.2.2.43 对许可证缺少数字签名的处理功能的测试方法如下：

测试编号	License_082	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器许可证响应中授权许可证缺少数字签名参数的处理功能。		
预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送发送许可证缺少数字签名的许可证响应消息； c) 客户端解析内容授权服务器返回的响应消息，并终止当前协议。		
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果许可证格式错误，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.2.44 对许可证数字签名错误的处理功能的测试方法如下：

测试编号	License_083	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端对内容授权服务器许可证响应中数字签名错误的处理功能。		

预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入。
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送许可证signature参数错误的响应消息； c) 客户端解析内容授权服务器发送的响应消息，并终止当前协议。
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果许可证数字签名字段错误，许可证响应格式符合GY/T 277—2019中8.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。

A.2.2.45 对获取无限制播放授权的处理功能的测试方法如下：

测试编号	License_084	项目属性	可选
测试对象	DRM客户端		
测试描述	测试许可证中密钥使用规则为无限制播放授权时在客户端的播放权限功能。		
预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入； c) 内容授权服务器存在且仅存在1条该客户端的业务授权数据，授权规则为无限制播放授权。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送许可证响应，发送许可证响应消息，许可证中密钥使用规则为无限制播放； c) DRM客户端解析内容授权服务器发送的许可证格式； d) 查看DRM客户端播放权限。		
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果显示许可证响应消息格式、内容均正确，符合GY/T 277—2019中8.3的规定； c) DRM客户端解析许可证的密钥使用规则单元keyRulesNum为0，播放权限为无限制播放，许可证中的授权仅包括且严格遵循业务授权数据，符合GY/T 277—2019中7.2.6的规定； d) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.2.46 对获取按时间段播放授权的处理功能的测试方法如下：

测试编号	License_085	项目属性	可选
测试对象	DRM客户端		
测试描述	测试许可证中密钥使用规则为按时间段授权播放时在客户端的播放权限功能。		
预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入； c) 内容授权服务器存在且仅存在1条该客户端的业务授权数据，授权规则为按时间段授权。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送许可证响应消息； c) DRM客户端解析内容授权服务器发送的许可证格式； d) 查看DRM客户端播放权限。		
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果显示许可证响应消息格式、内容均正确，符合GY/T 277—2019中8.3的规定； c) DRM客户端解析许可证的密钥使用规则单元keyRulesNum为1，keyRuleType为时间段，播放权限为按时间段授权播放，许可证中的授权仅包括且严格遵循业务授权数据，符合GY/T 277—2019中7.2.6的规定； d) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.2.47 对获取按次数播放授权的处理功能的测试方法如下：

测试编号	License_086	项目属性	可选
测试对象	DRM客户端		
测试描述	测试许可证中密钥使用规则为按次数授权播放时在客户端的播放权限功能。		
预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入； c) 内容授权服务器存在且仅存在1条该客户端的业务授权数据，授权规则为按次数授权。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送许可证响应消息； c) DRM客户端解析内容授权服务器发送的许可证格式； d) 查看DRM客户端播放权限。		

符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果显示许可证响应消息格式、内容均正确，符合GY/T 277—2019中8.3的规定； c) DRM客户端解析许可证的密钥使用规则单元keyRulesNum为1，keyRuleType为次数，播放权限为按次数授权播放，许可证中的授权仅包括且严格遵循业务授权数据，符合GY/T 277—2019中7.2.6的规定； d) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。

A.2.2.48 对获取按时长播放授权的处理功能的测试方法如下：

测试编号	License_087	项目属性	可选
测试对象	DRM客户端		
测试描述	测试许可证中密钥使用规则为按时长授权播放时在客户端的播放权限功能。		
预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入； c) 内容授权服务器存在且仅存在1条该客户端的业务授权数据，授权规则为按时长授权。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送许可证响应消息； c) DRM客户端解析内容授权服务器发送的许可证格式； d) 查看DRM客户端播放权限。		
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果显示许可证响应消息格式、内容均正确，符合GY/T 277—2019中8.3的规定； c) DRM客户端解析许可证的密钥使用规则单元keyRulesNum为2，keyRuleType分别为起始时间和截止时间，播放权限为按时长授权播放，许可证中的授权仅包括且严格遵循业务授权数据，符合GY/T 277—2019中7.2.6的规定； d) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.2.49 对按累计时间段播放授权的处理功能的测试方法如下：

测试编号	License_088	项目属性	可选
测试对象	DRM客户端		
测试描述	测试许可证中密钥使用规则为按累计时间段授权播放时在客户端的播放权限功能。		
预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入； c) 内容授权服务器存在且仅存在1条该客户端的业务授权数据，授权规则为按累计时间段授权。		

测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送许可证响应； c) DRM客户端解析内容授权服务器发送的许可证格式； d) 查看DRM客户端播放权限。
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果显示许可证响应消息格式、内容均正确，符合GY/T 277—2019中8.3的规定； c) DRM客户端解析许可证的密钥使用规则单元keyRulesNum为1，keyRuleType为累计时间段，播放权限为按累计时间段授权播放，许可证中的授权仅包括且严格遵循业务授权数据，符合GY/T 277—2019中7.2.6的规定； d) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。

A.2.2.50 对按输出规则无限制播放授权的处理功能的测试方法如下：

测试编号	License_089	项目属性	可选
测试对象	DRM客户端		
测试描述	测试许可证中密钥使用规则为按输出规则授权播放时在客户端的播放权限功能。		
预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入； c) 内容授权服务器存在且仅存在1条该客户端的业务授权数据，授权规则为按无限制输出规则授权。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送许可证响应； c) DRM客户端解析内容授权服务器发送的许可证格式； d) 查看DRM客户端播放权限。		
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果显示许可证响应消息格式、内容均正确，符合GY/T 277—2019中8.3的规定； c) DRM客户端解析许可证的密钥使用规则单元keyRulesNum为1，keyRuleType为输出规则，播放权限为按无限制输出规则授权播放，许可证中的授权仅包括且严格遵循业务授权数据，符合GY/T 277—2019中7.2.6的规定； d) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.2.51 对按输出规则为HDCP1.4播放授权的处理功能的测试方法如下：

测试编号	License_090	项目属性	可选
测试对象	DRM客户端		
测试描述	测试许可证中密钥使用规则为按输出规则为HDCP1.4授权播放时在客户端的播放权限功能。		

预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入； c) 内容授权服务器存在且仅存在1条该客户端的业务授权数据，授权规则为按输出规则为HDCP1.4授权。
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送许可证响应； c) DRM客户端解析内容授权服务器发送的许可证格式； d) 查看DRM客户端播放权限。
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果显示许可证响应消息格式、内容均正确，符合GY/T 277—2019中8.3的规定； c) DRM客户端解析许可证的密钥使用规则单元keyRulesNum为1，keyRuleType为输出规则，播放权限为按输出规则为HDCP1.4授权播放，许可证中的授权仅包括且严格遵循业务授权数据，符合GY/T 277—2019中7.2.6的规定； d) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。

A.2.2.52 对按输出规则为HDCP2.2播放授权的处理功能的测试方法如下：

测试编号	License_091	项目属性	可选
测试对象	DRM客户端		
测试描述	测试许可证中密钥使用规则为按输出规则为HDCP2.2授权播放时在客户端的播放权限功能。		
预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入； c) 内容授权服务器存在且仅存在1条该客户端的业务授权数据，授权规则为按输出规则为HDCP2.2授权。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送许可证响应； c) DRM客户端解析内容授权服务器发送的许可证格式； d) 查看DRM客户端播放权限。		

符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果显示许可证响应消息格式、内容均正确，符合GY/T 277—2019中8.3的规定； c) DRM客户端解析许可证的密钥使用规则单元keyRulesNum为1，keyRuleType为输出规则，播放权限为按输出规则位HDCP2.2授权播放，许可证中的授权仅包括且严格遵循业务授权数据，符合GY/T 277—2019中7.2.6的规定； d) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。

A.2.2.53 对按输出规则不允许播放授权的处理功能的测试方法如下：

测试编号	License_092	项目属性	可选
测试对象	DRM客户端		
测试描述	测试许可证中密钥使用规则为按输出规则不允许授权播放时在客户端的播放权限功能。		
预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入； c) 内容授权服务器存在且仅存在1条该客户端的业务授权数据，授权规则为按累输出规则不允许授权。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送许可证响应； c) DRM客户端解析内容授权服务器发送的许可证格式； d) 查看DRM客户端播放权限。		
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果显示许可证响应消息格式、内容均正确，符合GY/T 277—2019中8.3的规定； c) DRM客户端解析许可证的密钥使用规则单元keyRulesNum为1，keyRuleType为输出规则，播放权限为按输出规则不允许授权播放，许可证中的授权仅包括且严格遵循业务授权数据，符合GY/T 277—2019中7.2.6的规定； d) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.2.54 对按软件安全级别播放授权的处理功能的测试方法如下:

测试编号	License_093	项目属性	可选
测试对象	DRM客户端		
测试描述	测试许可证中密钥使用规则为按软件安全级别授权播放时在客户端的播放权限功能。		

预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入； c) 内容授权服务器存在且仅存在1条该客户端的业务授权数据，授权规则为按软件安全级别授权。
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送许可证响应； c) DRM客户端解析内容授权服务器发送的许可证格式； d) 查看DRM客户端播放权限。
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果显示许可证响应消息格式、内容均正确，符合GY/T 277—2019中8.3的规定； c) DRM客户端解析许可证的密钥使用规则单元keyRulesNum为1，keyRuleType为安全级别，播放权限为按软件安全级别授权播放，许可证中的授权仅包括且严格遵循业务授权数据，符合GY/T 277—2019中7.2.6的规定； d) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。

A.2.2.55 对按硬件安全级别播放授权的处理功能的测试方法如下：

测试编号	License_094	项目属性	可选
测试对象	DRM客户端		
测试描述	测试许可证中密钥使用规则为按硬件安全级别授权播放时在客户端的播放权限功能。		
预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入； c) 内容授权服务器存在且仅存在1条该客户端的业务授权数据，授权规则为按硬件安全级别授权。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送许可证响应； c) DRM客户端解析内容授权服务器发送的许可证格式； d) 查看DRM客户端播放权限。		
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果显示许可证响应消息格式、内容均正确，符合GY/T 277—2019中8.3的规定； c) DRM客户端解析许可证的密钥使用规则单元keyRulesNum为1，keyRuleType为安全级别，播放权限为按硬件安全级别授权播放，许可证中的授权仅包括且严格遵循业务授权数据，符合GY/T 277—2019中7.2.6的规定； d) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.2.2.56 对按增强硬件安全级别播放授权的处理功能的测试方法如下：

测试编号	License_095	项目属性	可选
测试对象	DRM客户端		
测试描述	测试许可证中密钥使用规则为按增强硬件安全级别授权播放时在客户端的播放权限功能。		
预置条件	设备： a) DRM客户端； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 内容授权服务器已经完成合法数字证书的置入； b) DRM客户端已完成合法数字证书的置入； c) 内容授权服务器存在且仅存在1条该客户端的业务授权数据，授权规则为按增强硬件安全级别授权。		
测试步骤	a) DRM客户端发起2-pass许可证获取请求消息，消息格式和内容均正确； b) 内容授权服务器向DRM客户端发送许可证响应； c) DRM客户端解析内容授权服务器发送的许可证格式； d) 查看DRM客户端播放权限。		
符合性判定	a) DRM客户端发送向内容授权服务器发送的许可证请求消息格式、内容均符合GY/T 277—2019中8.2的规定； b) DRM客户端解析结果显示许可证响应消息格式、内容均正确，符合GY/T 277—2019中8.3的规定； c) DRM客户端解析许可证的密钥使用规则单元keyRulesNum为1，keyRuleType为安全级别，播放权限为按增强硬件安全级别授权播放，许可证中的授权仅包括且严格遵循业务授权数据，符合GY/T 277—2019中7.2.6的规定； d) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.3 密钥同步与密钥查询协议测试

A.3.1 密钥网关服务器测试

A.3.1.1 对正确密钥同步请求的处理功能的测试方法如下：

测试编号	Key_001	项目属性	必选
测试对象	密钥网关服务器		
测试描述	测试密钥网关服务器对正确密钥同步请求的处理。		
预置条件	设备： a) 密钥管理服务器（测试平台）； b) 密钥网关服务器； c) OCSP服务器。 状态： a) 密钥管理服务器已完成合法数字证书的置入； b) 密钥网关服务器已完成合法数字证书的置入。		
测试步骤	a) 密钥管理服务器发起消息格式和内容均正确的密钥同步请求； b) 密钥网关服务器验证同步请求，并返回同步响应消息； c) 密钥管理服务器验证并正确解析密钥网关服务器返回的响应消息。		

符合性判定	a) 密钥网关服务器存储内容加密密钥并向密钥管理服务器发送的密钥同步响应消息状态为“success”（同步成功），消息格式符合GY/T 277—2019中9.2.3的规定； b) 签名算法符合GY/T 277—2019中附录B的规定。

A.3.1.2 对不支持请求的算法的密钥同步请求的处理功能的测试方法如下：

测试编号	Key_002	项目属性	必选
测试对象	密钥网关服务器		
测试描述	测试密钥网关服务器对“不支持请求算法的密钥同步请求”的处理。		
预置条件	设备： a) 密钥管理服务器（测试平台）； b) 密钥网关服务器； c) OCSP服务器。 状态： a) 密钥管理服务器已完成合法数字证书的置入； b) 密钥网关服务器已完成合法数字证书的置入。		
测试步骤	a) 密钥管理服务器发起消息格式正确，“selectedAlgorithm”字段不为“KMSProfile1”的密钥同步请求； b) 密钥网关服务器验证同步请求，并返回同步响应消息； c) 密钥管理服务器验证并正确解析密钥网关服务器返回的响应消息。		
符合性判定	a) 密钥网关服务器向密钥管理服务器返回的密钥同步响应消息状态为“doNotSupportSelectedAlgorithm”（不支持请求的算法）且消息格式符合GY/T 277—2019中9.2.3的规定； b) 签名算法符合GY/T 277—2019中附录B的规定。		

A.3.1.3 对密钥管理系统证书不合法的密钥同步请求的处理功能的测试方法如下：

测试编号	Key_003	项目属性	必选
测试对象	密钥网关服务器		
测试描述	测试密钥网关服务器对“密钥管理证书链错误的密钥同步请求”的处理。		
预置条件	设备： a) 密钥管理服务器（测试平台）； b) 密钥网关服务器； c) OCSP服务器。 状态： a) 密钥管理服务器已完成合法数字证书的置入； b) 密钥网关服务器已完成合法数字证书的置入。		
测试步骤	a) 密钥管理服务器发起消息格式正确，“certificateChain”字段不为内容提供者密钥管理系统证书链的密钥同步请求； b) 密钥网关服务器验证同步请求，并返回同步响应消息； c) 密钥管理服务器验证并正确解析密钥网关服务器返回的响应消息。		
符合性判定	a) 密钥网关服务器向密钥管理服务器返回的密钥同步响应消息状态为“certificationInvalid”（密钥管理证书不合法）且消息格式符合GY/T 277—2019中9.2.3的规定； b) 签名算法符合GY/T 277—2019中附录B的规定。		

A.3.1.4 对消息数字签名不正确的密钥同步请求的处理功能的测试方法如下：

测试编号	Key_004	项目属性	必选
测试对象	密钥网关服务器		
测试描述	测试密钥网关服务器对“消息数字签名不正确的密钥同步请求”的处理。		
预置条件	设备： a) 密钥管理服务器（测试平台）； b) 密钥网关服务器； c) OCSP服务器。 状态： a) 密钥管理服务器已完成合法数字证书的置入； b) 密钥网关服务器已完成合法数字证书的置入。		
测试步骤	a) 密钥管理服务器发起消息格式正确，“signature”字段内容错误的密钥同步请求； b) 密钥网关服务器验同步请求，证并返回同步响应消息； c) 密钥管理服务器验证并正确解析密钥网关服务器返回的响应消息。		
符合性判定	a) 密钥网关服务器向密钥管理服务器返回的密钥同步响应消息状态为“signatureInvalid”（密钥同步请求消息数字签名不正确）且消息格式符合GY/T 277—2019中9.2.3的规定； b) 签名算法符合GY/T 277—2019中附录B的规定。		

A.3.1.5 对未知错误的密钥同步请求的处理功能的测试方法如下：

测试编号	Key_005	项目属性	必选
测试对象	密钥网关服务器		
测试描述	测试密钥网关服务器对“未知错误的密钥同步请求”的处理。		
预置条件	设备： a) 密钥管理服务器（测试平台）； b) 密钥网关服务器； c) OCSP服务器。 状态： a) 密钥管理服务器已完成合法数字证书的置入； b) 密钥网关服务器已完成合法数字证书的置入。		
测试步骤	a) 密钥管理服务器发起消息格式正确，“type”或“version”或“kmsID”或“nonce”或“contentInfos”或“contentID”或“ceks”或“cekID”或“encCEK”或“contentRules”或“startTime”或“endTime”等字段，一个或多个，错误或缺失的密钥同步请求； b) 密钥网关服务器验证同步请求，并返回同步响应消息； c) 密钥管理服务器验证并正确解析密钥网关服务器返回的响应消息。		
符合性判定	a) 密钥网关服务器向密钥管理服务器返回的密钥同步响应消息状态为“unknownError”（未知错误）且消息格式符合GY/T 277—2019中9.2.3的规定； b) 签名算法符合GY/T 277—2019中附录B的规定。		

A.3.1.6 对正确密钥查询请求的处理功能的测试方法如下：

测试编号	Key_006	项目属性	必选
测试对象	密钥网关服务器		

测试描述	测试密钥网关服务器对正确密钥查询请求的处理。
预置条件	设备： a) 密钥网关服务器； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 密钥管理服务器已完成合法数字证书的置入； b) 密钥网关服务器已完成合法数字证书的置入。
测试步骤	a) 内容授权服务器发起消息格式和内容均正确的密钥查询请求； b) 密钥网关服务器验证查询请求，并返回查询响应消息； c) 内容授权服务器验证并正确解析密钥网关服务器返回的响应消息。
符合性判定	a) 密钥网关服务器向内容授权服务器返回的密钥查询响应消息状态为“success”（查询成功），消息格式符合GY/T 277—2019中9.3.3的规定； b) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。

A.3.1.7 对不支持请求的算法的密钥查询请求的处理功能的测试方法如下：

测试编号	Key_007	项目属性	必选
测试对象	密钥网关服务器		
测试描述	测试密钥网关服务器对“不支持请求的算法的查询请求”的响应。		
预置条件	设备： a) 密钥网关服务器； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 密钥管理服务器已完成合法数字证书的置入； b) 密钥网关服务器已完成合法数字证书的置入。		
测试步骤	a) 内容授权服务器发起消息格式正确，“selectedAlgorithm”字段不为“KMSProfile1”的密钥查询请求； b) 密钥网关服务器验证查询请求，并返回查询响应消息； c) 内容授权服务器验证并正确解析密钥网关服务器返回的响应消息。		
符合性判定	a) 密钥网关服务器向内容授权服务器返回的密钥查询响应消息状态为“doNotSupportSelectedAlgorithm”（不支持请求的算法）且消息格式符合GY/T 277—2019中9.3.3的规定； b) 签名算法符合GY/T 277—2019中附录B的规定。		

A.3.1.8 对找不到该内容ID的密钥查询请求的处理功能的测试方法如下：

测试编号	Key_008	项目属性	必选
测试对象	密钥网关服务器		
测试描述	测试密钥网关服务器对“找不到该内容ID的密钥查询请求”的处理。		

预置条件	设备： a) 密钥网关服务器； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 密钥管理服务器已完成合法数字证书的置入； b) 密钥网关服务器已完成合法数字证书的置入。
测试步骤	a) 内容授权服务器发起消息格式正确，“contentIDs”字段不为内容真实ID的密钥查询请求； b) 密钥网关服务器验证查询请求，并返回查询响应消息； c) 内容授权服务器验证并正确解析密钥网关服务器返回的响应消息。
符合性判定	a) 密钥网关服务器向内容授权服务器返回的密钥查询响应消息状态为“contentIDInvalid”（找不到该内容ID）且消息格式符合GY/T 277—2019中9.3.3的规定； b) 签名算法符合GY/T 277—2019中附录B的规定。

A.3.1.9 对DRM客户端证书不合法的密钥查询请求的处理功能的测试方法如下：

测试编号	Key_009	项目属性	必选
测试对象	密钥网关服务器		
测试描述	测试密钥网关服务器对“DRM客户端证书不合法的密钥查询请求”的处理。		
预置条件	设备： a) 密钥网关服务器； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 密钥管理服务器已完成合法数字证书的置入； b) 密钥网关服务器已完成合法数字证书的置入。		
测试步骤	a) 内容授权服务器发起消息格式正确，“drmClientCertificate”字段为客户端错误证书的密钥查询请求； b) 密钥网关服务器验证查询请求，并返回查询响应消息； c) 内容授权服务器验证并正确解析密钥网关服务器返回的响应消息。		
符合性判定	a) 密钥网关服务器向内容授权服务器返回的密钥查询响应消息状态为“deviceCertInvalid”（DRM客户端证书不合法）且消息格式符合GY/T 277—2019中9.3.3的规定； b) 签名算法符合GY/T 277—2019中附录B的规定。		

A.3.1.10 对内容许可授权系统证书不合法的密钥查询请求的处理功能的测试方法如下：

测试编号	Key_010	项目属性	必选
测试对象	密钥网关服务器		
测试描述	测试密钥网关服务器对“内容许可授权系统证书不合法的密钥查询请求”的处理。		
预置条件	设备： a) 密钥网关服务器； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 密钥管理服务器已完成合法数字证书的置入； b) 密钥网关服务器已完成合法数字证书的置入。		

测试步骤	a) 内容授权服务器发起消息格式正确，“certificateChain”字段为错误的内容授权证书链的密钥查询请求； b) 密钥网关服务器验证查询请求，并返回查询响应消息； c) 内容授权服务器验证并正确解析密钥网关服务器返回的响应消息。
符合性判定	a) 密钥网关服务器向内容授权服务器返回的密钥查询响应消息状态为“drmServerCertInvalid”（内容许可授权系统证书不合法）且消息格式符合GY/T 277—2019中9.3.3的规定； b) 签名算法符合GY/T 277—2019附录B的规定。

A.3.1.11 对内容许可授权系统不在白名单的密钥查询请求的处理功能的测试方法如下：

测试编号	Key_011	项目属性	必选
测试对象	密钥网关服务器		
测试描述	测试密钥网关服务器对“内容许可授权系统不在白名单的密钥查询请求”的处理。		
预置条件	设备： a) 密钥网关服务器； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 密钥管理服务器已完成合法数字证书的置入； b) 密钥网关服务器已完成合法数字证书的置入。		
测试步骤	a) 内容授权服务器发起消息格式正确，“certificateChain”字段为不在白名单的证书链的密钥查询请求； b) 密钥网关服务器验证查询请求，并返回查询响应消息； c) 内容授权服务器验证并正确解析密钥网关服务器返回的响应消息。		
符合性判定	a) 密钥网关服务器向内容授权服务器返回的密钥查询响应消息状态为“drmServerIDInvalid”（内容许可授权系统不在白名单）且消息格式符合GY/T 277—2019中9.3.3的规定； b) 签名算法符合GY/T 277—2019中附录B的规定。		

A.3.1.12 对消息数字签名不正确的密钥查询请求的处理功能的测试方法如下：

测试编号	Key_012	项目属性	必选
测试对象	密钥网关服务器		
测试描述	测试密钥网关服务器对“消息数字签名不正确的密钥查询请求”的处理。		
预置条件	设备： a) 密钥网关服务器； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 密钥管理服务器已完成合法数字证书的置入； b) 密钥网关服务器已完成合法数字证书的置入。		
测试步骤	a) 内容授权服务器发起消息格式正确，“signature”字段为错误签名的密钥查询请求； b) 密钥网关服务器验证查询请求，并返回查询响应消息； c) 内容授权服务器验证并正确解析密钥网关服务器返回的响应消息。		

符合性判定	a) 密钥网关服务器向内容授权服务器返回的密钥查询响应消息状态为“signatureInvalid”（密钥查询请求消息数字签名不正确）且消息格式符合GY/T 277—2019中9.3.3的规定； b) 签名算法符合GY/T 277—2019中附录B的规定。

A.3.1.13 对未知错误的密钥查询请求的处理功能的测试方法如下：

测试编号	Key_013	项目属性	必选
测试对象	密钥网关服务器		
测试描述	测试密钥网关服务器对“未知错误的密钥查询请求”的处理。		
预置条件	设备： a) 密钥网关服务器； b) 内容授权服务器（测试平台）； c) OCSP服务器。 状态： a) 密钥管理服务器已完成合法数字证书的置入； b) 密钥网关服务器已完成合法数字证书的置入。		
测试步骤	a) 内容授权服务器发起消息格式正确，“type”或“version”或“drmServerID”或“nonce”等字段，错误或者缺失的密钥查询请求； b) 密钥网关服务器验证查询请求，并返回查询响应消息； c) 内容授权服务器验证并正确解析密钥网关服务器返回的响应消息。		
符合性判定	a) 密钥网关服务器向内容授权服务器返回的密钥查询响应消息状态为“unknownError”（未知错误）且消息格式符合GY/T 277—2019中9.3.3的规定； b) 签名算法符合GY/T 277—2019中附录B的规定。		

A.3.2 密钥管理服务器测试

A.3.2.1 对正确密钥同步响应的处理功能的测试方法如下：

测试编号	Key_014	项目属性	必选
测试对象	密钥管理服务器		
测试描述	测试密钥管理服务器的密钥同步请求正确性以及对密钥网关服务器返回响应的处理功能。		
预置条件	设备： a) 密钥管理服务器； b) 密钥网关服务器（测试平台）； c) OCSP服务器。 状态： a) 密钥管理服务器已完成合法数字证书的置入； b) 密钥网关服务器已完成合法数字证书的置入。		
测试步骤	a) 密钥管理服务器发起消息格式和内容均正确的密钥同步请求； b) 密钥网关服务器验证同步请求，并响应状态为“success”（同步成功）的响应消息； c) 密钥管理服务器验证并正确解析密钥网关服务器返回的响应消息。		
符合性判定	a) 密钥管理服务器向密钥网关服务器发送的密钥同步请求消息格式和内容均正确，符合GY/T 277—2019中9.2.2的规定； b) 密钥管理服务器解析出的密钥同步响应消息状态为“success”（同步成功）且消息格式符合GY/T 277—2019中9.2.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.3.2.2 对不支持请求的算法同步请求的密钥同步响应的处理功能的测试方法如下：

测试编号	Key_014	项目属性	必选
测试对象	密钥管理服务器		
测试描述	测试密钥管理服务器的密钥同步请求正确性以及对密钥网关服务器返回响应的处理功能。		
预置条件	设备： a) 密钥管理服务器； b) 密钥网关服务器（测试平台）； c) OCSP服务器。 状态： a) 密钥管理服务器已完成合法数字证书的置入； b) 密钥网关服务器已完成合法数字证书的置入。		
测试步骤	a) 密钥管理服务器发起消息格式和内容均正确的密钥同步请求； b) 密钥网关服务器验证同步请求，并响应状态为“success”（同步成功）的响应消息； c) 密钥管理服务器验证并正确解析密钥网关服务器返回的响应消息。		
符合性判定	a) 密钥管理服务器向密钥网关服务器发送的密钥同步请求消息格式和内容均正确，符合GY/T 277—2019中9.2.2的规定； b) 密钥管理服务器解析出的密钥同步响应消息状态为“success”（同步成功）且消息格式符合GY/T 277—2019中9.2.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.3.2.3 对密钥管理系统证书不合法的密钥同步响应的处理功能的测试方法如下：

测试编号	Key_016	项目属性	必选
测试对象	密钥管理服务器		
测试描述	测试密钥管理服务器对“密钥管理证书不合法的密钥同步响应”的处理。		
预置条件	设备： a) 密钥管理服务器； b) 密钥网关服务器（测试平台）； c) OCSP服务器。 状态： a) 密钥管理服务器已完成合法数字证书的置入； b) 密钥网关服务器已完成合法数字证书的置入。		
测试步骤	a) 密钥管理服务器发起消息格式、内容均正确的密钥同步请求； b) 密钥网关服务器验证同步请求，并返回状态为“certificationInvalid”（内容提供者密钥管理系统证书不合法）的响应消息； c) 密钥管理服务器验证并正确解析密钥网关服务器返回的响应消息。		
符合性判定	a) 密钥管理服务器向密钥网关服务器发送的密钥同步请求消息格式和内容均正确，符合GY/T 277—2019中9.2.2的规定； b) 密钥管理服务器解析出的密钥同步响应消息状态为“certificationInvalid”（内容提供者密钥管理系统证书不合法）且消息格式符合GY/T 277—2019中9.2.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.3.2.4 对消息数字签名不正确的密钥同步响应的处理功能的测试方法如下：

测试编号	Key_017	项目属性	必选
测试对象	密钥管理服务器		
测试描述	测试密钥管理服务器对“消息数字签名不正确的密钥同步响应”的处理。		
预置条件	设备： a) 密钥管理服务器； b) 密钥网关服务器（测试平台）； c) OCSP服务器。 状态： a) 密钥管理服务器已完成合法数字证书的置入； b) 密钥网关服务器已完成合法数字证书的置入。		
测试步骤	a) 密钥管理服务器发起消息格式、内容均正确的密钥同步请求； b) 密钥网关服务器验证同步请求，并返回状态为“signatureInvalid”（密钥同步请求消息数字签名不正确）的响应消息； c) 密钥管理服务器验证并正确解析密钥网关服务器返回的响应消息。		
符合性判定	a) 密钥管理服务器向密钥网关服务器发送的密钥同步请求消息格式和内容均正确，符合GY/T 277—2019中9.2.2的规定； b) 密钥管理服务器解析出的密钥同步响应消息状态为“signatureInvalid”（密钥同步请求消息数字签名不正确）且消息格式符合GY/T 277—2019中9.2.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.3.2.5 对未知错误的密钥同步响应的处理功能的测试方法如下：

测试编号	Key_018	项目属性	必选
测试对象	密钥管理服务器		
测试描述	测试密钥管理服务器对“未知错误的密钥同步响应”的处理。		
预置条件	设备： a) 密钥管理服务器； b) 密钥网关服务器（测试平台）； c) OCSP服务器。 状态： a) 密钥管理服务器已完成合法数字证书的置入； b) 密钥网关服务器已完成合法数字证书的置入。		
测试步骤	a) 密钥管理服务器发起消息格式、内容均正确的密钥同步请求； b) 密钥网关服务器验证同步请求，并返回状态为“unknownError”（未知错误）的响应消息； c) 密钥管理服务器验证并正确解析密钥网关服务器返回的响应消息。		
符合性判定	a) 密钥管理服务器向密钥网关服务器发送的密钥同步请求消息格式和内容均正确，符合GY/T 277—2019中9.2.2的规定； b) 密钥管理服务器解析出的密钥同步响应消息状态为“unknownError”（未知错误）且消息格式符合GY/T 277—2019中9.2.3的规定； c) 签名算法和密钥加密算法均符合GY/T 277—2019中附录B的规定。		

A.3.3 内容授权服务器测试

A.3.3.1 对正确密钥查询响应的处理功能的测试方法如下：

测试编号	Key_019	项目属性	必选
测试对象	内容授权服务器		
测试描述	测试内容授权服务器密钥发送的密钥查询请求消息的正确性以及对密钥网关服务器返回的响应的处理。		
预置条件	设备： a) 密钥网关服务器（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 密钥网关服务器已完成合法数字证书的置入； b) 内容授权服务器已完成合法数字证书的置入。		
测试步骤	a) 内容授权服务器发起消息格式和内容均正确的密钥查询请求； b) 密钥网关服务器验证查询请求，并响应状态为“success”（查询成功）的响应消息； c) 内容授权服务器验证并正确解析密钥网关服务器返回的响应消息。		
符合性判定	a) 内容授权服务器向密钥网关服务器发送的密钥查询请求消息格式和内容均正确，符合GY/T 277—2019中9.3.2的规定； b) 内容授权服务器解析出的密钥查询响应消息状态为“success”（查询成功）且消息格式符合GY/T 277—2019中9.3.3的规定； c) 签名算法符合GY/T 277—2019中附录B的规定。		

A.3.3.2 对不支持请求的算法的密钥查询响应的处理功能的测试方法如下：

测试编号	Key_020	项目属性	必选
测试对象	内容授权服务器		
测试描述	测试内容授权服务器对“不支持请求算法的密钥查询响应”的处理。		
预置条件	设备： a) 密钥网关服务器（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 密钥管理服务器已完成合法数字证书的置入； b) 密钥网关服务器已完成合法数字证书的置入。		
测试步骤	a) 内容授权服务器发起消息格式和内容均正确的密钥查询请求； b) 密钥网关服务器验证查询请求，并响应状态为“doNotSupportSelectedAlgorithm”（不支持请求的算法）的响应消息； c) 内容授权服务器验证并正确解析密钥网关服务器返回的响应。		
符合性判定	a) 内容授权服务器向密钥网关服务器发送的密钥查询请求消息格式和内容均正确，符合GY/T 277—2019中9.3.2的规定； b) 内容授权服务器解析出的密钥查询响应消息消息状态为“doNotSupportSelectedAlgorithm”（不支持请求的算法）且消息格式符合GY/T 277—2019中9.3.3的规定； c) 签名算法符合GY/T 277—2019中附录B的规定。		

A.3.3.3 对找不到该内容ID的密钥查询响应的处理功能的测试方法如下：

测试编号	Key_021	项目属性	必选
测试对象	内容授权服务器		
测试描述	测试内容授权服务器对“找不到该内容ID的密钥查询响应”的处理。		
预置条件	设备： a) 密钥网关服务器（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 密钥管理服务器已完成合法数字证书的置入； b) 密钥网关服务器已完成合法数字证书的置入。		
测试步骤	a) 内容授权服务器发起消息格式和内容均正确的密钥查询请求； b) 密钥网关服务器验证查询请求，并响应状态为“contentIDInvalid”（找不到该内容ID）的响应消息； c) 内容授权服务器验证并解析的密钥查询响应消息。		
符合性判定	a) 内容授权服务器向密钥网关服务器发送的密钥查询请求消息格式和内容均正确，符合GY/T 277—2019中9.3.2的规定； b) 内容授权服务器解析出的密钥查询响应消息状态为“contentIDInvalid”（找不到该内容ID）且消息格式符合GY/T 277—2019中9.3.3的规定； c) 签名算法符合GY/T 277—2019中附录B的规定。		

A.3.3.4 对DRM客户端证书不合法的密钥查询响应的处理功能的测试方法如下：

测试编号	Key_022	项目属性	必选
测试对象	内容授权服务器		
测试描述	测试内容授权服务器对“DRM客户端证书不合法的密钥查询响应”的处理。		
预置条件	设备： a) 密钥网关服务器（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 密钥管理服务器已完成合法数字证书的置入； b) 密钥网关服务器已完成合法数字证书的置入。		
测试步骤	a) 内容授权服务器发起消息格式和内容均正确的密钥查询请求； b) 密钥网关服务器验证查询请求，并响应状态为“deviceCertInvalid”（DRM客户端证书不合法）的响应消息； c) 内容授权服务器验证并正确解析密钥网关服务器返回的响应消息。		
符合性判定	a) 内容授权服务器向密钥网关服务器发送的密钥查询请求消息格式和内容均正确，符合GY/T 277—2019中9.3.2的规定； b) 内容授权服务器解析出的密钥查询响应消息状态为“deviceCertInvalid”（DRM客户端证书不合法）且消息格式符合GY/T 277—2019中9.3.3的规定； c) 签名算法符合GY/T 277—2019中附录B的规定。		

A.3.3.5 对内容许可授权系统证书不合法的密钥查询响应的处理功能的测试方法如下：

测试编号	Key_022	项目属性	必选
测试对象	内容授权服务器		
测试描述	测试内容授权服务器对“DRM客户端证书不合法的密钥查询响应”的处理。		
预置条件	设备： a) 密钥网关服务器（测试平台）； b) 内容授权服务器； c) OCSP服务器； 状态： a) 密钥管理服务器已完成合法数字证书的置入； b) 密钥网关服务器已完成合法数字证书的置入。		
测试步骤	a) 内容授权服务器发起消息格式和内容均正确的密钥查询请求； b) 密钥网关服务器验证查询请求，并响应状态为“deviceCertInvalid”（DRM客户端证书不合法）的响应消息； c) 内容授权服务器验证并正确解析密钥网关服务器返回的响应消息。		
符合性判定	a) 内容授权服务器向密钥网关服务器发送的密钥查询请求消息格式和内容均正确，符合GY/T 277—2019中9.3.2的规定； b) 内容授权服务器解析出的密钥查询响应消息状态为“deviceCertInvalid”（DRM客户端证书不合法）且消息格式符合GY/T 277—2019中9.3.3的规定； c) 签名算法符合GY/T 277—2019中附录B的规定。		

A.3.3.6 对内容许可授权系统不在白名单的密钥查询响应的处理功能的测试方法如下：

测试编号	Key_024	项目属性	必选
测试对象	内容授权服务器		
测试描述	测试内容授权服务器对“内容许可授权系统不在白名单的密钥查询响应”的处理。		
预置条件	设备： a) 密钥网关服务器（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 密钥管理服务器已完成合法数字证书的置入； b) 密钥网关服务器已完成合法数字证书的置入。		
测试步骤	a) 内容授权服务器发起消息格式和内容均正确的密钥查询请求； b) 密钥网关服务器验证查询请求，并响应状态为“drmServerIDInvalid”（内容许可授权系统不在白名单）的响应消息； c) 内容授权服务器验证并正确解析密钥网关服务器返回的响应消息。		
符合性判定	a) 内容授权服务器向密钥网关服务器发送的密钥查询请求消息格式和内容均正确，符合GY/T 277—2019中9.3.2的规定； b) 内容授权服务器解析出的密钥查询响应消息响应状态为“drmServerIDInvalid”（内容许可授权系统不在白名单）且消息格式符合GY/T 277—2019中9.3.3的规定； c) 签名算法符合GY/T 277—2019中附录B的规定。		

A.3.3.7 对消息数字签名不正确的密钥查询响应的处理功能的测试方法如下：

测试编号	Key_025	项目属性	必选
测试对象	内容授权服务器		
测试描述	测试内容授权服务器对“消息数字签名不正确的密钥查询响应”的处理。		
预置条件	设备： a) 密钥网关服务器（测试平台）； b) 内容授权服务器； c) OCSP服务器； 状态： a) 密钥管理服务器已完成合法数字证书的置入； b) 密钥网关服务器已完成合法数字证书的置入。		
测试步骤	a) 内容授权服务器发起消息格式和内容均正确的密钥查询请求； b) 密钥网关服务器验证查询请求，并响应状态为“signatureInvalid”（密钥查询请求消息数字签名不正确）的响应消息； c) 内容授权服务器验证并正确解析密钥网关服务器返回的响应消息。		
符合性判定	a) 内容授权服务器向密钥网关服务器发送的密钥查询请求消息格式和内容均正确，符合GY/T 277—2019中9.3.2的规定； b) 内容授权服务器解析出的密钥查询响应消息响应状态为“signatureInvalid”（密钥查询请求消息数字签名不正确）且消息格式符合GY/T 277—2019中9.3.3的规定； c) 签名算法符合GY/T 277—2019中附录B的规定。		

A.3.3.8 对未知错误的密钥查询响应的处理功能的测试方法如下：

测试编号	Key_026	项目属性	必选
测试对象	内容授权服务器		
测试描述	测试内容授权服务器对“未知错误的密钥查询响应”的处理。		
预置条件	设备： a) 密钥网关服务器（测试平台）； b) 内容授权服务器； c) OCSP服务器。 状态： a) 密钥管理服务器已完成合法数字证书的置入； b) 密钥网关服务器已完成合法数字证书的置入。		
测试步骤	a) 内容授权服务器发起消息格式和内容均正确的密钥查询请求； b) 密钥网关服务器验证查询请求，并响应状态为“unknownError”（未知错误）的响应消息； c) 内容授权服务器验证并正确解析密钥网关服务器返回的响应消息。		
符合性判定	a) 内容授权服务器向密钥网关服务器发送的密钥查询请求消息格式和内容均正确，符合GY/T 277—2019中9.3.2的规定； b) 内容授权服务器解析出的密钥查询响应消息响应状态为“unknownError”（未知错误）且消息格式符合GY/T 277—2019中9.3.3的规定； c) 签名算法符合GY/T 277—2019中附录B的规定。		

附 录 B
（规范性）
系统运行标准符合性测试方法

B.1 内容加密方法和封装格式测试

B.1.1 直播场景测试

B.1.1.1 对基于AVS+编码SM4-CBC加密的视音频内容测试的测试方法如下：

测试编号	Content_101	项目属性	必选
测试对象	AVS+编码、SM4-CBC加密的视音频内容		
测试描述	对承载了AVS+编码SM4-CBC加密的视频序列的TS文件进行测试。		
测试步骤	a) 使用测试平台实时抓取DRM客户端和内容加密服务器之间传输的AVS+编码、SM4-CBC加密的视音频流； b) 解析该视音频流，提取出ChinaDRM描述子和CEI等字段，其中包括视频序列的加密方法（SM4-CBC）和编码方法（AVS+）以及内容解密密钥ID等信息，同时提取出被加密视音频数据部分。		
符合性判定	通过解析结果显示，TS流中加密方法符合GY/T 277—2019中6.2.1和6.2.2的规定，封装格式符合GY/T 277—2019中6.3.1的规定。		

B.1.1.2 对基于AVS+编码SM4-SAMPLE加密的视音频内容测试的测试方法如下：

测试编号	Content_102	项目属性	必选
测试对象	AVS+编码、SM4-SAMPLE加密的视音频内容		
测试描述	对承载了AVS+编码SM4-SAMPLE加密的视频序列的TS文件进行测试。		
测试步骤	a) 使用测试平台实时抓取DRM客户端和内容加密服务器之间传输的AVS+编码、SM4-SAMPLE加密的视音频流； b) 解析该视音频流，提取出ChinaDRM描述子和CEI等字段，其中包括视频序列的加密方法（SM4-SAMPLE）和编码方法（AVS+）以及内容解密密钥ID等信息，同时提取出被加密视音频数据部分。		
符合性判定	通过解析结果显示，视音频流中加密方法符合GY/T 277—2019中6.2.1和6.2.2的规定，封装格式符合GY/T 277—2019中6.3.1的规定。		

B.1.1.3 对基于AVS2编码SM4-CBC加密的视音频内容测试的测试方法如下：

测试编号	Content_103	项目属性	必选
测试对象	AVS2编码、SM4-CBC加密的视音频内容		
测试描述	对承载了AVS/AVS2编码SM4-CBC加密的视频序列的TS文件进行测试。		
测试步骤	a) 使用测试平台实时抓取DRM客户端和内容加密服务器之间传输的AVS2编码、SM4-CBC加密的视音频流； b) 解析该视音频流，提取出ChinaDRM描述子和CEI等字段，其中包括视频序列的加密方法（SM4-CBC）和编码方法（AVS2）以及内容解密密钥ID等信息，同时提取出被加密视音频数据部分。		
符合性判定	通过解析结果显示，TS流中加密方法符合GY/T 277—2019中6.2.1和6.2.2的规定，封装格式符合GY/T 277—2019中6.3.1的规定。		

B.1.1.4 对基于AVS2编码SM4-SAMPLE加密的视音频内容测试的测试方法如下：

测试编号	Content_104	项目属性	必选
测试对象	AVS2编码、SM4-SAMPLE加密的视音频内容		
测试描述	对承载了AVS2编码SM4-SAMPLE加密的视频序列的TS文件进行测试。		
测试步骤	a) 使用测试平台实时抓取DRM客户端和内容加密服务器之间传输的AVS2编码、SM4-SAMPLE加密的视音频流； b) 解析该视音频流，提取出ChinaDRM描述子和CEI等字段，其中包括视频序列的加密方法（SM4-SAMPLE）和编码方法（AVS2）以及内容解密密钥ID等信息，同时提取出被加密视音频数据部分。		
符合性判定	通过解析结果显示，视音频流中加密方法符合GY/T 277—2019中6.2.1和6.2.2的规定，封装格式符合GY/T 277—2019中6.3.1的规定。		

B.1.1.5 对基于H.264编码SM4-CBC加密的视音频内容测试的测试方法如下：

测试编号	Content_105	项目属性	必选
测试对象	H.264编码、SM4-CBC加密的视音频内容		
测试描述	对承载了H.264编码SM4-CBC加密的视频序列的TS文件进行测试。		
测试步骤	a) 使用测试平台实时抓取DRM客户端和内容加密服务器之间传输的H.264编码、SM4-CBC加密的视音频流； b) 解析该视音频流，提取出ChinaDRM描述子和CEI等字段，其中包括视频序列的加密方法（SM4-CBC）和编码方法（H.264）以及内容解密密钥ID等信息，同时提取出被加密视音频数据部分。		
符合性判定	通过解析结果显示，TS流中加密方法符合GY/T 277—2019中6.2.1和6.2.3的规定，封装格式符合GY/T 277—2019中6.3.1的规定。		

B.1.1.6 对基于H.264编码SM4-SAMPLE加密的视音频内容测试的测试方法如下：

测试编号	Content_106	项目属性	必选
测试对象	H.264编码、SM4-SAMPLE加密的视音频内容		
测试描述	对承载了H.264编码SM4-SAMPLE加密的视频序列的TS文件进行测试。		
测试步骤	a) 使用测试平台实时抓取DRM客户端和内容加密服务器之间传输的H.264编码、SM4-SAMPLE加密的视音频流； b) 解析该视音频流，提取出ChinaDRM描述子和CEI等字段，其中包括视频序列的加密方法（SM4-SAMPLE）和编码方法（H.264）以及内容解密密钥ID等信息，同时提取出被加密视音频数据部分。		
符合性判定	通过解析结果显示，TS流中加密方法符合GY/T 277—2019中6.2.1和6.2.3的规定，封装格式符合GY/T 277—2019中6.3.1的规定。		

B.1.1.7 对基于H.265编码SM4-CBC加密的视音频内容测试的测试方法如下：

测试编号	Content_107	项目属性	必选
测试对象	H.265编码、SM4-CBC加密的视音频内容		
测试描述	对承载了H.265编码SM4-CBC加密的视频序列的TS文件进行测试。		

测试步骤	a) 使用测试平台实时抓取DRM客户端和内容加密服务器之间传输的H.265编码、SM4-CBC加密的视音频流； b) 解析该视音频流，提取出ChinaDRM描述子和CEI等字段，其中包括视频序列的加密方法（SM4-CBC）和编码方法（H.265）以及内容解密密钥ID等信息，同时提取出被加密视音频数据部分。
符合性判定	通过解析结果显示，TS流中加密方法符合GY/T 277—2019中6.2.1和6.2.4的规定，封装格式符合GY/T 277—2019中6.3.1的规定。

B.1.1.8 对基于H.265编码SM4-SAMPLE加密的视音频内容测试的测试方法如下：

测试编号	Content_108	项目属性	必选
测试对象	H.265编码、SM4-SAMPLE加密的视音频内容		
测试描述	对承载了H.265编码SM4-SAMPLE加密的视频序列的TS文件进行测试。		
测试步骤	a) 使用测试平台实时抓取DRM客户端和内容加密服务器之间传输的H.265编码、SM4-SAMPLE加密的视音频流； b) 解析该视音频流，提取出ChinaDRM描述子和CEI等字段，其中包括视频序列的加密方法（SM4-SAMPLE）和编码方法（H.265）以及内容解密密钥ID等信息，同时提取出被加密视音频数据部分。		
符合性判定	通过解析结果显示，TS流中加密方法符合GY/T 277—2019中6.2.1和6.2.4的规定，封装格式符合GY/T 277—2019中6.3.1的规定。		

B.1.2 点播场景测试

B.1.2.1 对基于DASH传输的H.264编码SM4-CBC加密MP4视音频内容测试的测试方法如下：

测试编号	Content_109	项目属性	必选
测试对象	基于DASH传输的H.264编码、SM4-CBC加密的MP4内容		
测试描述	对DASH传输的H.264编码SM4-CBC加密的MP4文件进行测试。		
测试步骤	a) 使用测试平台实时抓取DRM客户端和内容加密服务器之间传输的MPD文件； b) 解析该MPD文件，提取出实际视音频内容所在URL位置,同时解析ContentProtection中的版权信息； c) 根据URL通过网络接收MP4； d) 解析该MP4，从ProtectionSystemSpecificHeaderBox和保护模式信息盒中提取出该MP4的加密算法（SM4-CBC），并提取出加密的视音频内容。		
符合性判定	通过解析结果显示，MP4中加密方法符合GY/T 277—2019中6.2.3和6.3.3的规定，封装格式符合GY/T 277—2019中6.3.2的规定。		

B.1.2.2 对基于DASH传输的H.264编码SM4-SAMPLE加密MP4视音频内容测试的测试方法如下：

测试编号	Content_110	项目属性	必选
测试对象	基于DASH传输的H.264编码、SM4-SAMPLE加密的MP4内容		
测试描述	对DASH传输的H.264编码SM4-SAMPLE加密的MP4文件进行测试。		
测试步骤	a) 使用测试平台实时抓取DRM客户端和内容加密服务器之间传输的MPD文件； b) 解析该MPD文件，提取出实际视音频内容所在URL位置，同时解析ContentProtection中的版权信息； c) 根据URL通过网络接收MP4； d) 解析该MP4，从ProtectionSystemSpecificHeaderBox和保护模式信息盒中提取出该MP4的加密算法（SM4-SAMPLE），并提取出加密的视音频内容。		

符合性判定	通过解析结果显示，MP4中加密方法符合GY/T 277—2019中6.2.3和6.3.3的规定，封装格式符合GY/T 277—2019中6.3.2的规定。

B.1.2.3 对基于DASH传输的H.265编码SM4-CBC加密MP4视音频内容测试的测试方法如下：

测试编号	Content_111	项目属性	必选
测试对象	基于DASH传输的H.265编码、SM4-CBC加密的MP4内容		
测试描述	对DASH传输的H.265编码SM4-CBC加密的MP4文件进行测试。		
测试步骤	a) 使用测试平台实时抓取DRM客户端和内容加密服务器之间传输的MPD文件； b) 解析该MPD文件，提取出实际视音频内容所在URL位置,同时解析ContentProtection中的版权信息； c) 根据URL通过网络接收MP4； d) 解析该MP4，从ProtectionSystemSpecificHeaderBox和保护模式信息盒中提取出该MP4的加密算法（SM4-CBC），并提取出加密的视音频内容。		
符合性判定	通过解析结果显示，MP4中加密方法符合GY/T 277—2019中6.2.3和6.3.3的规定，封装格式符合GY/T 277—2019中6.3.2的规定。		

B.1.2.4 对基于DASH传输的H.265编码SM4-SAMPLE加密MP4视音频内容测试的测试方法如下：

测试编号	Content_112	项目属性	必选
测试对象	基于DASH传输的H.265编码、SM4-SAMPLE加密的MP4内容		
测试描述	对DASH传输的H.265编码SM4-SAMPLE加密的MP4文件进行测试。		
测试步骤	a) 使用测试平台实时抓取DRM客户端和内容加密服务器之间传输的MPD文件； b) 解析该MPD文件，提取出实际视音频内容所在URL位置,同时解析ContentProtection中的版权信息； c) 根据URL通过网络接收MP4； d) 解析该MP4，从ProtectionSystemSpecificHeaderBox和保护模式信息盒中提取出该MP4的加密算法（SM4-SAMPLE），并提取出加密的视音频内容。		
符合性判定	通过解析结果显示，MP4中加密方法符合GY/T 277—2019中6.2.3和6.3.3的规定，封装格式符合GY/T 277—2019中6.3.2的规定。		

B.1.2.5 对基于HLS传输的H.264编码SM4-CBC加密的TS文件测试的测试方法如下：

测试编号	Content_113	项目属性	必选
测试对象	基于HLS传输的H.264编码、SM4-CBC加密的TS文件		
测试描述	对HLS传输的H.264编码SM4-CBC加密的TS文件进行测试。		
测试步骤	a) 使用测试平台实时抓取DRM客户端和内容加密服务器之间传输的M3U8文件； b) 解析该M3U8文件，提取出所承载的实际视音频内容的加密方法（SM4-CBC），编码方法（H.264）等信息。		
符合性判定	通过解析结果显示，TS流中加密方法符合GY/T 277—2019中6.2.1和6.2.3的规定，封装格式符合GY/T 277—2019中6.3.4的规定。		

B.1.2.6 对基于HLS传输的H.264编码SM4-SAMPLE加密的TS文件测试的测试方法如下：

测试编号	Content_114	项目属性	必选
测试对象	基于HLS传输的H.264编码、SM4-SAMPLE加密的TS文件		

测试描述	对HLS传输的H.264编码SM4-SAMPLE加密的TS文件进行测试。
测试步骤	a) 使用测试平台实时抓取DRM客户端和内容加密服务器之间传输的M3U8文件； b) 解析该M3U8文件，提取出所承载的实际视音频内容的加密方法（SM4-SAMPLE），编码方法（H.264）。
符合性判定	通过解析结果显示，TS流中加密方法符合GY/T 277—2019中6.2.1和6.2.3的规定，封装格式符合GY/T 277—2019中6.3.4的规定。

B.1.2.7 对基于HLS传输的H.265编码SM4-CBC加密的TS文件测试的测试方法如下：

测试编号	Content_115	项目属性	必选
测试对象	基于HLS传输的H.265编码、SM4-CBC加密的TS文件		
测试描述	对HLS传输的H.265编码SM4-CBC加密的TS文件进行测试。		
测试步骤	a) 使用测试平台实时抓取DRM客户端和内容加密服务器之间传输的M3U8文件； b) 解析该M3U8文件，提取出所承载的实际视音频内容的加密方法（SM4-CBC），编码方法（H.265）。		
符合性判定	通过解析结果显示，TS流中加密方法符合GY/T 277—2019中6.2.1和6.2.3的规定，封装格式符合GY/T 277—2019中6.3.4的规定。		

B.1.2.8 对基于HLS传输的H.265编码SM4-SAMPLE加密的TS文件测试的测试方法如下：

测试编号	Content_116	项目属性	必选
测试对象	基于HLS传输的H.265编码、SM4-SAMPLE加密的TS文件		
测试描述	对HLS传输的H.265编码SM4-SAMPLE加密的TS文件进行测试。		
测试步骤	a) 使用测试平台实时抓取DRM客户端和内容加密服务器之间传输的M3U8文件； b) 解析该M3U8文件，提取出所承载的实际视音频内容的加密方法（SM4-SAMPLE），编码方法（H.265）。		
符合性判定	通过解析结果显示，TS流中加密方法符合GY/T 277—2019中6.2.1和6.2.3的规定，封装格式符合GY/T 277—2019中6.3.4的规定。		

B.2 许可证获取测试

B.2.1 对许可证获取请求测试的测试方法如下：

测试编号	License_101	项目属性	必选
测试对象	DRM客户端		
测试描述	测试DRM客户端发送的许可证获取请求消息的标准符合性。		
测试步骤	a) 测试平台捕获DRM客户端发起的2-pass许可证获取请求消息； b) 解析许可证获取请求消息； c) 验证消息签名。		
符合性判定	a) 许可证获取请求消息格式正确，符合GY/T 277—2019中8.3的规定； b) 签名算法符合GY/T 277—2019中附录B的规定。		

B.2.2 对许可证获取响应测试的测试方法如下：

测试编号	License_102	项目属性	必选
测试对象	内容授权服务器		
测试描述	测试内容授权服务器返回的许可证获取响应消息的标准符合性。		

测试步骤	a) 测试平台捕获内容授权服务器返回的2-pass许可证获取响应消息； b) 解析许可证获取响应消息； c) 验证消息签名。
符合性判定	a) 许可证获取响应消息格式正确，符合GY/T 277—2019中8.4的规定； b) 签名算法符合GY/T 277—2019中附录B的规定。

B.3 密钥同步请求测试

B.3.1 对密钥同步请求测试的测试方法如下：

测试编号	Key_101	项目属性	必选
测试对象	密钥管理服务器		
测试描述	测试密钥管理服务器发起的密钥同步请求消息的标准符合性。		
测试步骤	a) 测试平台捕获密钥管理服务器发起的密钥同步请求消息； b) 解析密钥同步请求消息内容； c) 验证消息签名。		
符合性判定	a) 密钥管理服务器发送的密钥同步请求消息格式正确，符合GY/T 277—2019中9.2.2的规定； b) 签名算法和密钥加密算法符合GY/T 277—2019中附录B的规定。		

B.3.2 对密钥同步响应测试的测试方法如下：

测试编号	Key_102	项目属性	必选
测试对象	密钥网关服务器		
测试描述	测试密钥网关服务器返回的密钥同步响应消息的标准符合性。		
测试步骤	a) 测试平台捕获密钥网关服务器返回的密钥同步响应消息； b) 解析密钥同步响应消息内容； c) 验证消息签名。		
符合性判定	a) 密钥管理服务器发送的密钥同步响应消息格式正确，符合GY/T 277—2019中9.2.3的规定； b) 签名算法符合GY/T 277—2019中附录B的规定。		

B.3.3 对密钥查询请求测试的测试方法如下：

测试编号	Key_103	项目属性	必选
测试对象	内容授权服务器		
测试描述	测试内容授权服务器发起的密钥查询请求消息的标准符合性。		
测试步骤	a) 测试平台捕获内容授权服务器发起的密钥查询请求消息； b) 解析密钥查询请求消息内容； c) 验证消息签名。		
符合性判定	a) 内容授权服务器发送的密钥查询请求消息格式正确，符合GY/T 277—2019中9.3.2的规定； b) 签名算法符合GY/T 277—2019中附录B的规定。		

B.3.4 对密钥查询响应测试的测试方法如下：

测试编号	Key_104	项目属性	必选
测试对象	密钥网关服务器		

测试描述	测试密钥网关服务器返回的密钥查询响应消息的标准符合性。
测试步骤	a) 测试平台捕获密钥网关服务器返回的密钥查询响应消息； b) 解析密钥查询响应消息内容； c) 验证消息签名。
符合性判定	a) 内容授权服务器发送的密钥查询响应消息格式正确，符合GY/T 277—2019中9.3.3的规定； b) 签名算法和密钥加密算法符合GY/T 277—2019中附录B的规定。