

GY

**INDUSTRY STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GY/T 335-2020

**Video and audio content distribution digital rights management
standard compliance test
(English Translation)**

Issued on: November 9, 2020

Implemented on: November 9, 2020

Issued by: State Administration of Radio and Television

Table of Contents

- Foreword
- 1 Scope
- 2 Normative references
- 3 Terms and definitions
- 4 Abbreviations
- 5 Overview
- 6 Standard compliance test content
 - 6.1 Content encryption method
 - 6.2 License format
 - 6.3 License acquisition agreement

Foreword

This document is in accordance with the provisions of GB/T 1.1-2020 "Guidelines for Standardization Work Part 1: Structure and Drafting Rules of Standardization Documents" Drafting.

1 Scope

This document specifies the compliance test content and test methods of GY/T 277-2019.

This document is applicable to the compliance test of GY/T 277-2019.

2 Normative references

The contents of the following documents constitute the indispensable clauses of this document through normative references in the text. Among them, dated reference documents, Only the version corresponding to that date is applicable to this document; for undated references, the latest version (including all amendments) is applicable to this document file.

GY/T 277-2019 Technical Specification for Digital Rights Management of Video and Audio Content Distribution

3 Terms and definitions

The terms and definitions defined in GY/T 277-2019 and the following are applicable to this document.

Content encryption server the entity that encrypts digital media content in the DRM server. The implementation form includes, but is not limited to, dedicated equipment, software services, etc.

Content authorization server the entity that queries the content encryption key from the key gateway in the DRM server and encapsulates it into a license and sends it to the DRM client. The implementation forms include but not limited to special equipment, software services, etc.

Key management server the entity responsible for receiving the content encryption key information of the content encryption server and performing safe storage and distribution in the DRM server, realizes the shape Types include but are not limited to special equipment, software services, etc.

Key gateway server

The DRM server is responsible for receiving the content encryption key synchronized by the key management server, and receiving the key query of the content authorization server Entities, implementation forms include but are not limited to special equipment, software services, etc.

OCSP server

The entity that provides the OCSP response to the DRM server. The implementation form includes, but is not limited to, dedicated equipment, software services, etc.

Testing platform

A platform for standard compliance testing of the digital rights management system for video and audio content distribution.

4 Abbreviations

The following abbreviations apply to this document.

CA Certification Authority CBC Cipher Block Chain CEI Content Encryption Information (Content Encryption Information) ChinaDRM China Digital Rights Management (China Digital Rights Management) DASH uses the HTTP protocol to transmit dynamic adaptive streaming media protocol (Dynamic Adaptive Streaming over HTTP) DRM Digital Rights Management (Digital Rights Management) HTTP Hyper Text Transport Protocol (Hyper Text Transport Protocol) HLS HTTP-based real-time streaming media protocol (Http Live Streaming) ID unique identifier (Identifier) MPD Media Presentation Description MPEG Moving Picture Experts Group (Moving Picture Experts Group) OCSP Online Certificate Status Protocol (Online Certificate Status Protocol) PMT Program Mapping Table TS Transport Stream URI Universal Resource Identifier (Uniform Resource Identifier) URL Uniform Resource Locator (Uniform Resource Locator)

5 Overview

Video and audio content distribution digital rights management system standard compliance testing includes. content encryption method and format packaging testing, content authorization Server test, key management server test, key gateway server test, DRM client test five parts. Number of video and audio content distributed

Figure 1 shows the compliance test framework of the word copyright management system standard.

6.1.1 Overview

The protected digital content in the system should meet the content encryption and packaging requirements specified in Chapter 6 of GY/T 277-2019, and the encrypted content stream or the media description file should contain the content identification and the information for obtaining the license. The extended data of the basic stream of the encrypted content should contain internal the content encryption information CEI is used to indicate how the subsequent video is encrypted. The CEI should include the encryption identifier and the current content encryption key identifier Symbol, the next content encryption key identifier, and the initial vector corresponding to the current content encryption key. Specific CEI grammar requirements should meet the grammatical format of Table 1 in GY/T 277-2019.CEI_DATA, the encrypted coded data needs to be converted to prevent ambiguity conflict of the start code.

The conversion rules must meet the requirements of 6.2.5 in GY/T 277-2019.

6.1.2 TS packaging method

When the MPEG-TS encapsulation format is used for transmission, the DRM descriptor structure should be set in the PMT table. The descriptor should specify the encrypted content format, Encryption method, license acquisition URI and other information. The specific DRM descriptor grammar format should comply with the provisions of Table 3 in GY/T 277-2019, where the value range of the video encoding format field of the encrypted content shall comply with the provisions of Table 4 in GY/T 277-2019; the encryption method of the video content shall comply with Comply with the provisions of Table 5 in GY/T 277-2019.

For AVS/AVS2 encoded content, the content encryption method should meet the requirements of 6.2.1 and 6.2.2 in GY/T 277-2019, and the content is encapsulated the format should meet the requirements of 6.3.1 in GY/T 277-2019.

For H.264 encoded content, the content encryption method should meet the requirements of 6.2.1 and 6.2.3 in GY/T 277-2019, and the content encapsulation format the formula should meet the requirements of 6.3.1 in GY/T 277-2019.

For H.265 encoded content, the content encryption method should meet the requirements of 6.2.1 and 6.2.4 in GY/T 277-2019, and content encapsulation the format should meet the requirements of 6.3.1 in GY/T 277-2019.

6.1.3 MPEG-DASH

For content distributed using the DASH protocol, the content packaging format should meet the requirements of 6.3.2 in GY/T 277-2019, and the content encryption format the formula should meet the requirements of 6.3.3 in GY/T 277-2019.

For H.264 encoded content, the encryption method should meet the requirements of 6.2.1 and 6.2.3 in GY/T 277-2019; for H.265 encoded content, the encryption method should meet the requirements of 6.2.1 and 6.2.4 of GY/T 277-2019.

6.1.4 HLS

For content distributed using the HLS protocol, the content packaging format should meet the requirements of 6.3.4 in GY/T 277-2019.

For H.264 encoded content, the encryption method should meet the requirements of 6.2.1 and 6.2.3 in GY/T 277-2019; for H.265 encoded content, the encryption method should meet the requirements of 6.2.1 and 6.2.4 of GY/T 277-2019.

6.2 License format

The license format shall comply with the provisions of 7.1 of GY/T 277-2019.

The license code shall comply with the provisions of 7.2 of GY/T 277-2019.

6.3.1 License acquisition request

The format of the license acquisition request message sent by the DRM client to the content authorization server shall comply with the provisions of 8.2 in GY/T 277-2019.

When the DRM client sends an illegal request, the content authorization server should have an abnormal fault tolerance mechanism, and the possible status information should comply with GY/T the provisions of 277-2019 in 8.4.

6.3.2 License acquisition response

The format of the license acquisition response message sent by the content authorization server to the DRM client shall comply with the provisions of 8.3 of GY/T 277-2019.

When the content authorization server sends an illegal response, the DRM client should have an abnormal fault tolerance mechanism, and the possible status information should comply with GY/T the provisions of 277-2019 in 8.4.