

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

GY/T 246-2020

Replacing GY/T 246-2011

**Video and audio content distribution digital rights management
IPTV digital rights management system integration
(English Translation)**

Issued on: November 9, 2020

Implemented on: November 9, 2020

Issued by: State Administration of Radio and Television

Table of Contents

1 Scope	1
2 Normative references	1
3 Abbreviations	1
4 Integrated Framework	1
5 Encryption and Authorization of Live Content	2
5.1 Encryption method of live content	2
5.2 Live content authorization mechanism	3
6 On-demand content encryption and authorization	3
6.1 Encryption method of on-demand content	3
6.2 Authorization mechanism for on-demand content	3
7 DRM Client Integration	4
7.1 DRM Client Integration Mechanism	4
7.2 IPTV smart terminal playback process	4

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.

This document replaces GY/T 246-2011 "Digital Rights Management System and IPTV Integrated Broadcast Control Platform Interface Technical Specification", and it is in line with GY/T 246-Compared with 2011, the main technical changes are as follows.

- Modified the scope and clarified that it is applicable to the integrated deployment and implementation of the IPTV digital rights management system (see Chapter 1, Chapter 1 of the 2011 edition) chapter);
- Revised the normative references (see Chapter 2, Chapter 2 of the 2011 edition);
- Deleted terms and definitions (Chapter 3 of the 2011 edition);
- Deleted system functions and architecture (Chapter 5 of the 2011 edition);
- Added an integrated framework (see Chapter 4);
- Deleted the A-type interface (Chapter 6 of the 2011 edition);
- Added live content encryption and authorization (see Chapter 5);

- Deleted the B-type interface (Chapter 7 of the 2011 edition);
- Added on-demand content encryption and authorization (see Chapter 6);
- Deleted the C interface (Chapter 8 of the 2011 edition);
- Added DRM client integration (see Chapter 7).

1 Scope

This document specifies the IPTV digital rights management system integration framework, live content encryption and authorization, on-demand content encryption and authorization, and DRM Client integration.

This document is applicable to the integrated deployment and implementation of the IPTV digital rights management system.

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
GY/T 333-2020 Video and audio content distribution digital rights management cable digital TV digital rights management system integration
ISO/IEC 23000-19:2018 Information Technology Multimedia Application Format (MPEG-A) Part 19: Common Media for Fragmented Media CMAF (Information technology-Multimedia application format (MPEG-A)-Part

19 Common media application format (CMAF) for segmented media)

3 Abbreviations

The following abbreviations apply to this document.

CBC Cipher Block Chain
CEI Content Encryption Information (Content Encryption Information)
ChinaDRM China Digital Rights Management (China Digital Rights Management)
CRL Certificate Revocation List (Certification Revocation List)
DRM Digital Rights Management (Digital Rights Management)
EPG Electronic Program Guide (Electronic Program Guide)
HLS HTTP-based real-time streaming media protocol (Http Live Streaming)
MPD Media Presentation Description
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)

4 Integration framework the IPTV DRM system includes the IPTV integrated broadcast control total platform DRM system and the IPTV integrated broadcast control sub-platform DRM system. IPTV integrated broadcast control total level the DRM system of the station should include. live content encryption, on-demand content encryption, key management and other subsystems; IPTV integrated broadcast control sub-platform DRM system should Including. live content encryption, on-demand content encryption, key management, key gateway, content authorization and other subsystems.

The IPTV DRM system integration framework is shown in Figure 1.

5 Encryption and authorization of live content

5.1 Encryption method of live content Encryption of live content should be based on the method in 6.2 of GY/T 277-2019 to encrypt the basic stream of live content.

The content encryption information CEI is added to the exhibition data, and the ChinaDRM descriptor is added to the PMT table of the transport stream. CEI grammar see GY/T 277-2019

Table 1 in the ChinaDRM descriptor, see Table 3 in GY/T 277-2019, DRM_data_bytes in the ChinaDRM descriptor should include live broadcast

Channel ID.

5.2 Live content authorization mechanism Live broadcast encryption should be configured with live broadcast channel identification, live broadcast encryption mode, live broadcast key update frequency, key management URL and other configuration information, press According to the configured encryption mode and key update frequency, the live content encryption key is requested from the key management to encrypt the live content.

For the key management interface to apply for a live encryption key, see 7.1.2 in GY/T 333-2020.

The key management should send the current encryption key and the next encryption key to the live encryption every time, and synchronize the live encryption key to the key gateway.

For the interface of synchronizing the live encryption key to the key gateway, see 9.2 in GY/T 277-2019.

When the current content encryption key expires, the live broadcast encryption should switch to the next content encryption key, and apply for a new content encryption from the key management Key.

IPTV intelligent terminal equipment applies for live content authorization license from the content authorization subsystem through the IPTV integrated broadcast control

sub-platform authentication and authorization system Provable, the content authorization subsystem queries the content encryption key from the key gateway subsystem after receiving the live content authorization license application, and encapsulates it into the content authorization license is sent to the IPTV intelligent terminal device through the authentication and authentication system. Between the key gateway subsystem and the content authorization subsystem for the key query interface, see 9.3 in GY/T 277-2019. For the license acquisition interface between the content authorization subsystem and the authentication and authentication system, see Chapter 8 in GY/T 277-2019.

The IPTV smart terminal device decrypts and plays the live content according to the content authorization license, and finds the CEI information in the live broadcast during the live broadcast when a key update occurs, check whether the corresponding content encryption key is stored locally. If no corresponding key is found locally, start a new one Licensing application for live broadcast content.

6 On-demand content encryption and authorization

6.1 On-demand content encryption method when IPTV on-demand uses DASH to distribute content, please refer to 6.3.2 of GY/T 277-2019 for MPD file regulations, and content encryption should follow GY/T the provisions of 6.3.3 in 277-2019.

When IPTV on-demand uses ISO/IEC 23000-19 to distribute content, encryption should follow the provisions of 6.3.3 in GY/T 277-2019, and for the provisions of the cited documents, see 6.3.2 and 6.3.4 in GY/T 277-2019.

When IPTV on-demand uses HLS to distribute content, the content encryption package adopts TS file format, supporting H.264, H.265, AVS, AVS2, etc.

Video encoding. The content encryption can adopt full encryption mode or partial encryption mode. The content encryption algorithm should adopt SM4 algorithm, and the encryption mode should adopt SM4 algorithm.

Use CBC mode. The elementary stream of the encrypted content contains CEI data, and the CEI data contains the unique identifier of the content encryption key and the initial vector.

M3U8 file contains

The content encryption system assigns encryption tasks to realize content encryption. For the interface between content management and on-demand content encryption subsystem, see GY/T 333-6.3 in 2020.

On-demand content encryption After receiving the content encryption task, apply for on-demand content encryption from the key management...