

GY

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

GY/T 333-2020

**Video and audio content distribution digital rights management
Cable digital TV 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

Foreword	
1 Scope	
2 Normative references	
3 Abbreviations	
4 Integrated Framework	
5 Authorization mechanism	
5.1 Live broadcast authorization mechanism	
5.2 On-demand authorization mechanism	
6 Content encryption	
6.1 Content encryption method	
6.2 Content usage rules	
6.3 On-demand encryption interface	
7 Key Management	
7.1 Live key management	
7.2 On-demand key management	
8 Content authorization	
8.1 Overview	
8.2 Live Channel Authorization	
8.3 On-demand content authorization	
9 Terminal Integration	
9.1 Terminal integration method	
9.2 How to insert DRM client certificate	
9.3 DRM client upgrade and transformation	
Appendix A (normative) DRM client certificate insertion interface API	
A.1 DRM client certificate offline burning interface	
A.2 DRM client operating environment interface extension	

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 core of DRM system integration framework, content encryption, key management, content authorization, and terminal integration for cable digital TV.

Mechanism and interface protocol.

This document is applicable to the integrated deployment and implementation of the DRM system of digital cable television.

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 quotations Only the version corresponding to the date is applicable to this document; for undated reference documents, the latest version (including all amendments) is applicable in this document.

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

API Application Programming Interface (Application Programming Interface) 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) FTP File Transfer Protocol HLS HTTP-based real-time streaming media protocol (Http Live Streaming) HTTP Hyper Text Transport Protocol (Hyper Text Transport Protocol) ID unique identifier (Identifier) JSON JS Object Notation (JavaScript Object Notation) MPD Media Presentation Description NFS Network File System (Network File System) OTP One Time Programmable PGP Pretty Good Privacy PMT Program Mapping Table REE Rich Execution Environment (Rich Execution Environment) TA Trusted Application TEE Trusted Execution Environment (Trusted Execution Environment) TS Transport Stream URI Universal Resource Identifier (Uniform Resource Identifier) URL Uniform Resource Locator (Uniform Resource Locator) uimsbf unsigned integer, most significant bit first

4 Integration framework

The digital cable TV DRM system is used to protect the copyright of the IP two-way cable digital TV live and on-demand content, and to ensure that the digital TV content passes the two-way IP cable network is distributed to the terminal for the safety of the whole process of playing and outputting. The cable digital TV DRM system should comply with GY/T 277-2019 Relevant regulations include DRM server system and DRM client. The DRM server system should include live broadcast encryption, on-demand encryption, and live broadcast key management.

Management, on-demand key management, key gateway, content authorization and other core subsystems, through live encryption, on-demand encryption, content authorization and wired data the collaboration of the digital TV operating system realizes the server-side integration of the cable digital TV DRM system, and the encrypted live content of the live broadcast is passed through the live content Distributed and sent to smart terminals such as set-top boxes. The encrypted content on demand is sent to smart terminals such as set-top boxes through on-demand content distribution.

The DRM client function is integrated in smart terminals such as set-top boxes to realize end-to-end protection of IP two-way cable digital TV live broadcast and on-demand content copyright.

The integrated framework of the DRM system of digital cable television is shown in Figure 1.

5.1 Live broadcast authorization mechanism

Live broadcast encryption performs live broadcast content encryption according to the configured encryption mode and key update frequency. The live content encryption key comes from the key management Rationale.

The key management should generate the current content encryption key and the next content encryption key for live broadcast encryption, and send them to the live broadcast encryption at the same time.

Step to the key gateway.

Live encryption updates the key according to the configured key update frequency. When the content encryption key expires, it switches to the next content encryption Key, and apply for a new content encryption key from the key management; each time the key management sends the current encryption key and the next encryption key to the direct Broadcast encryption, and synchronize the live encryption key to the key gateway.

The terminal device applies for the live content authorization license according to the live channel identification, and the content authorization queries from the authentication and

authentication after receiving the application.

The device's playback authority is based on the live broadcast channel ID to query the live encryption key from the key gateway. If the terminal device has playback authority, the the current content encryption key and the next content encryption key of the channel are encapsulated in the live content authorization license and sent to the terminal.

The terminal equipment decrypts and plays the live content according to the content authorization license, and finds that the key is generated in the CEI information during the live broadcast when updating, you should check whether the corresponding content encryption key is stored locally. If the corresponding key is not found locally, start the new live content Authorization application.

5.2 On-demand authorization mechanism on-demand content management and maintenance of on-demand content encryption mode, encrypted content unique identifier, encrypted content URL and other information, by encrypting the content the system issues an encryption task to achieve content encryption.

After the content is encrypted, it is distributed through the on-demand content distribution system.

The content encryption keys are synchronized to the key gateway, and the content authorization passes the authentication and authentication after receiving the terminal on-demand content authorization license request.

The right-accounting system queries the terminal's playback license, queries the content encryption key from the key gateway, and encapsulates it into a content authorization license and sends it to the terminal.

The DRM client of the terminal device decrypts and plays the content according to the key usage rule through the content authorization license.

6.1.1 Live broadcast encryption method

Live broadcast encryption includes local encryption and third-party encryption. In the case of third-party encryption, the key management of the third-party organization will the channel content encryption key is synchronized to the key gateway of the operating agency.

Live broadcast encryption applies for the live content encryption key from the key management to encrypt the live channel content. In actual deployment, live broadcast encryption can be used it is deployed as an independent device, and can also be deployed as a functional module in a live encoding/transcoding device.

6.1.2 On-demand encryption method when using TS to distribute content on-demand, the content encryption shall encrypt the basic stream according to the method in 6.2 of GY/T 277-2019.