

GY

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

GY/T 334-2020

**Video and audio content distribution digital rights management
Internet 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 Terms and definitions	
4 Abbreviations	
5 Integration framework	
6 Content encryption	
7 Key Management	
8 Content authorization	
8.1 Content authorization mechanism	
8.2 Content review mechanism	
9 Client Integration	
9.1 Internet TV terminal playback process	

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 integration framework, system functions and interface protocols of the Internet TV digital rights management system.

This document is applicable to the integrated deployment and implementation of the Internet TV 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

3 Terms and definitions

The following terms and definitions apply to this document.

License

Description of control information such as access rights, usage rules, and keys of digital media content.

[Source. GY/T 277-2019, definition 3.2] 3.2 DRM client the trusted entity in the device is responsible for enforcing the permissions and restrictions related to DRM content.

[Source. GY/T 277-2019, definition 3.4] 3.3 Device the entity that consumes content with the DRM client installed.

[Source. GY/T 277-2019, definition 3.3] 3.4 DRM content Digital media content managed by DRM technology.

[Source. GY/T 277-2019, definition 3.6] 3.5 Ciphertext Encrypted information.

[Source. GY/T 277-2019, definition 3.7] 3.6 Encryption in order to generate ciphertext, that is, to hide the information content of the data, the data is (reversibly) transformed by a cryptographic algorithm.

[Source. GY/T 277-2019, definition 3.8] 3.7 Decryption the reverse process corresponding to the encryption process. That is, the ciphertext data is inversely transformed by the cryptographic algorithm.

[Source. GY/T 277-2019, definition 3.9] 3.8 Key Control the sequence of symbols for cryptographic transformation operations (for example, encryption, decryption, cryptographic verification function calculation, signature generation, or signature verification).

[Source. GY/T 277-2019, definition 3.10]

4 Abbreviations

The following abbreviations apply to this document.

CRL certificate revocation list (Certificate Revocation List) DRM Digital Rights Management (Digital Rights Management) EPG Electronic Program Guide (Electronic Program Guide) OCSP Online Certificate Status Protocol (Online Certificate Status Protocol) TEE Trusted Execution Environment (Trusted Execution Environment) URL Uniform Resource Locator (Uniform Resource Locator)

5 Integration framework

The Internet TV digital rights management system includes content encryption, key management, key gateway, content authorization, and DRM client Cardiac Function. The integrated framework of the Internet TV digital rights management system is shown in Figure 1.

6 Content encryption

The content can be injected into the content distribution network after being encrypted by the content encryption system of the Internet TV operating system, or in the content provider's the content encryption system is encrypted and injected into the content distribution network.

The content management system issues content encryption tasks to the content encryption system. After receiving the content encryption tasks, the content encryption system the management system applies for the content encryption key to encrypt the content in accordance with the specified encryption algorithm and encryption mode. After the content encryption is completed, the content is stored Go to the location specified by the content encryption task and notify the key management system to synchronize the key to the key gateway system.

The content management system should maintain content encryption mode, content unique identification, content usage rules, etc., when issuing content encryption tasks, it should Carry content unique identification and necessary content usage rules. After the content is encrypted, before the content is released, the content distribution should be able to it can obtain information such as content encryption mode, content unique identifier, content encoding format, etc., which is used to encapsulate index files such as M3U8.

If the content is encrypted by the content provider, the content provider should synchronize the content's unique identifier, encrypted content address, etc. to the Internet.

Depending on the content management system of the operator, it is convenient for Internet TV operators to review encrypted content.

The content management system should synchronize information such as whether the content is encrypted and the unique identification of the content to the EPG system, and the Internet TV terminal application should be able to this information can be used to determine whether the DRM client instance needs to be initialized during playback authentication, and to request a license acquisition request message from the DRM client.

The content encryption package should comply with the provisions of GY/T 333-2020, 6.1; the interface protocol between content management and content encryption should comply with the provisions of GY/T 333-2020 in 6.3.

7 Key Management

The key management system generates content encryption keys for the content encryption system, and is responsible for synchronizing the content encryption keys to the key gateway.

The interface between content encryption and key management, and the key synchronization interface between key management and key gateway shall comply with GY/T 333-2020 Provisions in 7.2.

8.1 Content authorization mechanism

The content management system is responsible for managing information such as content unique identification, content usage rules, content encryption mode, encrypted content URL, etc.

Assign an encryption task to the content encryption system to implement content encryption. After the content encryption is completed, the content encryption key is synchronized to the Internet TV operation system the key gateway system of the system, the encrypted content is distributed through the content distribution network.

The content authorization system of the Internet TV operating system uniformly provides content authorization licenses for Internet TV terminal applications through the authentication system certificate.

The key query interface between the key gateway system and the content authorization system shall comply with the provisions of 9.3 of GY/T 277-2019. Content authorization the license acquisition interface between the system and the authentication system shall comply with the provisions of Chapter 8 in GY/T 277-2019.

8.2 Content review mechanism

After Internet TV content is encrypted, the encrypted content should be reviewed before the content distribution system injects the content into the content distribution network.

The content review system should apply for the client certificate and private key for content review from the certificate management system, and configure the key gateway system URL and certificate the book chain and other information are obtained from the content management system of the Internet TV operating system to obtain the unique identification and content address of the content to be reviewed, according to GY/T the 9.3 interface in 277-2019 applies for the content encryption key from the key gateway, and uses the content encryption key to decrypt the playback content for review.