

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

GY/T 277-2019

**Technical specification of digital rights management for video
audio content distribution
(English Translation)**

Issued on: January 1, 1970

Implemented on: July 5, 2019

Issued by: State Administration of Radio and Television

Table of Contents

Foreword
1 Scope
2 Normative references
3 Terms and definitions
4 Acronyms
5 Architecture
5.1 Overview
5.2 Logical architecture
5.3 Content authorization
5.4 Key Management
5.5 Security Mechanism
5.6 Trust Model
6 Content encryption
6.1 Overview
6.2 Content encryption method

Foreword

This standard was drafted in accordance with the rules given in GB/T 1.1-2009.

This standard replaces GY/T 277-2014 "Technical Specifications for Internet TV Digital Rights Management". Compared with GY/T 277-2014, the technical changes are as follows.

- Revised scope (see Chapter 1, Chapter 1 of the 2014 edition);
- Revised normative references (see Chapter 2, Chapter 2 of the 2014 edition);
- Revised terms and definitions, changed DRM agent to DRM client (see Chapter 3, Chapter 3 of the 2014 edition);
- Revised the overview (see Chapter 5.1, Chapter 5 of the 2014 edition);
- Revised the logical architecture (see Chapter 5.2, Chapter 5 of the 2014 edition);
- Added content authorization (see 5.3);
- Added key management (see 5.4);
- The security mechanism has been modified (see 5.5, 9.2 in the 2014 version);

- Modified the trust model (see 5.6, 2014 version 9.1);
- Added content encryption method (see 6.2);
- Modified the content packaging format (see Chapter 6.3, Chapter 6 of the 2014 edition);
- Revised license structure (see 7.1, 2014 version 7.1);
- The license code has been modified (see 7.2, 2014 version 7.2);
- Revised license acquisition agreement (see Chapter 8, Chapter 8 of the 2014 edition);
- Added DRM server (see Chapter 9);
- Added DRM client (see Chapter 10);
- Added digital certificate format, online certificate authentication protocol and certificate revocation list format (see Appendix A);
- Modified the cryptographic algorithm (see Appendix B, Appendix A of the 2014 edition);
- Added DRM client functional interface (see Appendix C);
- Added DRM client runtime environment interface (see Appendix D);
- Removed the description of adding support for ChinaDRM in the streaming media based on the HLS protocol (see Appendix B of the 2014 edition).

This standard is under the jurisdiction of the National Radio, Film and Television Standardization Technical Committee (SAC/TC 239).

This standard was drafted. State Administration of Radio and Television, Academy of Radio and Television Science, China Central Radio and Television Station, Shenzhen Hisilicon Co., Ltd., Intel (China) Co., Ltd., Beijing Jiangnan Tianan Technology Co., Ltd., Beijing Digital Taihe Technology Co., Ltd., Beijing Yongxin Shibo Digital TV Technology Co., Ltd., Beijing Digital Video Technology Co., Ltd., Irdeto Technology (Beijing) Co., Ltd., Shanghai Guomao Digital Technology Co., Ltd., Huashu Digital TV Media Group Co., Ltd., Guangdong South New Media Co., Ltd., China Communications Media University, Beijing ATV Information Technology Co., Ltd., BestTV Network TV Technology Development Co., Ltd., Hunan Happy Sunshine Interactive Entertainment Music Media Co., Ltd., Beijing iQiyi Technology Co., Ltd., Alibaba (China) Co., Ltd., Liaoning Radio and Television Station, Shanghai Culture Radio and Television Group Co., Ltd., Beijing Radio and Television Station.

1 Scope

This standard specifies the logical architecture, technical mechanism, content encryption, license format, and license for digital rights management of video and audio content distribution.

Certificate acquisition agreement, and related technical requirements of DRM server and DRM client.

This standard applies to the copyright protection of digital TV, IPTV, Internet TV and other video and audio content distribution processes.

2 Normative references

The following documents are essential for the application of this document. For dated references, only the dated version applies to this document.

For undated references, the latest version (including all amendments) applies to this document.

GB/T 17964-2008 Information security technology block cipher algorithm working mode
 GB/T 20518-2018 Information Security Technology Public Key Infrastructure Digital Certificate Format
 GB/T 32097-2016 Information Security Technology SM4 Block Cipher Algorithm
 GB/T 32905-2016 Information Security Technology SM3 Password Hash Algorithm
 GB/T 32918.2-2016 Information Security Technology SM2 Elliptic Curve Public Key Key Algorithm Part 2. Digital Signature Algorithm
 GB/T 32918.4-2016 Information Security Technology SM2 Elliptic Curve Public Key Key Algorithm Part 4. Public Key Encryption Algorithm
 GB/T 36322-2018 Information Security Technology Cryptographic Equipment Application Interface Specification
 GY/T 257.1-2012 Advanced Audio and Video Coding and Decoding for Radio and Television Part 1. Video
 GY/T 299.1-2016 High-efficiency audio and video coding Part 1. Video
 ISO 14496-12.:2015 Information technology. Audio and video object coding. Part 12. ISO Basic Media File Format (Information technology-Coding of audio-visual objects-Part 12. ISO base media file format)
 ISO 23001-7.:2016 Information Technology MPEG System Technology Part 7. ISO Basic Media File Format File General Encryption (Information technology-MPEG systems technologies-Part 7. Common encryption in ISO base media file format files)
 ISO 23009-4.:2013 Information technology. HTTP-based dynamic adaptive streaming (DASH). Part 4. Segment encryption and authentication (Information technology-Dynamic adaptive streaming over HTTP (DASH)-Part 4. Segment encryption and authentication)
 IETF RFC 2045 Multi-Target Internet Mail Extensions Part 1. Internet Message Body Format (Multipurpose internet mail extensions-Part 1. Format of internet message bodies)
 IETF RFC 2104 HMAC. Keyed-Hashing for Message Authentication
 IETF RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol-OCSP (X.509 Internet Public Key Infrastructure Online Certificate Status Protocol-OCSP)
 IETF RFC 3279 Internet X.509 Public Key Infrastructure Certificates and Certificate Revocation List Algorithms and Identification (Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile)
 IETF RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile)
 ECMA 404 The

JSON data interchange format

3 Terms and definitions

The following terms and definitions apply to this document.

Content provider

A functional entity that owns digital media content and provides digital media content with copyright information.

License

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

Device

An entity that consumes content with a DRM client installed.

DRM client

A trusted entity in the device that enforces permissions and restrictions related to DRM content.

DRM server DRM server an entity that provides license services to DRM clients.

DRM content

Digital media content managed with DRM technology.

Ciphertext

Encrypted information.

Encryption

In order to generate ciphertext, that is, the information content of hidden data, the data is (reversibly) transformed by a cryptographic algorithm.

Decryption

The reverse process corresponding to the encryption process. That is, the ciphertext data is inversely transformed by a cryptographic algorithm.

3.10

Key

A sequence of symbols that controls cryptographic transformation operations such as encryption, decryption, calculation of cryptographic check functions, signature generation, or signature verification.