

GY

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

GY/T 336-2020

**Video and audio content distribution digital rights management
system compliance requirements
(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 DRM server product compliance requirements	
6.1 Functional requirements	
6.2 Standard compliance requirements	
6.3 Safety requirements	

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 function, performance, standard compliance test requirements of the digital rights management system for the distribution of video and audio content, and system integration and safety management evaluation requirements for operation and maintenance.

This document is applicable to the research and development, integration, construction, operation and maintenance of the digital rights management system for the distribution of video and audio content.

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.

GB/T 37092-2018 Information Security Technology Cryptographic Module Security

Requirements 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 27002 Information Technology Security Technology Information Security Control Practice Code (Information technology-Security techniques-Code of practice for information security controls)

3 Terms and definitions

The following terms and definitions apply to this document.

Hardware root of trust the security primitive composed of hardware is responsible for providing a set of credible and critical security functions. It is designed to always operate in the expected manner OK and immutable.

Secure bootloader

The process of establishing an initial state of trust for instructions and data contained in hardware or software before being executed. Usually the hardware and increase the secure boot loading function with strong hardware security level is rooted in the hardware.

Hardware execution environment; HEE the hardware root of trust used to enforce a secure hardware boundary for DRM applications. It can be a hardware root of trust, a secure the combination of a bootloader, a secure operating system, a secure processor, or the secure operating mode of a single processor.

Root detection

When it is found that the device has been damaged, the device/software or software area can be accessed while detecting that the device/software or software area can be accessed.

Other software is hidden.

Software execution environment; SEE A software-based mechanism used to isolate or protect the execution environment of software during execution.

Special tool

Widely used dedicated electronic or software tools, including but not limited to memory managers, debuggers (for example, software-based bus Analyzer, interactive disassembler) or decompiler, integrated development environment, compiler, JTAG probe reader and similar software development products Product.

User accessible bus

Designed and provided for end users, allowing end users to upgrade or access smart cards, PCMCIA, Cardbus, USB or PCI, etc.

Data bus for quasi-slot or other plug-and-play facilities.

Note: The user-accessible bus does not include the storage bus, CPU bus, and similar parts of the device's internal architecture that are not allowed to be accessed by end users.

4 Abbreviations

The following abbreviations apply to this document.

CA Certification Authority CMAF Common Media Application Format (Common Media Application Format) CPU central processing unit DASH uses the HTTP protocol to transmit dynamic adaptive streaming media protocol (Dynamic Adaptive Streaming over HTTP) DRM Digital Rights Management (Digital Rights Management) HLS HTTP-based real-time streaming media protocol (HTTP Live Streaming) HMAC hashed message authentication code (Hashed Message Authentication Code) JTAG Joint Test Action Group (Joint Test Action Group) OCSP Online Certificate Status Protocol (Online Certificate Status Protocol) PC Personal Computer (Personal Computer) PCI defines the standard of the local bus (Peripheral Component Interconnect) PCMCIA Personal Computer Card (Personal Computer Memory Card International Association) TS transport stream USB Universal Serial Bus (Universal Serial Bus)

5 Overview

The compliance requirements of the digital rights management system for the distribution of video and audio content include the compliance requirements for DRM products and the compliance requirements for the implementation of the DRM system.

DRM product compliance requirements are used to guide the R&D and integration of DRM server products and the integration of DRM clients in terminal devices, mainly including functional requirements, standard compliance requirements and safety requirements.

DRM system implementation compliance requirements are used to guide the integrated construction and operation and maintenance of DRM systems, and mainly refer to the security requirements during implementation.

6.1 Functional requirements

The functions of DRM server products should include five types of live content encryption, on-demand content encryption, key management, key gateway, and content authorization.

The specific requirements are as follows.

a) Encryption of live content.

1) Should support one or more of the live content encryption and packaging such as real-time TS, HLS, DASH, CMAF, etc.;

- 2) Should support AVS, AVS2, H.264, H.265 and other video encoding formats;
 - 3) It should support the application of live content encryption key through key management;
 - 4) The live broadcast encryption key should be updated at a configurable frequency;
 - 5) The live broadcast encryption delay should not be higher than 500ms;
 - 6) It should support second-level content encryption key update frequency.
- b) On-demand content encryption.
- 1) Should support one or more of TS files, HLS, DASH, CMAF and other content encryption packages;
 - 2) Should support AVS, AVS2, H.264, H.265 and other video encoding formats;
 - 3) It should support the application of encryption keys for on-demand content through key management.
- c) Key management.
- 1) Support receiving and processing content encryption key applications;
 - 2) Should support secure storage and management of content encryption keys;
 - 3) Should support the synchronization of content encryption keys to the key gateway.
- d) Key gateway.
- 1) Support receiving and processing live/on-demand content encryption key requests for key management;
 - 2) Support for secure storage and management of live/on-demand content encryption keys;
 - 3) It should support receiving and processing content authorization live/on-demand content encryption key requests.
- e) Content authorization.
- 1) It should support receiving and processing DRM client live/on-demand content authorization license requests;
 - 2) It shall support requesting the encryption key for live/on-demand content from the key gateway.

6.2 Standard compliance requirements

The standard compliance requirements of DRM server products include live content encryption, on-demand content encryption, key management, key gateway and content the specific requirements are as follows.

- a) Encryption of live content.