International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.1006

(10/2016)

SERIES J: CABLE NETWORKS AND TRANSMISSION OF TELEVISION, SOUND PROGRAMME AND OTHER MULTIMEDIA SIGNALS

Conditional access and protection – Digital rights management for cable television multiscreen service

Specification of IP-VoD DRM for cable television multiscreen system in multi-DRM environment

Recommendation ITU-T J.1006

International Telecommunication Union

Recommendation ITU-T J.1006

Specification of IP-VoD DRM for cable television multiscreen system in multi-DRM environment

Summary

Recommendation ITU-T J.1006 describes the specification of IP-VoD DRM for cable television multiscreen system in multi-DRM environment which includes an encryption system commonly adopted to multiple DRMs.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T J.1006	2016-10-14	9	11.1002/1000/13055

Keywords

Common encryption, IP-VoD, multi-DRM.

---

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Introduction

IP-based video on demand (VoD) service which is available inside and outside of homes will inevitably increase the data traffic of media streaming and downloading over IP networks. Although video delivery has been done with HTTP streaming methods, there are no compatibilities among the methods. Consequently, ISO/IEC has standardized [ISO/IEC 23009-1] which has a feature that dynamically adapts the transmission rate.

Digital rights management (DRM) technology for content right protection is used in combination with device authentication. ITU-T has issued a Recommendation for architecture and requirements of DRM for cable television multiscreen [ITU-T J.1005]. Several types of DRM methods are currently deployed by industries and industry groups, and each method closely depends on content holder's right protection policy. In addition, because cable television multiscreen system can use multiple DRM methods, the contents delivery under the environment is expected to be simple as much as is possible. For example, content encryption scheme [ISO/IEC 23001-7] is commonly used among DRM methods. Common encryption scheme has advantages to reduce storage requirements and bandwidth requirements within IP networks located between cable platform and content delivery network (CDN) because of the content that is encrypted once for DRMs. The effectiveness of [ISO/IEC 23001-7] is very similar to the one of Simulcrypt (see [b-ETSI TS 103 197]). The structural relationship of cable platform and CDN is referred to in Appendix I.

Recommendation ITU-T J.1006

Specification of IP-VoD DRM for cable television multiscreen system in multi-DRM environment

1 Scope

This Recommendation describes the specification of IP-VoD DRM for cable television multiscreen system in a multi-DRM environment which includes an encryption system commonly adopted to multiple DRMs. In particular, this Recommendation specifies multi-DRM based on common encryption [ISO/IEC 23001-7] which can be categorized as a common communication interface type among the multi-DRM types that are defined in Appendix III of [ITU-T J.1005].

For stream transmission technique [ISO/IEC 23009-1] shall be used and MPEG-2 TS is optionally used. This Recommendation does not include the details of MPEG-2 TS specified by [ITU-T H.262].

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T H.262] Recommendation ITU-T H.262 (2012) | ISO/IEC 13818-2:2013, *Information technology – Generic coding of moving pictures and associated audio information: Video.*

[ITU-T H.264] Recommendation ITU-T H.264 (2016) | ISO/IEC 14496-10:2012, *Advanced video coding for generic audiovisual services.*

[ITU-T H.265] Recommendation ITU-T H.265 (2015) | ISO/IEC 23008-2 (2013), *High efficiency video coding.*

[ITU-T J.1005] Recommendation ITU-T J.1005 (2015), *Architecture and requirements of digital rights management (DRM) for cable television multiscreen.*

[ITU-R BT.2020-2] Recommendation ITU-R BT.2020-2 (2015), *Parameter values for ultra-high definition television systems for production and international programme exchange.*

[ETSI TS 103 285] ETSI TS 103 285 V1.1.1 (2015), *Digital Video Broadcasting (DVB); MPEG-DASH Profile for Transport of ISO BMFF Based DVB Services over IP Based Networks.*

[ISO/IEC 23001-7] ISO/IEC 23001-7: 2012, *Information technology – MPEG systems technologies – Part 7: Common encryption in ISO base media file format files.*

[ISO/IEC 23001-7 Amd.1] ISO/IEC 23001-7: 2012, *Information technology - MPEG systems technologies - Part 7: Common encryption in ISO base media file format files, Amendment 1: AES-CBC-128 and key rotation.*

[ISO/IEC 23009-1] ISO/IEC 23009-1:2012, *Information technology – Dynamic adaptive streaming over HTTP (DASH) – Part 1: Media presentation description and segment formats*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 multi-DRM [ITU-T J.1005]: A system which can select suitable DRM from two or more DRMs based on the special feature of service, the load of a system, a network situation, etc.

3.1.2 IP-VoD [ITU-T J.1005]: A service to deliver video content following a request from a user. IP-VoD supplies each video content on-demand basis.

3.1.3 ultra high definition television (UHD-TV) [ITU-R BT.2020-2]: UHDTV provides viewers with an enhanced visual experience primarily by a wider field of view that covers a considerable part of the human natural visual field with appropriate screen sizes relevant to usage at home and in public places. Signal formats contributing to increasing the compression efficiency are desirable for UHDTV systems since they have a larger number of pixels than HDTV systems.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AES Advanced Encryption Standard

AVC Advanced Video Coding

CBC Cipher Block Chaining

CDN Content Delivery Network

CENC Common Encryption in ISO Base Media File Format

CP Content Protection

CTR Counter

DASH Dynamic Adaptive Streaming over HTTP

DRM Digital Rights Management

ECL Entitlement Control License

EML Entitlement Management License

HD High Definition

HEVC High Efficiency Video Coding

HTTP Hypertext Transfer Protocol

KID Key Identification

MPD Media Presentation Description

MPEG Moving Picture Experts Group

NAL Network Abstraction Layer

PF Platform

SD Standard Definition

SP Service Provider

TS Transport Stream

UHD Ultra High Definition

VoD Video on Demand

W3C World Wide Web Consortium

5 Conventions

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords "is prohibited from" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

The keywords "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider (SP). Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

In the body of this document and its annexes, the words shall, shall not, should, and may sometimes appear, in which case they are to be interpreted, respectively, as is required to, is prohibited from, is recommended, and can optionally. The appearance of such phrases or keywords in an appendix or in material explicitly marked as informative are to be interpreted as having no normative intent.

6 Multi-DRM specifications for IP-VoD multiscreen service

6.1 General

In this Recommendation, the architecture and requirements of DRM is required to refer to [ITU-T J.1005]. Appendix I shows an overview of IP-VoD multi-DRM with an example that user terminals use different DRM.

For content protection the common encryption scheme [ISO/IEC 23001-7] is required to be referred to. Appendix II describes the view of [ISO/IEC 23001-7] and related encryption key management manner.

Content protection specified in clause 8 of [ETSI TS 103 285] on the usage of specific parameters that are defined within media presentation description (MPD) of [ISO/IEC 23009-1] and within [ISO/IEC 23001-7] is required to be referred to together with the differences shown in the remaining clauses of clause 6 of this Recommendation.

Appendix IV describes the protocol stack model for IP-VoD.

6.2 Encryption mode

Media data is required to be encrypted using advanced encryption standard (AES) 128-bit in counter (CTR) mode. AES 128-bit in cipher block chaining (CBC) mode is optionally used.

Encrypted network abstraction layer (NAL) structured video tracks such as [ITU-T H.264] and [ITU-T H.265] is required to use subsample protection. All other types of encrypted tracks are required to use full sample encryption.

For the details of CTR mode operation [ISO/IEC 23001-7] is required to be referred to. For CBC mode operation [ISO/IEC 23001-7] and [ISO/IEC 23001-7 Amd.1] are required to be referred to.

6.3 Encryption of different representations

Encryption specification for different representations shall refer to clause 8.3 of [ETSI TS 103 285]. Ultra high definition (UHD) content is recommended to be treated in addition to high definition (HD) and standard definition (SD) content. In case where UHD content is contained with HD and/or SD content in one presentation and MPD of [ISO/IEC 23009-1], but different license rights are given for each resolution, then they are required to be contained in different Adaptation Sets, each with different ContentProtection descriptors in the Adaptation Set.

6.4 Key rotation

Key rotation is optionally supported to allow entitlement changes during streaming contents. In that case media segments may be used to deliver new media keys changed within a track.

Initialization segments of [ISO/IEC 23009-1] may contain one or more Protection System Specific Header 'pssh' boxes in the Movie 'moov' box which are specified by [ISO/IEC 23001-7]. Media Segments may also include 'pssh' boxes in Movie Fragment 'moof' boxes.

'pssh' boxes carried in the Media Segments deliver information about new keys, licenses or sub-licenses and ensure that random access to each segment remains possible and that the DRM Player receives updated information in advance for continuous playback. DRM may require information from 'pssh' boxes from both Initialization Segment and Media Segment in order to obtain media keys used for key rotation.

MPD and media segment of [ISO/IEC 23009-1] are depicted in Appendix II for reference.

Various possible key rotation methods, such as sending an explicit signalling message to indicate future key identifications (KIDs), using a dynamic adaptive streaming over http (DASH) period as minimum key duration, delivering future keys in pssh, or using key hierarchy scheme with entitlement message license (EML) and entitlement control license (ECL), are introduced in [b-DASH-IF-IOP].

Especially, in case of key hierarchy method, two or more pairs of KID and ECL shall be included in the Data field of 'pssh' box, which is defined in [ISO/IEC 23001-7], as shown in the Figure 1 to prevent client storm or service delay on key change boundaries. The detail work flow of key hierarchy method is defined in Annex A.

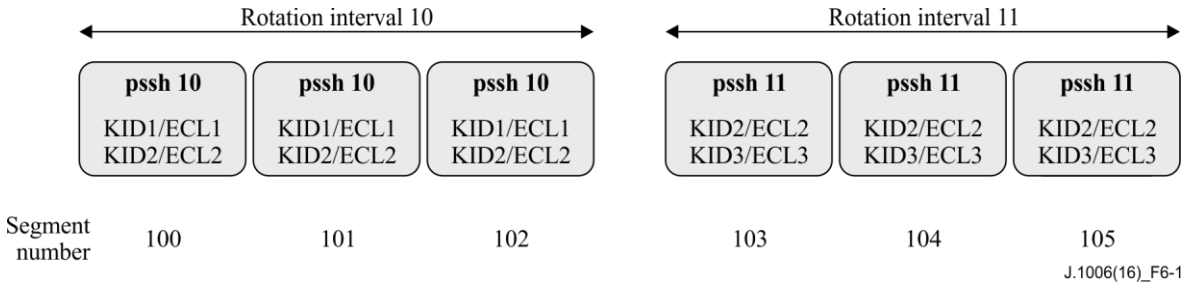

Figure 6-1 – Example of 'pssh' boxes in key rotation aspect

Annex A

Work flow of key hierarchy method for key rotation

(This annex forms an integral part of this Recommendation.)

The work flow of key hierarchy method for key rotation is shown in Figure A.1. In this work flow, 'DRM system X' is an example name for one of the proprietary DRM systems, and the license server and DRM client are dedicated ones to 'DRM system X'.

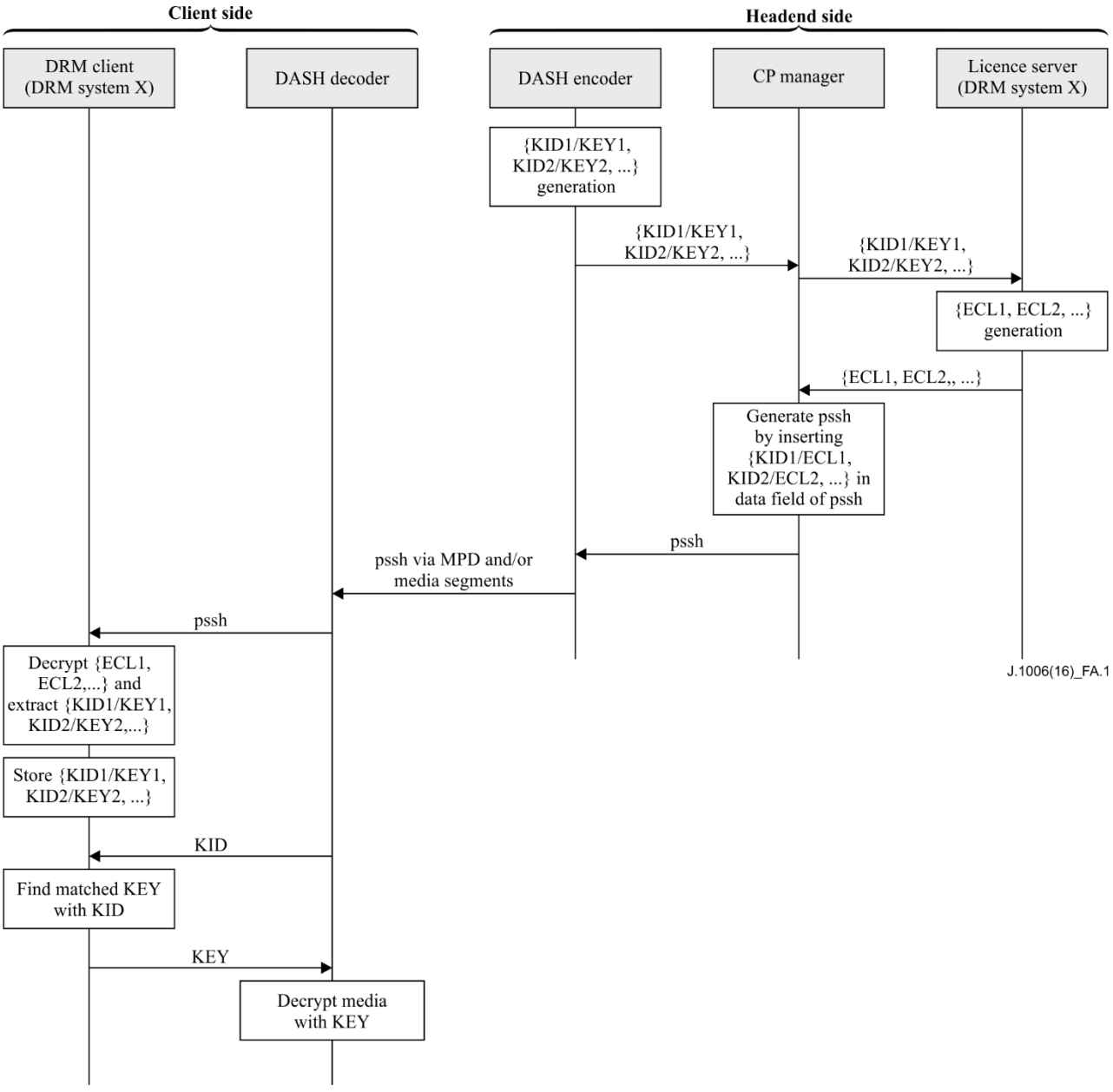

Figure A.1 – work flow of key hierarchy method for key rotation

The detail descriptions for each flow of Figure A.1 are as follows.

(1) DASH encoder generates pairs of KID and media encryption key like {KID1/KEY1, KID2/KEY2, …}. At this time, two or more pairs of KID/KEY shall be included for current and future KID. The generated values are delivered to content protection (CP) manager. Note that the form of pairs of KID/KEY is a proprietary DRM system's matter.

(2) CP manager relays the received KID/KEY values to license server.

(3) License server generates ECLs that includes encrypted KID/KEY values. Then license server returns the list of ECLs to CP manager. Note that the detail specification of ECL is a proprietary DRM system's matter.

(4) CP manager generates 'pssh' box with KID and ECL pairs. The list of KID and ECL pairs shall be inserted in Data field that is defined in [ISO/IEC 23001-7]. Then the generated 'pssh' box is delivered to DASH encoder.

(5) DASH encoder sends 'pssh' box through MPD and/or media segments as specified in [ISO/IEC 23009-1].

(6) DASH decoder parses the received DASH stream and filters 'pssh' box. Then DASH decoder delivers 'pssh' box to DRM client.

(7) DRM client gets the list of KID and KEY pairs from ECLs. Then store the list of KID and KEY pairs, {KID1/KEY1, KID2/KEY2, …}, in secure database area after decrypting them. Note that higher level key in EML is used for decrypting encrypted KEYs in ECL. The detail specification EML is a proprietary DRM system's matter.

(8) DRM client receives KID from DASH decoder, finds the matched KEY with the received KID from stored database then DRM client returns the KEY to DASH decoder.

(9) DASH decoder decrypts DASH media stream with KEY received from DRM client.

Appendix I

Overview of IP-VoD multi-DRM

(This appendix does not form an integral part of this Recommendation.)

Multi-DRM is the system which can choose a suitable DRM following service features, user terminal features and so on.

Figure I.1 depicts multi-DRM related functional components from content provisioning to content distribution to user terminal devices. Although the components in the figure are the same as the ones in Figure 6-1 cable platform and DRM in [ITU-T J.1005], Figure I.1 shows an example of a situation where different DRMs are used with different user terminals.

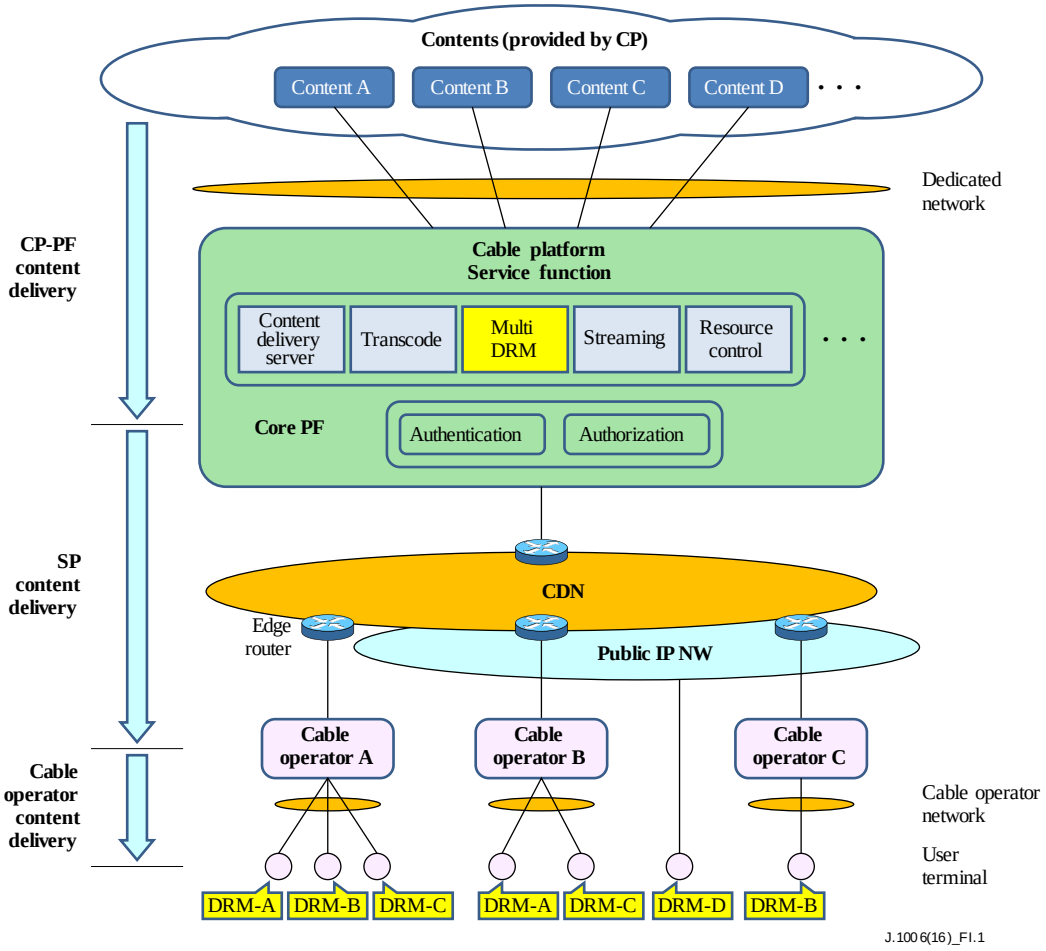

Figure I.1 – Cable Platform and multi-DRM

Appendix II

Common encryption

(This appendix does not form an integral part of this Recommendation.)

Common encryption scheme enables the encryption of content data in a manner which is common to different DRMs using multi-DRM key management system. [ISO/IEC 23001-7] which specifies standard encryption and key mapping method is used as a common encryption scheme for IP-VoD service. [ISO/IEC 23001-7] has the following features.

(1) [CENC] is the technology commonly used for encrypted contents delivery under the environment where different types of DRM exist.

(2) [CENC] has many affinities with IP-VoD specifications which include media source extension by World Wide Web consortium (W3C) and MPEG-DASH.

Figure II.1 shows a conceptual structure of [ISO/IEC 23001-7]. Content data is encrypted by AES 128-bit with a content encryption key. On the other hand DRM specific information such as licenses, rights, and license acquisition information can be stored in an ISO Base Media file using a Protection System Specific Header. Each instance of this box stored in the file corresponds to one applicable DRM system identified by a DRM System ID.

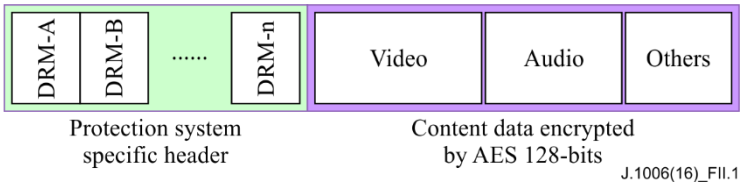

Figure II.1 – Conceptual structure of [ISO/IEC 23001-7]

Media encrypted by means of [ISO/IEC 23001-7] may need DRM specific information to decrypt. [ISO/IEC 23001-7] defines Protection System Specific Header 'pssh' box to carry the information. DRM is identified by SystemID parameter in the 'pssh' box. DRM specific information within the MPD of [ISO/IEC 23009-1] may also be identified in the ContentProtection element.

Initialization segments of [ISO/IEC 23009-1] may contain one or more 'pssh' boxes in the Movie ('moov') box. Media segments may also include 'pssh' boxes in Movie Fragment ('moof') boxes. Figure II.2 and Figure II.3 may be useful for easy understanding of MPD and media segment.

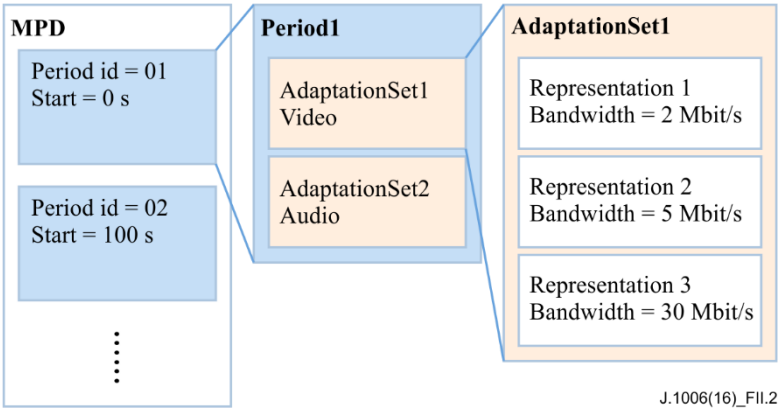

Figure II.2 – Example of MPD model of [ISO/IEC 23009-1]

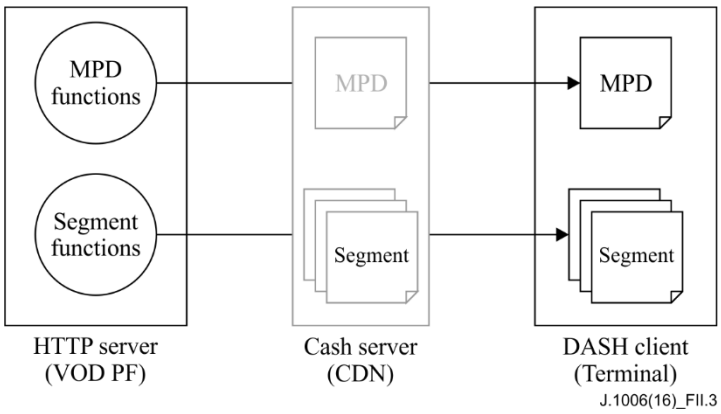

Figure II.3 – Conceptual image of MPD and Media Segment flow of [ISO/IEC 23009-1]

Appendix III

IP-VoD content flow

(This appendix does not form an integral part of this Recommendation.)

Figure III.1 explains the flow of IP-VoD contents protected by DRM. Each box in the figure shows function element of DRM. Contents from a transcoder are encrypted with a contents key stored in a key management server.

The contents key is forwarded to client device by each DRM. For example, when a client device uses DRM-A, the device requests the key management server to deliver the contents key encrypted by DRM-A delivery key. The client device then decrypts the content data with the delivered contents key.

In this way IP-VoD contents encrypted with the same contents key so called common encryption can be used among different DRMs.

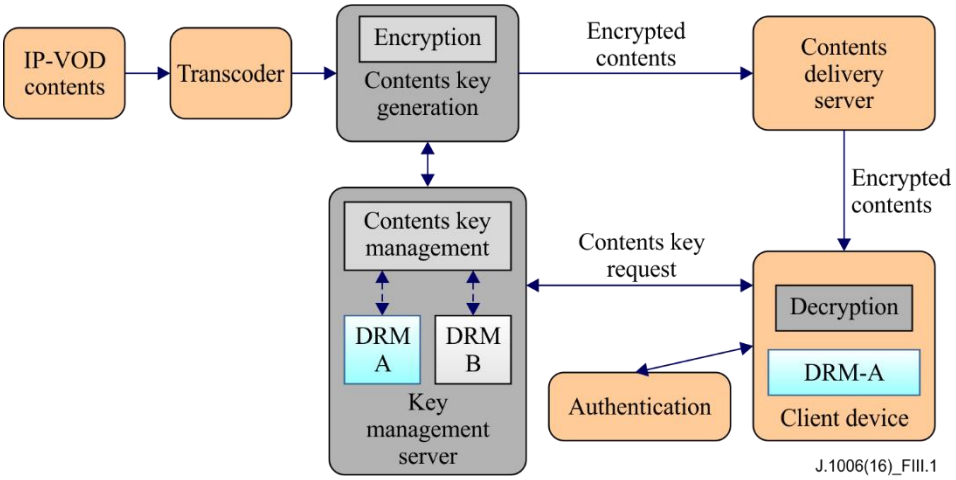

Figure III.1 – IP-VoD contents flow

Appendix IV

Protocol Stack for IP-VoD over cable TV network in multi-DRM

(This appendix does not form an integral part of this Recommendation.)

Figure IV.1 is referred to as a protocol stack model for stream transmission adopted to [ISO/IEC 23009-1] of IP-VoD.

Specifications for the protocols are listed in Table IV.1.

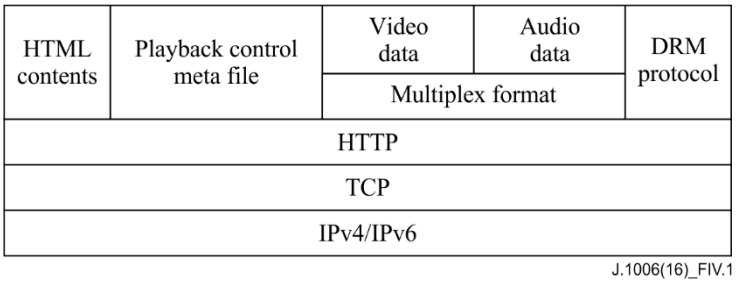

Figure IV.1 – Protocol stack model of IP-VoD

Table IV.1 – Specification list of the protocols

HTTP	RFC 2616: Hypertext Transfer Protocol-HTTP/1.1
TCP	RFC 793: Transmission Control Protocol
IPv6	RFC 2460: Internet Protocol Version 6 (IPv6) Specification
IP	RFC 791: Internet Protocol

Bibliography

[b-ITU-T F.750] Recommendation ITU-T F.750 (2005), *Metadata framework.*

[b-ITU-T H.721] Recommendation ITU-T H.721 (2015), *IPTV terminal devices: Basic model*

[b-ITU-T H.751] Recommendation ITU-T H.751 (2013), *Metadata for rights information interoperability in IPTV services.*

[b-ITU-T J.127] Recommendation ITU-T J.127 (2004), *Transmission protocol for multimedia webcasting over TCP/IP networks.*

[b-ITU-T Y.1910] Recommendation ITU-T Y.1910 (2008), *IPTV functional architecture.*

[b-DASH-IF-IOP] DASH Industry Forum (2015), *Guidelines for Implementation: DASH-IF Interoperability Points.*

[b-ETSI TS 103 197] ETSI TS 103 197 V1.5.1 (2008-10), *Digital Video Broadcasting (DVB); Head-end implementation of DVB SimulCrypt*.

[b-IPTVFJ STD-0002] IPTV forum Japan, *VoD Specifications Version 1.1*.

[b-JLabs SPEC-030] JLabs SPEC-030 (2015), *Operational Specification for Internet Protocol Video on Demand Services.*

[b-PRDASH] Microsoft, *MPEG DASH Content Protection using Microsoft PlayReady*, accessible from http://www.microsoft.com/playready/documents/

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	**Cable networks and transmission of television, sound programme and other multimedia signals**
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2017