International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.1005

(08/2015)

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

Architecture and requirements of digital rights management (DRM) for cable television multiscreen

Recommendation ITU-T J.1005

International Telecommunication Union

Recommendation ITU-T J.1005

Architecture and requirements of digital rights management (DRM) for cable television multiscreen

Summary

Recommendation ITU-T J.1005 specifies the architecture and requirements for a digital rights management (DRM) system for a cable television content delivery service including multiple device viewing experiences. It is anticipated that the architecture and requirements identified in this Recommendation can be applied to the DRM service that covers protected IP-type content (IP VoD, IP linear TV, etc.) delivery from a content provider or cable operator to end terminal devices (PC, tablet, smartphones, etc.) via a cable television network.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T J.1005	2015-08-13	9	11.1002/1000/12570

* 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 not 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/.

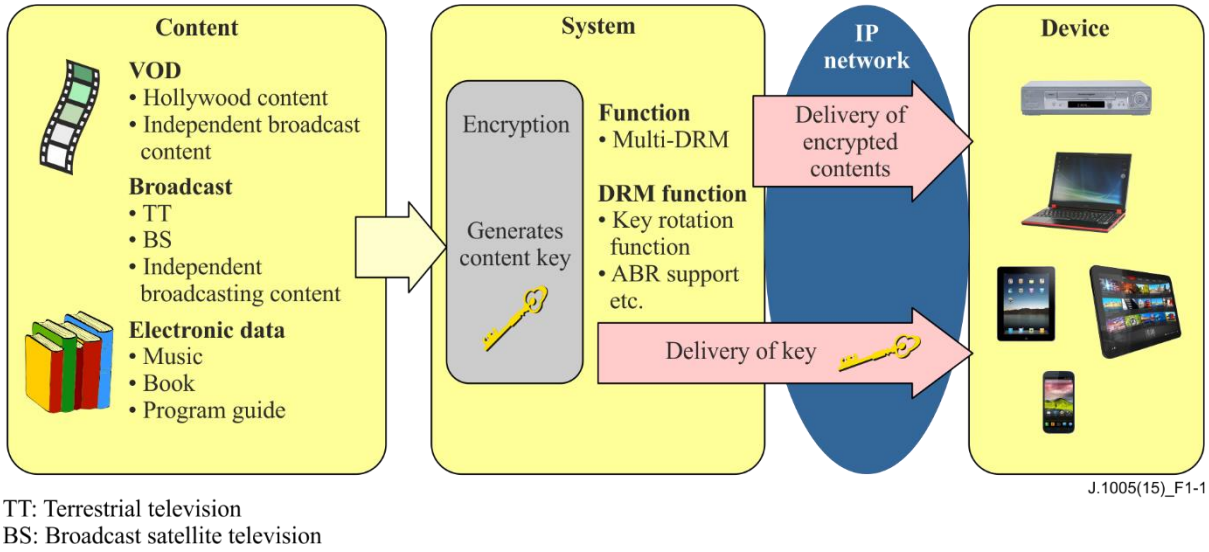
Table of Contents

		Page
1	Scope	1
2	References	1
3	Definitions	1
3.1	Terms defined elsewhere	1
3.2	Terms defined in this Recommendation	2
4	Abbreviations and acronyms	2
5	Conventions	3
6	Overview of DRM for cable television multiscreen	4
6.1	Cable platform and DRM	4
6.2	Service model	6
6.3	Delivery method and content protection	6
7	Architecture of DRM for cable television multiscreen	7
7.1	Components and flow	9
7.2	Encoder/Transcoder	10
7.3	Content package server (encryption)	10
7.4	Content delivery server	10
7.5	Licence server	11
7.6	Domain management server	11
7.7	Client device	11
7.8	Authentication server	12
8	Requirements of the DRM system for cable television multiscreen	12
8.1	System requirements	12
8.2	Functional requirements	13
8.3	Service requirements	14
8.4	DRM content format requirements	16
Appendix I – Use cases		18
Appendix II – Service scenarios		20
II.1	Online streaming	20
II.2	Purchase of download content	21
II.3	Rental	21
II.4	Subscription	22
Appendix III – Multi-DRM service types		24
III.1	Multi-DRM type I: Plug-in type	24
III.2	Multi-DRM type II: Common communication interface type	24
III.3	Multi-DRM type III: Download type	25
Bibliography		26

Introduction

The rapid deployment of smartphones and tablet devices has changed people's TV watching habits in the home and outdoors. TV Everywhere services, including IP linear TV and IP video on demand (VoD), will inevitably increase the traffic of media streaming and downloading over IP networks that enable both in-home and outdoor services. In such a case, a digital rights management (DRM) technology is required for content rights protection based on device authentication.

Currently DRM is an aggregation of different technologies and each DRM closely depends on the content holder's rights. DRM architecture and requirements for cable operators are required to be standardized so that they can deploy new services in keeping with content holders' rights that shall cover cable customers' multiple devices.



TT: Terrestrial television
BS: Broadcast satellite television

Figure 1-1 – DRM for cable television IP video service

As shown in Figure 1-1, there are three aspects of DRM: content, headend and end terminal devices. The DRM function is itself independent from content delivery network structures. This Recommendation provides an overview of DRM for cable television multiscreen and defines DRM architecture. The requirements of DRM for cable television multiscreen are also described based on a defined architecture model. In accordance with these requirements, this Recommendation considers DRM specifications which contain a DRM licence scenario for future services. This Recommendation describes content format specifications because this is related to the existing DRM system. A possible implementation of a DRM system that satisfies these requirements and considerations is also described.

Generally raw contents (content that has not been encrypted and that are mostly supplied by the content provider) are entered into the platform. After the authentication of the cable customer and of the customer's end terminal devices by the identity provider (IdP) function in the platform, the DRM server encrypts the content using the content key. The encrypted contents are distributed to the customer's end terminal devices over the content delivery network (CDN) and the cable network. The content key is encrypted by another key (the device key) for secure key delivery and distributed separately from the contents. The end terminal device which has a DRM licence can only decrypt the content distributed by the content key and the device key of the end terminal device.

Recommendation ITU-T J.1005

Architecture and requirements of digital rights management (DRM) for cable television multiscreen

1 Scope

This Recommendation specifies the architecture and requirements for a DRM system for a cable television content delivery service including multiple device viewing experiences. It is anticipated that the architecture and requirements identified in this Recommendation can be applied to the DRM service that covers protected IP-type contents (IP VOD, IP linear, etc.) delivery from content providers or cable operators to end terminal devices (PC, tablet, smartphones, etc.) via cable platforms, content delivery networks (CDNs), headend and cable networks.

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.222.0] Recommendation ITU-T H.222.0 | ISO/IEC 13818-1:2013, *Information technology – Generic coding of moving pictures and associated audio information: Systems*.

[ITU-T H.265] Recommendation ITU-T H.265 (2015), *High efficiency video coding*.

[ISO/IEC 14496-12] ISO/IEC 14496-12:2012, *Information technology – Coding of audio-visual objects – Part 12: ISO base media file format.*

[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 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 authentication [b-ITU-T X.800]: See data origin authentication and peer-entity authentication.

3.1.2 authorization [b-ITU-T J.260]: The act of determining if a particular privilege, such as access to telecommunications resource, can be granted to the presenter of a particular credential.

3.1.3 content provider [b-ITU-T Y.1910]: The entity that owns or is licenced to sell content or content assets.

3.1.4 content delivery network [b-ITU-T F.750]: A network optimized for delivering digital content.

3.1.5 data origin authentication [b-ITU-T X.800]: The corroboration that the source of data received is as claimed.

3.1.6 digital rights management [b-ITU-T X.1193]: A synonym for service and content protection or content protection, depending upon the context of use.

3.1.7 identity provider [b-ITU-T X.1252]: An entity that verifies, maintains, manages, and may create and assign identity information of other entities.

3.1.8 linear broadcast [b-ITU-T Y.1910]: Also known as linear TV. A television service in which a continuous stream flows in real time from the service provider to the terminal device and where the user cannot control the temporal order in which contents are viewed.

3.1.9 peer-entity authentication [b-ITU-T X.800]: The corroboration that a peer entity in an association is the one claimed.

3.1.10 platform [b-ITU-T J.296]: A business entity that manages and operates a collection service on a network of digital broadcasting.

3.1.11 revocation [b-ITU-T X.1252]: The annulment by someone having the authority, of something previously done.

3.1.12 service provider [b-ITU-T M.1400]: A general reference to an operator that provides telecommunication services to customers and other users, either on a tariff or contract basis. A service provider may or may not operate a network. A service provider may or may not be a customer of another service provider.

3.1.13 streaming [b-ITU-T Y.2253]: Streaming service over multi-connection provides multimedia features such as video/audio/text/graphics/data in real time supported by the required level of QoS/QoE, security, interactivity and reliability.

3.1.14 video on demand (VoD)[b-ITU-T Y.1910]: A service in which the end user can, on demand, select and view video content and where the end user can control the temporal order in which the video content is viewed (e.g., the ability to start the viewing, pause, fast forward, rewind, etc.).

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 content key: A key used to protect the cable content data stream(s).

3.2.2 domain: A group of devices defined by a rights issuer such that the rights issuer can issue rights to objects for the group that can be processed by all devices within the group and only by those devices.

3.2.3 multi-DRM: A system which can select suitable DRM from two or more DRMs based on a special service feature, the load of a system, a network situation, etc.

3.2.4 IP VoD: A service to deliver video content following a request from a user. IP-VOD supplies each video content on an on-demand basis.

3.2.5 non-STB: Personal computers (PCs), tablets and smartphone devices other than set-top boxes (STBs) which are capable of handling IP based interactive services.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ABR Adaptive Bit Rate

BS	Broadcast Satellite television
CAS	Conditional Access System
CDN	Content Delivery Network
CENC	Common Encryption scheme
CP	Content Provider
CPCM	Content Protection and Copy Management
DASH	Dynamic Adaptive Streaming over HTTP
DECE	Digital Entertainment Content Ecosystem
DOCSIS	Data Over Cable Service Interface Specifications
DRM	Digital Rights Management
DTCP	Digital Transmission Content Protection
FTTH	Fibre To The Home
HD	High Definition
HDS	HTTP Dynamic Streaming
HLS	HTTP Live Streaming
HFC	Hybrid Fibre/Coaxial
LTE	Long Term Evolution
MPEG	Moving Picture Experts Group
MSS	Microsoft Smooth Streaming
PF	Platform
SMS	Subscriber Management System
SDK	Software Development Kit
STB	Set-Top Box
SP	Service Provider
VoD	Video on Demand

5 Conventions

In this Recommendation:

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document 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 document 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. 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 Overview of DRM for cable television multiscreen

6.1 Cable platform and DRM

Content right protection is becoming more important due to various emerging contents, distribution of hi-quality movies, enhancement of user experiences and changes in media procurement styles, etc. The DRM system offers a content rights protection method that can be applied in such a varied service environment. By exchanging licence information between a customer terminal device and a DRM system, a DRM licenced terminal device can decrypt the content that was encrypted in the DRM system prior to content distribution. In this Recommendation the contents to be protected by DRM are generally contents for IP linear and IP VoD services. It is anticipated that platform providers will select, install and maintain the necessary DRM system. However, a service provider (SP) and a cable operator can also take the place of the platform provider.

Figure 6-1 depicts DRM related functional components from content provisioning to content distribution for end terminal devices. The contents are mainly provided by content providers (CPs) and supplied securely to cable platforms via a dedicated network. The cable platform is operated by a platform provider. An SP delivers contents between a cable platform and a cable operator and the cable operator distributes the contents to the customer's end terminal device. In Figure 6-1, the DRM functions such as content packaging (encryption and licence distribution, etc.) are provided in the cable platform. This however is just one example and the DRM function can be installed either in the SP server or in the cable operator's server. The content can be transmitted over the open-basis distribution method already standardized in [ISO/IEC 23009-1]. The licence distribution sequence including DRM message data, etc. for DRM services must be transmitted securely between the cable platform and end terminal devices in accordance with each DRM system.

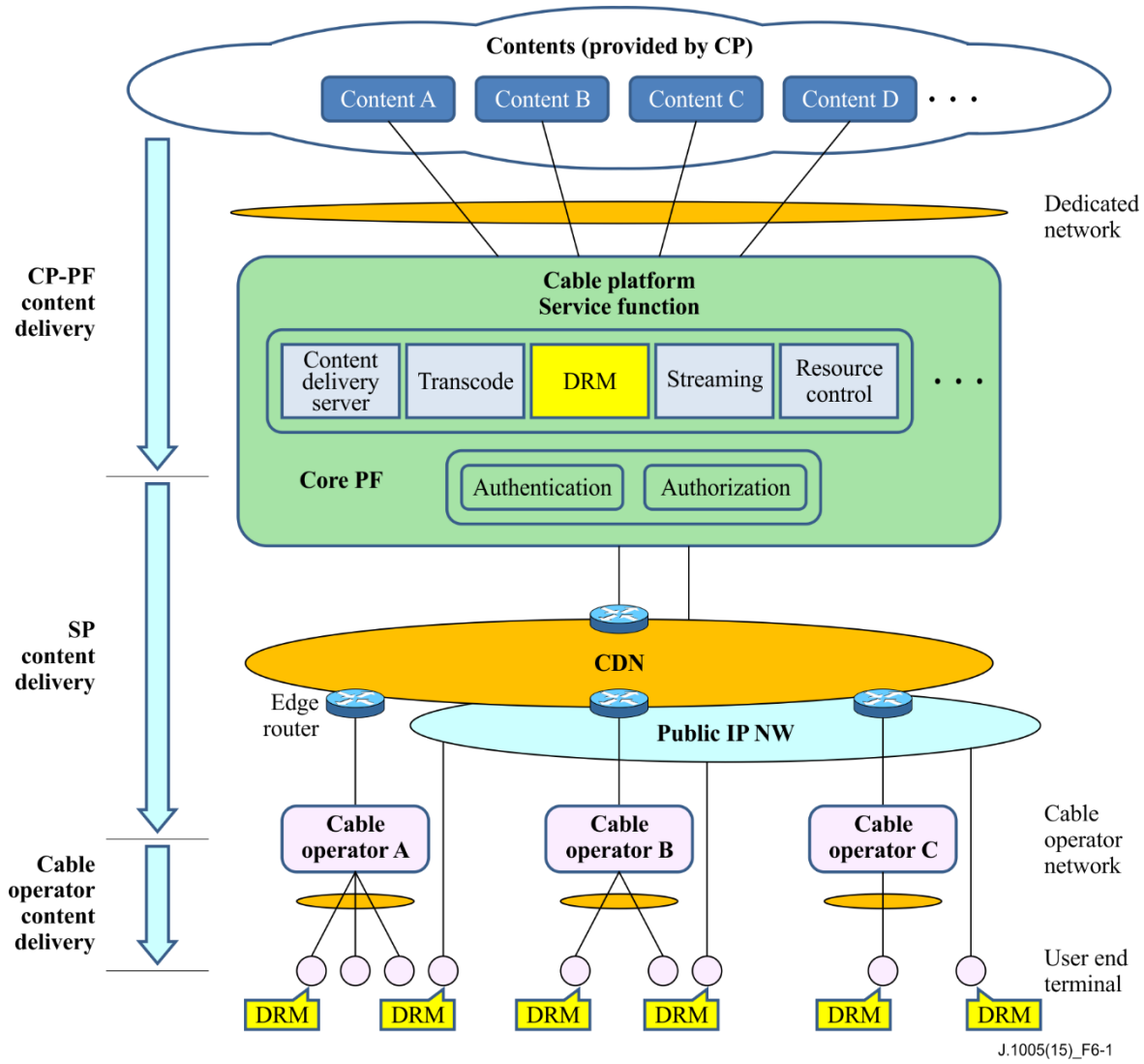


Figure 6-1 – Cable platform and DRM

Before starting cable services including content delivery, user authentication and service authorization are mandatory at the cable platform. The SP then judges the delivery of content (for example, confirming the exclusive control of condition for simultaneous viewing). After clearance of this judgement, the SP selects the content delivery method and DRM system, encrypts the content via the DRM system and sends the content to the cable operator's headend system. The content is delivered to the subscriber's end terminals (STB, PC, tablet and smartphone, etc.) via the cable operator's network. The SP delivers a licence with a set timing and delivery method. Only the licence on the end terminal can decrypt the content and only then can the subscriber enjoy the content viewing.

The timing of licence delivery depends on the DRM system and its usage scenario. Various DRM scenarios are available in the current content market in which DRM offers licence delivery after content distribution, licence delivery before content distribution or licence delivery at every content distribution.

DRM is required to protect content with encryption between the content provider and user end terminals and DRM must follow the compliance rules and robustness rules which shall be provided by the DRM system supplier.

6.2 Service model

Figure 6-2 shows an expected service model of IP video content delivery. The video content protected by DRM is delivered to the STB or non STB end-terminal located in the subscriber's home via the cable platform, the CDN and the cable operator's network. The content can also be used for outdoor remote services with DRM. In addition, a direct delivery service to non-STB end-terminals outdoors is also expected via a public IP network with DRM. For examples of DRM use-cases, refer to Appendix I.

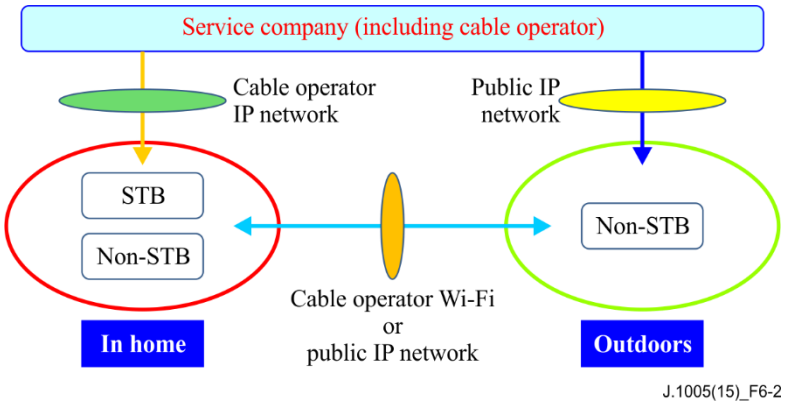


Figure 6-2 – An expected service model of IP video content delivery

6.3 Delivery method and content protection

Table 6-1 shows the relationship between the delivery method and content protection. Terrestrial and satellite broadcast contents are outside of the scope of this Recommendation.

Table 6-1 – Delivery method and content protection

Services	Contents	Network	End-terminals	Content rights protection	Remarks
IP linear TV	Terrestrial broadcast and satellite broadcast contents	Cable operator's network	STB	Outside of the scope of this Recommendation	e.g., IPTV Forum specification [b-IPTVFJ STD-0004]
			Non- STB	Outside of the scope of this Recommendation	e.g., IPTV Forum specification [b-IPTVFJ STD-0004]
		Public IP network	Non-STB	Outside of the scope of this Recommendation	e.g., IPTV Forum specification [b-IPTVFJ STD-0004]
	Community broadcast contents	Cable operator network	STB	DRM of this Recommendation	
			Non-STB	DRM of this Recommendation	
		Public IP network	Non-STB	DRM of this Recommendation	

Table 6-1 – Delivery method and content protection

Services	Contents	Network	End-terminals	Content rights protection	Remarks
IP VoD	VoD Contents	Cable operator network	STB	DRM of this Recommendation	
			Non-STB	DRM of this Recommendation	
		Public IP network	Non-STB	DRM of this Recommendation	
Transfer between terminals	Stored contents	Local network	Non-STB	DRM of this Recommendation Usage of link protection technologies is allowed after termination of DRM.	DLNA (DTCP-IP) is expected. The content right protection after DRM is outside of the scope of this Recommendation.
		Remote network	Non-STB	DRM of this Recommendation Usage of link protection technologies is allowed after termination of DRM.	DLNA (DTCP+) is expected. The content right protection after DRM is outside of the scope of this Recommendation.
NOTE – The definitions of local network and remote network shall be identical to the definitions specified by each content protection method.					

7 Architecture of DRM for cable television multiscreen

The DRM system is a dedicated system for content rights protection of IP based services (e.g., IP linear TV and IP VoD) that are delivered via a cable platform. The model of a general DRM system and the expected signal flow are shown in Figure 7-1. The DRM system is a function of the cable platform. The raw content located outside of the platform (PF) is sent to the DRM system after format transformation (e.g., encoding, transcoding) at the PF. Upon request by a DRM client (installed at a user end terminal device), the DRM system shall start encryption of the content and deliver a DRM licence (including decryption key) for the client. The encrypted content is sent to the DRM client by the content delivery server. The content delivery server itself is sometimes installed outside of the DRM system.

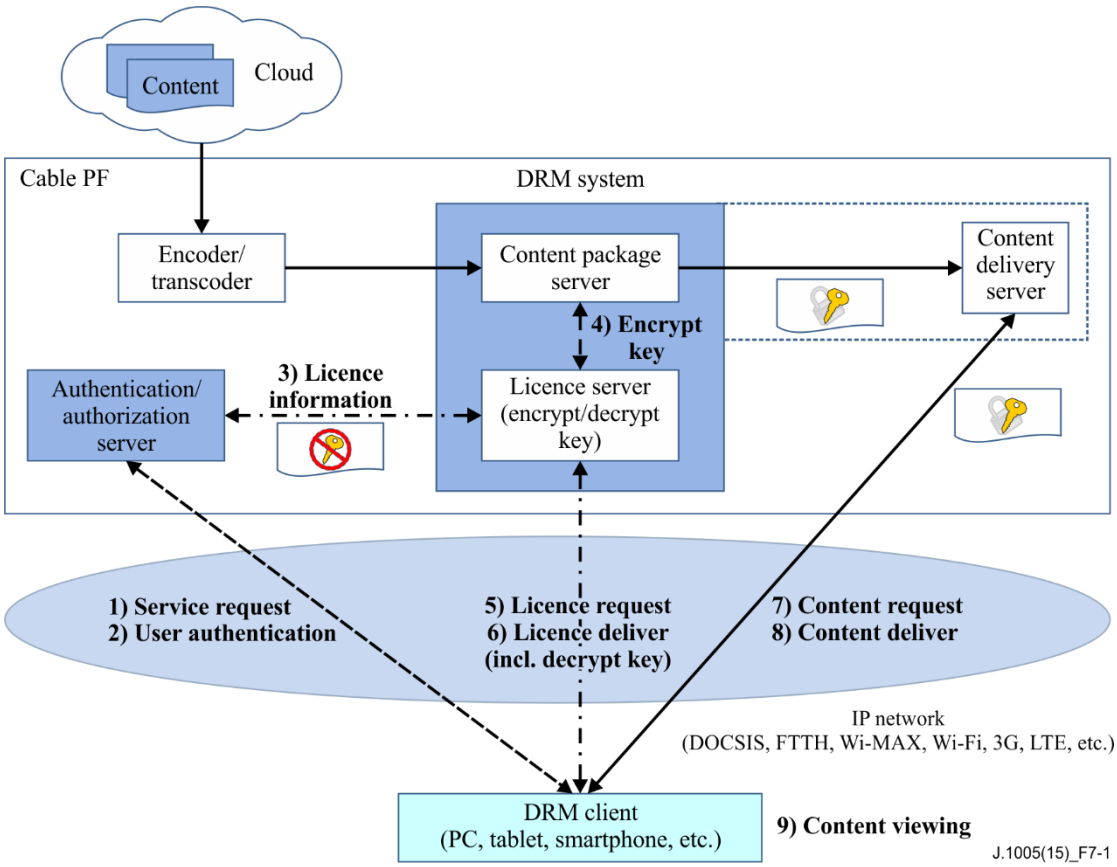


Figure 7-1 – Model of a general DRM system and expected signal flow (example)

The general process of the DRM system for the content distribution service is as follows:

(1) Service request: The subscriber (user) accesses the portal site of the cable operator through the DRM client for reception of service.

(2) User authentication/authorization: The portal site transfers the user request to the authentication/authorization server in the cable PF. User authentication/authorization is carried out at this server for personal identification and service reception authorization.

(3) Exchange of licence information: After user authentication/authorization, the SP decides whether to deliver the content to CDN considering available resources and other conditions. After this decision the DRM licence information is exchanged between the authentication/authorization server and the licence server.

(4) Generation of encryption key and content encryption: In accordance with the contract between the subscriber and the cable operator, the DRM licence server generates the encryption key and issues a licence and sends the key to the content package server for encryption of the content. It is anticipated that some services will require content encryption in advance before issuance of a licence.

(5) Request for a licence: The DRM client requests a licence from the licence server that shall contain a decryption key.

(6) Delivery of licence: The licence server delivers the licence for content decryption to the DRM client.

(7) Content request: Through the DRM client, the user requests the content that is stored in the content server.

(8) Content delivery: Upon the DRM client's request, the content delivery server sends the encrypted content using the adaptive bit rate (ABR) system. Two models are expected; a

reactive (post-delivery) model that issues the licence after content delivery, and a proactive (pre-delivery) model that issues the licence before content delivery.

(9) Content viewing: The DRM client decrypts the content using the decryption key contained in the licence and the user starts viewing content.

The DRM system is optionally required to handle a multi-DRM system as described in Appendix III.

7.1 Components and flow

The DRM system components and communication flow needed for construction of a DRM system are shown in Figure 7-2.

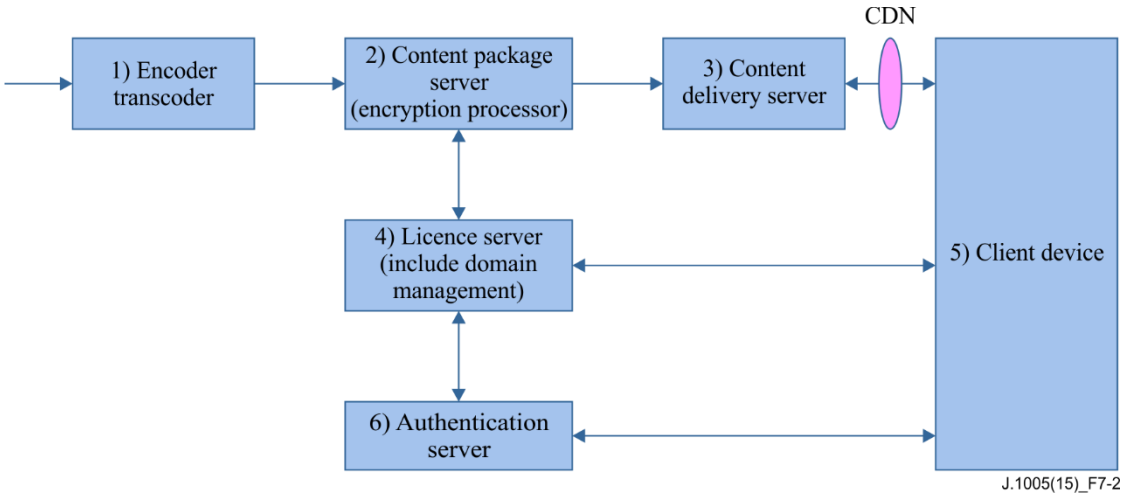


Figure 7-2 – DRM system components and communication flow

The functional overview of the DRM system components shown in Figure 7-2 is described in Table 7-1.

Table 7-1 – Functional overview of DRM system components

Component	Functional overview
(1) Encoder/Transcoder	Pre-processing for encryption of live stream, encoding of media file and transforming of container, etc.
(2) Content package server	Encryption of content to be delivered
(3) Content delivery server/ Content delivery network (CDN)	Upon request of content viewing, confirmation of session establishment Delivery of packaged content
(4) Licence server	Licence issuing and delivering for permitted client in cooperation with authentication server Domain management function is included in some cases.
(5) Client device Player implemented in DRM client	Based on user request of playback, requesting and receiving the licence, decrypting the content and playback
(6) Authentication server	User authentication and confirmation of subscriber information in cooperation with cable operator's SMS

An example of DRM processing flow is shown in Figure 7-3.

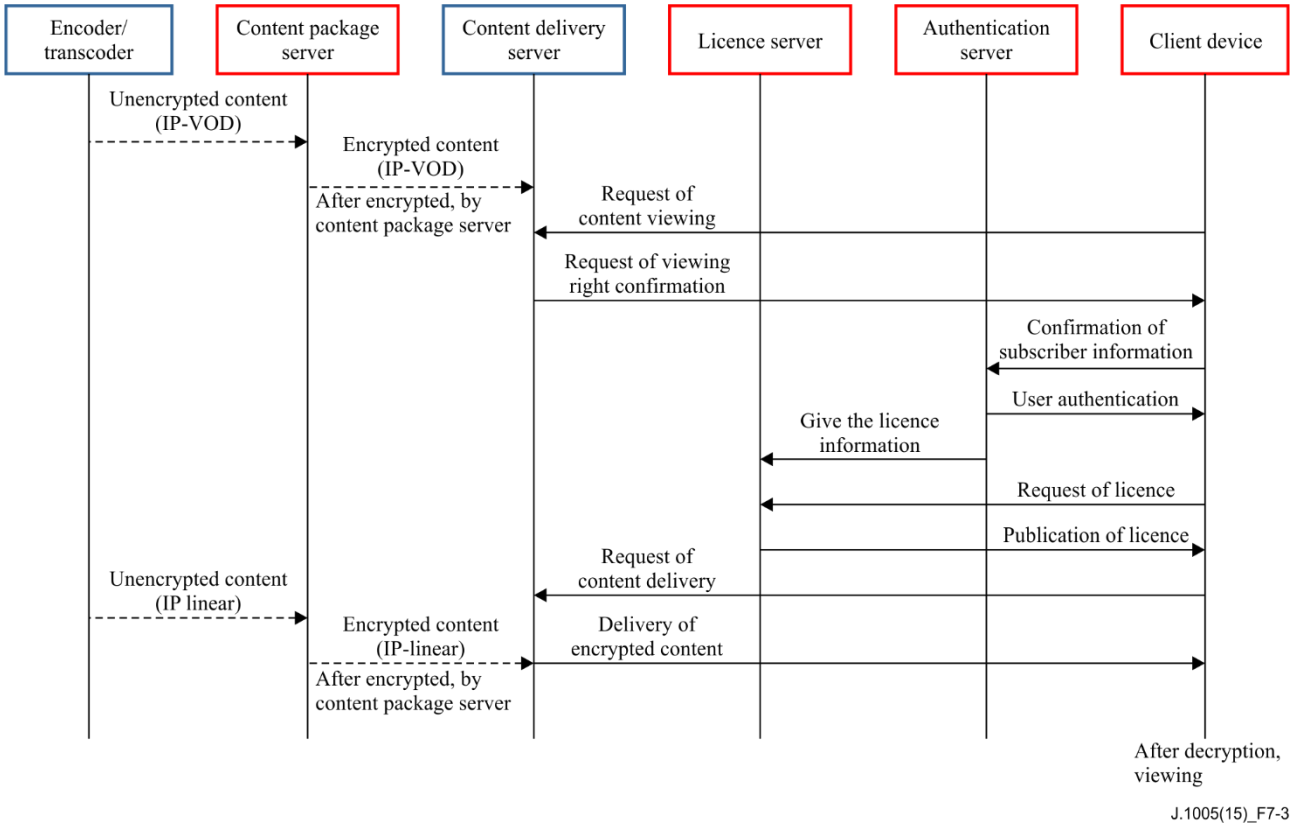


Figure 7-3 – Example of DRM processing flow

The role of each component of the DRM system is as follows.

7.2 Encoder/Transcoder

The encoder transforms the content to a deliverable data and format for the network and the transcoder transforms the content to receivable data (appropriate number of pixels, etc.) for devices. The DRM system shall process high definition (HD) content. The DRM system does not encrypt in this timing. The DRM system should use the MPEG2-TS/MP4 content format based on [ITU-T H.265].

7.3 Content package server (encryption)

The content package server component shall encrypt content using an international or proprietary specification of encryption in alignment with a content format such as the ISO base media file format [ISO/IEC 14496-12] or the MPEG-2 transport stream [ISO/IEC 13818-1]. For information on related container format specifications, the licence embedded method in the content file and the implementation of IP linear service, refer to clause 8.4. The content package server should implement the key rotation function with time duration. In the case of multi-DRM, the encryption key shall be common to contents. In decrypting the content, the client shall use each DRM key.

7.4 Content delivery server

The content delivery server delivers content to the client device in accordance with the content delivery method. The client device shall implement a module and function in the player component of the client device. The content delivery server shall deliver protected content to STB and/or non-STB devices (e.g., PC, tablet, smartphone, etc.).

7.5 Licence server

The licence server acquires user information from the authentication server for management and delivery of the licence. It generates licence information according to the DRM scenario described in Appendix II. It shall deliver a licence to a client device upon request. For information on the licence, refer to clause 8.3. The licence shall include the licence use case, licence delivery method and licence period control (limitation of playback period). For information on output/export control of content, refer to clause 8.3.

It should be noted that there are exclusive controls for simultaneous viewing as a content licence requirement from the content provider. This inhibits viewing of the same content by one user with STB and non-STB devices at the same time. This session management is outside of the scope in this Recommendation; however the cloud or the PF needs to be managed. In the case of VoD content viewing, the DRM system shall confirm that the user is not viewing the same content simultaneously, then it requests a licence. This Recommendation describes session control by the content delivery server, however session management by cloud or PF shall be also allowed independently. This matter is implementation-dependent. In addition, when the DRM server detects purchasing and viewing of the same content by a user, exclusive control for simultaneous viewing can be realized without delivering a licence to the device.

7.6 Domain management server

A user can specify a group of devices as a domain. In the case that a domain-bind licence is given to a device, all of the devices in the domain can use the protected content. The user can add and delete devices in the domain as long as the total number of the devices in the domain does not exceed a limit defined by the service. The domain management server holds a list of the entity (user, family, group of user, etc.) and evaluates the domain service availability. In addition, the domain management server shall check the number of available devices (in accordance with policy) and shall decide on the connection to the user. It is desirable to limit the maximum number of devices but this may be more strictly required by the content holder.

7.7 Client device

The client DRM shall be implemented in each client device individually as shown in Figure 7-4. The client DRM shall have a player function securely embedded in the device for the decryption and display of the content.

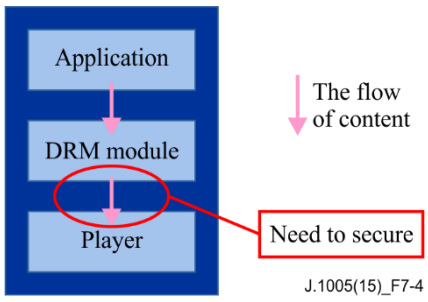


Figure 7-4 – Structure of client DRM

In addition, the decrypted content shall be displayed on other securely connected display devices that conform to the control requirement described for the delivered licence. This detailed method is implementation-dependent. The DRM system shall be able to deliver protected content to client devices (STB, PC, smartphone, tablet, etc.).

7.8 Authentication server

The PF includes an authentication/authorization function as described in clause 6. In the case of access to service by the user, the authentication server executes authentication and authorization by verifying the user ID and password stored in the cable operator subscriber management system (SMS). The authentication server forwards this result to the licence server in the DRM system and licence processing is started. A detailed description of the method of authentication and authorization is outside of the scope of this Recommendation.

8 Requirements of the DRM system for cable television multiscreen

This clause describes requirements for the DRM system (functions to be provided by the DRM system as a whole) and functional requirements for a single DRM (functions to be provided by a DRM method). In addition, service and DRM content format requirements are described.

8.1 System requirements

SSR-001: DRM for cable television multiscreen is required to protect rights of contents including video, audio, captions and other data.

SSR-002: DRM for cable television multiscreen is required to support both streaming and download services.

SSR-003: DRM for cable television multiscreen is required to support cable business related to DRM (IP linear TV, IP VoD services, etc.) over the cable platform. In such circumstance a DRM method shall be selectable by cable operators and/or platform providers.

SSR-004: DRM for cable television multiscreen is required to support adaptive bit rate (ABR). Usage of ABR is mandatory for the delivery of digital contents over the IP network from a cable PF.

SSR-005: DRM for cable television multiscreen is required to control the licence delivery sequence (DRM message data, etc.) and licence management (generation of content encryption key, etc.).

SSR-006: DRM for cable television multiscreen is required to control recording and viewing of content required by the content owner or SP in accordance with the contract between concerned parties.

SSR-007: DRM for cable television multiscreen is required to support HD video contents. As end terminal devices in the market already support HD video content (4K/8K video in future) and the user requirement for high quality video is strong, DRM shall support HD or more hi-resolution video contents. (DRM is required to control available resolution of video.)

SSR-008: DRM for cable television multiscreen is required to limit the maximum numbers of downloadable end terminals. This may become mandatory if approval of the content rights of a content holder is required.

SSR-009: DRM for cable television multiscreen is required to control exclusive simultaneous viewing. In the case of a strict requirement for the control of exclusive simultaneous viewing from the content provider (CP), there is a case that the DRM system be required to protect the content rights for two or more individual end terminals having the same user ID.

SSR-010: DRM for cable television multiscreen is required to support the content format for MPEG2-TS/MP4, and ITU-T H.265 video in the future. These are considered major file formats for contents currently owned by content holders and expected for the TV Everywhere service.

SSR-011: DRM for cable television multiscreen is required to be included in an environment where the multi-DRM system works. For a description of the multi-DRM system, it is recommended to refer to Appendix III. In such a system the content encryption key is commonly used and when decryption

is required via a request from an end terminal, each DRM shall decrypt the content via each device key.

SSR-012: DRM for cable television multiscreen is required to support key renewal over time (i.e., key rotation function). This is useful to prevent tapping and some content holders require this function. Aspects of the key rotation function are shown in Figure 8-1. The content key is changed at set time intervals to enforce the security of content protection.

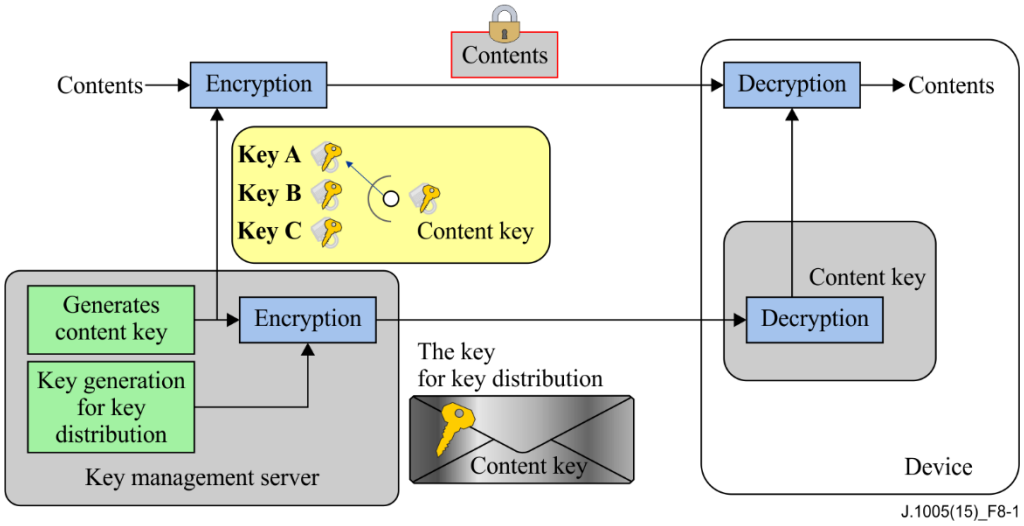


Figure 8-1 – Aspects of the key rotation function

SSR-013: DRM for cable television multiscreen is required to deliver the protected content to the STB in which the DRM licence is stored. Furthermore, the DRM system shall be able to deliver the content to at least one of the end terminals listed below:

- PC (Windows, Mac)
- smartphone (Android, iOS, Windows)
- Tablet (Android, iOS, Windows)

The link protection method (DTCP-IP, DTCP+) is optionally required for continual rights protection after the termination of DRM, however this is outside of the scope of this Recommendation.

SSR-014: When a user accesses a service at the beginning, the authentication server shall authenticate the user with verification of user ID and password stored in the subscriber management system (SMS), the authorization server is required to verify user's eligibility for the requested service. DRM for cable television multiscreen is required to respect this decision and to initiate the DRM licence process.

SSR-015: DRM for cable television multiscreen shall have a revocation function to invalidate the DRM process and stop services at each end terminal.

8.2 Functional requirements

FR-001: DRM for cable television multiscreen is required to control the decryption of contents via a licence based on a viewing contract for streaming and download services. Furthermore, in the case of a download service, common holding of the contents (common holding of licence information by a domain) is required.

FR-002: DRM for cable television multiscreen is required to protect rights of recorded contents.

FR-003: DRM for cable television multiscreen is required to deliver licence information containing the content key and control method in accordance with each DRM technology provider.

FR-004: DRM for cable television multiscreen is required to supply the content key bound by each end device. It is expected that the viewing service is only allowed by a registered end device.

FR-005: DRM for cable television multiscreen is required to supply the content key bound by a domain. Figure 8-2 depicts aspects of the domain function. Content viewing is allowed by the end terminals belonging to the domain, but is not allowed in a different domain. The domain function helps to reduce network resource utilization due to local decryption of content and common holding of licences for download services.

FR-006: DRM for cable television multiscreen is required to control the period of content reproduction. The content delivery service is expected to apply within a limited period (rental model, etc.).

FR-007: DRM for cable television multiscreen is required to control external output, copying and movement of contents.

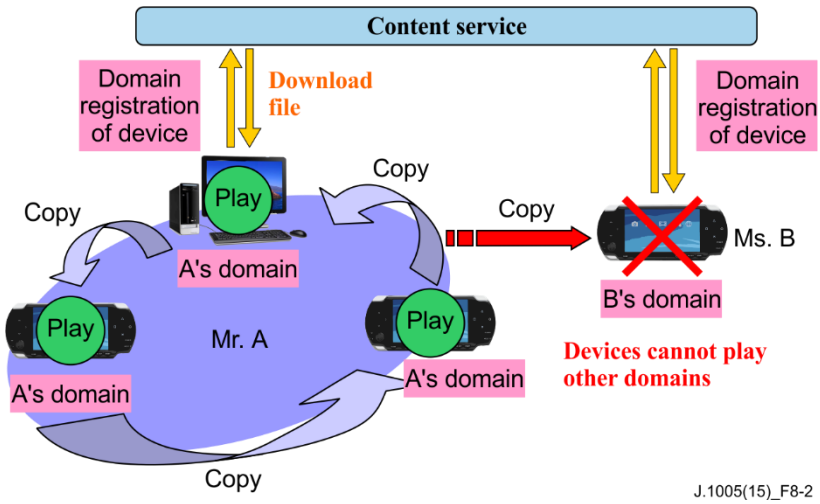


Figure 8-2 – Aspects of the domain function

8.3 Service requirements

This clause describes a desired service to be realized by DRM itself for the delivery of cable services. The functions that could not be fulfilled by DRM itself, such as restriction of the number of device registrations by domain function, limitation of the number of simultaneous viewing terminals or restriction of the content usage period given by the licence server, might be realized through the cooperation of other functions within the DRM system. The DRM functions described in this Recommendation, such as licence, period restriction, output control, copying, moving, etc. shall be implemented to fulfil the compliance rules and the robustness rules provided by the DRM technology supplier. In the case of security problems in the DRM-embedded terminal, a revocation to invalidate the terminal function might be allowed. Each DRM technology supplier's policy shall be referred to in cases of revocation.

SER-001: Licence

The licence contains control information for DRM content usage, decryption keys (content key, domain key (SER-002) and service key (SER-003)). The usage of DRM content shall be controlled by one or more chained licences. An SP shall be able to select service control information such as service period through the request of a CP, in accordance with use cases and DRM scenarios.

Detailed methods or mechanisms shall be in accordance with the specifications described by the DRM technology suppliers. Differences in terminology for licences or names of keys in said technology supplier specifications shall be resolved.

SER-002: Bind-licence

The bind-licence shall limit DRM content usage for a specific terminal device by binding keys (content key, etc.) with the terminal device. It is desirable that personal devices such as PCs, smartphones and tablets can handle DRM technology over the multi platforms controlled by cable operators. A domain function of DRM can fulfil this requirement. Under the licence issued by the domain function, DRM can limit the usage of DRM content in the specific domain by sharing keys among devices belonging to the same domain.

Device bind: This is an encryption method of the content key using the dedicated device encryption key. This method enables the specific device to decrypt the content using the re-generated content key on the device in accordance with the delivered licence.

Domain bind: This is an encryption method of the content key using the specific domain encryption key. The terminal device shall obtain the domain key before the reception of the domain bind licence. As DRM is designed not to limit the number of terminal devices which join the domain, in the case of limiting the maximum number of devices within the domain, the DRM system shall provide other methods outside the domain to do so.

SER-003: Chained licence

Chaining a single licence per DRM content and a common licence which has common control information for several DRM contents may create a unified DRM control system for new services. In a subscription service scenario, in order to control the usage of different DRM contents uniformly, each licence in a content shall have an encrypted content key and a service key for subscription shall also be used as the encryption key of the content key. That is to say, a licence for the delivery of the service key contains a service key encrypted by the device key and domain key. This is an example of a chained licence.

SER-004: Delivery of licence

DRM shall start a licence delivery sequence based on the DRM header information provided by itself or any other method. The method for obtaining DRM header information shall be in accordance with the DRM technology supplier specification or with specific rules set by the SP.

In the case of using a DRM header embedded in a content file, a client can receive a licence after reception of part or all of a content. In the case of any other method being used, there will be no restriction on the before/after relationship between licence delivery and content delivery, except for the case where the licence retains information necessary for content delivery. Some DRM scenarios require delivery of the licence which is embedded in the content file. In such cases a common usable licence may be embedded for multiple clients in the group.

SER-005: Licence storing

Licence storing shall be controlled in accordance with the DRM scenario. The storing method shall be in accordance with the DRM technology supplier specification or other specific rules such as the compliance rule and/or robustness rule.

SER-006: Limiting period

DRM shall be able to judge the usage of content at every request based on the limiting period rule if the content is attached to the limiting period rule. Basically the limiting period control shall be in accordance with licence, however the licence server can control the period if allowed by the cable operator. The type of limiting period shall be respected by the DRM scenario in accordance with a request by the CP or SP. In the case of a rental service, it is assumed that the limiting period starts at content procurement time, or at the first play back or a combination of these events. In the case of a subscription service, the same can be applied, however it is desirable to use the licence chain in anticipation of an extension of the contract period.

SER-007: Output control

DRM shall allow transfer of content only to the sink device which is approved by a compliance rule of the DRM technology supplier. In the case of content transferred toward a specific output, which is approved by the DRM technology supplier beforehand (such as analogue output, digital output, DTCP, HDCP, etc.), it is required to be in accordance with the output control method described in a compliance rule, or with the output control information. The CP can decide how to control the output for each content in accordance with the compliance rule instructed by the licence.

SER-008: Copy and move

DRM shall control copy or move actions via a licence or licence server, or a combination of both. DRM shall support copy and move actions with the methods described below:

Copy and move without release of DRM: This is the method for copy and move between devices embedded in the same DRM technology. Copy using the domain function is an example. The domain function enables copying of DRM content within the domain applying the content and licence file transfer method. In this case there is no need for re-delivery of the content and licence to the device addressed. Upon approval of the content rights holder, copy and move are also available using the DRM specific licence transfer function.

Export to security domain outside of DRM (copy and move with release of DRM): This is the method for exporting content toward a specific domain such as digital transmission content protection (DTCP) approved by the compliance rule of the DRM technology supplier. In the case of different export conditions for each content, it is required to control the copy and move in accordance with the licence attached to the content.

8.4 DRM content format requirements

This clause describes a necessary content format for protection by DRM, a content container format and a relationship with the content delivery method.

CFR-001: Application to content container format

It is necessary to consider DRM binding method as corresponding to the content container format (encryption method and embedding method of the DRM header in the content container) for content encryption and decryption with DRM in receiving devices. Container format is a file format defined to hold various encoded content data such as audio, video, caption and metadata.

In the services assumed in this Recommendation, it is desirable to define a DRM binding for a container format of delivered content so that multiple devices receiving content streaming services can receive content protected by DRM. It is also desirable to develop devices utilizing these methods.

Application developers need to implement DRM binding when developing playback applications of DRM content for various devices. In some cases by including DRM binding in development and in other cases utilizing tools such as software development kits (SDKs) provided by DRM providers.

CFR-002: DRM header

The DRM header is required to be defined as an item of data including information for obtaining the necessary licence for playback from the licence server when watching content protected by DRM in devices.

For each DRM system, the DRM header format is defined according to its specification by the DRM technology provider and it is necessary to adhere to the specification for the process to run correctly within the DRM module.

CFR-003: Applicable content delivery method

When delivering content in the cable platform, as in the case of content delivery by streaming, methods which have adaptive bit rate (ABR) functionality are required.

CFR-004: Constraint of container format

Applicable content container format is required to be defined for each content delivery method. The container format to be prepared depends on the selection of the content delivery method. Therefore, in selecting a content delivery method, it is necessary to consider this constraint.

CFR-005: Consideration on application of MPEG-DASH

The content delivery method by MPEG-DASH is defined by the International Standard [ISO/IEC 23009-1], as opposed to other content delivery methods defined by specific technology providers. In addition, as the container format specification [ISO/IEC 14496-12] and the DRM binding specification [ISO/IEC 23001-7] are also defined as the International Standard, many DRM methods conform to MPEG-DASH.

In these circumstances, due to the mitigation effect for constraints and conditions in selecting a DRM method, it is desirable to adopt the content delivery method based on MPEG-DASH as far as possible.

CFR-006: Considerations on the key rotate function

When delivering content in an IP linear TV service, in the case of content protection by DRM per channel, continuing to use only one content key for each channel sometimes does not meet the security requirements of the content provider. In these cases, it is necessary to adopt the DRM method with the key rotate function which changes the content key in a certain period, and it is desirable that the following items are met in the selected DRM method.

In the case that these security requirements are not able to be met via the DRM method, it is desirable to achieve the security requirements through collaboration with the conditional access system (CAS) system.

1) As there are many channels in the general IP linear TV service, it is required that viewing rights can be managed, for example, in order to disable viewing of all the channels when the contract is expired.

2) It is required to hold a mechanism to avoid the possibility of interruption of viewing due to the licence obtaining procedure while watching content.

   For example, it is required that the key for decrypting a group of content keys (changed in a certain period) can be obtained in advance by embedding an encrypted content key in the content.

3) It is required that there is a mechanism to suppress the delay prior to the start of viewing due to the licence obtaining procedure when changing the channel of the DRM content in the IP linear TV service.

Appendix I

Use cases

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

Possible basic use cases for the IP video delivery service by cable operator or SP are categorized in Tables I.1 and I.2. Table I.1 shows the use cases for reception and viewing at an end terminal without secondary content usage (i.e., remote viewing, copy and move, etc.). Table I.2 describes use cases for content delivery between end terminals in the home or outdoors, with secondary content usage.

Table I.1 – Use cases for reception and viewing at the end terminal

Number	Style of reception or viewing	Content for delivery	Place of reception or viewing	End terminal
A-1	Reception of broadcast programme	IP linear content	In-home	STB
				Non-STB
			Outdoors	Non-STB
A-2	Viewing of recorded programme	IP linear content	In-home	STB
				Non-STB
			Outdoors	Non-STB
A-3	Recording of programme	IP linear content	In-home	STB
				Non-STB
			Outdoors	Non-STB
A-4	Exchanging end terminal	IP linear content	In-home	STB to Non-STB
				Non-STB to STB
				Non STB to Non-STB
			Outdoors	Non STB to Non-STB
A-5	Streaming viewing	IP VoD content	In-home	STB
				Non-STB
			Outdoors	Non-STB
A-6	Viewing after download	IP VoD content	In-home	STB
				Non-STB
			Outdoors	Non-STB
A-7	Downloading	IP VoD content	In-home	STB
				Non-STB
			Outdoors	Non-STB

Table I.2 – Use cases for content delivery between end terminals in-home or outdoors

Number	Transmission method	Content for delivery	Place of reception or viewing	End terminal
B-1	Streaming	Recorded IP linear content	In-home	STB to Non-STB
			In-home	Non-STB to STB
			In-home	Non-STB to Non-STB
		Recorded IP VoD content	In-home	STB to Non-STB
			In-home	Non-STB to STB
			In-home	Non-STB to Non-STB
B-2	Remote streaming	Recorded IP linear content	Outdoors	STB to Non-STB
			In-home	Non-STB to STB
			Outdoors	Non-STB to Non-STB
		Recorded IP VoD content	Outdoors	STB to Non-STB
			In-home	Non-STB to STB
			Outdoors	Non-STB to Non-STB
B-3	Copy	Recorded IP linear content	In-home	STB to Non-STB
			In-home	Non-STB to STB
			In-home	Non-STB to Non-STB
		Recorded IP VoD content	In-home	STB to Non-STB
			In-home	Non-STB to STB
			In-home	Non-STB to Non-STB
B-4	Move	Recorded IP linear content	In-home	STB to Non-STB
			In-home	Non-STB to STB
			In-home	Non-STB to Non-STB
		Recorded IP VoD content	In-home	STB to Non-STB
			In-home	Non-STB to STB
			In-home	Non-STB to Non-STB

Tables I.1 and I.2 show use cases for possible services, however this Recommendation does not exclude other use cases.

Appendix II

Service scenarios

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

This appendix describes general DRM service scenarios to be expected in the delivery of a cable service. A DRM scenario is a description of an action of terminal or device in such a case of licence obtainment or DRM content playback. Not limited to the scenarios in this Recommendation, it will be possible to study other scenarios in specific events.

Taking into account cable operator efforts to create various business models, this Recommendation does not specify a timing of charging, etc.

In addition in this appendix, an example of content rights protection using a DRM scenario is described in line with each use case in Appendix I. The example is not required to be set in force as its nature is not mandatory. This Recommendation covers DRM scenarios based on desirable DRM specifications, but does not specify the way content protection using link protection technology is defined in the Digital living network alliance (DLNA (www.dlna.org)).

Possible combinations between use cases and DRM scenarios are summarized in Table II.1.

II.1 Online streaming

The terminal or device shall get a licence in every event of content playback. The obtained licence cannot be stored in the device and is only usable for the sessions allowed by the licence. Only the device permitted by the licence can playback DRM content.

1) Adaptation to the use case of reception or watching IP linear content at a terminal (informative)

For use case A-1: Watching broadcast content, this scenario could be adapted to the service in which the licence shall be confirmed in every event of connection to the content (or channel) of the IP linear service. As an exceptional case, this scenario could be adapted to the use cases of A-2: Playback of recorded content, A-3: Content recording and A-4: Exchange of watching terminal in the case where storage of recorded content is allowed and licence confirmation is required in every action of recorded content playback.

2) Adaptation to the use case of reception or watching IP-VoD content at a terminal (informative)

For use case A-5: Watching streaming content, this scenario could be adapted to the service in which the licence shall be confirmed in every event of DRM content playback. For the case of content storage after downloading, in case where the licence shall be confirmed in every event of DRM content playback, this scenario could be adapted to the use cases of A-6: Playback of downloaded content and A-7: Download.

3) Adaptation to the use case of content transfer between terminals (informative)

For all use cases, this scenario could be adapted to the service in which the licence shall be confirmed in every event of DRM content playback at a secondary terminal, after storage of the DRM content at the original terminal by way of downloading or recording and transfer to the secondary terminal. Some DRM systems have a function to issue a licence at the original terminal. In such a case, the original terminal will not be necessary to obtain a licence from the licence server provided by service operator.

II.2 Purchase of download content

In this scenario, regardless of the timing of the licence obtainment at the terminal (before or at the time of content download), the terminal can obtain a licence only once. The licence is stored at the terminal and is usable without a time limitation. DRM content could be replayed at only licenced terminal indefinitely. Upon approval by a CP, an operator or a content holder, all registered terminals could playback content using an appropriate DRM without a time limitation.

1) Adaptation to the use case of reception or watching IP linear content at a terminal (informative)

This scenario (purchase of a download content (or channel) of an IP linear service) is not a common case, however it could be adapted to use cases A-2: Playback of recorded content and A-3 Content recording in the case where the storage of a DRM content and indefinite service via the obtained licence are allowed. Use case A-1: Watching broadcast content is not applicable because this scenario is for a download service. Use case A-4: Exchange of watching terminal could be understood as being the same as the use case of content transfer between terminals.

2) Adaptation to the use case of reception or watching IP-VoD content at a terminal (informative)

This scenario could be adapted to use cases A-6: Playback of downloaded content and A-7: Download in the case where an indefinite watching service via an obtained licence is allowed for a stored DRM content. Use case A-5: Watching streaming content is not applicable because this scenario is for a download service.

3) Adaptation to the use case of content transfer between terminals (informative)

Upon approval by the CP, operator or content holder, this scenario could be applied by licence re-distribution through a licence server or through the addition of a domain function to a secondary terminal. For a more detailed description see SER-008 in clause 8.3.

II.3 Rental

In this scenario, regardless of the timing of the licence obtainment at a terminal (before or at the time of content download), the terminal could obtain a licence only once at the beginning of the DRM content rental service. The licence is stored at the terminal and usable within the duration given by the licence. The DRM content could be replayed only at the licenced terminal within the validity period of the licence.

1) Adaptation to the use case of reception or watching IP linear content at a terminal (informative)

For use case A-1: Watching broadcast content, this scenario could be adapted to the service in which a limited duration service controlled by a licence is allowed for a specific content (or channel) delivered by an IP linear service. This scenario could also be adapted to use cases A-2: Playback of recorded content and A-3 Content recording in the case where a limited duration service controlled by a licence is allowed for a stored DRM content delivered by an IP linear service. Use case A-4: Exchange of watching terminal could be understood as being the same use case as that of content transfer between terminals.

2) Adaptation to the use case of reception or watching IP-VoD content at a terminal (informative)

For use case A-5: Watching streaming content, this scenario could be adapted to the service in which a limited duration service controlled by an obtained licence is allowed for a specific DRM content. This scenario could also be adapted to use cases A-6: Playback of downloaded content and A-7: Download in the case where a limited duration service controlled by a licence is allowed for a downloaded and stored DRM content delivered by an IP-VoD service.

3) Adaptation to the use case of content transfer between terminal devices (informative)

This scenario can be adapted by way of a re-delivery of a licence toward a targeted terminal device, domain function and licence transfer from a source device to a sink device, etc., under approval of the content rights holder such as a CP or cable operator. For a more detailed description of copy and move see clause 8.3 regarding SER-008. This scenario can be applicable for use case A-4: Exchange of watching terminal.

II.4 Subscription

It is not necessary to specify the timing of licence obtaining by the terminal device (whether before the download or at the same time as the download), a subscription licence shall be obtained at the start point of a subscription service or at first usage time of a DRM content. The licence shall be stored in a terminal device and it is usable in the period given by the licence. The subscription licence enables a terminal device to play back contents that are registered in the subscription service. The DRM content can only be played back by the terminal device that has a subscription licence with the effective period.

1) Adaptation to the use case of reception or watching IP linear content at a terminal (informative)

Although it is not a common scenario, for use case A-1: Watching broadcast content, this scenario could be adapted to the service in which specific IP linear contents can be played back only in a specific period indicated by an obtained licence. This scenario could also be adapted to use cases A-2: Playback of recorded content and A-3 Content recording for a limited duration service by a subscription licence in the case where storing a DRM content and play back of the content are allowed by the subscription licence. Use case A-4: Exchange of watching terminal could be understood as the same use case of content transfer between terminals.

2) Adaptation to the use case of reception or watching IP-VoD content at a terminal (informative)

For use case A-5: Watching streaming content, this scenario could be adapted to the service in which a limited duration service controlled by an obtained licence is allowed for a specific DRM content. This scenario could also be adapted to use cases A-6: Playback of downloaded content and A-7: Download in the case that a limited duration service by a licence is allowed for a stored DRM content delivered by an IP-VoD service.

3) Adaptation to the use case of content transfer between terminal devices (informative)

This scenario can be adapted by way of re-delivery of a licence toward a targeted terminal device, domain function, etc., under approval of a content rights holder such as a CP or a cable operator. For more detailed information of copy and move see clause 8.3 regarding SER-008. For use case A-4: Exchange of watching terminal, this scenario can be applicable.

In the IP linear service mentioned above, "channel" is treated as a synonym of content. In the channel, contents classified by time or series are also the object of DRM and the above scenarios are also applicable.

Table II.1 summarizes possible combinations between use cases and scenarios. The relationship with link-protection technology, such as DLNA, is outside of the scope of this Recommendation.

Table II.1 – Possible combinations between use cases and scenarios

Use cases		DRM scenarios			
		(1) On-line streaming	**(2) Content download**	**(3) Rental**	**(4) Subs-cription**
(1) Reception or watching IP linear content (IP linear TV)	Use case A-1: Watching broadcast content	○	N/A	○	○
	Use case A-2: Playback of recorded content, and Use case A-3: Content recording	Δ	Δ	Δ	Δ
	Use case A-4: Exchange of watching terminal	○	○	○	○
(2) Reception or watching IP VoD content (IP VoD)	Use case A-5: Watching streaming content	○	○	○	○
	Use case A-6: Download and playback, and Use case A-7: Download	○	○	○	○
(3) Content transfer between terminal devices	Use case B-1: Streaming	○	○	○	○
	Use case B-2: Remote streaming	○	○	○	○
	Use case B-3: Copy	○	○	○	○
	Use case B-4: Move	○	○	○	○
NOTE – ○: Applicable, Δ: Not common but applicable, N/A: Not applicable					

Appendix III

Multi-DRM service types

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

Multi-DRM is a system taht can select suitable DRM services from two or more DRM(s) based on the special feature of a service, the load of a system, a network situation, etc. Taking into account the currently deployed relevant services, we can categorize the multi-DRM services into three types. Appendix III describes these three types of multi-DRM. When a cable operator selects one of these three types the requirement in the selected type becomes mandatory. A multi-DRM system is shown in Figure III.1.

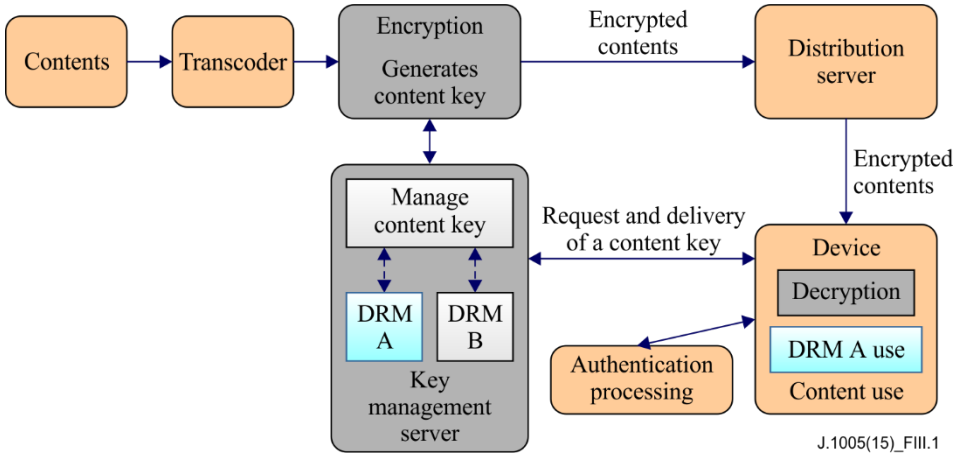


Figure III.1 – A multi-DRM system

III.1 Multi-DRM type I: Plug-in type

This multi-DRM type is the same as the Google DRM plug-in type. Smart mobile device manufacturers have to embed multiple DRM clients into it before release to the market. The advantage of this type is that it is easy to run multiple DRM services once the subscriber's devices are equipped with the DRMs that the cable service operator wants to provide. However, if a subscriber's device is not equipped with the DRM that the cable service operator wants to run, it is impossible to provide the multi-DRM service. A multi-DRM plug-in type scheme is shown in Figure III.2.

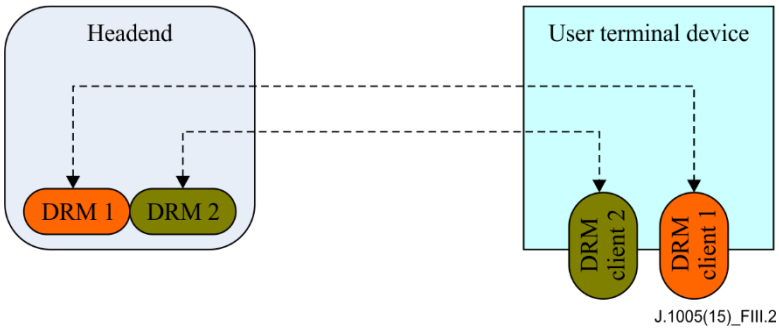


Figure III.2 – DRM plug-in type scheme

III.2 Multi-DRM type II: Common communication interface type

The ultraviolet common file format scheme can be considered as a multi-DRM type system. This system uses server-based DRM interoperability technology. A DRM server and a DRM client communicate via the standardized common communication interface. Contents are also delivered

with the common file format. The licenced application in a user terminal device has a function of interpreting the standardized communications.

The advantage of this technology is that cable service operators can run any DRM freely if the DRMs are guaranteed to be in accordance with the common communication interface. However, it is not easy to ensure that all participants such as content providers, streaming providers, cable service operators, retailers and client implementers follow the standardized common communication interface scheme. A common communication interface type scheme is shown in Figure III.3.

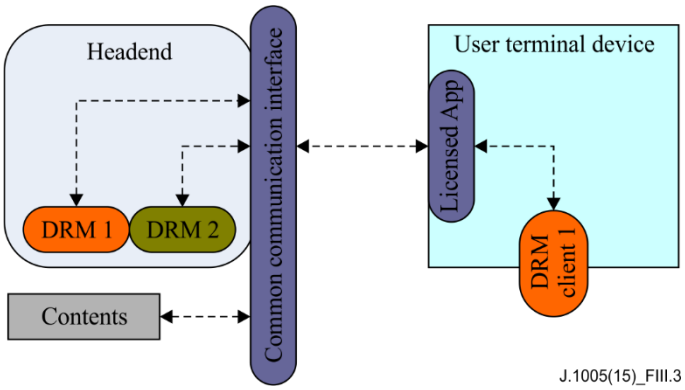


Figure III.3 – Common communication interface type multi-DRM

III.3 Multi-DRM type III: Download type

The final type of Multi-DRM is a downloadable DRM scheme. This concept is very similar to the renewable or downloadable conditional access system. In this type, cable service operators download DRM clients that they want to operate in the subscriber's device. The most important issue in this type is that the downloaded DRM client must be securely protected while it is delivered through the on-line network.

The advantage of this type of DRM scheme is that the number of participants in this scheme is much fewer than in the common communication interface scheme. The necessary participants are only cable service operators and client implementers. However, it requires extra costs for setting up the download system for cable service operators as well as the standardized interface between the download servers and download applications in user terminal devices. A download type multi-DRM scheme is shown in Figure III.4.

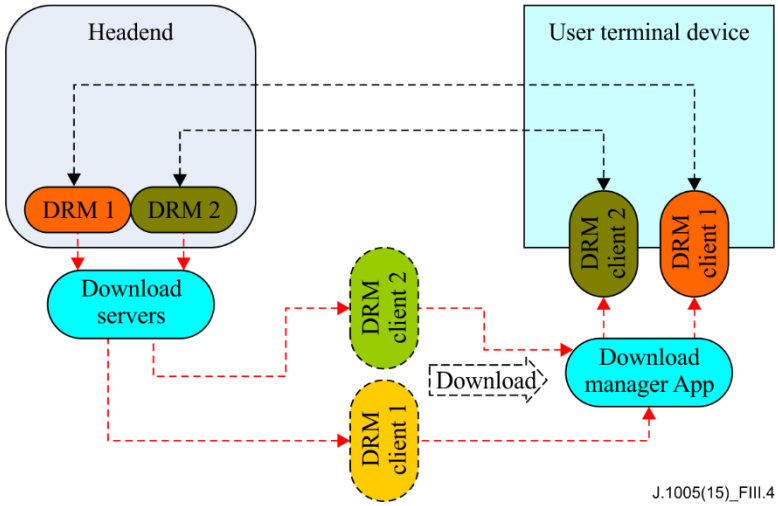


Figure III.4 – Download type multi-DRM scheme

Bibliography

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

[b-ITU-T J.205] Recommendation ITU-T J.205 (2012), *Requirements for an application control framework using integrated broadcast and broadband digital television*.

[b-ITU-T J.260] Recommendation ITU-T J.260 (2005), *Requirements for preferential telecommunications over IPCablecom networks*.

[b-ITU-T J.296] Recommendation ITU-T J.296 (2012), *Specifications for a hybrid cable set-top box*.

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

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

[b-ITU-T M.1400] Recommendation ITU-T M.1400 (2015), *Designations for interconnections among operator's networks*.

[b-ITU-T M.3320] Recommendation ITU-T M.3320 (1997), *Management requirements framework for the TMN X-Interface*.

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.1191] Recommendation ITU-T X.1191 (2009), *Functional requirements and architecture for IPTV security aspects*.

[b-ITU-T X.1193] Recommendation ITU-T X.1193 (2011), *Key management framework for secure internet protocol television (IPTV) services*.

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions*.

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

[b-ITU-T Y.2252] Recommendation ITU-T Y.2252 (2012), *Identification and configuration of resources for multi-connection*.

[b-ITU-T Y.2253] Recommendation ITU-T Y.2253 (2014), *Capabilities of multi-connection to support streaming services*.

[b-DTCP] *DTCP Volume 1 Supplement E Mapping DTCP to IP* (Informational Version) Revision 1.4 (2011).

[b-DTCPS] *Digital Transmission Content Protection Specification Volume 1* (Informational Version) Revision 1.7 2011.
http://www.dtcp.com/documents/dtcp/info-20111214-dtcp-v1-rev-1-p-7.pdf

[b-IPTVFJ] IPTVFJ STD-0004 (2010), *IP Broadcasting Specifications Version 1.2*.

[b-MRLNAF] *Marlin Adaptive Streaming Specification – Full Profile, V1.0*.
http://www.marlin-community.com/develop/downloads/specifications/

[b-MRLNAS] *Marlin Adaptive Streaming Specification – Simple Profile, V1.0.*
http://www.marlin-community.com/develop/downloads/specifications/

[b-MRLNBBTS] *Marlin Broadband Transport Stream Specification.*
http://www.marlin-community.com/develop/downloads/specifications/

[b-MRLNFF] *Marlin File Formats Specification.* http://www.marlin-community.com/develop/downloads/specifications/

[b-MRLNIPTVES] *Marlin IPTV End-point Service Specification.* http://www.marlin-community.com/develop/downloads/specifications/

[b-OMA-RD-DRM] OMA-RD-DRM-V2_0-20110419-C (2011), *OMA DRM Requirements*.

[b-OMA-TS-DRM] OMA-TS-DRM-DRM-V2_2-20110419-C (2011), *DRM Specification*.

[b-PIFF] Microsoft *Protected Interoperable File Format*. http://www.iis.net/learn/media/smooth-streaming/protected-interoperable-file-format

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

[b-PRFORMAT] *Microsoft PlayReady Format Specification*. Available under NDA and/or a special contract.

[b-PRHEADER] Microsoft *PlayReady Header Object*. http://www.microsoft.com/playready/documents/

[b-PRM2TS] Microsoft *Applying PlayReady encryption to MPEG-2 TS.* Available under NDA and/or a special contract.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
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	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
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 and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2015