IEC 62698

Edition 1.0 2013-03

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Multimedia home server systems – Rights information interoperability for IPTV

Systèmes de serveur domestique multimédia – Interopérabilité d'information des droits pour TVIP

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

Useful links:

IEC publications search - www.iec.ch/searchpub

The advanced search enables you to find IEC publications by a variety of criteria (reference number, text, technical committee,…).
It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available on-line and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Liens utiles:

Recherche de publications CEI - www.iec.ch/searchpub

La recherche avancée vous permet de trouver des publications CEI en utilisant différents critères (numéro de référence, texte, comité d'études,…).
Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

Just Published CEI - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications de la CEI. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (VEI) en ligne.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.

IEC 62698

Edition 1.0 2013-03

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Multimedia home server systems – Rights information interoperability for IPTV

Systèmes de serveur domestique multimédia – Interopérabilité d'information des droits pour TVIP

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX XB

ICS 33.160.60; 35.240.99

ISBN 978-2-83220-684-3

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

MULTIMEDIA HOME SERVER SYSTEMS – RIGHTS INFORMATION INTEROPERABILITY FOR IPTV

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62698 has been prepared by technical area 8: Multimedia home server systems, of IEC technical committee 100: Audio, video and multimedia systems and equipment.

Parts of the text of this standard have been developed in collaboration with ITU-T/Study Group 16: Multimedia application platforms and end systems for IPTV.

NOTE The ITU-T Recommendation, which is the parallel text of this standard, is ITU-T Recommendation H.751 "Metadata for rights information interoperability in IPTV services" and is under revision/approval. See ITU website for more details.

The text of this standard is based on the following documents:

CDV	Report on voting
100/1947/CDV	100/1998/RVC

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

At present, there are no mechanisms or rules for flexible digital distribution that allow the easy exchange of content based on individual commitments between content creators and consumers. This is because a technological and social environment where there is a sense of trust between copyright holders and consumers who feel safe about information distribution is not always perfectly provided.

To provide content creators and consumers with this type of content usage environment, to give them more opportunities for all kinds of digital content regardless of the support they use to store it, interoperability is required that will enable the IPTV systems and equipment that make up the envisioned value chain to communicate and work with each other across different systems which manage content distribution.

Rights Information Interoperability (RII) solves these issues by helping to provide content rights holders and consumers with common semantics and core elements that extend across different systems which manage content distribution.

MULTIMEDIA HOME SERVER SYSTEMS – RIGHTS INFORMATION INTEROPERABILITY FOR IPTV

1 Scope

This International Standard defines the common semantics and core elements on rights information interoperability for IPTV systems/equipment that is subject to multimedia content to be used across different platforms legally.

The rights information includes rights and security related metadata that is described in ITU-T Recommendation H.750.

Rights related information, such as content ID, permission issuer ID and permission receiver ID, which is used to bridge between rights related metadata, is considered in this standard. On the other hand, rights management and content protection technology are beyond the scope of this standard.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 62227:2008, *Multimedia home server systems – Digital rights permission code*

IEC/TR 62636:2009, *Multimedia home server systems – Implementation of digital rights permission code*

ISO 3166-1, *Codes for the representation of names of countries and their subdivisions – Part 1: Country codes*

ITU-T Recommendation H.750:2009, *High-level specification of metadata for IPTV services*

ITU-T Recommendation X.509, *Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks*

3 Abbreviations and acronyms

For the purposes of this document, the following abbreviations and acronyms apply.

AAC	Advanced Audio Coding
AACS	Advanced Access Content System
CD	Compact Disc
CGMS	Copy Generation Management System
CM	Commercial Message
CPRM	Content Protection for Recordable Media
DCF	DRM Content Format
DRM	Digital Rights Management

DRPC	Digital Rights Permission Code
DSA	Digital Signature Algorithm
DTCP	Digital Transmission Content Protection
DVD	Digital Versatile Disk
EC-DSA	Elliptic Curve Digital Signature Algorithm
GC	Group Content
GIF	Graphic Interchange Format
HD	High Definition
HDCP	High-bandwidth Digital Content Protection
HDD	Hard Disk Drive
ID	Identifier
IPTV	Internet Profile TeleVision
JPEG	Joint Photographic Experts Group
MP3	MPEG Audio Layer-3
MPEG	Moving Picture Experts Group
MTMO	Marlin Trust Management Organization
OMA	Open Mobile Alliance
PCM	Pulse Code Modulation
PNG	Portable Network Graphics
RII	Rights Information Interoperability
RSA	Rivest Shamir Adleman
SAFIA	Security Architecture For Intelligent Attachment
SHA	Secure Hash Algorithm
VCPS	Video Content Protection System
VOD	Video On Demand
WIPO	World Intellectual Property Organization

4 Systems: the RII environment

4.1 General

This standard gives the high-level standard of the metadata for rights information interoperability, including representation of the minimum required elements.

The RII metadata provides descriptive and contextual classification for representing rights information using the permission framework.

RII is concerned with finding the greatest common denominators in rights expressions that include the minimum required components when trying to implement the mutual use of rights information.

It is about conveying rights information in units of groups of context expressions called permissions.

Here we consider the constituent components of permissions. Permissions can encode “what from whom to whom under what conditions” using context expressions. When permissions are sent to a terminal, the minimum required components are the subject information in the permissions that corresponds to the “what from whom to whom” part, and the content usage information that corresponds to the “under what conditions” part.

4.2 Permission subjects

One permission subject is the issuer information that expresses the “from whom” part of the permissions. This information is held by the service provider, and in RII, its minimum required component is the rights holder ID.

Only the issuer ID is included because in RII, it is sufficient if the service provider and the terminal can identify who is granting the permissions. It is not necessary to send all of the issuer information from the server to the terminal. Therefore, the rights holder ID corresponds to the Issuer ID in RII context expressions. The service provider receives the digital rights permission code from the terminal and loads the rights holder ID included in the Issuer ID to identify the rights holder who granted the permissions.

Another permission subject is receiver information that expresses the “to whom” part of the permissions. In RII, that minimum required component is the User ID/Device ID.

Only the receiver ID is included because in RII, it is sufficient if the service provider and the terminal can identify to whom the permissions are being granted. Therefore, the User ID/Device ID corresponds to the Receiver ID in RII context expressions. The terminal receives the digital rights permission code from the service provider and determines whether or not the User ID/Device ID included in the Receiver ID corresponds to the local terminal, or the service provider receives the digital rights permission code from the terminal and loads the User ID/Device ID included in the Receiver ID to identify the user to whom permissions were granted.

Another permission subject is information about the content for which permissions are being granted, which is expressed in the “what” part. In RII, that minimum required component is the Content ID.

Only the Content ID is included in RII because it is sufficient for the service provider and the terminal to be able to identify the content for which permissions are being granted. The terminal receives the digital rights permission code from the service provider and determines that the content that corresponds to the Content ID is being granted.

4.3 Permission limit components

One permission limit component is the type of the permissions (hereinafter referred to as “the permission classification component”), which expresses stipulations about what is being granted. These permissions are agreed upon between the issuer and the receiver. This is information that the receiver needs to be able to check offline. In RII, those minimum required components are the following: a type that indicates whether the permission content being granted is public or not (hereinafter referred to as “the disclosure class”), a type that indicates the purpose of use being granted (hereinafter referred to as the “purpose class”), a type that indicates the billing format being granted (hereinafter referred to as the “charge model class”), a type that indicates the request format being granted (hereinafter referred to as the “request class”), a type that indicates the sponsor format being granted (hereinafter referred to as the “sponsor class”, a type that indicates the usage format being granted (hereinafter referred to as the “usage class”), and a type that indicates the territory being granted, (hereinafter referred to as the "territory class”). These permission limit components are included in RII because it is necessary to be able to see that information even in an offline environment that is not connected to a network. This is so that the terminal can determine what type of permissions are being granted between the service provider and the terminal.

Another permission limit component contains limiting conditions that are in addition to the restrictions in the items granted above. These are mainly items of information that limit the type of permissions stipulated by the usage class. In RII, those minimum required components are the permission usage format and its limiting conditions (hereinafter referred to as "normal usage limits”), content usage limits for compliant terminals (hereinafter referred to as the “permission management system limits”), and the limits on output of the content to non-compliant terminals or media (hereinafter referred to as the “simultaneous output limits”).

These permission limit components are included in RII, because it is necessary for the rights they correspond to, to be seen on the terminal even in an offline environment that is not connected to a network. This is so that the terminal can determine under what conditions the types of permissions are limited between the service provider and the terminal.

RII does not provide a method of encoding context expressions for permissions. The encoding method is already standardized using existing standard technology. Instead, Clause B.2 shows the example of adding context expressions expressed using natural language in IEC 62227 (DRPC).

RII is a set of items to be considered when each content is distributed and permission for such distribution is generated.

Therefore RII is not defined from a technical perspective, but rather on the basis of permission information that rights holders actually employ in the field. RII itself does not have the ability to regulate content usage behaviour.

Restricting the use of content to terms specified in the permission is an administrative issue or a DRM systems issue. RII does not have exclusive policy. Implementers of each DRM or content distribution systems can choose their own subset and usage scheme of RII, based on their necessity and resource. They can even limit the application to a simple displaying of permission and not use their rights management.

5 Permission subject identifiers

5.1 Permission subject identifiers

Permission subject identifiers is comprised of three identifiers: Content identifier assigned to the subject content, Issuer identifier and Receiver identifier respectively, assigned to each permission issuer and receiver.

5.2 Content identifier

Content identifier is information to uniquely identify the content. It is required to be assigned to each content that is subject to permission. IEC 62227:2008, 5.5.4, specifies permission subject content identifiers.

5.3 Issuer identifier

Issuer identifier is information to uniquely identify the permission issuer. Issuer identifier may be used not only to identify a rights holder, a service provider and a home server, but also for consumption tracking, rights report and content management. IEC 62227:2008, 5.5.5, specifies permission subject issuer identifiers.

5.4 Receiver identifier

Receiver identifier is information to uniquely identify the permission receiver. Receiver identifier may be used to identify an end-user, a device and a set of end-users. IEC 62227:2008,5.5.6, specifies permission subject receiver identifiers.

6 Permission classification

6.1 Permission classification

Permission classification indicates the class of the permission. It should be described according to the conditions indicated in the permission agreement.

6.2 Disclosure class

Disclosure class includes classification indicating whether a given permission is a closed permission for a specified player or an open permission for an unspecified group of players. The closed permission information can be accessed by the permission issuer and receiver. Possible values are “open permission”, “closed permission” and “other”. Open permission is the permission that is received according to previously arranged default conditions. Closed permission is the permission that is received through a separate, individually negotiated contract.

IEC 62227:2008, 5.6.4, specifies a permission classification for signalling and carrying disclosure information. Clause B.2 of IEC/TR 62636:2009, provides use-case scenarios to implement the disclosure class.

6.3 Purpose class

Purpose class includes classification indicating the purpose of content usage, such as commercial, public, education, not-for-profit and promotion. To ensure the consumption of content under the condition could be subject to domain management. Possible values are “commercial”, “public”, “non-profit”, “promotion”, “education” and “other”.

Commercial permission is the permission for a business use. Public permission is the permission for a public use. Non-profit permission is the permission for a public use. Promotion permission is the permission for a promotion use. Education permission is the permission for an education use.

IEC 62227:2008, 5.6.5, specifies a permission classification for signalling and carrying usage purpose information. Clause B.2 of IEC/TR 62636:2009, provides use-case scenarios to implement the usage purpose class.

6.4 Charge model class

Charge model class includes classification including the charge method such as free-of-charge and for-charge. The charge model class might include “pay-per-view” (charged per viewing), and “subscription” (fixed periodic charge). Both of these conditions should not be used at the same time, but rather if one is selected the other is not used. Possible values are “free of charge”, “pay per use”, “subscription”, “coupon”.

IEC 62227:2008, 5.6.6, specifies a permission classification for signalling and carrying charge model information. Clause B.2 of IEC/TR 62636:2009, provides use-case scenarios to implement the charge model class.

6.5 Sponsor class

Sponsor class includes classification indicating the sponsor type such as advertising model, premium model, coupon model and consumption information disclosure model.

Advertising model describes the condition of viewing ads in the content consumption. Premium model, coupon model and consumption information disclosure model describe the conditions for the content acquisition. In the premium model there can be a specific advertiser to sponsor specific content. In the coupon model there can be multiple advertisers to sponsor the content. In disclosure model the content can be exchanged for end-user consumption information. The control of trick play and the function of point exchange are required to be implemented for these models. Possible values are “No sponsor”, “Advertisement model without force viewing”, “Advertisement model with force viewing”, “Advertisement model with pre/post viewing”, “Advertisement model with alternative viewing”, “Advertisement model with blanket viewing”, “Premium model”, “Coupon model”, “Privacy information disclosure model” and “Other”.

IEC 62227:2008, 5.6.9, specifies a permission classification for signalling and carrying sponsor information. IEC/TR 62636:2009, 5.17, and IEC/TR 62636:2009, 5.18, provide use-case scenarios to implement the sponsor class.

6.6 Territory class

Territory class includes classification indicating the territory of content consumption such as country and region. It is required to implement the technology, such as domain management, to specify the territory in which content is consumed. Possible values are region code, country code (ISO 3166-1) and Zip code.

IEC 62227:2008, 5.6.10, specifies a permission classification for signalling and carrying territory information. Clause B.2 of IEC/TR 62636:2009, provides use-case scenarios to implement the territory class.

6.7 Usage class

Usage class includes classification indicating the usage type such as transmission type, store type, reuse type, and redistribution type based on usage environment.

IEC 62227:2008, 5.6.11, specifies a permission classification for signalling and carrying usage information. Clause B.2 of IEC/TR 62636:2009, provides use-case scenarios to implement the usage class.

Elements required in usage class are listed below.

- Transmission type expresses an distribution form of content into target domains and comformance devices. For example, if the value is "download", the content can be downloaded into conformance devices. Possible values are "broadcast", "streaming", "download" and "physical media".
  - IEC 62227:2008, 5.6.11.2, usage_type, specifies a permission classification for signalling and carrying usage class information.
- Store type expresses an accumulation form of content in target domains and conformance devices. For example, if the value is "fixation", the content can be stored in conformance devices. Possible values are "fixation" and "non-fixation".
  - IEC 62227:2008, 5.6.11.2, usage_type, specifies a permission classification for signalling and carrying usage class information.
- Reuse type expresses the secondary usage type of content in target domains and compliance devices. Possible values are enable or disable of secondary usage, move, copy, export, share, edit, modify and super distribution.
  - IEC 62227:2008, 5.6.11.4, move_flag, 5.6.11.5, copy_flag, 5.6.11.6, export_flag, 5.6.11.7, share_flag, 5.6.11.8, edit_flag, 5.6.11.9, modify_flag, 5.6.11.10, super_distribution_flag, specifies a permission classification for signalling and carrying usage class information.
- Redistribution type expresses the forwarding type of content from target domains and compliance devices (e.g. enable or disable).
  - IEC 62227:2008, 5.6.11.3, redistribution_type, specifies a permission classification for signalling and carrying usage class information.

6.8 Compilation class

Compilation class includes classification indicating content depending on whether or not the permission issuer is allowed to combine and sell multiple pieces of content. It is required to ensure consistency in playback with playlist. Possible values are true if play-list is enabled, false, if play-list is disabled.

IEC 62227:2008, 5.7.3.2.6, playlist_parameter, specifies a permission condition for signalling and carrying compilation information.

7 Permission limit components

7.1 Permission limit components

Classification limit components include information indicating the restriction of the permission conditions that is described in the permission classification. It can be described for restricting the conditions indicated in the permission agreement.

7.2 General usage condition

7.2.1 General

General usage condition is an element comprising a usage form and its limit conditions under which the content can be permitted to be used in target domains and compliant devices. It includes information restricting the usage condition for content consumption such as playback usage, print usage and execute usage.

Playback usage is an element of the usage form that the content can be rendered temporarily under keeping perceptible. Playback usage condition expresses the limit that the content can be permitted to playback in target domains and compliance devices.

IEC 62227:2008, 5.7.3.2, specifies a permission constraint for signalling and carrying playback condition.

Print usage is an element of the usage form that the content can be rendered permanently on the physically fixed object. Print usage condition expresses the limit that the content can be permitted to print in target domains and compliance devices.

IEC 62227:2008, 5.7.3.3, specifies a permission constraint for signalling and carrying print condition.

Execution usage is an element of the usage form that the content can be rendered temporarily with the calculation process. Execution usage condition expresses the limit that the content can be permitted to execute in target domains and compliance devices.

IEC 62227:2008, 5.7.3.4, specifies a permission constraint for signalling and carrying execution condition.

7.2.2 Quality limits

Quality limits includes information indicating the quality of distributed content. Permission issuers typically represent it as qualitative levels such as LEVEL1 (high quality), LEVEL2 (standard quality), LEVEL3 (low quality) and LEVEL4 (other). For example, if the value is "LEVEL1", the content can be permitted to use (play, print or execute) with the best quality. Possible values are "LEVEL1", "LEVEL2", "LEVEL3" and "LEVEL4".

IEC 62227:2008, 5.7.3.2.4, quality_parameter, specifies a quality condition for playback usage. IEC 62227:2008, 5.7.3.3.4, quality_parameter, specifies a quality condition for print usage. IEC 62227:2008, 5.7.3.4.4, service_level_parameter, specifies a quality condition for execution usage.

7.2.3 Lifetime limits

Lifetime limits includes information indicating the lifetime of distributed content. Permission issuers typically specify time period, day count and date period.

Elements required in lifetime limits are listed below.

NOTE Unless otherwise specified, the subclause references within the same dashed paragraph all refer to IEC 62227:2008, as indicated at the beginning of each dashed item.

- Time period expresses the number of hours during which the content is permitted to be used (play, print or execute) in target domains and compliance devices. For example, if the value is twenty-four, the content can be used for 24 h after its reception in compliance devices. Possible values are natural numbers and the unit is hour (e.g., 24 h, 48 h).

  - IEC 62227:2008, 5.7.3.2.13, time_period_parameter, can describe the element with the same meaning on playback usage. 5.7.3.3.11 time_period_parameter can describe the element with the same meaning on print usage. 5.7.3.4.12 time_period_parameter can describe the element with the same meaning on playback usage.

- Day count expresses the number of dates during which the content is permitted to be used (play, print or execute) in target domains and compliance devices. For example, if the value is seven, the content can be used for 7 days after its reception in compliance devices. Possible values are natural values and the unit is day (e.g. 1 day, 7 days).

  - IEC 62227:2008, 5.7.3.2.14, day_count_parameter, can describe the element with the same meaning on playback usage. 5.7.3.3.12 day_count_parameter can describe the element with the same meaning on print usage. 5.7.3.4.13 day_count_control_parameter can describe the element with the same meaning on excution usage.

- Date period expresses the term limit until which the content is permitted to be used (play, print or execute) in target domain and compliant devices. For example, if the value is from 2010/11/01 to 2010/11/30, the content can be used from 1st November 2010 to 30th November 2010. Possible values are dates (start date and end date) and the unit is date (e.g., period from start date to end date).

  - IEC 62227:2008, 5.7.3.2.15, start_date_parameter, can describe the element with the same meaning as for playback usage. 5.7.3.3.13, start_date_parameter, can describe the element with the same meaning as for on print usage. 5.7.3.4.14, start_date_parameter, can describe the element with the same meaning as for on playback usage.

  - IEC 62227:2008, 5.7.3.2.16, end_date_parameter, can describe the element with the same meaning as for on playback usage. 5.7.3.3.14, end_date_parameter, can describe the element with the same meaning as for on print usage. 5.7.3.4.15, end_date_parameter, can describe the element with the same meaning as for on playback usage.

7.2.4 Permission management system limits

Permission management system limits includes information indicating which content management method should be used for the permission management such as digital watermark, rights report and digital copy protection.

For example, if the value is "digital copy protection", a compliance device, on its usage time (playing, printing or executing), is required to protect the content using a DRM. Possible values are "digital copy protection", "digital watermark" and "rights report". It may take a value of –1 for the meaning "other".

IEC 62227:2008, 5.7.3.2.5, permission_management_model_parameter, can describe the element with the same meaning as for on playback usage. IEC 62227:2008, 5.7.3.3.5, permission_management_model_parameter, can describe the element with the same meaning on print usage and IEC 62227:2008, 5.7.3.4.5, permission_management_model_parameter, can describe the element with the same meaning on execute usage.

7.2.5 Simultaneous output limits

Simultaneous output limits includes information indicating the permitted number of simultaneous output for each content consumption. For example, if the value is two, a compliance device (playing, printing or executing) can be permitted during its usage time to export the content toward two displays simultaneously. Possible values are non-negative integers.

It may take a value of –1 for the meaning "other".

IEC 62227:2008, 5.7.3.2.17, simultaneous_output_parameter, can describe the element with the same meaning on playback usage.

7.3 Extended usage condition

Extended usage condition includes information indicating the extended condition to the regular usage condition. This condition is under further study.

8 Data management condition

Data management condition includes information indicating the condition that is subject to saving the original content or re-issuing permission. The device shall be able to control a variety of services and content for the end-user consumption under specific conditions described for data management.

Permission issuers typically specify encryption flag, copy count, transcode type, expiration date, and other usage conditions concerning data management.

Elements required in the data management condition are listed below.

- Encryption flag indicates whether the content needs to be encrypted or not. Possible values are true if encryption is required, false, if encryption is not required.
  - IEC 62227:2008, 5.9.3.3, encryption_flag, can describe the element with the same meaning.
- Copy count expresses the number of times that the content can be permitted to copy in target domains and compliance devices. If the value is 1, there can be two copies including the original one. Possible values are non-negative integers. It may take a value of –1 for the meaning "other".
  - IEC 62227:2008, 5.9.3.4, copy count, can describe the element with the same meaning.
- Move count expresses the number of times that the content can be permitted to move in target domains and compliance devices. MOVE usually means a combination of copying the content and deleting the original one. Possible values are non-negative integers. It may take a value of –1 for the meaning "other".
  - IEC 62227:2008, 5.9.3.5, move count, can describe the element with the same meaning.
- Transcode type expresses the type of transcoding in which the content can be permitted to store in target domain and compliant devices. Possible values are MPEG-1, MPEG-2, H.264, JPEG, GIF, PNG, Linear PCM, AAC and MP3.
  - IEC 62227:2008, 5.9.3.6, transcode type, can describe the element with the same meaning.
- Maximum transcode rate expresses the highest bit rate that can be permitted to transcode the content for storing in a target domain and compliant devices. Possible values are non-negative real numbers and the unit is kbit/s.
  - IEC 62227:2008, 5.9.3.7, maximum transcode rate, can describe the element with the same meaning.
- Minimum transcode rate expresses the lowest bit rate that can be permitted to transcode the content for storing in a target domain and compliant devices. Possible values are non-negative real numbers and the unit is kbit/s.
  - IEC 62227:2008, 5.9.3.8, minimum transcode rate, can describe the element with the same meaning.
- Expiration date expresses the term limit that can be permitted to store content in a target domain and compliant devices. Possible values are dates; the unit is date.
  - IEC 62227:2008, 5.9.3.9, expiration date, can describe the element with the same meaning.

- Sublicense count expresses the number of times that can be permitted to issue sub-licenses in a target domain and compliant devices. Possible values are non-negative integers.
  - IEC 62227:2008, 5.9.3.10, sublicense count, can describe the element with the same meaning.
- Time-line edit flag indicates whether editing the content with respect to a time-line and saving the resulting content is permitted or not. Possible values are true, if time-line edit is enabled, false, if time-line edit is disabled.
  - IEC 62227:2008, 5.9.3.11, time-line edit, can describe the element with the same meaning.

9 Data export condition

Data export condition includes information indicating the condition that is subject to exporting the original content to non-compliant objects. The device shall be able to control a variety of services and content for the end-user consumption under specific conditions described for data management.

Permission issuers typically specify storage media, encoding type, control type, time period, day count, date period, and other usage condition about exporting the content.

Elements required in data export condition are listed below.

- Encryption flag indicates whether the content needs to be encrypted or not. Possible values are true, if encryption is required, false, if encryption is not required.
  - IEC 62227:2008, 5.9.3.3, encryption_flag, can describe the element with the same meaning.
- Copy count expresses the number of times that the content can be permitted to copy into target domains and compliance devices. If the value is 1, there can be two copies including the original one. Possible values are non-negative integers. It may take a value of –1 for the meaning "other".
  - IEC 62227:2008, 5.9.3.4, copy count, can describe the element with the same meaning.
- Move count expresses the number of times that the content can be permitted to move in target domains and compliance devices. MOVE usually means a combination of copying the content and deleting the original one. Possible values are non-negative integers. It may take a value of –1 for the meaning "other".
  - IEC 62227:2008, 5.9.3.5, move count, can describe the element with the same meaning.
- Transcode type expresses the type of transcoding in which the content can be permitted to store in a target domain and compliant devices. Possible values are MPEG-1, MPEG-2, H.264, JPEG, GIF, PNG, Linear PCM, AAC and MP3.
  - IEC 62227:2008, 5.9.3.6, transcode type, can describe the element with the same meaning.
- Maximum transcode rate expresses the highest bit rate that can be permitted to transcode the content for storing in a target domain and compliant devices. Possible values are non-negative real numbers and the unit is kbit/s.
  - IEC 62227:2008, 5.9.3.7, maximum transcode, rate can describe the element with the same meaning.
- Minimum transcode rate expresses the lowest bit rate that can be permitted to transcode the content for storing in a target domain and compliant devices. Possible values are non-negative real numbers and the unit is kbit/s.
  - IEC 62227:2008, 5.9.3.8, minimum transcode rate, can describe the element with the same meaning.

- Expiration date expresses the limit term that can be permitted to store content in a target domain and compliant devices. Possible values are dates; the unit is date.
  - IEC 62227:2008, 5.9.3.9, expiration date, can describe the element with the same meaning.
- Sublicense count expresses the number of times that can be permitted to issue sub-licenses in a target domain and compliant devices. Possible values are non-negative integers.
  - IEC 62227:2008, 5.9.3.10, sublicense count, can describe the element with the same meaning.
- Time-line edit flag indicates whether editing the content with respect to a time-line and saving the resulting content is permitted or not. Possible values are true, if time-line edit is enabled, false, if time-line edit is disabled.
  - IEC 62227:2008, 5.9.3.11, time-line edit, can describe the element with the same meaning.

Annex A
(informative)

SECURITY related issues

A.1 Tamper detection

A.1.1 General

Distribution format data representing digital rights permissions have to be detected whether or not they have been falsified by any one, therefore, these distribution format data have to involve a digital signature.

As applicable examples of digital signature algorithms, EC-DSA with SHA and RSA/DSA with SHA are given. The concrete standard of signature should depend on each service system.

The rough composition of distribution format data is depicted in the Table A.1.

Table A.1 – Rough composition of distribution format data

Description	Digital rights permissions data	Digital signature	Certificate or PkiPath
The following information is involved. – Number of hierarchy of PkiPath – Signature algorithm – Key length – Encryption parameters, etc.	Data representing digital rights permissions	Digital signature of digital rights permissions data which is generated through algorithm and standard specified in the description.	Certificate or chain of certificates which authenticate the digital signature.

A.1.2 Authentication

The issuer of digital rights permissions data generates public/private key pairs, and he obtains a certificate of the public key from the appropriate certificate authority.

The issuer generates the digital signature of the digital rights permissions data by using the above private key, and creates the distribution format data by adding the signature and the certificate to the digital rights permissions data.

Standards of certificates for digital signature of digital rights permissions data shall comply with ITU-T Recommendation X.509.

If the certificate contains a certificate chain, PkiPath as defined in ITU-T Recommendation X.509 is used.

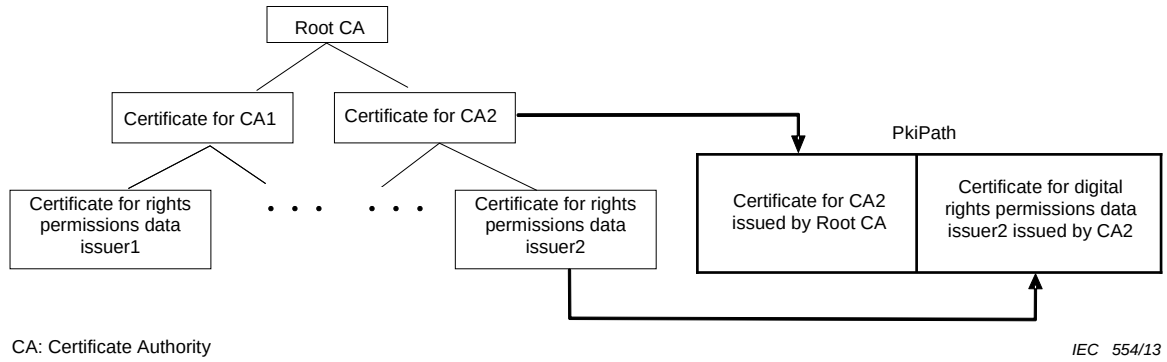


Figure A.1 – Example of PkiPath

Figure A.1 shows an example a of PkiPath. The number of the hierarchy of PkiPath depends on the operational standard of each service system and this information shall be specified in the description area of the distribution format data.

A.1.3 Signature

The following algorithms are applicable to signature generation and verification.

EC-DSA with SHA

RSA/DSA with SHA

Key lengths and encryption parameters of EC-DSA, RSA/DSA and SHA depend on each service system standard, and this type of information has to be specified in the description area of the distribution format data.

A.2 Secret keeping

It is service system dependent whether or not distribution format data representing digital rights permissions have to be kept secret.

In the case that the digital rights permissions data have to be kept secret, the protection standard depends on each service system standard too, and is not described in this standard.

Annex B
(informative)

Syntax (encoding)

B.1 General

Considering the implementation for IPTV services, these metadata would need to be encoded by a common standardized format. There is a requirement that a representation scheme of rights related metadata should be based on a common syntax for its interoperability.

This clause shows the typical 23 use-cases scenarios described in IEC/TR 62636. In Clasue B.2, these scenarios divide into permission conditions tables using IEC 62227 syntaxes.

- Content purchase
- Rental with time or playback limit
- Subscription
- Direct retrieval of content from a device: Scenario 1
- Direct retrieval of content from a device: Scenario 2
- Unlimited play
- Preview
- Multiple permissions for a multipart DCF
- Inheritance
- Export of OMA DRM content
- Combinations of constraint elements
- FairPlay
- CPRM
- SAFIA
- Ringtones
- Download of content free with advertising
- Streaming of content free with advertising
- Giveaways
- Coupons (discount points)
- Privacy information disclosure
- Copying 9 times with unlimited moving
- Subscription games
- Software rental

B.2 DRPC syntaxes tables of the twenty three scenarios

This clause shows DRPC syntaxe tables (see IEC 62227) of the twenty three scenarios in Clause B.1 that expand four main elements; ContentID, IssuerID, Receiver ID and Permission Conditions into the sub-elements which specify the practical value of each elements in the scenarios, see Tables B.1 to B.6.

In subscription scenario, there are three different permission codes,

a) a parent permission code which represents a permission condition of a subscription contract itself and

b) two children permission codes which represent permission conditions of music contents.

Note that Receiver ID assumes to have a fixed value “HJPC01000000001”.

Table B.1 – Permission actors and permission classifications

NO	Content ID	Scenario	Disclosure Class	Usage Purpose Class	Charge Model Class	Billing Class	Application Class	Sponsor Class	Territory Class	Usage Class	Receiver ID
1	SMJP010000000201	Content purchase	Open	Commercial	Fee-based	Individual	Individual	No Sponsor	Reserved	Download, Reuse, Move, Copy, Export	UJPI 010000000101
2	VPJP010000000202	Rental with time or playback limit	Open	Commercial	Fee-based	Individual	Individual	No Sponsor	Reserved	Download	UJPI 010000000101
3	SMJP010000000210	Subscription	Open	Commercial	Fee-based, Subscription	Individual	Individual	No Sponsor	Reserved	Download, Reuse, Copy	UJPI 010000000101
4	SMJP010000000211	Subscription child 1	Open	Commercial	Fee-based, Subscription	Individual	Individual	No Sponsor	Reserved	Download, Reuse, Copy	UJPI 010000000101
5	SMJP010000000212	Subscription child 2	Open	Commercial	Fee-based, Subscription	Individual	Individual	No Sponsor	Reserved	Download, Reuse, Copy	UJPI 010000000101
6	SMJP010000000221	Direct retrieval of content from a device: Scenario 1	Open	Commercial	Fee-based	Individual	Individual	No Sponsor	Reserved	Download	UJPD010000000101
7	VEJP010000000222	Direct retrieval of content from a device: Scenario 2	Open	Commercial	Fee-based	Individual	Individual	No Sponsor	Reserved	Streaming	UJPD010000000101
8	VPJP010000000301	Unlimited play	Open	Commercial	Fee-based	Individual	Individual	No Sponsor	Reserved	Download, Reuse, Copy	UJPI 010000000101
9	VPJP010000000302	Preview	Open	Commercial	Fee-based	Individual	Individual	No Sponsor	Reserved	Streaming	UJPI 010000000101
10	TMJP010000000303	Multiple permissions for a multipart DCF (Lyrics)	Open	Commercial	Fee-based	Individual	Individual	No Sponsor	Reserved	Download	UJPD010000000101
11	SMJP010000000303	Multiple permissions for a multipart DCF (Song)	Open	Commercial	Fee-based	Individual	Individual	No Sponsor	Reserved	Download	UJPD010000000101
12	TMJP010000000304	Inheritance	Open	Commercial	Free	Individual	Individual	No Sponsor	Reserved	Streaming	UJPD010000000101
13	VPJP010000000305	Export of OMA DRM content	Open	Commercial	Fee-based	Individual	Individual	No Sponsor	Reserved	Download, Reuse, Copy	UJPI 010000000101
14	VPJP010000000306	Combinations of constraint elements	Open	Commercial	Fee-based	Individual	Individual	No Sponsor	Reserved	Streaming	UJPI 010000000101
15	VPJP010000000501	FairPlay	Open	Commercial	Fee-based	Individual	Individual	No Sponsor	Reserved	Download	UJPD010000000101
16	VPJP010000000502	CPRM	Open	Commercial	Fee-based	Individual	Individual	No Sponsor	Reserved	Download	UJPD010000000101
17	VPJP010000000503	SAFIA	Open	Commercial	Fee-based	Individual	Individual	No Sponsor	Reserved	Streaming	UJPD010000000101
18	SMJP010000000504	Ringtones	Open	Commercial	Fee-based	Individual	Individual	No Sponsor	Reserved	Download, Reuse, Export	UJPD010000000101
19	VPJP010000000601	Download of content free with advertising	Open	Commercial	Free	Individual	Individual	No Sponsor	Reserved	Streaming	UJPD010000000101
20	VPJP010000000602	Streaming of content free with advertising	Open	Commercial	Free	Individual	Individual	No Sponsor	Reserved	Download, Reuse, Copy, Export	UJPI 010000000101
21	VPJP010000000603	Giveaways	Open	Commercial	Free	Individual	Individual	No Sponsor	Reserved	Download, Reuse, Export	UJPI 010000000101
22	VPJP010000000604	Coupons (discount points)	Open	Commercial	Free	Individual	Individual	No Sponsor	Reserved	Download, Reuse, Copy, Export	UJPI 010000000101
23	VPJP010000000605	Privacy information disclosure	Open	Commercial	Free	Individual	Individual	No Sponsor	Reserved	Download, Reuse, Copy, Export	UJPD010000000101
24	VPJP010000000701	Copying 9 times with unlimited moving	Open	Commercial	Fee-based	Individual	Individual	Time-synchronized Forced Viewing	Reserved	Download, Reuse, Copy	UJPI 010000000101
25	PGJP010000000101	Subscription games	Open	Commercial	Fee-based	Individual	Individual	Time-synchronized Forced Viewing	Reserved	Streaming	UJPI 010000000101
26	PSJP010000000101	Software rental	Open	Commercial	Fee-based	Individual	Individual	Giveaway Model	Reserved	Download, Reuse, Copy	UJPI 010000000101
						Individual	Individual	Coupon Model	Reserved	Download, Reuse, Copy	UJPI 010000000101
						Individual	Individual	Advertising Model	Reserved	Streaming	UJPI 010000000101
						Individual	Individual	No Sponsor	Reserved	Fixed Broadcast Delivery, Reuse, Move, Copy	UJPI 010000000101
						Individual	Individual	No Sponsor	Reserved	Download	UJPI 010000000101
						Individual	Individual	No Sponsor	Reserved	Download	UJPI 010000000101

Table B.2 – Playback usage conditions

		Playback Usage Condition									
NO		Quality Parameter		Playlist	Num of Playback	Num of Playback Hours	Num of Playback Days	Playback Period	Simultaneous Output	Parental Guidance	Countable Time (Seconds)
1	SMJP010000000201	LEVEL1,LEVEL2,LEVEL3,LEVEL4	DRM	Allow						General	
2	VPJP010000000202	LEVEL1,LEVEL2,LEVEL3	DRM	Forbid	240:00:00	48:0:0		2008/03/28 0:0:0-2008/03/29 11:59:59		General	30
3	SMJP010000000210	LEVEL1,LEVEL2,LEVEL3	DRM	Allow						General	
4	SMJP010000000211	LEVEL1,LEVEL2,LEVEL3	DRM	Allow						General	
5	SMJP010000000212	LEVEL1,LEVEL2,LEVEL3	DRM	Allow						General	
6	SMJP010000000221	LEVEL1,LEVEL2,LEVEL3	DRM	Allow						General	
7	VFJP010000000222	LEVEL1,LEVEL2,LEVEL3	DRM	Allow						General	
8	VPJP010000000301	LEVEL1,LEVEL2,LEVEL3,LEVEL4	DRM	Allow						General	
9	VPJP010000000302	LEVEL1,LEVEL2,LEVEL3	DRM	Allow	24:00:00					General	30
10	TMJP010000000303	LEVEL1,LEVEL2,LEVEL3,LEVEL4	DRM	Forbid	24:00:00					General	30
11	SMJP010000000303	LEVEL1,LEVEL2,LEVEL3,LEVEL4	DRM	Forbid	24:00:00					General	30
12	TMJP010000000304	LEVEL1,LEVEL2,LEVEL3,LEVEL4	DRM	Forbid	72:00:00			2008/09/01 0:0:0-2008/09/30 11:59:59		General	30
12	TMJP010000000304	LEVEL1,LEVEL2,LEVEL3	DRM	Forbid	240:00:00			2008/07/01 0:0:0-2008/08/31 11:59:59		General	30
13	VPJP010000000305	LEVEL1,LEVEL2,LEVEL3,LEVEL4	DRM	Allow						General	
14	VPJP010000000306	LEVEL1,LEVEL2,LEVEL3	DRM	Forbid	48:00:00	0:30:00		2008/05/01 0:0:0-2008/06/30 11:59:59		General	30
14	VPJP010000000306	LEVEL1,LEVEL2,LEVEL3	DRM	Forbid	240:00:00	0:00:30		2008/04/01 0:0:0-2008/06/30 11:59:59		General	30
15	VPJP010000000501	LEVEL1,LEVEL2,LEVEL3	DRM	Allow						General	
16	VPJP010000000502	LEVEL1,LEVEL2,LEVEL3	DRM	Allow						General	
17	VPJP010000000503	LEVEL1,LEVEL2,LEVEL3	DRM	Allow						General	
18	SMJP010000000504	LEVEL1,LEVEL2,LEVEL3		Allow						General	
19	VPJP010000000601	LEVEL1,LEVEL2,LEVEL3,LEVEL4	DRM	Forbid						General	
20	VPJP010000000602	LEVEL1,LEVEL2,LEVEL3	DRM	Forbid						General	
21	VPJP010000000603	LEVEL1,LEVEL2,LEVEL3	DRM	Allow						General	
22	VPJP010000000604	LEVEL1,LEVEL2,LEVEL3	DRM	Allow						General	
23	VPJP010000000605	LEVEL1,LEVEL2,LEVEL3	DRM	Allow						General	
24	VPJP010000000701	LEVEL1,LEVEL2,LEVEL3	DRM	Allow					1	General	

Table B.3 – Printout usage conditions

		Print usage condition						
	Content ID		Permission Management Type	Num of Printouts	Num of Printout Hours	Num of Printout Days	Printout Period	Parental Guidance
10	TMJP010000000303	LEVEL1,LEVEL2,LEVEL3	DRM	1				General
12	TMJP010000000304	LEVEL1,LEVEL2,LEVEL3,LEVEL4	DRM	10			2008/09/01 0:0:0-2008/09/30 11:59:59	General
12	TMJP010000000304	LEVEL1,LEVEL2,LEVEL3,LEVEL4	DRM	3			2008/09/01 0:0:0-2008/09/30 11:59:59	General

Table B.4 – Execution usage conditions

		Execute usage contition							
	Content ID		Permission Management Type	Num of Executions	Num of Execution Hours	Num of Execution Days	Execution Period	Parental Guidance	Countable Time (Seconds)
25	PGJP010000000101	LEVEL1,LEVEL2,LEVEL3	DRM				2008/06/20 0:0:0-2008/06/27 23:59:59	General	
26	PSJP010000000101	LEVEL1,LEVEL2,LEVEL3	DRM				2008/06/20 0:0:0-2008/06/30 23:59:59	General	

Table B.5 – Data management conditions

Data management condition											
NO	Content ID	Target ID	Encryption Flag	Copy Count	Move Count	Transcode Type	Maximum Transcode Rate	Minimum Transcode Rate	Expiration Date	Sublicense Count	Timeline Edit
1	SMJP010000000201	UJPD010000000201	TRUE	ff	0				2008/09/26 0:0:0	0	Forbid
2	VPJP010000000202	UJPD010000000101	TRUE	0	1				2008/12/31 0:0:0	0	Forbid
3	SMJP010000000210	UJPD010000000201	TRUE	0	0				2008/07/31 0:0:0	0	Forbid
6	SMJP010000000221	UJPD010000000101	TRUE	0	0				9999/12/31 0:0:0	0	Forbid
8	VPJP010000000301		TRUE	ff	0				9999/12/31 0:0:0	0	Allow
10	TMJP010000000303	UJPD010000000101	TRUE	0	0				9999/12/31 0:0:0	0	Forbid
11	SMJP010000000303	UJPD010000000101	TRUE	0	0				9999/12/31 0:0:0	0	Forbid
12	TMJP010000000304	UJPD010000000101	TRUE	0	0				9999/12/31 0:0:0	0	Forbid
15	VPJP010000000501	UJPD010000000201	TRUE	ff	0				2009/03/26 0:0:0	ff	Forbid
17	VPJP010000000503		TRUE	ff	0				9999/12/31 0:0:0	0	Allow
18	SMJP010000000504	UJPD010000000201	TRUE	ff	0				9999/12/31 0:0:0	0	Forbid
19	VPJP010000000601	UJPD010000000201	TRUE	ff	0				9999/12/31 0:0:0	0	Forbid
21	VPJP010000000603	UJPD010000000201	TRUE	ff	0				9999/12/31 0:0:0	0	Forbid
22	VPJP010000000604	UJPD010000000201	TRUE	ff	0				9999/12/31 0:0:0	0	Forbid
23	VPJP010000000605	UJPD010000000201	TRUE	ff	0				9999/12/31 0:0:0	0	Forbid
24	VPJP010000000701		TRUE	9	ff				9999/12/31 0:0:0	0	Allow
25	PGJP010000000101	UJPD010000000101	FALSE	0	0				2008/06/30 23:59:59	0	Forbid
26	PSJP010000000101	UJPD010000000101	FALSE	0	0				2008/06/30 23:59:59	0	Forbid

Table B.6 – Data output conditions

Data export condition										
NO	Content ID	Storage Media Type	Encoding Type	Protection Type	Control Type	Move Indicator Flag	Export Count	Time Period	Day Count	Export Period
1	SMJP010000000201	CD								
13	VPJP010000000305	DVD	MPEG*2,H.264	CPRM, DTCP	Copy No More		Copy 9			
15	VPJP010000000501	CD								
16	VPJP010000000502	DVD	MPEG*2,H.264	CPRM	Copy No More		Copy 3			
17	VPJP010000000503	HDD		SAFIA	Copy No More		Copy 10			
18	SMJP010000000504	Flash Memory		CPRM	Copy No More		Copy 10			

Annex C
(informative)

Rights information interoperability background

C.1 General

The distribution of digital content or copyrighted digital work has already been studied from various angles. From the standpoint of digital information distribution in particular, various DRM (Digital Rights Management) systems have been offered and various distribution models such as “superdistribution” have been proposed. However, although the technology and infrastructure to support digital distribution are now in place, no mechanisms or rules for flexible digital distribution that allow the easy exchange of content based on individual commitments between content creators and consumers has been established. The reality is that at present, a technological and social environment where there is a sense of trust between copyright holders and consumers who feel safe about information distribution is not always perfectly provided.

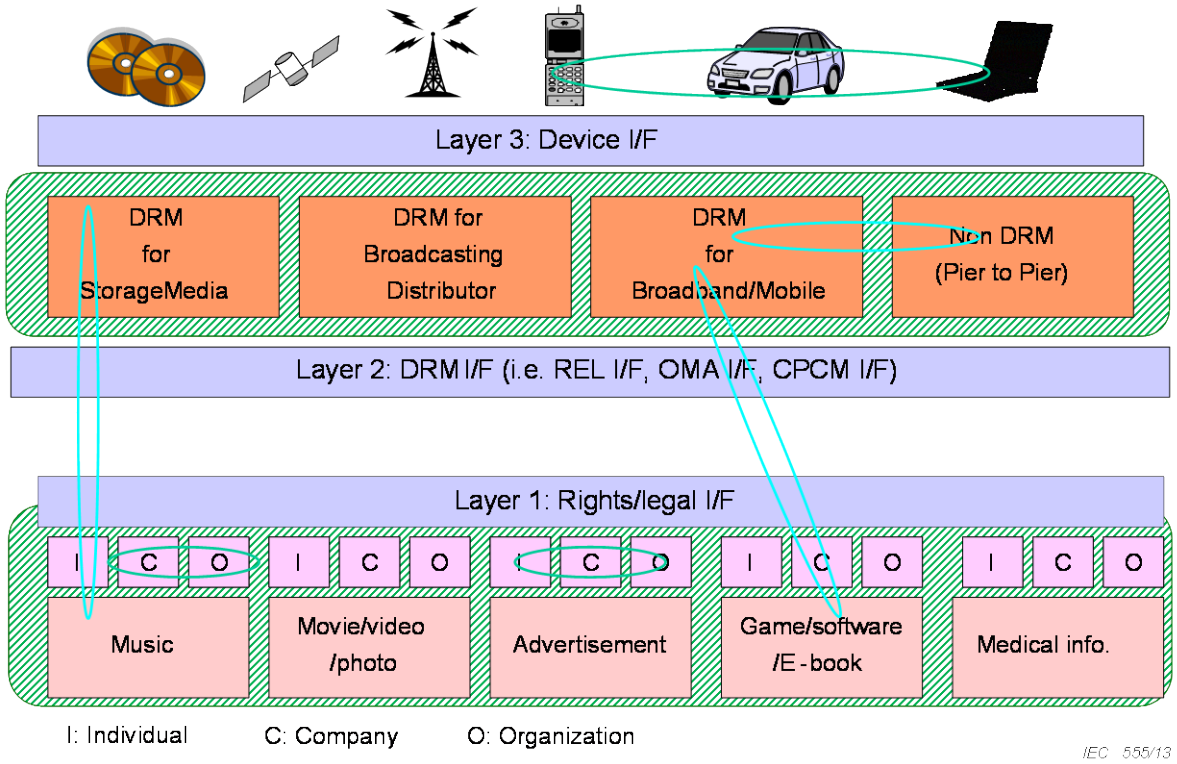


Figure C.1 – Concept – Rights information interoperability

Taking movies as a typical case, the creation of content is generally a group effort, and responsibilities are shared among various individuals. As a result, the financial and personal rights to the final content and the compensation that are to be divided among those involved is uncertain. Since no technology for managing usage fees based on the volume of content consumed has yet been established, it is difficult to say that appropriate compensation is being consistently distributed to all members of a group.

The result is that while content creators want many more opportunities for their content to be used by consumers, there is no system that makes this possible. Consequently, appropriate permissions commitments are not shown and everyone involved is obliged to accept lost opportunities. In addition, the development of the technology for the mobile phones and simple terminals that make content available to the consumer, who is on the front lines of content consumption, is progressing without competing companies achieving interoperability.

Paradoxically, this results in more inconveniences for the consumer. Moreover, while DRM with a certain level of functionality is available, it does not necessarily meet the needs of consumers. Therefore, consumers are generally forced to purchase content in inconvenient ways even though it would be technologically possible to render it more convenient for them.

Rights Information Interoperability (RII) enables to study measures to resolve these problems from two standpoints. The first is engineering: building the infrastructure for a next generation of digital information distribution systems by developing technology that achieves a combination of interoperability and accessibility for the consumer. The second is law: building the social infrastructure for next generation rights processing by providing a new framework for the management and exchange of digital rights permission information among rights holders and consumers. RII provides the standard for an ideal system that merges the two together and helps make interoperability a reality for groups of existing DRM systems scattered throughout the world, see Figure C.1.

C.2 Relationship between rights and digital permissions

Digital rights permissions are the specific components by which rights are exercised.

Holders of the rights defined in current copyright law do not contribute to content distribution if they do not effectively use those rights, even though they hold them. Unfortunately, in most situations where rights are currently exercised, digital rights permissions are often used as components for suing when rights are infringed.

The action of granting digital rights permissions is action that forms an agreement between holders (multiple) who hold declared rights and holders (multiple) who do not have rights according to copyright law but who shall confirm the granting or refusal of permissions for business usage. It also acknowledges that it is acceptable to enable specific content consumption services.

Proper content distribution includes the mutual actions of granting and receiving digital rights permissions (without requiring a lot of time, if possible). Explicit rights and potential rights show that the rights holders agree that “to comprehensively grant all permissions = it is acceptable to enable the specific content consumption services”, and if that is not confirmed, the situation is not one where digital rights permissions have been obtained. However, not all of these permissions can be confirmed in the various license agreements between the parties involved.(see example, below) This is where we run up against the limitations of the law. What compensates for this is technology.

Specifically,

a) code language technology that carries the shared elements that identify the scattered content and the parties associated with that content,

b) code language technology that carries the shared elements that identify information about the specific content consumption services.

These two components convert the latest information about the multi-layered, intertwining contractual relationships into digital data and show that the rights holders agree that it is acceptable to enable the specific content consumption services for the content that has been converted to digital data. The services, applications and devices technologically interpret that agreement and enable legal content consumption.

RII stands for “Rights Information Interoperability”. This is synonymous with management of continually updated digital rights permissions information. Components a) and b) above ensure that as a minimal condition, all of the rights defined in the existing copyright law are expressed. It shall also assure future extensibility, meaning that any new “agreement that it is acceptable to enable specific content consumption services” to appear in the future, will also be technologically expressed.

Example

A representative rights holder B for film A grants the screening rights as stipulated in Japanese copyright law to a Chinese distributor.

↓

Chinese consumer G enjoys film A that belongs to Japanese representative rights holder B.

Streams it?

Downloads it?

Owns recording media?

In other words, this cannot be expressed using currently existing legal techniques alone. For example, if rights holder company H, who grants the rights permissions for film content A, enters into a B2B (business to business) content usage license agreement with distributor U, who runs a downloading business, it is not possible to capture all of the specific service formats in advance. In particular, if we imagine that services that are not yet known will be enabled in the future, the employees responsible for legal affairs shall do everything they can to create increasingly dense and unreadable documents that predict forms of content consumption (this may be the case, but there are also limits to how much it is possible to enumerate the extended uses of fair use regulations and rights limit regulations). The physical license agreement generally states the agreement. Or, there is only a general agreement and an actual license agreement or contractual relationship does not exist. In that situation, prior to having a license agreement, it is critical to have information management for content consumption that is backed by technology in order to legally manage the forms of consumption targeted to more finely differentiated final consumers.

Grant digital rights permissions ⇔ Receive digital rights permissions

c) Cases where content that one owns and controls is enjoyed, and that form of consumption is agreed upon in a prior contractual relationship,

d) Cases where content that one owns and controls is enjoyed, and where that form of consumption is not agreed upon in a prior contractual relationship,

   1) cases where it is possible to obtain permission after consumption,

   2) cases where it is not possible to obtain permission after after consumption.

In future content distribution, it is desirable to have this information integrated into the content in some format in advance (without distinguishing between digital and analog).

Annex D
(informative)

Two basic technologies for enabling RII

D.1 Code language technology that carries the shared elements that identify the scattered content and the parties associated with that content

D.1.1 General

In this digital age, digital technology and networked environments are used, and a wide variety of content and content creators and users exist. The information about them is recorded in the native language of each country as rights related metadata, and on occasion this information is translated into another language. Even if the individual meaning it points to is the same, there are many cases where rights related metadata multiplies or is duplicated. We are establishing code language technology that simplifies these pieces of rights related metadata as much as possible and expresses their common elements.

D.1.2 Rights related metadata and simple tag ID code

Rights related metadata is a general term for information surrounding and related to an object of consumption and enjoyment (film, music, photos, etc.), which is called content or a product, etc.

Rights related metadata can be divided roughly into three types.

a) Open metadata

Examples of open metadata include the product name, official author, etc.

b) Closed metadata

Examples of closed metadata include the auther's real name, bank info, etc.

c) Bridge metadata

Bridge metadata is the shared ID or detailed usage format code that ties together metadata groups a) and b).

Figure D.1 show the relationships between a), b) and c).

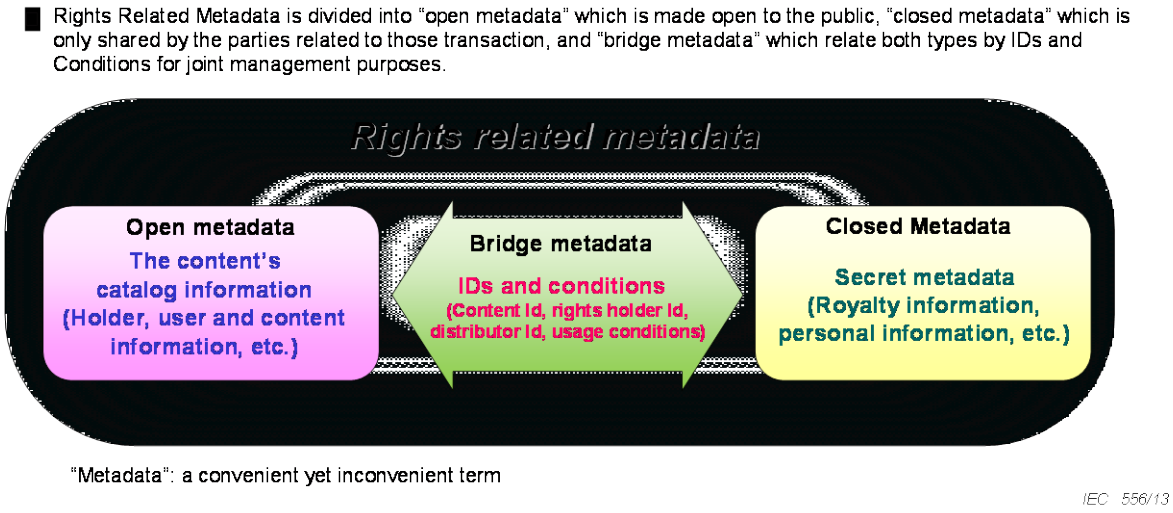


Figure D.1 – Common semantics of Metadata

Figure D.2 shows a practical usage example of shared IDs in bridge metadata.

- As various rights holders are involved with content such as audi c- visual work, the consolidation of name-list information is needed for determining the actual rights holders and the royalties to pay them.
- This name-list information is necessary in the context of “closed information,” shared information that is necessary for contracts etc. among content holders and rights holders only, and also in the context of “open information,” catalog- like information for the purpose of gaining a deeper knowledge r egarding the content in question, between content holders and users or users and consumers.
- For this reason, it is effective to carry out information bridgi ng for both parties, using Rights Holder IDs as a means for association.

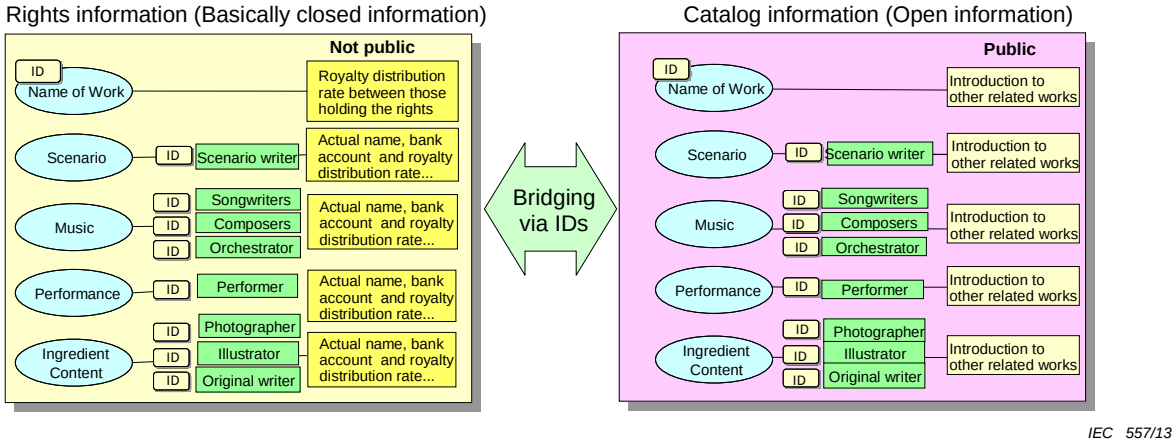


Figure D.2 – The necessity of information consolidation for content distribution

D.1.3 Shared ID system

In order to facilitate content distribution from here on out, it is essential that IDs to identify contents, rights holders and users are commonly used through databases, and that mechanisms for making access from the outside is improved. For this reason, a shared ID system is necessary. The assignment of IDs shared between respective organizations and commercial entities will effectively serve such a function.

a) Content ID

In this digital age, there are countless digital files that function as masters on and outside the net. IEC 62227 specifies the structure of the container carrying the content ID on a shared ID system. The shared ID system has been defined in order to uniquely identify this content. It has a total of 16 digits. First, the types of consumed content are divided into five general attributes. These global attributes are further arranged into established genres, and the content consumption attribute is expressed using two digits. Next, the country of origin for that content is expressed using 2-digit WIPO country codes.

For example, film content created inside Japan is expressed by VPJP~. “VP” is the abbreviation for “Visual Program”. Similarly, photographic content created inside Japan is expressed by “IPJP~”, where “IP” is the abbreviation for “Image Program”.

b) Business ID

1) Rights holder ID

IEC 62227:2008, 5.5.5 specifies the structure of the container carrying the rights holder ID on a shared ID system. It is an ID that commonly identifies the creators, individual rights holders, rights holder companies and rights organizations associated with the content identified using the above content ID.

2) User ID

IEC 62227:2008, 5.5.6 specifies the structure of the container carrying the user ID on a shared ID system. It is ID that commonly identifies the distributor, broadcaster, end consumer, device owned by the consumer and service group used by the consumer, using the content identified as using the above content ID.

D.2 Code language technology that carries the shared elements of the specific content consumer services

D.2.1 General

Carries and expresses the shared elements of specific differentiated content consumption services that cannot be fully expressed using the rights encompassed by copyright law. IEC 62227 specifies the permission classification component and the permission limitation component for specific content consumer services.

D.2.2 Classification

The classification is comprised of seven items defined from a particularly legal perspective. There are four core items of the content in question that shall be written in all of the license agreements:

a) usage purpose;

b) whether or not the content consumption is charged or free and whether or not there is a sponsor;

c) specific usage consumption format;

d) territory of the usage consumption.

In addition, within these four elements there are items that encode

- whether or not these four elements are open to the public and
- if these four elements correspond to requests and claims for B2B rights processing.

D.2.3 Limit components

The four core elements discussed above fundamentally shall be encoded. In contrast, limit components are only encoded if that encoding is required. However, these are components that express information about DRM or information about the latest services that are backed by new technology that may appear in future. There are seven items that shall be used to limit specific content consumption:

a) Personal limit component

Note that when using GC (Group Content) distribution services, it is possible to bundle and group in ways that go beyond content genres.

– Compilation permission (free, by product, by album, compilation within the same artist, compilation within the same company).

b) Transmission and distribution machine setup control component

– CM control (free: consent to skip CM, refuse to skip CM, time-synchronized forced viewing, before and after viewing, time custom viewing, blanket).

c) Quality limit component

– Recording media limit component (see IEC 62227:2008, 5.10.4.4, storage_media_type).

d) Compression format standard (see IEC 62227:2008, 5.9.3.6, transcode type).

e) Bit rate limit component (see IEC 62227:2008, 5.9.3.7, maximum transcode rate).

f) Lifetime (life control) limit component (free, count limit, time period limit, expiration limit).

g) Security limit component (watermark, DRM, rights report).

D.3 Common semantics for RII

RII represents a bridge metadata which unites open information and closed information by Ids and conditions.

Bridge metadata are divided into “Identification” which is made to identify content holder, content user and content itself, “Classification” which is made to relate permission classifications and “Limit components” which is made to relate permission conditions on agreements.

Common semantics for RII is composed of “Identification”, “Classification” and “Limit components”, see Figure D.3.

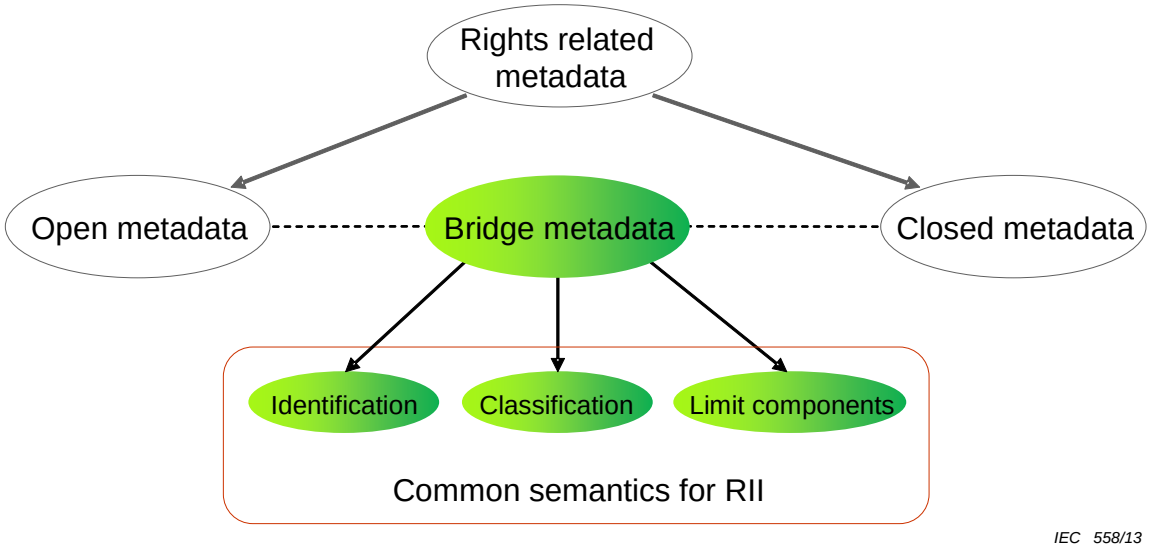


Figure D.3 – Common semantics for RII

D.4 Core elements and common semantics for RII

Each component for RII is divided into core elements which are created to specify the details of the bridge information. Figure D.4 shows core elements and common semantics for RII.

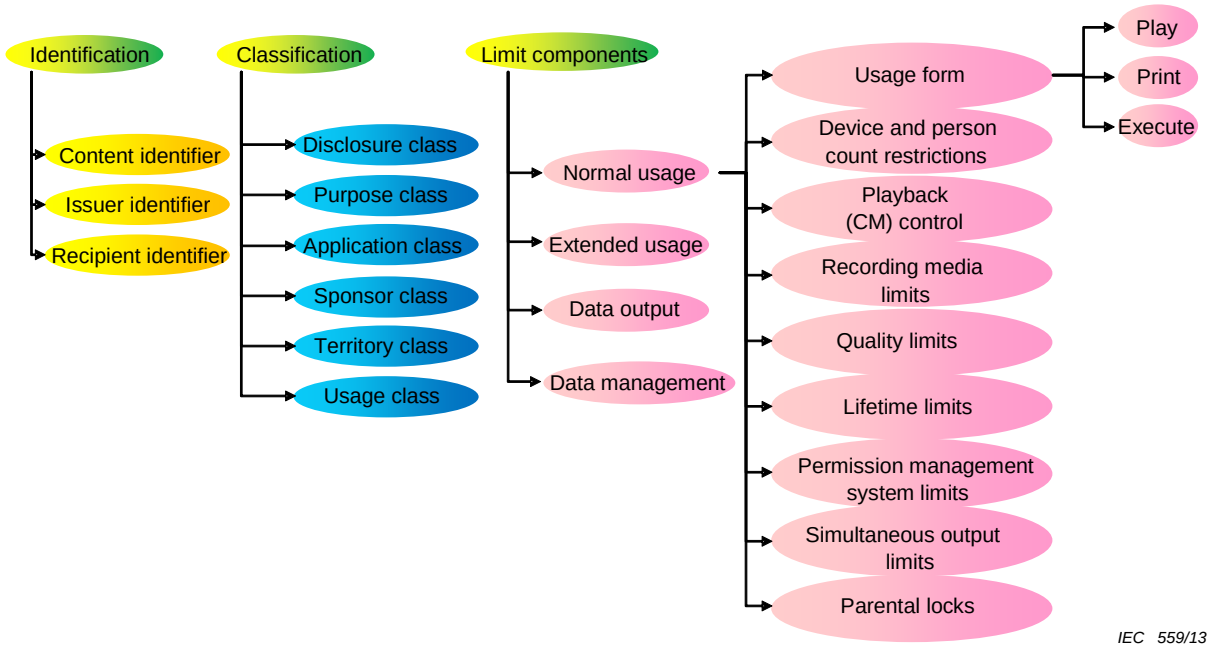


Figure D.4 – Core elements and common semantics for RII

Annex E
(informative)

RII elements corresponding to existing DRM

Tables E.1 to E.11 show the RII (Rights Information Interoperability) elements corresponding to existing DRM (Digital Rights Management) elements in detail.

Table E.1 – Marlin BB (broadband)

Elements of content protection	Marlin BB
Distribution format	Content independent Support following container for transporting content data • MP4 ISO/IEC 14496-14:2003 Other
Content usage permission 1) License requirement → confirmation of contract → content distribution 2) Distribution of license	When DRM server receives a license aquisition request from a terminal, it confirms to a customer management system and a contract management system to be able to distribute the requested license. If possible, it distributes the license embedding rendering obligation and output control information (COPY/MOVE/EXPORT) correnspponds to the contract. DRM server distributes license bound to the target object which is selected from devices, users, subscriptions and domains in accordance with the order of content distributor. Any license being bound to a device is available to any user who has the right to use the device. Any license being bound to a user is available to the user using any device he has the right to use it. Any license being bound to a subscription is available to any user who has the subscription using any device he has the right to use. Any license being bound to a domain is available to any user using any device belonging to the domain when he has the right to use the device or is available to any user belonging to the domain using any device he has the right to use. Users that have usage rights of devices are registered in the server DRM system for each device.
Management of permission issuer, receiver and issue date	Running dependent Possible to manage through the license distribution log on the center Manage users and devices Manage users that have the right to use the specific device and devices available to the specific user Manage available subscription to use a license; users having the subscription and devices that the users have the rights to use. Manage deletion of the rights for users to use a device dynamically.
License storage on a nonvolatile area in a terminal	Available
License move/copy	Available
Encrypted content storage on a nonvolatile area in a terminal	Available

Elements of content protection		Marlin BB
Content playback control	Playback period	It controls playback and output by a code module running on a VM in a DRM client. Code modules are made on a DRM server and are distributed to DRM clients. Even if conditions of playback and output are being changed, client side is independent from a module or a hardware update. It is sufficient to execute a code module on a VM which is being transported from a DRM server. It is possible to control playback and output flexibly.
	Digital copy control information	
	Serial interface output control	
	Analog output copy control	
	Video quality control information	
	Decoded content data retention mode	
	Decoded content data retention state	
	High speed digital I/F protection information	
	CopyRestrictionMode	
	User-defined information	
Control information for exporting to other DRM		
Content data concealment		AES + SCTE 52
Authentication of DRM systems		Authentication of client DRM and server DRM are implemented by using public certificates which are issued by a certificate authority authorized by MTMO. RSA-DSA (1 024 bit/2 048 bit key) with SHA256 Revocation lists of client DRM and server DRM are available.
Communication protection between DRMs		Concealment of communication data RSA 1 024 bit, 2 048 bit RSA 1.5 | RSA-OAEP AES 128 bit Check a tamper of communication data RSA – SHA 1 | RSA – SHA 256 Secret data concealment between DRM system nodes RSA 1 024 bit, 2 048 bit RSA 1.5 | RSA-OAEP AES 128 bit Check a falsification of secret data between DRM system nodes. HMAC – SHA1 RSA – SHA1 | RSA – SHA256

Table E.2 – Marlin IPTV-ES (end-point service), Download license, EXPORT for Copy with Direct Key Delivery

Elements of content protection		Marlin IPTV-ES
		Download license
		EXPORT for Copy with Direct Key Delivery
Distribution format		Download
Content usage permission 1) License requirement → comfirmation of contract → content distribution 2) Distribution of license		When a DRM server receives a license acquisition request from a terminal, it confirms to a customer management system and contract management system whether the terminal has the rights to get the requested license. If possible, it distributes the license embedding playback control information that corresponds to the contract.
Management of permission issuer, receiver and issue date		Running dependent It is possible to manage a license distribution log in the center.
License storage on a nonvolatile area in a terminal		Available
License move/copy		Only available to export to other DRMs
Encrypted content storage on a nonvolatile area in a terminal		Available
Content usage control	Playback period	
	Digital copy control information	
	Serial interface output control	
	Analog output copy control	
	Video quality control information	
	Decoded content data retention mode	
	Decoded content data retention state	
	High speed digital I/F protection information	
	CopyRestrictionMode	
	User-defined information	
Control information for exporting to other DRM		The following elements are available to specify a playback control information for each media. Export to DTCP. Export to CPRM for DVD. Export to CPRM for SD Video. Export to CPRM for SD Audio. Export to MG-R (SVR) for Memory Stick PRO. Export to MG-R (SAR) for Memory Stick and Memory Stick PRO. Export to VCPS. Export to MG-R (SVR) for EMPR. Export to MG-R (SAR) for ATRAC Audio Device. Export to SAFIA for iVDR TV Recording Export to SAFIA for iVDR Audio Recording Export to AACS Blu-ray Disc Recordable for BD-R/RE. Export to AACS Blu-ray Disc Recordable for Red Laser Media.
Content data concealment		

Elements of content protection	Marlin IPTV-ES
	Download license
	EXPORT for Copy with Direct Key Delivery
Authentication of DRM systems	Authentication of client DRM and server DRM is carried out by using a public key certificate which is issued by authentication center as authorized by MTMO. EC-DSA (224 bit key) with SHA256 Run revocation lists. Client DRM can be revoked by each device. Server DRM can be revoked by license distribution server.
Communication protection between DRMs	EC-DH (224 bit key) + EC-DSA (224 bit key) + AES (128 bit key) + SHA 256

Table E.3 – Marlin IPTV-ES, Download license, EXTRACT with Direct Key Delivery, Download

Elements of content protection	Marlin IPTV-ES
	Download license
	EXTRACT with Direct Key Delivery
Distribution format	Downloading
Content usage permission 1) License requirement → comfirmation of contract → content distribution 2) Distribution of license	When DRM server receives a license aquisition request from a terminal, it confirms to a customer management system and a contract management system to be able to distribute the requested license. If possible, it distributes licenses embedding playback control information that corresponds to the contract.
Management of permission issuer, receiver and issue date	Running dependent It is possible to manage as a license distribution log on the center
License storage on a nonvolatile area in a terminal	Available
License move/copy	Not available
Encrypted content storage on a nonvolatile area in a terminal	Available

Elements of content protection		Marlin IPTV-ES
		Download license
		EXTRACT with Direct Key Delivery
Content usage control	Playback period	NotBefore, NotAfter
	Digital copy control information	DigitalRecordingControlData 11: Copy never * Follow APS Control Data for analog output
	Serial interface output control	CopyControlType 01: Serial interface encoding output
	Analog output copy control	APS Control Data 00: Copy free 01: Pseudo-synchronizing pulse 10: Pseudo-synchronizing pulse + two line inverted burst 11: Pseudo-synchronizing pulse + four line inverted burst
	Video quality control information	ImageConstraintToken 1: unbound
	Decoded content data retention mode	RetentionMode 0: Permit retention
	Decoded content data retention state	RetentionState 111: 90 min
	High speed digital I/F protection information	EncryptionMode 1: non-protection
	CopyRestrictionMode	
	User-defined information	Not defined
Control information for exporting to other DRM		
Content data concealment		AES (128 bit key) + SCTE 52
Authentication of DRM systems		Authentication of client DRM and server DRM is carried out by using a public key certificate which is issued by an authentication center as authorized by MTMO. EC-DSA (224 bit key) with SHA256 Run revocation lists. Client DRM can be revoked by each device. Server DRM can be revoked by each license distribution server.
Communication protection between DRMs		EC-DH (224 bit key) + EC-DSA (224 bit key) + AES (128 bit key) + SHA 256

Table E.4 – Marlin IPTV-ES, Download license, EXTRACT with Direct Key Delivery, VOD streaming

Elements of content protection		Marlin IPTV-ES
		Download license
		EXTRACT with Direct Key Delivery
Distribution format		VOD streaming
Content usage permission 1) License requirement → comfirmation of contract → content distribution 2) Distribution of license		When DRM server receives a license acquisition request from a terminal, it confirms to a customer management system and a contract management system whether the terminal has the rights to get the requesting license. If possible, it distributes the license embedding playback control information that corresponds to the contract.
Management of permission issuer, receiver and issue date		Running dependent It is possible to manage as a license distribution log in the center.
License storage on a nonvolatile area in a terminal		Available
License move/copy		Not available
Encrypted content storage on a nonvolatile area in a terminal		Not available except for keeping a quality of playback
Content usage control	Playback period	NotBefore, NotAfter
	Digital copy control information	DigitalRecordingControlData 11: Copy never * Follow APS Control Detail as analog output
	Serial interface output control	CopyControlType 01 : Serial interface encoding output
	Analog output copy control	APS Control Data 00: Copy free 01: Pseudo-synchronizing pulse 10: Pseudo-synchronizing pulse + two line inverted burst 11: Pseudo-synchronizing pulse + four line inverted burst
	Video quality control information	ImageConstraintToken 1: unbound
	Decoded content data retention mode	RetentionMode 0: Retention
	Decoded content data retention state	RetentionState 111: 90 min
	High speed digital I/F protection information	EncryptionMode 1: non-protection
	CopyRestrictionMode	
	User-defined information	undefined
Control information for exporting to other DRM		
Content data concealment		AES (128 bit key) + SCTE 52
Authentication of DRM systems		Authentication of client DRM and server DRM is carried out by using a public key certification which is issued by an authentication center as authorized by MTMO. EC-DSA (224 bit key) with SHA256 Run revocation lists. Client DRM can be revoked by each device. Server DRM can be revoked by license distribution server.
Communication protection between DRMs		EC-DH (224 bit key) + EC-DSA (224 bit key) + AES (128 bit key) + SHA 256

Table E.5 – Marlin IPTV-ES, Broadcast license, EXTRACT with IndirectKey Delivery license, Terrestrial re-distribution/BS (broadcasting satellite) re-distribution

Elements of content protection		Marlin IPTV-ES
		Broadcast license
		EXTRACT with Indirect Key Delivery license
Distribution format		Terrestrial re-distribution/BS re-distribution
Content usage permission 1) License requirement → comfirmation of contract → content distribution 2) Distribution of license		Permission to playback a content confirms, when a terminal requests a license, to a customer management system and a contract management system whether the terminal has the rights to get a requested license (work key). If possible, a DRM server distributes a license embedding information about available channels and available period of reception. Broadcastring data received is permitted to be copied/moved to other media/devices as following to digital copy control information and copy control information set in multiplexed ECM. (Copy/Move is only valid for one generation. Copy/Move is not possible in second generation). There are no playback period limits for a content which is stored in received devices and for a content which is moved/copied to other media/devices.
		Playback controls the information of broadcasting data that follows the terrestrial broadcast and BS broadcast playback control information.
Management of permission issuer, receiver and issue date		Running dependent It is possible to manage it as a license distribution log in the center.
License storage on a nonvolatile area in a terminal		Available
License move/copy		Not available
Encrypted content storage on a nonvolatile area in a terminal		It is not permitted except for keeping a playback quality.
Content usage control	Playback period	NotBefore, NotAfter * There is an offset period in which it is possible to update a license period from NotAfter.
	Digital copy control information	It follows a digital copy control descriptor of SI.
	Serial interface output control	
	Analog output copy control	
	Video quality control information	It succeeds content usage descriptor of SI.
	Decoded content data retention mode	
	Decoded content data retention state	
	High speed digital I/F protection information	
	CopyRestrictionMode	
	User-defined information	undefined
Control information for exporting to other DRM		
Content data concealment		AES (128 bit key) + SCTE 52

Elements of content protection	Marlin IPTV-ES
	Broadcast license
	EXTRACT with Indirect Key Delivery license
Authentication of DRM systems	Authentication of client DRM and server DRM is carried out by using a public key certification which is issued by authentication center as authorized by MTMO. EC-DSA (224 bit key) with SHA256 Run revocation lists. Client DRM can be revoked by each device. Server DRM can be revoked by license distribution server.
Communication protection between DRMs	EC-DH (224 bit key) + EC-DSA (224 bit key) + AES (128 bit key) + SHA 256

Table E.6 – Marlin IPTV-ES, Broadcast license, EXTRACT with DirectKey Delivery license, IP multicast

Elements of content protection	Marlin IPTV-ES
	Broadcasting license.
	EXTRACT with Indirect Key Delivery license
Distribution format	IP multicast
Content usage permission 1) License requirement → comfirmation of contract → content distribution 2) Distribution of license	Permission to playback a content confirms, when a terminal requests a license, to a customer management system and a contract management system whether the terminal has the rights to get a requested license (work key). If possible, a DRM server distributes a license embedding information about available channels and available period of reception. Broadcastring data received is permitted to be copied/moved to other media/devices as following to digital copy control information and copy control information set in multiplexed ECM. (Copy/Move is only valid for one generation. Copy/Move is not possible in second generation). There are no playback period limits for a content which is stored in received devices and for a content which is moved/copied to other media/devices.
	Playback control information of broadcasting data is set/modified by channel in the center.
Management of permission issuer, receiver and issue date	Running dependent It is possible to manage as a license distribution log in the center.
License storage on a nonvolatile area in a terminal	Available
License move/copy	Not available
Encrypted content storage on a nonvolatile area in a terminal	It is not permitted except for keeping a playback quality.

Elements of content protection		Marlin IPTV-ES
		Broadcasting license.
		EXTRACT with Indirect Key Delivery license
Content usage control	Playback period	NotBefore, NotAfter * There is an offset period in which it is possible to update a license period from NotAfter.
	Digital copy control information	DigitalRecordingControlData 00: Constrained condition 10: Copy one generation 11: Copy never * Follow APS Control Data as analog output
	Serial interface output control	CopyControlType 01 : Serial interface encoding output
	Analog output copy control	APS Control Data 00: Copy free 01: Pseudo-synchronized pulse 10: Pseudo-synchronized pulse + two line inverted burst 11: Pseudo-synchronized pulse + four line inverted burst
	Video quality control information	ImageConstraintToken 1: unbound
	Decoded content data retention mode	RetentionMode 0: Retention
	Decoded content data retention state	RetentionState 111: 90 min
	High speed digital I/F protection information	EncryptionMode 0: Protect 1: Non-protect
	CopyRestrictionMode	
	User-defined information	undefined
Control information for exporting to other DRM		
Content data concealment		AES (128 bit key) + SCTE 52
Authentication of DRM systems		Authentication of client DRM and server DRM is carried out by using a public key certification which is issued by an authentication center as authorized by MTMO. EC-DSA (224 bit key) with SHA256 Run revocation lists. Client DRM can be revoked by each device. Server DRM can be revoked by license distribution server.
Communication protection between DRMs		EC-DH (224 bit key) + EC-DSA (224 bit key) + AES (128 bit key) + SHA 256

Table E.7 – Marlin IPTV-ES, VOD license, EXTRACT with Simple Key Delivery license

Elements of content protection		Marlin IPTV-ES
		VOD license
		EXTRACT with Simple Key Delivery license
Distribution format		VOD streaming
Content usage permission 1) License requirement → comfirmation of contract → content distribution 2) Distribution of license		When a server DRM receives a license acuisition request from a terminal, it confirms to a customer management system and contract management system whether the terminal has rights to get a requested license. If possible, it distributes the license embedding playback control information that corresponds to the contract.
Management of permission issuer, receiver and issue date		Running dependent It is possible to manage it as a license distribution log in the center.
License storage on a nonvolatile area in a terminal		Not available
License move/copy		Not available
Encrypted content storage on a nonvolatile area in a terminal		It is not available except for keeping playback quality.
Content usage control	Playback period	
	Digital copy control information	DigitalRecordingControlData 11: Copy never * Follow APS Control Detail as analog output
	Serial interface output control	CopyControlType 01: Serial interface encoding output
	Analog output copy control	APS Control Data 00: Copy free 01: Pseudo-synchronized pulse 10: Pseudo-synchronized pulse + two line inverted burst 11: Pseudo-synchronized pulse + four line inverted burst
	Video quality control information	ImageConstraintToken 1: unbound
	Decoded content data retention mode	RetentionMode 0: Retention
	Decoded content data retention state	RetentionState 111: 90 min
	High speed digital I/F protection information	EncryptionMode 1: Non protection
	CopyRestrictionMode	
	User-defined information	undefined
Control information for exporting to other DRM		
Content data concealment		AES (128 bit key) + SCTE 52
Authentication of DRM systems		Authentication of client DRM and server DRM is carried out by using a public key certification which is issued by an authentication center as authorized by MTMO. EC-DSA (224 bit key) with SHA256 Run revocation lists. Client DRM can be revoked by each device. Server DRM can be revoked by license distribution server.
Communication protection between DRMs		EC-DH (224 bit key) + EC-DSA (224 bit key) + AES (128 bit key) + SHA 256

Table E.8 – WM-DRM (Windows Media DRM)

Elements of content protection		WM-DRM
Distribution format		Download
Content usage permission 1) License requirement → comfirmation of contract → content distribution 2) Distribution of license		Encrypted content protected by using a key which is encrypted in a license and related to a specific terminal. Both rights and rules which restrict available period and playback count, etc. are included in the license rather than the content. By separating a license from content, a server DRM can issue different licenses for the same content.
Management of permission issuer, receiver and issue date		It is possible in license server
License storage on a nonvolatile area in a terminal		Available
License move/copy		Not available to other PC and network devices. Available to portable devices/media(in this case, AllowCopy is required.)
Encrypted content storage on a nonvolatile area in a terminal		Available
Content usage control	Playback period	The content provider is allowed to combine a following constraints alternatively. • Following a calendar date, a license can be valid or not. • A license can be revoked after a specific time period starting from the first use. • A license can be revoked after a specific time period starting from the first installation to PCs or devices. Following a playback count condition, a license can be revoked.
	Digital copy control information Serial interface output control Analog output copy control Video quality control information	<Audio output protection> 1. Non protection 2. Obfuscation (Protection by Secure Audio Path. Digital output is permitted.) 3. Encryption low (Protection by Secure Audio Path. Digital output is denied.) 4. Encryption middle 5. Encryption high <Video output protection> 1. Non protection 2. Obfuscation (For analog video: Copy Generation Management System) 3. Encryption low (For non-compression digital video: High-Bandwidth Digital Content Protection using secure path such as COPPv1, HDCP up stream protocol, etc.) 4. Encryption middle 5. Encryption high (Compressed digital video: Microsoft Link Protection which has an approximate rectriction)
	Decoded content data retention mode	Not available
	Decoded content data retention state	–
	High speed digital I/F protection information	–
	CopyRestrictionMode	–
	User-defined information	–
Control information for exporting to other DRM		Not available
Content data concealment		As a requrement of network devices, following encryption technology is considering • AES (128 bits) using both ECB and CTR mode

Elements of content protection	WM-DRM
Authentication of DRM systems	By linking each terminal to a server indentically, the system security increases considerably. If terminals infringe on security, they can be identified in licensing process and revoked. It is possible to revoke by a license server.
Communication protection between DRMs	With respect to the requirements of network devices, the following encryption technologies exist. • 2 048 bit RSA encryption that can store and protect a private key • SHA-256 that has 2048 bit RSA encryption and AES OMAC1

Table E.9 – OMA DRM v2.0

Elements of content protection	OMA DRM v2.0
	CMLA (Content Management License Administrator)
Distribution format	• Download • Streaming
Content usage permission 1) License requirement → comfirmation of contract → content distribution 2) Distribution of license	When Server DRM receives a license acquisition requirement from a terminal to a rights holder, it confirms to a customer management system and a contract management system whether the terminal has rights to get the requested license. If possible, it distributes a license embedding a playback control information correnspronds to the contract.
Management of permission issuer, receiver and issue date	The content issuer, rights issuer and DRM agent are defined, and it is possible to manage it by the rights holder.
License storage on a nonvolatile area in a terminal	Available
License move/copy	If these devices are in the same domain, the content and rights object can be shared. If these devices do not belong to a common domain, only the content can be copied.
Encrypted content storage on a nonvolatile area in a terminal	Available

Elements of content protection		OMA DRM v2.0
		CMLA (Content Management License Administrator)
Content usage control	Playback period	Describe in rights object
	Digital copy control information	Out of scope in OMA DRM. In CMLA technical specification, there are description to support HDCP and DTCP
	Serial interface output control	
	Analog output copy control	
	Video quality control information	
	Decoded content data retention mode	Out of scope in OMA DRM.
	Decoded content data retention state	Out of scope in OMA DRM
	High speed digital I/F protection information	Out of scope in OMA DRM
	CopyRestrictionMode	–
	User-defined information	–
Control information for exporting to other DRM		1) EXPORT is available 2) The way to transport from OMA DRM to other protection mechanisms is not defined. 3) Permission and restriction of the following elements are available by rights object • Export permission • DRM system to export • Copy/move selection when it is exported.
Content data concealment		EncryptionMethod Field 0x0 No encryption 0x1 AES(128 bit) + CBC 0x2 AES(128 bit) + CTR
Authentication of DRM systems		A terminal has own secret/public key and certificate. In a certificate, there are the author's name, device type, the software version, the serial number, and the certificate determines whether a rights holder trusts a terminal or not.
Communication protection between DRMs		Rights information is protected by a rights information acquisition protocol.

Table E.10 – AACS, basic

Elements of content protection		AACS
		Basic title
Distribution format		• Consumer software (Pre-recorded media) • Disc for broadcast (Recordable media)
Content usage permission 1) License requirement → comfirmation of contract → content distribution 2) Distribution of license		It is possible to decode a content by a combination of the device key in the playback device and encrypted title keys in the media.
Management of permission issuer, receiver and issue date		The basic title does not connect online.
License storage on a nonvolatile area in a terminal		Basic title does not connect online
License move/copy		[Move] It is possible to move a title which records in recordable media. [Copy] Not available
Encrypted content storage on a nonvolatile area in a terminal		Basic title doesn't connect on line
Content usage control	Playback period	Not available
	Digital copy control information	In order to prevent illegal copies, it is required to have a secure digital interface such as HDMI on audio/video output.
	Serial interface output control	
	Analog output copy control	
	Video quality control information	
	Decoded content data retention mode	Out of scope
	Decoded content data retention state	Out of scope
	High speed digital I/F protection information	For preventing illegal copy, it is required to secure digital interface such as HDMI on audio/video output
	CopyRestrictionMode	–
	User-defined information	–
Control information for exporting to other DRM		Not available
Content data concealment		AES(128 bit)
Authentication of DRM systems		–
Communication protection between DRMs		–

Table E.11 – AACS, extended

Elements of content protection		AACS
		Extended title
Distribution format		• Consumer software • Recordable disc for broadcasting • AACS Network Download Content • AACS On-line Enabled Content • AACS Streamed Content
Content usage permission 1) License requirement → comfirmation of contract → content distribution 2) Distribution of license		After authentication online by an authentication server, the content is decoded by a combination of the device key in a playback terminal and the encrypted title key in a media.
Management of permission issuer, receiver and issue date		Authentication management by authentication server is running dependent
License storage on a nonvolatile area in a terminal		Only titles which have cacheable attributes are available.
License move/copy		[move] Title recorded in recordable medhia can be moved. [Copy]y It is managed by a managed copy. It is required to authenticate online.
Encrypted content storage on a nonvolatile area in a terminal		<AACS Network Download Content> Nerver Store. Available to record on the media such as BD <AACS On-line Enabled Content> Available to the title that has a cacheable attribute <AACS Streamed Content> Never Store.
Content usage control	Playback period	Only titles that have a cacheable attribute are available. It is specified by period, after and before attribute.
	Digital copy control information	
	Serial interface output control	
	Analog output copy control	
	Video quality control information	
	Decoded content data retention mode	Out of scope
	Decoded content data retention state	Out of scope
	High speed digital I/F protection information	Out of scope
	CopyRestrictionMode	–
	User-defined information	–
Control information for exporting to other DRM		Not available
Content data concealment		AES(128 bit)

Elements of content protection	AACS
	Extended title
Authentication of DRM systems	A terminal connect authentication server which is described in Title Usage File of Title and transport content id. Authentication server authenticate it.
Communication protection between DRMs	TLS_RSA_WITH_AES_128_CBC_SHA

Bibliography

The following documents provide additional or detailed information on each organization.

ISO/IEC 14496-14:2003, *Information technology – Coding of audiovisual objects– Part 14: MP4 file format*

Amendment 1:2010, *Handling of MPEG-4 audio enhancement layers*

ARIB TR-B14, *Operational guidelines for digital terrestrial television broadcasting*

_____

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

SYSTÈMES DE SERVEUR DOMESTIQUE MULTIMÉDIA – INTEROPÉRABILITÉ D'INFORMATION DES DROITS POUR TVIP

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de la CEI. La CEI n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de brevet. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale CEI 62698 a été établie par le domaine technique 8: Systèmes de serveur domestique multimédia, du Comité d'études 100 de la CEI: Systèmes et appareils audio, vidéo et multimédia.

Certaines parties du texte de cette norme ont été élaborées en collaboration avec l'UIT-T/Groupe d'études 16: Plateformes d'application mutimédia et systèmes finaux pour TVIP.

NOTE La Recommandation UIT-T, s'agissant du texte parallèle à cette norme, est la recommandation UIT-T H.751 "Métadonnées pour l'interopérabilité d'information des droits pour TVIP" et est en révision/approbation. Voir le site web de l'UIT pour plus de détails.

Le texte de cette norme est issu des documents suivants:

CDV	Report on voting
100/1947/CDV	100/1998/RVC

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de la CEI sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION

Il n'existe pas actuellement des mécanismes ou des règles de distribution numérique souples permettant d'échanger facilement un contenu, sur la base d'engagements individuels entre créateurs et consommateurs de contenu. Ceci est dû au fait qu'un environnement technologique et social de confiance entre les détenteurs de droits d'auteur et les consommateurs, sécurisant la distribution des informations, n'est pas toujours parfaitement fourni.

Pour fournir aux créateurs et aux consommateurs ce type d'environnement d'utilisation de contenu, pour leur donner un plus grand nombre d'opportunités pour tous les types de contenu numérique, quel que soit le support qu'ils utilisent pour les stocker, une interopérabilité est nécessaire, permettant aux systèmes et aux matériels de TVIP de constituer le circuit de valorisation envisagé pour communiquer et travailler mutuellement sur différents systèmes qui gèrent la distribution de contenu.

L'interopérabilité d'information des droits (RII) résout ces problèmes en facilitant la fourniture aux détenteurs de droits de contenu et aux consommateurs d'une sémantique et d'éléments fondamentaux communs s'étendant sur différents systèmes gérant la distribution de contenu.

SYSTÈMES DE SERVEUR DOMESTIQUE MULTIMÉDIA – INTEROPÉRABILITÉ D'INFORMATION DES DROITS POUR TVIP

1 Domaine d'application

La présente Norme internationale définit la sémantique et les éléments fondamentaux communs d'interopérabilité d'information des droits pour les systèmes/matériels de TVIP permettant d'utiliser légalement un contenu multimédia sur différentes plates-formes.

L'information des droits comporte des métadonnées associées aux droits et à la sécurité, qui sont décrites dans l'UIT-T H.750.

Les informations associées aux droits telles que l'identifiant de contenu, l'identifiant de l'émetteur d'autorisation et l'identifiant du récepteur d'autorisation, qui sont utilisées pour constituer un pont entre les métadonnées concernant les droits, sont considérées dans la présente norme. D'autre part, la technologie de gestion des droits et de protection des contenus ne fait pas partie du domaine d'application de la présente norme.

2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

CEI 62227:2008, *Systèmes serveurs multimédia domestiques – Codes numériques des autorisations des droits* (disponible en anglais seulement)

CEI/TR 62636:2009, *Multimedia home server systems – Implementation of digital rights permission code* (disponible en anglais seulement)

ISO 3166-1, *Codes pour la représentation des noms de pays et de leurs subdivisions – Partie 1: Codes de pays*

Recommandation UIT-T X.509, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut*

Recommandation UIT-T H.750:2009, *Spécification de haut niveau des métadonnées pour les services de TVIP*

3 Abréviations et acronymes

Pour les besoins du présent document, les abréviations et acronymes suivants s'appliquent.

AAC	Codage audio évolué *(Advanced Audio Coding)*
AACS	Système évolué d'accès au contenu *(Advanced Access Content System)*
CD	Disque Compact *(Compact Disc)*
CGMS	Système de gestion de la génération de copies *(Copy Generation Management System*)
CPRM	Protection du contenu pour support enregistrable *(Content Protection for Recordable Media*)

DTCP	Protection de contenu de transmission numérique *(Digital Transmission Content Protection)*
DVD	Disque numérique polyvalent *(Digital Versatile Disc)*
GIF	Format d'échange graphique *(Graphic Interchange Format)*
HD	Haute définition
HDCP	Protection de contenu numérique en haute définition *(High-bandwidth Digital Content Protection)*
HDD	Disque dur *(Hard Disk Drive)*
ID	Identifiant
JPEG	Groupe mixte d'experts en photographie *(Joint Photographic Experts Group)*
MP3	MPEG Couche audio 3
MPEG	Groupe d'experts des images animées *(Moving Picture Experts Group)*
MIC	Modulation par impulsions et codage
MTMO	Marlin Trust Management Organization
PNG	Graphique de réseaux portables *(Portable Network Graphics)*
RII	Interopérabilité d'information des droits *(Rights Information Interoperability)*
SAFIA	Architecture de sécurité pour pièce jointe intelligente *(Security Architecture For Intelligent Attachment)*
VCPS	Système de protection de contenu vidéo *(Video Content Protection System)*
TVIP	*(Internet Profile TeleVision)*
CM	Message publicitaire *(Commercial Message)*
OMPI	Organisation Mondiale de la Propriété Intellectuelle

4 Systèmes: l'environnement RII

4.1 Généralités

La présente norme constitue la norme de haut niveau des métadonnées pour l'interopérabilité d'information des droits incluant la représentation des éléments minimums requis.

Les métadonnées de RII fournissent une classification descriptive et contextuelle pour représenter les informations des droits en utilisant le cadre d'autorisation.

La RII concerne la recherche des plus grands dénominateurs communs des expressions de droits incluant les composants minimum requis lorsqu'on essaye de mettre en œuvre l'utilisation mutuelle d'information des droits.

Elle concerne l'acheminement des informations des droits en unités de groupes d'expressions de contexte, appelées autorisations.

On considère ici les composants constitutifs des autorisations. Les autorisations peuvent coder «quoi de qui à qui dans quelles conditions» en utilisant des expressions de contexte. Lorsque des autorisations sont envoyées à un terminal, les composants minimum requis sont les informations sujets dans les autorisations correspondant à la partie «quoi de qui à qui» et les informations d'utilisation de contenu correspondant à la partie «dans quelles conditions».

4.2 Sujets d'autorisation

Un sujet d'autorisation est constitué des informations de l'émetteur exprimant la partie «de qui» des autorisations. Ces informations sont détenues par le fournisseur de service et dans la RII, leur composant minimum requis est l'identifiant du détenteur de droits.

Seul l'identifiant de l'émetteur est inclus car dans la RII, il suffit que le fournisseur de service et le terminal puissent identifier qui accorde les autorisations. Il n'est pas nécessaire d'envoyer toutes les informations de l'émetteur du serveur au terminal. L'identifiant du détenteur de droits correspond donc à l'identifiant de l'émetteur dans les expressions de contexte de RII. Le fournisseur de service reçoit le code d'autorisation de droits numériques depuis le terminal et charge l'identifiant du détenteur de droits inclus dans l'identifiant de l'émetteur pour identifier le détenteur de droits qui a accordé les autorisations.

Un autre sujet d'autorisation est constitué des informations du récepteur exprimant la partie «à qui» des autorisations. Dans la RII, ce composant minimum requis est l'identifiant d'utilisateur/identifiant de dispositif.

Seul l'identifiant du récepteur est inclus car dans la RII, il suffit que le fournisseur de service et le terminal puissent identifier à qui sont accordées les autorisations. L'identifiant de l'utilisateur/identifiant du dispositif correspond donc à l'identifiant du récepteur dans les expressions de contexte de RII. Le terminal reçoit le code d'autorisation de droits numériques du fournisseur de service et détermine si l'identifiant d'utilisateur/identifiant de dispositif inclus dans l'identifiant de récepteur correspond ou non au terminal local ou le fournisseur de service reçoit le code d'autorisation de droits numérique du terminal et charge l'identifiant d'utilisateur/identifiant de dispositif inclus dans l'identifiant de récepteur pour identifier l'utilisateur à qui les autorisations ont été accordées.

Un autre sujet d'autorisation est constitué des informations concernant le contenu pour lequel les autorisations sont accordées, qui est exprimé dans la partie «quoi». Dans la RII, ce composant minimum requis est l'identifiant de contenu.

Seul l'identifiant de contenu est inclus dans la RII, car il suffit que le fournisseur de service et le terminal soient capables d'identifier le contenu pour lequel sont accordées les autorisations. Le terminal reçoit le code d'autorisation de droits numériques du fournisseur de service et détermine que le contenu correspondant à l'identifiant de contenu est accordé.

4.3 Composants de limite d'autorisation

Un composant de limite d'autorisation est le type des autorisations (appelé ci-après «composant de classification d'autorisation») exprimant des stipulations concernant ce qui est accordé. Ces autorisations font l'objet d'un accord entre l'émetteur et le récepteur. Il s'agit des informations dont le récepteur a besoin pour pouvoir effectuer un contrôle hors ligne. Dans la RII, les composant minimums requis sont les suivants: un type indiquant si le contenu de l'autorisation accordée est public ou non (appelé ci-après «classe disclosure»), un type indiquant le but d'utilisation accordé (appelé ci-après «classe purpose»), un type indiquant le format de facturation accordé (appelé ci-après «classe charge model»), un type indiquant le format de demande accordé (appelé ci-après «classe request»), un type indiquant le format de commanditaire accordé (appelé ci-après «classe sponsor»), un type indiquant le format d'utilisation accordé (appelé ci-après «classe usage») et un type indiquant le territoire accordé (appelé ci-après «classe territory»). Ces composants de limite d'autorisation sont inclus dans la RII car il est nécessaire de pouvoir observer ces informations même dans un environnement hors-ligne qui n'est pas connecté à un réseau. Ceci est tel que le terminal peut déterminer le type des autorisations qui sont accordées entre le fournisseur de service et le terminal.

Un autre composant limite d'autorisation contient des conditions de limitation qui s'ajoutent aux restrictions des points accordés ci-dessus. Ce sont principalement des informations qui limitent le type d'autorisations stipulé par la classe usage. Dans la RII, ces composant minimums requis sont le format d'utilisation d'autorisation et ses conditions de limitation (appelées ci-après «limites d'utilisation normale»), les limites d'utilisation de contenu pour les terminaux conformes (appelées ci-après «limites du système de gestion d'autorisations») et les limites concernant la sortie du contenu sur des terminaux non conformes ou sur un support (appelées ci-après «limites de sorties simultanées»).

Ces composants de limite d'autorisation sont inclus dans la RII car il est nécessaire que les droits auxquels ils correspondent soient observés sur le terminal même dans un environnement hors-ligne qui n'est pas connecté à un réseau. Ceci est tel que le terminal peut déterminer dans quelles conditions les types d'autorisations sont limités entre le fournisseur de service et le terminal.

La RII ne fournit pas de méthode de codage d'expressions de contexte pour les autorisations. La méthode de codage est déjà normalisée en utilisant une technologie normalisée existante. En remplacement, l'Article B.2 montre l'exemple de l'addition d'expressions de contexte exprimées en utilisant un langage naturel dans la CEI 62227 (DRPC).

La RII est un ensemble d'éléments à considérer lorsque chaque contenu est distribué et que l'autorisation d'une telle distribution est générée.

La RII n'est donc pas définie d'un point de vue technique mais plutôt en se basant sur des informations d'autorisation utilisées réellement par les détenteurs de droits dans le domaine. La RII elle-même n'a pas la possibilité de réglementer le comportement de l'utilisation du contenu.

La limitation de l'utilisation d'un contenu aux termes spécifiés dans l'autorisation est une question administrative ou une question concernant les systèmes de DRM. La RII ne comporte pas de politique exclusive. Les responsables de la mise en œuvre de chaque DRM ou les systèmes de distribution de contenu peuvent choisir leur propre sous-ensemble et configuration d'utilisation de RII, sur la base de leurs nécessités et de leurs ressources. Ils peuvent même limiter l'application à un simple affichage d'autorisation et ne pas utiliser la gestion des droits.

5 Identifiants de sujet d'autorisation

5.1 Identifiants de sujet d'autorisation

L'identifiant de sujet d'autorisation est constitué de trois identifiants; le contenu d'identifiant assigné au contenu de sujet, l'identifiant d'émetteur et l'identifiant du récepteur respectivement, soumis à chaque autorisation de l'émetteur et du récepteur.

5.2 Identifiant de contenu

L'identifiant de contenu est constitué d'informations permettant d'identifier le contenu de manière unique. Il est exigé d'être assigné à chaque contenu soumis à autorisation. La CEI 62227:2008, 5.5.4 spécifie les identifiants de contenu soumis à autorisation.

5.3 Identifiant d'émetteur

L'identifiant d'émetteur est constitué d'informations permettant d'identifier de manière unique l'émetteur d'autorisation. L'identifiant d'émetteur peut être utilisé, non seulement pour identifier un détenteur de droits, un fournisseur de service et un serveur domestique, mais également pour le suivi de la consommation, le rapport des droits et la gestion de contenu. La CEI 62227:2008, 5.5.5 spécifie les identifiants d'émetteur soumis à autorisation.

5.4 Identifiant de récepteur

L'identifiant de récepteur est constitué d'informations permettant d'identifier de manière unique le récepteur d'autorisation. L'identifiant de récepteur peut être utilisé pour identifier un utilisateur final, un dispositif et un ensemble d'utilisateurs finaux. La CEI 62227:2008, 5.5.6 spécifie les identifiants de récepteur soumis à autorisation.

6 Classification d'autorisation

6.1 Classification d'autorisation

La classification d'autorisation indique la classe de l'autorisation. Il convient de la décrire en fonction des conditions indiquées dans l'accord d'autorisation.

6.2 Classe Disclosure

La classe Disclosure comporte une classification indiquant si une autorisation donnée est une autorisation fermée pour un lecteur spécifié ou une autorisation ouverte pour un groupe de lecteurs non spécifié. L'émetteur et le récepteur d'autorisation peuvent accéder aux informations d'autorisation fermée. Les valeurs possibles sont «open permission», «closed permission» et «other». Open permission est l'autorisation reçue conformément à des conditions par défaut agencées au préalable. Closed permission est l'autorisation reçue par l'intermédiaire d'un contrat séparé négocié individuellement.

La CEI 62227, 5.6.4 spécifie une classification d'autorisation pour signaler et acheminer des informations de divulgation. L'Aritcle B.2 de la CEI/TR 62636:2009 fournit des scénarios de cas d'utilisation pour mettre en œuvre la classe de divulgation.

6.3 Classe Purpose

La classe Purpose comporte une classification indiquant le but de l'utilisation du contenu, par exemple commercial, public, éducatif, non lucratif et de promotion. Assurer la consommation de contenu dans la condition peut être soumis à une gestion de domaine. Les valeurs possibles sont «commercial», «public», «non-profit», «promotion», «éducation» et «other».

L'autorisation Commercial est l'autorisation pour une utilisation commerciale. L'autorisation Public est l'autorisation pour une utilisation publique. L'autorisation Non-profit est l'autorisation pour une utilisation publique. L'autorisation Promotion est l'autorisation pour une utilisation de promotion. L'autorisation Education est l'autorisation pour une utilisation éducative.

Dans la CEI 62227:2008, 5.6.5, la classe Usage Purpose spécifie une classification d'autorisation pour signaler et acheminer des informations de but d'utilisation. L'Aritcle B.2 de la CEI/TR 62636:2009, fournit des scénarios de cas d'utilisation pour mettre en œuvre la classe usage Purpose.

6.4 Classe Charge Model

La classe Charge Model comporte une classification incluant la méthode de paiement, par exemple gratuit et payant. La classe Charge Model peut inclure le «pay-per-view» (paiement à la séance) et «subscription» (paiement périodique fixe). Il convient de ne pas utiliser ces deux conditions en même temps, mais si l'une est sélectionnée, l'autre n'est pas utilisée. Les valeurs possibles sont «free of charge», «pay per use», «subscription», «coupon».

La CEI 62227:2008, 5.6.6, spécifie une classification d'autorisation pour signaler et acheminer des informations de modèle de paiement. L'Aritcle B.2 de la CEI/TR 62636:2009, fournit des scénarios de cas d'utilisation pour mettre en œuvre la classe Charge Model.

6.5 Classe Sponsor

La classe Sponsor comporte une classification incluant le type de commanditaire, par exemple un modèle publicitaire, un modèle de prime, un modèle de coupon et un modèle de divulgation d'informations de consommation.

Le modèle publicitaire décrit les conditions de visualisation des messages publicitaires dans la consommation de contenu. Le modèle de prime, le modèle de coupon et le modèle de

description d'informations de consommation décrivent les conditions d'acquisition du contenu. Dans le modèle de prime, il peut y avoir un annonceur spécifique pour promouvoir un contenu spécifique. Dans le modèle de coupon il peut y avoir plusieurs annonceurs pour promouvoir le contenu. Dans le modèle de divulgation, le contenu peut être remplacé par les informations de consommation de l'utilisateur final. Il est nécessaire de mettre en œuvre pour ces modèles le contrôle de jeu et la fonction d'échange de points. Les valeurs possibles sont «No sponsor», «Advertisement model without force viewing», «Advertisement model with force viewing», «Advertisement model with pre/post viewing», «Advertisement model with alternative viewing», «Advertisement model with blanket viewing», «Premium model», «Coupon model», «Privacy information disclosure model» et «Other».

La CEI 62227:2008, 5.6.9, spécifie une classification d'autorisation pour signaler et acheminer des informations de mandataire. La CEI/TR 62636: 5.17, et la CEI/TR 62636: 5.18, fournissent des scénarios de cas d'utilisation pour mettre en œuvre la classe de mandataire.

6.6 Classe Territory

La classe Territory comporte une classification indiquant le territoire de consommation du contenu, par exemple un pays et une région. Il est requis de mettre en œuvre la technologie, par exemple la gestion de domaine, pour spécifier le territoire dans lequel le contenu est consommé. Les valeurs possibles sont region code, country code (ISO 3166-1) et Zip code.

La CEI 62227:2008, 5.6.10, spécifie une classification d'autorisation pour signaler et acheminer des informations de territoire. L'Aritcle B.2 de la CEI/TR 62636:2009, fournit des scénarios de cas d'utilisation pour mettre en œuvre la classe territory.

6.7 Classe Usage

La classe Usage comporte une classification indiquant le type d'utilisation, par exemple le type de transmission, le type de stockage, le type de réutilisation et le type de redistribution, sur la base de l'environnement d'utilisation.

Dans la CEI 62227:2008, 5.6.11, la classe Usage spécifie une classification d'autorisation pour signaler et acheminer des informations d'utilisation. L'Aritcle B.2 de la CEI/TR 62636:2009, fournit des scénarios de cas d'utilisation pour mettre en œuvre la classe usage.

Les éléments requis dans la classe Usage sont énumérés ci-dessous.

- Le type Transmission exprime une forme de distribution de contenu dans des domaines cible et des dispositifs en conformité. Si, par exemple, la valeur est «download», le contenu peut être téléchargé dans des dispositifs en conformité. Les valeurs possibles sont «broadcast», «streaming», «download» et «physical media».
  - Dans la CEI 62227:2008, 5.6.11.2, usage_type, spécifie une classification d'autorisation pour signaler et acheminer des informations de classe usage.
- Le type Store exprime une forme d'accumulation de contenu dans les domaines cible et les dispositifs en conformité. Si, par exemple, la valeur est «fixation», le contenu peut être enregistré dans des dispositifs en conformité. Les valeurs possibles sont «fixation» et «non-fixation».
  - Dans la CEI 62227:2008, 5.6.11.2, usage_type, spécifie une classification d'autorisation pour signaler et acheminer des informations de classe usage.
- Le type Reuse exprime le type d'utilisation secondaire de contenu dans des domaines cible et des dispositifs en conformité. Les valeurs possibles sont enable or disable secondary usage, move, copy, export, share, edit, modify et super distribution.
  - Dans la CEI 62227:2008, 5.6.11.4, move_flag, 5.6.11.5, copy_flag, 5.6.11.6, export_flag, 5.6.11.7, share_flag, 5.6.11.8, edit_flag, 5.6.11.9, modify_flag, 5.6.11.10, super_distribution_flag, spécifient une classification d'autorisation pour signaler et acheminer des informations de classe usage.

- Le type Redistribution exprime le type d'acheminement de contenu depuis des domaines cible et des dispositifs en conformité (par exemple, enable ou disable).
  - Dans la CEI 62227:2008, 5.6.11.3, redistribution_type, spécifie une classification d'autorisation pour signaler et acheminer des informations de classe usage.

6.8 Classe Compilation

La classe Compilation comporte une classification indiquant un contenu selon que l'émetteur d'autorisation est autorisé ou non à combiner et à vendre plusieurs éléments de contenu. Il est requis d'assurer la cohérence de la lecture avec une liste de lecture. Les valeurs possibles sont True dans le cas d'activation de la liste de lecture, False dans le cas de la désactivation de la liste de lecture.

Dans la CEI 62227:2008, 5.7.3.2.6, playlist_parameter, spécifie une condition d'autorisation pour signaler et acheminer des informations de compilation.

7 Composants de limite d'autorisation

7.1 Composants de limite d'autorisation

Les composants de limite de classification comportent des informations indiquant la restriction des conditions d'autorisation décrites dans la classification d'autorisation. Elle peut être décrite pour restreindre les conditions indiquées dans l'accord d'autorisation.

7.2 Condition générale d'utilisation

7.2.1 Généralités

La condition générale d'utilisation est un élément comprenant une forme d'utilisation et ses conditions limites dans lesquelles il peut être autorisé d'utiliser le contenu dans des domaines cible et des dispositifs en conformité. Elle comporte des informations limitant la condition d'utilisation à la consommation de contenu, par exemple l'utilisation en lecture, l'utilisation en impression et l'utilisation en exécution.

L'utilisation en lecture est un élément de la forme d'utilisation tel que le contenu peut être temporairement restitué tout en restant perceptible. La condition d'utilisation en lecture exprime la limite dans laquelle le contenu peut être autorisé à être lu dans des domaines cible et des dispositifs en conformité.

La CEI 62227:2008, 5.7.3.2, spécifie une contrainte d'autorisation pour la signalisation et l'acheminement de condition de lecture.

L'utilisation en impression est un élément de la forme d'utilisation tel que le contenu peut être restitué en permanence sur l'objet physiquement fixe. La condition d'utilisation en impression exprime la limite dans laquelle le contenu peut être autorisé à être imprimé dans des domaines cible et des dispositifs en conformité.

La CEI 62227:2008, 5.7.3.3, spécifie une contrainte d'autorisation pour la signalisation et l'acheminement de condition d'impression.

L'utilisation en exécution est un élément de la forme d'utilisation tel que le contenu peut être restitué temporairement avec le processus de calcul. La condition d'utilisation en exécution exprime la limite dans laquelle le contenu peut être autorisé à être exécuté dans des domaines cible et des dispositifs en conformité.

La CEI 62227:2008, 5.7.3.4, spécifie une contrainte d'autorisation pour la signalisation et l'acheminement de condition d'exécution.

7.2.2 Quality Limits

Quality Limits comporte des informations indiquant la qualité du contenu distribué. Les fournisseurs d'autorisation les représentent généralement sous forme de niveaux qualitatifs tels que LEVEL1 (haute qualité), LEVEL2 (qualité standard), LEVEL3 (basse qualité) and LEVEL4 (autre). Si, par exemple, la valeur est «LEVEL1», on peut autoriser l'utilisation du contenu (lecture, impression ou exécution) avec la meilleure qualité. Les valeurs possibles sont «LEVEL1», «LEVEL2», «LEVEL3» et «LEVEL4».

Dans la CEI 62227:2008, 5.7.3.2.4, quality_parameter, spécifie une condition de qualité pour l'utilisation en lecture. Dans la CEI 62227:2008, 5.7.3.3.4, quality_parameter, spécifie une condition de qualité pour l'utilisation en impression. Dans la CEI 62227:2008, 5.7.3.4.4, service_level_parameter, spécifie une condition de qualité pour l'utilisation en exécution.

7.2.3 Lifetime Limits

Lifetime Limits comporte des informations indiquant la durée de vie du contenu distribué. Les émetteurs d'autorisation spécifient généralement une période de temps, un nombre de jours et une période de date.

Les éléments requis dans Lifetime Limits sont énumérés ci-dessous.

NOTE Sauf indication contraire, le numéro du paragraphe dans le même tiret se réfère à la CEI 62227:2008, comme indiqué au début de chaque tiret.

- Time period exprime le nombre d'heures pendant lesquelles l'utilisation du contenu est autorisée (lecture, impression ou exécution) dans des domaines cible et des dispositifs en conformité. Si, par exemple, la valeur est twenty-four, le contenu peut être utilisé pendant 24 h après réception dans des dispositifs en conformité. Les valeurs possibles sont des nombres naturels et l'unité est l'heure (par exemple, 24 h, 48 h).
  - Dans la CEI 62227:2008, 5.7.3.2.13, time_period_parameter, peut décrire l'élément avec la même signification sur l'utilisation en lecture. 5.7.3.3.11, time_period_parameter, peut décrire l'élément avec la même signification sur l'utilisation en écriture. 5.7.3.4.12, time_period_parameter, peut décrire l'élément avec la même signification sur l'utilisation en lecture.
- Day count exprime le nombre de dates pendant lesquelles on peut autoriser l'utilisation du contenu (lecture, impression ou exécution) dans des domaines cible et des dispositifs en conformité. Si par exemple la valeur est seven, le contenu peut être utilisé pendant 7 jours après réception dans des dispositifs en conformité. Les valeurs possibles sont des nombres naturels et l'unité est le jour (par exemple, 1 jour, 7 jours).
  - Dans la CEI 62227:2008, 5.7.3.2.14, day_count_parameter, peut décrire l'élément avec la même signification sur l'utilisation en lecture. 5.7.3.3.12, day_count_parameter, peut décrire l'élément avec la même signification sur l'utilisation en impression. 5.7.3.4.13, day_count_control_parameter, peut décrire l'élément avec la même signification sur l'utilisation en exécution.
- Date period exprime la date limite jusqu'à laquelle on peut autoriser l'utilisation du contenu (lecture, impression ou exécution) dans un domaine cible et des dispositifs en conformité. Si, par exemple, la valeur est de 2010/11/01 à 2010/11/30, le contenu peut être utilisé du 1er novembre 2010 au 30 novembre 2010. Les valeurs possibles sont des dates (date de début et date de fin) et l'unité est la date (par exemple, la période de la date de début à la date de fin).
  - Dans la CEI 62227:2008, 5.7.3.2.15, start_date_parameter, peut décrire l'élément avec la même signification sur l'utilisation en lecture. 5.7.3.3.13, start_date_parameter, peut décrire l'élément avec la même signification sur l'utilisation en impression. 5.7.3.4.14, start_date_parameter, peut décrire l'élément avec la même signification sur l'utilisation en lecture.
  - Dans la CEI 62227:2008, 5.7.3.2.16, end_date_parameter, peut décrire l'élément avec la même signification sur l'utilisation en lecture. 5.7.3.3.14, end_date_parameter, peut

décrire l'élément avec la même signification sur l'utilisation en impression. 5.7.3.4.15, end_date_parameter, peut décrire l'élément avec la même signification sur l'utilisation en lecture.

7.2.4 Permission Management System Limits

Permission Management System Limits comporte des informations indiquant la méthode de gestion de contenu qu'il convient d'utiliser pour la gestion des autorisations, par exemple, le filigrane numérique, le rapport des droits et la protection contre la copie numérique.

Si, par exemple, la valeur est «digital copy protection», il est exigé d'un dispositif en conformité, de protéger le contenu pendant son temps d'utilisation (lecture, impression ou exécution) en utilisant une DRM. Les valeurs possibles sont «digital copy protection», «digital watermark» et «rights report». Sa valeur peut être de –1 pour la signification «other».

Dans la CEI 62227:2008, 5.7.3.2.5, permission_management_model_parameter, peut décrire l'élément avec la même signification sur l'utilisation en lecture. Dans la CEI 62227:2008, 5.7.3.3.5, permission_management_model_parameter, peut décrire l'élément avec la même signification sur l'utilisation en impression et dans la CEI 62227:2008, 5.7.3.4.5, permission_management_ model_parameter, peut décrire l'élément avec la même signification sur l'utilisation en exécution.

7.2.5 Simultaneous Output Limits

Simultaneous Output Limits comporte des informations indiquant le nombre autorisé de sorties simultanées pour chaque consommation de contenu. Si par exemple la valeur est de deux, un dispositif en conformité pendant son temps d'utilisation (lecture, impression ou exécution) peut être autorisé à exporter le contenu simultanément vers deux dispositifs d'affichage. Les valeurs possibles sont des entiers non négatifs.

Sa valeur peut être de –1 pour la signification «other».

Dans la CEI 62227:2008, 5.7.3.2.17, simultaneous_output_parameter, peut décrire l'élément avec la même signification sur l'utilisation en lecture.

7.3 Extended Usage Condition

Extended Usage Condition comporte des informations indiquant la condition étendue à la condition d'utilisation régulière. Cette condition est à l'étude.

8 Data Management Condition

Data Management Condition comporte des informations indiquant la condition faisant l'objet de sauvegarde du contenu d'origine ou la permission de réédition. Le dispositif doit être capable de contrôler la consommation par l'utilisateur final d'une diversité de services et de contenus dans des conditions spécifiques décrites pour la gestion des données.

Les émetteurs d'autorisation spécifient généralement un indicateur de chiffrement, un nombre de copies, un type de transcodage, une date d'expiration et une autre condition d'utilisation concernant la gestion des données.

Les éléments requis dans Data Management Condition sont énumérés ci-dessous.

- Indicateur Encryption destiné à indiquer s'il est nécessaire ou non de chiffrer le contenu. Les valeurs possibles sont true si le chiffrement est requis, false si le chiffrement n'est pas requis.
  - Dans la CEI 62227:2008, 5.9.3.3, encryption_flag, peut décrire l'élément avec la même signification.

- Copy count exprime le nombre de fois où il peut être autorisé de copier le contenu dans des domaines cible et des dispositifs en conformité. Si la valeur est 1, il peut y avoir deux copies, incluant celle d'origine. Les valeurs possibles sont des entiers non négatifs. Sa valeur peut être de -1 pour la signification «other».
  - Dans la CEI 62227:2008, 5.9.3.4, copy count, peut décrire l'élément avec la même signification.
- Move count exprime le nombre de fois où il peut être autorisé de déplacer le contenu dans des domaines cible et des dispositifs en conformité. MOVE signifie habituellement une combinaison de la copie du contenu et de l'effacement de l'original. Les valeurs possibles sont des entiers non négatifs. Sa valeur peut être de –1 pour la signification «other».
  - Dans la CEI 62227:2008, 5.9.3.5, move count, peut décrire l'élément avec la même signification.
- Transcode type exprime le type de transcodage dans lequel il peut être autorisé d'enregistrer le contenu dans un domaine cible et des dispositifs en conformité. Les valeurs possibles sont MPEG-1, MPEG-2, H.264, JPEG, GIF, PNG, Linear PCM, AAC et MP3.
  - Dans la CEI 62227:2008, 5.9.3.6, transcode type, peut décrire l'élément avec la même signification.
- Maximum transcode rate exprime le débit binaire le plus élevé pouvant être autorisé pour transcoder le contenu pour l'enregistrer dans un domaine cible et dans des dispositifs en conformité. Les valeurs possibles sont des nombres réels non négatifs et l'unité est le kbit/s.
  - Dans la CEI 62227:2008, 5.9.3.7, maximum transcode rate, peut décrire l'élément avec la même signification.
- Minimum transcode rate exprime le débit binaire le plus bas pouvant être autorisé pour transcoder le contenu pour l'enregistrer dans un domaine cible et dans des dispositifs en conformité. Les valeurs possibles sont des nombres réels non négatifs et l'unité est le kbit/s.
  - Dans la CEI 62227:2008, 5.9.3.8, minimum transcode rate, peut décrire l'élément avec la même signification.
- Expiration date exprime la date limite à laquelle il peut être autorisé de stocker un contenu dans un domaine cible et dans des dispositifs en conformité. Les valeurs possibles sont des dates; l'unité est la date.
  - Dans la CEI 62227:2008, 5.9.3.9, expiration date, peut décrire l'élément avec la même signification.
- Sublicense count exprime le nombre de fois où il peut être autorisé de délivrer des licences secondaires dans des domaines cible et des dispositifs en conformité. Les valeurs possibles sont des entiers non négatifs.
  - Dans la CEI 62227:2008, 5.9.3.10, sublicense count, peut décrire l'élément avec la même signification.
- L'indicateur Time-line edit indique si l'édition du contenu par rapport à une référence de temps et la sauvegarde du contenu résultant est autorisée ou non. Les valeurs possibles sont true pour l'activation de l'édition de la référence de temps, false pour la désactivation de l'édition de la référence de temps.
  - Dans la CEI 62227:2008, 5.9.3.11, time-line edit, peut décrire l'élément avec la même signification.

9 Data Export Condition

Data Export Condition comporte des informations indiquant la condition soumise à l'export du contenu d'origine vers des objets non conformes. Le dispositif doit être capable de contrôler la consommation par l'utilisateur final d'une diversité de services et de contenus dans des conditions spécifiques décrites pour l'export des données.

Les émetteurs d'autorisation spécifient généralement le support de stockage, le type de codage, le type de contrôle, la période de temps, le nombre de jours, la période de date et d'autres conditions d'utilisation concernant l'export du contenu.

Les éléments requis dans Data Export Condition sont énumérés ci-dessous.

- Indicateur Encryption destiné à indiquer s'il est nécessaire ou non de chiffrer le contenu. Les valeurs possibles sont true si le chiffrement est requis, false si le chiffrement n'est pas requis.
  - Dans la CEI 62227:2008, 5.9.3.3, encryption_flag, peut décrire l'élément avec la même signification.
- Copy count exprime le nombre de fois où il peut être autorisé de copier le contenu dans des domaines cible et des dispositifs en conformité. Si la valeur est 1, il peut y avoir deux copies, incluant celle d'origine. Les valeurs possibles sont des entiers non négatifs. Sa valeur peut être de –1 pour la signification «other».
  - Dans la CEI 62227:2008, 5.9.3.4, copy count, peut décrire l'élément avec la même signification.
- Move count exprime le nombre de fois où il peut être autorisé de déplacer le contenu dans des domaines cible et des dispositifs en conformité. MOVE signifie habituellement une combinaison de la copie du contenu et de l'effacement de l'original. Les valeurs possibles sont des entiers non négatifs. Sa valeur peut être de –1 pour la signification «other».
  - Dans la CEI 62227:2008, 5.9.3.5, move count, peut décrire l'élément avec la même signification.
- Transcode type exprime le type de transcodage dans lequel il peut être autorisé d'enregistrer le contenu dans un domaine cible et des dispositifs en conformité. Les valeurs possibles sont MPEG-1, MPEG-2, H.264, JPEG, GIF, PNG, Linear PCM, AAC et MP3.
  - Dans la CEI 62227:2008, 5.9.3.6, transcode type, peut décrire l'élément avec la même signification.
- Maximum transcode rate exprime le débit binaire le plus élevé pouvant être autorisé pour transcoder le contenu pour l'enregistrer dans un domaine cible et dans des dispositifs en conformité. Les valeurs possibles sont des nombres réels non négatifs et l'unité est le kbit/s.
  - Dans la CEI 62227:2008, 5.9.3.7, maximum transcode rate, peut décrire l'élément avec la même signification.
- Minimum transcode rate exprime le débit binaire le plus bas pouvant être autorisé pour transcoder le contenu pour l'enregistrer dans un domaine cible et dans des dispositifs en conformité. Les valeurs possibles sont des nombres réels non négatifs et l'unité est le kbit/s.
  - Dans la CEI 62227:2008, 5.9.3.8, minimum transcode rate, peut décrire l'élément avec la même signification.
- Expiration date exprime la date limite à laquelle il peut être autorisé d'enregistrer un contenu dans un domaine cible et dans des dispositifs en conformité. Les valeurs possibles sont des dates; l'unité est la date.
  - Dans la CEI 62227:2008, 5.9.3.9, expiration date, peut décrire l'élément avec la même signification.
- Sublicense count exprime le nombre de fois où il peut être autorisé de délivrer des licences secondaires dans des domaines cible et des dispositifs en conformité. Les valeurs possibles sont des entiers non négatifs.
  - Dans la CEI 62227:2008, 5.9.3.10, sublicense count, peut décrire l'élément avec la même signification.
- L'indicateur Time-line edit indique si l'édition du contenu par rapport à une référence de temps et la sauvegarde du contenu résultant est autorisée ou non. Les valeurs possibles

sont true pour l'activation de l'édition de la référence de temps, false pour la désactivation de l'édition de la référence de temps.

– Dans la CEI 62227:2008, 5.9.3.11, time-line edit, peut décrire l'élément avec la même signification.

Annexe A
(informative)

Problèmes relatifs à la SÉCURITÉ

A.1 Détection de fraude

A.1.1 Généralités

On doit détecter si les données de format de distribution représentant des autorisations de droits numériques ont été ou non falsifiées par quiconque, ces données de format de distribution doivent donc impliquer une signature numérique.

On donne comme exemples applicables d'algorithmes de signature numérique, EC-DSA avec SHA et RSA/DSA avec SHA. Il convient que la norme concrète de la signature dépende de chaque système de service.

La composition brute des données de format de distribution est représentée dans le Tableau A.1.

Tableau A.1 – Composition brute des données de format de distribution

Description	Données d'autorisation des droits numériques	Signature numérique	Certificat ou PkiPath
Les informations suivantes sont impliquées. – Numéro de hiérarchie du Pkipath – L'algorithme de signature – Longueur de clé – Paramètres de chiffrement, etc.	Données représentant les autorisations de droits numériques	Signature numérique des données d'autorisation des droits numériques générée par l'algorithme et la norme spécifiés dans la description.	Certificat ou chaîne de certificats authentifiant la signature numérique.

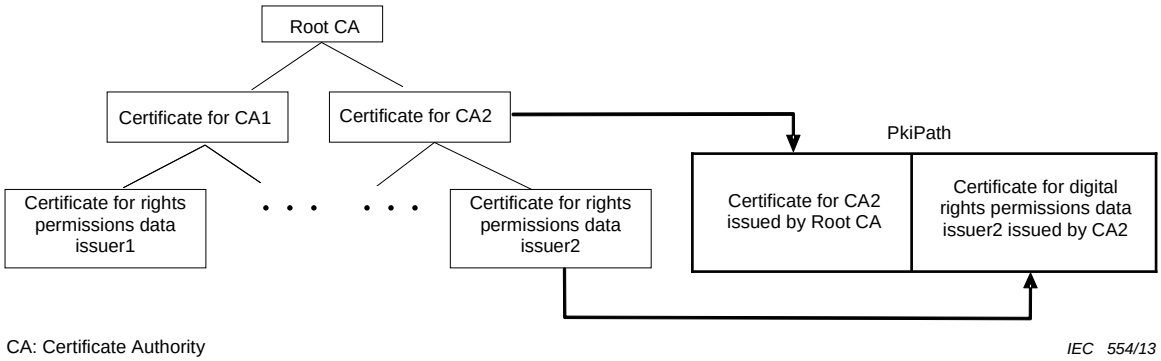
A.1.2 Authentification

L'émetteur des données d'autorisation des droits numériques génère une paire de clés publique/privée et obtient un certificat de la clé publique auprès d'une autorité de certification appropriée.

L'émetteur génère la signature numérique des données d'autorisation des droits numériques en utilisant la clé privée ci-dessus, et crée les données de format de distribution en ajoutant la signature et le certificat aux données d'autorisation des droits numériques.

Les normes des certificats pour la signature numérique des données d'autorisation des droits numériques doivent être conformes à la Recommandation UIT-T X.509.

Dans le cas où le certificat contient une chaîne de certificats, on utilise, PkiPath défini dans la Recommandation UIT-T X.509.



Légende

Anglais	Français
RootCA	RootCA
Certificate for CA1	Certificat pour CA1
Certificate for CA2	Certificat pour CA2
Certificate for rights permissions data issuer1	Certificat pour données d'autorisation de droit issuer1
Certificate for rights permissions data issuer2	Certificat pour données d'autorisation de droit issuer2
CA: Certificate Authority	CA: Autorité de certification
PkiPath	PkiPath
Certificate for CA2 issued by Root CA	Certificat pour CA2 délivré par Root CA
Certificate for digital rights permissions data issuer2 issued by CA2	Certificat pour les données d'autorisation des droits numériques issuer2 délivré par CA2

Figure A.1 – Exemple de PkiPath

Le numéro de la hiérarchie de PkiPath dépend de la norme de fonctionnement de chaque système de service et ces informations doivent être spécifiées dans la zone de description des données de format de distribution.

A.1.3 Signature

Les algorithmes suivants sont applicables à la génération et la vérification de signature.

EC-DSA avec SHA

RSA/DSA avec SHA

Les longueurs de clé et les paramètres de chiffrement de EC-DSA, RSA/DSA et SHA dépendent de chaque norme de système de service et ces informations doivent être spécifiées dans la zone description des données de format de distribution.

A.2 Conservation du secret

Le fait que les données de format de distribution représentant des autorisations de droits numériques doivent être maintenues secrètes dépend du système de service.

Dans le cas où les données d'autorisation des droits numériques doivent être maintenues secrètes, la norme de protection dépend également de chaque norme de système de service et n'est pas décrite dans la présente norme.

Annexe B
(informative)

Syntaxe (codage)

B.1 Généralités

En considérant la mise en œuvre pour des services de TVIP, ces métadonnées doivent être codées par un format normalisé commun. Il existe une exigence selon laquelle il convient que la configuration de représentation des métadonnées concernant les droits soit basée sur une syntaxe commune pour assurer son interopérabilité.

Cet article présente les scénarios des 23 cas d'utilisation types décrits dans la CEI/TR 62636. Dans l'Article B.2, ces scénarios sont divisés dans des tableaux de conditions d'autorisation utilisant les syntaxes de la CEI 62227.

- Achat de contenu
- Location avec limite de temps ou de lecture
- Abonnement
- Récupération directe de contenu à partir d'un dispositif: Scénario 1
- Récupération directe de contenu à partir d'un dispositif: Scénario 2
- Lecture illimitée
- Prévisualisation
- Autorisations multiples pour un DCF en plusieurs parties
- Héritage
- Export de contenu OMA DRM
- Combinaison d'éléments de contrainte
- FairPlay
- CPRM
- SAFIA
- Ringtones
- Téléchargement de contenu libre avec publicité
- Lecture en continu de contenu libre avec publicité
- Jeux
- Coupons (points de remise)
- Description d'informations confidentielles
- Copie 9 fois avec déplacement illimité
- Abonnement à des jeux
- Location de logiciels

B.2 Tableaux de syntaxes DRPC des vingt-trois scénarios

Cet article décrit les tableaux de syntaxe DRPC (voir CEI 62227) des vingt-trois scénarios de B.1 divisant quatre éléments principaux; ContentID, IssuerID, Receiver ID et Permission Conditions en sous-éléments spécifiant la valeur pratique de chaque élément dans les scénarios (Tableaux B.1-B.6).

Dans le scénario d'abonnement, il existe trois codes d'autorisation différents,

a) un code d'autorisation parentale représentant une condition d'autorisation d'un contrat d'abonnement lui-même et

b) deux codes d'autorisation pour enfants représentant les conditions d'autorisation de contenus musicaux.

NOTE On suppose que Receiver ID prend la valeur fixe «HJPC01000000001».

Tableau B.1 – Acteurs d'autorisation et classifications des autorisations

NO	Content ID	Scenario	Disclosure Class	Usage Purpose Class	Charge Model Class	Billing Class	Application Class	Sponsor Class	Territory Class	Usage Class	Receiver ID
1	SMJP010000000201	Content purchase	Open	Commercial	Fee-based	Individual	Individual	No Sponsor	Reserved	Download, Reuse, Move, Copy, Export	UJPI 010000000101
2	VPJP010000000202	Rental with time or playback limit	Open	Commercial	Fee-based	Individual	Individual	No Sponsor	Reserved	Download	UJPI 010000000101
3	SMJP010000000210	Subscription	Open	Commercial	Fee-based, Subscription	Individual	Individual	No Sponsor	Reserved	Download, Reuse, Copy	UJPI 010000000101
4	SMJP010000000211	Subscription child 1	Open	Commercial	Fee-based, Subscription	Individual	Individual	No Sponsor	Reserved	Download, Reuse, Copy	UJPI 010000000101
5	SMJP010000000212	Subscription child 2	Open	Commercial	Fee-based, Subscription	Individual	Individual	No Sponsor	Reserved	Download, Reuse, Copy	UJPI 010000000101
6	SMJP010000000221	Direct retrieval of content from a device: Scenario 1	Open	Commercial	Fee-based	Individual	Individual	No Sponsor	Reserved	Download	UJPD010000000101
7	VFJP010000000222	Direct retrieval of content from a device: Scenario 2	Open	Commercial	Fee-based	Individual	Individual	No Sponsor	Reserved	Streaming	UJPD010000000101
8	VPJP010000000301	Unlimited play	Open	Commercial	Fee-based	Individual	Individual	No Sponsor	Reserved	Download, Reuse, Copy	UJPI 010000000101
9	VPJP010000000302	Preview	Open	Commercial	Fee-based	Individual	Individual	No Sponsor	Reserved	Streaming	UJPI 010000000101
10	TMJP010000000303	Multiple permissions for a multipart DCF (Lyrics)	Open	Commercial	Fee-based	Individual	Individual	No Sponsor	Reserved	Download	UJPD010000000101
11	SMJP010000000303	Multiple permissions for a multipart DCF (Song)	Open	Commercial	Fee-based	Individual	Individual	No Sponsor	Reserved	Download	UJPD010000000101
12	TMJP010000000304	Inheritance	Open	Commercial	Free	Individual	Individual	No Sponsor	Reserved	Streaming	UJPD010000000101
13	VPJP010000000305	Export of OMA DRM content	Open	Commercial	Fee-based	Individual	Individual	No Sponsor	Reserved	Download	UJPD010000000101
14	VPJP010000000306	Combinations of constraint elements	Open	Commercial	Fee-based	Individual	Individual	No Sponsor	Reserved	Download, Reuse, Export	UJPD010000000101
15	VPJP010000000501	FairPlay	Open	Commercial	Fee-based	Individual	Individual	No Sponsor	Reserved	Streaming	UJPD010000000101
16	VPJP010000000502	CPRM	Open	Commercial	Fee-based	Individual	Individual	No Sponsor	Reserved	Download, Reuse, Copy, Export	UJPI 010000000101
17	VPJP010000000503	SAFIA	Open	Commercial	Fee-based	Individual	Individual	No Sponsor	Reserved	Download, Reuse, Export	UJPI 010000000101
18	SMJP010000000504	Ringtones	Open	Commercial	Fee-based	Individual	Individual	No Sponsor	Reserved	Download, Reuse, Copy, Export	UJPI 010000000101
19	VPJP010000000601	Download of content free with advertising	Open	Commercial	Free	Individual	Individual	No Sponsor	Reserved	Download, Reuse, Copy, Export	UJPD010000000101
20	VPJP010000000602	Streaming of content free with advertising	Open	Commercial	Free	Individual	Individual	Time-synchronized Forced Viewing	Reserved	Download, Reuse, Copy	UJPI 010000000101
21	VPJP010000000603	Giveaways	Open	Commercial	Free	Individual	Individual	Time-synchronized Forced Viewing	Reserved	Streaming	UJPI 010000000101
22	VPJP010000000604	Coupons (discount points)	Open	Commercial	Free	Individual	Individual	Giveaway Model	Reserved	Download, Reuse, Copy	UJPI 010000000101
23	VPJP010000000605	Privacy information disclosure	Open	Commercial	Free	Individual	Individual	Coupon Model	Reserved	Download, Reuse, Copy	UJPI 010000000101
24	VPJP010000000701	Copying 9 times with unlimited moving	Open	Commercial	Fee-based	Individual	Individual	Advertising Model	Reserved	Streaming	UJPI 010000000101
25	PGJP010000000101	Subscription games	Open	Commercial	Fee-based	Individual	Individual	No Sponsor	Reserved	Fixed Broadcast Delivery, Reuse, Move, Copy	UJPI 010000000101
26	PSJP010000000101	Software rental	Open	Commercial	Fee-based	Individual	Individual	No Sponsor	Reserved	Download	UJPI 010000000101
						Individual	Individual	No Sponsor	Reserved	Download	UJPI 010000000101

Légende

Anglais	Français
NO	N°
Content ID	Identifiant de contenu
Scenario	Scénario
Disclosure Class	Classe Disclosure
Usage Purpose Class	Classe Usage Purpose

Anglais	Français
Charge Model Class	Classe Charge Model
Content purchase	Achat de contenu
open	ouvert
commercial	commercial
Fee-based	payant
Rental with time or playback limit	Location avec limite de temps ou de lecture
Subscription	Abonnement
Fee-based, Subscription	Payant, abonnement
Subscription child 1	Abonnement enfant 1
Subscription child 2	Abonnement enfant 2
Direct retrieval of content form a device: Scenario 1	Récupération directe de contenu à partir d'un dispositif: Scénario 1
Direct retrieval of content form a device: Scenario 2	Récupération directe de contenu à partir d'un dispositif: Scénario 2
Unlimited play	Lecture illimitée
Preview	Prévisualisation
Multiple permissions for a multipart DCF (Lyrics)	Autorisations multiples pour un DCF en plusieurs parties (Paroles)
Multiple permissions for a multipart DCF (Song)	Autorisations multiples pour un DCF en plusieurs parties (Chansons)
Inheritance	Héritage
Free	Gratuit
Export of OMA DRM content	Export de contenu OMA DRM
Combinations of constraint elements	Combinaisons d'éléments de contrainte
Download of content free with advertising	Téléchargement de contenu libre avec publicité
Streaming of content free with advertising	Lecture en continu de contenu libre avec publicité
Giveaways	Jeux
Coupons (discount points)	Coupons (points de remise)
Privacy information disclosure	Description d'informations confidentielles
Copying 9 times with unlimited moving	Copie 9 fois avec déplacement illimité
Subscription games	Abonnement à des jeux
Software rental	Location de logiciels
Anglais (second table)	Français
Billing Class	Classe Billing
Application Class	Classe Application
Sponsor Class	Classe Sponsor
Territory Class	Classe Territory
Usage Class	Classe usage
Receiver ID	Identifiant de récepteur
Individual	Individu
No sponsor	Pas de mandataire
Reserved	Réservé
Download, Reuse, Move, Copy, Export	Téléchargement, Réutilisation, Déplacement, Copie, Export
Download	Téléchargement
Download, Reuse, Copy	Téléchargement, Réutilisation, Copie

Anglais	Français
Streaming	Lecture en continu
Download, Reuse, Export	Téléchargement, Réutilisation, Export
Download, Reuse, Copy, Export	Téléchargement, Réutilisation, Copie, Export
Time-synchronized Forced Viewing	Visualisation forcée synchronisée dans le temps
Giveaway Model	Modèle de jeu
Coupon Model	Modèle de coupon
Advertising Model	Modèle publicitaire
Fixed Broadcast Delivery, Reuse, Move, Copy	Fourniture de diffusion fixe, Réutilisation, Déplacement, Copie

Tableau B.2 – Condition d'utilisation en lecture

		Playback Usage Condition									
NO		Quality Parameter		Playlist	Num of Playback	Num of Playback Hours	Num of Playback Days	Playback Period	Simultaneous Output	Parental Guidance	Countable Time (Seconds)
1	SMJP010000000201	LEVEL1,LEVEL2,LEVEL3,LEVEL4	DRM	Allow						General	
2	VPJP010000000202	LEVEL1,LEVEL2,LEVEL3	DRM	Forbid	240:00:00	48:0:0		2008/03/28 0:0:0-2008/03/29 11:59:59		General	30
3	SMJP010000000210	LEVEL1,LEVEL2,LEVEL3	DRM	Allow						General	
4	SMJP010000000211	LEVEL1,LEVEL2,LEVEL3	DRM	Allow						General	
5	SMJP010000000212	LEVEL1,LEVEL2,LEVEL3	DRM	Allow						General	
6	SMJP010000000221	LEVEL1,LEVEL2,LEVEL3	DRM	Allow						General	
7	VFJP010000000222	LEVEL1,LEVEL2,LEVEL3	DRM	Allow						General	
8	VPJP010000000301	LEVEL1,LEVEL2,LEVEL3,LEVEL4	DRM	Allow						General	
9	VPJP010000000302	LEVEL1,LEVEL2,LEVEL3	DRM	Allow	24:00:00					General	30
10	TMJP010000000303	LEVEL1,LEVEL2,LEVEL3,LEVEL4	DRM	Forbid	24:00:00					General	30
11	SMJP010000000303	LEVEL1,LEVEL2,LEVEL3,LEVEL4	DRM	Forbid	24:00:00					General	30
12	TMJP010000000304	LEVEL1,LEVEL2,LEVEL3,LEVEL4	DRM	Forbid	72:00:00			2008/09/01 0:0:0-2008/09/30 11:59:59		General	30
12	TMJP010000000304	LEVEL1,LEVEL2,LEVEL3	DRM	Forbid	240:00:00			2008/07/01 0:0:0-2008/08/31 11:59:59		General	30
13	VPJP010000000305	LEVEL1,LEVEL2,LEVEL3,LEVEL4	DRM	Allow						General	
14	VPJP010000000306	LEVEL1,LEVEL2,LEVEL3	DRM	Forbid	48:00:00	0:30:00		2008/05/01 0:0:0-2008/06/30 11:59:59		General	30
14	VPJP010000000306	LEVEL1,LEVEL2,LEVEL3	DRM	Forbid	240:00:00	0:00:30		2008/04/01 0:0:0-2008/06/30 11:59:59		General	30
15	VPJP010000000501	LEVEL1,LEVEL2,LEVEL3	DRM	Allow						General	
16	VPJP010000000502	LEVEL1,LEVEL2,LEVEL3	DRM	Allow						General	
17	VPJP010000000503	LEVEL1,LEVEL2,LEVEL3	DRM	Allow						General	
18	SMJP010000000504	LEVEL1,LEVEL2,LEVEL3		Allow						General	
19	VPJP010000000601	LEVEL1,LEVEL2,LEVEL3,LEVEL4	DRM	Forbid						General	
20	VPJP010000000602	LEVEL1,LEVEL2,LEVEL3	DRM	Forbid						General	
21	VPJP010000000603	LEVEL1,LEVEL2,LEVEL3	DRM	Allow						General	
22	VPJP010000000604	LEVEL1,LEVEL2,LEVEL3	DRM	Allow						General	
23	VPJP010000000605	LEVEL1,LEVEL2,LEVEL3	DRM	Allow						General	
24	VPJP010000000701	LEVEL1,LEVEL2,LEVEL3	DRM	Allow					1	General	

Légende

Anglais	Français
Playback Usage Condition	Condition d'utilisation en lecture
NO	N°
Quality Parameter	Paramètre de qualité
Playlist	Liste de lecture
Num of Playback	Nombre de lectures
Num of Playback Hours	Nombre d'heures de lecture
Num of Playback Days	Nombre de jours de lecture
Playback period	Période de lecture
Simultaneous Output	Sortie simultanée
Parental Guidance	Guide parental
Countable Time (Seconds)	Temps comptabilisable (secondes)
Level1, Level2….	
Allow	Autorisation
General	Général
Forbid	Interdiction

Tableau B.3 – Condition d'utilisation en impression

		Print usage condition						
	Content ID		Permission Management Type	Num of Printouts	Num of Printout Hours	Num of Printout Days	Printout Period	Parental Guidance
10	TMJP010000000303	LEVEL1,LEVEL2,LEVEL3	DRM	1				General
12	TMJP010000000304	LEVEL1,LEVEL2,LEVEL3,LEVEL4	DRM	10			2008/09/01 0:0:0-2008/09/30 11:59:59	General
12	TMJP010000000304	LEVEL1,LEVEL2,LEVEL3,LEVEL4	DRM	3			2008/09/01 0:0:0-2008/09/30 11:59:59	General

Légende

Anglais	Français
Print usage condition	Condition d'utilisation en impression
Content ID	Identifiant de contenu
Permission Management Type	Type de gestion d'autorisation
Num of Printouts	Nombre d'impressions
Num of Printout Hours	Nombre d'heures d'impression
Num of Printout Days	Nombre de jours d'impression
Printout Period	Période d'impression
Parental Guidance	Guide parental
General	Général

Tableau B.4 – Condition d'utilisation en exécution

		Execute usage contition							
	Content ID		Permission Management Type	Num of Executions	Num of Execution Hours	Num of Execution Days	Execution Period	Parental Guidance	Countable Time (Seconds)
25	PGJP010000000101	LEVEL1,LEVEL2,LEVEL3	DRM				2008/06/20 0:0:0-2008/06/27 23:59:59	General	
26	PSJP010000000101	LEVEL1,LEVEL2,LEVEL3	DRM				2008/06/20 0:0:0-2008/06/30 23:59:59	General	

Légende

Anglais	Français
Execute usage condition	Condition d'utilisation en exécution
Content ID	Identifiant de contenu
Permission Management Type	Type de gestion d'autorisation
Num of Executions	Nombre d'exécutions
Num of Execution Hours	Nombre d'heures d'exécution
Num of Execution Days	Nombre de jours d'exécution
Execution Period	Période d'exécution
Parental Guidance	Guide parental
Countable Time (Seconds)	Temps comptabilisable (secondes)
General	Général

Tableau B.5 – Condition de gestion des données

Data management condition											
NO	Content ID	Target ID	Encryption Flag	Copy Count	Move Count	Transcode Type	Maximum Transcode Rate	Minimum Transcode Rate	Expiration Date	Sublicense Count	Timeline Edit
1	SMJP010000000201	UJPD010000000201	TRUE	ff	0				2008/09/26 0:0:0	0	Forbid
2	VPJP010000000202	UJPD010000000101	TRUE	0	1				2008/12/31 0:0:0	0	Forbid
3	SMJP010000000210	UJPD010000000201	TRUE	0	0				2008/07/31 0:0:0	0	Forbid
6	SMJP010000000221	UJPD010000000101	TRUE	0	0				9999/12/31 0:0:0	0	Forbid
8	VPJP010000000301		TRUE	ff	0				9999/12/31 0:0:0	0	Allow
10	TMJP010000000303	UJPD010000000101	TRUE	0	0				9999/12/31 0:0:0	0	Forbid
11	SMJP010000000303	UJPD010000000101	TRUE	0	0				9999/12/31 0:0:0	0	Forbid
12	TMJP010000000304	UJPD010000000101	TRUE	0	0				9999/12/31 0:0:0	0	Forbid
15	VPJP010000000501	UJPD010000000201	TRUE	ff	0				2009/03/26 0:0:0	ff	Forbid
17	VPJP010000000503		TRUE	ff	0				9999/12/31 0:0:0	0	Allow
18	SMJP010000000504	UJPD010000000201	TRUE	ff	0				9999/12/31 0:0:0	0	Forbid
19	VPJP010000000601	UJPD010000000201	TRUE	ff	0				9999/12/31 0:0:0	0	Forbid
21	VPJP010000000603	UJPD010000000201	TRUE	ff	0				9999/12/31 0:0:0	0	Forbid
22	VPJP010000000604	UJPD010000000201	TRUE	ff	0				9999/12/31 0:0:0	0	Forbid
23	VPJP010000000605	UJPD010000000201	TRUE	ff	0				9999/12/31 0:0:0	0	Forbid
24	VPJP010000000701		TRUE	9	ff				9999/12/31 0:0:0	0	Allow
25	PGJP010000000101	UJPD010000000101	FALSE	0	0				2008/06/30 23:59:59	0	Forbid
26	PSJP010000000101	UJPD010000000101	FALSE	0	0				2008/06/30 23:59:59	0	Forbid

Légende

Anglais	Français
Data management condition	Condition de gestion des données
NO	N°
Target ID	Identifiant cible
Content ID	Identifiant de contenu
Encryption Flag	Indicateur de chiffrement
Copy Count	Compte de copies
Move Count	Compte de déplacements
Transcode Type	Type de transcodage
Maximum Transcode Rate	Vitesse de transcodage maximale
Minimum Transcode Rate	Vitesse de transcodage minimale
Expiration Date	Date d'expiration
Sublicense Count	Compte de sous-licences
Timeline Edit	Edition de référence de temps
Forbid	Interdiction
Allow	Autorisation
True	
False	

Tableau B.6 – Condition de sortie des données

Data export condition										
NO	Content ID	Storage Media Type	Encoding Type	Protection Type	Control Type	Move Indicator Flag	Export Count	Time Period	Day Count	Export Period
1	SMJP010000000201	CD								
13	VPJP010000000305	DVD	MPEG*2,H.264	CPRM, DTCP	Copy No More		Copy 9			
15	VPJP010000000501	CD								
16	VPJP010000000502	DVD	MPEG*2,H.264	CPRM	Copy No More		Copy 3			
17	VPJP010000000503	HDD		SAFIA	Copy No More		Copy 10			
18	SMJP010000000504	Flash Memory		CPRM	Copy No More		Copy 10			

Légende

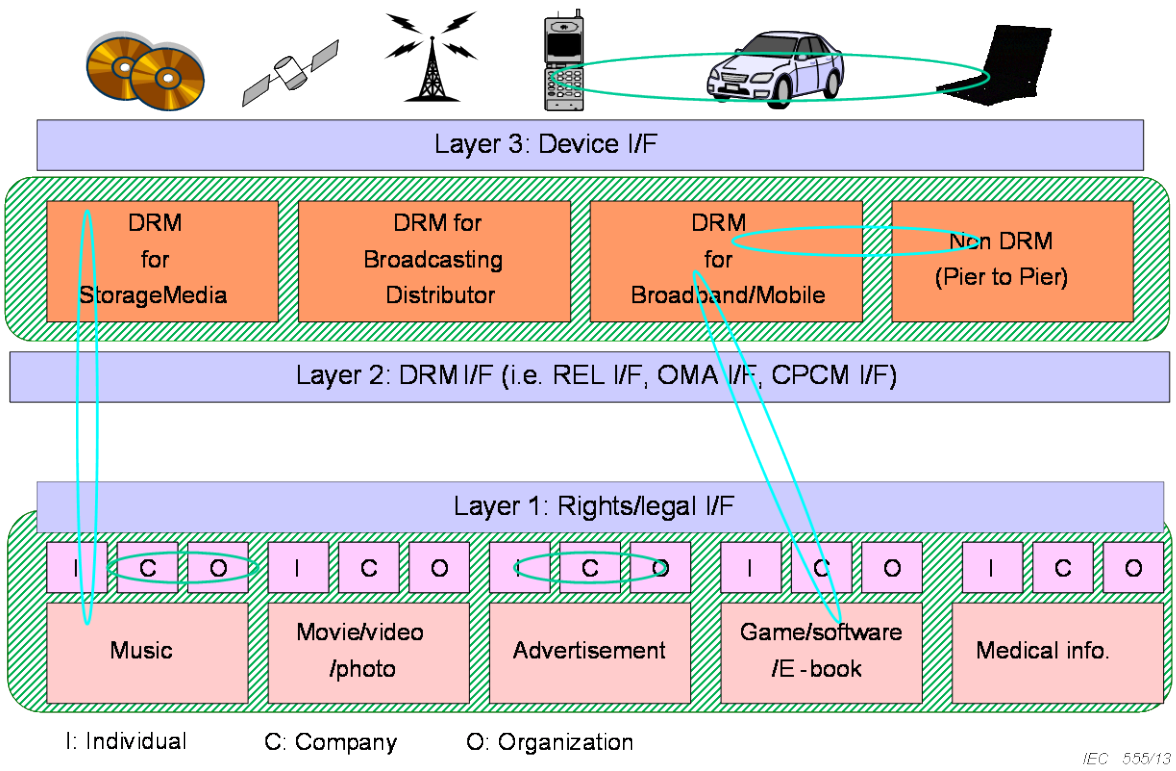
Anglais	Français
Data export condition	Condition d'export des données
NO	N°
Content ID	Identifiant de contenu
Storage Media Type	Type de support de stockage
Encoding Type	Type de codage
Protection Type	Type de protection
Control Type	Type de contrôle
Move Indicator Flag	Indicateur de déplacement
Export Count	Compte d'export
Time Period	Période de temps
Day Count	Compte de jours
Export Period	Période d'export
Copy No More	Plus de copie
Copy 9	Copie 9
Copy 3	Copie 3
Copy 10	Copie 10
Flash Memory	Mémoire flash

Annexe C
(informative)

Interopérabilité d'information des droits, arrière-plan

C.1 Généralités

La distribution de contenu numérique ou de travail numérique protégé par des droits d'auteur a déjà été étudiée sous divers aspects. Du point de vue de la distribution des informations numériques en particulier, divers systèmes de DRM (gestion des droits numériques) ont été proposés et divers modèles de distribution, par exemple «superdistribution» ont été proposés. Toutefois, bien que la technologie et l'infrastructure permettant de prendre en charge la distribution numérique soient désormais en place, il n'existe aucun mécanisme ni règle de distribution numérique souple permettant d'échanger facilement un contenu sur la base d'engagements individuels entre créateurs et consommateurs de contenu. La réalité est qu'actuellement, un environnement technologique et social de confiance entre les détenteurs de droits d'auteur et les consommateurs sécurisant la distribution d'informations n'est pas toujours parfaitement fourni.



Légende

Anglais	Français
Layer 3: Device I/F	Couche 3: Interface de dispositif
DRM for StorageMedia	DRM pour support de stockage
DRM for Broadcasting Distributor	DRM pour distributeur de diffusion
DRM for Broadband/Mobile	DRM pour large bande/mobile
Non DRM (pier to pier)	Non DRM (homologue à homologue)
Layer 2: DRM I/F (i.e. REL I/F, OMA I/F, CPCM I/F)	Couche 2: Interface DRM (c'est-à-dire interface REL, interface OMA, interface CPCM)
Layer 1: Rights/legal I/F	Couche 1: Interface droits/légale

Anglais	Français
Music	Musique
Movie/Video/Photo	Film/vidéo/photo
Advertisement	Publicité
Game/Software/E-Book	Jeu/logiciel/livre électronique
Other (i.e. News, Medical info. Patent info.)	Autre (c'est-à-dire informations, informations médicales, informations brevet)
I: Individual	I: Individu
C: Company	C: Société
O: Organization	O: Organisme

Figure C.1 – Concept – Interopérabilité des informations des droits

En considérant les films comme cas types, la création de contenu est généralement un effort de groupe et les responsabilités sont partagées entre plusieurs personnes. En conséquence, il existe une incertitude sur les droits financiers et personnels relatifs au contenu final et à la compensation, devant être partagés entre ces personnes. Puisqu'il n'a encore été établi aucune technologie pour gérer les tarifs d'usage en se basant sur le volume de contenu consommé, il est difficile d'affirmer qu'une compensation appropriée est distribuée d'une manière cohérente à tous les membres d'un groupe.

Le résultat est que bien que les créateurs de contenu souhaitent que leur contenu soit utilisé beaucoup plus souvent par les consommateurs, aucun système ne le permet. En conséquence, aucun engagement d'autorisation approprié n'est présenté et chaque personne impliquée doit accepter la perte d'opportunités. De plus, le développement de la technologie des téléphones portables et des terminaux simples rendant les contenus disponibles au consommateur, constituant l'avant-garde de la consommation de contenu, progresse sans que les sociétés en concurrence ne parviennent à une interopérabilité. Paradoxalement, ceci entraîne un plus grand nombre d'inconvénients pour le consommateur. De plus, bien que des DRM ayant un certain niveau de fonctionnalité soient disponibles, ils ne satisfont pas nécessairement aux besoins des clients. Les clients sont donc obligés d'acheter un contenu par des moyens malcommodes même s'il est technologiquement possible de les leur rendre plus commode.

L'interopérabilité des informations des droits (RII) permet d'étudier des mesures pour résoudre ces problèmes de deux points de vue. Le premier est l'ingénierie: Construction de l'infrastructure pour une génération suivante de systèmes de distribution d'informations numériques en développant une technologie permettant d'obtenir une combinaison d'interopérabilité et de commodité pour le consommateur. Le second est la loi: établissement de l'infrastructure sociale pour le traitement des droits de la génération suivante en fournissant un nouveau cadre pour la gestion et l'échange d'informations d'autorisation des droits numériques entre les détenteurs et les consommateurs de droits. La RII constitue la norme d'un système idéal permettant de fusionner les deux et facilitant une interopérabilité devenant une réalité pour des groupes de systèmes de DRM existants dispersés dans le monde.

C.2 Relation entre les droits et les autorisations numériques

Les autorisations de droits numériques sont les composants spécifiques au moyen desquels les droits sont exercés.

Les détenteurs des droits définis dans la loi actuelle sur les droits d'auteur ne contribuent pas à la distribution de contenu s'ils n'utilisent pas efficacement ces droits, même s'ils les détiennent. Malheureusement, dans la plupart des situations où des droits sont exercés, les

autorisations des droits numériques sont souvent utilisées comme des composants permettant d'exercer des poursuites lorsque des droits sont enfreints.

L'action d'octroi d'autorisations de droits numériques est une action constituant un accord entre des détenteurs (multiples) détenant des droits déclarés et des détenteurs (multiples) n'ayant pas de droits relatifs à la loi sur les droits d'auteur mais devant confirmer l'octroi ou le refus des autorisations pour une utilisation commerciale. Elle confirme également qu'il est acceptable d'activer des services de consommation de contenus spécifiques.

Une distribution correcte de contenu doit inclure les actions mutuelles d'octroi et de réception des autorisations des droits numériques (sans nécessiter beaucoup de temps si possible). Les droits explicites et les droits potentiels montrent que les détenteurs de droits sont d'accord sur le fait que «pour octroyer entièrement toutes les autorisations = il est acceptable d'activer les services de consommation de contenu spécifique» et si ceci n'est pas confirmé, la situation n'est pas une situation ou des autorisations de droits numériques ont été obtenus. Toutefois, toutes ces autorisations ne peuvent pas être confirmées dans les divers accords de licence entre les parties impliquées (voir l'exemple ci-dessous). C'est la raison pour laquelle on se heurte aux limitations de la loi. La technologie permet de les compenser.

De façon spécifique,

a) la technologie du langage de codage comportant les éléments partagés identifiant le contenu dispersé et les parties associées à ce contenu,
b) la technologie du langage de codage comportant les éléments partagés identifiant des informations concernant les services de consommation de contenu spécifique.

Ces deux composantes convertissent en données numériques les informations les plus récentes concernant les relations contractuelles multicouches entremêlées et montrent que les détenteurs de droits sont d'accord pour qu'il soit acceptable d'activer les services de consommation de contenu spécifique pour le contenu ayant été converti en données numériques. Les services, applications et dispositifs interprètent technologiquement cet accord et permettent une consommation légale du contenu.

RII signifie «Interopérabilité des informations des droits». Ceci est synonyme de la gestion des informations d'autorisation des droits numériques continuellement mis à jour. Les composantes a) et b) ci-dessus assurent comme condition minimale que tous les droits définis dans la loi existante sur les droits d'auteur sont exprimés. Ceci doit également garantir une possibilité d'extension future, ce qui signifie que tout nouvel «accord acceptable pour activer des services de consommation de contenu spécifique» apparaissant dans l'avenir sera également exprimé technologiquement.

Exemple

Le représentant du détenteur de droits B pour le film A octroie à un distributeur chinois des droits de projection comme stipulé dans la loi japonaise sur les droits d'auteur.

↓

Le consommateur chinois G profite du film A appartenant au représentant du détenteur de droits japonais B.

Le lit-il en continu?

Le télécharge-il?

Possède-t-il un support d'enregistrement?

En d'autres termes, ceci ne peut pas être exprimé en utilisant les seules techniques légales actuellement existantes. Si par exemple la société détentrice de droits H octroyant les autorisations de droits pour le contenu du film A entre dans un accord de licence d'utilisation

de contenu B2B (Business to Business) avec le distributeur U, qui exploite un commerce de téléchargement, il n'est pas possible de saisir à l'avance l'ensemble des formats de services spécifiques. Si l'on imagine en particulier que des services qui ne sont pas encore connus seront activés dans l'avenir, les employés responsables des services juridiques doivent tout mettre en œuvre pour pouvoir créer des documents de plus en plus denses et illisibles prédisant les formes de consommation de contenu (tel peut être le cas, mais il existe également des limites au nombre possible d'énumérations des utilisations étendues de règlements d'utilisation juste et de règlements de limite des droits). L'accord de licence physique mentionne généralement l'accord. Sinon, il n'existe qu'un accord général et il n'existe pas d'accord de licence réel ou de relation contractuelle. Dans ce cas, avant d'obtenir un accord de licence, il est essentiel que la gestion des informations de consommation de contenu soit répercutée par la technologie pour gérer légalement les formes de consommation ciblée à des consommateurs finaux différenciés plus précisément.

Octroi d'autorisations de droits numériques ⇔ Réception d'autorisations de droits numériques

c) Cas où le contenu détenu et contrôlé est utilisé et dans cette forme de consommation fait l'objet d'un accord dans une relation contractuelle antérieure.

d) Cas où le contenu détenu et contrôlé est utilisé et dans cette forme de consommation ne fait pas l'objet d'un accord dans une relation contractuelle antérieure;

   1) cas où il est possible d'obtenir une autorisation après consommation;

   2) cas où il n'est pas possible d'obtenir une autorisation après consommation.

Dans une future distribution de contenu, il est souhaitable que ces informations soient intégrées à l'avance dans le contenu dans un certain format (sans faire de distinction entre le numérique et l'analogique).

Annexe D
(informative)

Deux technologies de base pour activer la RII

D.1 Technologie du langage de codage comportant des éléments partagés identifiant le contenu dispersé et les parties associées à ce contenu

D.1.1 Généralités

A l'ère numérique, la technologie numérique et les environnements en réseau sont utilisés et il existe une large diversité de contenus et de créateurs et utilisateurs de contenu. Les informations qui les concernent sont enregistrées dans la langue maternelle de chaque pays sous forme de métadonnées concernant les droits et ces informations sont traduites à l'occasion dans une autre langue. Même si la signification individuelle qu'elle souligne est la même, il existe un grand nombre de cas où les métadonnées concernant les droits se multiplient ou sont dupliquées. On détermine une technologie de langage de codage simplifiant ces éléments de métadonnées concernant les droits dans la mesure du possible et exprimant leurs éléments communs.

D.1.2 Métadonnées concernant les droits et code d'identification de balisage simple

Les métadonnées concernant les droits sont un terme générique pour les informations environnantes et associées à un objet de consommation et de divertissement (film, musique, photos, etc.) appelé contenu ou produit, etc.

Les métadonnées concernant les droits peuvent être divisées grossièrement en trois types.

a) Métadonnées ouvertes

   Des exemples de métadonnées ouvertes comportent le nom de produit, l'auteur officiel, etc.

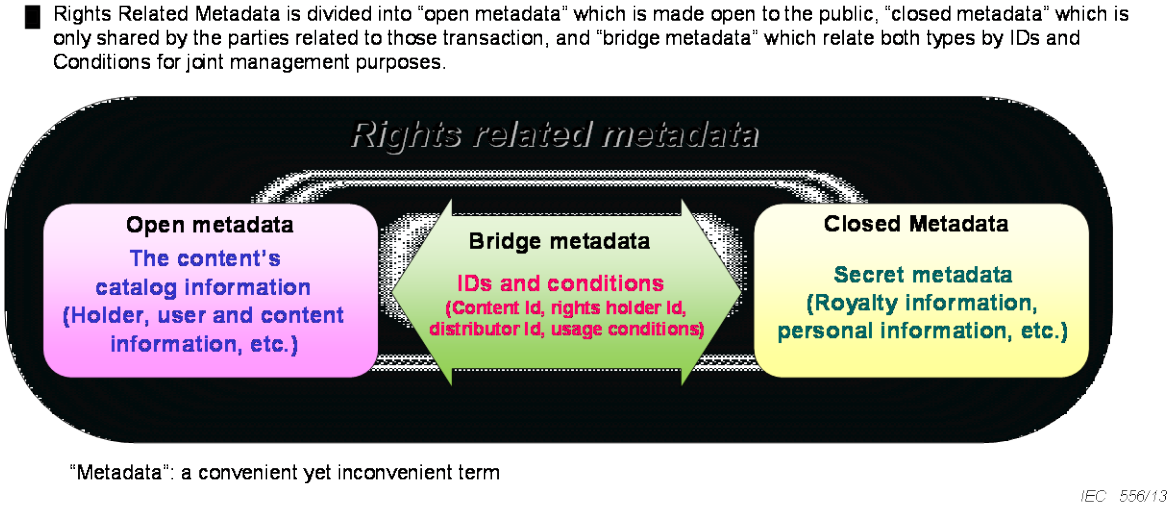
b) Métadonnées fermées

   Des exemples de métadonnées fermées comportent le nom réel de l'auteur, les informations bancaires, etc.

c) Métadonnées de pont

   Les métadonnées de pont sont constituées de l'identifiant partagé ou du code de format d'utilisation détaillé reliant les groupes de métadonnées a) et b).

L'illustration suivante montre les relations entre a), b) et c).



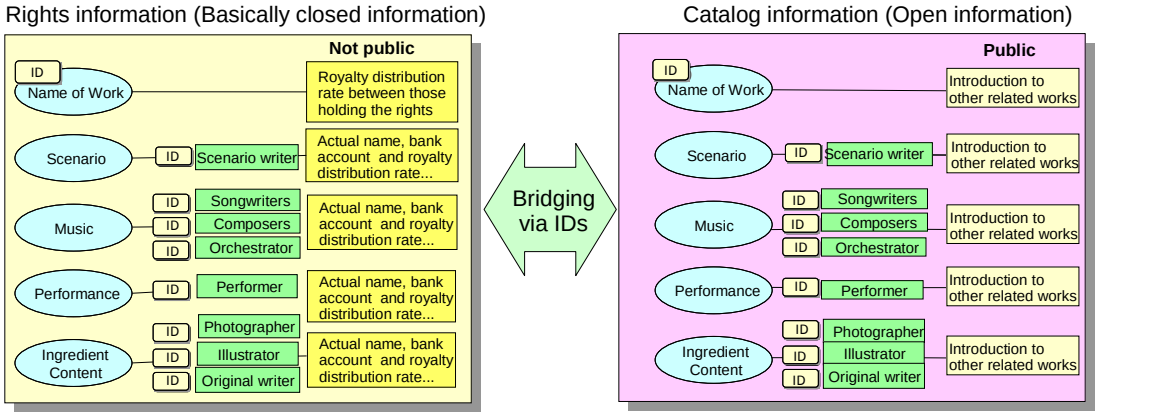
Légende

Anglais	Français
Rights Related Metadata is divided into “open metadata” which is made open to the public, “closed metadata” which is only shared by the parties related to those transactions, and “bridge metadata” which relate both types by IDs and Conditions for joint management purposes.	Métadonnées concernant les droits est divisé en «métadonnées ouvertes» rendues ouvertes au public, «métadonnées fermées» partagées uniquement par la transaction associée aux parties et «métadonnées de pont» concernant les deux types par identifiants et conditions pour gestion commune.
Rights Related Metadata	Métadonnées concernant les droits
Open Metadata	Métadonnées ouvertes
The content's catalog information (Holder, user and content information, etc.)	Informations du catalogue de contenu (informations sur le détenteur, l'utilisateur et le contenu, etc.)
Bridge Metadata	Métadonnées de pont
IDs and Conditions (Content Id, rights holder Id, distributor Id, usage conditions)	Identifiants et conditions (identifiant de contenu, Identifiant de détenteur des droits, Identifiant de distributeur, conditions d'utilisation)
Closed Metadata	Métadonnées fermées
Secret metadata (Royalty information, personal information, etc.)	Métadonnées secrètes (informations sur les royalties, informations personnelles, etc.)
“Metadata”: a convenient yet inconvenient term	«Métadonnées» terme commode et malcommode

Figure D.1 – Sémantique commune des métadonnées

L'illustration suivante montre un exemple d'utilisation pratique d'identifiants partagés dans des métadonnées de pont.

- As various rights holders are involved with content such as audi c- visual work, the consolidation of name-list information is needed for determining the actual rights holders and the royalties to pay them.
- This name-list information is necessary in the context of “closed information,” shared information that is necessary for contracts etc. among content holders and rights holders only, and also in the context of “open information,” catalog- like information for the purpose of gaining a deeper knowledge r egarding the content in question, between content holders and users or users and consumers.
- For this reason, it is effective to carry out information bridgi ng for both parties, using Rights Holder IDs as a means for association.



Légende

Anglais	Français
As various rights holders are involved with content such as audio-visual work, the consolidation of name-list information is needed for determining the actual rights holders and the royalties to pay them.	Puisque divers détenteurs de droits sont impliqués avec le contenu tel qu'un travail audiovisuel, la consolidation des informations de liste de noms est nécessaire pour déterminer les détenteurs de droits réels et les royalties qui leur sont dues.
This name-list information is necessary in the context of “closed information”, shared information that is necessary for contracts etc. among content holders and right holders only, and also in the context of “open information”, catalog-like information for the purpose of gaining a deeper knowledge regarding the content in question, between content holders and users or users and consumers.	Ces informations de liste de noms sont nécessaires dans le contexte des «informations fermées», informations partagées qui sont nécessaires pour les contrats, etc. entre les détenteurs de contenu et les détenteurs de droits seulement et aussi dans le contexte des «informations ouvertes», informations de type catalogue ayant pour but d'obtenir une connaissance plus approfondie du contenu en question, entre les détenteurs de contenu et les utilisateurs ou entre les utilisateurs et consommateurs.
For this reason, it is effective to carry out information bridging for both parties, using Rights Holder IDs as a means for association.	Pour cette raison, il est efficace d'effectuer un pontage d'informations pour les deux parties, en utilisant les identifiant de détenteurs de droits comme moyen d'association.
Rights Information (Basically Closed Information)	Informations sur les droits (informations fondamentalement fermées)
Catalog Information (Open Information)	Informations de catalogue (informations ouvertes)
ID	Identifiant
Name of Work	Nom du travail
Not Public	Non public
Royalty distribution rate between those holding the rights	Taux de distribution des royalties entre les détenteurs des droits
Public	Public
Introduction to other related works	Introduction à d'autres travaux associés
Scenario	Scénario

Anglais	Français
Scenario writer	Scénariste
Actual name, bank account and royalty distribution rate…	Nom réel, compte bancaire et taux de distribution des royalties…
Music	Musique
Songwriters	Auteurs
Composers	Compositeurs
Orchestrator	Orchestrateur
Performance	Interprétation
Performer	Interprète
Ingredient Content	Contenu des ingrédients
Photographer	Photographe
Illustrator	Illustrateur
Original writer	Ecrivain original
Bridging via IDs	Pontage par l'intermédiaire d'identifiants

Figure D.2 – Nécessité de consolidation des informations pour la distribution de contenu

D.1.3 Système de partage d'identifiants

Afin de faciliter la distribution de contenu à partir de maintenant, il est essentiel que les identifiants pour identifier le contenu, les détenteurs de droits et les utilisateurs soient couramment utilisés par les bases de données, et que les mécanismes pour rendre l'accès de l'extérieur soit améliorés. Pour cette raison, le système d'identification commune est nécessaire. L'affectation d'identifiants communs entre les organisations respectives et les entités commerciales servira efficacement une telle fonction.

a) Identifiant de contenu

A l'ère numérique, il existe une multitude de fichiers numériques fonctionnant comme maîtres sur le réseau ou à l'extérieur. La CEI 62227 spécifie la structure du récipient transportant l'identifiant de contenu sur le système d'identifiants partagés. Le système d'identifiants partagés a été défini pour identifier ce contenu de manière unique. Il comporte 16 chiffres au total. Les types de contenus consommés sont d'abord divisés en cinq attributs généraux. Ces attributs globaux sont ensuite agencés en genres déterminés et l'attribut de consommation de contenu est exprimé en utilisant deux chiffres. Le pays d'origine de ce contenu et ensuite exprimé en utilisant les codes de pays WIPO sur 2 chiffres.

Par exemple, un contenu de film créé au Japon est exprimé par VPJP~. «VP» est l'abréviation de «Visual Program» (programme visuel). De façon similaire, un contenu photographique créé au Japon est exprimé par «IPJP~», où «IP» est l'abréviation de «programme d'image».

b) Identifiant commercial

1) Identifiant de détenteur de droits

La CEI 62227:2008, 5.5.5, spécifie la structure du récipient transportant l'identifiant de détenteur de droits sur le système d'identifiants partagés. Il s'agit d'un identifiant qui identifie généralement les créateurs, les détenteurs individuels de droits, les sociétés détentrices de droits et les organismes de droits associés au contenu identifié en utilisant l'identifiant de contenu ci-dessus.

2) Identifiant d'utilisateur

La CEI 62227:2008, 5.5.6, spécifie la structure du récipient transportant l'identifiant d'utilisateur sur le système d'identifiant partagé. Il s'agit d'un identifiant qui identifie

généralement le distributeur, le diffuseur, le consommateur final, le dispositif détenu par le consommateur et le groupe de services utilisé par le consommateur, en utilisant le contenu identifié à l'aide de l'identifiant de contenu ci-dessus.

D.2 Technologie du langage de codage comportant les éléments partagés des services de consommation de contenu spécifique

D.2.1 Généralités

Transporte et exprime les éléments partagés de services de consommation de contenus spécifiques différenciés ne pouvant pas être entièrement exprimés en utilisant les droits englobés par la loi sur les droits d'auteur. La CEI 62227 spécifie le composant de classification d'autorisation et le composant de limitation d'autorisation pour les services de client de contenu spécifique.

D.2.2 Classification

La classification est constituée de sept éléments définis d'un point de vue particulièrement légal. Quatre éléments fondamentaux du contenu en question doivent être écrits dans tous les accords de licence:

a) but de l'utilisation;

b) le fait que la consommation de contenu est payante ou gratuite et le fait qu'il y ait ou non un mandataire;

c) format de consommation d'utilisation spécifique;

d) territoire de la consommation d'utilisation.

De plus, il existe des points dans ces quatre éléments qui codent

- le fait que ces quatre éléments soient ou non ouverts au public et
- si ces quatre éléments correspondent aux demandes et déclarations pour le traitement des droits B2B.

D.2.3 Composants limites

Les quatre éléments principaux décrits ci-dessus doivent fondamentalement être codés. En revanche, les composants limites ne sont codés que si un codage est requis. Il existe toutefois des composants exprimant des informations concernant la DRM ou des informations concernant les services les plus récents pris en charge par une nouvelle technologie pouvant apparaître dans l'avenir. Il y a sept éléments qui doivent être utilisés:

a) Composants limites personnels

Lorsqu'on utilise les services de distribution GC (contenu de groupe), il est possible d'effectuer des associations et regroupements au delà des genres de contenu.)

– Autorisation de compilation (gratuit, par produit, par album, compilation d'un même artiste, compilation au sein de la même société).

b) Composant de commande de mise en œuvre de machine de transmission et de distribution

– Commande CM (gratuit: consentement pour ignorer CM, refus d'ignorer CM, visualisation forcée synchronisée dans le temps, avant et après visualisation, visualisation personnalisée dans le temps, couverture).

c) Composant de limite de qualité

– Composant de limite de support d'enregistrement (voir la CEI 62227:2008, 5.10.4.4, storage_media_type).

d) Norme de format de compression (voir la CEI 62227:2008, 5.9.3.6, transcode type)

e) Composant de limite de débit binaire (voir la CEI 62227:2008, 5.9.3.7, maximum transcode rate)

f) Composant de limite de durée de vie (commande de durée de vie) (gratuit, comptage limité, limite de période de temps, limite d'expiration)

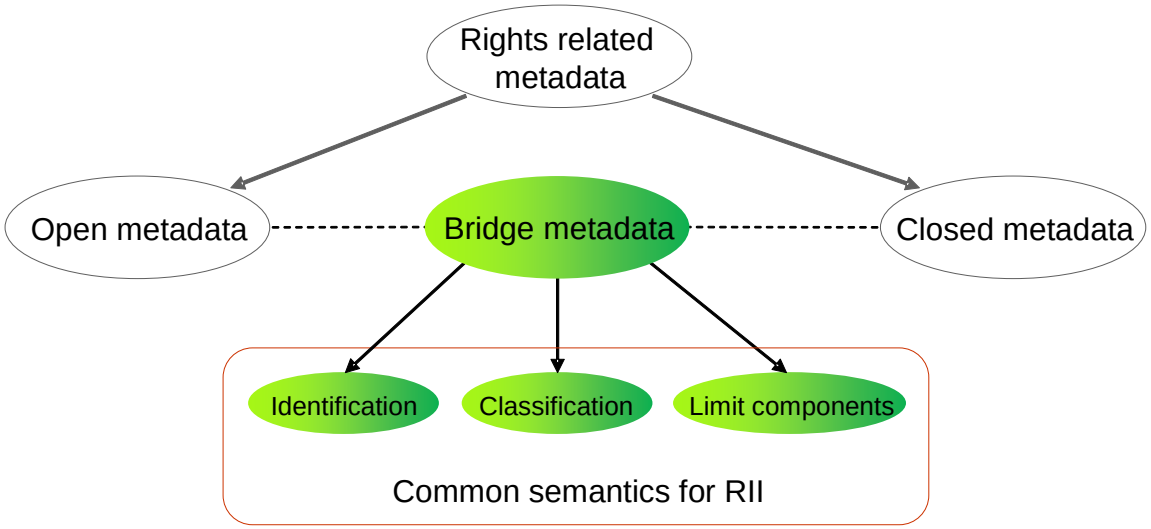
g) Composants de limite de sécurité (filigrane, DRM, rapports de droits).

D.3 Sémantique commune pour RII

La RII représente des métadonnées de pont réunissant les informations ouvertes et les informations fermées par des identifiants et des conditions.

Les métadonnées de pont sont divisées en «Identification» permettant d'identifier le détenteur de contenu, l'utilisateur de contenu et le contenu lui-même, «Classification» permettant d'associer les classifications d'autorisation et «Limit components» permettant d'associer les conditions d'autorisation sur les accords.

La sémantique commune pour la RII est constituée de «Identification», «Classification» et «Limit components», voir la Figure D.3.



Légende

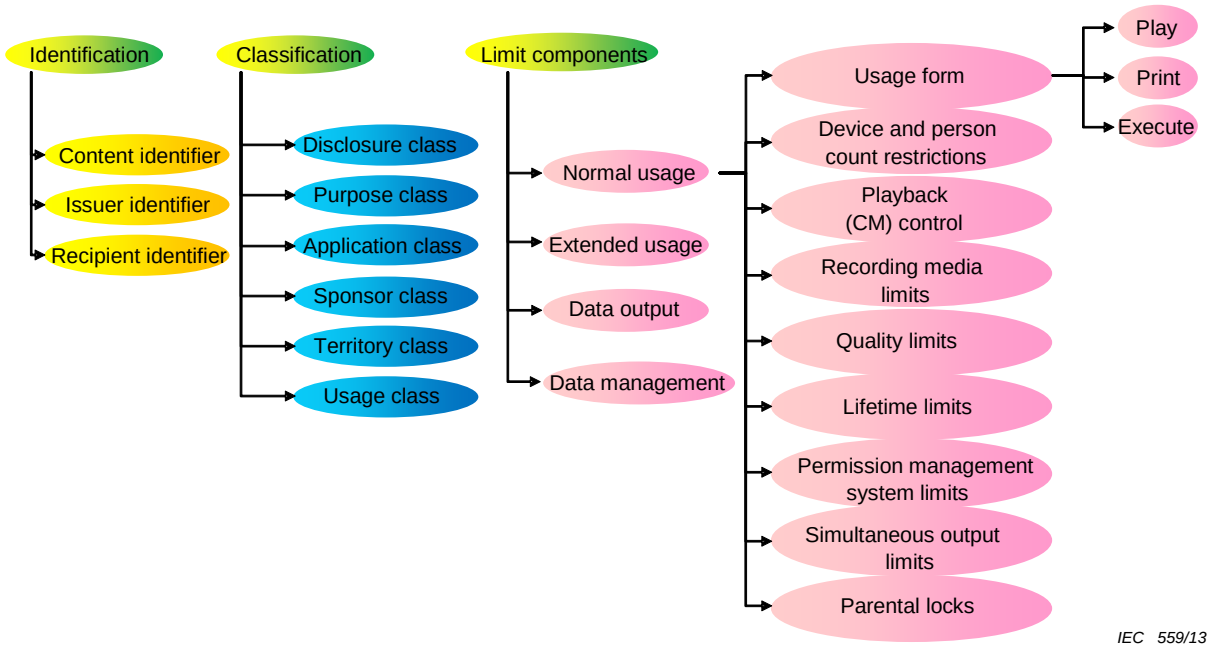
Anglais	Français
Rights related metadata	Métadonnées concernant les droits
Open metadata	Métadonnées ouvertes
Bridge metadata	Métadonnées de pont
Closed metadata	Métadonnées fermées
Identification	Identification
Classification	Classification
Limit components	Composants limites
Common semantics for RII	Sémantique commune pour la RII

Figure D.3 – Sémantique commune pour la RII

D.4 Éléments fondamentaux et sémantique commune pour la RII

Chaque composant pour la RII est divisé en éléments fondamentaux qui sont réalisés pour spécifier les détails des informations de pont.

La Figure D.4 présente les éléments fondamentaux et la sémantique commune pour la RII.



Légende

Anglais	Français
Identification	Identification
Classification	Classification
Limit components	Composants limites
Content identifier	Identifiant de contenu
Issuer identifier	Identifiant d'émetteur
Recipient identifier	Identifiant de récepteur
Disclosure class	Classe Disclosure
Purpose class	Classe Purpose
Application class	Classe Application
Sponsor class	Classe Sponsor
Territory class	Classe Territory
Usage class	Classe Usage
Normal usage terms	Termes d'utilisation normale
Extended usage terms	Termes d'utilisation étendue
Data output terms	Termes de sortie des données
Data management terms	Termes de gestion des données
Usage form	Formulaire d'utilisation
Device and person count restrictions	Restrictions de dispositif et de compte de personne
Playback (CM) control	Contrôle de lecture (CM)

Anglais	Français
Recording media limits	Limites de support d'enregistrement
Quality limits	Limites de qualité
Lifetime limits	Limites de durée de vie
Permission management system limits	Limites du système de gestion d'autorisation
Simultaneous output limits	Limites de sorties simultanées
Parental locks	Verrouillages parentaux
Play	Lecture
Print	Impression
Execute	Exécution

Figure D.4 – Eléments fondamentaux et sémantique commune pour la RII

Annexe E
(informative)

Eléments de la RII correspondant à une DRM existante

Les Tableaux E.1 à E.11 présentent les éléments RII (Interopérabilité des informations des droits) correspondant aux éléments DRM (Gestion des droits numériques) existants en détail.

Tableau E.1 – Marlin BB

Elements of content protection	Marlin BB
Distribution format	Content independent Support following container for transporting content data • MP4 ISO/IEC 14496-14:2003 Other
Content usage permission 1) License requirement → confirmation of contract → content distribution 2) Distribution of license	When DRM server receives a license aquisition request from a terminal, it confirms to a customer management system and a contract management system to be able to distribute the requested license. If possible, it distributes the license embedding rendering obligation and output control information (COPY/MOVE/EXPORT) correnspons to the contract. DRM server distributes license bound to the target object which is selected from devices, users, subscriptions and domains in accordance with the order of content distributor. Any license being bound to a device is available to any user who has the right to use the device. Any license being bound to a user is available to the user using any device he has the right to use it. Any license being bound to a subscription is available to any user who has the subscription using any device he has the right to use. Any license being bound to a domain is available to any user using any device belonging to the domain when he has the right to use the device or is available to any user belonging to the domain using any device he has the right to use. Users that have usage rights of devices are registered in the server DRM system for each device.
Management of permission issuer, receiver and issue date	Running dependent Possible to manage through the license distribution log on the center Manage users and devices Manage users that have the right to use the specific device and devices available to the specific user Manage available subscription to use a license; users having the subscription and devices that the users have the rights to use. Manage deletion of the rights for users to use a device dynamically.
License storage on a nonvolatile area in a terminal	Available
License move/copy	Available
Encrypted content storage on a nonvolatile area in a terminal	Available

Elements of content protection		Marlin BB
Content playback control	Playback period	It controls playback and output by a code module running on a VM in a DRM client. Code modules are made on a DRM server and are distributed to DRM clients. Even if conditions of playback and output are being changed, client side is independent from a module or a hardware update. It is sufficient to execute a code module on a VM which is being transported from a DRM server. It is possible to control playback and output flexibly.
	Digital copy control information	
	Serial interface output control	
	Analog output copy control	
	Video quality control information	
	Decoded content data retention mode	
	Decoded content data retention state	
	High speed digital I/F protection information	
	CopyRestrictionMode	
	User-defined information	
Control information for exporting to other DRM		
Content data concealment		AES + SCTE 52
Authentication of DRM systems		Authentication of client DRM and server DRM are implemented by using public certificates which are issued by a certificate authority authorized by MTMO. RSA-DSA (1 024 bit/2 048 bit key) with SHA256 Revocation lists of client DRM and server DRM are available.
Communication protection between DRMs		Concealment of communication data RSA 1 024 bit, 2 048 bit RSA 1.5 | RSA-OAEP AES 128 bit Check a tamper of communication data RSA – SHA 1 | RSA – SHA 256 Secret data concealment between DRM system nodes RSA 1 024 bit, 2 048 bit RSA 1.5 | RSA-OAEP AES 128 bit Check a falsification of secret data between DRM system nodes. HMAC – SHA1 RSA – SHA1 | RSA – SHA256

Légende

Anglais	Français
Elements of content protection	Eléments de protection de contenu
Marlin BB	Marlin BB
Distribution format	Format de distribution
Content independent	Indépendant du contenu
Support following container for transporting content data – MP4 ISO/IEC 14496-14:2003	Support suivant le récipient pour transporter les données de contenu – MP4 ISO/CEI 14496-14:2003
Other	Autre
Content usage permission	Autorisation d'utilisation de contenu
1) License requirement->comfirmation of contract-> content distribution	1) Exigence de licence -> confirmation de contrat -> distribution de contenu

Anglais	Français
2) Distribution of license	2) Distribution de licence
When DRM server receives a license aquisition request from a terminal, it confirms to a customer management system and a contract management system to be able to distribute the requested license.	Lorsqu'un serveur de DRM reçoit une demande d'acquisition de licence d'un terminal, il confirme à un système de gestion de consommateur et un système de gestion de contrat qu'il peut distribuer la licence demandée.
If possible, it distributes the license embedding rendering obligation and output control information (COPY/MOVE/EXPORT) corresponds to the contract.	Il distribue, si possible, la licence incorporant une obligation de restitution et les informations de commande de sortie (COPY/MOVE/EXPORT) correspondent au contrat.
DRM server distributes license bound to the target object which is selected from devices, users, subscriptions and domains in accordance with the order of content distributor.	Le serveur de DRM distribue la licence liée à l'objet sensible qui est sélectionné à partir de dispositifs, utilisateurs, abonnements et domaines conformément à l'ordre du distributeur de contenu.
Any license being bound to a device is available to any user who has the right to use it.	Toute licence associée à un dispositif est disponible pour un utilisateur quelconque ayant le droit d'utilisation.
Any license being bound to a user is available to the user using any device he has the right to use.	Toute licence liée à un utilisateur est disponible à l'utilisateur utilisant un quelconque dispositif qu'il a le droit d'utiliser.
Any license being bound to a subscription is available to any user who has the subscription using any device he has the right to use.	Toute licence liée à un abonnement est disponible à un quelconque utilisateur possédant l'abonnement utilisant un quelconque dispositif qu'il a le droit d'utiliser.
Any license being bound to a domain is available to any user using any device belonging to the domain when he has the right to use the device or is available to any user belonging to the domain using any device he has the right to use.	Toute licence liée à un domaine est disponible à un quelconque utilisateur utilisant un quelconque dispositif appartenant au domaine lorsqu'il a le droit d'utiliser le dispositif ou disponible à tout utilisateur appartenant au domaine utilisant un quelconque dispositif qu'il a le droit d'utiliser.
Users that have usage rights of devices are registered in the server DRM system for each device.	Les utilisateurs ayant des droits d'utilisation de dispositifs sont enregistrés dans le système de DRM du serveur pour chaque dispositif.
Management of permission issuer, receiver and issue date	Gestion de l'émetteur, du récepteur de permission et de la date d'édition
Running dependent	Dépend du fonctionnement
Possible to manage through the license distribution log on the center	Possibilité de gestion par le journal de distribution de licence sur le centre
Manage users and devices	Gestion des utilisateurs et des dispositifs
Manage users that have the right to use the specific device and devices available to the specific user	Gestion des utilisateurs ayant le droit d'utiliser le dispositif spécifique et des dispositifs disponibles à l'utilisateur spécifique
Manage available subscription to use a license; users having the subscription and devices that the users have the rights to use.	Gestion de l'abonnement disponible pour utiliser une licence, les utilisateurs possédant l'abonnement et les dispositifs que les utilisateurs ont le droit d'utiliser
Manage deletion of the rights for users to use a device dynamically.	Suppression de la gestion des droits pour les utilisateurs pour utiliser un dispositif de façon dynamique.
License storage on a nonvolatile area in a terminal	Stockage de licence sur une zone non volatile dans un terminal
Available	Disponible
License move/copy	Déplacement/copie de licence
Encrypted content storage on a nonvolatile area in a terminal	Stockage de contenu chiffré sur une zone non volatile dans un terminal
Content playback control	Contrôle de lecture de contenu
Playback period	Période de lecture
Digital copy control information	Informations de contrôle de copie numérique

Anglais	Français
Serial interface output control	Contrôle de sortie d'interface série
Analog output copy control	Contrôle de copie de sortie analogique
Video quality control information	Informations de contrôle de qualité vidéo
Decoded content data retention mode	Mode de rétention de données de contenu décodé
Decoded content data retention stage	Étage de rétention de données de contenu décodé
High speed digital I/F protection information	Informations de protection d'interface numérique à grande vitesse
CopyRestrictionMode	Mode de restriction de copie
User-defined information	Informations définies par l'utilisateur
Control information for exporting to other DRM	Informations de contrôle pour export vers une autre DRM
It controls playback and output by a code module running on a VM in a DRM client.	Contrôle la lecture et la sortie par un module de code s'exécutant sur un VM dans une DRM cliente
Code modules are made on a DRM server and are distributed to DRM clients.	Les modules de code sont réalisés sur un serveur de DRM et sont distribués aux clients de DRM
Even if conditions of playback and output are changed, client side is independent form a module or a hardware update. It is sufficient to execute a code module on a VM which is transported from a DRM server.	Même si les conditions de lecture et de sortie sont modifiées, le côté client est indépendant d'une mise à jour de module ou de matériel. Il suffit d'exécuter un module de code sur un VM transporté depuis un serveur de DRM.
It is possible to control playback and output flexibly.	Il est possible de contrôler la lecture et la sortie de manière souple.
Content data concealment	Annulation des données de contenu
Authentication of DRM systems	Authentification des systèmes de DRM
Authentication of client DRM and server DRM are implemented by using public certificates which are issued by a certificate authority authorized by MTMO. RSA-DSA (1 024 bit/2 048 bit key) with SHA256	L'authentification du DRM de client et du DRM de serveur est mise en œuvre en utilisant des certificats publics qui sont délivrés par une autorité de certification autorisée par MTMO. RSA-DSA (clé 1 024 bits/2 048 bits) avec SHA256
Revocation lists of client DRM and server DRM are available.	Les listes de révocation de DRM de client et de DRM de serveurs sont disponibles.
Communication protection between DRMs	Protection de communication entre DRM.
Concealment of communication data	Masquage des données de communication
Check a tamper of communication data	Contrôle de fraude des données de communication
Secret data concealment between DRM system nodes	Masquage des données secrètes entre nœuds du système de DRM
Check a falsification of secret data between DRM system nodes	Contrôle de falsification des données secrètes entre nœuds du système de DRM

Tableau E.2 – Marlin IPTV-ES, licence de téléchargement, EXPORT pour copie avec fourniture de clé directe

Elements of content protection		Marlin IPTV-ES
		Download license
		EXPORT for Copy with Direct Key Delivery
Distribution format		Download
Content usage permission 1) License requirement → comfirmation of contract → content distribution 2) Distribution of license		When a DRM server receives a license acquisition request from a terminal, it confirms to a customer management system and contract management system whether the terminal has the rights to get the requested license. If possible, it distributes the license embedding playback control information that corresponds to the contract.
Management of permission issuer, receiver and issue date		Running dependent It is possible to manage a license distribution log in the center.
License storage on a nonvolatile area in a terminal		Available
License move/copy		Only available to export to other DRMs
Encrypted content storage on a nonvolatile area in a terminal		Available
Content usage control	Playback period	
	Digital copy control information	
	Serial interface output control	
	Analog output copy control	
	Video quality control information	
	Decoded content data retention mode	
	Decoded content data retention state	
	High speed digital I/F protection information	
	CopyRestrictionMode	
	User-defined information	
Control information for exporting to other DRM		The following elements are available to specify a playback control information for each media. Export to DTCP. Export to CPRM for DVD. Export to CPRM for SD Video. Export to CPRM for SD Audio. Export to MG-R (SVR) for Memory Stick PRO. Export to MG-R (SAR) for Memory Stick and Memory Stick PRO. Export to VCPS. Export to MG-R (SVR) for EMPR. Export to MG-R (SAR) for ATRAC Audio Device. Export to SAFIA for iVDR TV Recording Export to SAFIA for iVDR Audio Recording Export to AACS Blu-ray Disc Recordable for BD-R/RE. Export to AACS Blu-ray Disc Recordable for Red Laser Media.
Content data concealment		

Elements of content protection	Marlin IPTV-ES
	Download license
	EXPORT for Copy with Direct Key Delivery
Authentication of DRM systems	Authentication of client DRM and server DRM is carried out by using a public key certificate which is issued by authentication center as authorized by MTMO. EC-DSA (224 bit key) with SHA256 Run revocation lists. Client DRM can be revoked by each device. Server DRM can be revoked by license distribution server.
Communication protection between DRMs	EC-DH (224 bit key) + EC-DSA (224 bit key) + AES (128 bit key) + SHA 256

Légende

Anglais	Français
Elements of content protection	Eléments de protection de contenu
Marlin IPTV-ES	Marlin IPTV-ES
Download license	Licence de téléchargement
EXPORT for Copy with Direct Key Delivery	EXPORT pour copie avec fourniture de clé directe
Distribution format	Format de distribution
Download	Téléchargement
Content usage permission	Autorisation d'utilisation de contenu
1) License requirement->comfirmation of contract->content distribution	1) Exigence de licence -> confirmation de contrat -> distribution de contenu
2) Distribution of license	2) Distribution de licence
When a DRM server receives a license aquisition request from a terminal, it confirms to a customer management system and contract management system whether the terminal has the rights to get the requested license	Lorsqu'un serveur de DRM reçoit une demande d'acquisition de licence d'un terminal, il confirme à un système de gestion de consommateur et un système de gestion de contrat si le terminal possède les droits d'obtention de la licence demandée.
If possible, it distributes the license embedding playback control information that corresponds to the contract.	Il distribue si possible la licence incorporant les informations de commande de lecture correspondant au contrat.
Management of permission issuer, receiver and issue date	Gestion de l'émetteur, du récepteur de permission et de la date d'édition
Running dependent	Dépend du fonctionnement
It is possible to manage a license distribution log in the center	Possibilité de gestion par le journal de distribution de licence sur le centre
License storage on a nonvolatile area in a terminal	Stockage de licence sur une zone non volatile dans un terminal
Available	Disponible
License move/copy	Déplacement/copie de licence
Only available to export to other DRMs	Disponible seulement pour export vers d'autres DRM
Encrypted content storage on a nonvolatile area in a terminal	Stockage de contenu chiffré sur une zone non volatile dans un terminal
Content usage control	Contrôle d'utilisation de contenu
Playback period	Période de lecture
Digital copy control information	Informations de contrôle de copie numérique
Serial interface output control	Contrôle de sortie d'interface série
Analog output copy control	Contrôle de copie de sortie analogique

Anglais	Français
Video quality control information	Informations de contrôle de qualité vidéo
Decoded content data retention mode	Mode de rétention de données de contenu décodé
High speed digital I/F protection information	Informations de protection d'interface numérique à grande vitesse
CopyRestrictionMode	Mode de restriction de copie
User-defined information	Informations définies par l'utilisateur
Control information for exporting to other DRM	Informations de contrôle pour export vers une autre DRM
The following elements are available to specify the playback control information for each media	Les éléments suivants sont disponibles pour spécifier des informations de contrôle de lecture pour chaque support
Export to DTCP	Export vers DTCP
Export to CPRM for DVD	Export vers CPRM pour DVD
Export to CPRM for SD Video	Export vers CPRM pour SD Video
Export to CPRM for SD Audio	Export vers CPRM pour SD Audio
Export to MG-R (SVR) for Memory Stick PRO	Export vers MG-R (SVR) pour Memory Stick PRO
Export to MG-R (SAR) for Memory Stick and Memory Stick PRO	Export vers MG-R (SAR) pour Memory Stick et Memory Stick PRO
Export to VCPS.	Export vers VCPS.
Export to MG-R (SVR) for EMPR.	Export vers MG-R (SVR) pour EMPR.
Export to MG-R (SAR) for ATRAC Audio Device.	Export vers MG-R (SAR) pour ATRAC Audio Device.
Export to SAFIA for iVDR TV Recording	Export vers SAFIA pour enregistrement TV iVDR
Export to SAFIA for iVDR Audio Recording	Export vers SAFIA pour enregistrement audio iVDR
Export to AACS Blu-Ray Disc Recordable for BD-R/RE.	Export vers AACS disque Blu-Ray enregistrable pour BD-R/RE.
Export to AACS Blu-Ray Disc Recordable for Red Laser Media.	Export vers AACS disque Blu-Ray enregistrable pour support laser rouge.
Content data concealment	Annulation des données de contenu
Authentication of DRM systems	Authentification des systèmes de DRM
Authentication of client DRM and server DRM is carried out by using a public key certificate which is issued by an authentication center as authorized by MTMO.	L'authentification du DRM de client et du DRM de serveur est effectuée en utilisant un certificat de clé publique qui est délivré par un centre d'authentification autorisé par MTMO.
EC-DSA (224 bit key) with SHA256	EC-DSA (clé 224 bits) avec SHA256
Run revocation lists. Client DRM can be revoked by each device. Server DRM can be revoked by license distribution server.	Exécution de listes de révocation. Le DRM de client peut être révoqué par chaque dispositif. Le DRM de serveur peut être révoqué par le serveur de distribution de licence.
Communication protection between DRMs	Protection de communication entre DRM.
EC-DH (224 bit key) + EC-DSA (224 bit key) + AES (128 bit key) + SHA 256	EC-DH (clé 224 bits) + EC-DSA (clé 224 bits) + AES (clé 128 bits) + SHA 256

Tableau E.3 – Marlin IPTV-ES, licence de téléchargement, EXTRACTION avec fourniture de clé directe, téléchargement

Elements of content protection		Marlin IPTV-ES
		Download license
		EXTRACT with Direct Key Delivery
Distribution format		Downloading
Content usage permission 1) License requirement → comfirmation of contract → content distribution 2) Distribution of license		When DRM server receives a license aquisition request from a terminal, it confirms to a customer management system and a contract management system to be able to distribute the requested license. If possible, it distributes licenses embedding playback control information that corresponds to the contract.
Management of permission issuer, receiver and issue date		Running dependent It is possible to manage as a license distribution log on the center
License storage on a nonvolatile area in a terminal		Available
License move/copy		Not available
Encrypted content storage on a nonvolatile area in a terminal		Available
Content usage control	Playback period	NotBefore, NotAfter
	Digital copy control information	DigitalRecordingControlData 11: Copy never * Follow APS Control Data for analog output
	Serial interface output control	CopyControlType 01: Serial interface encoding output
	Analog output copy control	APS Control Data 00: Copy free 01: Pseudo-synchronizing pulse 10: Pseudo-synchronizing pulse + two line inverted burst 11: Pseudo-synchronizing pulse + four line inverted burst
	Video quality control information	ImageConstraintToken 1: unbound
	Decoded content data retention mode	RetentionMode 0: Permit retention
	Decoded content data retention state	RetentionState 111: 90 min
	High speed digital I/F protection information	EncryptionMode 1: non-protection
	CopyRestrictionMode	
	User-defined information	Not defined
Control information for exporting to other DRM		
Content data concealment		AES (128 bit key) + SCTE 52
Authentication of DRM systems		Authentication of client DRM and server DRM is carried out by using a public key certificate which is issued by an authentication center as authorized by MTMO. EC-DSA (224 bit key) with SHA256 Run revocation lists. Client DRM can be revoked by each device. Server DRM can be revoked by each license distribution server.

Elements of content protection	Marlin IPTV-ES
	Download license
	EXTRACT with Direct Key Delivery
Communication protection between DRMs	EC-DH (224 bit key) + EC-DSA (224 bit key) + AES (128 bit key) + SHA 256

Légende

Anglais	Français
Elements of content protection	Eléments de protection de contenu
Marlin IPTV-ES	Marlin IPTV-ES
Download license	Licence de téléchargement
EXTRACT with Direct Key Delivery	EXTRACTION avec fourniture de clé directe
Distribution format	Format de distribution
Download	Téléchargement
Content usage permission	Autorisation d'utilisation de contenu
1) License requirement->comfirmation of contract->content distribution	1) Exigence de licence -> confirmation de contrat -> distribution de contenu
2) Distribution of license	2) Distribution de licence
When DRM server receives a license aquisition request from a terminal, it confirms to a customer management system and a contract management system to be able to distribute the requested license.	Lorsqu'un serveur de DRM reçoit une demande d'acquisition de licence d'un terminal, il confirme à un système de gestion de consommateur et un système de gestion de contrat qu'il peut distribuer la licence demandée.
If possible, it distributes licenses embedding playback control information that corresponds to the contract.	Il distribue si possible la licence incorporant les informations de commande de lecture correspondant au contrat.
Management of permission issuer, receiver and issue date	Gestion de l'émetteur, du récepteur de permission et de la date d'édition
Running dependent	Dépend du fonctionnement
It is possible to manage as a license distribution log on the center	Possibilité de gestion par le journal de distribution de licence sur le centre
License storage on a nonvolatile area in a terminal	Stockage de licence sur une zone non volatile dans un terminal
Available	Disponible
License move/copy	Déplacement/copie de licence
Not available	Non disponible
Encrypted content storage on a nonvolatile area in a terminal	Stockage de contenu chiffré sur une zone non volatile dans un terminal
Content usage control	Contrôle d'utilisation de contenu
Playback period	Période de lecture
NotBefore, NotAfter	Pas avant, pas après
Digital copy control information	Informations de contrôle de copie numérique
DigitalRecordingControlData	Données de contrôle d'enregistrement numérique
11: Copy never	11: Jamais de copie
* Follow APS Control Data for analog output	* Suit données de contrôle APS pour sortie analogique
Serial interface output control	Contrôle de sortie d'interface série
CopyControlType	Type de contrôle de copie
01: Serial interface encoding output	01: Sortie de codage d'interface série
Analog output copy control	Contrôle de copie de sortie analogique

Anglais	Français
APS Control Data	Données de contrôle APS
00: Copy free	00: Copie libre
01: Pseudo-synchronizing pulse	01: mpulsion de pseudo-synchronisation
10: Pseudo-synchronizing pulse + two line inverted burst	10: Impulsion de pseudo-synchronisation + salve inversée de deux lignes
11: Pseudo-synchronizing pulse + four line inverted burst	11: Impulsion de pseudo-synchronisation + salve inversée de quatre lignes
Video quality control information	Informations de contrôle de qualité vidéo
ImageConstraintToken	Jeton de contrainte d'image
1: unbound	1: sans lien
Decoded content data retention mode	Mode de rétention de données de contenu décodé
RetentionMode	Mode de rétention
0: Permit retention	0: Rétention autorisée
Decoded content data retention state	Etat de rétention de données de contenu décodé
RetentionState	Etat de rétention
111: 90 min	111: 90 min
High speed digital I/F protection information	Informations de protection d'interface numérique à grande vitesse
EncryptionMode	Mode de chiffrement
1: non-protection	1: pas de protection
CopyRestrictionMode	Mode de restriction de copie
User-defined information	Informations définies par l'utilisateur
Not defined	Non défini
Control information for exporting to other DRM	Informations de contrôle pour export vers une autre DRM
Content data concealment	Annulation des données de contenu
AES (128 bit key) + SCTE 52	AES (clé 128 bits) + SCTE 52
Authentication of DRM systems	Authentification des systèmes de DRM
Authentication of client DRM and server DRM is carried out by using a public key certificate which is issued by an authentication center as authorized by MTMO.	L'authentification du DRM de client et du DRM de serveur est effectuée en utilisant un certificat de clé publique qui est délivré par un centre d'authentification autorisé par MTMO.
EC-DSA (224 bit key) with SHA256	EC-DSA (clé 224 bits) avec SHA256
Run revocation lists. Client DRM can be revoked by each device. Server DRM can be revoked by each license distribution server.	Exécution de listes de révocation. Le DRM de client peut être révoqué par chaque dispositif. Le DRM de serveur peut être révoqué par le serveur de distribution de licence.
Communication protection between DRMs	Protection de communication entre DRM
EC-DH (224 bit key) + EC-DSA (224 bit key) + AES (128 bit key) + SHA 256	EC-DH (clé 224 bits) + EC-DSA (clé 224 bits) + AES (clé 128 bits) + SHA 256

Tableau E.4 – Marlin IPTV-ES, licence de téléchargement, EXTRACTION avec fourniture de clé directe, lecture en continu de VOD

Elements of content protection		Marlin IPTV-ES
		Download license
		EXTRACT with Direct Key Delivery
Distribution format		VOD streaming
Content usage permission 1) License requirement → comfirmation of contract → content distribution 2) Distribution of license		When DRM server receives a license acquisition request from a terminal, it confirms to a customer management system and a contract management system whether the terminal has the rights to get the requesting license. If possible, it distributes the license embedding playback control information that corresponds to the contract.
Management of permission issuer, receiver and issue date		Running dependent It is possible to manage as a license distribution log in the center.
License storage on a nonvolatile area in a terminal		Available
License move/copy		Not available
Encrypted content storage on a nonvolatile area in a terminal		Not available except for keeping a quality of playback
Content usage control	Playback period	NotBefore, NotAfter
	Digital copy control information	DigitalRecordingControlData 11: Copy never * Follow APS Control Detail as analog output
	Serial interface output control	CopyControlType 01 : Serial interface encoding output
	Analog output copy control	APS Control Data 00: Copy free 01: Pseudo-synchronizing pulse 10: Pseudo-synchronizing pulse + two line inverted burst 11: Pseudo-synchronizing pulse + four line inverted burst
	Video quality control information	ImageConstraintToken 1: unbound
	Decoded content data retention mode	RetentionMode 0: Retention
	Decoded content data retention state	RetentionState 111: 90 min
	High speed digital I/F protection information	EncryptionMode 1: non-protection
	CopyRestrictionMode	
	User-defined information	undefined
Control information for exporting to other DRM		
Content data concealment		AES (128 bit key) + SCTE 52
Authentication of DRM systems		Authentication of client DRM and server DRM is carried out by using a public key certification which is issued by an authentication center as authorized by MTMO. EC-DSA (224 bit key) with SHA256 Run revocation lists. Client DRM can be revoked by each device. Server DRM can be revoked by license distribution server.

Elements of content protection	Marlin IPTV-ES
	Download license
	EXTRACT with Direct Key Delivery
Communication protection between DRMs	EC-DH (224 bit key) + EC-DSA (224 bit key) + AES (128 bit key) + SHA 256

Légende

Anglais	Français
Elements of content protection	Eléments de protection de contenu
Marlin IPTV-ES	Marlin IPTV-ES
Download license	Licence de téléchargement
EXTRACT with Direct Key Delivery	EXTRACTION avec fourniture de clé directe
Distribution format	Format de distribution
VOD streaming	Lecture en continue de VOD
Content usage permission	Autorisation d'utilisation de contenu
1) License requirement->comfirmation of contract->content distribution	1) Exigence de licence -> confirmation de contrat -> distribution de contenu
2) Distribution of license	2) Distribution de licence
When DRM server receives a license aquisition request from a terminal, it confirms to a customer management system and a contract management system whether the terminal has the rights to get the requesting license.	Lorsqu'un serveur de DRM reçoit une demande d'acquisition de licence d'un terminal, il confirme à un système de gestion de consommateur et un système de gestion de contrat si le terminal possède les droits d'obtention de la licence demandée.
If possible, it distributes licenses embedding playback control information that corresponds to the contract.	Il distribue, si possible, la licence incorporant les informations de commande de lecture correspondant au contrat.
Management of permission issuer, receiver and issue date	Gestion de l'émetteur, du récepteur de permission et de la date d'édition
Running dependent	Dépend du fonctionnement
It is possible to manage it as a license distribution log in the center.	Possibilité de gestion par le journal de distribution de licence sur le centre.
License storage on a nonvolatile area in a terminal	Stockage de licence sur une zone non volatile dans un terminal
Available	Disponible
License move/copy	Déplacement/copie de licence
Not available	Non disponible
Encrypted content storage on a nonvolatile area in a terminal	Stockage de contenu chiffré sur une zone non volatile dans un terminal
Not available except for keeping a quality of playback	Non disponible sauf pour conserver une qualité de lecture
Content usage control	Contrôle d'utilisation de contenu
Playback period	Période de lecture
NotBefore, NotAfter	Pas avant, pas après
Digital copy control information	Informations de contrôle de copie numérique
DigitalRecordingControlData	Données de contrôle d'enregistrement numérique
11: Copy never	11: Jamais de copie
* Follow APS Control Details as analog output	* Suit détails de contrôle APS comme sortie analogique
Serial interface output control	Contrôle de sortie d'interface série
CopyControlType	Type de contrôle de copie

Anglais	Français
01: Serial interface encoding output	01: Sortie de codage d'interface série
Analog output copy control	Contrôle de copie de sortie analogique
APS Control Data	Données de contrôle APS
00: Copy free	00: Copie libre
01: Pseudo-synchronizing pulse	01: Impulsion de pseudo-synchronisation
10: Pseudo-synchronizing pulse + two line inverted burst	10: Impulsion de pseudo-synchronisation + salve inversée de deux lignes
11: Pseudo-synchronizing pulse + four line inverted burst	11: Impulsion de pseudo-synchronisation + salve inversée de quatre lignes
Video quality control information	Informations de contrôle de qualité vidéo
ImageConstraintToken	Jeton de contrainte d'image
1: unbound	1: sans lien
Decoded content data retention mode	Mode de rétention de données de contenu décodé
RetentionMode	Mode de rétention
0: Retention	0: Rétention
Decoded content data retention state	Etat de rétention de données de contenu décodé
RetentionState	Etat de rétention
111: 90 min	111: 90 min
High speed digital I/F protection information	Informations de protection d'interface numérique à grande vitesse
EncryptionMode	Mode de chiffrement
1: non-protection	1: pas de protection
CopyRestrictionMode	Mode de restriction de copie
User-defined information	Informations définies par l'utilisateur
undefined	Non défini
Control information for exporting to other DRM	Informations de contrôle pour export vers une autre DRM
Content data concealment	Annulation des données de contenu
AES (128 bit key) + SCTE 52	AES (clé 128 bits) + SCTE 52
Authentication of DRM systems	Authentification des systèmes de DRM
Authentication of client DRM and server DRM is carried out by using a public key certification which is issued by an authentication center as authorized by MTMO.	L'authentification du DRM de client et du DRM de serveur est effectuée en utilisant un certificat de clé publique qui est délivré par un centre d'authentification autorisé par MTMO.
EC-DSA (224 bit key) with SHA256	EC-DSA (clé 224 bits) avec SHA256
Run revocation lists. Client DRM can be revoked by each device. Server DRM can be revoked by license distribution server.	Exécution de listes de révocation. Le DRM de client peut être révoqué par chaque dispositif. Le DRM de serveur peut être révoqué par le serveur de distribution de licence.
Communication protection between DRMs	Protection de communication entre DRM
EC-DH (224 bit key) + EC-DSA (224 bit key) + AES (128 bit key) + SHA 256	EC-DH (clé 224 bits) + EC-DSA (clé 224 bits) + AES (clé 128 bits) + SHA 256

Tableau E.5 – Marlin IPTV-ES, licence de diffusion, EXTRACTION avec licence de fourniture de clé indirecte, redistribution terrestre/redistribution BS

Elements of content protection		Marlin IPTV-ES
		Broadcast license
		EXTRACT with Indirect Key Delivery license
Distribution format		Terrestrial re-distribution/BS re-distribution
Content usage permission 1) License requirement → comfirmation of contract → content distribution 2) Distribution of license		Permission to playback a content confirms, when a terminal requests a license, to a customer management system and a contract management system whether the terminal has the rights to get a requested license (work key). If possible, a DRM server distributes a license embedding information about available channels and available period of reception. Broadcastring data received is permitted to be copied/moved to other media/devices as following to digital copy control information and copy control information set in multiplexed ECM. (Copy/Move is only valid for one generation. Copy/Move is not possible in second generation). There are no playback period limits for a content which is stored in received devices and for a content which is moved/copied to other media/devices.
		Playback controls the information of broadcasting data that follows the terrestrial broadcast and BS broadcast playback control information.
Management of permission issuer, receiver and issue date		Running dependent It is possible to manage it as a license distribution log in the center.
License storage on a nonvolatile area in a terminal		Available
License move/copy		Not available
Encrypted content storage on a nonvolatile area in a terminal		It is not permitted except for keeping a playback quality.
Content usage control	Playback period	NotBefore, NotAfter * There is an offset period in which it is possible to update a license period from NotAfter.
	Digital copy control information	It follows a digital copy control descriptor of SI.
	Serial interface output control	
	Analog output copy control	
	Video quality control information	It succeeds content usage descriptor of SI.
	Decoded content data retention mode	
	Decoded content data retention state	
	High speed digital I/F protection information	
	CopyRestrictionMode	
	User-defined information	undefined
Control information for exporting to other DRM		
Content data concealment		AES (128 bit key) + SCTE 52

Elements of content protection	Marlin IPTV-ES
	Broadcast license
	EXTRACT with Indirect Key Delivery license
Authentication of DRM systems	Authentication of client DRM and server DRM is carried out by using a public key certification which is issued by authentication center as authorized by MTMO. EC-DSA (224 bit key) with SHA256 Run revocation lists. Client DRM can be revoked by each device. Server DRM can be revoked by license distribution server.
Communication protection between DRMs	EC-DH (224 bit key) + EC-DSA (224 bit key) + AES (128 bit key) + SHA 256

Légende

Anglais	Français
Elements of content protection	Eléments de protection de contenu
Marlin IPTV-ES	Marlin IPTV-ES
Broadcast license	Licence de diffusion
EXTRACT with Indirect Key Delivery license	EXTRACTION avec licence de fourniture de clé indirecte
Distribution format	Format de distribution
Terrestrial re-distribution/BS re-distribution	Redistribution terrestre/redistribution BS
Content usage permission	Autorisation d'utilisation de contenu
1) License requirement->comfirmation of contract->content distribution	1) Exigence de licence -> confirmation de contrat -> distribution de contenu
2) Distribution of license	2) Distribution de licence
Permission to playback a content confirms, when a terminal requests a license, to a customer management system and a contract management system whether the terminal has the rights to get a requested license (work key)	L'autorisation de lecture d'un contenu confirme, lorsqu'un terminal demande une licence, à un système de gestion de consommateur et un système de gestion de contrat si le terminal possède les droits d'obtention d'une licence demandée (clé de travail).
If possible, a DRM server distributes a license embedding information about available channels and available period of reception.	Si possible, le serveur de DRM distribue une licence incorporant les informations concernant les canaux disponibles et la période de réception disponible.
Broadcasting data received is permitted to be copied/moved to other media/devices as following to digital copy control information and copy control information set in multiplexed ECM. (Copy/Move are only valid for one generation. Copy/Move in second generation is not possible.)	Il est autorisé de copier/déplacer les données de diffusion reçues vers d'autres supports/dispositif à la suite des informations de contrôle de copie numérique et des informations de contrôle de copie déterminées dans l'ECM multiplexe. (Copie/déplacement ne sont valables que pour une génération. Il n'est pas possible d'effectuer une copie/déplacement d'une deuxième génération.)
There are no playback period limits for a content which is stored in received devices and for a content which is moved/copied to other media/devices.	Il n'y a pas de limite de période de lecture pour un contenu stocké dans des dispositifs reçus et pour un contenu déplacé/copié vers d'autres supports/dispositifs.
A playback controls the information of broadcasting data that follows the terrestrial broadcast and BS broadcast playback control information.	Une lecture contrôle les informations des données de diffusion à la suite d'une diffusion terrestre et des informations de contrôle de lecture de diffusion BS.
Management of permission issuer, receiver and issue date	Gestion de l'émetteur, du récepteur de permission et de la date d'édition
Running dependent	Dépend du fonctionnement

Anglais	Français
It is possible to manage it as a license distribution log in the center.	Possibilité de gestion par le journal de distribution de licence sur le centre.
License storage on a nonvolatile area in a terminal	Stockage de licence sur une zone non volatile dans un terminal
Available	Disponible
License move/copy	Déplacement/copie de licence
Not available	Non disponible
Encrypted content storage on a nonvolatile area in a terminal	Stockage de contenu chiffré sur une zone non volatile dans un terminal
It is not permitted except for keeping a playback quality.	Pas autorisé sauf pour conserver une qualité de lecture.
Content usage control	Contrôle d'utilisation de contenu
Playback period	Période de lecture
NotBefore, NotAfter	Pas avant, pas après
* There is an offset period in which it is possible to update a license period from NotAfter.	* Il existe une période de décalage où il est possible de mettre à jour la période de licence à partir de "pas après".
Digital copy control information	Informations de contrôle de copie numérique
It follows a digital copy control descriptor of SL	Fait suite au descripteur de contrôle de copie numérique de SL
Serial interface output control	Contrôle de sortie d'interface série
Analog output copy control	Contrôle de copie de sortie analogique
Video quality control information	Informations de contrôle de qualité vidéo
It succeeds content usage descriptor of SL	Fait suite au descripteur d'utilisation de contenu de SL
Decoded content data retention mode	Mode de rétention de données de contenu décodé
Decoded content data retention state	Etat de rétention de données de contenu décodé
High speed digital I/F protection information	Informations de protection d'interface numérique à grande vitesse
CopyRestrictionMode	Mode de restriction de copie
User-defined information	Informations définies par l'utilisateur
undefined	Non défini
Control information for exporting to other DRM	Informations de contrôle pour export vers une autre DRM
Content data concealment	Annulation des données de contenu
AES (128 bit key) + SCTE 52	AES (clé 128 bits) + SCTE 52
Authentication of DRM systems	Authentification des systèmes de DRM
Authentication of client DRM and server DRM is carried out by using a public key certification which is issued by an authentication center as authorized by MTMO.	L'authentification du DRM de client et du DRM de serveur est effectuée en utilisant un certificat de clé publique qui est délivré par un centre d'authentification autorisé par MTMO.
EC-DSA (224 bit key) with SHA256	EC-DSA (clé 224 bits) avec SHA256
Run revocation lists. Client DRM can be revoked by each device. Server DRM can be revoked by license distribution server.	Exécution de listes de révocation. Le DRM de client peut être révoqué par chaque dispositif. Le DRM de serveur peut être révoqué par le serveur de distribution de licence.
Communication protection between DRMs	Protection de communication entre DRM
EC-DH (224 bit key) + EC-DSA (224 bit key) + AES (128 bit key) + SHA 256	EC-DH (clé 224 bits) + EC-DSA (clé 224 bits) + AES (clé 128 bits) + SHA 256

Tableau E.6 – Marlin IPTV-ES, licence de diffusion, EXTRACTION avec licence de fourniture de clé directe, multidiffusion IP

Elements of content protection	Marlin IPTV-ES
	Broadcasting license.
	EXTRACT with Indirect Key Delivery license
Distribution format	IP multicast
Content usage permission 1) License requirement → comfirmation of contract → content distribution 2) Distribution of license	Permission to playback a content confirms, when a terminal requests a license, to a customer management system and a contract management system whether the terminal has the rights to get a requested license (work key). If possible, a DRM server distributes a license embedding information about available channels and available period of reception. Broadcastring data received is permitted to be copied/moved to other media/devices as following to digital copy control information and copy control information set in multiplexed ECM. (Copy/Move is only valid for one generation. Copy/Move is not possible in second generation). There are no playback period limits for a content which is stored in received devices and for a content which is moved/copied to other media/devices.
	Playback control information of broadcasting data is set/modified by channel in the center.
Management of permission issuer, receiver and issue date	Running dependent It is possible to manage as a license distribution log in the center.
License storage on a nonvolatile area in a terminal	Available
License move/copy	Not available
Encrypted content storage on a nonvolatile area in a terminal	It is not permitted except for keeping a playback quality.

Elements of content protection		Marlin IPTV-ES
		Broadcasting license.
		EXTRACT with Indirect Key Delivery license
Content usage control	Playback period	NotBefore, NotAfter * There is an offset period in which it is possible to update a license period from NotAfter.
	Digital copy control information	DigitalRecordingControlData 00: Constrained condition 10: Copy one generation 11: Copy never * Follow APS Control Data as analog output
	Serial interface output control	CopyControlType 01 : Serial interface encoding output
	Analog output copy control	APS Control Data 00: Copy free 01: Pseudo-synchronized pulse 10: Pseudo-synchronized pulse + two line inverted burst 11: Pseudo-synchronized pulse + four line inverted burst
	Video quality control information	ImageConstraintToken 1: unbound
	Decoded content data retention mode	RetentionMode 0: Retention
	Decoded content data retention state	RetentionState 111: 90 min
	High speed digital I/F protection information	EncryptionMode 0: Protect 1: Non-protect
	CopyRestrictionMode	
	User-defined information	undefined
Control information for exporting to other DRM		
Content data concealment		AES (128 bit key) + SCTE 52
Authentication of DRM systems		Authentication of client DRM and server DRM is carried out by using a public key certification which is issued by an authentication center as authorized by MTMO. EC-DSA (224 bit key) with SHA256 Run revocation lists. Client DRM can be revoked by each device. Server DRM can be revoked by license distribution server.
Communication protection between DRMs		EC-DH (224 bit key) + EC-DSA (224 bit key) + AES (128 bit key) + SHA 256

Légende

Anglais	Français
Elements of content protection	Eléments de protection de contenu
Marlin IPTV-ES	Marlin IPTV-ES
Broadcasting license	Licence de diffusion
EXTRACT with Indirect Key Delivery license	EXTRACTION avec licence de fourniture de clé indirecte
Distribution format	Format de distribution

Anglais	Français
IP multicast	Multidiffusion IP
Content usage permission	Autorisation d'utilisation de contenu
1) License requirement->comfirmation of contract->content distribution	1) Exigence de licence -> confirmation de contrat -> distribution de contenu
2) Distribution of license	2) Distribution de licence
Permission to playback a content confirms, when a terminal requests a license, to a customer management system and a contract management system whether the terminal has the rights to get a requested license (work key)	L'autorisation de lecture d'un contenu confirme, lorsqu'un terminal demande une licence, à un système de gestion de consommateur et un système de gestion de contrat si le terminal possède les droits d'obtention d'une licence demandée (clé de travail).
If possible, a DRM server distributes a license embedding information about available channels and available period of reception.	Si possible, le serveur de DRM distribue une licence incorporant les informations concernant les canaux disponibles et la période de réception disponible.
Broadcasting data received is permitted to be copied/moved to other media/devices as following to digital copy control information and copy control information set in multiplexed ECM. (Copy/Move are only valid for one generation. Copy/Move in second generation is not possible.)	Il est autorisé de copier/déplacer les données de diffusion reçues vers d'autres supports/dispositif à la suite des informations de contrôle de copie numérique et des informations de contrôle de copie déterminées dans l'ECM multiplexe. (Copie/déplacement ne sont valables que pour une génération. Il n'est pas possible d'effectuer une copie/déplacement d'une deuxième génération)
There are no playback period limits for a content which is stored in received devices and for a content which is moved/copied to other media/devices.	Il n'y a pas de limite de période de lecture pour un contenu stocké dans des dispositifs reçus et pour un contenu déplacé/copié vers d'autres supports/dispositifs.
Playback control information of broadcasting data is set/modifed by channel in the center.	Les informations de contrôle de lecture des données de diffusion sont fixées/modifié par canal dans le centre.
Management of permission issuer, receiver and issue date	Gestion de l'émetteur, du récepteur de permission et de la date d'édition
Running dependent	Dépend du fonctionnement
It is possible to manage it as a license distribution log in the center.	Possibilité de gestion par le journal de distribution de licence sur le centre.
License storage on a nonvolatile area in a terminal	Stockage de licence sur une zone non volatile dans un terminal
Available	Disponible
License move/copy	Déplacement/copie de licence
Not available	Non disponible
Encrypted content storage on a nonvolatile area in a terminal	Stockage de contenu chiffré sur une zone non volatile dans un terminal
It is not permitted except for keeping a playback quality.	Pas autorisé sauf pour conserver une qualité de lecture.
Content usage control	Contrôle d'utilisation de contenu
Playback period	Période de lecture
NotBefore, NotAfter	Pas avant, pas après
* There is an offset period in which it is possible to update a license period from NotAfter.	* Il existe une période de décalage où il est possible de mettre à jour la période de licence à partir de "pas après".
Digital copy control information	Informations de contrôle de copie numérique
DigitalRecordingControlData	Données de contrôle d'enregistrement numérique
00: Constrained condition	00: Condition contrainte
10: Copy one generation	10: Copie une génération
11: Copy never	11: Jamais de copie

Anglais	Français
* Follows APS Control Data as analog output.	* Suit données de contrôle APS comme sortie analogique.
Serial interface output control	Contrôle de sortie d'interface série
CopyControlType	Type de contrôle de copie
01: Serial interface encoding output	01: Sortie de codage d'interface série
Analog output copy control	Contrôle de copie de sortie analogique
APS Control Data	Données de contrôle APS
00: Copy free	00: Copie libre
01: Pseudo-synchronized pulse	01: Impulsion pseudo-synchronisée
10: Pseudo-synchronized pulse + two line inverted burst	10: Impulsion pseudo-synchronisée + salve inversée de deux lignes
11: Pseudo-synchronized pulse + four line inverted burst	11: Impulsion pseudo-synchronisée + salve inversée de quatre lignes
Video quality control information	Informations de contrôle de qualité vidéo
ImageConstraintToken	Jeton de contrainte d'image
1: unbound	1: sans lien
Decoded content data retention mode	Mode de rétention de données de contenu décodé
RetentionMode	Mode de rétention
0: Retention	0: Rétention
Decoded content data retention state	Etat de rétention de données de contenu décodé
RetentionState	Etat de rétention
111: 90 min	111: 90 min
High speed digital I/F protection information	Informations de protection d'interface numérique à grande vitesse
EncryptionMode	Mode de chiffrement
0: Protect	0: Protection
1: Non-protect	1: Pas de protection
CopyRestrictionMode	Mode de restriction de copie
User-defined information	Informations définies par l'utilisateur
undefined	non défini
Control information for exporting to other DRM	Informations de contrôle pour export vers une autre DRM
Content data concealment	Annulation des données de contenu
AES (128 bit key) + SCTE 52	AES (clé 128 bits) + SCTE 52
Authentication of DRM systems	Authentification des systèmes de DRM
Authentication of client DRM and server DRM is carried out by using a public key certification which is issued by an authentication center as authorized by MTMO.	L'authentification du DRM de client et du DRM de serveur est effectuée en utilisant un certificat de clé publique qui est délivré par un centre d'authentification autorisé par MTMO.
EC-DSA (224 bit key) with SHA256	EC-DSA (clé 224 bits) avec SHA256
Run revocation lists. Client DRM can be revoked by each device. Server DRM can be revoked by license distribution server.	Exécution de listes de révocation. Le DRM de client peut être révoqué par chaque dispositif. Le DRM de serveur peut être révoqué par le serveur de distribution de licence.
Communication protection between DRMs	Protection de communication entre DRM
EC-DH (224 bit key) + EC-DSA (224 bit key) + AES (128 bit key) + SHA 256	EC-DH (clé 224 bits) + EC-DSA (clé 224 bits) + AES (clé 128 bits) + SHA 256

Tableau E.7 – Marlin IPTV-ES, licence VOD, EXTRACTION avec licence de fourniture de clé simple

Elements of content protection		Marlin IPTV-ES
		VOD license
		EXTRACT with Simple Key Delivery license
Distribution format		VOD streaming
Content usage permission 1) License requirement → comfirmation of contract → content distribution 2) Distribution of license		When a server DRM receives a license acuisition request from a terminal, it confirms to a customer management system and contract management system whether the terminal has rights to get a requested license. If possible, it distributes the license embedding playback control information that corresponds to the contract.
Management of permission issuer, receiver and issue date		Running dependent It is possible to manage it as a license distribution log in the center.
License storage on a nonvolatile area in a terminal		Not available
License move/copy		Not available
Encrypted content storage on a nonvolatile area in a terminal		It is not available except for keeping playback quality.
Content usage control	Playback period	
	Digital copy control information	DigitalRecordingControlData 11: Copy never * Follow APS Control Detail as analog output
	Serial interface output control	CopyControlType 01: Serial interface encoding output
	Analog output copy control	APS Control Data 00: Copy free 01: Pseudo-synchronized pulse 10: Pseudo-synchronized pulse + two line inverted burst 11: Pseudo-synchronized pulse + four line inverted burst
	Video quality control information	ImageConstraintToken 1: unbound
	Decoded content data retention mode	RetentionMode 0: Retention
	Decoded content data retention state	RetentionState 111: 90 min
	High speed digital I/F protection information	EncryptionMode 1: Non protection
	CopyRestrictionMode	
	User-defined information	undefined
Control information for exporting to other DRM		
Content data concealment		AES (128 bit key) + SCTE 52
Authentication of DRM systems		Authentication of client DRM and server DRM is carried out by using a public key certification which is issued by an authentication center as authorized by MTMO. EC-DSA (224 bit key) with SHA256 Run revocation lists. Client DRM can be revoked by each device. Server DRM can be revoked by license distribution server.

Elements of content protection	Marlin IPTV-ES
	VOD license
	EXTRACT with Simple Key Delivery license
Communication protection between DRMs	EC-DH (224 bit key) + EC-DSA (224 bit key) + AES (128 bit key) + SHA 256

Légende

Anglais	Français
Elements of content protection	Éléments de protection de contenu
Marlin IPTV-ES	Marlin IPTV-ES
VOD license	Licence VOD
EXTRACT with Simple Key Delivery license	EXTRACTION avec licence de fourniture de clé simple
Distribution format	Format de distribution
VOD Streaming	Lecture en continu VOD
Content usage permission	Autorisation d'utilisation de contenu
1) License requirement->comfirmation of contract->content distribution	1) Exigence de licence -> confirmation de contrat -> distribution de contenu
2) Distribution of license	2) Distribution de licence
When a server DRM receives a license aquisition request from a terminal, it confirms to a customer management system and contract management system whether the terminal has rights to get the requested license.	Lorsqu'un serveur de DRM reçoit une demande d'acquisition de licence d'un terminal, il confirme à un système de gestion de consommateur et un système de gestion de contrat si le terminal possède les droits d'obtention de la licence demandée.
If possible, it distributes the license embedding playback control information that corresponds to the contract.	Si possible, il distribue la licence incorporant les informations de contrôle de lecture correspondant au contrat.
Management of permission issuer, receiver and issue date	Gestion de l'émetteur, du récepteur de permission et de la date d'édition
Running dependent	Dépend du fonctionnement
It is possible to manage it as a license distribution log in the center.	Possibilité de gestion par le journal de distribution de licence sur le centre.
License storage on a nonvolatile area in a terminal	Stockage de licence sur une zone non volatile dans un terminal
Not available	Non disponible
License move/copy	Déplacement/copie de licence
Encrypted content storage on a nonvolatile area in a terminal	Stockage de contenu chiffré sur une zone non volatile dans un terminal
It is not available except for keeping playback quality.	Non disponible sauf pour conserver une qualité de lecture
Content usage control	Contrôle d'utilisation de contenu
Playback period	Période de lecture
Digital copy control information	Informations de contrôle de copie numérique
DigitalRecordingControlData	Données de contrôle d'enregistrement numérique
11: Copy never	11: Jamais de copie
* Follows APS Control Detail as analog output	* Suit détails de contrôle APS comme sortie analogique
Serial interface output control	Contrôle de sortie d'interface série
CopyControlType	Type de contrôle de copie
01: Serial interface encoding output	01: Sortie de codage d'interface série

Anglais	Français
Analog output copy control	Contrôle de copie de sortie analogique
APS Control Data	Données de contrôle APS
00: Copy free	00: Copie libre
01: Pseudo-synchronized pulse	01: Impulsion pseudo-synchronisée
10: Pseudo-synchronized pulse + two line inverted burst	10: Impulsion pseudo-synchronisée + salve inversée de deux lignes
11: Pseudo-synchronized pulse + four line inverted burst	11: Impulsion pseudo-synchronisée + salve inversée de quatre lignes
Video quality control information	Informations de contrôle de qualité vidéo
ImageConstraintToken	Jeton de contrainte d'image
1: unbound	1: sans lien
Decoded content data retention mode	Mode de rétention de données de contenu décodé
RetentionMode	Mode de rétention
0: Retention	0: Rétention
Decoded content data retention state	Etat de rétention de données de contenu décodé
RetentionState	Etat de rétention
111: 90 min	111: 90 min
High speed digital I/F protection information	Informations de protection d'interface numérique à grande vitesse
EncryptionMode	Mode de chiffrement
1: Non-protection	1: Pas de protection
CopyRestrictionMode	Mode de restriction de copie
User-defined information	Informations définies par l'utilisateur
undefined	non défini
Control information for exporting to other DRM	Informations de contrôle pour export vers une autre DRM
Content data concealment	Annulation des données de contenu
AES (128 bit key) + SCTE 52	AES (clé 128 bits) + SCTE 52
Authentication of DRM systems	Authentification des systèmes de DRM
Authentication of client DRM and server DRM is carried out by using a public key certification which is issued by an authentication center as authorized by MTMO.	L'authentification du DRM de client et du DRM de serveur est effectuée en utilisant un certificat de clé publique qui est délivré par un centre d'authentification autorisé par MTMO.
EC-DSA (224 bit key) with SHA256	EC-DSA (clé 224 bits) avec SHA256
Run revocation lists. Client DRM can be revoked by each device. Server DRM can be revoked by license distribution server.	Exécution de listes de révocation. Le DRM de client peut être révoqué par chaque dispositif. Le DRM de serveur peut être révoqué par le serveur de distribution de licence.
Communication protection between DRMs	Protection de communication entre DRM
EC-DH (224 bit key) + EC-DSA (224 bit key) + AES (128 bit key) + SHA 256	EC-DH (clé 224 bits) + EC-DSA (clé 224 bits) + AES (clé 128 bits) + SHA 256

Tableau E.8 – WM-DRM

Elements of content protection		WM-DRM
Distribution format		Download
Content usage permission 1) License requirement → comfirmation of contract → content distribution 2) Distribution of license		Encrypted content protected by using a key which is encrypted in a license and related to a specific terminal. Both rights and rules which restrict available period and playback count, etc. are included in the license rather than the content. By separating a license from content, a server DRM can issue different licenses for the same content.
Management of permission issuer, receiver and issue date		It is possible in license server
License storage on a nonvolatile area in a terminal		Available
License move/copy		Not available to other PC and network devices. Available to portable devices/media(in this case, AllowCopy is required.)
Encrypted content storage on a nonvolatile area in a terminal		Available
Content usage control	Playback period	The content provider is allowed to combine a following constraints alternatively. • Following a calendar date, a license can be valid or not. • A license can be revoked after a specific time period starting from the first use. • A license can be revoked after a specific time period starting from the first installation to PCs or devices. Following a playback count condition, a license can be revoked.
	Digital copy control information Serial interface output control Analog output copy control Video quality control information	<Audio output protection> 1. Non protection 2. Obfuscation (Protection by Secure Audio Path. Digital output is permitted.) 3. Encryption low (Protection by Secure Audio Path. Digital output is denied.) 4. Encryption middle 5. Encryption high <Video output protection> 1. Non protection 2. Obfuscation (For analog video: Copy Generation Management System) 3. Encryption low (For non-compression digital video: High-Bandwidth Digital Content Protection using secure path such as COPPv1, HDCP up stream protocol, etc.) 4. Encryption middle 5. Encryption high (Compressed digital video: Microsoft Link Protection which has an approximate rectriction)
	Decoded content data retention mode	Not available
	Decoded content data retention state	–
	High speed digital I/F protection information	–
	CopyRestrictionMode	–
	User-defined information	–
Control information for exporting to other DRM		Not available

Elements of content protection	WM-DRM
Content data concealment	As a requrement of network devices, following encryption technology is considering • AES (128 bits) using both ECB and CTR mode
Authentication of DRM systems	By linking each terminal to a server indentically, the system security increases considerably. If terminals infringe on security, they can be identified in licensing process and revoked. It is possible to revoke by a license server.
Communication protection between DRMs	With respect to the requirements of network devices, the following encryption technologies exist. • 2 048 bit RSA encryption that can store and protect a private key • SHA-256 that has 2048 bit RSA encryption and AES OMAC1

Légende

Anglais	Français
Elements of content protection	Eléments de protection de contenu
WM-DRM	WM-DRM
Distribution format	Format de distribution
Download	Téléchargement
Content usage permission	Autorisation d'utilisation de contenu
1) License requirement->confirmation of contract->content distribution	1) Exigence de licence -> confirmation de contrat -> distribution de contenu
2) Distribution of license	2) Distribution de licence
Encrypted content protected by using a key which is encrypted in a license and related to a specific terminal.	Chiffrement de contenu protégé utilisant une clé chiffrée dans la licence et concernant un terminal spécifique.
Both rights and rules which restrict the available period and playback count, etc. are included in the license rather than the content.	Les droits et règles limitant la période disponible et le compte de lecture, etc., sont inclus dans la licence plutôt que dans le contenu.
By separating a license from content, a server DRM can issue different licenses for the same content.	En séparant une licence du contenu, la DRM de serveur peut délivrer différentes licences pour le même contenu.
Management of permission issuer, receiver and issue date	Gestion de l'émetteur, du récepteur de permission et de la date d'édition
It is possible in a license server.	Possible dans le serveur de licence
License storage on a nonvolatile area in a terminal	Stockage de licence sur une zone non volatile dans un terminal
Available	Disponible
License move/copy	Déplacement/copie de licence
Not available to other PC and network devices.	Non disponible pour les autres PC et dispositifs réseau.
Available to portable devices/media (in this case, AllowCopy is required.)	Disponible pour les dispositifs/supports portables (dans ce cas, AllowCopy est requis)
Encrypted content storage on a nonvolatile area in a terminal	Stockage de contenu chiffré sur une zone non volatile dans un terminal
Content usage control	Contrôle d'utilisation de contenu
Playback period	Période de lecture
The content provider is allowed to combine the following constraints alternatively.	Il est possible que le fournisseur de contenu combine les contraintes suivantes en variante.

Anglais	Français
- Following a calendar date, a license can be valid or not.	- Une licence peut être valable ou non après une date calendaire.
- A license can be revoked after a specific time period starting from the first use.	- Une licence peut être révoquée après une période de temps spécifique depuis la première utilisation.
- A license can be revoked after a specific time period starting from the first installation to PCs or devices. Following a playback count condition, a license can be revoked.	- Une licence peut être révoquée après une période de temps spécifique depuis la première utilisation sur des PC ou dispositifs. Une licence peut être révoquée après une condition de compte de lecture.
Digital copy control information	Informations de contrôle de copie numérique
<Audio output protection>	<Protection de sortie audio>
1. Non protection	1. Pas de protection
2. Obfuscation (Protection by secure audio path. Digital output is permitted.)	2. Camouflage (Protection par chemin audio sécurisé. Autorisation de sortie numérique)
Obfuscation	Camouflage
3. Encryption low (Protection by secure audio path. Digital output is denied.)	3. Chiffrement bas (Protection par chemin audio sécurisé. Déni de sortie numérique)
4. Encryption middle	4. Chiffrement moyen
5. Encryption high	5. Chiffrement élevé
<Video output protection>	<Protection de sortie vidéo>
1. Non protection	1. Pas de protection
2. Obfuscation (For analog video: Copy Generation Management System)	2. Camouflage (Pour vidéo analogique: Système de gestion de génération de copie)
3. Encryption low (For non-compression digital video: High-Bandwidth Digital Content Protection using secure path, such as COPPv1, HDCP up stream protocol, etc.)	3. Chiffrement bas (Pour vidéo numérique non compressée: Protection de contenu numérique de grande largeur de bande utilisant un chemin sécurisé, tel que COPPv1, protocole amont HDCP, etc.)
4. Encryption middle	4. Chiffrement moyen
5. Encryption high (Compressed digital video: Microsoft Link Protection which has an approximate restriction)	5. Chiffrement élevé (Vidéo numérique compressée: Protection de lien Microsoft ayant une restriction approximative)
Serial interface output control	Contrôle de sortie d'interface série
Analog output copy control	Contrôle de copie de sortie analogique
Video quality control information	Informations de contrôle de qualité vidéo
Decoded content data retention mode	Mode de rétention de données de contenu décodé
Not available	Non disponible
Decoded content data retention state	Etat de rétention de données de contenu décodé
High speed digital I/F protection information	Informations de protection d'interface numérique à grande vitesse
CopyRestrictionMode	Mode de restriction de copie
User-defined information	Informations définies par l'utilisateur
Control information for exporting to other DRM	Informations de contrôle pour export vers une autre DRM
Not available	Non disponible
Content data concealment	Annulation des données de contenu
As a requirement of network devices the following encryption technology is considered.	On considère la technologie de chiffrement suivante comme exigence des dispositifs réseau
AES (128 bits) using both of ECB and CTR mode.	AES (128 bits) utilisant les deux modes ECB et CTR.
Authentication of DRM systems	Authentification des systèmes de DRM

Anglais	Français
By linking each terminal to a server identically, the system security increases considerably.	La sécurité du système devient importante en reliant chaque terminal au serveur de manière identique.
If terminals infringe on security, they can be identified in the licensing process and be revoked.	Si des terminaux enfreignent la sécurité, ils peuvent être identifiés dans le processus de licence et révoqués.
It is possible to revoke by a license server.	Il est possible de révoquer par un serveur de licence.
Communication protection between DRMs	Protection de communication entre DRM
With respect to the requirements of network devices, the following encryption technologies exist.	Les techniques de chiffrement suivantes existent comme exigence des dispositifs réseau.
2 048 bit RSA encryption that can store and protect a private key.	Chiffrement RSA 2 048 bits pouvant stocker et protéger une clé privée.
SHA-256 that has 2 048 bit RSA encryption and AES O MAC1	SHA-256 ayant un chiffrement de 2 048 bits RSA et AES O MAC1

Tableau E.9 – OMA DRM v2.0

Elements of content protection	OMA DRM v2.0
	CMLA (Content Management License Administrator)
Distribution format	• Download • Streaming
Content usage permission 1) License requirement → comfirmation of contract → content distribution 2) Distribution of license	When Server DRM receives a license acquisition requirement from a terminal to a rights holder, it confirms to a customer management system and a contract management system whether the terminal has rights to get the requested license. If possible, it distributes a license embedding a playback control information correnspondsto the contract.
Management of permission issuer, receiver and issue date	The content issuer, rights issuer and DRM agent are defined, and it is possible to manage it by the rights holder.
License storage on a nonvolatile area in a terminal	Available
License move/copy	If these devices are in the same domain, the content and rights object can be shared. If these devices do not belong to a common domain, only the content can be copied.
Encrypted content storage on a nonvolatile area in a terminal	Available

Elements of content protection		OMA DRM v2.0
		CMLA (Content Management License Administrator)
Content usage control	Playback period	Describe in rights object
	Digital copy control information	Out of scope in OMA DRM. In CMLA technical specification, there are description to support HDCP and DTCP
	Serial interface output control	
	Analog output copy control	
	Video quality control information	
	Decoded content data retention mode	Out of scope in OMA DRM.
	Decoded content data retention state	Out of scope in OMA DRM
	High speed digital I/F protection information	Out of scope in OMA DRM
	CopyRestrictionMode	–
	User-defined information	–
Control information for exporting to other DRM		1) EXPORT is available 2) The way to transport from OMA DRM to other protection mechanisms is not defined. 3) Permission and restriction of the following elements are available by rights object • Export permission • DRM system to export • Copy/move selection when it is exported.
Content data concealment		EncryptionMethod Field 0x0 No encryption 0x1 AES(128 bit) + CBC 0x2 AES(128 bit) + CTR
Authentication of DRM systems		A terminal has own secret/public key and certificate. In a certificate, there are the author's name, device type, the software version, the serial number, and the certificate determines whether a rights holder trusts a terminal or not.
Communication protection between DRMs		Rights information is protected by a rights information acquisition protocol.

Légende

Anglais	Français
Elements of content protection	Eléments de protection de contenu
OMA DRM v2.0	OMA DRM v2.0
CMLA (Content Management license Administrator)	CMLA (Administrateur de licence de gestion de contenu)
Distribution format	Format de distribution
Download	Téléchargement
Streaming	Lecture en continu
Content usage permission	Autorisation d'utilisation de contenu
1) License requirement->confirmation of contract->content distribution	1) Exigence de licence -> confirmation de contrat -> distribution de contenu

Anglais	Français
2) Distribution of license	2) Distribution de licence
When Server DRM receives a license acquisition requirement from a terminal to a rights holder, it confirms to a customer management system and a contract management system whether the terminal has rights to get the requested license.	Lorsqu'un serveur de DRM reçoit une exigence d'acquisition de licence d'un terminal à un détenteur de droits, il confirme à un système de gestion de consommateur et un système de gestion de contrat si le terminal possède les droits d'obtention de la licence demandée.
If possible, it distributes a license embedding a playback control information that corresponds to the contract.	Si possible, il distribue une licence incorporant des informations de contrôle de lecture correspondant au contrat.
Management of permission issuer, receiver and issue date	Gestion de l'émetteur, du récepteur de permission et de la date d'édition
The content issuer, rights issuer and DRM agent are defined, and it is possible to manage it by the rights holder.	L'émetteur de contenu, l'émetteur de droits et l'agent DRM sont définis et il est possible de le gérer par le détenteur de droits.
License storage on a nonvolatile area in a terminal	Stockage de licence sur une zone non volatile dans un terminal
Available	Disponible
License move/copy	Déplacement/copie de licence
If these devices are in the same domain, the content and rights object can be shared.	S'il s'agit des dispositifs du même domaine, le contenu et l'objet de droits peuvent être partagés.
If these devices do not belong to a common domain, only the content can be copied.	S'il s'agit des dispositifs n'appartenant pas à un domaine commun, seul le contenu peut être copié.
Encrypted content storage on a nonvolatile area in a terminal	Stockage de contenu chiffré sur une zone non volatile dans un terminal
Content usage control	Contrôle d'utilisation de contenu
Playback period	Période de lecture
Describe in rights object.	Décrit dans l'objet de droits.
Digital copy control information	Informations de contrôle de copie numérique
Out of scope in OMA DRM.	En dehors du domaine d'application dans OMA DRM.
In the technical specification of CMLA, there is a description to support HDCP and DTCP.	Dans la spécification technique CMLA, il existe une description pour prendre en charge HDCP et DTCP.
Serial interface output control	Contrôle de sortie d'interface série
Analog output copy control	Contrôle de copie de sortie analogique
Video quality control information	Informations de contrôle de qualité vidéo
Decoded content data retention mode	Mode de rétention de données de contenu décodé
Out of scope in OMA DRM	En dehors du domaine d'application dans OMA DRM.
Decoded content data retention state	Etat de rétention de données de contenu décodé
High speed digital I/F protection information	Informations de protection d'interface numérique à grande vitesse
CopyRestrictionMode	Mode de restriction de copie
User-defined information	Informations définies par l'utilisateur
Control information for exporting to other DRM	Informations de contrôle pour export vers une autre DRM
1) EXPORT is available	1) EXPORT est disponible
2) The way to transport from OMA DRM to other protection mechanisms is not defined.	2) non défini pour la façon de transporter OMA DRM vers d'autres mécanismes de protection
3) Permission and restriction of the following elements are available by rights object	3) L'autorisation et la restriction des éléments suivants sont disponibles par objet de droits.

Anglais	Français
Export permission	Autorisation d'export
DRM system to export	Système de DRM à exporter
Copy/move selection when it is exported.	Copie/déplacement de sélection lorsqu'elle est exportée
Content data concealment	Annulation des données de contenu
EncryptionMethod Field	Champ EncryptionMethod
0x0---No encryption	0x0---Pas de chiffrement
0x1---AES (128 bit) + CBC	0x1---AES (128 bits) + CBC
0x2---AES (128 bit) + CTR	0x2---AES (128 bits) + CTR
Authentication of DRM systems	Authentification des systèmes de DRM
A terminal has its own secret/public key and certificate.	Un terminal a ses propres clé secrète/publique et certificat
In a certificate, there are the author's name, device type, the software version, the serial number, and the certificate determines whether a rights holder trusts a terminal or not.	Dans un certificat, on trouve le nom du créateur, le type de dispositif, la version de logiciel, le numéro de série et la détermination du fait qu'un détenteur de droits a confiance ou non dans un terminal au moyen du certificat
Communication protection between DRMs	Protection de communication entre DRM
Rights information is protected by a rights information acquisition protocol.	Les informations des droits sont protégées par le protocole d'acquisition d'informations des droits.

Tableau E.10 – AACS, de base

Elements of content protection		AACS
		Basic title
Distribution format		• Consumer software (Pre-recorded media) • Disc for broadcast (Recordable media)
Content usage permission 1) License requirement → comfirmation of contract → content distribution 2) Distribution of license		It is possible to decode a content by a combination of the device key in the playback device and encrypted title keys in the media.
Management of permission issuer, receiver and issue date		The basic title does not connect online.
License storage on a nonvolatile area in a terminal		Basic title does not connect online
License move/copy		[Move] It is possible to move a title which records in recordable media. [Copy] Not available
Encrypted content storage on a nonvolatile area in a terminal		Basic title doesn't connect on line
Content usage control	Playback period	Not available
	Digital copy control information	In order to prevent illegal copies, it is required to have a secure digital interface such as HDMI on audio/video output.
	Serial interface output control	
	Analog output copy control	
	Video quality control information	
	Decoded content data retention mode	Out of scope
	Decoded content data retention state	Out of scope
	High speed digital I/F protection information	For preventing illegal copy, it is required to secure digital interface such as HDMI on audio/video output
	CopyRestrictionMode	–
	User-defined information	–
Control information for exporting to other DRM		Not available
Content data concealment		AES(128 bit)
Authentication of DRM systems		–
Communication protection between DRMs		–

Légende

Anglais	Français
Elements of content protection	Eléments de protection de contenu
AACS	AACS
Basic title	Titre de base

Anglais	Français
Distribution format	Format de distribution
Consumer software (Pre-recorded media)	Logiciel consommateur (Support préenregistré)
Disc for broadcast (Recordable media)	Disque pour diffusion (Support enregistrable)
Content usage permission	Autorisation d'utilisation de contenu
1) License requirement->comfirmation of contract->content distribution	1) Exigence de licence -> confirmation de contrat -> distribution de contenu
2) Distribution of license	2) Distribution de licence
It is possible to decode a content by a combination of the device key in the playback device and the encrypted title keys in the media.	Il est possible de décoder un contenu en combinaison entre la clé de dispositif dans le dispositif de lecture et les clés de titres chiffrés dans le support.
Management of permission issuer, receiver and issue date	Gestion de l'émetteur, du récepteur de permission et de la date d'édition
The basic title does not connect online.	Le titre de base ne se connecte pas en ligne.
License storage on a nonvolatile area in a terminal	Stockage de licence sur une zone non volatile dans un terminal
License move/copy	Déplacement/copie de licence
[Move] It is possible to move a title which records in recordable media.	[Move] Il est possible de déplacer le titre qui s'enregistre sur un support enregistrable..
[Copy] Not available	[Copy] Non disponible
Encrypted content storage on a nonvolatile area in a terminal	Stockage de contenu chiffré sur une zone non volatile dans un terminal
Basic title doesn't connect on line	Le titre de base ne se connecte pas en ligne
Content usage control	Contrôle d'utilisation de contenu
Playback period	Période de lecture
Digital copy control information	Informations de contrôle de copie numérique
In order to prevent illegal copies, it is required to have a secure digital interface such as HDMI on audio/video output.	Pour empêcher une copie illégale, il est requis de disposer d'une interface numérique sécurisée, telle que HDMI sur la sortie audio/vidéo.
Serial interface output control	Contrôle de sortie d'interface série
Analog output copy control	Contrôle de copie de sortie analogique
Video quality control information	Informations de contrôle de qualité vidéo
Decoded content data retention mode	Mode de rétention de données de contenu décodé
Out of scope	En dehors du domaine d'application
Decoded content data retention state	Etat de rétention de données de contenu décodé
High speed digital I/F protection information	Informations de protection d'interface numérique à grande vitesse
CopyRestrictionMode	Mode de restriction de copie
User-defined information	Informations définies par l'utilisateur
Control information for exporting to other DRM	Informations de contrôle pour export vers une autre DRM
Content data concealment	Annulation des données de contenu
AES (128 bit)	AES (128 bits)
Authentication of DRM systems	Authentification des systèmes de DRM
Communication protection between DRMs	Protection de communication entre DRM

Tableau E.11 – AACS, étendu

Elements of content protection		AACS
		Extended title
Distribution format		• Consumer software • Recordable disc for broadcasting • AACS Network Download Content • AACS On-line Enabled Content • AACS Streamed Content
Content usage permission 1) License requirement → comfirmation of contract → content distribution 2) Distribution of license		After authentication online by an authentication server, the content is decoded by a combination of the device key in a playback terminal and the encrypted title key in a media.
Management of permission issuer, receiver and issue date		Authentication management by authentication server is running dependent
License storage on a nonvolatile area in a terminal		Only titles which have cacheable attributes are available.
License move/copy		[move] Title recorded in recordable medhia can be moved. [Copy]y It is managed by a managed copy. It is required to authenticate online.
Encrypted content storage on a nonvolatile area in a terminal		<AACS Network Download Content> Nerver Store. Available to record on the media such as BD <AACS On-line Enabled Content> Available to the title that has a cacheable attribute <AACS Streamed Content> Never Store.
Content usage control	Playback period	Only titles that have a cacheable attribute are available. It is specified by period, after and before attribute.
	Digital copy control information	
	Serial interface output control	
	Analog output copy control	
	Video quality control information	
	Decoded content data retention mode	Out of scope
	Decoded content data retention state	Out of scope
	High speed digital I/F protection information	Out of scope
	CopyRestrictionMode	–
	User-defined information	–
Control information for exporting to other DRM		Not available

Elements of content protection	AACS
	Extended title
Content data concealment	AES(128 bit)
Authentication of DRM systems	A terminal connect authentication server which is described in Title Usage File of Title and transport content id. Authentication server authenticate it.
Communication protection between DRMs	TLS_RSA_WITH_AES_128_CBC_SHA

Légende

Anglais	Français
Elements of content protection	Eléments de protection de contenu
AACS	AACS
Extended title	Titre étendu
Distribution format	Format de distribution
Consumer software	Logiciel consommateur
Recordable disc for broadcasting	Disque enregistrable pour diffusion
AACS Network Download Content	Contenu du téléchargement du réseau AACS
AACS On-line Enabled Content	Contenu activé en ligne AACS
AACS Streamed Content	Contenu lu en continu AACS
Content usage permission	Autorisation d'utilisation de contenu
1) License requirement->confirmation of contract->content distribution	1) Exigence de licence -> confirmation de contrat -> distribution de contenu
2) Distribution of license	2) Distribution de licence
After authentication online by authentication server, the content is decoded by combination of the device key in a playback terminal and the encrypted title key in a media.	Après l'authentification en ligne par le serveur d'authentification, le contenu est décodé par une combinaison de la clé du dispositif dans un terminal de lecture et la clé du titre chiffré dans un support.
Management of permission issuer, receiver and issue date	Gestion de l'émetteur, du récepteur de permission et de la date d'édition
Authentication management by authentication server is running dependent	La gestion d'authentification par le serveur d'authentification dépend du fonctionnement
License storage on a nonvolatile area in a terminal	Stockage de licence sur une zone non volatile dans un terminal
Only titles which have cacheable attributes are available	Seuls les titres ayant un attribut Cacheable sont disponibles
License move/copy	Déplacement/copie de licence
[Move] Title recorded in recordable media can be moved.	[Move] Le titre enregistré sur le support enregistrable peut être déplacé.
[Copy] It is managed by a managed copy. It is required to authenticate online.	[Copy] Il est géré par la copie gérée. Une authentification en ligne est requise.
Encrypted content storage on a nonvolatile area in a terminal	Stockage de contenu chiffré sur une zone non volatile dans un terminal
<AACS Network Download Content> Never Store. Available to record on the media such as BD	<AACS Network Download Content> Jamais stocké. Disponible pour enregistrement sur le support tel que BD

Anglais	Français
<AACS On-line Enabled Content> *Available to the title that has a cacheable attribute*	*<AACS On-line Enabled Content>* *Disponible pour le titre ayant l'attribut Cacheable*
Content usage control	Contrôle d'utilisation du contenu
Playback period	Période de lecture
Only titles that have a cacheable attribute are available.	Seuls les titres ayant l'attribut Cacheable sont disponibles.
It is specified by period, after and before attribute.	Spécifié par l'attribut période, après et avant.
Digital copy control information	Informations de contrôle de copie numérique
Serial interface output control	Contrôle de sortie d'interface série
Analog output copy control	Contrôle de copie de sortie analogique
Video quality control information	Informations de contrôle de qualité vidéo
Decoded content data retention mode	Mode de rétention de données de contenu décodé
Out of scope	En dehors du domaine d'application
Decoded content data retention state	Etat de rétention de données de contenu décodé
High speed digital I/F protection information	Informations de protection d'interface numérique à grande vitesse
CopyRestrictionMode	Mode de restriction de copie
User-defined information	Informations définies par l'utilisateur
Control information for exporting to other DRM	Informations de contrôle pour export vers une autre DRM
Not available	Non disponible
Content data concealment	Annulation des données de contenu
AES (128 bit)	AES (128 bits)
Authentication of DRM systems	Authentification des systèmes de DRM
A terminal connects to an authentication server which is described in Title Usage File of Title and transport content id. The authentication server authenticates it.	Un terminal se connecte à un serveur d'authentification qui est décrit dans Title Usage File of Title et l'identifiant de contenu de transport. Le serveur d'authentification l'authentifie.
Communication protection between DRMs	Protection de communication entre DRM
TLS_RSA_WITH_AES_128_CBC_SHA	TLS_RSA_WITH_AES_128_CBC_SHA

Bibliographie

Les documents suivants donnent des informations supplémentaires ou détaillées sur chaque organisme.

ISO/IEC 14496-14:2003, *Technologies de l'information – Codage des objets audiovisuels – Partie 14: Format de fichier MP4*

Amendment 1:2010, *Traitement des couches d'amétioration MPEG-4 audio*

ARIB TR-B14, *Operational guidelines for digital terrestrial television broadcasting*

———————

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch