

INTERNATIONAL STANDARD

NORME INTERNATIONALE



Multimedia home server systems – Digital rights permission code

Systèmes serveurs multimédia domestiques – Codes numériques des autorisations des droits



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2012 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.

If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de la CEI ou du Comité national de la CEI du pays du demandeur.

Si vous avez des questions sur le copyright de la CEI ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de la CEI de votre pays de résidence.

IEC Central Office
3, rue de Varembe
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It also gives information on projects, replaced and withdrawn publications.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.

INTERNATIONAL STANDARD

NORME INTERNATIONALE



Multimedia home server systems – Digital rights permission code

Systèmes serveurs multimédia domestiques – Codes numériques des autorisations des droits

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 33.160.60; 35.240.99

ISBN 978-2-8322-0539-6

Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

CONTENTS

FOREWORD.....	6
INTRODUCTION to Amendment 1	8
INTRODUCTION.....	9
1 Scope.....	10
2 Normative references	10
3 Terms, definitions and abbreviations	10
3.1 Terms and definitions	10
3.2 Abbreviated terms	16
4 Permission code framework.....	17
4.1 General.....	17
4.2 Assumptions associated with the permission code.....	18
4.2.1 Binary relationships within the content distribution value chain	18
4.2.2 Permission issued for a group of content	18
4.2.3 Common code center for permissions	19
4.2.4 Usage report	19
4.2.5 Application scenario of the permission code	19
4.2.6 Harmonization with DRM systems.....	20
4.3 Components of a permission code.....	20
4.3.1 Permission actor.....	20
4.3.2 Permission classification	23
4.3.3 Content usage	23
4.3.4 Content data handling	24
5 Permission code configuration.....	25
5.1 General.....	25
5.2 Notation	26
5.2.1 Numerical values	26
5.3 Permission code system.....	26
5.4 Version unit.....	27
5.4.1 Structure	27
5.4.2 Version unit tag	27
5.4.3 Reserved.....	28
5.4.4 Version.....	28
5.5 Permission actor unit.....	28
5.5.1 Structure	28
5.5.2 Permission actor unit tag	28
5.5.3 Total bytes of identifiers	28
5.5.4 Content identifier	28
5.5.5 Issuer identifier.....	30
5.5.6 Receiver identifier	32
5.6 Permission classification unit†.....	33
5.6.1 Structure	33
5.6.2 Permission classification unit tag	33
5.6.3 Reserved.....	33
5.6.4 Disclosure class	33
5.6.5 Usage purpose class	34

5.6.6	Charge model class	35
5.6.7	Billing class	35
5.6.8	Application class	36
5.6.9	Sponsor class	36
5.6.10	Territory class	37
5.6.11	Usage class	37
5.7	General usage condition unit	40
5.7.1	Unit structure	40
5.7.2	General usage condition header	40
5.7.3	General usage condition descriptor	40
5.8	Extended use condition unit	49
5.8.1	Unit structure	50
5.8.2	Extended use condition header	50
5.9	Data management condition unit	50
5.9.1	Unit structure	50
5.9.2	Data management condition header	51
5.9.3	Data management condition	52
5.10	Data export condition unit	54
5.10.1	Unit structure	54
5.10.2	Data export condition header	54
5.10.3	Data export condition descriptor	54
5.10.4	General export descriptor	55
Annex A (informative)	Permission code requirements for home servers and playback devices	59
Annex B (informative)	Use-case scenario	64
Annex C (informative)	Issuing a permission code	72
Figure 1	– Permission code environment	18
Figure 2	– Permission code environment	24
Figure 3	– Permission code configuration	27
Figure 4	– Basic structure of permission code unit	27
Figure 5	– General usage condition unit	40
Figure 6	– Data management condition unit	50
Figure 7	– Data export condition unit	54
Figure 8	– Extended use condition unit	50
Figure A.1	– Permission code and domain	60
Figure A.2	– Re-issuing permission information	61
Figure A.3	– Re-issuing permission among permission code compliant objects is allowed	62
Figure A.4	– Re-issuing permission within a domain is allowed	62
Figure A.5	– Other conditions	63
Figure B.1	– Permission code structuring (1/2)	64
Figure B.2	– Permission code structuring (2/2)	65
Figure B.3	– Permission code example with respect to FairPlay (1/2)	65
Figure B.4	– Permission code example with respect to FairPlay (2/2)	66
Figure B.5	– Permission code example with respect to CPRM (1/2)	67

Figure B.6 – Permission code example with respect to CPRM (2/2)	67
Figure B.7 – Permission code example with respect to SAFIA (1/2)	68
Figure B.8 – Permission code example with respect to SAFIA (2/2)	68
Figure B.9 – Permission code example with respect to PC distribution (streaming)	69
Figure B.10 – Permission code example with respect to PC distribution (download) (1/2)	70
Figure B.11 – Permission code example with respect to PC distribution (download) (2/2)	70
Figure B.12 – Permission code example with respect to ringtones (1/2)	71
Figure B.13 – Permission code example with respect to ringtones (2/2)	71
Figure C.1 – The flow of issuing a permission code to grant access to a single piece of content (for access on a home server)	72
Figure C.2 – The flow of issuing a permission code to grant access to a single piece of content (for access on a client device)	73
Figure C.3 – The flow of issuing a permission code to grant access to subscription content (for access on a home server)	74
Figure C.4 – The flow of issuing a permission code to grant access to subscription content (for access on a client device)	75
Table 1 – Distinct tag interpretation	26
Table 2 – Structure of version unit	27
Table 3 – Structure of permission actor unit	28
Table 4 – Structure of content identifier descriptor	29
Table 5 – Content type code interpretation	29
Table 6 – Structure of issuer identifier descriptor	30
Table 7 – Issuer role code interpretation	31
Table 8 – Issuer configuration code interpretation	31
Table 9 – Structure of receiver identifier descriptor	32
Table 10 – Receiver role code interpretation	32
Table 11 – Receiver configuration code interpretation	32
Table 12 – Structure of permission classification unit	33
Table 13 – Structure of disclosure class	34
Table 14 – disclosure_type (DT) interpretation	34
Table 15 – Structure of usage purpose class	34
Table 16 – usage_purpose_type (UPT) interpretation	34
Table 17 – Structure of charge model class	35
Table 18 – charge_model_type (CMT) interpretation	35
Table 19 – Structure of billing class	36
Table 20 – billing_type (BT) interpretation	36
Table 21 – Structure of application class	36
Table 22 – application_type (AT) interpretation	36
Table 23 – Structure of sponsor class	37
Table 24 – Configuration of sponsor_type (ST)	37
Table 25 – Structure of territory class	37
Table 26 – Structure of usage class	38
Table 27 – Usage_type (UT) interpretation	38

Table 28 – Configuration of redistribution_Type	39
Table 29 – Structure of general usage condition header	40
Table 30 – Tag values of descriptors	41
Table 31 – Structure of playback usage condition descriptor	41
Table 32 – Structure of print usage condition descriptor	44
Table 33 – Structure of execute usage condition descriptor	47
Table 34 – Structure of data management condition header	51
Table 35 – Structure of data management condition	52
Table 36 – Structure of encryption flag (EF)	52
Table 37 – Transcode type interpretation	53
Table 38 – Structure of time-line flag (TF)	53
Table 39 – Structure of data export condition header	54
Table 40 – Tag values of descriptors	55
Table 41 – Structure of general export descriptor	55
Table 42 – storage_media_type (SMT) interpretation	56
Table 43 – encoding_type (ET) interpretation	56
Table 44 – protection_type (PT) interpretation	57
Table 45 – control_type (CT) interpretation	57
Table 46 – Structure of extended use condition header	50

IECNORM.COM : Click to view the full PDF of IEC 62227:2008+A1:2012

INTERNATIONAL ELECTROTECHNICAL COMMISSION

MULTIMEDIA HOME SERVER SYSTEMS – DIGITAL RIGHTS PERMISSION CODE

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 provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
- 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.

International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this document may involve the use of patent.

IEC takes no position concerning the evidence, validity and scope of these patent rights.

The holder of this patent right has assured IEC that it is willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holders of these patent rights are registered with IEC. Information may be obtained from:

DENTSU INC.
Media Marketing Division
1-8-1, Higashi-shimbashi, Minato-ku, Tokyo 105-7001
JAPAN

Attention is drawn to the possibility that some of the elements of this standard may be the subject of patent rights other than those identified above. IEC shall not be held responsible for identifying any or all such patent rights.

This consolidated version of IEC 62227 consists of the first edition (2008) [documents 100/1287/CDV and 100/1374/RVC] and its amendment 1 (2012) [documents 100/1953/CDV and 100/2011/RVC]. It bears the edition number 1.1.

The technical content is therefore identical to the base edition and its amendment and has been prepared for user convenience. A vertical line in the margin shows where the base publication has been modified by amendment 1. Additions and deletions are displayed in red, with deletions being struck through.

International Standard IEC 62227 has been prepared by technical area 8: Multimedia home server systems, of IEC technical committee 100: Audio, video and multimedia systems and equipment.

The French version of this standard has not been voted upon.

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

The committee has decided that the contents of the base publication and its amendments 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 to Amendment 1

The revision of IEC 62227:2008 has become necessary to specify the new additional definition of the descriptor. This Amendment 1 contains the following significant technical changes with respect to the base publication IEC 62227:

- new definition of content type is added;
- new element definition of permission purpose classification is added.

In addition, this amendment will provide editorial changes that will improve the clarity and the understanding of the text.

IECNORM.COM : Click to view the full PDF of IEC 62227:2008+AMD1:2012 CSV

INTRODUCTION

The common ID system is used to systematically identify every entity, device and content that would be involved in the course of digitally distributing content. The permission code can express various sets of permission information and permission conditions necessary for content transmission in a remarkably short code form. The permission code is not defined from a technical perspective, but rather on the basis of permission information that rights holders actually employ in the field, even if the permission code is recognized for its technical effectiveness with respect to digital distribution of content.

IECNORM.COM : Click to view the full PDF of IEC 62227:2008+AMD1:2012 CSV

MULTIMEDIA HOME SERVER SYSTEMS – DIGITAL RIGHTS PERMISSION CODE

1 Scope

This International Standard defines the permission code, a set of permission related information in short code form, primarily intended for home server systems. The permission code is comprised of a common ID system (content ID, issuer ID, receiver ID, device ID, etc.) and a narrowly-defined permission code.

The common ID system is used to systematically identify every entity, device and content that would be involved in the course of digitally distributing content. The permission code can express various sets of permission information and permission conditions necessary for content transmission in a remarkably short code form. The permission code is not defined from a technical perspective, but rather on the basis of permission information that rights holders actually employ in the field. Even after, the permission code is recognized for its technical effectiveness with respect to digital distribution of content.

2 Normative references

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

ISO 3166-1:2006, *Codes for the representation of names of countries and their subdivisions – Part 1: Country codes*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this document the following terms and definitions apply.

3.1.1

permission

act by a certain issuing entity to authorize use for content to a certain receiving entity under a certain set of permission classifications and usage conditions

NOTE The issuing entity and/or the receiving entity may not only be human, but also a device, storage medium, organization, domain or another entity.

3.1.2

permission management server

a server that issues a permission code based on a permission agreement

NOTE The server is equipped with a

- a) license server,
- b) a function that forwards the permission code to a distribution server, and
- c) a function that receives a content usage report from the license server and the distribution server.

3.1.3

compliant license server

a server that issues a license based on a permission code

NOTE The server is equipped with

- a) a server system (including home server),
- b) a function that generates necessary keys for content access based on a permission code, and
- c) a function that forwards the license to a client device. A license contains information about the content's permitted scope of use based on a permission code.

3.1.4

license server

a compliant license server (unless otherwise specified, a compliant license server is simply referred to as a license server)

3.1.5

compliant license

license issued by a compliant license server

3.1.6

license

a compliant license (unless otherwise specified, a compliant license is simply referred to as a license)

3.1.7

home server

client device that serves as a gateway for a home domain

3.1.8

client device

device that becomes the actor of content access and is compliant with permission code terms

3.1.9

compliant device

device that possesses the function to control content access based upon a compliant license

3.1.10

domain

set of actors to which a common set of rules apply in the context of content management

3.1.11

home domain

home-based content usage environment, permitted by rights holders

3.1.12

legacy device

non-compliant device that does not control content access based upon compliant licenses

3.1.13

disclosure type

permission classification that specifies the disclosure class for the permission, including open permission and closed permission

3.1.14

open permission

permission under disclosure type that is received according to previously arranged default conditions

3.1.15

closed permission

permission under disclosure type that is received through a separate, individually negotiated contract

3.1.16

application type

permission classification that specifies the application class for the permission, including ad hoc permission and blanket permission

3.1.17

ad hoc permission

an application type that grants permissions on a per usage unit basis

3.1.18

blanket permission

an application type that grants permissions in aggregate for use within a given time period

NOTE Time periods may include monthly, annual or other time increments.

3.1.19

billing type

permission classification that specifies the billing class for the permission, including ad hoc billing and blanket billing

3.1.20

ad hoc billing

billing type that bills on a per content basis

3.1.21

blanket billing

billing type that bills on monthly, annual or other time-based increments

3.1.22

usage purpose type

permission classification that specifies the usage purpose class for the permission, including commercial, public, not-for-profit, promotion

3.1.23

commercial permission

usage purpose type that permits use for commercial purposes

3.1.24

public permission

usage purpose type that permits use for public purposes

3.1.25

not-for-profit permission

usage purpose type that permits use for non-profit purposes

3.1.26

promotion permission

usage purpose type that permits use for promotional purposes

3.1.27

charge model type

permission classification that specifies the charge model class for the permission, including pay and free, etc.

3.1.28

pay permission

charge model type that permits use for charge

3.1.29**free permission**

charge model type that permits use free of charge

3.1.30**pay per use**

pay permission that charges per use

3.1.31**subscription**

pay permission that charges per time period

3.1.32**coupon**

pay permission that uses coupons, a form of pseudo-currency that can be exchanged with a given piece of content

NOTE A coupon is distributed to users by the content's sponsor in order to increase user contact with said sponsor.

3.1.33**sponsor type**

permission classification that specifies the sponsor class for the permission, including advertising model, premium model, coupon model and personal information disclosure model

3.1.34**advertising model**

a sponsor type that specifies the advertising reception mode

3.1.35**time synchronized forced viewing**

advertising model that forces the synchronization of advertising viewing and content access

3.1.36**pre/post viewing**

advertising model that forces advertising viewing pre/post access

3.1.37**arbitrary time**

advertising model that allows for arbitrary advertising viewing, a kind of viewing in which users are allowed to choose their favorite timing to view advertising

3.1.38**blanket**

advertising model that forces advertising viewing across the board, whereby the terms of advertising viewing and content access will apply to a broad scope of services associated with the content

NOTE Under blanket, advertising viewing is a condition upon which content access is allowed. However, the timing in which advertising is viewed is not limited to those that are synchronized with content. For example, a user may be allowed to access content after viewing a special advertising channel.

3.1.39**premium model**

sponsor type that uses content for premium purposes, whereby, "premium" refers to a promotional practice in which a sponsor provides content access to a user as reward for the user's contact with said sponsor

3.1.40

coupon model

sponsor type that uses content as a gift for coupons

NOTE A coupon is distributed by the content's sponsor in order to increase user contact with said sponsor. That is promotional practice in which coupon, a form of pseudo-currency, is exchanged with contents.

3.1.41

personal information disclosure model

sponsor type that deems personal information disclosed as consideration for content access

3.1.42

usage type

permission classification that specifies the usage class for the permission, including broadcast permission and streaming permission

3.1.43

territory ID

identifier that specifies the territory for the permission, including country and area

3.1.44

redistribution type

permission classification that specifies the redistribution class for the permission, including simultaneous redistribution, programmed streaming and on-demand streaming

3.1.45

non-fixation permission

usage type that permits content use without storage

3.1.46

fixation permission

usage type that permits content use with storage

3.1.47

broadcast permission

usage type that permits broadcast use of content

3.1.48

streaming permission

usage type that permits streaming use of content

3.1.49

broadcast storage permission

usage type that permits broadcast use of content with storage

3.1.50

download permission (on-demand)

usage type that permits broadcast use of content with storage and delivery on-demand

3.1.51

redistribution permission

usage type that permits content use with redistribution

3.1.52

programmed streaming

redistribution permission and/or a streaming permission for content streamed in accordance with program listings

3.1.53**on-demand streaming**

redistribution permission and/or a streaming permission for content streamed on-demand

3.1.54**reuse permission**

usage type that permits reuse of content

3.1.55**move**

usage type that permits the moving of content to a compliant medium under reuse permission

NOTE Permission conditions are further specified under parameter.

3.1.56**copy**

usage type that permits the copying of content to a compliant medium under reuse permission

NOTE Permission conditions are further specified under parameter.

3.1.57**share**

usage type that permits the sharing of content in the home domain under reuse permission

NOTE Permission conditions are further specified under parameter.

3.1.58**export**

usage type that permits the exporting of content to a non-compliant medium under reuse permission

NOTE Permission conditions are further specified under parameter.

3.1.59**edit**

usage type that permits the processing of the time axis of content

3.1.60**modify**

usage type that permits the processing of anything other than the time axis of content

3.1.61**super distribution**

usage type that permits the super distribution of content to a compliant medium under reuse permission

NOTE Permission conditions are further specified under parameter. Super distribution allows encrypted content to be distributed (and redistributed) freely, so long as associated licenses and content keys are transferred securely.

3.1.62**permission code**

a code system that represents codes through a common system so that permissions from 2 parties with differing DRM implementations can interoperate with each other

3.1.63**parent permission code**

permission code issued for a group of content

3.1.64

child permission code

permission code issued for an individual piece of content belonging to a larger group

3.1.65

ID center

an authorized organization which assigns and manages permission actor IDs

3.2 Abbreviated terms

ID	Identifier
DRM	Digital Rights Management (System)
CPRM	Content Protection for Recordable Media
DVD-RW	Digital Versatile Disk ReWritable
AACS	Advanced Access Content System
ISBN	International Standard Book Number
HDD	Hard Disk Drive
DVD	Digital Versatile Disk
DVD-R	Digital Versatile Disk Recordable
DTCP	Digital Transmission Content Protection
TRM	Tamper Resistant Module
XML	Extensible Markup Language
RBP	Relative Byte Position
ASCII	American Standard Code for Information Interchange
ISO	International Organization for Standardization
UTC	Coordinated Universal Time
MPEG	Moving Picture Experts Group
NTSC	National Television Standards Committee
Jpeg	Joint Photographic Experts Group
GIF	Graphic Interchange Format
PNG	Portable Network Graphics
PCM	Pulse Code Modulation
AAC	Advanced Audio Coding
MP3	MPEG Audio Layer-3
HDCP	High-bandwidth Digital Content Protection
CGMS	Copy Generation Management System
SAFIA	Security Architecture For Intelligent Attachment

VCPS	Video Content Protection System
WMT	Windows Media Technology
uimsbf	unsigned integer, most significant bit first
bslbf	bit string, leftmost bit first
imsbf	integer, most significant bit first
CD	Compact Disc
HD	High Definition

4 Permission code framework

4.1 General

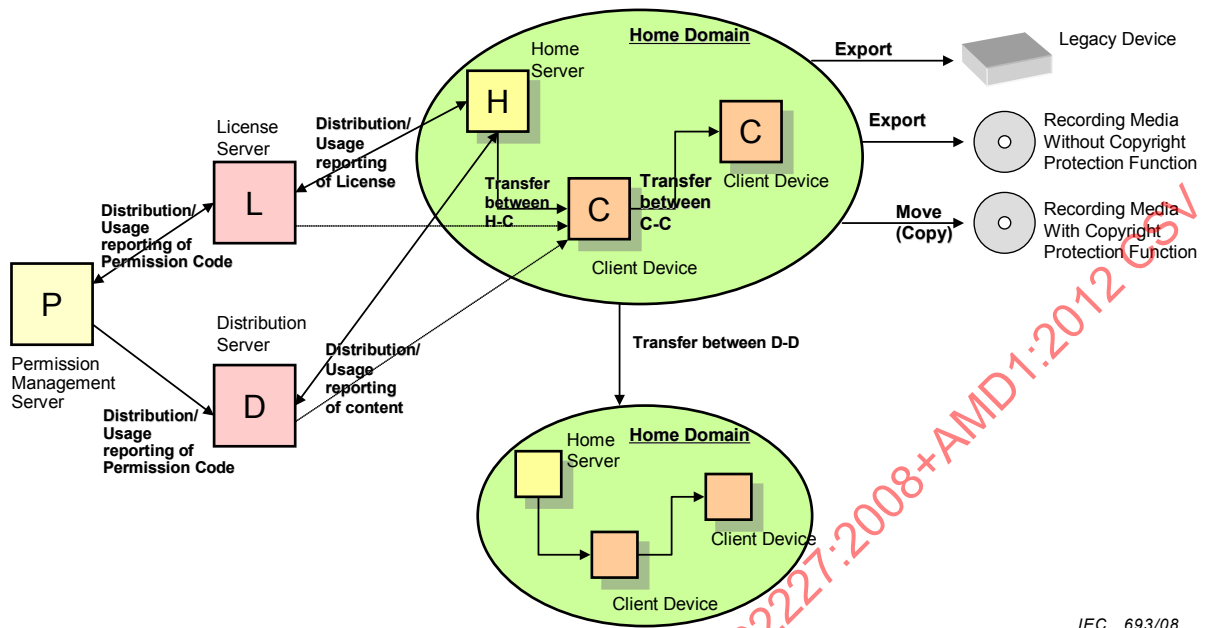
This standard defines permission as “an act by a certain issuing entity to authorize use for content to a certain receiving entity under a certain set of permission classifications, usage conditions, data management conditions and data export conditions”.

In order to distribute permission information with its associated content, this standard represents permission information through 5 digital expressions, including permission actor ID, permission classification, usage condition, data management condition and data export condition. Permission actor ID is comprised of 3 identifiers; a content ID assigned to the subject content and an issuer ID and receiver ID respectively, assigned to each permission issuer and receiver. Permission classification indicates the class (or type) of the permission. Usage condition, data management condition and data export condition detail restrictions placed in the content.

We hereby define the permission code framework and the permission code as a code and framework that combine these 5 elements; permission actor ID, permission classification, usage condition, data management condition and data export condition. The basic permission code is configured using a “tag – size – data” structure. This structure makes it easy to extend the permission code. This standard specifies these configuration requirements in detail.

Within the home server environment, permission codes are used to notify users of associated permission information upon content use, to generate DRM licenses to protect content rights and to report usage upon content use.

The diagram illustrates the permission code usage environment subject to this specification. The permission management server is an actor that issues permission codes in response to requests from entities issuing permissions. The license server is an actor that generates licenses concerning the protection of content rights. The distribution server is an actor that delivers content to the home server environment. Additionally, the home domain represents the content usage environment that conforms to the home. The home server and client devices are playback devices that belong to the home domain.



IEC 693/08

Figure 1 – Permission code environment

4.2 Assumptions associated with the permission code

4.2.1 Binary relationships within the content distribution value chain

Permission between 2 entities, the issuing entity and the receiving entity, is the unit of Permission defined for a permission code. Stated another way, in the event that an intermediate entity exists between an issuing entity and a receiving entity, a permission code shall be generated between the intermediate entity and the issuing entity, as well as the intermediate entity and the receiving entity, respectively. For example, if an intermediate entity, Z, exists between Issuer A and Receiver B, two permission codes shall be generated; one between A and Z, and the other between Z and B.

4.2.2 Permission issued for a group of content

Permission for a body of content linked with a content ID is the unit of permission defined for a permission code. In other words, if one desires to meaningfully group content subject to permission, one would generate a permission code by assigning a content ID to this group of Content. When doing so, individual permission codes are also generated for the respective pieces of content that belong to this content group, using content identifiers associated with each content unit. The manner in which the content ID assigned to the content group as well as the respective content identifiers that belong to the group is associated is left up to implementation, and is hence not defined within this standard.

This standard refers to permission codes for groups as parent permission codes. Similarly, this standard refers to permission codes for individual content comprising the group as child permission codes. The parent permission code is a permission code to realize the permission for the overall group. The parent permission code includes permission information associated with the group. The parent permission code is used when granting permission for subscription use. For example, a parent permission code can be utilized for a subscription service that allows for an unlimited amount of access to content from a group of 100 songs for 500 yen during a one month period. Similarly, the child permission code is a permission code that specifies usage permissions for individual pieces of content within a group. The child permission code includes the permission information for individual pieces of content

encompassed within a group. For example, child permission codes can be utilized for the aforementioned subscription service to specify permissions for each of the 100 individual pieces of content.

The contents of the child permission code can not exceed the scope of permission of the parent permission code. This constraint maintains logical consistency between individual permissions that comprise the larger group and the permission for the group.

4.2.3 Common code center for permissions

The common code center is an organizational body that issues and renews permission codes.

A permission code is issued through the permission management server and then delivered to the license server and distribution server.

The home server and client devices utilize permission codes included within the license, and do not directly connect to the common code center.

4.2.4 Usage report

Delivery service providers that have received usage permissions for content, keep track of content use so they can report it back to permission issuers. Usage history is tracked in the following 2 ways.

- a) Delivery service providers keep track of the content delivered.
- b) After receiving content, home servers and client devices keep track of usage.

In this standard, the permission code is prescribed as a common code to track usage using the second method above. Permission codes are used as identification codes to uniquely specify permissions when reporting content use.

Usage reporting is conducted between the permission management server and the license server, as well as between the permission management server and the distribution server. The reporting protocol is out of scope of this standard.

4.2.5 Application scenario of the permission code

The permission code specified in this standard is a description language used to express the terms of permission. The use of this common language allows for not only content distribution to occur smoothly, but also for different DRM systems to be managed under a uniform system.

For example, let us take a look at online music distribution. As part of their business of receiving consideration for transmitting content to end users, content distributors negotiate content usage permission contracts with record labels. The contents of this permission can be expressed through the use of permission codes.

Distributors can reissue permission and/or transmit permitted content to end users within the scope of the permission contract and/or the permission code. When doing so, the permission terms to be granted to end users can be expressed through the use of permission codes. End users can likewise access content and copy content within the scope indicated in the permission code.

Note that the permission code is primarily a language to indicate the terms of permission, and it, in itself, does not have the ability to regulate content usage behavior. Restricting the use of content to terms specified in the permission is an administrative issue or a DRM systems issue. A permission code compliant object refers to an object such as drm systems, playback devices, storage media and servers, etc. that has the ability to understand and act in accordance with permission codes as specified in this standard.

Permission terms intended for DRM systems that are not permission code compliant can also be expressed through the use of permission codes. Therefore, in order to export content from a permission code compliant DRM system to a non-compliant system, the object at the source of export shall translate the contents of the permission code in a manner that would conform to the DRM rules of the export target.

For example, CPRM used in DVD-RW, AACMS used in Blu-Ray disks are some of the DRM systems that are not permission code compliant. These types of storage media protect content with their respective types of DRM systems and do not recognize permission codes. Thus, when exporting and/or copying content to such storage media, permission conditions shall be translated to accommodate the target's DRM system.

In this standard, the act of outputting content to a non-compliant object from a permission code compliant object is referred to as "export". Meanwhile, the act of passing content back and forth within a permission code compliant object or between permission code compliant objects is referred to as "management".

4.2.6 Harmonization with DRM systems

As mentioned above, the permission code is primarily a language to indicate the terms of permission, and it does not have exclusive policy.

Every DRM system, no matter whether it is a new or existing one, can decide to use the permission code. On the contrary, every DRM system can decide not to use the permission code. Even if it decides to use the permission code, it could limit the application to a simple displaying of permission and keep without using for rights management.

In addition, the permission expressed by the permission code meets requirements of content holders and covers the range of permission expressed by existing DRM systems. Moreover, the permission code is designed to be extended for any additional requirements from new DRM permission and business model.

Therefore, no DRM system conflict with each other, by it uses the permission code or not, or by the operation of the permission code. In other words, the permission code harmonizes with all DRM systems. The permission code can be the central hub among DRM systems.

4.3 Components of a permission code

4.3.1 Permission actor

4.3.1.1 General

A permission actor is an actor that exchanges permission, or an actor that has its actions regulated as a result of permission, permission actors are comprised of three actors as follows.

- Permission issuer
- Permission receiver
- Content

These actors are each identified by a permission actor identifier, and linked to the permission code.

4.3.1.2 Permission actor identifier

A permission actor identifier is assigned to each respective permission actor. The identifier is used to distinguish the actors among issuer, receiver and content.

The permission code's permission actor identifier has the ability to subsume an existing ID system. For example, with respect to issuer IDs, some rights organizations maintain ID systems with member ids or internal management ids. Identifiers for internal management also exist for content. Open systems such as the ISBN code for publications are already in place. By placing a header/prefix specified in the permission code onto these existing id systems, these existing identifiers can be repurposed as permission actor identifiers. This allows for a smooth transition from existing systems.

With permission receivers in particular, the permission actor is frequently an individual end user without the kind of existing ID system mentioned above from which to draw upon. Furthermore, the DRM utilizing the permission code shall be able to decipher the nature of the user that would be accessing the content. For these purposes, the standard allows for identifiers of respective devices that intermediate the content distribution chain to serve as receiver IDs.

Permission actor ids are assigned and managed by id centers. Existing organizations such as rights holder agencies, for example, can become ID centers. This means existing organizations would be able to assign permission actor ids by combining the ID center code and a code from the existing code system used within the organization itself. There may be multiple ID centers for each permission actor category.

The following are some examples in which device IDs are used as alternate identifiers of individuals. Each example has its own respective pros and cons. The methodology chosen is left up to implementation and is out of scope of this standard. This standard will define the framework for permission actors only. The actual manner in which permission actor identifiers are assigned will be specified in a separate implementation-level document.

- Use identifiers (serial numbers etc.) that belong to viewing, recording and playback devices, such as televisions and video recorders, as alternate identifiers for individual end users.
- Use identifiers (serial numbers etc.) that belong to integrated or removable storage media, such as HDD, DVD media and memory cards, as alternate identifiers for individual end users.
- Use identifiers (phone numbers etc.) that belong to quasi-personal devices (devices that can generally be thought of as belonging to an individual, though not in the strictest sense), such as cell phones, as alternate identifiers for individual end users.

4.3.1.3 Domain

A domain in this standard refers to a set of actors to which a common set of rules apply in the context of content management. These common set of rules can be applied to each piece of content, or applied independently from content.

Generally, usage permissions for content have been bound to storage media or devices. For example, "this content cannot be copied to other storage media," or "this content can only be played on this device", are some of the common ways in which content have been handled. However, when permission is granted to a domain instead, all storage media and devices that belong to it are handled equally and will operate under a common set of permission terms and rules.

For example, consider home domains. A home domain refers to "a set of devices present within a given home. A content permission issuer can issue permission to freely copy content a within the home domain." Here, the permission receiver would have the ability to handle content a in accordance with the common rule: content a can be freely copied within the home domain.

Likewise, a set of devices that belong to a school can be defined as a school domain. Assuming content b will be used for educational purposes, a permission issuer can issue permission that “allows copying and editing of content b within the school domain.” Here, the permission receiver would be able to extract and compile portions of content b needed, and insert them within the school’s own content to create new educational material. The permission receiver can also copy the resulting content to devices that belong to the school domain across classrooms.

As described, content usage permissions can be bound to domains. On the other hand, other types of permission bindings can also be supported. For example, permission can be bound to an individual storage media unit in a conventional manner (for example, “no copying allowed from this disk”). Permission can also be bound to an individual user (for example, only Mr. X can view this content). The advantage of binding permissions to domains in contrast to conventional permissions issued to individual units is in their ability to constrain undesirable diffusion of content for the benefit of rights holders while allowing for the sharing of content within a community.

An unlimited number of domains exist. A domain may encompass another, or domains may overlap each other. Examples of the types of domains and usage patterns within those domains include, “home domain: can freely copy content within the home,” “school domain: so long as the usage purpose is educational, content can be edited and used on devices that belong to the school” and “company domain,” etc.

As illustrated, a domain can be characterized as a collective of permission receivers. An actor that belongs to the domain is permitted to act as a receiver of the permission in question. In other words, a domain is also a permission receiver and is assigned a permission actor identifier.

The domains discussed in this standard are issuer-defined domains: the permission issuer and permission receiver set the domain based on mutually agreed terms when content use is granted. This domain is discussed in the following subclause.

4.3.1.4 Issuer-defined domain

An issuer-defined domain refers to a domain within which the content’s rights protection information can be shared. It is set forth by a permission issuer and is set based on mutual agreement between a permission issuer and a permission receiver.

In practice, the scope limits the issuer-defined domain to within the home or school etc., making it mostly equivalent to a physical boundary. Conceptually, however, it is not merely a grouping of adjoining devices, storage media or humans, but rather that with a more logically constructed scope. For example, in thinking about home domains, one can view not only the devices that physically exist within the home as part of the home domain, but also mobile devices that belong to a family member as well as appliances, etc. held in a vacation home as part of the devices that comprise the home domain. However, the manner by which one would determine whether or not these objects belong to the domain is outside of the scope of this standard and will be specified in a separate implementation-level document.

With educational content, as long as the usage purpose is educational, rights such as redistribution, fixation and edit are typically granted. One can assume that, in a school environment, multiple devices are linked through the network, and educational content is freely viewed, edited and stored. Consequently, it becomes necessary to ensure that the content would only be used inside the school. This is the reason why issuer-defined domains are defined.

Similarly, by defining issuer-defined domains such as a home domain, permission issuers can guarantee permission receivers the right to personal use of content within the home domain.

The significance of this domain is in its ability to enable permission issuers to confirm that their content is handled in accordance with the terms of the permission. This scheme assumes that the issuer of the permission code would have means with which to specify devices, storage media, and users that belong to the domain to ensure such confirmation can take place.

4.3.2 Permission classification

In this standard, permission classification is used to specify the permission's classification, and is comprised of disclosure class, usage purpose class, charge model class, billing class, application class, sponsor class, territory class, and usage class and is asserted positively. Therefore, the permission code interprets the contents indicated within the permission classification as permission granted by the permission issuer.

Permission classification describes the contents of notifications intended for human users. It is equivalent to, for example, copyright notices found at the beginning of packaged filmed entertainment.

4.3.3 Content usage

4.3.3.1 General

In this standard, the content usage and/or terms are comprised of the following 4 elements:

- a) General usage condition which describes conditions on a usage mode basis;
- b) Extended usage condition which describes extended conditions to the regular usage condition;
- c) Data management condition which describes conditions that pertain to saving the original content or re-issuing permission codes, and
- d) Data export condition which describes conditions that pertain to exporting original content to non-compliant objects.

When interpreting similar conditions, conditions that have stricter terms than the other shall be applied. Furthermore, the permission code shall be deemed non-interpretable in cases in which an interpretation by a non-compliant object causes a discrepancy.

4.3.3.2 General usage condition

General usage condition is comprised of the content's end usage mode, and the usage conditions that regulate such use. It represents permission to use content based on the permission issuer's specified usage mode, and its usage condition.

This standard will define three usage modes: play, print and execute.

4.3.3.3 Extended usage condition

Extended usage conditions supplement conditions that cannot be expressed as general usage conditions. This standard will not specify its contents.

4.3.3.4 Data management condition

Data management condition describes management conditions that apply when original content is fixed (stored) within a compliant object. It represents permission to manage content within a management target specified by the permission issuer in accordance with the management conditions specified.

This standard considers compliant objects as management targets.

4.3.3.5 Data export condition

Data export condition describes export conditions that apply when exporting content to non-compliant objects. It represents permission to export content to an export target specified by the permission issuer in accordance with the export conditions specified.

This standard defines general-purpose export conditions.

4.3.4 Content data handling

4.3.4.1 General

The permission code proposed assumes that, when transmitted, content and its permission code would follow the path illustrated in the diagram below. The diagram illustrates the permission management server which represents the permission manager for content, the distribution server and license server which represent distributors of content and licenses, and the domain which represents usage actors (including home and school, etc.) of content. We assume that the device within the domain that receives the permission code directly from the permission management server, distribution server or license server is capable of handling this specification's permission code. In addition, depending on the permission code setting, the compliant objects from within the domain may export to other non-compliant objects outside of the domain.

Permission Code Environment

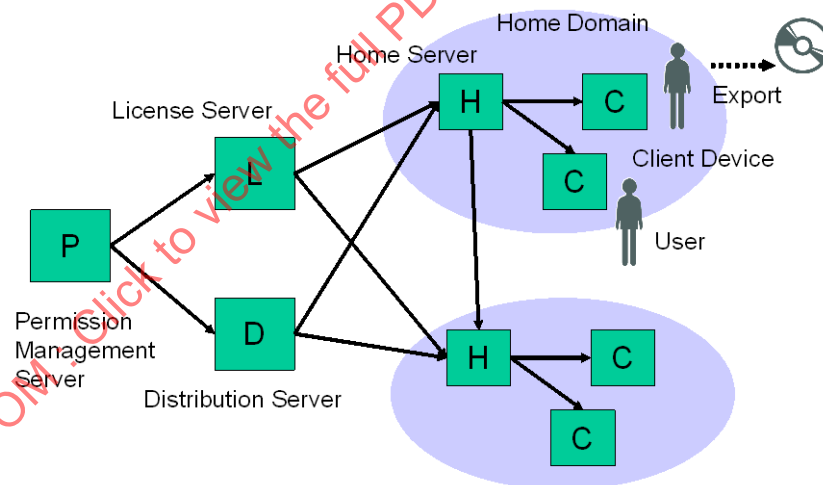


Figure 2 – Permission code environment

4.3.4.2 Data management among the permission code compliant objects

The permission code defines the domain as a collective of devices etc. with unique identifiers. Here, devices may include a storage device, a playback device, an editing device, or an ID card identifying a user. The permission issuer either directly (with identifiers) or indirectly (through the number of device IDs managed by a home server) ascertains devices present within a specific domain.

Respective devices within the domain are allowed to handle data on an equal basis within the scope of the permission code in exchange for having devices that belong to the domain ascertained by permission issuers. Specifically, all devices within the domain are allowed to handle data in accordance with the permission, including storing data, transcoding and play.

4.3.4.3 Data export to non-permission code compliant objects

With respect to data export to non-permission code compliant objects (devices and domains), the permission code is configured assuming the following 3 cases. Note that many cases involving export to non-permission code compliant objects limit the number of times export can occur. In this case, it becomes necessary for a specific device to uniformly manage the number of exports.

- a) Instances in which the data export target required for the use of data is not permission code compliant, such as the case with export to a display device or a speaker etc.
- b) Instances in which export to non permission code compliant storage media such as CPRM compliant DVD-R is allowed. Or, instances in which export to transmission media such as DTCP etc. is allowed.
- c) Instances in which content is exported to another non-permission code compliant object.

After export to a non-permission code compliant object, the permission code can neither manage nor control the behaviour of content nor devices. However, by translating the permission code to the export target DRM system's content control information, interoperability between permission code compliant objects and legacy DRM systems can be achieved.

5 Permission code configuration

5.1 General

This clause will discuss the permission code's format. The primary purpose of permission codes, as aforementioned, is to communicate the permission issuer's permission intent to the permission receiver. Therefore, the manner in which respective DRM systems operate in accordance with the permission code is entirely left to the operating policies of respective DRM systems and/or the implementation of respective devices. Hence, interpretation of the permission code at the operating level shall be specified within respective DRM specifications.

Furthermore, the terms specified within the permission code can generally be thought of in two categories:

- a) a description of the contents to be communicated to an end user (human), and
 - b) a description of operating instructions geared towards devices that comprise the DRM system.
- a) refers to, for example, an equivalent to copyright notices displayed at the beginning of packaged filmed entertainment. In many cases, it does not possess enforceable power with respect to DRM systems. b) refers to the equivalent to copy control information. The intent is for DRM systems that interpret this permission code to operate in accordance with the respective terms contained within the permission code.

This standard will place a † mark on the former to distinguish these two categories.

The permission code has another configuration policy, data size saving. It is assumed that the permission code is protected by TRMs, which cost much more than non-TRMs in aspect of processing and storage. Therefore, the permission information is expressed in coded style as the permission code, other than redundant description such as XML, in order to minimize its length and necessary data processing in consideration of being processed by TRMs directly.

5.2 Notation

5.2.1 Numerical values

5.2.1.1 Decimal notation

A decimal number is expressed as decimal digits 0 to 9.

5.2.1.2 Hexadecimal notation

A hexadecimal number is expressed as hexadecimal digits 0 to 9 and A to F prefixed by the symbol "0x".

5.2.1.3 Binary notation

A binary number is expressed as binary digits 0 or 1 suffixed by the symbol b.

5.2.1.4 Bit string

bslbf shall be a bit string with left bit first.

5.2.1.5 Unsigned numerical value

uimsbf shall be an unsigned integer with most significant bit first.

5.2.1.6 Distinct tags

A distinct tag is expressed as follows. See 5.3.

Table 1 – Distinct tag interpretation

Value	Tag
0x00	Reserved
0x01	Version unit
0x02-0x0F	Reserved
0x10	Permission actor unit
0x11	Permission classification unit
0x12	General usage condition unit
0x13	Extended usage condition unit
0x14	Data management condition unit
0x15	Data export condition unit

5.2.1.7 Reserved field

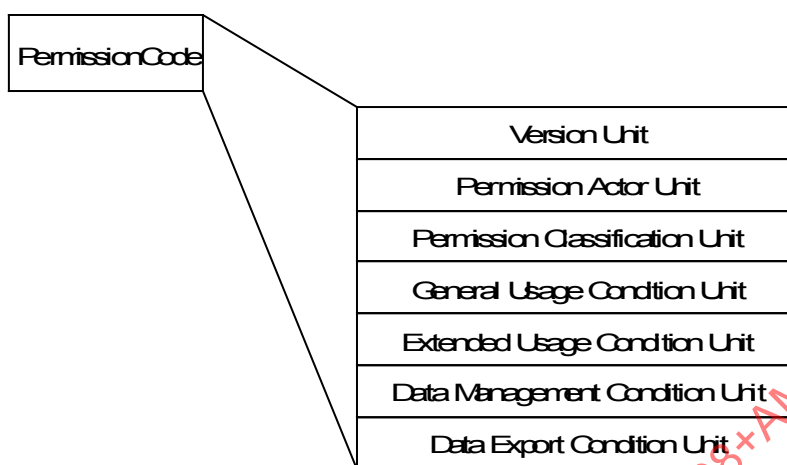
All bits in the reserved fields shall be set to 0b.

5.3 Permission code system

The permission code is comprised of seven kinds of information units, as shown below.

While the permission code is comprised of multiple units, it does not necessarily require all units. Some units may be omitted depending on the nature of the permission contents. In addition, while the general order is as follows, it is not limited to this order.

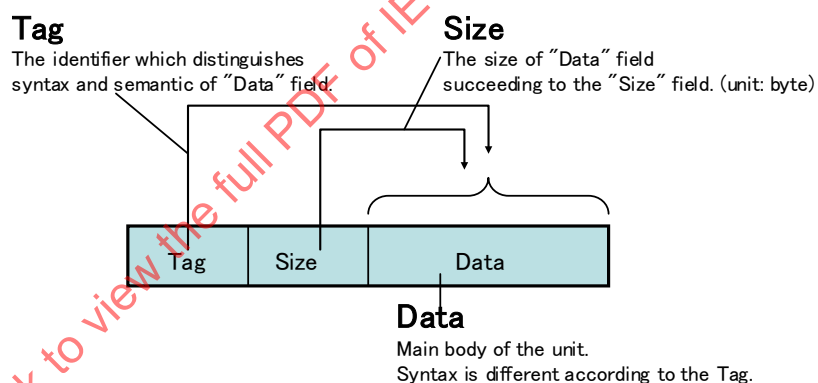
The permission code has a hierarchical structure, tag – length – main data. The top tag determines the main data portion's syntax. Please refer to 5.2.1.6 for more information regarding tags.



IEC 695/08

Figure 3 – Permission code configuration

Permission Code –
Basic Structure of Each Unit



IEC 696/08

Figure 4 – Basic structure of permission code unit

5.4 Version unit

5.4.1 Structure

Table 2 – Structure of version unit

RBP	Length in bytes	Field name	Contents
0	1	Version unit tag	TAG
1	1	Reserved	bslbf
2	1	Version	VER

5.4.2 Version unit tag

This field shall be set to 0x01.

5.4.3 Reserved

This field shall be reserved for future standardization and all bytes shall be set to 0x00.

5.4.4 Version

This field shall be set to 0x10. It means version 1.0. The first 4 bits represent the major-version, and the 4 bits that follow represent the minor-version.

5.5 Permission actor unit

5.5.1 Structure

Table 3 – Structure of permission actor unit

RBP	Length in bytes	Field name	Contents
0	1	Permission actor unit tag	TAG
1	1	Total bytes of identifiers (=S)	uimsbf
2	id1	Content ID descriptor (=id1)	bslbf
2+id1	id2	Issuer ID descriptor (=id2)	bslbf
2+id1+id2	S-id1-id2	Receiver ID descriptor	bslbf

With respect to permission codes, the authority to assign permission actor identifiers belongs to ID centers that manage the permission actors. Thus, permission actors are expressed using the combination of identifiers assigned to these ID centers (refer to 5.5.4.4, 5.5.5.5, 5.5.6.5), and unique identifiers that are assigned by respective organizations based upon their own respective policies.

Hence, with respect to the latter unique ID, existing proprietary ID systems maintained by rights management ID centers can be used on an “as is” basis, allowing for a smooth migration to the use of permission codes.

5.5.2 Permission actor unit tag

This field shall be set to 0x10.

5.5.3 Total bytes of identifiers

This field represents the total bytes allotted for content ID, issuer ID and receiver ID descriptors.

5.5.4 Content identifier

5.5.4.1 Structure

Table 4 – Structure of content identifier descriptor

Syntax	Bits	Identifier
Content_Identifier_descriptor() { content_type_code	16	bslbf
if ((content_type_code >> 8) == ASCII) { Country Code	16	char(2)
ID Center Code	32	char(4)
Unique Code	64	char(8)
} else { extended_identifier_length	16	uimbsf
extended_identifier	n	bslbf
} }		

5.5.4.2 Content type code

This field represents the content classification. Table 5 shows the interpretation of content type code when its first byte is ASCII. Otherwise, it is reserved.

Table 5 – Content type code interpretation

Content classification	Interpretation
SM	Sound Music
SD	Sound Drama
SP	Sound Program
SN	Sound News
SA	Sound Ad
SO	Sound Object
VM	Visual Music
VD	Visual Drama
VP	Visual Program
VF	Visual Film
VC	Visual Comic
VN	Visual News
VA	Visual Ad
VO	Visual Object
TP	Text Program
TD	Text Drama
TM	Text Music
TT	Text Thesis
TN	Text News
TO	Text Object
IB	Image Book
IP	Image Program
II	Image Illustration
IC	Image Comic
IM	Image Music

Content classification	Interpretation
IA	Image Ad
IO	Image Object
PG	Program Game
PS	Program Soft
PM	Program Music
PA	Program Ad
PO	Program Object
GG	General Group

5.5.4.3 Country code

The value of this field utilizes the two letter ISO country code (ISO 3136-1) format.

5.5.4.4 ID center code

This field represents the identifier assigned to the ID center.

5.5.4.5 Unique code

This field represents the unique code assigned by the ID center.

5.5.4.6 extended_identifier_length

This field describes the length of the extended identifier in bytes. The value of this field depends on its own structure.

5.5.4.7 extended_identifier

This field represents the extended identifier necessary to further identify the target content in question.

5.5.5 Issuer identifier

5.5.5.1 Structure

Table 6 – Structure of issuer identifier descriptor

Syntax	Bits	Identifier
Issuer_Identifier_descriptor() { issuer_role_code if (issuer_role_code == ASCII) { Country Code Issuer Configuration Code ID Center Code Unique Code } else { extended_identifier_length extended_identifier } }	8 16 8 32 64 16 n	bslbf char(2) char(1) char(4) char(8) uimsbf bslbf

5.5.5.2 Issuer role code

This field represents the issuer's role with respect to the permission.

Table 7 – Issuer role code interpretation

Value	Interpretation
0x00-0x43	Reserved
0x44	Distributor identifier
0x45-0x47	Reserved
0x48	Holder identifier
0x49-0xff	Reserved

5.5.5.3 Country code

The value of this field utilizes the two letter ISO country code (ISO 3136-1) format.

5.5.5.4 Issuer configuration code

This field represents the Issuer's configuration with respect to its operation.

Table 8 – Issuer configuration code interpretation

Issuer configuration	Interpretation
O	Organization
C	Company
I	Individual
D	Device (including storage medium)

5.5.5.5 ID center code

This field represents an identification number assigned to the issuer with respect to its configuration in the order of application (2 digit number). If the issuer configuration code is D (device), there is no operator code.

5.5.5.6 Unique code

This field represents the unique code assigned within the operator's operating configuration.

5.5.5.7 extended_identifier_length

This field describes the length of the extended identifier in bytes. The value of this field depends on its own structure.

5.5.5.8 extended_identifier

This field represents the extended identifier necessary to further identify the target Issuer in question.

5.5.6 Receiver identifier

5.5.6.1 Structure

Table 9 – Structure of receiver identifier descriptor

Syntax	Bits	Identifier
Receiver_Identifier_descriptor() { receiver_role_code if (receiver_role_code == ASCII) { Country code Receiver configuration code ID center code Unique code } else { extended_identifier_length extended_identifier } }	8 16 8 32 64 16 n	bslbf char(2) char(1) char(4) char(8) uimsbf bslbf

5.5.6.2 Receiver role code

This field represents the receiver's role with respect to permission.

Table 10 – Receiver role code interpretation

Value	Interpretation
0x00-0x43	Reserved
0x44	Distributor identifier
0x45-0x47	Reserved
0x48	Holder identifier
0x49-0x54	Reserved
0x55	User identifier
0x56-0xff	Reserved

5.5.6.3 Country code

The value of this field utilizes the two letter ISO country code (ISO 3136-1) format.

5.5.6.4 Receiver configuration code

This field represents the receiver's configuration with respect to its operation.

Table 11 – Receiver configuration code interpretation

Receiver configuration	Interpretation
O	Organization
C	Company
I	Individual
D	Device (including storage medium)

5.5.6.5 ID center code

This field represents an identification number assigned to the receiver with respect to its configuration in the order of application (2 digit number). If the receiver configuration code is D (device), there is no operator code.

5.5.6.6 Unique code

This field represents the unique code assigned within the operator's operating configuration.

5.5.6.7 extended_identifier_length

This field describes the length of the extended identifier in bytes. The value of this field depends on its own structure.

5.5.6.8 extended_identifier

This field represents the extended identifier necessary to further identify the target receiver in question.

5.6 Permission classification unit†

5.6.1 Structure

Table 12 – Structure of permission classification unit

Relative bit position	Length in bits	Field name	Contents
0	8	Permission classification unit tag	TAG
8	8	Reserved	bslbf
16	2	Disclosure class	bslbf
18	3	Usage purpose class	bslbf
21	5	Charge model class	bslbf
26	2	Billing class	bslbf
28	2	Application class	bslbf
30	2 4	Sponsor class	bslbf
32 34	3	Territory class	bslbf
35 37	13 19	Usage class	bslbf

5.6.2 Permission classification unit tag

This field shall be set to 0x11.

5.6.3 Reserved

This field shall be reserved for future standardization and all bytes shall be set to 0x00.

5.6.4 Disclosure class

This class specifies the terms of disclosure for the permission, including open permission and closed permission.

Table 13 – Structure of disclosure class

Syntax	Bits	Identifier
Disclosure_Class () { disclosure_type }	2	bslbf

The disclosure type field specifies the type of disclosure class.

Table 14 – disclosure_type (DT) interpretation

Value	Interpretation
00b	Reserved
01b	Indicates DT is open permission
10b	Indicates DT is closed permission
11b	Indicates DT is other

5.6.5 Usage purpose class

5.6.5.1 Structure

This class specifies the usage purpose for the permission, including commercial, public and promotion.

Table 15 – Structure of usage purpose class

Syntax	Bits	Identifier
Usage_Purpose_Class () { usage_purpose_type }	3	bslbf

5.6.5.2 usage_purpose_type

This field specifies the type of usage purpose class.

Table 16 – usage_purpose_type (UPT) interpretation

Value	Interpretation
000b	Reserved
001b	Indicates UPT is commercial permission
010b	Indicates UPT is public permission
011b	Indicates UPT is not-for-profit permission
100b	Indicates UPT is promotion permission
101b	Indicates UPT is education permission
111b	Indicates UPT is other

5.6.6 Charge model class

5.6.6.1 Structure

This class specifies the charge model for the permission.

Table 17 – Structure of charge model class

Syntax	Bits	Identifier
Charge_Model_Class () { charge_model_type if (charge_model_type==10b) { pay_per_use_flag subscription_flag coupon_flag } else { reserved } }	2 1 1 1 3	bslbf bslbf bslbf bslbf bslbf

5.6.6.2 charge_model_type

This field specifies the type of charge model class.

Table 18 – charge_model_type (CMT) interpretation

Value	Interpretation
00b	Reserved
01b	Indicates CMT is free of charge
10b	Indicates CMT is for charge
11b	Indicates CMT is other

5.6.6.3 pay_per_use_flag

If value is 1b, it indicates the content is permitted to be charged as pay-per-use. If value is 0b, it indicates the content is not permitted to be charged as pay-per-use.

5.6.6.4 subscription_flag

If value is 1b, it indicates the content is permitted to be distributed as subscription. If value is 0b, it indicates the content is not permitted to be distributed as subscription.

5.6.6.5 coupon_flag

If value is 1b, it indicates the content is permitted to be distributed in exchange for coupons. If value is 0b, it indicates the content is not permitted to be distributed in exchange for coupons.

5.6.7 Billing class

This class specifies the terms of billing for the permission.

If CMT is free of charge, it should be other (11b).

Table 19 – Structure of billing class

Syntax	Bits	Identifier
Billing_Class () { billing_type }	2	bslbf

The billing_type field specifies the type of billing class.

Table 20 – billing_type (BT) interpretation

Value	Interpretation
00b	Reserved
01b	Indicates BT is ad hoc billing
10b	Indicates BT is blanket billing
11b	Indicates BT is other

5.6.8 Application class

This class specifies the terms of application for the permission, including ad hoc permission and blanket permission.

Table 21 – Structure of application class

Syntax	Bits	Identifier
Application_Class () { application_type }	2	bslbf

The application_type field specifies the type of application class.

Table 22 – application_type (AT) interpretation

Value	Interpretation
00b	Reserved
01b	Indicates AT is ad hoc permission
10b	Indicates AT is blanket permission
11b	Indicates AT is other

5.6.9 Sponsor class

This class specifies the terms of sponsorship for the permission and is including advertising model, premium model, coupon model and personal information disclosure model. When selecting advertising model, an option amongst time synchronized forced viewing, pre/post viewing, time arbitrary, and blanket shall be specified.

Table 23 – Structure of sponsor class

Syntax	Bits	Identifier
Sponsor_Class () { sponsor_type }	4	bslbf

The sponsor_type field specifies the type of sponsor class.

Table 24 – Configuration of sponsor_type (ST)

Value	Interpretation
0000b	Indicates ST does not exist
0001b	Reserved
0010b	Indicates ST is advertising model / no forced viewing
0011b	Indicates ST is advertising model / time synchronized forced viewing
0100b	Indicates ST is advertising model / pre/post viewing
0101b	Indicates ST is advertising model / arbitrary time
0110b	Indicates ST is advertising model / blanket
0111b	Indicates ST is advertising model / other
1000b	Indicates ST is premium model
1001b	Indicates ST is coupon model
1010b	Indicates ST is privacy information disclosure model
1111b	Indicates ST is other

5.6.10 Territory class

This class specifies the applicable territory for the permission, including country, area, domain and device, etc. An “and” condition is used to specify multiplicity when the permission is intended for multiple territories. Territory is the equivalent of “region code” in DVD-Video.

Table 25 – Structure of territory class

Syntax	Bits	Identifier
Territory_Class () { territory_id }	3	bslbf

The “territory_id” field specifies the identifier for the territory.

5.6.11 Usage class

5.6.11.1 Structure

This class specifies the terms of use for the permission, including broadcast permission and streaming permission.

Portions of the usage class overlap with contents within general usage condition, data management condition and data export condition, mentioned later in this standard. Nonetheless, contents of the permission specified within the usage class are messages intended for users (humans), and/or recordings of contract terms by implication.

Table 26 – Structure of usage class

Syntax	Bits	Identifier
Usage_Class () {		
usage_type	3	bslbf
redistribution_type	2	bslbf
move_flag	1	bslbf
copy_flag	1	bslbf
export_flag	1	bslbf
share_flag	1	bslbf
edit_flag	1	bslbf
modify_flag	1	bslbf
super_distribution_flag	1	bslbf
reserved	7	bslbf
}		

5.6.11.2 usage_type

This field specifies the type of usage class.

Table 27 – Usage_type (UT) interpretation

Value	Interpretation
000b	Reserved
001b	Indicates UT is non-fixation permission – Broadcast Permission
010b	Indicates UT is non-fixation permission – Streaming permission
011b	Indicates UT is other
100b	Indicates UT is fixation permission – Broadcast storage permission (programmed) – No reuse permission
101b	Indicates UT is fixation permission – Broadcast storage permission (programmed) – Reuse permission
110b	Indicates UT is fixation permission – Download permission (on-demand) – No reuse permission
111b	Indicates UT is fixation permission – Download permission (on-demand) – Reuse permission

5.6.11.3 redistribution_type

This field specifies the type of redistribution class.

Table 28 – Configuration of redistribution_Type

Value	Interpretation
00b	Reserved
01b	Indicates simultaneous redistribution if usage type is 001b, 101b Indicates programmed streaming if usage type is 010b, 111b
10b	Indicates redistribution within area if usage type is 001b, 101b Indicates on-demand streaming if usage type is 010b, 111b
11b	Indicates redistribution outside of area if usage type is 001b, 101b

5.6.11.4 move_flag

If value is 1b, it indicates the content is permitted to be moved. If value is 0b, it indicates the content is not permitted to be moved.

5.6.11.5 copy_flag

If value is 1b, it indicates the content is permitted to be copied (or, duplicated). If value is 0b, it indicates the content is not permitted to be copied.

5.6.11.6 export_flag

If value is 1b, it indicates the content is permitted to be exported to storage media other than the one in which it is currently stored. If value is 0b, it indicates the content is not permitted to be exported.

5.6.11.7 share_flag

If value is 1b, it indicates the content is permitted to be shared among multiple users or organizations. If value is 0b, it indicates the content is not permitted to be shared.

5.6.11.8 edit_flag

If value is 1b, it indicates the content is permitted to be edited. If value is 0b, it indicates the content is not permitted to be edited.

5.6.11.9 modify_flag

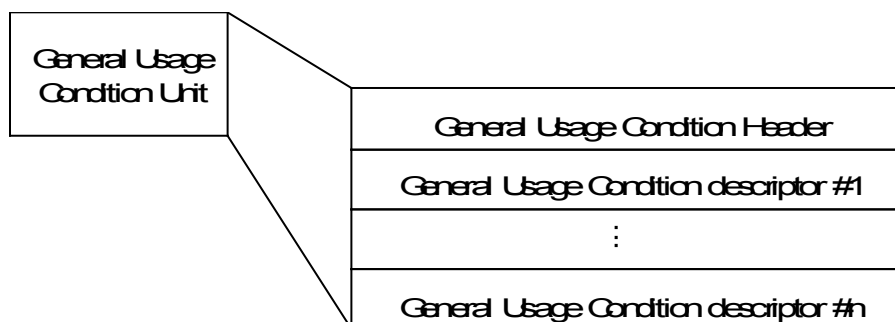
If value is 1b, it indicates the content is permitted to be modified. If value is 0b, it indicates the content is not permitted to be modified.

5.6.11.10 super_distribution_flag

If value is 1b, it indicates the content is permitted to be super-distributed. If value is 0b, it indicates the content is not permitted to be distributed via super-distribution.

5.7 General usage condition unit

5.7.1 Unit structure



IEC 697/08

Figure 5 – General usage condition unit

5.7.2 General usage condition header

5.7.2.1 Structure

Table 29 – Structure of general usage condition header

RBP	Length in bytes	Field name	Contents
0	1	General usage condition tag	TAG
1	2	Length of general usage condition descriptor(s)	uimsbf
3	1	Number of general usage condition descriptor(s)	uimsbf

5.7.2.2 General usage condition tag

This field shall be set to 0x12.

5.7.2.3 Length of general usage condition descriptor(s)

This field specifies the length of general usage condition descriptor(s) in bytes.

5.7.2.4 Number of general usage condition descriptors

This field specifies the number of general usage condition descriptors following this field.

5.7.3 General usage condition descriptor

5.7.3.1 Structure

Each general usage condition descriptor specifies a descriptor tag, descriptor length and usage conditions.

Table 30 – Tag values of descriptors

Value	Tag
0x00	Reserved
0x01	Playback usage condition descriptor
0x02	Print usage condition descriptor
0x03	Execute usage condition descriptor
0x04-0xff	Reserved

5.7.3.2 Playback usage condition descriptor

5.7.3.2.1 Structure

Table 31 – Structure of playback usage condition descriptor

Syntax	Bits	Identifier
playback_usage_condition_descriptor() {		
descriptor_tag	8	uimbsf
descriptor_length	8	uimbsf
quality_parameter	4	uimbsf
permission_management_model_parameter	4	uimbsf
playlist_parameter	1	bslbf
playback_count_control_flag	1	bslbf
time_period_control_flag	1	bslbf
day_count_control_flag	1	bslbf
date_period_control_flag	1	bslbf
reserved	4 3	bslbf
if (playback_count_control_flag == 1b) {		
playback_count_parameter	8	uimbsf
}		
if (time_period_control_flag == 1b) {		
accumulation_flag	1	bslbf
time_period_parameter	31	uimbsf
}		
if (day_count_control_flag == 1b) {		
day_count_parameter	8	uimbsf
}		
if (date_period_control_flag == 1b) {		
start_date_parameter	40	imsbf
end_date_parameter	40	imsbf
}		
simultaneous_output_parameter	8	uimbsf
parental_guidance_parameter	8	uimbsf
usage_time_frame_parameter	16	uimbsf
}		

5.7.3.2.2 descriptor_tag

This field shall be set to 0x01.

5.7.3.2.3 descriptor_length

This field specifies the length of the descriptor in bytes.

5.7.3.2.4 quality_parameter

Quality parameter conforms to usage quality levels. If more than 1 level is applied, it indicates all applied levels are permitted. For example, if both LV1F and LV2F are asserted, the content is permitted for use in both high quality and standard quality settings.

Quality parameter is a parameter that constrains the usage quality of content. Quality is specified at 4 levels. These levels include high quality, standard, low quality and extension.

- LEVEL1 (high quality) flag (LV1F)
If value is 1b, it indicates permission applies to LEVEL1 (high quality). If value is 0b, it indicates it does not apply.
- LEVEL2 (standard) flag (LV2F)
If value is 1b, it indicates permission applies to LEVEL2 (standard). If value is 0b, it indicates it does not apply.
- LEVEL3 (low quality) flag (LV3F)
If value is 1b, it indicates permission applies to LEVEL3 (low quality). If value is 0b, it indicates it does not apply.
- LEVEL4 (extension) flag (LV4F)
If value is 1b, it indicates permission applies to LEVEL4 (extension). If value is 0b, it indicates it does not apply.

5.7.3.2.5 permission_management_model_parameter

Permission management model parameter is a parameter that limits the permission management method of the content. There are 4 permission management models. These are DRM, digital watermark, rights reporting and extension. If more than 1 level is applied, that shows all applied levels are permitted. For example, if both DRMF (DRM flag) and DWF (digital watermark flag) are asserted, the content is permitted for use with DRM or with digital watermark.

- DRM flag (DRMF)
If value is 1b, it indicates that protection by DRM is required. If value is 0b, it indicates that protection by DRM is not required.
- digital watermark flag (DWF)
If value is 1b, it indicates that protection by digital watermark is required. If value is 0b, it indicates that protection by digital watermark is not required.
- rights reporting flag (RRF)
If value is 1b, it indicates that rights reporting is required. If value is 0b, it indicates that rights reporting is not required.
- extension flag (EXTF)
If value is 1b, it indicates Permission applies to extension. If value is 0b, it indicates it does not apply.

5.7.3.2.6 playlist_parameter

If value is 1b, it indicates playback through a playlist is permitted. If value is 0b, playback through a playlist is not permitted.

NOTE Playback through playlist may be referred to as “playlist edit”. In “playlist edit”, the content itself is not edited, but playback sequence is. Be careful to note the difference from “time-line edit” defined in 5.9.3.11.

5.7.3.2.7 playback_count_control_flag

If value is 1b, it indicates playback count control applies. If value is 0b, it indicates it does not apply.

5.7.3.2.8 time_period_control_flag

If value is 1b, it indicates time period control applies. If value is 0b, it indicates it does not apply.

NOTE If both time_period_parameter and day_count_paramter are described, the time_period_parameter is prior.

5.7.3.2.9 day_count_control_flag

If value is 1b, it indicates day count control applies. If value is 0b, it indicates it does not apply.

5.7.3.2.10 date_period_control_flag

If value is 1b, it indicates date period control applies. If value is 0b, it indicates it does not apply.

5.7.3.2.11 playback_count_parameter

This field specifies the number of times the content can be played back.

5.7.3.2.12 accumulation_flag

If value is 1b, it measures day count and time control with cumulative time. If value is 0b, it measures day count and time control with absolute time.

5.7.3.2.13 time_period_parameter

This field specifies the number of seconds the content can be played back for.

5.7.3.2.14 day_count_parameter

This field specifies the number of days the content can be played back for.

5.7.3.2.15 start_date_parameter

This field specifies the start date from which the content can be played back. The unit of value is second and the value '0' shows Jan. 1st, 1970 00:00:00 UTC.

5.7.3.2.16 end_date_parameter

This field specifies the end date till which the content can be played back. The unit of value is second and the value '0' shows Jan. 1st, 1970 00:00:00 UTC.

5.7.3.2.17 simultaneous_output_parameter

This field represents the maximum number of simultaneous access to content. If value is 0xff, it indicates simultaneous access is not limited. The value 0x00 is reserved for future use.

5.7.3.2.18 parental_guidance_parameter

This field represents the content's parental guidance rating. Parental guidance specifies the applicable age range through the rating system. If value is 0xff, it indicates the applicable age is not limited. The value 0x00 is reserved for future use.

5.7.3.2.19 usage_time_frame_parameter

This field specifies the number of seconds of playback time-frame. The playback device determines "one playback incident" when the content is played back for the seconds specified by this field.

5.7.3.3 Print usage condition descriptor

5.7.3.3.1 Structure

Table 32 – Structure of print usage condition descriptor

Syntax	Bits	Identifier
print_usage_condition_descriptor() {		
descriptor_tag	8	uimsbf
descriptor_length	8	uimsbf
quality_parameter	4	uimsbf
permission_management_model_parameter	4	uimsbf
printout_count_control_flag	1	bslbf
time_period_control_flag	1	bslbf
day_count_control_flag	1	bslbf
date_period_control_flag	1	bslbf
reserved	4	bslbf
if (printout_count_control_flag == 1b) {		
printout_count_parameter	8	uimsbf
}		
if (time_period_control_flag == 1b) {		
reserved	1	bslbf
time_period_parameter	31	uimsbf
}		
if (day_count_control_flag == 1b) {		
day_count_parameter	8	uimsbf
}		
if (date_period_control_flag == 1b) {		
start_date_parameter	40	imsbf
end_date_parameter	40	imsbf
}		
parental_guidance_parameter	8	uimsbf
}		

5.7.3.3.2 descriptor_tag

This field shall be set to ~~0x04~~ 0x02.

5.7.3.3.3 descriptor_length

This field describes the length of the descriptor in bytes.

5.7.3.3.4 quality_parameter

Quality parameter conforms to usage quality levels. If more than 1 level is applied, it indicates all applied levels are permitted. For example, if both LV1F and LV2F are asserted, the content is permitted for use in both high quality and standard quality settings.

Quality parameter is a parameter that constrains the usage quality of content. Quality is specified at 4 levels. These levels include high quality, standard, low quality and extension.

- LEVEL1 (high quality) flag (LV1F)
If value is 1b, it indicates permission applies to LEVEL1 (high quality). If value is 0b, it indicates it does not apply.
- LEVEL2 (standard) flag (LV2F)
If value is 1b, it indicates permission applies to LEVEL2 (standard). If value is 0b, it indicates it does not apply.
- LEVEL3 (low quality) flag (LV3F)
If value is 1b, it indicates permission applies to LEVEL3 (low quality). If value is 0b, it indicates it does not apply.
- LEVEL4 (extension) flag (LV4F)
If value is 1b, it indicates permission applies to LEVEL4 (extension). If value is 0b, it indicates it does not apply.

5.7.3.3.5 permission_management_model_parameter

Permission management model parameter is a parameter that limits the permission management method of the content. There are 4 permission management models. These are DRM, digital watermark, rights reporting, and extension. If more than 1 level is applied, that shows all applied levels are permitted. For example, if both DRMF (DRM flag) and DWF (digital watermark flag) are asserted, the content is permitted for use with DRM or with digital watermark.

- DRM flag (DRMF)
If value is 1b, it indicates that protection by DRM is required. If value is 0b, it indicates that protection by DRM is not required.
- digital watermark flag (DWF)
If value is 1b, it indicates that protection by digital watermark is required. If value is 0b, it indicates that protection by digital watermark is not required.
- rights reporting flag (RRF)
If value is 1b, it indicates that rights reporting is required. If value is 0b, it indicates that rights reporting is not required.
- extension flag (EXTF)
If value is 1b, it indicates permission applies to extension. If value is 0b, it indicates it does not apply.

5.7.3.3.6 printout_count_control_flag

If value is 1b, it indicates printout count control applies. If value is 0b, it indicates it does not apply.

5.7.3.3.7 time_period_control_flag

If value is 1b, it indicates time period control applies. If value is 0b, it indicates it does not apply.

NOTE If both time_period_parameter and day_count_paramter are described, the time_period_parameter is prior.

5.7.3.3.8 day_count_control_flag

If value is 1b, it indicates day period control applies. If value is 0b, it indicates it does not apply.

5.7.3.3.9 date_period_control_flag

If value is 1b, it indicates date period control applies. If value is 0b, it indicates it does not apply.

5.7.3.3.10 printout_count_parameter

This field specifies the number of times the content can be printed.

5.7.3.3.11 time_period_parameter

This field specifies the number of seconds the content can be printed for.

5.7.3.3.12 day_count_parameter

This field specifies the number of days the content can be printed for.

5.7.3.3.13 start_date_parameter

This field specifies the start date from which the content can be printed. The unit of value is second, and the value '0' shows Jan. 1st, 1970 00:00:00 UTC.

5.7.3.3.14 end_date_parameter

This field specifies the end date till which the content can be printed. The unit of value is second, and the value '0' shows Jan. 1st, 1970 00:00:00 UTC.

5.7.3.3.15 parental_guidance_parameter

This field specifies the content's parental guidance rating. Parental guidance ratings specify the applicable age range of the content through a rating system. If value is 0x00, it indicates the parameter is reserved. If value is 0xff, it indicates the content is applicable to all ages.

5.7.3.4 Execute usage condition descriptor

5.7.3.4.1 Structure

Table 33 – Structure of execute usage condition descriptor

Syntax	Bits	Identifier
execute_usage_condition_descriptor() {		
descriptor_tag	8	uimsbf
descriptor_length	8	uimsbf
service_level_parameter	4	uimsbf
permission_management_model_parameter	4	uimsbf
execution_count_period_control_flag	1	bslbf
time_period_control_flag	1	bslbf
day_count_control_flag	1	bslbf
date_period_control_flag	1	bslbf
reserved	4	bslbf
if (execution_count_control_flag == 1b) {		
execution_count_parameter	8	uimsbf
}		
if (time_period_control_flag == 1b) {		
accumulation_flag	1	bslbf
reserved	7	bslbf
time_period_parameter	8	uimsbf
}		
if (day_count_control_flag == 1b) {		
day_count_parameter	8	uimsbf
}		
if (date_period_control_flag == 1b) {		
start_date_parameter	40	imsbf
end_date_parameter	40	imsbf
}		
parental_guidance_parameter	8	uimsbf
usage_time_frame_parameter	16	uimsbf
}		

5.7.3.4.2 descriptor_tag

This field shall be set to ~~0x02~~ 0x03.

5.7.3.4.3 descriptor_length

This field specifies the length of the descriptor in bytes.

5.7.3.4.4 service_level_parameter

Service level parameter is a parameter that constrains the level of functions which the content serves. It is specified at 4 levels. These levels include full control, standard, trial and extension.

If more than 1 level is applied, it indicates all applied levels are permitted. For example, if both LV1F and LV2F are asserted, the content is permitted for use in both high quality and standard quality settings.

- LEVEL1 (full control) flag (LV1F)
If value is 1b, it indicates permission applies to LEVEL1 (full control). If value is 0b, it indicates it does not apply.
- LEVEL2 (standard) flag (LV2F)
If value is 1b, it indicates permission applies to LEVEL2 (standard). If value is 0b, it indicates it does not apply.
- LEVEL3 (trial) flag (LV3F)
If value is 1b, it indicates permission applies to LEVEL3 (trial). If value is 0b, it indicates it does not apply.
- LEVEL4 (extension) flag (LV4F)
If value is 1b, it indicates permission applies to LEVEL4 (extension). If value is 0b, it indicates it does not apply.

5.7.3.4.5 permission_management_model_parameter

Permission management model parameter is a parameter that constrains the permission management method of the content. There are 4 permission management models. These models are under the management of DRM, digital watermark, rights reporting, and extension. If more than 1 level is applied, it indicates all applied levels are permitted. For example, if both LV1F and LV2F are asserted, the content is permitted for use under the management of either DRM or digital watermark or both.

- DRM flag (DRMF)
If value is 1b, it indicates that the protection by DRM is required. If value is 0b, it indicates that the protection by DRM is not required.
- digital watermark flag (DWF)
If value is 1b, it indicates that the protection by digital watermark is required. If value is 0b, it indicates that the protection by digital watermark is not required.
- rights reporting flag (RRF)
If value is 1b, it indicates that rights reporting is required. If value is 0b, it indicates that rights reporting is not required.
- extension flag (EXTF)
If value is 1b, it indicates permission applies to extension. If value is 0b, it indicates it does not apply.

5.7.3.4.6 execution_count_control_flag

If value is 1b, it indicates execution count control applies. If value is 0b, it indicates it does not apply.

5.7.3.4.7 time_period_control_flag

If value is 1b, it indicates time period control applies. If value is 0b, it indicates it does not apply.

NOTE If both time_period_parameter and day_count_paramter are described, the time_period_parameter is prior.

5.7.3.4.8 day_count_control_flag

If value is 1b, it indicates day count control applies. If value is 0b, it indicates it does not apply.

5.7.3.4.9 date_period_control_flag

If value is 1b, it indicates date period control applies. If value is 0b, it indicates it does not apply.

5.7.3.4.10 execution_count_parameter

This field specifies the number of times the content can be executed.

5.7.3.4.11 accumulation_flag

If value is 1b, it measures day count and time control with cumulative time. If value is 0b, it measures day count and time control with absolute time.

5.7.3.4.12 time_period_parameter

This field specifies the number of hours the permission receiver is allowed to execute the content for.

5.7.3.4.13 day_count_control_parameter

This field specifies the number of days the permission receiver is allowed to execute the content for.

5.7.3.4.14 start_date_parameter

This field specifies the start date from which the content can be executed. The unit of value is second, and the value '0' shows Jan. 1st, 1970 00:00:00 UTC.

5.7.3.4.15 end_date_parameter

This field specifies the end date till which the content can be executed. The unit of value is second, and the value '0' shows Jan. 1st, 1970 00:00:00 UTC.

5.7.3.4.16 parental_guidance_parameter

This field specifies the content's parental guidance rating. Parental guidance ratings specify the applicable age range of the content through a rating system. If value is 0x00, it indicates the parameter is reserved. If value is 0xff, it indicates the content is applicable to all ages.

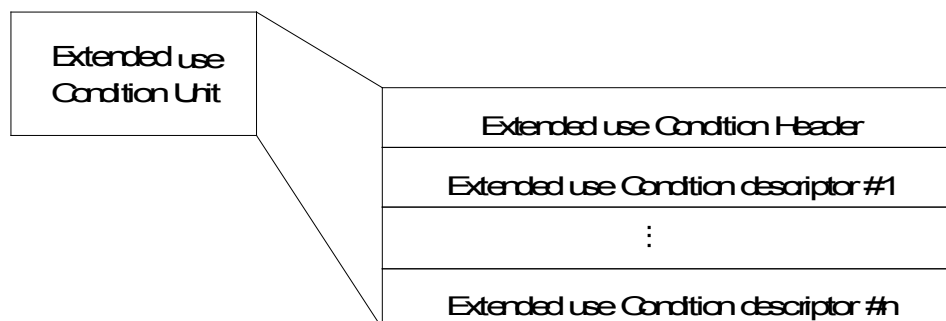
5.7.3.4.17 usage_time_frame_parameter

This field specifies the number of seconds of execution time-frame. The execute device determines one execution incident when the content is executed for the seconds specified by this field.

5.8 Extended use condition unit

~~This unit shall be reserved for future standardization.~~

5.8.1 Unit structure



IEC 2133/12

Figure 8 – Extended use condition unit

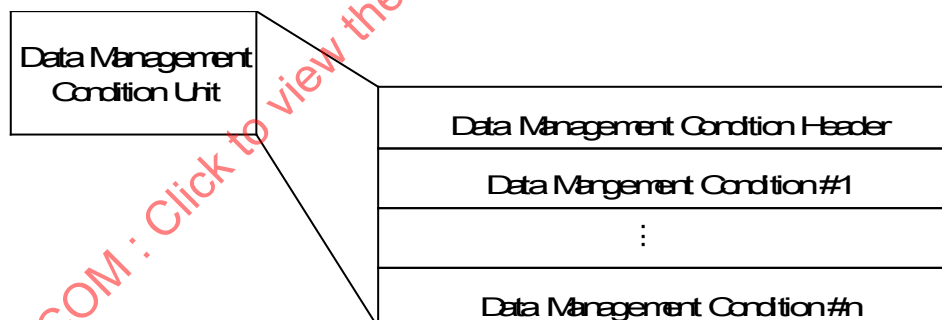
5.8.2 Extended use condition header

Table 46 – Structure of extended use condition header

RBP	Length in bytes	Field name	Contents
0	1	Extended use condition tag	TAG
1	2	Length of extended use condition(s)	uimsbf
3	1	Number of extended use condition descriptors	uimsbf

5.9 Data management condition unit

5.9.1 Unit structure



IEC 698/08

Figure 6 – Data management condition unit

With respect to data management conditions, there are instances in which detailed conditions change based on the device or user, etc. That manages the data. For example, copying may be allowed up to 5 times for a device within the domain, while copying is allowed only once for devices outside of the domain.

To express this, the data management condition unit has a header, and data management condition #n that corresponds to respective receiver identifiers subject to the respective terms.

5.9.2 Data management condition header

5.9.2.1 Structure

Table 34 – Structure of data management condition header

RBP	Length in bytes	Field name	Contents
0	1	Data management condition tag	TAG
1	2	Length of data management condition(s)	uimsbf
3	1	Number of data management conditions	uimsbf

5.9.2.2 Data management condition tag

This field shall be set to 0x14.

5.9.2.3 Length of data management condition(s)

This field specifies the length of data management condition(s) in bytes.

5.9.2.4 Number of data management conditions

This field specifies the number of data management conditions following this field.

5.9.3 Data management condition

5.9.3.1 Structure

Table 35 – Structure of data management condition

RBP	Length in bytes	Field name	Contents
0	16	Data management target identifier	bslbf
16	1	Encryption flag	bslbf
17	1	Copy count	uimsbf
18	1	Move count	uimsbf
19	4	Transcode type	bslbf
23	4	Maximum transcode rate	uimsbf
27	4	Minimum transcode rate	uimsbf
31	5	Expiration date	uimsbf
36	1	Sublicense count	uimsbf
37	1	Time-line edit	uimsbf

5.9.3.2 Data management target identifier

This field represents the target identifier to be managed. It is the same structure as the receiver identifier.

Each data management condition #n will apply the following conditions to the device, user, organization, domain, etc. That belongs to the ID specified within this field.

5.9.3.3 encryption_flag

Table 36 – Structure of encryption flag (EF)

bit7	bit0
Reserved	EF

If the value of TF is 1b, it indicates encryption is needed. If the value is 0b, it indicates encryption is not needed.

5.9.3.4 Copy count

This field specifies the number of times the content can be copied.

5.9.3.5 Move count

This field specifies the number of times the content can be moved.

5.9.3.6 Transcode type

This field specifies the type of transcoding.

Table 37 – Transcode type interpretation

Bit Position	Interpretation
0	Indicates transcode type is not limited
1	Indicates transcode type is mpeg-1
2	Indicates transcode type is mpeg-2
3	Indicates transcode type is ntsc
4	Indicates transcode type is h.264
5	Indicates transcode type is jpeg
6	Indicates transcode type is gif
7	Indicates transcode type is png
8	Indicates transcode type is linear pcm
9	Indicates transcode type is aac
10	Indicates transcode type is mp3
11-30	Reserved
31	Indicates transcode type is original encoding type (the content is never to be transcoded.)

5.9.3.7 Maximum transcode rate

This field specifies the rate of transcoding in kb/s. The value 0xffffffff means that maximum transcode rate is not limited.

5.9.3.8 Minimum transcode rate

This field specifies the rate of transcoding in kb/s. The value 0x00000000 means that minimum transcode rate is not limited.

5.9.3.9 Expiration date

This field specifies the expiration date to be managed.

If it indicates “not specified”, then it shall be 0xffffffff.

5.9.3.10 Sublicense count

This field specifies the number of sublicenses that can be issued. If value is 0x00, it indicates sublicensing is not permitted. If value is 0xff, it indicates sublicense count is unlimited.

5.9.3.11 Time-line edit**Table 38 – Structure of time-line flag (TF)**

bit7	bit0
Reserved	TF

If the value of TF is 1b, it indicates that editing the original content with respect to a time-line and saving the resulting content is permitted. If the value is 0b, it is not permitted.

NOTE “Time-line edit” defined here is to edit the entity of the content. Be careful about the difference from playlist edit which is “time-line edited playback”. See 5.7.3.2.6.

5.10 Data export condition unit

5.10.1 Unit structure

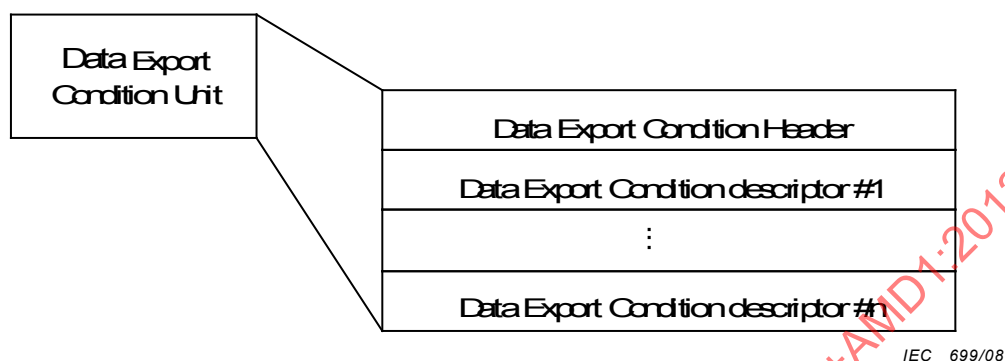


Figure 7 – Data export condition unit

5.10.2 Data export condition header

5.10.2.1 Structure

Table 39 – Structure of data export condition header

RBP	Length in bytes	Field Name	Contents
0	1	Data export condition tag	TAG
1	2	Length of data export condition(s)	uimsbf
3	1	Number of data export condition descriptors	uimsbf

5.10.2.2 Data export condition tag

This field shall be set to 0x15.

5.10.2.3 Length of data export condition(s)

This field specifies the length of data export condition(s) in bytes.

5.10.2.4 Number of data export condition descriptors

This field specifies the number of data export condition descriptors following this field.

5.10.3 Data export condition descriptor

Data export condition descriptor specifies a descriptor tag, descriptor length and export conditions.

Table 40 – Tag values of descriptors

Value	Tag
0x00	Reserved
0x01	General export descriptor
0x02-0xFF	Reserved

5.10.4 General export descriptor

5.10.4.1 Structure

Table 41 – Structure of general export descriptor

Syntax	Bits	Identifier
general_export_descriptor() {		
descriptor_tag	8	uimsbf
descriptor_length	8	uimsbf
storage_media_type	32	bslbf
encoding_type	32	bslbf
protection_type	32	bslbfbslbf
control_type	8	bslbf
move_indicate_flag	1	bslbf
time_period_control_flag	1	bslbf
day_count_control_flag	1	bslbf
date_period_control_flag	1	bslbf
reserved	4	bslbf
if (move_indecate_flag == 0b){		
export_count_parmameter	8	uimsbf
}		
if (time_period_control_flag == 1b) {		
reserved	1	bslbf
time_period_parameter	31	uimsbf
}		
if (day_count_control_flag == 1b) {		
day_count_parameter	8	uimsbf
}		
if (date_period_control_flag == 1b) {		
start_date_parameter	40	imsbf
end_date_parameter	40	imsbf
}		
}		

5.10.4.2 descriptor_tag

This field shall be set to 0x01.

5.10.4.3 descriptor_length

This field describes the length of the descriptor in bytes.

5.10.4.4 storage_media_type

This field represents the permitted type of storage media that the content can be exported to.

Table 42 – storage_media_type (SMT) interpretation

Bit position	Interpretation
0	Indicates SMT is not limited
1	Indicates SMT is CD
2	Indicates SMT is DVD
3	Indicates SMT is HDD
4	Indicates SMT is flush memory
5	Indicates SMT is HD-quality optical disc
6-31	Reserved

5.10.4.5 encoding_type

This field specifies the type of encoding that the content must be exported with.

Table 43 – encoding_type (ET) interpretation

Bit Position	Interpretation
0	Indicates ET is not limited
1	Indicates ET is MPEG-1
2	Indicates ET is MPEG-2
3	Indicates ET is NTSC
4	Indicates ET is H.264
5	Indicates ET is JPEG
6	Indicates ET is GIF
7	Indicates ET is PNG
8	Indicates ET is linear PCM
9	Indicates ET is AAC
10	Indicates ET is MP3
11-30	Reserved
31	Indicates ET is original encoding type (The Content is to be exported in the same encoding type as original Content. In other words, the Content is not transcoded.)

5.10.4.6 protection_type

This field represents the permitted type of protection under which the content must be exported.

Table 44 – protection_type (PT) interpretation

Bit position	Interpretation
0	Indicates PT is no protection (No content protection is required.)
1	Indicates PT is CPRM
2	Indicates PT is DTCP
3	Indicates PT is HDCP
4	Indicates PT is analog copy control
5	Indicates PT is CGMS
6	Indicates PT is SAFIA
7	Indicates PT is AACs
8	Indicates PT is VCPS
9-31	Reserved

5.10.4.7 control_type

This field represents the permitted protection control under which the content must be exported.

Table 45 – control_type (CT) interpretation

Value	Interpretation
0x00	Indicates CT is not specified
0x01-0x0F	Reserved
0x11	Indicates CT is copy never
0x12	Indicates CT is copy no more
0x13	Indicates CT is copy once
0x14-0xFF	Reserved

5.10.4.8 move_indicate_flag

If value is 1b, it indicates that export means move. If value is 0b, it indicates that export means copy.

5.10.4.9 time_period_control_flag

If value is 1b, it indicates time period control applies. If value is 0b, it indicates it does not apply.

NOTE If both time_period_parameter and day_count_paramter are described, the time_period_parameter is prior.

5.10.4.10 day_count_control_flag

If value is 1b, it indicates day count control applies. If value is 0b, it indicates it does not apply.

5.10.4.11 date_period_control_flag

If value is 1b, it indicates date period control applies. If value is 0b, it indicates it does not apply.

5.10.4.12 export_count_parameter

This field specifies the number of times the content can be exported. If value is 0xff, it indicates count_period_parameter is unlimited.

5.10.4.13 time_period_parameter

This field specifies the number of seconds the content can be exported for.

5.10.4.14 day_count_parameter

This field specifies the number of days the content can be exported for.

5.10.4.15 start_date_parameter

This field specifies the start date from which the content can be exported. The unit of value is second, and the value '0' shows Jan. 1st, 1970 00:00:00 UTC.

5.10.4.16 end_date_parameter

This field specifies the end date until which the content can be exported. The unit of value is second, and the value '0' shows Jan. 1st, 1970 00:00:00 UTC.

Annex A (informative)

Permission code requirements for home servers and playback devices

A.1 Handling permission codes within the home server and client device

The home server and client device are receivers of the content rights holder's permission. A permission code is comprised of the content sold / distributed, and its permission.

The following is a set of requirements in handling permission codes within home servers and client devices.

- a) When a home server or a client device purchases access rights to content, the permission code must definitively reach the home server or client device without alteration by a third party.
- b) A permission code that has reached a home server or a client device must be retained inside the media with access rights until they are destroyed by the user, invalidated or lost due to destruction of the media it resides in, etc. At the same time, the contents of the permission code shall never be altered during its possession.
- c) The home server and client device must be able to render (display, print) the content in accordance to the contents of the contract specified in the permission code.

The strength of security will be dependent on implementation.

The following are minimum requirements for implementation.

- d) The permission code must be incorporated within the license and distributed with the license.
- e) The drm implementation module shall have an interface that enables users to safely reference the permission details that the values within the license's permission code specify.
- f) Define verbiage that express the contract details that correspond to each value within the permission code. Display the defined verbiage when presenting contract details to users.

In addition, the following is an optional requirement.

- g) Collect information to understand the degree in which the contract expressed in the permission is adhered to when content is accessed within the home server and client device. Establish a system capable of sending such information to the license server or the permission management server as necessary.

A.2 Examples for handling content and permission codes with domain identifiers

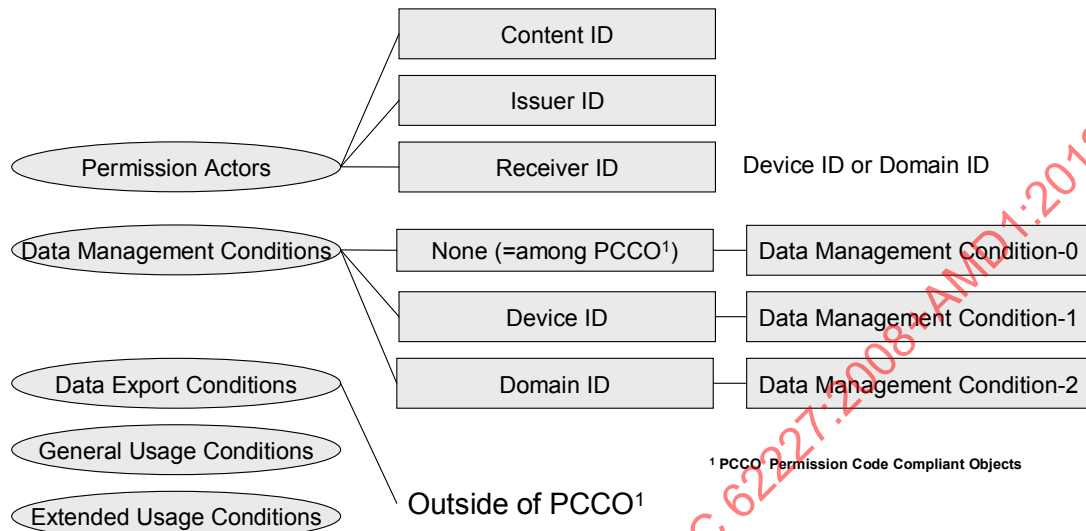
A.2.1 General

This subclause provides examples that illustrate the manner in which devices shall handle content and permission codes that include domain identifiers.

A.2.2 Specifying domain identifiers within a permission code

A.2.2.1 How domains appear in a permission code

Domains appear as receiver identifiers and/or data management conditions within permission codes as specified in this standard, see Figure A.1.



IEC 700/08

Figure A.1 – Permission code and domain

A.2.2.2 When a domain ID is specified as the receiver ID

When a domain ID is specified as the receiver ID, permission specified within general usage conditions, extended usage conditions and data export conditions is applied to devices and storage media that belong to the domain. Therefore, the device that receives this permission code is able to re-issue the same permission to other devices and storage media that belong to this domain.

It is assumed that certain preventative mechanisms would be in place through the management of domain keys, etc. These preventative mechanisms may prevent devices that do not belong to the domain from spoofing the domain ID or prevent such devices from the use of content even in the unlikely event that a license is received due to successful spoofing of the domain ID.

In cases in which the same domain id is also specified in the data management condition, the data management condition will take precedence over the receiver ID.

A.2.2.3 When a domain ID is specified in the data management condition

When a domain ID is specified in the data management condition, the conditions are interpreted as rules of exception or priority.

General usage conditions, extended usage conditions and data export conditions are deemed as permissions intended for the device or storage media that first received the content.

A.2.3 Process flow for re-issuing permission information

Figure A.2 shows a diagram for re-issuing of the permission information.

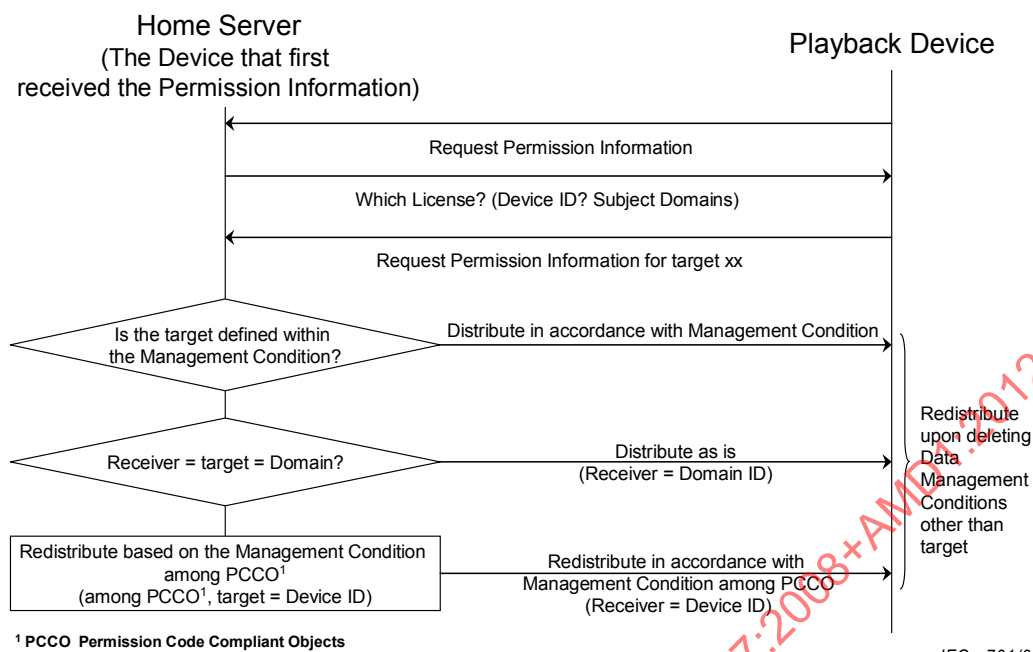


Figure A.2 – Re-issuing permission information

The following applies to the process flow of permission information.

- Device b, the device requesting the permission code to be re-issued places the request with device a, the first device that received the permission information. Device b specifies the device ID, storage media ID or domain ID; the actor to be subject of the permission re-issuance.
- If the permission code's management condition contains a specific ID, device a will re-issue the permission code to the receiver id specified in accordance with the management condition.
- If the identifier for the first receiver of the permission code and the identifier specified as subject of re-issuance are both the same domain ID, the permission code is re-issued with the domain ID left in tact as the receiver ID.
- If none of the above applies, the permission code is re-issued with the receiver ID as the specified ID in accordance with management conditions placed on devices among permission code compliant objects

Note that when permission codes are re-issued, data management conditions that concern actors other than the ID specified as the receiver ID will be deleted prior to redistribution.

A.2.4 Restrictions concerning counts

When redistributing permission codes, care should be taken as follows when restrictions concerning counts are involved:

- Restriction on copy count under data management conditions;
- Restriction on export count under data export conditions;
- Restriction on usage count under general usage conditions.

With respect to count restrictions, the following must be true.

(The count specified within the permission code first received.)

=(the count remaining on the first device that received the permission code)

+(the count specified on the permission code to be re-issued)

The following permission codes with count restrictions can be re-issued when this process is managed by setting the sublicensing count specified in the permission code to zero.

The example below illustrates copy count restrictions under data management conditions.

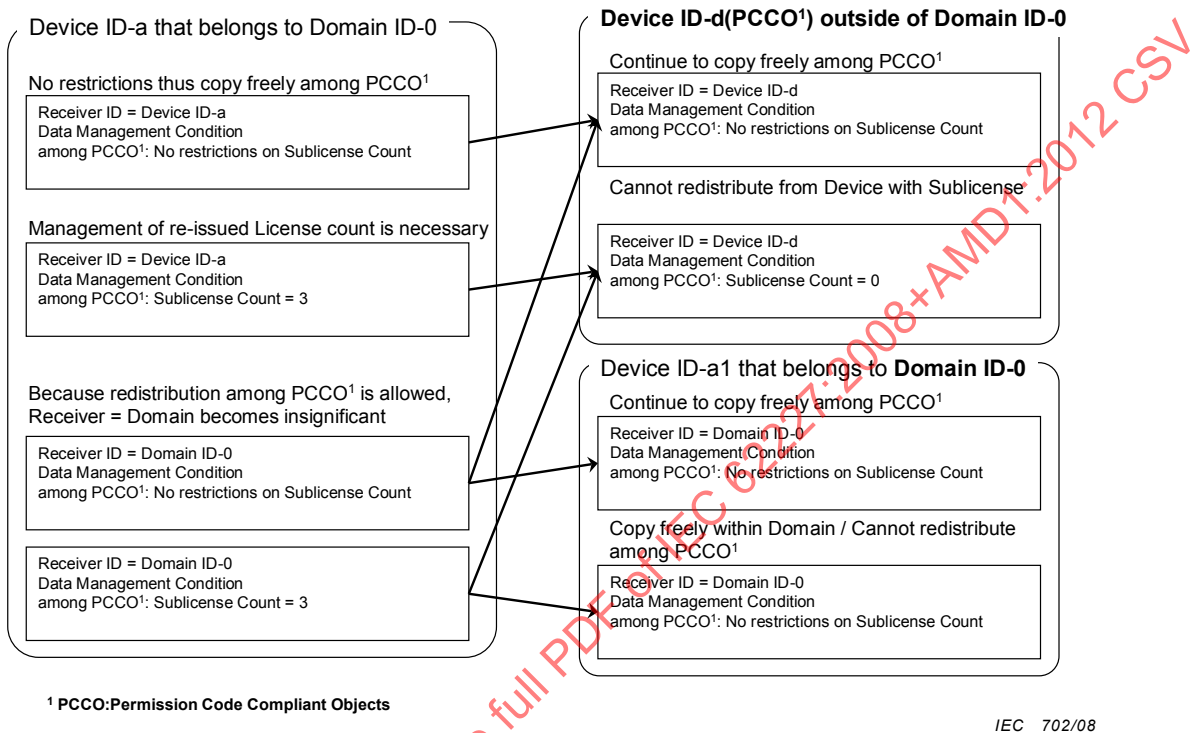


Figure A.3 – Re-issuing permission among permission code compliant objects is allowed

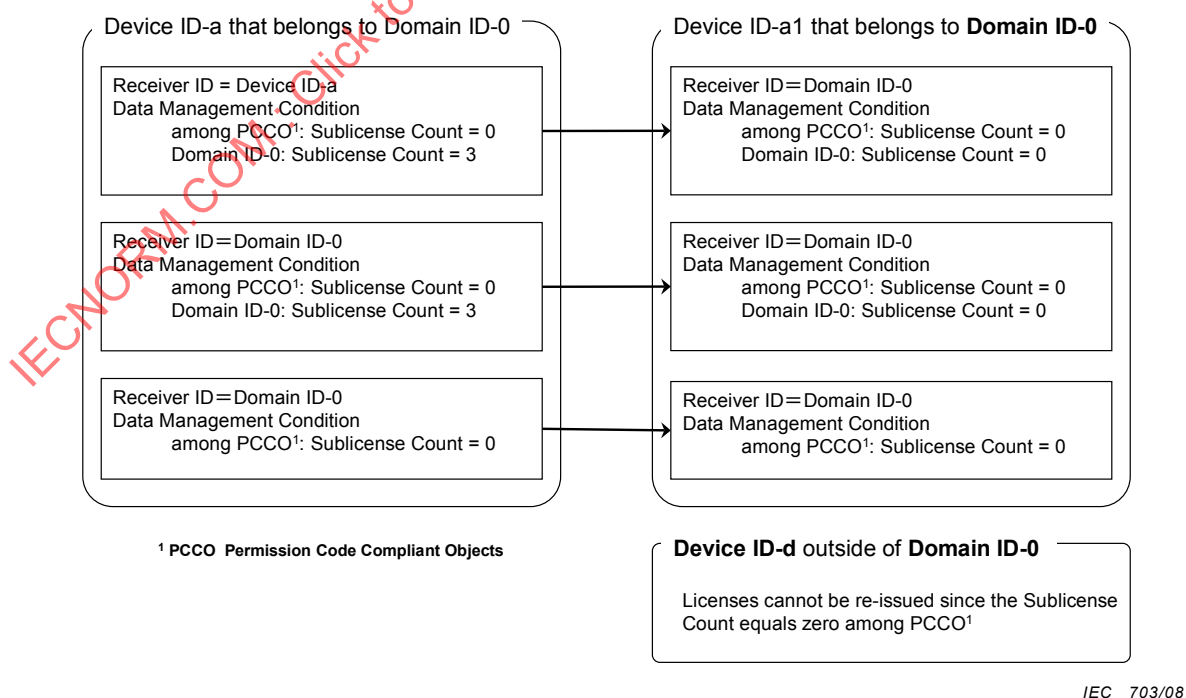
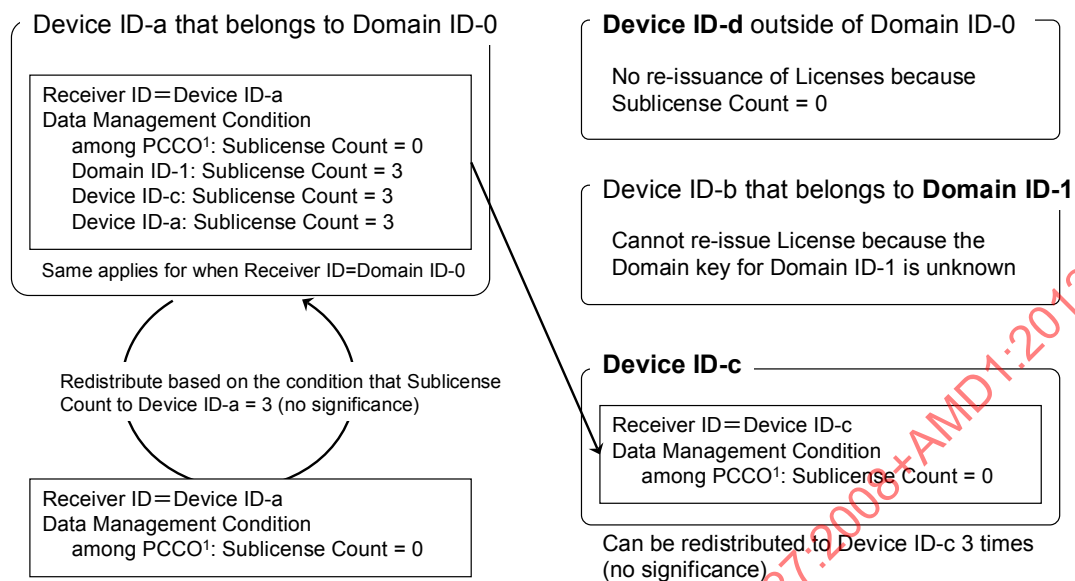


Figure A.4 – Re-issuing permission within a domain is allowed



IEC 704/08

Figure A.5 – Other conditions

IECNORM.COM : Click to view the full PDF of IEC 62227:2008+AMD1:2012 CSV

Annex B (informative)

Use-case scenario

B.1 Anticipated use-cases

The following is a set of anticipated use-cases for the use of permission codes.

- A producer issues usage permission directly to an end user
- An aggregator issues usage permission to a delivery service provider
- A delivery service provider issues usage permission to a home domain
- A delivery service provider issues usage permission to a device
- A delivery service provider reports usage with respect to a permission code
- A permission manager searches for a rights holder by using the content identifier included within the permission code as a search parameter

B.2 Immediately available use cases

B.2.1 General

This subclause illustrates use cases that can be realized with the use of permission codes. The structure of a permission code is illustrated graphically below.

The permission code is designed as it harmonizes with DRM systems, and its permission cover the range of permission of existing DRM systems. Here some examples are illustrated, but the permission code is applicable for other various DRM systems.

Permission Code Structuring (1/2)

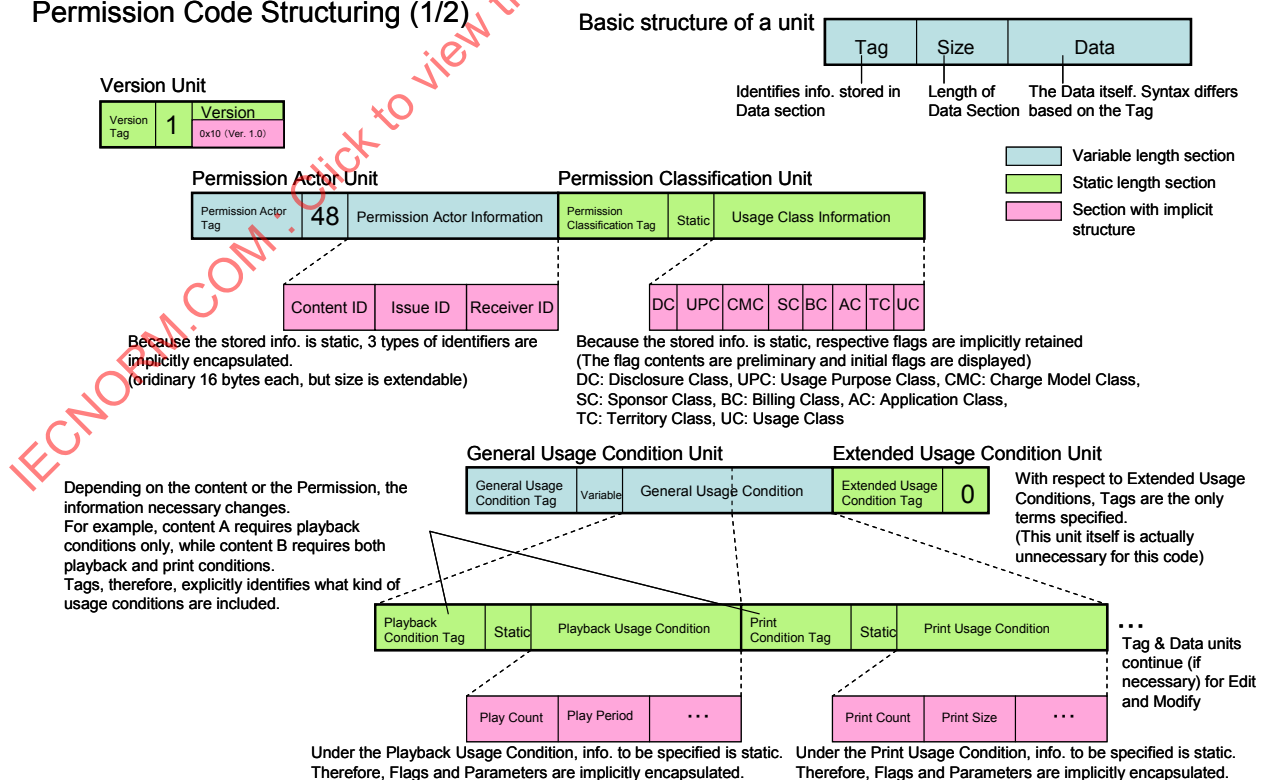


Figure B.1 – Permission code structuring (1/2)

Permission Code Structuring (2/2)

The structure that specifies a record for each management subject, after the field that specifies the number of records, is implicit. However, note that since the number of management subjects is variable, in general the length is variable.

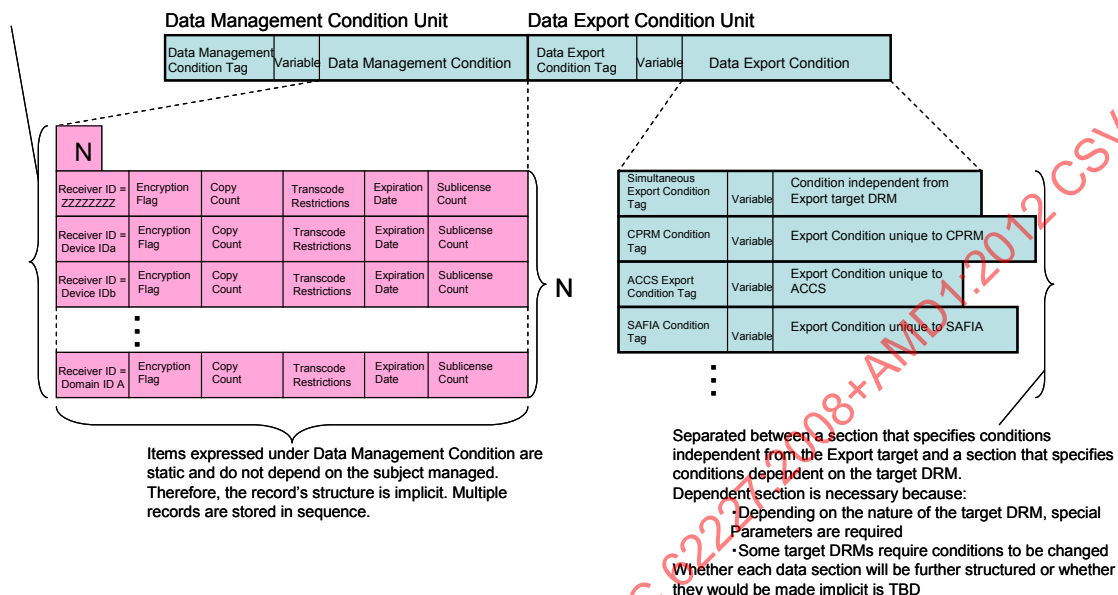


Figure B.2 – Permission code structuring (2/2)

IEC 706/08

B.2.2 Permission code example with respect to fairplay

Permission code conditions: As long as Mr. A is using the content, there is no restriction to copy or play. Export to CDs is allowed up to 10 times.

Permission Code Example with respect to Fairplay (1/2)

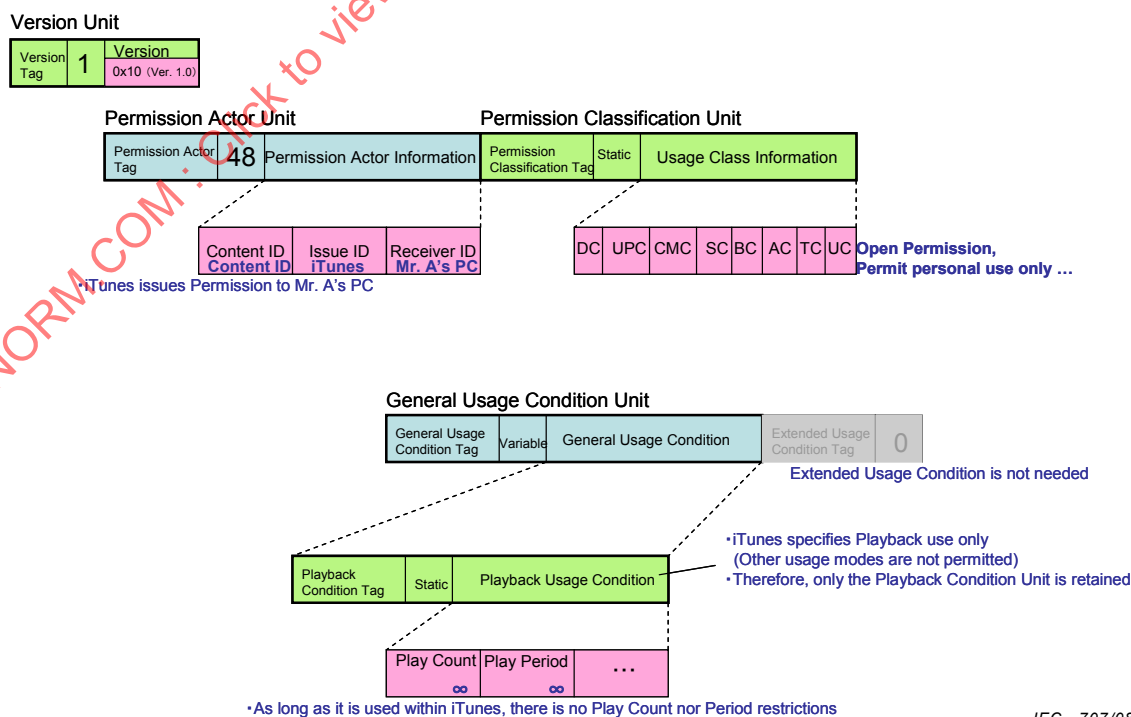
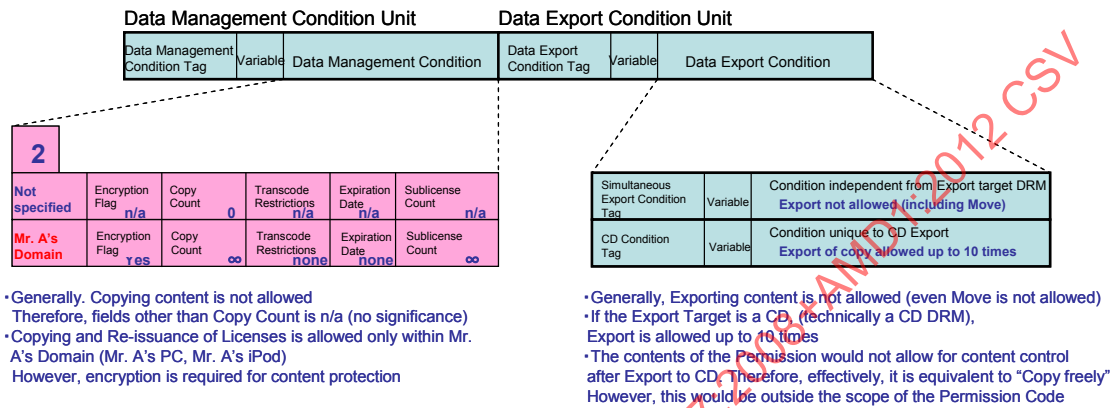


Figure B.3 – Permission code example with respect to FairPlay (1/2)

IEC 707/08

Permission Code example with respect to FairPlay (2/2)



After changing PCs, FairPlay re-authenticates Mr. A by re-connecting to the server. Expressing this process through the Permission Code, Sublicense Count to Mr. A would be ∞, with the Sublicense issued from the iTunes server. This would be a management method unique to this particular DRM and would be reflected as such in this section.

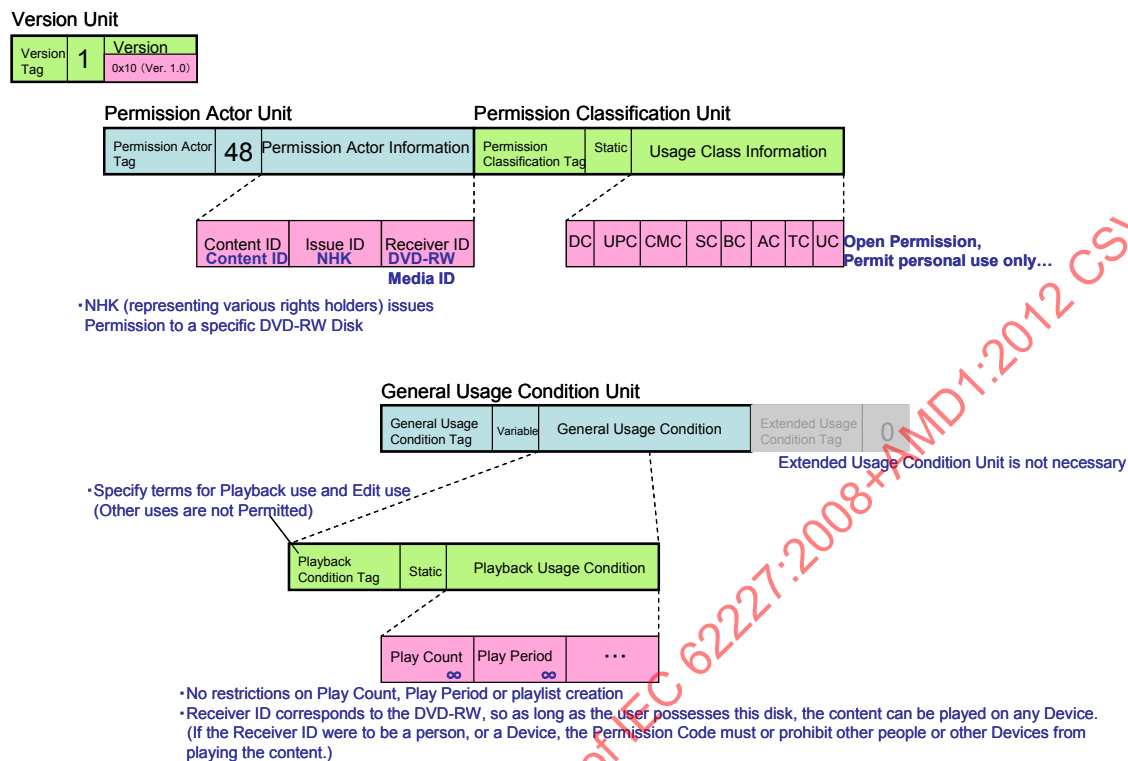
IEC 708/08

Figure B.4 – Permission code example with respect to FairPlay (2/2)

B.2.3 Permission code example with respect to CPRM (DVD-RW VR mode)

Permission code conditions: no restrictions on playback. Edit and playlist creation are allowed while further copy creation is not allowed. Move is allowed as long as further content instances are not created in the process.

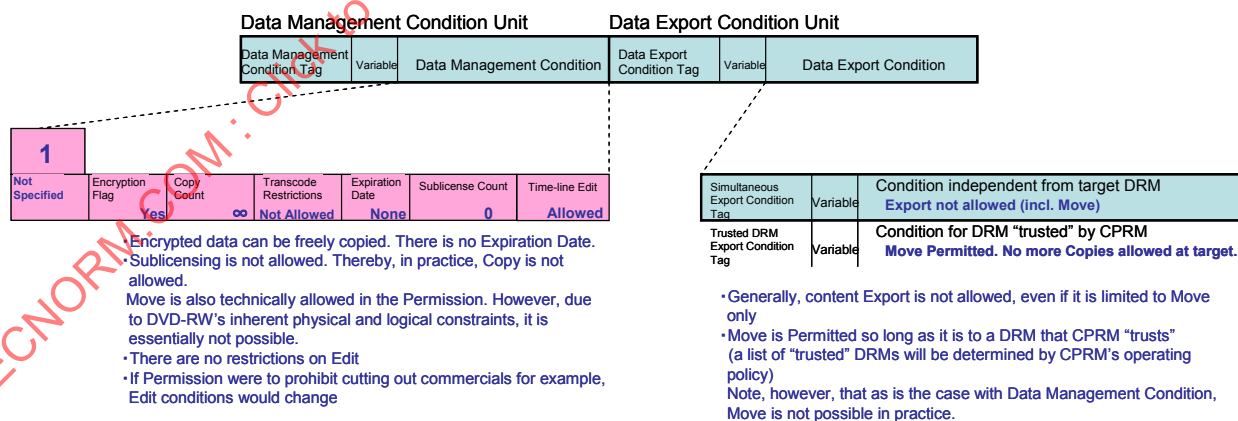
Permission Code Example with respect to CPRM (DVD-RW VR Mode)(1/2)



IEC 709/08

Figure B.5 – Permission code example with respect to CPRM (1/2)

Permission Code Example with respect to CPRM (DVD-RW VR Mode) (2/2)



IEC 710/08

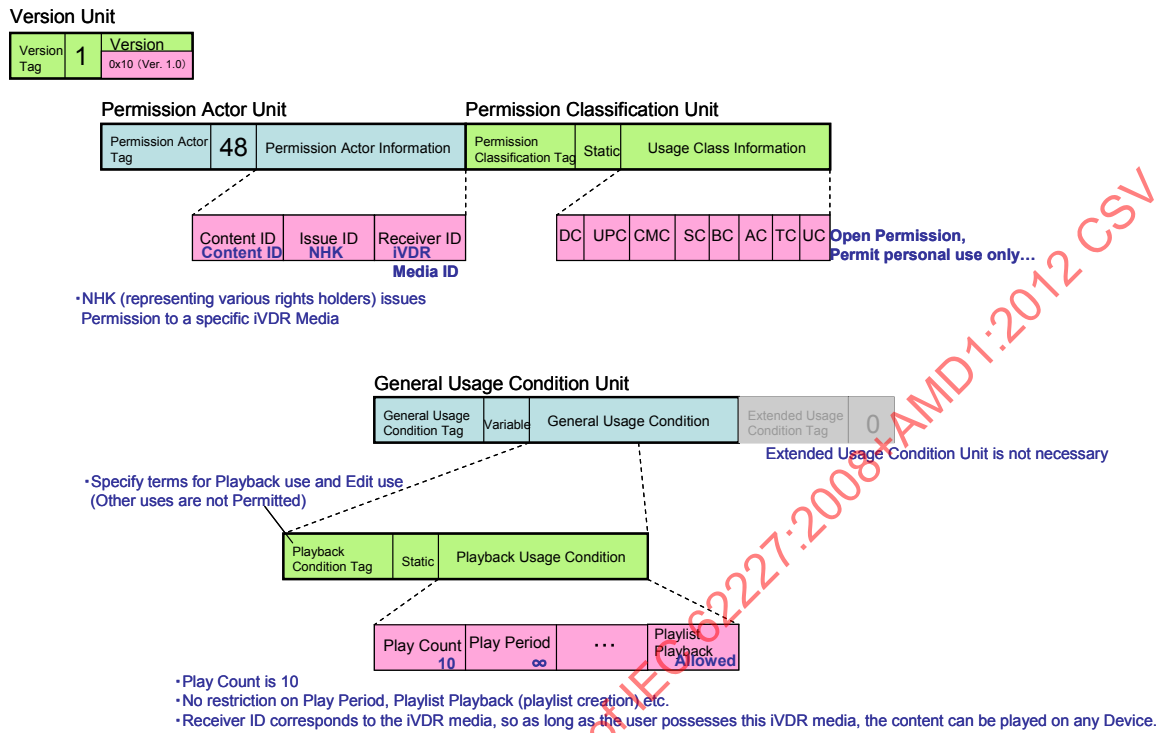
Figure B.6 – Permission code example with respect to CPRM (2/2)

B.2.4 Permission code example with respect to SAFIA

Permission code conditions: copy count is 10, and making further copies at the copy target is not allowed. Play count is 10. Edit and playlist creation are allowed. Move is allowed so long as no further content instances are created in the process.

NOTE The current SAFIA standard does not allow for simultaneous use of copy control and play count control. In addition, the current TV recording standard cannot apply copy count controls. This is a future potential use case.

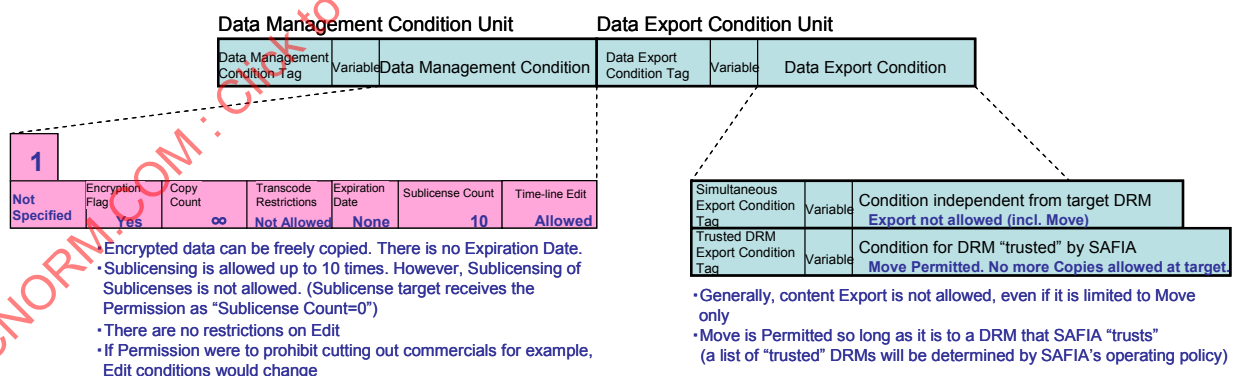
Permission Code Example with respect to SAFIA (1/2)



IEC 711/08

Figure B.7 – Permission code example with respect to SAFIA (1/2)

Permission Code Example with respect to SAFIA (2/2)



IEC 712/08

Figure B.8 – Permission code example with respect to SAFIA (2/2)

B.2.5 Key permission code examples with respect to PC distribution (WMT, streaming)

Permission code conditions: copy count is 0, and making further copies at the copy target is not allowed. There are no restrictions on play count. There is an expiration date. Edit and playlist creation are not allowed. Move is not allowed.

Key Permission Code Examples with respect to PC distribution (WMT, streaming)

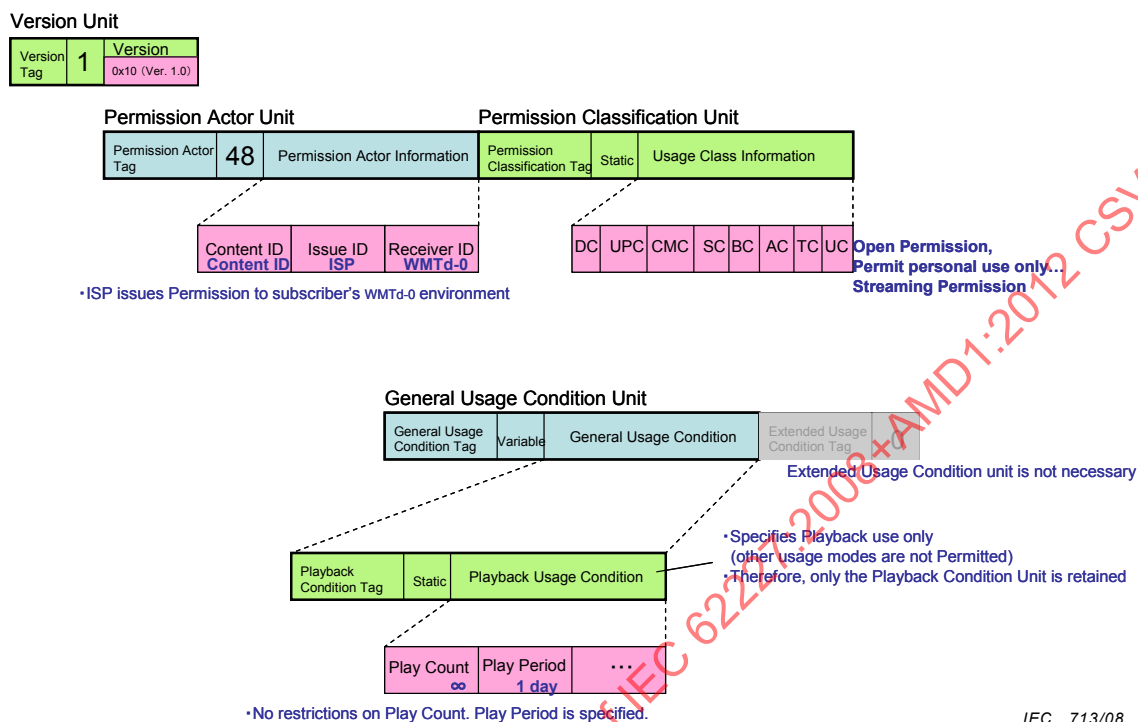


Figure B.9 – Permission code example with respect to PC distribution (streaming)

NOTE In this permission, usage type of permission classification is streaming permission. This does not mean that the end user is permitted to re-distribute the content by streaming, but this means that the end user is permitted to watch this content in streaming way. When the end user receives this permission code, the content is already distributed by streaming.

B.2.6 Key permission code example with respect to PC distribution (WMT, download)

Permission code conditions: copy count is 3, and making further copies at the copy target is not allowed. There are no restrictions on play count. There are no play period restrictions. Move is allowed so long as no further content instances are created in the process.

Key Permission Code Examples with respect to PC distribution (WMT, download) (1/2)

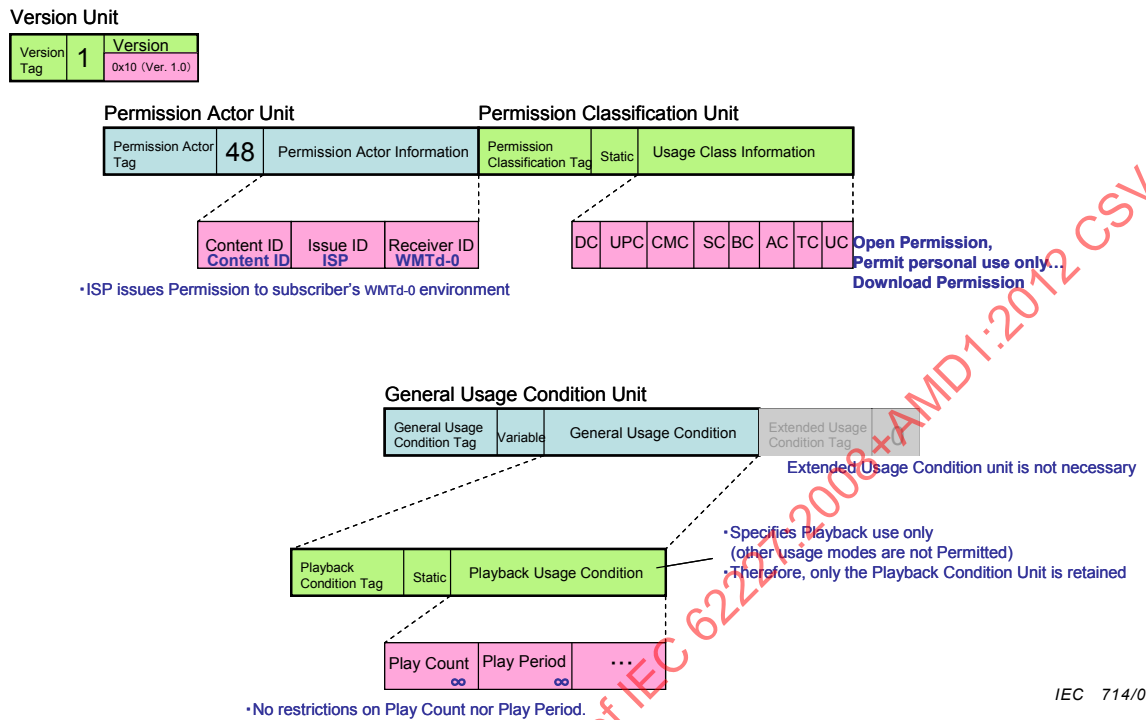


Figure B.10 – Permission code example with respect to PC distribution (download) (1/2)

Key Permission Code Example with respect to PC distribution (WMT, download) (2/2)

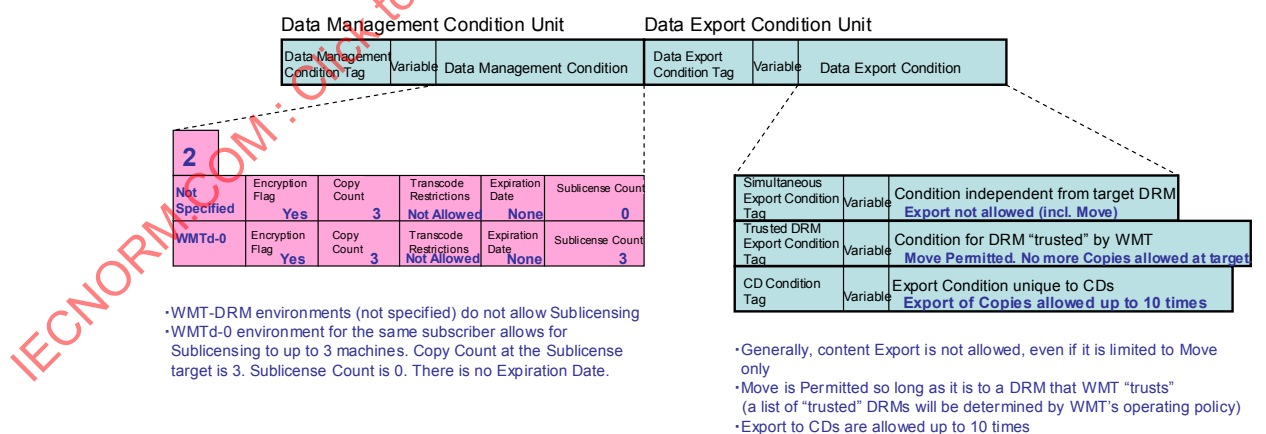


Figure B.11 – Permission code example with respect to PC distribution (download) (2/2)

B.2.7 Key permission code example with respect to ringtones

Permission code conditions: copy is not allowed, and therefore it is not possible to make further copies at a copy target. There are no restrictions on play count nor play period. Move is not allowed.

Key Permission Code Examples with respect to ringtones (1/2)

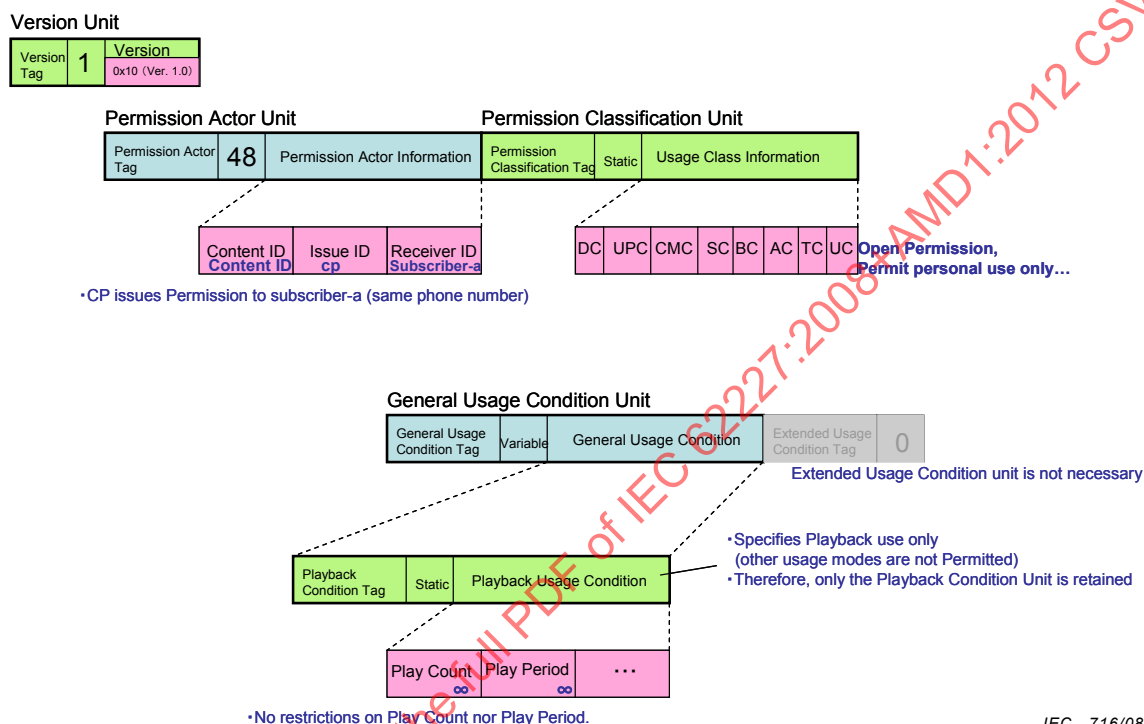


Figure B.12 – Permission code example with respect to ringtones (1/2)

Key Permission Code Example with respect to ringtones (2/2)

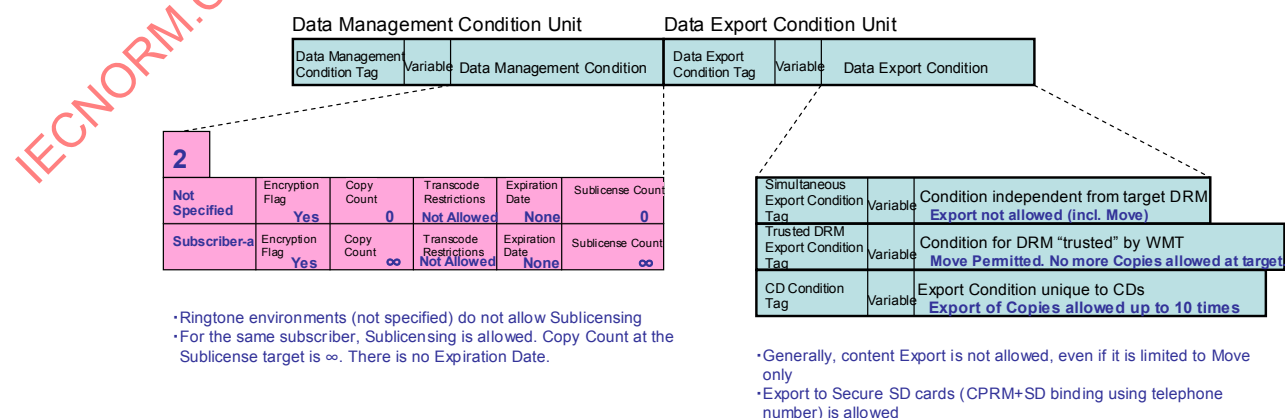


Figure B.13 – Permission code example with respect to ringtones (2/2)

Annex C (informative)

Issuing a permission code

C.1 Permission code and home server

The delivery service provider has the capacity to issue permission to a home server. By connecting to the permission management center, the delivery service provider can request the permission management center to issue permission and the acquired permission code to the home server.

a) Issuing a permission code to grant access for a single piece of content

When providing content individually, permission is expressed by utilizing a single permission code. One permission code is issued for each piece of content. Each permission code contains the content's permission information.

When accessing content on a home server, the license is exchanged between the license server and the home server.

When accessing content on a client device, the license is exchanged between the license server and the client device.

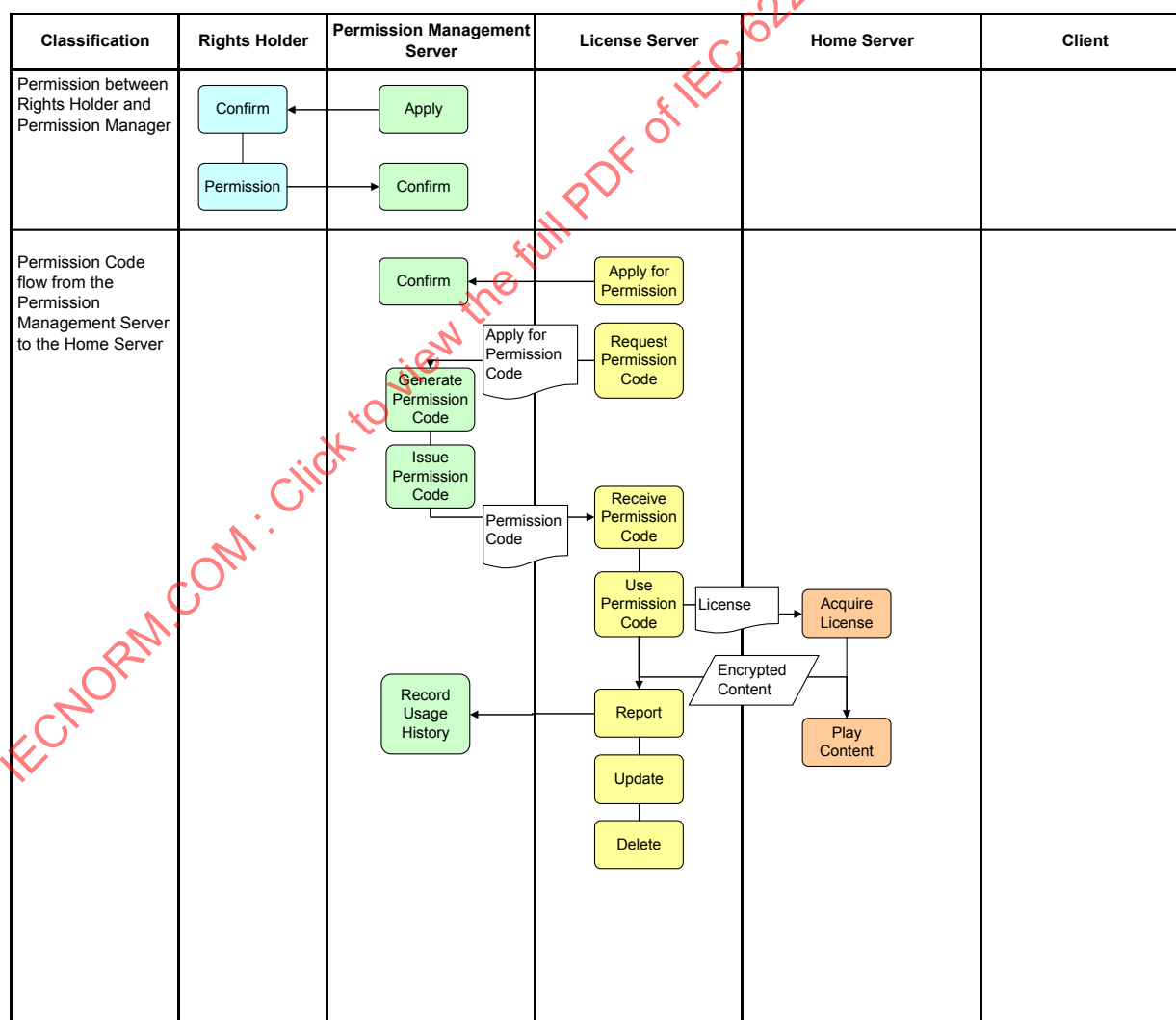
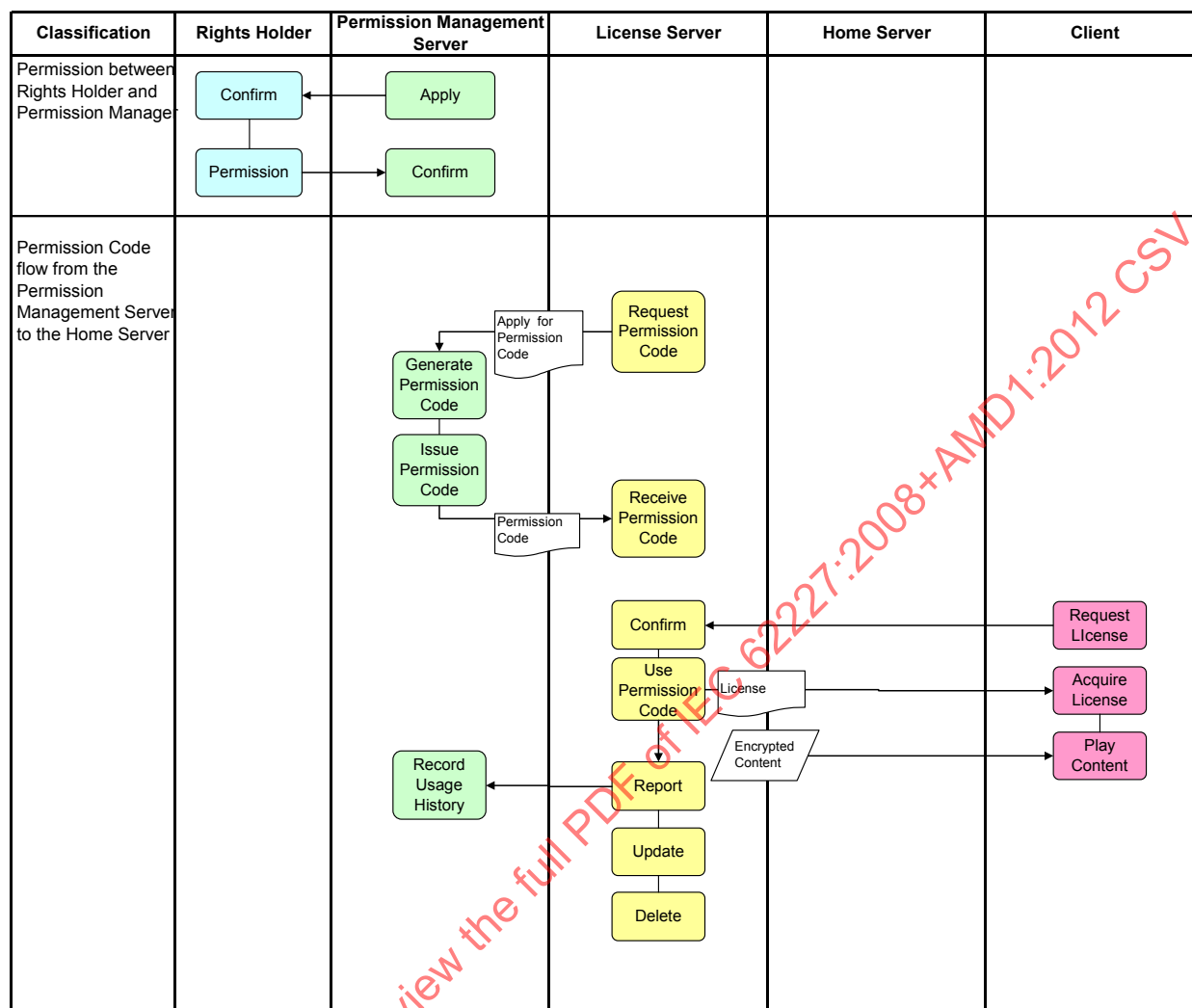


Figure C.1 – The flow of issuing a permission code to grant access to a single piece of content (for access on a home server)

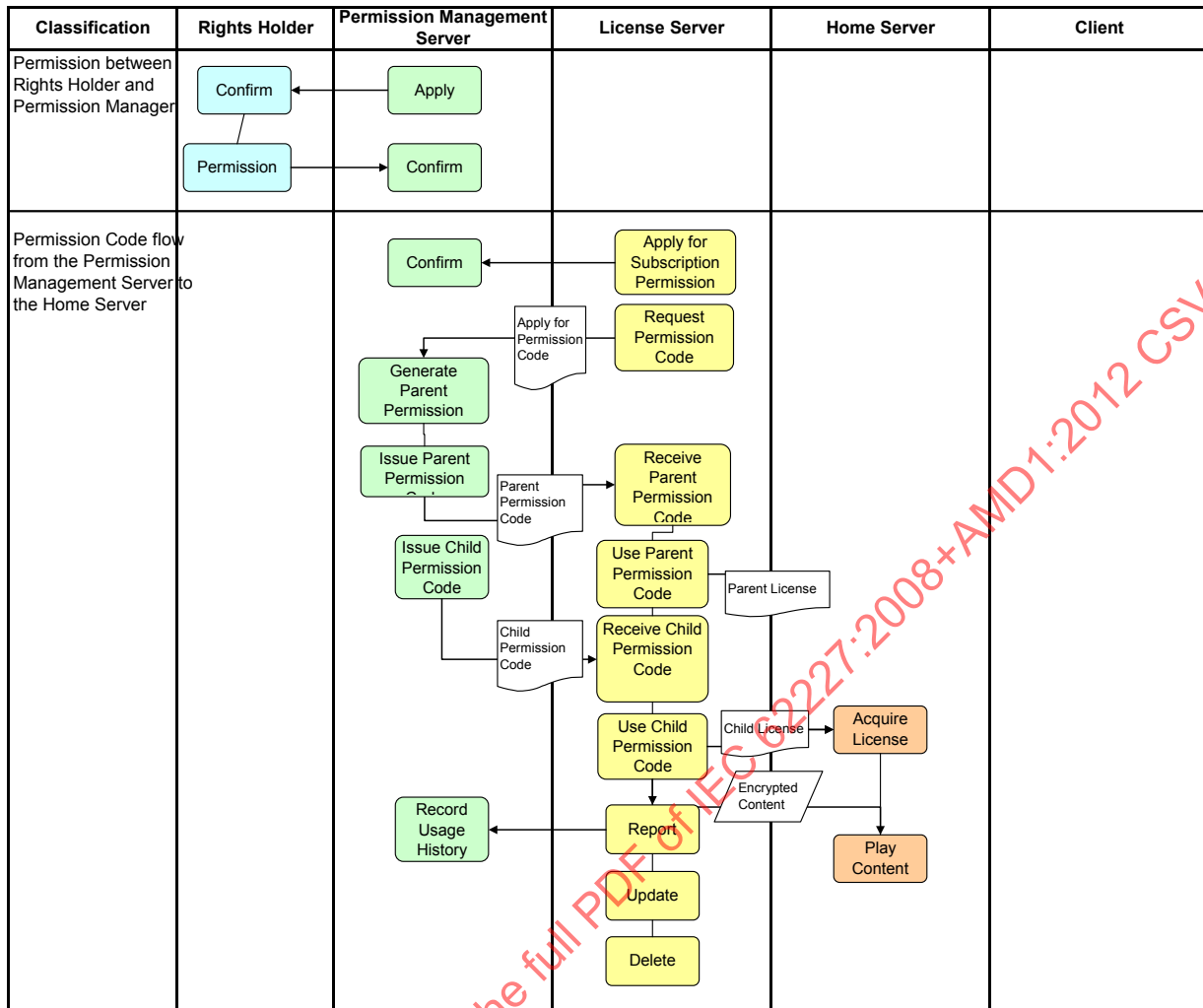


IEC 719/08

Figure C.2 – The flow of issuing a permission code to grant access to a single piece of content (for access on a client device)

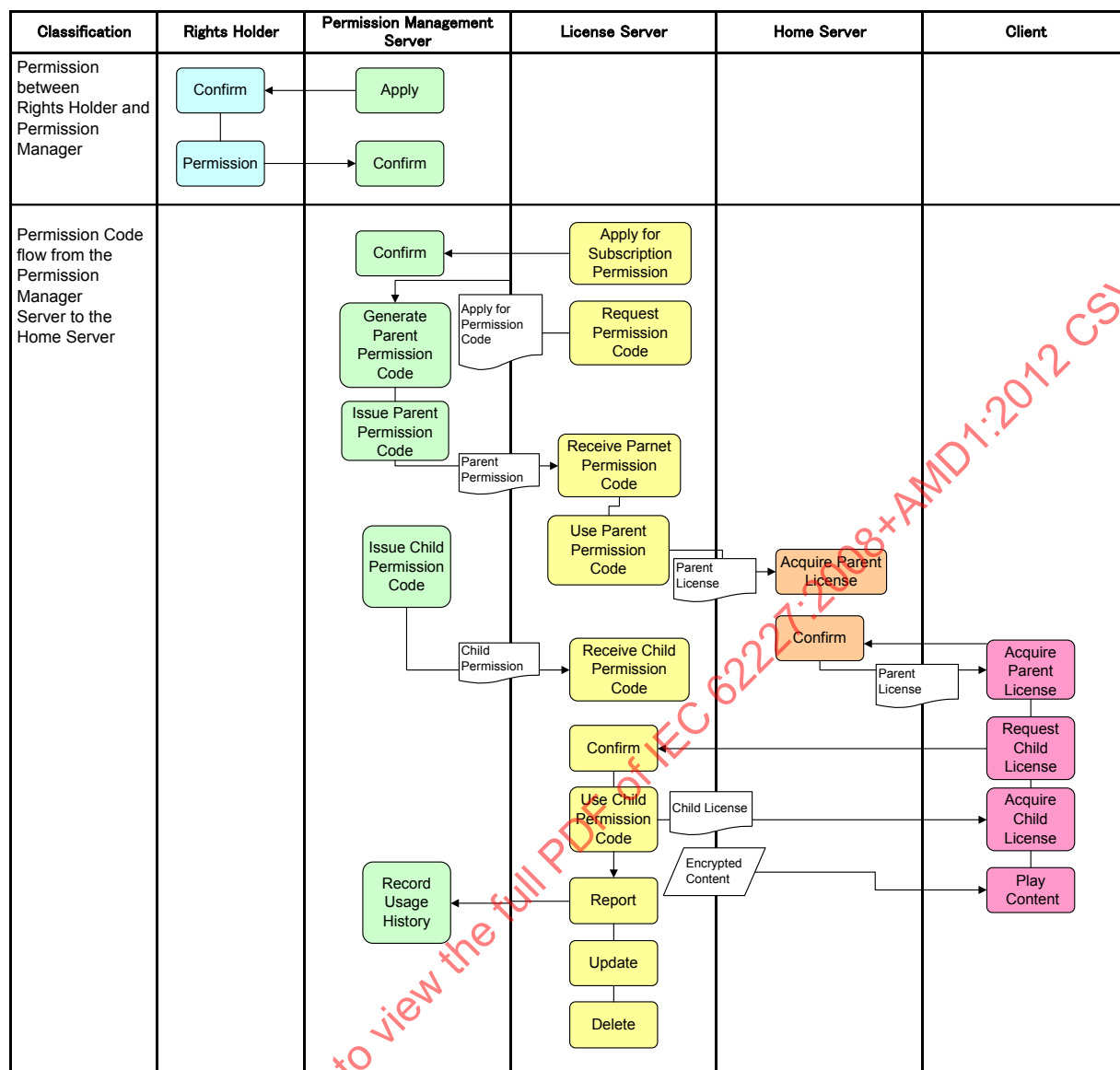
b) Issuing a permission code to grant access for subscription content

When offering a subscription service, permission is expressed using a parent permission code and a child permission code. A parent permission code is a permission code issued to grant access to a subscription service and contains permission information concerning the subscription. A child permission code is a permission code issued for each piece of content being offered as part of the subscription service and contains permission information concerning the content.



IEC 720/08

Figure C.3 – The flow of issuing a permission code to grant access to subscription content (for access on a home server)



IEC 721/08

Figure C.4 – The flow of issuing a permission code to grant access to subscription content (for access on a client device)

C.2 Managing home domains

When the client device accesses content that has been authorized for domain access, it acquires the domain access license from the home server, and the content access license from the license server.

By instituting a system whereby the content license cannot be accessed without a domain license, content access will require the acquisition of both domain and content access licenses.

Therefore, the client device will require a content license and a domain license, 2 types of licenses, in order to access content.

The following are several ways in which a device can be registered to a given domain:

- upon purchase of a device and storage media, the permission Issuer is notified with the device ID and storage media ID;
- place a domain management server within the home and register purchased devices and storage media.

The process of determining whether or not a given device or storage media belongs to a given domain can be managed as follows:

- the permission Issuer manages the process: the device contacts the permission issuer as necessary;
- a domain Management server manages the process: the device contacts the domain Management Server as necessary;
- the device / storage media itself is aware of the domain it belongs to.

IECNORM.COM : Click to view the full PDF of IEC 62227:2008+AMD1:2012 CSV

IECNORM.COM : Click to view the full PDF of IEC 62227:2008+AMD1:2012 CSV

SOMMAIRE

AVANT-PROPOS	82
INTRODUCTION à l'Amendement 1	84
INTRODUCTION	84
1 Domaine d'application	86
2 Références normatives	86
3 Termes, définitions et abréviations	86
3.1 Termes et définitions	86
3.2 Termes abrégés	92
4 Cadre du code d'autorisation	94
4.1 Généralités	94
4.2 Hypothèses associées au code d'autorisation	96
4.2.1 Relations binaires dans la chaîne de valeurs de distribution de contenu	96
4.2.2 Autorisation délivrée à un groupe de contenus	96
4.2.3 Centre de code commun pour les autorisations	96
4.2.4 Rapport d'utilisation	97
4.2.5 Scénario d'application du code d'autorisation	97
4.2.6 Harmonisation avec les systèmes de DRM (Gestion numérique des droits, en anglais «Digital Rights Management»)	98
4.3 Composants d'un code d'autorisation	98
4.3.1 Acteur d'autorisation	98
4.3.2 Classification d'autorisation	101
4.3.3 Utilisation du contenu	101
4.3.4 Gestion des données de contenu	102
5 Configuration du code d'autorisation	104
5.1 Généralités	104
5.2 Notation	105
5.2.1 Valeurs numériques	105
5.3 Système de code d'autorisation	106
5.4 Version unit	107
5.4.1 Structure	107
5.4.2 Version unit tag	107
5.4.3 Reserved	107
5.4.4 Version	108
5.5 Permission actor unit	108
5.5.1 Structure	108
5.5.2 Permission actor unit tag	108
5.5.3 Total bytes of identifiers	108
5.5.4 Identifiant de contenu	108
5.5.5 Identifiant d'émetteur	110
5.5.6 Identifiant de récepteur	112
5.6 Permission classification unit†	113
5.6.1 Structure	113
5.6.2 Permission classification unit tag	113
5.6.3 Reserved	113

5.6.4	Disclosure class	113
5.6.5	Usage purpose class	114
5.6.6	Charge model class	114
5.6.7	Billing class	115
5.6.8	Application class	116
5.6.9	Sponsor class	116
5.6.10	Territory class	117
5.6.11	Usage class	117
5.7	Unité general usage condition	120
5.7.1	Structure de l'unité	120
5.7.2	En-tête des conditions générales d'utilisation	120
5.7.3	Descripteur general usage condition	120
5.8	Unité extended use condition	129
5.8.1	Structure de l'unité	130
5.8.2	En-tête extended use condition	130
5.9	Unité data management condition	130
5.9.1	Structure de l'unité	130
5.9.2	En tête de condition de gestion des données	131
5.9.3	Data management condition	131
5.10	Unité data export condition	134
5.10.1	Structure de l'unité	134
5.10.2	En tête de condition d'export des données	135
5.10.3	Descripteur data export condition	135
5.10.4	Descripteur general export	136
Annexe A (informative) Exigences du code d'autorisation pour les serveurs résidentiels et les dispositifs de lecture		140
Annexe B (informative) Scénario de cas d'utilisation		150
Annexe C (informative) Fourniture d'un code d'autorisation		174
Figure 1 – Environnement du code d'autorisation		95
Figure 2 – Environnement du code d'autorisation		103
Figure 3 – Configuration du code d'autorisation		106
Figure 4 – Structure de base de l'unité permission code		107
Figure 5 – Unité general usage condition		120
Figure 6 – Unité data management condition		131
Figure 7 – Unité data export condition		134
Figure 8 – Unité extended use condition		130
Figure A.1 – Code d'autorisation et domaine		141
Figure A.2 – Redistribution des informations d'autorisation		143
Figure A.3 – La redistribution d'autorisation parmi les objets conformes au code d'autorisation est autorisée		146
Figure A.4 – La redistribution d'autorisation dans un domaine est autorisée		148
Figure A.5 – Autres conditions		149
Figure B.1 – Structuration de code d'autorisation (1/2)		153
Figure B.2 – Structuration de code d'autorisation (2/2)		154
Figure B.3 – Exemple de code d'autorisation concernant le FairPlay (1/2)		156

Figure B.4 – Exemple de code d'autorisation concernant le FairPlay (2/2)	157
Figure B.5 – Exemple de code d'autorisation concernant la CPRM (1/2)	159
Figure B.6 – Exemple de code d'autorisation concernant la CPRM (2/2)	161
Figure B.7 – Exemple de code d'autorisation concernant la SAFIA (Architecture de sécurité pour annexe intelligente, en anglais «Security Architecture For Intelligent Attachment») (1/2)	162
Figure B.8 – Exemple de code d'autorisation concernant la SAFIA (Architecture de sécurité pour annexe intelligente, en anglais «Security Architecture For Intelligent Attachment») (2/2)	164
Figure B.9 – Exemple de code d'autorisation concernant la distribution à des PC (diffusion en continu)	166
Figure B.10 – Exemple de code d'autorisation concernant la distribution à des PC (téléchargement) (1/2)	168
Figure B.11 – Exemple de code d'autorisation concernant la distribution à des PC (téléchargement) (2/2)	170
Figure B.12 – Exemple de code d'autorisation concernant des sonneries de téléphone (1/2).....	172
Figure B.13 – Exemple de code d'autorisation concernant des sonneries de téléphone (2/2).....	173
Figure C.1 – Organigramme de la fourniture d'un code d'autorisation pour octroyer l'accès à un contenu unique (pour accès sur un serveur résidentiel)	176
Figure C.2 – Organigramme de la fourniture d'un code d'autorisation pour octroyer l'accès à un contenu unique (pour accès sur un dispositif client).....	178
Figure C.3 – Organigramme de la fourniture d'un code d'autorisation pour octroyer l'accès à un contenu par abonnement (pour accès sur un serveur résidentiel)	180
Figure C.4 – Organigramme de la fourniture d'un code d'autorisation pour octroyer l'accès à un contenu par abonnement (pour accès sur un dispositif client)	183
Tableau 1 – Interprétation de Distinct tag.....	105
Tableau 2 – Structure de version unit.....	107
Tableau 3 – Structure de permission actor unit	108
Tableau 4 – Structure du descripteur content identifier	109
Tableau 5 – Interprétation de Content type code.....	109
Tableau 6 – Structure du descripteur issuer identifier	110
Tableau 7 – Interprétation de Issuer role code	111
Tableau 8 – Interprétation de Issuer configuration code	111
Tableau 9 – Structure du descripteur receiver identifier	112
Tableau 10 – Interprétation de Receiver role code	112
Tableau 11 – Interprétation du Receiver configuration code.....	112
Tableau 12 – Structure de permission classification unit	113
Tableau 13 – Structure de disclosure class	114
Tableau 14 – Interprétation de disclosure_type (DT).....	114
Tableau 15 – Structure de usage purpose class.....	114
Tableau 16 – Interprétation de usage_purpose_type (UPT).....	114
Tableau 17 – Structure de charge model class.....	115
Tableau 18 – Interprétation de charge_model_type (CMT).....	115
Tableau 19 – Structure de billing class	116

Tableau 20 – Interprétation de billing_type (BT).....	116
Tableau 21 – Structure de application class.....	116
Tableau 22 – Interprétation de application_type (AT).....	116
Tableau 23 – Structure de sponsor class.....	117
Tableau 24 – Configuration de sponsor_type (ST).....	117
Tableau 25 – Structure de territory class.....	117
Tableau 26 – Structure de usage class.....	118
Tableau 27 – Interprétation de usage_type (UT).....	118
Tableau 28 – Configuration de redistribution_Type.....	119
Tableau 29 – Structure d'en-tête des conditions générales d'utilisation.....	120
Tableau 30 – Valeurs de balise de descripteurs.....	121
Tableau 31 – Structure du descripteur playback usage condition.....	121
Tableau 32 – Structure du descripteur print usage condition.....	124
Tableau 33 – Structure du descripteur esecute usage condition.....	127
Tableau 34 – Structure de l'en-tête de conditions de gestion de données.....	131
Tableau 35 – Structure de data management condition.....	132
Tableau 36 – Structure d'encryption flag (EF).....	132
Tableau 37 – Interprétation de transcode type.....	133
Tableau 38 – Structure de l'indicateur time-line edit (TF).....	134
Tableau 39 – Structure de l'en-tête de condition d'export de données.....	135
Tableau 40 – Valeurs de balise de descripteurs.....	135
Tableau 41 – Structure du descripteur general export.....	136
Tableau 42 – Interprétation de storage_media_type (SMT).....	137
Tableau 43 – Interprétation d'encoding_type (ET).....	137
Tableau 44 – Interprétation de protection_type (PT).....	138
Tableau 45 – Interprétation de control_type (CT).....	138
Tableau 46 – Structure de l'en-tête extended use condition.....	130

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

**SYSTÈMES SERVEURS MULTIMÉDIA DOMESTIQUES –
CODES NUMÉRIQUES DES AUTORISATIONS DES DROITS**

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 n'a prévu aucune procédure de marquage valant indication d'approbation et n'engage pas sa responsabilité pour les équipements déclarés conformes à une de ses Publications.
- 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.

La Commission Electrotechnique Internationale (CEI) attire l'attention sur le fait qu'il est déclaré que la conformité au présent document peut impliquer l'utilisation d'un brevet.

La CEI ne prend pas position concernant la preuve, la validité et le domaine d'application de ces droits de propriété industrielle.

Le détenteur de ces droits de propriété industrielle a assuré à la CEI qu'il souhaitait négocier des licences avec des demandeurs dans le monde entier, selon des termes et des conditions raisonnables et non discriminatoires. À cet égard, la déclaration de détenteurs de ces droits de propriété est enregistrée à la CEI. Des informations peuvent être obtenues auprès de:

DENTSU INC.
Media Marketing Division
1-8-1, Higashi-shimbashi, Minato-ku, Tokyo 105-7001
JAPON

L'attention est attirée sur le fait que certains des éléments de la présente norme peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues autres que ceux qui sont identifiés ci-dessus. La CEI ne saurait être tenue pour responsable de l'identification de l'un quelconque ou de la totalité de ces droits de propriété industrielle.

Cette version consolidée de la CEI 62227 comprend la première édition (2008) [documents 100/1287/CDV et 100/1374/RVC] et son amendement 1 (2012) [documents 100/1953/CDV et 100/2011/RVC]. Elle porte le numéro d'édition 1.1.

Le contenu technique de cette version consolidée est donc identique à celui de l'édition de base et à son amendement; cette version a été préparée par commodité pour l'utilisateur. Une ligne verticale dans la marge indique où la publication de base a été modifiée par l'amendement 1. Les ajouts et les suppressions apparaissent en rouge, les suppressions sont barrées.

La Norme internationale CEI 62227 a été établie par le domaine technique 8: Systèmes de serveurs résidentiels multimédia, du comité d'études 100 de la CEI: Systèmes et appareils audio, vidéo et multimédia.

Le texte anglais de cette norme est issu des documents 100/1287/CDV et 100/1374/RVC.

Le rapport de vote 100/1374/RVC donne toute information sur le vote ayant abouti à l'approbation de cette norme.

La version française n'a pas été soumise au vote.

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

Le comité a décidé que le contenu de la publication de base et de ses amendements 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 à l'Amendement 1

La révision de la CEI 62227:2008 est devenue nécessaire pour spécifier la nouvelle définition complémentaire du descripteur. Le présent Amendement 1 contient les modifications techniques significatives suivantes par rapport à l'édition de base de la CEI 62227:

- ajout d'une nouvelle définition du content type;
- ajout d'une nouvelle définition d'élément de la Permission purpose classification.

Cet amendement contient aussi des modifications pour clarifier le texte ainsi que pour permettre une meilleure compréhension.

IECNORM.COM : Click to view the full PDF of IEC 62227:2008+AMD1:2012 CSV

INTRODUCTION

Le système d'identifiants communs est utilisé pour identifier systématiquement chaque entité, dispositif et contenu impliqués au cours de la distribution numérique du contenu. Le code d'autorisation peut exprimer divers ensembles d'informations d'autorisation et les conditions d'autorisation nécessaires pour la transmission de contenu sous forme d'un code remarquablement court. Le code d'autorisation n'est pas défini du point de vue technique mais plutôt en se basant sur les informations d'autorisation actuellement utilisées dans le domaine par les détenteurs de droits, même si le code d'autorisation est reconnu pour son efficacité technique vis-à-vis de la distribution numérique de contenu.

IECNORM.COM : Click to view the full PDF of IEC 62227:2008+AMD1:2012 CSV

SYSTÈMES SERVEURS MULTIMÉDIA DOMESTIQUES – CODES NUMÉRIQUES DES AUTORISATIONS DES DROITS

1 Domaine d'application

La présente Norme internationale définit le code d'autorisation qui est un ensemble d'informations associées à une autorisation sous forme d'un code court, destiné principalement aux systèmes de serveurs résidentiels. Le code d'autorisation est constitué d'un système d'identifiants communs (identifiant de contenu, identifiant d'émetteur, identifiant de récepteur, identifiant de dispositif, etc.) et d'un code d'autorisation de définition restreinte.

Le système d'identifiants communs est utilisé pour identifier systématiquement chaque entité, dispositif et contenu impliqués au cours de la distribution numérique du contenu. Le code d'autorisation peut exprimer divers ensembles d'informations d'autorisation et les conditions d'autorisation nécessaires pour la transmission de contenu sous forme d'un code remarquablement court. Le code d'autorisation n'est pas défini du point de vue technique mais plutôt en se basant sur les informations d'autorisation actuellement utilisées dans le domaine par les détenteurs de droits. Même après, le code d'autorisation est reconnu pour son efficacité technique vis-à-vis de la distribution numérique de contenu.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. 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).

ISO 3166-1:2006, *Codes pour la représentation des noms de pays et de leurs subdivisions - Partie 1: Codes de pays*

3 Termes, définitions et abréviations

3.1 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

3.1.1

autorisation

acte d'une certaine entité émettrice pour autoriser à une certaine entité réceptrice l'utilisation d'un contenu conformément à un certain ensemble de classifications d'autorisation et de conditions d'utilisation

NOTE L'entité émettrice et/ou l'entité réceptrice peuvent non seulement être des êtres humains, mais également un dispositif, un support de stockage, un organisme, un domaine ou une autre entité.

3.1.2

serveur de gestion d'autorisation

serveur délivrant un code d'autorisation sur la base d'un accord d'autorisation

NOTE Le serveur est muni

- a) d'un serveur de licence,
- b) d'une fonction acheminant le code d'autorisation à un serveur de distribution, et
- c) d'une fonction recevant un rapport d'utilisation de contenu du serveur de licence et du serveur de distribution.

3.1.3

serveur de licence conforme

serveur délivrant une licence sur la base d'un code d'autorisation

NOTE Le serveur est muni

- a) d'un système serveur (incluant un serveur résidentiel),
- b) d'une fonction générant les clés nécessaires pour l'accès au contenu, sur la base d'un code d'autorisation, et
- c) d'une fonction acheminant la licence à un dispositif client. Une licence contient des informations concernant le domaine d'application de l'utilisation autorisée du contenu, sur la base d'un code d'autorisation.

3.1.4

serveur de licence

serveur de licence conforme (sauf spécification contraire, un serveur de licence conforme est appelé simplement serveur de licence)

3.1.5

licence conforme

licence délivrée par un serveur de licence conforme

3.1.6

licence

licence conforme (sauf spécification contraire, une licence conforme est appelée simplement licence)

3.1.7

serveur résidentiel

dispositif client servant de passerelle pour un domaine résidentiel

3.1.8

dispositif client

dispositif devenant l'acteur de l'accès au contenu et conforme aux termes du code d'autorisation

3.1.9

dispositif conforme

dispositif doté de la fonction permettant de contrôler l'accès à un contenu sur la base d'une licence conforme

3.1.10

domaine

ensemble d'acteurs auxquels s'applique un ensemble de règles communes dans le contexte de la gestion de contenu

3.1.11

domaine résidentiel

environnement d'utilisation de contenu à domicile, autorisée par les détenteurs de droits

3.1.12

dispositif existant

dispositif non conforme ne contrôlant pas l'accès à un contenu sur la base de licences conformes

3.1.13

type de divulgation

classification d'autorisation spécifiant la classe « disclosure » de l'autorisation, incluant une autorisation ouverte et une autorisation fermée

3.1.14

autorisation ouverte

autorisation soumise au type de divulgation, reçue en fonction de conditions par défaut agencées au préalable

3.1.15

autorisation fermée

autorisation soumise au type de divulgation, reçue par l'intermédiaire d'un contrat séparé négocié individuellement

3.1.16

type d'application

classification d'autorisation spécifiant la classe application de l'autorisation, incluant une autorisation ad hoc et une autorisation générale

3.1.17

autorisation ad hoc

type d'application octroyant des autorisations par utilisation

3.1.18

autorisation générale

type d'application octroyant des autorisations de manière globale pour une utilisation pendant une période de temps donnée

NOTE Les périodes de temps peuvent inclure des incréments mensuels, annuels ou selon d'autres périodicités.

3.1.19

type de facture

classification d'autorisation spécifiant la classe billing de l'autorisation, incluant une facture ad hoc et une facture générale

3.1.20

facture ad hoc

type de facture s'effectuant par contenu

3.1.21

facture générale

type de facture s'effectuant mensuellement, annuellement ou selon d'autres incréments de temps

3.1.22

type de but d'utilisation

classification d'autorisation spécifiant la classe usage « purpose » de l'autorisation, incluant une autorisation commerciale, publique, sans but lucratif, promotionnelle

3.1.23

autorisation commerciale

type de but d'utilisation autorisant une utilisation à des fins commerciales

3.1.24

autorisation publique

type de but d'utilisation autorisant une utilisation à des fins publiques

3.1.25

autorisation sans but lucratif

type de but d'utilisation autorisant une utilisation à des fins sans but lucratif

3.1.26**autorisation promotionnelle**

type de but d'utilisation autorisant une utilisation à des fins promotionnelles

3.1.27**type de modèle de tarification**

classification d'autorisation spécifiant la classe charge model de l'autorisation, incluant une autorisation payante et gratuite, etc.

3.1.28**autorisation payante**

type de modèle de tarification autorisant une utilisation à titre payant

3.1.29**autorisation gratuite**

type de modèle de tarification autorisant une utilisation à titre gratuit

3.1.30**paiement à l'utilisation**

autorisation payante tarifiée à l'utilisation

3.1.31**abonnement**

autorisation payante tarifiée par période de temps

3.1.32**coupon**

autorisation payante utilisant des coupons, sorte de pseudo-monnaie pouvant être échangée contre un contenu donné

NOTE Un coupon est distribué aux utilisateurs par le parrain du contenu pour améliorer le contact de l'utilisateur avec ledit parrain.

3.1.33**type de parrain**

classification d'autorisation spécifiant la classe sponsor de l'autorisation, incluant un modèle publicitaire, un modèle premium, un modèle de coupon et un modèle de divulgation d'informations personnelles

3.1.34**modèle publicitaire**

type de parrain spécifiant le mode de réception de la publicité

3.1.35**visualisation forcée synchronisée dans le temps**

modèle publicitaire forçant la synchronisation de la visualisation de publicité et de l'accès au contenu

3.1.36**pré/post visualisation**

modèle publicitaire forçant le pré/post accès à la visualisation de publicité

3.1.37**heure arbitraire**

modèle publicitaire permettant la visualisation arbitraire de publicité, type de visualisation dans lequel les utilisateurs sont autorisés à choisir leur heure préférée pour visualiser la publicité

3.1.38

générale

modèle publicitaire forçant la visualisation quotidienne de publicité, tel que les termes de visualisation de publicité et d'accès au contenu s'appliquent à une large gamme de services associés au contenu

NOTE La visualisation générale de publicité est une condition d'autorisation d'accès au contenu. Le minutage de la visualisation de publicité n'est toutefois pas limité aux publicités synchronisées avec un contenu. Un utilisateur peut par exemple être autorisé à accéder à un contenu après avoir visualisé une chaîne publicitaire spéciale.

3.1.39

modèle premium

parrain utilisant un contenu pour un premium, où le terme «premium» se réfère à une pratique promotionnelle dans laquelle un parrain fournit à un utilisateur un accès à un contenu sous forme de récompense en contrepartie du contact de l'utilisateur avec ledit parrain

3.1.40

modèle de coupon

type de parrain utilisant un contenu sous forme de cadeau pour obtenir des coupons

NOTE Un coupon est distribué par le parrain du contenu pour améliorer le contact de l'utilisateur avec ledit parrain. Il s'agit d'une pratique promotionnelle dans laquelle un coupon, sorte de pseudo-monnaie, est échangé contre un contenu.

3.1.41

modèle de divulgation d'informations personnelles

type de parrain considérant que des informations personnelles doivent être divulguées pour accéder au contenu

3.1.42

type d'utilisation

classification d'autorisation spécifiant la classe usage de l'autorisation, incluant une autorisation de diffusion large et une autorisation de diffusion en continu

3.1.43

identifiant de territoire

identifiant spécifiant le territoire concerné par l'autorisation, incluant le pays et la zone

3.1.44

type de redistribution

classification d'autorisation spécifiant la classe redistribution de l'autorisation, incluant une redistribution simultanée, une diffusion en continu programmée et une diffusion en continu à la demande

3.1.45

autorisation sans enregistrement

type d'utilisation autorisant l'utilisation du contenu sans mémorisation

3.1.46

autorisation avec enregistrement

type d'utilisation autorisant l'utilisation du contenu avec mémorisation

3.1.47

autorisation de diffusion large

type d'utilisation autorisant l'utilisation du contenu par diffusion large

3.1.48

autorisation de diffusion en continu

type d'utilisation autorisant l'utilisation du contenu par diffusion en continu

3.1.49**autorisation de mémorisation de diffusion large**

type d'utilisation autorisant l'utilisation de la diffusion large du contenu avec mémorisation

3.1.50**autorisation de téléchargement (à la demande)**

type d'utilisation autorisant l'utilisation de la diffusion large du contenu avec mémorisation et fourniture à la demande

3.1.51**autorisation de redistribution**

type d'utilisation autorisant l'utilisation du contenu avec redistribution

3.1.52**diffusion en continu programmée**

autorisation de redistribution et/ou autorisation de diffusion en continu d'un contenu diffusé en continu conformément à des listes de programmes

3.1.53**diffusion en continu à la demande**

autorisation de redistribution et/ou autorisation de diffusion en continu d'un contenu diffusé en continu à la demande

3.1.54**autorisation de réutilisation**

type d'utilisation autorisant la réutilisation du contenu

3.1.55**transfert**

type d'utilisation autorisant le transfert d'un contenu vers un support conforme conformément à une autorisation de réutilisation

NOTE Les conditions d'autorisation sont spécifiées en outre avec un paramétrage.

3.1.56**copie**

type d'utilisation autorisant la copie d'un contenu vers un support conforme conformément à une autorisation de réutilisation

NOTE Les conditions d'autorisation sont spécifiées en outre avec un paramétrage.

3.1.57**partage**

type d'utilisation autorisant le partage d'un contenu dans le domaine résidentiel conformément à une autorisation de réutilisation

NOTE Les conditions d'autorisation sont spécifiées en outre avec un paramétrage.

3.1.58**export**

type d'utilisation autorisant l'exportation de contenu vers un support non conforme conformément à une autorisation de réutilisation

NOTE Les conditions d'autorisation sont spécifiées en outre avec un paramétrage.

3.1.59**édition**

type d'utilisation autorisant le traitement de l'axe des temps du contenu

3.1.60

modification

type d'utilisation autorisant le traitement de tout ce qui n'est pas l'axe des temps du contenu

3.1.61

superdistribution

type d'utilisation autorisant la superdistribution d'un contenu vers un support conforme conformément à une autorisation de réutilisation

NOTE Les conditions d'autorisation sont spécifiées en outre avec un paramétrage. La superdistribution permet de distribuer (et de redistribuer) librement un contenu chiffré, dans la mesure où les licences et les clés de contenu associées sont transférées de manière sûre.

3.1.62

code d'autorisation

système de code représentant des codes dans un système commun tel que les autorisations provenant de 2 parties avec des mises en œuvre de DRM différentes peuvent interopérer entre elles

3.1.63

code d'autorisation parentale

code d'autorisation délivré pour un groupe de contenus

3.1.64

code d'autorisation pour les enfants

code d'autorisation délivré pour un contenu individuel appartenant à un groupe plus large

3.1.65

centre d'identifiant

organisme autorisé qui assigne et gère les identifiants des acteurs d'autorisation

3.2 Termes abrégés

ID	Identifiant
DRM	(Système de) Gestion numérique des droits (en anglais, «Digital Rights Management»)
CPRM	Protection de contenu pour support enregistrable (en anglais, «Content Protection for Recordable Media»)
DVD-RW	Disque numérique universel réinscriptible (en anglais, «Digital Versatile Disk ReWritable»)
AACS	Système évolué d'accès au contenu (en anglais, «Advanced Access Control System»)
ISBN	International Standard Book Number (en anglais, «International Standard Book Number»)
HDD	Disque dur (en anglais, «Hard Disk Drive»)
DVD	Disque numérique universel (en anglais, «Digital Versatile Disk»)
DVD-R	Disque numérique universel enregistrable (en anglais, «Digital Versatile Disk Recordable»)
DTCP	Protection de contenu de transmission numérique (en anglais, «Digital Transmission Content Protection»)
TRM	Module inviolable (en anglais, «Tamper Resistant Module»)

XML	Langage de balisage extensible (en anglais, «Extensible Markup Language»)
RBP	Position d'octet relative (en anglais, «Relative Byte Position»)
ASCII	«American Standard Code for Information Interchange»
ISO	Organisation Internationale de Normalisation (en anglais, «International Organization for Standardization»)
UTC	Temps universel coordonné (en anglais, «Coordinated Universal Time»)
MPEG	Groupe d'experts des images animées (en anglais, «Moving Picture Expert Group»)
NTSC	National Television Standards Committee
Jpeg	Groupe mixte d'experts en photographie (en anglais, «Joint Photographic Experts Group»)
GIF	Format d'échange graphique (en anglais, «Graphic Interchange Format»)
PNG	Graphiques de réseaux portables (en anglais, «Portable Network Graphics»)
MIC	Modulation par impulsions et codage
AAC	Codage audio évolué (en anglais, «Advanced Audio Coding»)
MP3	MPEG audio, couche 3
HDCP	Protection des contenus numériques en haute définition (en anglais, «High-bandwidth Digital Content Protection»)
CGMS	Système de gestion de génération de copie (en anglais, «Copy Generation Management System»)
SAFIA	Architecture de sécurité pour annexe intelligente (en anglais, «Security Architecture For Intelligent Attachment»)
VCPS	Système de protection de contenu vidéo (en anglais, «Video Content Protection System»)
WMT	Technologie de support Windows (en anglais, «Windows Media Technology»)
uimsbf	entier sans signe, bit le plus significatif en tête (en anglais, «unsigned integer most significant bit first»)
bslbf	chaîne de bits, bit de gauche en tête (en anglais, «bit string, left bit first»)
imsbf	entier, bit le plus significatif en tête (en anglais, «integer most significant bit first»)
CD	Disque Compact
HD	Haute définition

4 Cadre du code d'autorisation

4.1 Généralités

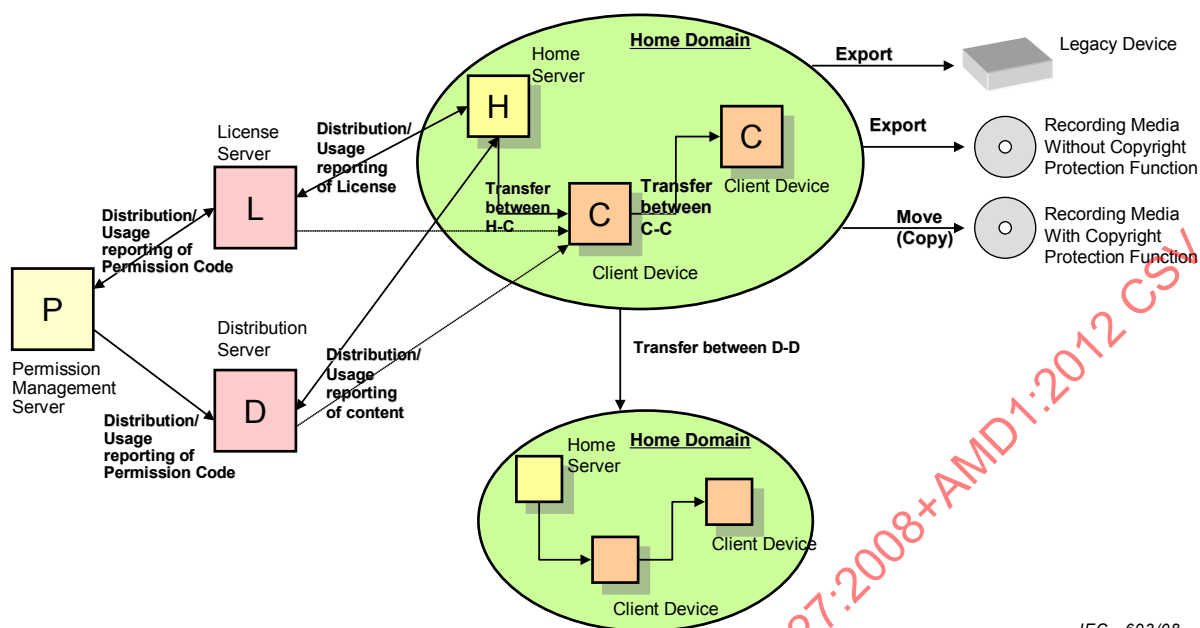
La présente norme définit l'autorisation comme un «acte d'une certaine entité émettrice pour autoriser à une certaine entité réceptrice l'utilisation d'un contenu conformément à un certain ensemble de conditions de classification d'autorisation, de conditions d'utilisation, de conditions de gestion de données et de conditions d'export de données».

Pour distribuer les informations d'autorisation avec le contenu qui leur est associé, la présente norme représente des informations d'autorisation au moyen de 5 expressions numériques, incluant l'identifiant de l'acteur d'autorisation, la classification d'autorisation, la condition d'utilisation, la condition de gestion de données et la condition d'export de données. L'identifiant de l'acteur d'autorisation est constitué de 3 identifiants; un identifiant de contenu assigné au contenu sujet et un identifiant d'émetteur et un identifiant de récepteur respectivement assignés à chaque émetteur et récepteur d'autorisation. La classification d'autorisation indique la classe (ou le type) de l'autorisation. La condition d'utilisation, la condition de gestion des données et la condition d'export de données donnent le détail des restrictions imposées au contenu.

On définit ainsi le cadre du code d'autorisation et le code d'autorisation sous forme de code et de cadre combinant ces 5 éléments; identifiant d'acteur d'autorisation, classification d'autorisation, condition d'utilisation, condition de gestion de données et condition d'export de données. Le code d'autorisation de base est configuré en utilisant une structure «balise-taille-données». Cette structure facilite l'extension du code d'autorisation. La présente norme spécifie en détail ces exigences de configuration.

Dans l'environnement de serveur résidentiel, des codes d'autorisation sont utilisés pour notifier aux utilisateurs les informations d'autorisation associées concernant l'utilisation de contenu, pour générer des licences DRM (Gestion numérique des droits, en anglais «Digital Rights Management») de protection des droits de contenu et pour rapporter l'utilisation de contenu.

Le diagramme illustre l'environnement d'utilisation de code d'autorisation sujet de la présente spécification. Le serveur de gestion d'autorisation est un acteur délivrant des codes d'autorisation en réponse à des demandes d'entités délivrant des autorisations. Le serveur de licence est un acteur générant des licences concernant la protection des droits de contenu. Le serveur de distribution est un acteur délivrant un contenu à l'environnement de serveur résidentiel. De plus, le domaine résidentiel représente l'environnement d'utilisation de contenu conforme à l'usage résidentiel. Le serveur résidentiel et les dispositifs clients sont des dispositifs de lecture appartenant au domaine résidentiel.



Légende

Anglais	Français
Permission Management Server	Serveur de gestion d'autorisation
Distribution/ Usage reporting of Permission Code	Rapport de distribution/utilisation de code d'autorisation
License Server	Serveur de licence
Distribution Server	Serveur de distribution
Distribution/ Usage reporting of License	Rapport de distribution/utilisation de Licence
Distribution/ Usage reporting of Content	Rapport de distribution/utilisation de contenu
Home Domain	Domaine résidentiel
Home Server	Serveur résidentiel
Transfer between H-C	Transfert entre H-C
Transfer between C-C	Transfert entre C-C
Client Device	Dispositif client
Export	Export
Move (Copy)	Transfert (copie)
Legacy Device	Dispositif existant
Recording Media Without Copyright Protection Function	Support d'enregistrement sans fonction de protection des droits d'auteur
Recording Media With Copyright Protection Function	Support d'enregistrement avec fonction de protection des droits d'auteur

Figure 1 – Environnement du code d'autorisation

4.2 Hypothèses associées au code d'autorisation

4.2.1 Relations binaires dans la chaîne de valeurs de distribution de contenu

L'autorisation entre 2 entités, l'entité émettrice et l'entité réceptrice, est l'unité d'autorisation définie pour un code d'autorisation. Énoncé différemment, dans le cas où il existe une entité intermédiaire entre une entité émettrice et une entité réceptrice, un code d'autorisation doit être respectivement généré entre l'entité intermédiaire et l'entité émettrice, ainsi qu'entre l'entité intermédiaire et l'entité réceptrice. Si par exemple une entité intermédiaire, Z, existe entre un émetteur A et un récepteur B, deux codes d'autorisation doivent être générés; un entre A et Z et l'autre entre Z et B.

4.2.2 Autorisation délivrée à un groupe de contenus

Une autorisation pour un corps de contenu lié à un identifiant de contenu est l'unité d'autorisation définie pour un code d'autorisation. En d'autres termes, si l'on souhaite regrouper de façon significative un sujet de contenu soumis à autorisation, on génère un code d'autorisation en assignant un identifiant de contenu à ce groupe de contenus. Ce faisant, des codes d'autorisation individuels sont également générés pour les contenus respectifs appartenant à ce groupe de contenus, en utilisant des identifiants de contenu associés à chaque unité « content ». La manière dont sont associés l'identifiant de contenu assigné au groupe de contenus ainsi que les identifiants de contenu respectifs appartenant au groupe est du domaine de la mise en œuvre et n'est donc pas définie dans cette norme.

La présente norme se réfère à des codes d'autorisation pour groupes sous forme de codes d'autorisation parentale. De façon similaire, cette norme se réfère à des codes d'autorisation pour contenu individuel comprenant le groupe sous forme de codes d'autorisation pour les enfants. Le code d'autorisation parentale est un code d'autorisation permettant d'obtenir l'autorisation pour le groupe complet. Le code d'autorisation parentale comporte des informations d'autorisation associées au groupe. Le code d'autorisation parentale est utilisé pour octroyer une autorisation pour une utilisation par abonnement. Un code d'autorisation parentale peut être utilisé par exemple pour un service d'abonnement permettant un nombre illimité d'accès à un contenu d'un groupe de 100 chansons pour 500 yens pendant une durée d'un mois. De façon similaire, le code d'autorisation pour les enfants est un code d'autorisation spécifiant des autorisations d'utilisation pour des contenus individuels dans un groupe. Le code d'autorisation pour les enfants comporte les informations d'autorisation pour des contenus individuels englobés dans un groupe. Des codes d'autorisation pour les enfants peuvent être utilisés par exemple pour le service d'abonnement mentionné ci-dessus pour spécifier des autorisations à chacun des 100 contenus individuels.

Le contenu du code d'autorisation pour les enfants ne peut pas dépasser le domaine d'application de l'autorisation du code d'autorisation parentale. Cette contrainte assure une cohérence logique entre des autorisations individuelles comprenant le groupe plus large et l'autorisation pour le groupe.

4.2.3 Centre de code commun pour les autorisations

Le centre de code commun est un organisme délivrant et renouvelant des codes d'autorisation.

Un code d'autorisation est délivré par l'intermédiaire du serveur de gestion d'autorisation, puis délivré au serveur de licence et au serveur de distribution.

Le serveur résidentiel et les dispositifs clients utilisent des codes d'autorisation inclus dans la licence et ne sont pas directement reliés au centre de code commun.

4.2.4 Rapport d'utilisation

Les fournisseurs de service de distribution ayant reçu des autorisations d'utilisation de contenu gardent la trace de l'utilisation du contenu de sorte qu'ils peuvent en référer aux émetteurs d'autorisation. Le suivi de l'historique d'utilisation s'effectue des 2 façons suivantes.

- a) Les fournisseurs de service de distribution gardent la trace du contenu fourni.
- b) Après réception du contenu, les serveurs résidentiels et les dispositifs clients gardent la trace de l'utilisation.

Dans la présente norme, le code d'autorisation est exigé en tant que code commun pour utilisation de la trace en utilisant la deuxième méthode ci-dessus. Les codes d'autorisation sont utilisés en tant que codes d'identification pour spécifier de manière unique les autorisations lors du rapport de l'utilisation de contenu.

Le rapport d'utilisation est effectué entre le serveur de gestion d'autorisation et le serveur de licence et aussi entre le serveur de gestion d'autorisation et le serveur de distribution. Le protocole du rapport ne fait pas partie du domaine d'application de la présente norme.

4.2.5 Scénario d'application du code d'autorisation

Le code d'autorisation spécifié dans la présente norme est un langage de description utilisé pour exprimer les termes de l'autorisation. L'utilisation de ce langage commun permet non seulement à la distribution de contenu de s'effectuer en douceur mais également de gérer différents systèmes de DRM (Gestion numérique des droits, en anglais «Digital Rights Management») sous un système uniforme.

Examinons par exemple la distribution de musique en ligne. En tant que partie de leur activité de réception de contrepartie en échange de la transmission de contenu aux utilisateurs finaux, les distributeurs de contenu négocient des contrats d'autorisation d'utilisation avec les éditeurs de disques. Le contenu de cette autorisation peut être exprimé en utilisant les codes d'autorisation.

Les distributeurs peuvent redistribuer une autorisation et/ou transmettre un contenu autorisé à des utilisateurs finaux dans le cadre du contrat d'autorisation et/ou du code d'autorisation. Ce faisant, les termes de l'autorisation à octroyer aux utilisateurs finaux peuvent être exprimés en utilisant les codes d'autorisation. De même, les utilisateurs finaux peuvent accéder au contenu et copier le contenu dans la limite indiquée dans le code d'autorisation.

Noter que le code d'autorisation est principalement un langage destiné à indiquer les termes de l'autorisation et il ne possède pas en lui-même la possibilité de réglementer le comportement d'utilisation du contenu. La limitation de l'utilisation du contenu aux termes spécifiés dans l'autorisation est une question administrative ou une question relevant du système de DRM. Un objet conforme au code d'autorisation se réfère à un objet tel que des systèmes de DRM, des dispositifs de lecture, des supports et des serveurs de stockage, etc., ayant la possibilité de comprendre les codes d'autorisation tels que spécifiés dans la présente norme et d'agir conformément à ceux-ci.

Les termes d'une autorisation destinée à des systèmes de DRM qui ne sont pas des codes d'autorisation conformes peuvent également être exprimés en utilisant des codes d'autorisation. Pour exporter un contenu d'un système de DRM conforme à un code d'autorisation vers un système non conforme, l'objet à la source de l'export doit donc traduire le contenu du code d'autorisation d'une manière conforme aux règles DRM de la cible de l'export.

Par exemple, la CPRM (Protection de contenu pour support enregistrable, en anglais «Content Protection for Recordable Media») utilisée dans un DVD-RW, l'AACS (Système évolué d'accès au contenu, en anglais «Advanced Access Control System») utilisé dans des disques Blu-ray constituent certains des systèmes de DRM qui ne sont pas conformes au code d'autorisation. Ces types de supports de stockage protègent le contenu avec leurs types respectifs de systèmes de DRM et ne reconnaissent pas les codes d'autorisation. Lors de l'export et/ou de la copie d'un contenu vers un tel support de stockage, les conditions d'autorisation doivent ainsi être traduites afin d'admettre le système de DRM de la cible.

Dans la présente norme, l'action de fournir en sortie un contenu à un objet non conforme depuis un objet conforme à un code d'autorisation est appelée «export». Par ailleurs, l'action d'aller et retour d'un contenu dans un objet conforme à un code d'autorisation ou entre des objets conformes à un code d'autorisation est appelée «gestion».

4.2.6 Harmonisation avec les systèmes de DRM (Gestion numérique des droits, en anglais «Digital Rights Management»)

Comme mentionné ci-dessus, le code d'autorisation est principalement un langage destiné à indiquer les termes de l'autorisation et il ne comporte pas de politique exclusive.

Chaque système de DRM (Gestion numérique des droits, en anglais «Digital Rights Management»), qu'il soit nouveau ou qu'il existe déjà, peut décider d'utiliser le code d'autorisation. Au contraire, chaque système de DRM peut décider de ne pas utiliser le code d'autorisation. Même s'il décide d'utiliser le code d'autorisation, il peut limiter l'application à un simple affichage de l'autorisation et le maintenir sans utiliser la gestion des droits.

De plus, l'autorisation exprimée par le code d'autorisation satisfait aux exigences des détenteurs de contenus et couvre la gamme d'autorisation exprimée par les systèmes de DRM existants. De plus, le code d'autorisation est conçu de manière à être étendu à des exigences supplémentaires d'une nouvelle autorisation de DRM et d'un nouveau modèle commercial.

En conséquence, aucun système de DRM n'est en conflit avec un autre, du fait qu'il utilise ou non du code d'autorisation ou de l'activation du code d'autorisation. En d'autres termes, le code d'autorisation est en harmonie avec tous les systèmes de DRM. Le code d'autorisation peut constituer le noyau central des systèmes de DRM.

4.3 Composants d'un code d'autorisation

4.3.1 Acteur d'autorisation

4.3.1.1 Généralités

Un acteur d'autorisation est un acteur échangeant une autorisation ou un acteur dont les actions sont réglementées en conséquence d'une autorisation, les acteurs d'autorisation sont constitués des trois acteurs suivants.

- Émetteur d'autorisation
- Récepteur d'autorisation
- Contenu

Chacun de ces acteurs est identifié par un identifiant d'acteur d'autorisation et est lié au code d'autorisation.

4.3.1.2 Identifiant d'un acteur d'autorisation

Un identifiant d'acteur d'autorisation est assigné à chaque acteur d'autorisation respectif. L'identifiant est utilisé pour distinguer les acteurs parmi l'émetteur, le récepteur et le contenu.

L'identifiant d'acteur d'autorisation du code d'autorisation a la possibilité de classifier un système d'identifiant existant. Par exemple, en ce qui concerne les identifiants d'émetteurs, certains organismes de droits gèrent des systèmes d'identifiant avec des identifiants de membres ou des identifiants de gestion interne. Des identifiant de gestion interne existent également pour le contenu. Des systèmes ouverts tels que le code ISBN pour les publications sont déjà en place. En plaçant un en-tête/préfixe spécifié dans le code d'autorisation sur ces systèmes d'identifiants existants, ces identifiants existants peuvent être adaptés comme identifiants d'acteur d'autorisation. Ceci permet une transition en douceur par rapport aux systèmes existants.

Avec les récepteurs d'autorisation en particulier, l'acteur d'autorisation est fréquemment un utilisateur final individuel ne faisant pas appel au type de système d'identifiant existant mentionné ci-dessus. De plus, la DRM (Gestion numérique des droits, en anglais «Digital Rights Management») utilisant le code d'autorisation doit être capable de déchiffrer la nature de l'utilisateur accédant au contenu. Dans ce but, la présente norme autorise à des identifiants de dispositifs respectifs intermédiaires dans la chaîne de distribution de contenu de servir d'identifiants de récepteur.

Les identifiants des acteurs d'autorisation sont assignés et gérés par des centres d'identifiant. Des organismes existants tels que des agences détentrices de droits par exemple peuvent devenir des centres d'identifiant. Ceci signifie que des organismes existants sont capables d'assigner des identifiants d'acteurs d'autorisation en combinant le code du centre d'identifiant et un code du système de codage existant utilisé avec l'organisme lui-même. Il peut y avoir plusieurs centres d'identifiant pour chaque catégorie d'acteur d'autorisation.

Certains exemples sont donnés ci-dessous, dans lesquels des identifiants de dispositif sont utilisés comme autres identifiants d'individu. Chaque exemple a ses propres partisans et adversaires. La méthodologie choisie est du ressort de la mise en œuvre et ne fait pas partie du domaine d'application de la présente norme. Cette norme définit uniquement le cadre pour les acteurs d'autorisation. La manière réelle dont les identifiants d'acteur d'autorisation sont assignés sera spécifiée dans un document séparé au niveau de la mise en œuvre.

- Identifiants d'utilisation (numéros de série, etc.) appartenant à des dispositifs de visualisation, d'enregistrement et de lecture, tels que des téléviseurs et des magnétoscopes, comme autres identifiants pour des utilisateurs individuels finaux.
- Identifiants d'utilisation (numéros de série, etc.) appartenant à un support de stockage intégré ou amovible, tel qu'un HDD (Disque dur, en anglais «Hard Disk Drive»), un support DVD et des cartes mémoire, comme autres identifiants pour des utilisateurs individuels finaux.
- Identifiants d'utilisation (numéros de téléphone, etc.) appartenant à des dispositifs quasi-personnels (dispositifs pouvant généralement être considérés comme appartenant à une personne, bien que ne l'étant pas au sens strict), tels que des téléphones portables, comme autres identifiants pour des utilisateurs individuels finaux.

4.3.1.3 Domaine

Dans la présente norme, un domaine se réfère à un ensemble d'acteurs auxquels s'applique un ensemble de règles communes dans le contexte de la gestion du contenu. Cet ensemble de règles communes peut être appliqué à chaque contenu ou appliqué indépendamment du contenu.

Les autorisations d'utilisation de contenu sont généralement liées à des supports ou à des dispositifs de stockage. Par exemple, «ce contenu ne peut pas être copié sur un autre support de stockage» ou «ce contenu ne peut être lu que sur ce dispositif» sont quelques-unes des manières courantes dont le contenu est géré. Toutefois, lorsqu'une autorisation est plutôt octroyée à un domaine, tous les supports et dispositifs de stockage appartenant à celui-ci sont gérés de manière équivalente et fonctionnent avec un ensemble commun de termes et de règles d'autorisation.

Considérons par exemple les domaines résidentiels. Un domaine résidentiel se réfère à «un ensemble de dispositifs présents dans un domicile donné. Un émetteur d'autorisation de contenu peut délivrer une autorisation pour copier librement un contenu au sein du domaine résidentiel». Le récepteur d'autorisation possède ici la possibilité de gérer un contenu conformément à la règle commune: le contenu a peut être librement copié au sein du domaine résidentiel.

De même, un ensemble de dispositifs appartenant à une école peut être défini comme un domaine scolaire. Si l'on suppose que le contenu b est utilisé à des fins éducatives, un émetteur d'autorisation peut délivrer une autorisation qui «autorise la copie et l'édition du contenu b dans le domaine scolaire». Le récepteur d'autorisation est ici capable d'extraire et de compiler des parties du contenu b nécessaires et de les insérer dans le contenu propre de l'école pour créer un nouveau matériel éducatif. Le récepteur d'autorisation peut également copier le contenu résultant dans des dispositifs appartenant au domaine scolaire parmi des salles de classe.

Comme décrit, les autorisations d'utilisation de contenu peuvent être liées à des domaines. Par ailleurs, d'autres types de liens d'autorisation peuvent également être pris en charge. Une autorisation peut par exemple être liée à une unité « individual storage media » d'une manière classique (par exemple, «la copie de ce disque n'est pas autorisée»). Une autorisation peut être liée à un utilisateur individuel (par exemple, seul Mr. X peut visualiser ce contenu). L'avantage de lier des autorisations à des domaines par opposition à des autorisations classiques délivrées à des unités individuelles est leur possibilité de limiter une diffusion de contenu indésirable au profit des détenteurs de droits tout en autorisant le partage de contenu au sein d'une communauté.

Il existe un nombre illimité de domaines. Un domaine peut en englober un autre ou des domaines peuvent se recouvrir. Des exemples de types de domaine et de motifs d'utilisation dans ces domaines comportent, «domaine résidentiel: peut copier librement un contenu à l'intérieur du domicile», «domaine scolaire: dans la mesure où le but de l'utilisation est éducatif, le contenu peut être édité et utilisé sur des dispositifs appartenant à l'école» et «domaine d'entreprise», etc.

Comme illustré, un domaine peut être caractérisé comme une collectivité de récepteur d'autorisation. Un acteur appartenant au domaine est autorisé à agir en tant que récepteur de l'autorisation en question. En d'autres termes, un domaine est également un récepteur d'autorisation et un identifiant d'acteur d'autorisation lui est assigné.

Les domaines présentés dans la présente norme sont des domaines définis par l'émetteur: l'émetteur d'autorisation et le récepteur d'autorisation déterminent le domaine en se basant sur des termes ayant fait l'objet d'un accord mutuel lorsque l'utilisation du contenu est octroyée. Ce domaine est expliqué dans le paragraphe suivant.

4.3.1.4 Domaine défini par l'émetteur

Un domaine défini par l'émetteur se réfère à un domaine au sein duquel des informations de protection des droits du contenu peuvent être partagées. Il est établi par un émetteur d'autorisation et est déterminé sur la base d'un accord mutuel entre un émetteur d'autorisation et un récepteur d'autorisation.

Dans la pratique, le domaine d'application limite le domaine défini par l'émetteur à l'intérieur du domicile ou d'une école, etc., le rendant pratiquement équivalent à une limite physique. Toutefois, de façon conceptuelle, il ne constitue pas simplement un regroupement de dispositifs, supports de stockage ou êtres humains voisins, mais plutôt un regroupement avec un domaine d'application élaboré de manière plus logique. Par exemple, en pensant à des domaines résidentiels, on peut considérer non seulement les dispositifs qui existent physiquement au sein du domicile en tant que partie du domaine résidentiel, mais également des dispositifs mobiles appartenant à un membre d'une famille ainsi que des appareils, etc., détenus dans une résidence secondaire, faisant partie des dispositifs constituant le domaine résidentiel. Toutefois, la manière dont on détermine si ces objets appartiennent ou non au

domaine ne fait pas partie du domaine d'application de la présente norme et seront spécifiés dans un document séparé au niveau de la mise en œuvre.

Avec un contenu éducatif, dans la mesure où le but de l'utilisation est éducatif, des droits tels que la redistribution, l'enregistrement et l'édition sont généralement octroyés. On peut supposer que dans un environnement scolaire, plusieurs dispositifs sont liés par l'intermédiaire du réseau et que le contenu éducatif est librement visualisé, édité et mémorisé. Il devient donc nécessaire de garantir que le contenu ne sera utilisé qu'à l'intérieur de l'école. C'est la raison pour laquelle des domaines déterminés par l'émetteur sont définis.

De façon similaire, en définissant des domaines déterminés par l'émetteur tels qu'un domaine résidentiel, les émetteurs d'autorisation peuvent garantir aux récepteurs d'autorisation le droit d'une utilisation personnelle de contenu au sein du domaine résidentiel.

La signification de ce domaine réside dans sa possibilité de permettre à des émetteurs d'autorisation de confirmer que leur contenu est géré conformément aux termes de l'autorisation. Cette configuration assure que l'émetteur du code d'autorisation dispose de moyens pour spécifier des dispositifs, des supports de stockage et des utilisateurs appartenant au domaine pour s'assurer que cette confirmation s'effectue.

4.3.2 Classification d'autorisation

Dans la présente norme, on utilise une classification d'autorisation pour spécifier la classification de l'autorisation et elle est constituée de la classe disclosure, de la classe usage purpose, de la classe charge model, de la classe billing, de la classe application, de la classe sponsor, de la classe territory et de la classe usage et elle est évaluée positivement. Le code d'autorisation interprète donc le contenu indiqué dans la classification d'autorisation comme autorisation octroyée par l'émetteur d'autorisation.

La classification d'autorisation décrit le contenu des modifications destinées à des utilisateurs humains. Elle est équivalente par exemple à des mentions de droits d'auteur que l'on trouve au début des films de divertissement conditionnés en paquet.

4.3.3 Utilisation du contenu

4.3.3.1 Généralités

Dans la présente norme, l'utilisation et/ou les termes du contenu sont constitués des 4 éléments suivants:

- a) Condition générale d'utilisation décrivant les conditions en se basant sur un mode d'utilisation;
- b) Condition étendue d'utilisation décrivant des conditions étendues par rapport à la condition habituelle d'utilisation;
- c) Condition de gestion des données décrivant les conditions concernant la sauvegarde du contenu d'origine ou les codes d'autorisation de réédition, etc.
- d) Condition d'export de données décrivant des conditions concernant l'export du contenu d'origine vers des objets non conformes.

Lors de l'interprétation de conditions similaires, les conditions qui ont des termes plus restrictifs que les autres doivent être appliquées. De plus, on doit estimer que le code d'autorisation n'est pas interprétable dans le cas où une interprétation par un objet non conforme provoque une incohérence.

4.3.3.2 Condition générale d'utilisation

La condition générale d'utilisation est constituée du mode d'utilisation par l'utilisateur final du contenu et des conditions d'utilisation qui réglementent cette utilisation. Elle représente

l'autorisation d'utiliser un contenu basé sur le mode d'utilisation spécifié par l'émetteur d'autorisation et sa condition d'utilisation.

La présente norme définit trois modes d'utilisation: lecture, impression et exécution.

4.3.3.3 Condition étendue d'utilisation

Les conditions étendues d'utilisation complètent les conditions ne pouvant pas être exprimées sous forme de conditions générales d'utilisation. La présente norme ne spécifie pas leur contenu.

4.3.3.4 Condition de gestion des données

La condition de gestion des données décrit les conditions de gestion s'appliquant lorsqu'un contenu original est enregistré (mémorisé) dans un objet conforme. Elle représente une autorisation de gestion de contenu dans une cible de gestion spécifiée par l'émetteur d'autorisation conformément aux conditions de gestion spécifiées.

La présente norme considère les objets conformes comme des cibles de gestion.

4.3.3.5 Condition d'export de données

La condition d'export de données décrit des conditions d'export qui s'appliquent lors de l'export du contenu d'origine vers des objets non conformes. Elle représente une autorisation de l'export de contenu dans une cible d'export spécifiée par l'émetteur d'autorisation conformément aux conditions d'export spécifiées.

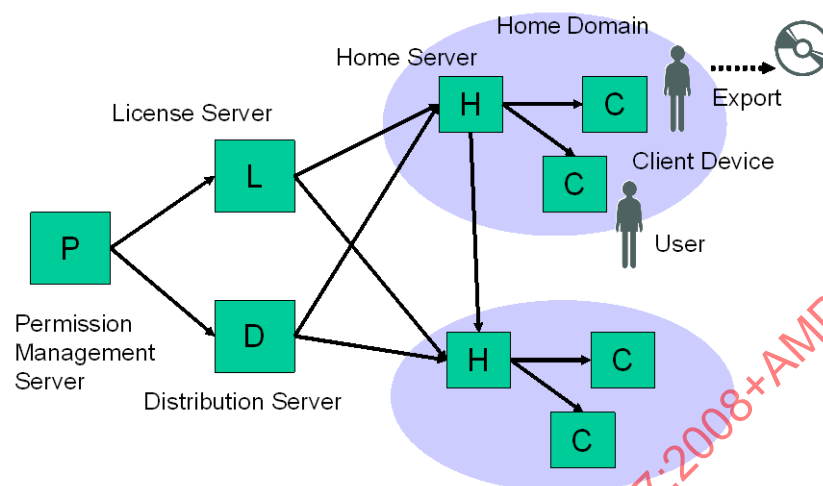
La présente norme définit les conditions d'export à usage général.

4.3.4 Gestion des données de contenu

4.3.4.1 Généralités

Le code d'autorisation proposé suppose que lors de la transmission le contenu et son code d'autorisation suivent le trajet illustré sur le diagramme ci-dessous. Le diagramme illustre le serveur de gestion d'autorisation qui représente le gestionnaire d'autorisation de contenu, le serveur de distribution et le serveur de licence qui représentent les distributeurs de contenu et de licence et le domaine qui représente les acteurs d'utilisation (incluant le domicile et l'école, etc.) de contenu. On suppose que le dispositif du domaine recevant directement le code d'autorisation du serveur de gestion d'autorisation, du serveur de distribution ou de serveur de licence, est capable de gérer le code d'autorisation de cette spécification. De plus, en fonction du paramétrage du code d'autorisation, les objets conformes issus du domaine peuvent être exportés vers d'autres objets non conformes en dehors du domaine.

Permission Code Environment



IEC 694/08

Légende

Anglais	Français
Permission Code Environment	Environnement de code d'autorisation
Permission Management Server	Serveur de gestion d'autorisation
License Server	Serveur de licence
Distribution Server	Serveur de distribution
Home Server	Serveur résidentiel
Home Domain	Domaine résidentiel
Export	Export
Client Device	Dispositif client
User	Utilisateur

Figure 2 – Environnement du code d'autorisation

4.3.4.2 Gestion des données parmi les objets conformes au code d'autorisation

Le code d'autorisation définit le domaine sous forme d'une collection de dispositifs, etc., avec des identifiants uniques. Les dispositifs peuvent ici inclure un dispositif de stockage, un dispositif de lecture, un dispositif d'édition ou une carte d'identifiant qui identifie un utilisateur. L'émetteur d'autorisation peut directement (avec des identifiants) ou indirectement (par l'intermédiaire du nombre d'identifiants de dispositif gérés par un serveur résidentiel) vérifier que des dispositifs sont présents dans un domaine spécifique.

Les dispositifs spécifiques du domaine sont autorisés à gérer des données d'une manière équitable au sein du domaine d'application du code d'autorisation en échange de dispositifs appartenant au domaine vérifié par les émetteurs d'autorisation. De façon spécifique, tous les dispositifs du domaine sont autorisés à gérer des données en conformité avec l'autorisation, ce qui inclut la mémorisation, le transcodage et la lecture de données.

4.3.4.3 Export de données vers des objets conformes à un code sans autorisation

En ce qui concerne l'export de données vers des objets (dispositifs et domaines) conformes à un code sans autorisation, le code d'autorisation est configuré en faisant l'hypothèse des 3 cas suivants. Noter qu'un grand nombre de cas impliquant l'export vers des objets conformes à un code sans autorisation limitent le nombre de fois où l'export peut être effectué. Dans ce cas, il devient nécessaire qu'un dispositif spécifique gère uniformément le nombre d'exports.

- a) Instances dans lesquelles la cible d'export des données requise pour l'utilisation des données est conforme à un code sans autorisation, par exemple dans le cas de l'export vers un dispositif d'affichage ou un haut-parleur, etc.
- b) Instances dans lesquelles l'export vers un support de stockage conforme à un code sans autorisation par exemple un DVD-R conforme à la CPRM (Protection de contenu pour support enregistrable, en anglais «Content Protection for Recordable Media») est autorisé. Ou instances dans lesquelles l'export vers un support de transmission tel que DTCP (Protection de contenu de transmission numérique, en anglais «Digital Transmission Content Protection»), etc., est autorisé.
- c) Instances dans lesquelles le contenu est exporté vers un autre objet conforme à un code sans autorisation.

Après l'export vers un objet conforme à un code sans autorisation, le code d'autorisation ne peut ni gérer ni contrôler le comportement, ni d'un contenu, ni de dispositifs. Toutefois, en traduisant le code d'autorisation en informations de contrôle de contenu du système de DRM (Gestion numérique des droits, en anglais «Digital Rights Management») cible d'export, on peut obtenir une interopérabilité entre des objets conformes à un code d'autorisation et des systèmes de DRM existants.

5 Configuration du code d'autorisation

5.1 Généralités

Cet article présente le format du code d'autorisation. Le but principal des codes d'autorisation, comme mentionné ci-dessus, est de communiquer la volonté d'autorisation de l'émetteur d'autorisation au récepteur d'autorisation. La manière dont les systèmes de DRM (Gestion numérique des droits, en anglais «Digital Rights Management») respectifs fonctionnent conformément au code d'autorisation est donc entièrement du ressort des politiques d'exploitation des systèmes de DRM respectifs et/ou de la mise en œuvre des dispositifs respectifs. Ainsi, l'interprétation du code d'autorisation au niveau fonctionnel doit être spécifiée dans les spécifications de DRM respectives.

De plus, les termes spécifiés dans le code d'autorisation peuvent généralement être considérés comme appartenant à deux catégories:

- a) une description du contenu à communiquer à un utilisateur final (humain), et
- b) une description des instructions d'exploitation adaptées aux dispositifs constituant le système de DRM.

a) se réfère par exemple à l'équivalent à des mentions de droits d'auteur affichées au début des films de divertissement conditionnés en paquet. Dans un grand nombre de cas, il ne dispose pas de pouvoir exécutoire vis-à-vis des systèmes de DRM. b) se réfère à l'équivalent des informations de contrôle de copie. Le but est que les systèmes de DRM interprètent ce code d'autorisation pour fonctionner conformément aux termes respectifs contenus dans le code d'autorisation.

La présente norme comporte une marque † sur la précédente pour distinguer ces deux catégories.

Le code d'autorisation possède une autre politique de configuration, l'économie de taille des données. On suppose que le code d'autorisation est protégé par TRM (Module inviolable, en anglais «Tamper Resistant Module»), ce qui est beaucoup plus onéreux que l'absence de TRM pour les aspects de traitement et de stockage. Les informations d'autorisation sont donc exprimées selon un style codé en tant que code d'autorisation autre qu'une description redondante, par exemple en XML, pour minimiser sa longueur et le traitement nécessaire des données considérées comme étant directement traitées par TRM.

5.2 Notation

5.2.1 Valeurs numériques

5.2.1.1 Notation décimale

Un nombre décimal est exprimé sous forme de chiffres décimaux de 0 à 9.

5.2.1.2 Notation hexadécimale

Un nombre hexadécimal est exprimé sous forme de chiffres hexadécimaux de 0 à 9 et de A à F, préfixés par le symbole «0x».

5.2.1.3 Notation binaire

Un nombre binaire est exprimé par le chiffre binaire 0 ou 1, avec le symbole b en suffixe.

5.2.1.4 Chaîne de bits

bslbf doit être une chaîne de bits, le bit de gauche en tête.

5.2.1.5 Valeur numérique sans signe

uimsbf doit être un entier sans signe, le bit le plus significatif en tête.

5.2.1.6 Distinct tag

Une balise distincte est exprimée comme suit. Voir 5.3.

Tableau 1 – Interprétation de Distinct tag

Valeur	Balise
0x00	Réservé
0x01	Unité version
0x02-0x0F	Réservé
0x10	Unité permission actor
0x11	Unité permission classification
0x12	Unité general usage condition
0x13	Unité extended usage condition
0x14	Unité data management condition
0x15	Unité data export condition

5.2.1.7 Champ Reserved

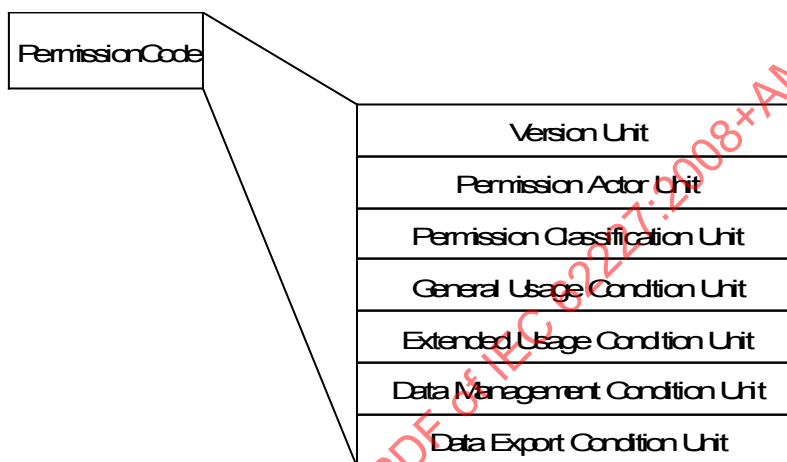
Tous les bits des champs réservés doivent être mis à 0b.

5.3 Système de code d'autorisation

Le code d'autorisation est constitué de sept types d'unités d'information, comme indiqué ci-dessous.

Bien que le code d'autorisation soit constitué de plusieurs unités, il ne nécessite pas obligatoirement toutes les unités. Certaines unités peuvent être omises selon la nature du contenu de l'autorisation. De plus, bien que l'ordre général soit le suivant, il n'est pas limité à cet ordre.

Le code d'autorisation présente la structure hiérarchique suivante, balise–longueur–données principales. La balise supérieure détermine la syntaxe de la partie de données principales. Se référer à 5.2.1.6 pour de plus amples informations concernant les balises.



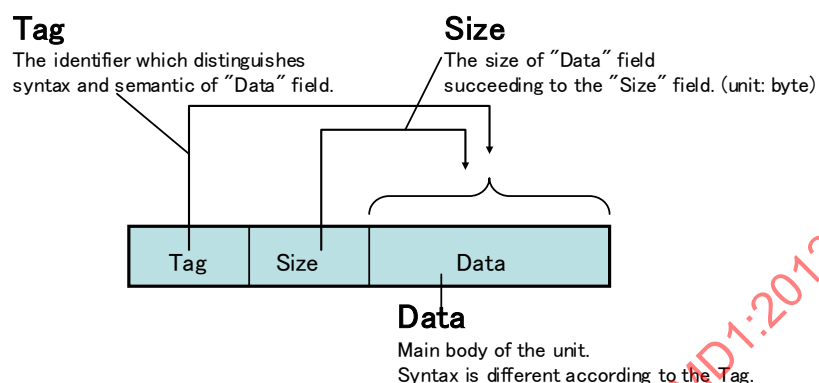
IEC 695/08

Légende

Anglais	Français
Version Unit	Unité Version
Permission Actor Unit	Unité Permission Actor
Permission Classification Unit	Unité Permission Classification
General Usage Condition Unit	Unité General Usage Condition
Extended Usage Condition Unit	Unité Extended Usage Condition
Data Management Condition Unit	Unité Data Management Condition
Data Export Condition Unit	Unité Data Export Condition

Figure 3 – Configuration du code d'autorisation

Permission Code – Basic Structure of Each Unit



IEC 696/08

Légende

Anglais	Français
Tag	Balise
The identifier which distinguishes syntax and semantic of "Data" field	Identifiant distinguant la syntaxe et la sémantique du champ "Data"
Size	Taille
The size of "Data" field succeeding to the "Size" field (unit: byte)	Taille du champ "Data" suivant le champ "Size" (unité: octet)
Data	Données
Main body of the unit Syntax is different according to the Tag	Corps principal de l'unité La syntaxe est différente selon la balise

Figure 4 – Structure de base de l'unité permission code

5.4 Version unit

5.4.1 Structure

Tableau 2 – Structure de version unit

RBP (Position d'octet relative, en anglais «Relative Byte Position»)	Longueur en octets	Nom du champ	Contenu
0	1	Version unit tag	TAG
1	1	Reserved	bslbf
2	1	Version	VER

5.4.2 Version unit tag

Ce champ doit être mis à 0x01.

5.4.3 Reserved

Ce champ doit être réservé pour une normalisation future et tous les octets doivent être mis à 0x00.

5.4.4 Version

Ce champ doit être mis à 0x10. Ceci signifie version 1.0. Les 4 premiers bits représentent la version majeure et les 4 bits qui suivent représentent la version mineure.

5.5 Permission actor unit

5.5.1 Structure

Tableau 3 – Structure de permission actor unit

RBP (Position d'octet relative, en anglais «Relative Byte Position»)	Longueur en octets	Nom du champ	Contenu
0	1	Permission actor unit tag	TAG
1	1	Total bytes of identifiers (=S)	uimsbf
2	id1	Content ID descriptor (=id1)	bslbf
2+id1	id2	Issuer ID descriptor (=id2)	bslbf
2+id1+id2	S-id1-id2	Receiver ID descriptor	bslbf

En ce qui concerne les codes d'autorisation, l'autorité pour assigner des identifiants d'acteur d'autorisation appartient aux centres d'identifiant qui gèrent les acteurs d'autorisation. Ainsi, les acteurs d'autorisation sont exprimés en utilisant une combinaison des identifiants assignés à ces centres d'identifiant (se référer à 5.5.4.4, 5.5.5.5, 5.5.6.5) et d'identifiants uniques qui sont assignés par des organismes respectifs sur la base de leurs propres politiques respectives.

Ainsi, en ce qui concerne ce dernier identifiant unique, des systèmes d'identifiants propriétaires existants gérés par des centres d'identifiant de gestion de droits peuvent être utilisés «tels quels», permettant une migration en douceur vers l'utilisation des codes d'autorisation.

5.5.2 Permission actor unit tag

Ce champ doit être mis à 0x10.

5.5.3 Total bytes of identifiers

Ce champ représente le nombre total d'octets alloués pour les descripteurs d'identifiant de contenu, d'identifiant d'émetteur et d'identifiant de récepteur.

5.5.4 Identifiant de contenu

5.5.4.1 Structure

Tableau 4 – Structure du descripteur content identifier

Syntaxe	Bits	Identifiant
Content_Identifier_descriptor() { content_type_code	16	bslbf
if ((content_type_code >> 8) == ASCII) {		
Country Code	16	char(2)
ID Center Code	32	char(4)
Unique Code	64	char(8)
} else {		
extended_identifier_length	16	uimsbf
extended_identifier	n	bslbf
}		
}		

5.5.4.2 Content type code

Ce champ représente la classification de contenu. Le Tableau 5 représente l'interprétation du code de type de contenu lorsque son premier octet est en ASCII. Sinon, il est réservé.

Tableau 5 – Interprétation de Content type code

Classification du contenu	Interprétation
SM	Musique acoustique
SD	Théâtre acoustique
SP	Programme acoustique
SN	Informations acoustique
SA	Publicité acoustique
SO	Objet acoustique
VM	Musique en vidéo
VD	Théâtre en vidéo
VP	Programme en vidéo
VF	Film en vidéo
VC	Bande dessinée en vidéo
VN	Informations en vidéo
VA	Publicité en vidéo
VO	Objet en vidéo
TP	Programme textuel
TD	Théâtre textuel
TM	Musique textuelle
TT	Thèse textuelle
TN	Informations textuelles
TO	Objet textuel
IB	Livre en image
IP	Programme en image
II	Illustration en image
IC	Bande dessinée en image

Classification du contenu	Interprétation
IM	Musique en image
IA	Publicité en image
IO	Objet en image
PG	Programme de jeu
PS	Programme logiciel
PM	Programme musical
PA	Programme publicitaire
PO	Programme d'objet
GG	Groupe général

5.5.4.3 Country code

La valeur de ce champ utilise le format de code de pays ISO à deux lettres (ISO 3136-1).

5.5.4.4 ID center code

Ce champ représente l'identifiant assigné au centre d'identifiant.

5.5.4.5 Unique code

Ce champ représente le code unique assigné par le centre d'identifiant.

5.5.4.6 extended_identifier_length

Ce champ décrit la longueur en octets de l'identifiant étendu. La valeur de ce champ dépend de sa propre structure.

5.5.4.7 extended_identifier

Ce champ représente l'identifiant étendu nécessaire pour une identification complémentaire du contenu cible en question.

5.5.5 Identifiant d'émetteur

5.5.5.1 Structure

Tableau 6 – Structure du descripteur issuer identifier

Syntaxe	Bits	Identifiant
Issuer_Identifier_descriptor() { issuer_role_code if (issuer_role_code == ASCII) { Country Code Issuer Configuration Code ID Center Code Unique Code } else { extended_identifier_length extended_identifier } }	8 16 8 32 64 16 n	bslbf char(2) char(1) char(4) char(8) uimsbf bslbf

5.5.5.2 Issuer role code

Ce champ représente le rôle de l'émetteur vis-à-vis de l'autorisation.

Tableau 7 – Interprétation de Issuer role code

Valeur	Interprétation
0x00-0x43	Réservé
0x44	Identifiant de distributeur
0x45-0x47	Réservé
0x48	Identifiant de détenteur
0x49-0xff	Réservé

5.5.5.3 Country Code

La valeur de ce champ utilise le format de code de pays ISO à deux lettres (ISO 3136-1).

5.5.5.4 Issuer Configuration Code

Ce champ représente la configuration de l'émetteur par rapport à son fonctionnement.

Tableau 8 – Interprétation de Issuer configuration code

Issuer configuration	Interprétation
O	Organisme
C	Entreprise
I	Individu
D	Dispositif (incluant un support de stockage)

5.5.5.5 ID Center Code

Ce champ représente un numéro d'identification assigné à l'émetteur par rapport à sa configuration dans l'ordre d'application (2 chiffres numériques). Si le code de configuration de l'émetteur est D (dispositif), il n'y a pas de code d'opérateur.

5.5.5.6 Unique Code

Ce champ représente le code unique assigné à la configuration de fonctionnement de l'opérateur.

5.5.5.7 extended_identifier_length

Ce champ décrit la longueur en octets de l'identifiant étendu. La valeur de ce champ dépend de sa propre structure.

5.5.5.8 extended_identifier

Ce champ représente l'identifiant étendu nécessaire pour une identification complémentaire de l'émetteur cible en question.

5.5.6 Identifiant de récepteur

5.5.6.1 Structure

Tableau 9 – Structure du descripteur receiver identifier

Syntaxe	Bits	Identifiant
Receiver_Identifier_descriptor() { receiver_role_code if (receiver_role_code == ASCII) { Country code Receiver configuration code ID center code Unique code } else { extended_identifier_length extended_identifier } }	8 16 8 32 64 16 n	bslbf char(2) char(1) char(4) char(8) uimsbf bslbf

5.5.6.2 Receiver role code

Ce champ représente le rôle du récepteur vis-à-vis de l'autorisation.

Tableau 10 – Interprétation de Receiver role code

Valeur	Interprétation
0x00-0x43	Réservé
0x44	Identifiant de distributeur
0x45-0x47	Réserve
0x48	Identifiant de détenteur
0x49-0x54	Réserve
0x55	Identifiant d'utilisateur
0x56-0xff	Réserve

5.5.6.3 Country code

La valeur de ce champ utilise le format de code de pays ISO à deux lettres (ISO 3136-1).

5.5.6.4 Receiver configuration code

Ce champ représente la configuration du récepteur par rapport à son fonctionnement.

Tableau 11 – Interprétation du Receiver configuration code

Receiver configuration	Interprétation
O	Organisme
C	Entreprise
I	Individu
D	Dispositif (incluant un support de stockage)

5.5.6.5 ID center code

Ce champ représente un numéro d'identification assigné au récepteur par rapport à sa configuration dans l'ordre d'application (2 chiffres numériques). Si le code de configuration du récepteur est D (dispositif), il n'y a pas de code d'opérateur.

5.5.6.6 Unique code

Ce champ représente le code unique assigné à la configuration de fonctionnement de l'opérateur.

5.5.6.7 extended_identifier_length

Ce champ décrit la longueur en octets de l'identifiant étendu. La valeur de ce champ dépend de sa propre structure.

5.5.6.8 extended_identifier

Ce champ représente l'identifiant étendu nécessaire pour une identification complémentaire du récepteur cible en question.

5.6 Permission classification unit†

5.6.1 Structure

Tableau 12 – Structure de permission classification unit

Position relative des bits	Longueur en bits	Nom du champ	Contenu
0	8	Permission classification unit tag	TAG
8	8	Reserved	bslbf
16	2	Disclosure class	bslbf
18	3	Usage purpose class	bslbf
21	5	Charge model class	bslbf
26	2	Billing class	bslbf
28	2	Application class	bslbf
30	2 4	Sponsor class	bslbf
32 34	3	Territory class	bslbf
35 37	13 19	Usage class	bslbf

5.6.2 Permission classification unit tag

Ce champ doit être mis à 0x11.

5.6.3 Reserved

Ce champ doit être réservé pour une normalisation future et tous les octets doivent être mis à 0x00.

5.6.4 Disclosure class

Cette classe spécifie les termes de la divulgation de l'autorisation, incluant une autorisation ouverte et une autorisation fermée

Tableau 13 – Structure de disclosure class

Syntaxe	Bits	Identifiant
Disclosure_Class () { disclosure_type }	2	bslbf

Le champ disclosure class spécifie le type de classe disclosure.

Tableau 14 – Interprétation de disclosure_type (DT)

Valeur	Interprétation
00b	Réservé
01b	Indique que DT est à open permission
10b	Indique que DT est à closed permission
11b	Indique que DT est à other

5.6.5 Usage purpose class

5.6.5.1 Structure

Cette classe spécifie l'usage général de l'autorisation, incluant une autorisation commerciale, publique et promotionnelle.

Tableau 15 – Structure de usage purpose class

Syntaxe	Bits	Identifiant
Usage_Purpose_Class () { usage_purpose_type }	3	bslbf

5.6.5.2 usage_purpose_type

Ce champ spécifie le type de classe usage purpose.

Tableau 16 – Interprétation de usage_purpose_type (UPT)

Valeur	Interprétation
000b	Réservé
001b	Indique que UPT est à commercial permission
010b	Indique que UPT est à public permission
011b	Indique que UPT est à not for profit permission
100b	Indique que UPT est à promotion permission
101b	Indique que UPT est à education permission
111b	Indique que UPT est à other

5.6.6 Charge model class

5.6.6.1 Structure

Cette classe spécifie le modèle de tarification de l'autorisation.

Tableau 17 – Structure de charge model class

Syntaxe	Bits	Identifiant
Charge_Model_Class () { charge_model_type if (charge_model_type==10b) { pay_per_use_flag subscription_flag coupon_flag } else { reserved } }	2 1 1 1 3	bslbf bslbf bslbf bslbf bslbf

5.6.6.2 charge_model_type

Ce champ spécifie le type de classe charge model.

Tableau 18 – Interprétation de charge_model_type (CMT)

Valeur	Interprétation
00b	Réservé
01b	Indique que CMT est à free of charge
10b	Indique que CMT est à for charge
11b	Indique que CMT est à other

5.6.6.3 pay_per_use_flag

Si la valeur est 1b, cela indique qu'il est autorisé d'appliquer un tarif du contenu facturé à l'utilisation. Si la valeur est 0b, cela indique qu'il n'est pas autorisé d'appliquer un tarif du contenu facturé à l'utilisation.

5.6.6.4 subscription_flag

Si la valeur est 1b, cela indique qu'il est autorisé de distribuer le contenu par abonnement. Si la valeur est 0b, cela indique qu'il n'est pas autorisé de distribuer le contenu par abonnement.

5.6.6.5 coupon_flag

Si la valeur est 1b, cela indique qu'il est autorisé de distribuer le contenu en échange de coupons. Si la valeur est 0b, cela indique qu'il n'est pas autorisé de distribuer le contenu en échange de coupons.

5.6.7 Billing class

Cette classe spécifie les termes de facturation de l'autorisation.

Si CMT est libre de charge, il convient qu'il soit autre (11b).

Tableau 19 – Structure de billing class

Syntaxe	Bits	Identifiant
Billing_Class () { billing_type }	2	bslbf

Le champ billing_type spécifie le type de classe billing.

Tableau 20 – Interprétation de billing_type (BT)

Valeur	Interprétation
00b	Réservé
01b	Indique que BT et à ad hoc billing
10b	Indique que BT et à blanket billing
11b	Indique que BT est à other

5.6.8 Application class

Cette classe spécifie les termes d'application de l'autorisation, incluant une autorisation ad hoc et une autorisation générale.

Tableau 21 – Structure de application class

Syntaxe	Bits	Identifiant
Application_Class () { application_type }	2	bslbf

Le champ application_type spécifie le type de classe application.

Tableau 22 – Interprétation de application_type (AT)

Valeur	Interprétation
00b	Réservé
01b	Indique que AT et à ad hoc permission
10b	Indique que AT et à blanket permission
11b	Indique que AT est à other

5.6.9 Sponsor class

Cette classe spécifie les termes de parrainage de l'autorisation, incluant un modèle publicitaire, un modèle premium, un modèle de coupon et un modèle de divulgation d'informations personnelles. Lorsqu'on sélectionne un modèle de publicité, on doit spécifier une option parmi la visualisation forcée synchronisée dans le temps, la pré/post-visualisation, arbitraire dans le temps et générale.

Tableau 23 – Structure de sponsor class

Syntaxe	Bits	Identifiant
Sponsor_Class () { sponsor_type }	4	bslbf

Le champ sponser_typ spécifie le type de classe sponsor.

Tableau 24 – Configuration de sponsor_type (ST)

Valeur	Interprétation
0000b	Indique ST à n'existe pas
0001b	Réservé
0010b	Indique que ST et à advertising model / no forced viewing
0011b	Indique que ST et à advertising model / time synchronized forced viewing
0100b	Indique que ST et à advertising model / pre / post viewing
0101b	Indique que ST est à advertising model / arbitrary time
0110b	Indique que ST est à advertising model / blanket
0111b	Indique que ST est à advertising model / other
1000b	Indique que ST est à premium model
1001b	Indique que ST est à coupon model
1010b	Indique que ST est à information disclosure model
1111b	Indique que ST est à other

5.6.10 Territory class

Cette catégorie spécifie le territoire applicable de l'autorisation, incluant le pays, la zone, le domaine et le dispositif, etc. Une condition «et» est utilisé pour spécifier une multiplicité lorsque l'autorisation est destinée à plusieurs territoires. Un territoire est l'équivalent d'un «code de région» dans un DVD vidéo.

Tableau 25 – Structure de territory class

Syntaxe	Bits	Identifiant
Territory_Class () { territory_id }	3	bslbf

Le champ «territory_id» spécifie l'identifiant du territoire.

5.6.11 Usage class

5.6.11.1 Structure

Cette classe spécifie les termes d'utilisation de l'autorisation, incluant une autorisation de diffusion large et une autorisation de diffusion en continu.

Des parties de la classe usage se chevauchent avec le contenu dans les conditions générales d'utilisation, les conditions de gestion de données et les conditions d'export de données, mentionnées ultérieurement dans la présente norme. Néanmoins, le contenu de l'autorisation spécifiée dans la classe usage est constitué de messages destinés à des utilisateurs (humains) et/ou des enregistrements de termes de contrat par implication.

Tableau 26 – Structure de usage class

Syntaxe	Bits	Identifiant
Usage_Class () {		
usage_type	3	bslbf
redistribution_type	2	bslbf
move_flag	1	bslbf
copy_flag	1	bslbf
export_flag	1	bslbf
share_flag	1	bslbf
edit_flag	1	bslbf
modify_flag	1	bslbf
super_distribution_flag	1	bslbf
reserved	7	bslbf
}		

5.6.11.2 usage_type

Ce champ spécifie le type de classe usage.

Tableau 27 – Interprétation de usage_type (UT)

Valeur	Interprétation
000b	Réservé
001b	Indique que UT est à non-fixation permission – Broadcast Permission
010b	Indique que UT est à non-fixation permission – Streaming Permission
011b	Indique que UT est à other
100b	Indique que UT est à fixation permission – Broadcast storage permission (programmed) – No reuse permission
101b	Indique que UT est à fixation permission – Broadcast storage permission (programmed) – Reuse permission
110b	Indique que UT est à fixation permission – Download permission (on demand) – No reuse permission
111b	Indique que UT est à fixation permission – Download permission (on demand) – Reuse permission

5.6.11.3 redistribution_type

Ce champ spécifie le type de classe redistribution.

Tableau 28 – Configuration de redistribution_Type

Valeur	Interprétation
00b	Réservé
01b	Indique une redistribution simultanée si le type d'utilisation est 001b, 101b Indique une diffusion en continu programmée si le type d'utilisation est 010b, 111b
10b	Indique une redistribution dans une zone si le type d'utilisation est 001b, 101b Indique une diffusion en continu à la demande si le type d'utilisation est 010b, 111b
11b	Indique une redistribution à l'extérieur d'une zone si le type d'utilisation est 001b, 101b

5.6.11.4 move_flag

Si la valeur est 1b, cela indique qu'il est autorisé de transférer le contenu. Si la valeur est 0b, cela indique qu'il n'est pas autorisé de transférer le contenu.

5.6.11.5 copy_flag

Si la valeur est 1b, cela indique qu'il est autorisé de copier (ou de reproduire) le contenu. Si la valeur est 0b, cela indique qu'il n'est pas autorisé de copier le contenu.

5.6.11.6 export_flag

Si la valeur est 1b, cela indique qu'il est autorisé d'exporter le contenu vers un support de stockage autre que celui sur lequel il est actuellement stocké. Si la valeur est 0b, cela indique qu'il n'est pas autorisé d'exporter le contenu.

5.6.11.7 share_flag

Si la valeur est 1b, cela indique qu'il est autorisé de partager le contenu entre plusieurs utilisateurs ou organismes. Si la valeur est 0b, cela indique qu'il n'est pas autorisé de partager le contenu.

5.6.11.8 edit_flag

Si la valeur est 1b, cela indique qu'il est autorisé d'éditer le contenu. Si la valeur est 0b, cela indique qu'il n'est pas autorisé d'éditer le contenu.

5.6.11.9 modify_flag

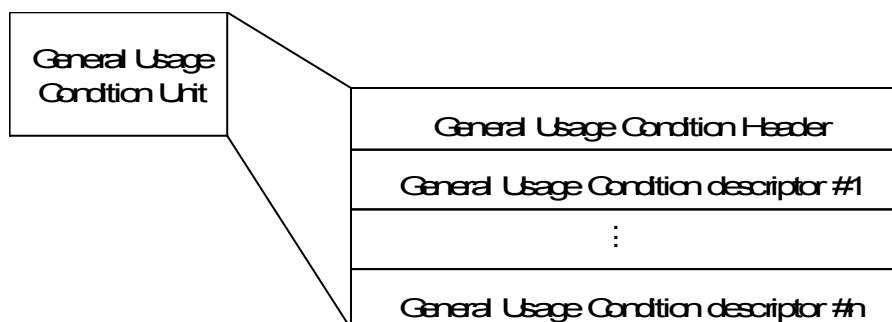
Si la valeur est 1b, cela indique qu'il est autorisé de modifier le contenu. Si la valeur est 0b, cela indique qu'il n'est pas autorisé de modifier le contenu.

5.6.11.10 super_distribution_flag

Si la valeur est 1b, cela indique qu'il est autorisé de sur-distribuer le contenu. Si la valeur est 0b, cela indique qu'il n'est pas autorisé de distribuer le contenu par l'intermédiaire d'une sur-distribution.

5.7 Unité general usage condition

5.7.1 Structure de l'unité



IEC 697/08

Légende

Anglais	Français
General Usage Condition Unit	Unité General Usage Condition
General Usage Condition Header	En-tête General Usage Condition
General Usage Condition descriptor #1	Descripteur #1 General Usage Condition
General Usage Condition descriptor #n	Descripteur #n General Usage Condition

Figure 5 – Unité general usage condition

5.7.2 En-tête des conditions générales d'utilisation

5.7.2.1 Structure

Tableau 29 – Structure d'en-tête des conditions générales d'utilisation

RBP (Position d'octet relative, en anglais «Relative Byte Position»)	Longueur en octets	Nom du champ	Contenu
0	1	General usage condition tag	TAG
1	2	Length of general usage condition descriptor(s)	uimsbf
3	1	Number of general usage condition descriptor(s)	uimsbf

5.7.2.2 General usage condition tag

Ce champ doit être mis à 0x12.

5.7.2.3 Length of general usage condition descriptor(s)

Ce champ définit la longueur en octets du ou des descripteurs de conditions générales d'utilisation.

5.7.2.4 Number of general usage condition descriptors

Ce champ définit le nombre de descripteurs de conditions générales d'utilisation qui suivent ce champ.

5.7.3 Descripteur general usage condition

5.7.3.1 Structure

Chaque descripteur general usage condition spécifie une balise de descripteur, une longueur de descripteur et des conditions d'utilisation.

Tableau 30 – Valeurs de balise de descripteurs

Valeur	Balise
0x00	Réservé
0x01	Descripteur playback usage condition
0x02	Descripteur print usage condition
0x03	Descripteur execute usage condition
0x04-0xff	Réservé

5.7.3.2 Descripteur playback usage condition

5.7.3.2.1 Structure

Tableau 31 – Structure du descripteur playback usage condition

Syntaxe	Bits	Identifiant
playback_usage_condition_descriptor() {		
descriptor_tag	8	uimsbf
descriptor_length	8	uimsbf
quality_parameter	4	uimsbf
permission_management_model_parameter	4	uimsbf
playlist_parameter	1	bslbf
playback_count_control_flag	1	bslbf
time_period_control_flag	1	bslbf
day_count_control_flag	1	bslbf
date_period_control_flag	1	bslbf
reserved	4 3	bslbf
if (playback_count_control_flag == 1b) {		
playback_count_parameter	8	uimsbf
}		
if (time_period_control_flag == 1b) {		
accumulation_flag	1	bslbf
time_period_parameter	31	uimsbf
}		
if (day_count_control_flag == 1b) {		
day_count_parameter	8	uimsbf
}		
if (date_period_control_flag == 1b) {		
start_date_parameter	40	imsbf
end_date_parameter	40	imsbf
}		
simultaneous_output_parameter	8	uimsbf
parental_guidance_parameter	8	uimsbf
usage_time_frame_parameter	16	uimsbf
}		

5.7.3.2.2 descriptor_tag

Ce champ doit être mis à 0x01.

5.7.3.2.3 descriptor_length

Ce champ définit la longueur en octets du descripteur.

5.7.3.2.4 quality_parameter

Paramètre de qualité conforme aux niveaux de qualité d'utilisation. Si plusieurs niveaux sont appliqués, indique que tous les niveaux appliqués sont autorisés. Si par exemple, à la fois LV1F et LV2F sont évalués, il est autorisé d'utiliser le contenu à la fois pour des réglages de haute qualité et standard.

Le paramètre quality est un paramètre qui contraint la qualité d'utilisation du contenu. La qualité est spécifiée à 4 niveaux. Ces niveaux comportent la haute qualité, la qualité standard, la basse qualité et une extension.

- Indicateur LEVEL1 (haute qualité) (LV1F)
Si la valeur est 1b, cela indique que l'autorisation s'applique à LEVEL1 (haute qualité). Si la valeur est 0b, cela indique qu'elle ne s'applique pas.
- Indicateur LEVEL2 (standard) (LV2F)
Si la valeur est 1b, cela indique que l'autorisation s'applique à LEVEL2 (standard). Si la valeur est 0b, cela indique qu'elle ne s'applique pas.
- Indicateur LEVEL3 (basse qualité) (LV3F)
Si la valeur est 1b, cela indique que l'autorisation s'applique à LEVEL3 (basse qualité). Si la valeur est 0b, cela indique qu'elle ne s'applique pas.
- Indicateur LEVEL4 (extension) (LV4F)
Si la valeur est 1b, cela indique que l'autorisation s'applique à LEVEL4 (extension). Si la valeur est 0b, cela indique qu'elle ne s'applique pas.

5.7.3.2.5 permission_management_model_parameter

Le paramètre permission management model est un paramètre qui limite la méthode de gestion d'autorisation du contenu. Il y a 4 modèles de gestion d'autorisation. Ces modèles sont la DRM (Gestion numérique des droits, en anglais «Digital Rights Management»), le filigrane, le rapport des droits et l'extension. Si plusieurs niveaux sont appliqués, ceci montre que tous les niveaux appliqués sont autorisés. Si par exemple à la fois DRMF (indicateur de DRM) et DWF (indicateur de filigrane numérique) sont positionnés, il est autorisé d'utiliser le contenu avec DRM ou avec un filigrane numérique.

- Indicateur de DRM (DRMF)
Si la valeur est 1b, cela indique qu'une protection par DRM est requise. Si la valeur est 0b, cela indique qu'une protection par DRM n'est pas requise.
- Indicateur de filigrane numérique (DWF)
Si la valeur est 1b, cela indique qu'une protection par filigrane numérique est requise. Si la valeur est 0b, cela indique qu'une protection par filigrane numérique n'est pas requise.
- Indicateur de rapport de droits (RRF)
Si la valeur est 1b, cela indique que le rapport de droits est requis. Si la valeur est 0b, cela indique que le rapport de droits n'est pas requis.
- Indicateur d'extension (EXTF)
Si la valeur est 1b, cela indique que l'autorisation s'applique à l'extension. Si la valeur est 0b, cela indique qu'elle ne s'applique pas.

5.7.3.2.6 **playlist_parameter**

Si la valeur est 1b, cela indique que la lecture par une liste d'écoute est autorisée. Si la valeur est 0b, la lecture par une liste d'écoute n'est pas autorisée.

NOTE La lecture par l'intermédiaire d'une liste d'écoute peut être appelée «édition de liste d'écoute». Dans «l'édition de liste d'écoute», le contenu lui-même n'est pas édité mais la séquence de lecture l'est. Faire attention à noter la différence par rapport à «l'édition de la ligne chronologique» définie en 5.9.3.11.

5.7.3.2.7 **playback_count_control_flag**

Si la valeur est 1b, cela indique que le contrôle de compte de lectures s'applique. Si la valeur est 0b, cela indique qu'il ne s'applique pas.

5.7.3.2.8 **time_period_control_flag**

Si la valeur est 1b, cela indique que le contrôle de période de temps s'applique. Si la valeur est 0b, cela indique qu'il ne s'applique pas.

NOTE Si à la fois `time_period_parameter` et `day_count_paramter` sont décrits, `time_period_parameter` est antérieur.

5.7.3.2.9 **day_count_control_flag**

Si la valeur est 1b, cela indique que le contrôle de compte de jours s'applique. Si la valeur est 0b, cela indique qu'il ne s'applique pas.

5.7.3.2.10 **date_period_control_flag**

Si la valeur est 1b, cela indique que le contrôle de période de date s'applique. Si la valeur est 0b, cela indique qu'il ne s'applique pas.

5.7.3.2.11 **playback_count_parameter**

Ce champ spécifie le nombre de fois où le contenu peut être lu.

5.7.3.2.12 **accumulation_flag**

Si la valeur est 1b, cela mesure le compte de jours et le contrôle de temps avec le temps cumulé. Si la valeur est 0b, cela mesure le compte de jours et le contrôle de temps avec le temps absolu.

5.7.3.2.13 **time_period_parameter**

Ce champ spécifie le nombre de secondes pendant lesquelles le contenu peut être lu.

5.7.3.2.14 **day_count_parameter**

Ce champ spécifie le nombre de jours pendant lesquels le contenu peut être lu.

5.7.3.2.15 **start_date_parameter**

Ce champ spécifie la date de départ à partir de laquelle le contenu peut être lu. L'unité de valeur est la seconde et la valeur «0» représente le 1er janvier, 1970.00:00:00 UTC.

5.7.3.2.16 **end_date_parameter**

Ce champ spécifie la date de fin jusqu'à laquelle le contenu peut être lu. L'unité de valeur est la seconde et la valeur «0» représente le 1er janvier, 1970.00:00:00 UTC.

5.7.3.2.17 simultaneous_output_parameter

Ce champ représente le nombre maximal d'accès simultanés au contenu. Si la valeur est 0xff, indique que l'accès simultané n'est pas limité. La valeur 0x00 est réservée pour une utilisation future.

5.7.3.2.18 parental_guidance_parameter

Ce champ représente l'assignation de guidage parental du contenu. Le guidage parental spécifie la tranche d'âge applicable dans le système d'assignation. Si la valeur est 0xff, indique que l'âge applicable n'est pas limité. La valeur 0x00 est réservée pour une utilisation future.

5.7.3.2.19 usage_time_frame_parameter

Ce champ spécifie le nombre de secondes de la trame de temps de lecture. Le dispositif de lecture détermine «un incident de lecture» lorsque le contenu est lu pendant la durée en secondes spécifiée par ce champ.

5.7.3.3 Descripteur print usage condition

5.7.3.3.1 Structure

Tableau 32 – Structure du descripteur print usage condition

Syntaxe	Bits	Identifiant
print_usage_condition_descriptor() {		
descriptor_tag	8	uimsbf
descriptor_length	8	uimsbf
quality_parameter	4	uimsbf
permission_management_model_parameter	4	uimsbf
printout_count_control_flag	1	bslbf
time_period_control_flag	1	bslbf
day_count_control_flag	1	bslbf
date_period_control_flag	1	bslbf
reserved	4	bslbf
if (printout_count_control_flag == 1b) {		
printout_count_parameter	8	uimsbf
}		
if (time_period_control_flag == 1b) {		
reserved	1	bslbf
time_period_parameter	31	uimsbf
}		
if (day_count_control_flag == 1b) {		
day_count_parameter	8	uimsbf
}		
if (date_period_control_flag == 1b) {		
start_date_parameter	40	imsbf
end_date_parameter	40	imsbf
}		
parental_guidance_parameter	8	uimsbf
}		

5.7.3.3.2 descriptor_tag

Ce champ doit être mis à ~~0x04~~ 0x02.

5.7.3.3.3 descriptor_length

Ce champ décrit la longueur en octets du descripteur.

5.7.3.3.4 quality_parameter

Paramètre de qualité conforme aux niveaux de qualité d'utilisation. Si plusieurs niveaux sont appliqués, cela indique que tous les niveaux appliqués sont autorisés. Si par exemple, à la fois LV1F et LV2F sont évalués, il est autorisé d'utiliser le contenu à la fois pour des réglages de haute qualité et standard.

Le paramètre quality est un paramètre qui contraint la qualité d'utilisation du contenu. La qualité est spécifiée à 4 niveaux. Ces niveaux comportent la haute qualité, la qualité standard, la basse qualité et une extension.

- Indicateur LEVEL1 (haute qualité) (LV1F)
Si la valeur est 1b, cela indique que l'autorisation s'applique à LEVEL1 (haute qualité). Si la valeur est 0b, cela indique qu'elle ne s'applique pas.
- Indicateur LEVEL2 (standard) (LV2F)
Si la valeur est 1b, cela indique que l'autorisation s'applique à LEVEL2 (standard). Si la valeur est 0b, cela indique qu'elle ne s'applique pas.
- Indicateur LEVEL3 (basse qualité) (LV3F)
Si la valeur est 1b, cela indique que l'autorisation s'applique à LEVEL3 (basse qualité). Si la valeur est 0b, cela indique qu'elle ne s'applique pas.
- Indicateur LEVEL4 (extension) (LV4F)
Si la valeur est 1b, cela indique que l'autorisation s'applique à LEVEL4 (extension). Si la valeur est 0b, cela indique qu'elle ne s'applique pas.

5.7.3.3.5 permission_management_model_parameter

Le paramètre permission management model est un paramètre qui limite la méthode de gestion d'autorisation du contenu. Il y a 4 modèles de gestion d'autorisation. Ces modèles sont la DRM (Gestion numérique des droits, en anglais «Digital Rights Management»), le filigrane numérique, le rapport des droits et l'extension. Si plusieurs niveaux sont appliqués, ceci montre que tous les niveaux appliqués sont autorisés. Si par exemple à la fois DRMF (indicateur de DRM) et DWF (indicateur de filigrane numérique) sont positionnés, il est autorisé d'utiliser le contenu avec DRM ou avec filigrane numérique.

- Indicateur de DRM (DRMF)
Si la valeur est 1b, cela indique qu'une protection par DRM est requise. Si la valeur est 0b, cela indique qu'une protection par DRM n'est pas requise.
- Indicateur de filigrane numérique (DWF)
Si la valeur est 1b, cela indique qu'une protection par filigrane numérique est requise. Si la valeur est 0b, cela indique qu'une protection par filigrane numérique n'est pas requise.
- Indicateur de rapport de droits (RRF)
Si la valeur est 1b, cela indique que le rapport de droits est requis. Si la valeur est 0b, cela indique que le rapport de droits n'est pas requis.
- Indicateur d'extension (EXTF)
Si la valeur est 1b, cela indique que l'autorisation s'applique à l'extension. Si la valeur est 0b, cela indique qu'elle ne s'applique pas.

5.7.3.3.6 printout_count_control_flag

Si la valeur est 1b, cela indique que le contrôle de compte d'impressions s'applique. Si la valeur est 0b, cela indique qu'elle ne s'applique pas.

5.7.3.3.7 time_period_control_flag

Si la valeur est 1b, cela indique que le contrôle de période de temps s'applique. Si la valeur est 0b, cela indique qu'il ne s'applique pas.

NOTE Si à la fois time_period_parameter et day_count_paramter sont décrits, time_period_parameter est antérieur.

5.7.3.3.8 day_count_control_flag

Si la valeur est 1b, cela indique que le contrôle de période de jour s'applique. Si la valeur est 0b, cela indique qu'il ne s'applique pas.

5.7.3.3.9 date_period_control_flag

Si la valeur est 1b, cela indique que le contrôle de période de date s'applique. Si la valeur est 0b, cela indique qu'il ne s'applique pas.

5.7.3.3.10 printout_count_parameter

Ce champ spécifie le nombre de fois où le contenu peut être imprimé.

5.7.3.3.11 time_period_parameter

Ce champ spécifie le nombre de secondes pendant lesquelles le contenu peut être imprimé.

5.7.3.3.12 day_count_parameter

Ce champ spécifie le nombre de jours pendant lesquels le contenu peut être imprimé.

5.7.3.3.13 start_date_parameter

Ce champ spécifie la date de départ à partir de laquelle le contenu peut être imprimé. L'unité de valeur est la seconde et la valeur «0» représente le 1er janvier, 1970.00:00:00 UTC.

5.7.3.3.14 end_date_parameter

Ce champ spécifie la date de fin jusqu'à laquelle le contenu peut être imprimé. L'unité de valeur est la seconde et la valeur «0» représente le 1er janvier, 1970.00:00:00 UTC.

5.7.3.3.15 parental_guidance_parameter

Ce champ spécifie l'assignation de guidage parental du contenu. L'assignation de guidage parental spécifie la tranche d'âge applicable du contenu par l'intermédiaire d'un système d'assignation. Si la valeur est 0x00, indique que le paramètre est réservé. Si la valeur est 0xff, indique que le contenu est applicable à tous les âges.

5.7.3.4 Descripteur execute usage condition

5.7.3.4.1 Structure

Tableau 33 – Structure du descripteur execute usage condition

Syntaxe	Bits	Identifiant
execute_usage_condition_descriptor() {		
descriptor_tag	8	uimsbf
descriptor_length	8	uimsbf
service_level_parameter	4	uimsbf
permission_management_model_parameter	4	uimsbf
execution_count_period_control_flag	1	bslbf
time_period_control_flag	1	bslbf
day_count_control_flag	1	bslbf
date_period_control_flag	1	bslbf
reserved	4	bslbf
if (execution_count_control_flag == 1b) {		
execution_count_parameter	8	uimsbf
}		
if (time_period_control_flag == 1b) {		
accumulation_flag	1	bslbf
reserved	7	bslbf
time_period_parameter	8	uimsbf
}		
if (day_count_control_flag == 1b) {		
day_count_parameter	8	uimsbf
}		
if (date_period_control_flag == 1b) {		
start_date_parameter	40	imsbf
end_date_parameter	40	imsbf
}		
parental_guidance_parameter	8	uimsbf
usage_time_frame_parameter	16	uimsbf
}		

5.7.3.4.2 descriptor_tag

Ce champ doit être mis à ~~0x02~~ 0x03.

5.7.3.4.3 descriptor_length

Ce champ définit la longueur en octets du descripteur.

5.7.3.4.4 service_level_parameter

Le paramètre service level est un paramètre qui contraint le niveau des fonctions desservies par le contenu. Il est spécifié à 4 niveaux. Ces niveaux comportent le contrôle complet, standard, d'essai et d'extension.

Si plusieurs niveaux sont appliqués, indique que tous les niveaux appliqués sont autorisés. Si par exemple, à la fois LV1F et LV2F sont évalués, il est autorisé d'utiliser le contenu à la fois pour des réglages de haute qualité et standard.

- Indicateur LEVEL1 (contrôle complet) (LV1F)
Si la valeur est 1b, cela indique que l'autorisation s'applique à LEVEL1 (contrôle complet). Si la valeur est 0b, cela indique qu'elle ne s'applique pas.
- Indicateur LEVEL2 (standard) (LV2F)
Si la valeur est 1b, cela indique que l'autorisation s'applique à LEVEL2 (standard). Si la valeur est 0b, cela indique qu'elle ne s'applique pas.
- Indicateur LEVEL3 (essai) (LV3F)
Si la valeur est 1b, cela indique que l'autorisation s'applique à LEVEL3 (essai). Si la valeur est 0b, cela indique qu'elle ne s'applique pas.
- Indicateur LEVEL4 (extension) (LV4F)
Si la valeur est 1b, cela indique que l'autorisation s'applique à LEVEL4 (extension). Si la valeur est 0b, cela indique qu'elle ne s'applique pas.

5.7.3.4.5 permission_management_model_parameter

Le paramètre permission management model est un paramètre qui contraint la méthode de gestion d'autorisation du contenu. Il y a 4 modèles de gestion d'autorisation. Ces modèles sont sous la gestion DRM (Gestion numérique des droits, en anglais «Digital Rights Management»), le filigrane numérique, le rapport des droits et l'extension. Si plusieurs niveaux sont appliqués, cela indique que tous les niveaux appliqués sont autorisés. Si par exemple LV1F et LV2F sont tous deux positionnés, il est autorisé d'utiliser le contenu sous la gestion de la DRM ou du filigrane numérique ou des deux.

- Indicateur de DRM (DRMF)
Si la valeur est 1b, cela indique que la protection par DRM est requise. Si la valeur est 0b, cela indique que la protection par DRM n'est pas requise.
- Indicateur de filigrane numérique (DWF)
Si la valeur est 1b, cela indique que la protection par filigrane numérique est requise. Si la valeur est 0b, cela indique que la protection par filigrane numérique n'est pas requise.
- Indicateur de rapport de droits (RRF)
Si la valeur est 1b, cela indique que le rapport de droits est requis. Si la valeur est 0b, cela indique que le rapport de droits n'est pas requis.
- Indicateur d'extension (EXTF)
Si la valeur est 1b, cela indique que l'autorisation s'applique à l'extension. Si la valeur est 0b, cela indique qu'elle ne s'applique pas.

5.7.3.4.6 execution_count_control_flag

Si la valeur est 1b, cela indique que le contrôle de compte d'exécutions s'applique. Si la valeur est 0b, cela indique qu'il ne s'applique pas.

5.7.3.4.7 time_period_control_flag

Si la valeur est 1b, cela indique que le contrôle de période de temps s'applique. Si la valeur est 0b, cela indique qu'il ne s'applique pas.

NOTE Si à la fois time_period_parameter et day_count_paramter sont décrits, time_period_parameter est antérieur.

5.7.3.4.8 day_count_control_flag

Si la valeur est 1b, cela indique que le contrôle de compte de jours s'applique. Si la valeur est 0b, cela indique qu'il ne s'applique pas.

5.7.3.4.9 date_period_control_flag

Si la valeur est 1b, cela indique que le contrôle de période de date s'applique. Si la valeur est 0b, cela indique qu'il ne s'applique pas.

5.7.3.4.10 execution_count_parameter

Ce champ spécifie le nombre de fois où le contenu peut être exécuté.

5.7.3.4.11 accumulation_flag

Si la valeur est 1b, cela mesure le compte de jours et le contrôle de temps avec le temps cumulé. Si la valeur est 0b, cela mesure le compte de jours et le contrôle de temps avec le temps absolu.

5.7.3.4.12 time_period_parameter

Ce champ définit le nombre d'heures pendant lesquelles le récepteur d'autorisation est autorisé à exécuter le contenu.

5.7.3.4.13 day_count_control_parameter

Ce champ définit le nombre de jours pendant lesquels le récepteur d'autorisation est autorisé à exécuter le contenu.

5.7.3.4.14 start_date_parameter

Ce champ spécifie la date de départ à partir de laquelle le contenu peut être exécuté. L'unité de valeur est la seconde et la valeur «0» représente le 1er janvier, 1970.00:00:00 UTC.

5.7.3.4.15 end_date_parameter

Ce champ spécifie la date de fin jusqu'à laquelle le contenu peut être exécuté. L'unité de valeur est la seconde et la valeur «0» représente le 1er janvier, 1970.00:00:00 UTC.

5.7.3.4.16 parental_guidance_parameter

Ce champ spécifie l'assignation de guidage parental du contenu. L'assignation de guidage parental spécifie la tranche d'âge applicable du contenu par l'intermédiaire d'un système d'assignation. Si la valeur est 0x00, indique que le paramètre est réservé. Si la valeur est 0xff, indique que le contenu est applicable à tous les âges.

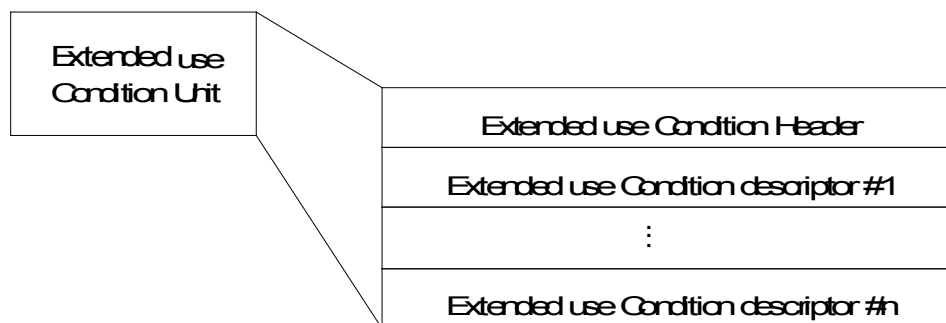
5.7.3.4.17 usage_time_frame_parameter

Ce champ spécifie le nombre de secondes de la trame de temps d'exécution. Le dispositif d'exécution détermine un incident d'exécution lorsque le contenu est exécuté pendant la durée en secondes spécifiée par ce champ.

5.8 Unité extended use condition

~~Cette unité doit être réservée pour une normalisation future.~~

5.8.1 Structure de l'unité



IEC 2183/12

Légende

Anglais	Français
Extended use condition unit	Unité <i>extended use condition</i>
Extended use condition header	En-tête <i>extended use condition</i>
Extended use condition descriptor	Descripteur <i>extended use condition</i> #1
Extended use condition descriptor	Descripteur <i>extended use condition</i> #n

Figure 8 – Unité *extended use condition*

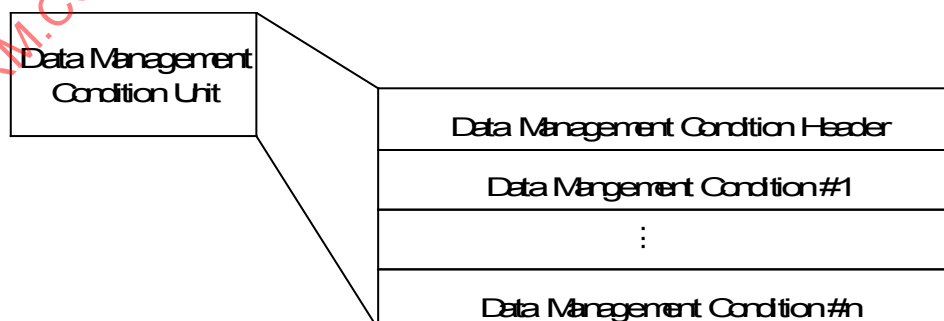
5.8.2 En-tête *extended use condition*

Tableau 46 – Structure de l'en-tête *extended use condition*

RBP	Longueur en octets	Nom du champ	Contenu
0	1	Extended use condition tag	TAG
1	2	Length of extended use condition(s)	uimsbf
3	1	Number of extended use condition descriptors	uimsbf

5.9 Unité data management condition

5.9.1 Structure de l'unité



IEC 698/08

Légende

Anglais	Français
Data Management Condition Unit	Unité Data Management Condition
Data Management Condition Header	En-tête Data Management Condition
Data Management Condition #1	Contition #1 Data Management Condition
Data Management Condition #n	Contition #n Data Management Condition

Figure 6 – Unité data management condition

En ce qui concerne les conditions de gestion de données, il existe des instances dans lesquelles les conditions détaillées changent, sur la base du dispositif ou de l'utilisateur, gérant les données. Par exemple, la copie peut être autorisée jusqu'à 5 fois pour un dispositif situé dans le domaine, tandis que la copie n'est autorisée qu'une seule fois pour des dispositifs extérieurs au domaine.

Pour exprimer ceci, l'unité data management condition possède un en-tête et la condition de gestion de données #n qui correspond aux identifiants de récepteur respectifs soumis aux termes respectifs.

5.9.2 En-tête de condition de gestion des données**5.9.2.1 Structure****Tableau 34 – Structure de l'en-tête de conditions de gestion de données**

RBP (Position d'octet relative, en anglais «Relative Byte Position»)	Longueur en octets	Nom du champ	Contenu
0	1	Data management condition tag	TAG
1	2	Length of data management condition(s)	uimsbf
3	1	Number of data management conditions	uimsbf

5.9.2.2 Data management condition tag

Ce champ doit être mis à 0x14.

5.9.2.3 Length of data management condition(s)

Ce champ spécifie la longueur en octets de la ou des conditions de gestion de données.

5.9.2.4 Number of data management conditions

Ce champ spécifie le nombre de conditions de gestion de données suivant ce champ.

5.9.3 Data management condition

5.9.3.1 Structure

Tableau 35 – Structure de data management condition

RBP (Position d'octet relative, en anglais «Relative Byte Position»)	Longueur en octets	Nom du champ	Contenu
0	16	Data management target identifier	bslbf
16	1	Encryption flag	bslbf
17	1	Copy count	uimsbf
18	1	Move count	uimsbf
19	4	Transcode type	bslbf
23	4	Maximum transcode rate	uimsbf
27	4	Minimum transcode rate	uimsbf
31	5	Expiration date	uimsbf
36	1	Sublicense count	uimsbf
37	1	Time-line edit	uimsbf

5.9.3.2 Identifiant data management target

Ce champ représente l'identifiant cible à gérer. Il a la même structure que celle de l'identifiant de récepteur.

Chaque condition de gestion de données #n applique les conditions suivantes au dispositif, à l'utilisateur, à l'organisme, au domaine, etc., appartenant à l'identifiant spécifié dans ce champ.

5.9.3.3 encryption_flag

Tableau 36 – Structure d'encryption flag (EF)

bit7	bit0
Reserved	EF

Légende

Anglais	Français
Reserved	Réservé

Si la valeur de TF est 1b, cela indique qu'un chiffrement est nécessaire. Si la valeur est 0b, cela indique qu'un chiffrement n'est pas nécessaire.

5.9.3.4 Copy count

Ce champ spécifie le nombre de fois où le contenu peut être copié.

5.9.3.5 Move count

Ce champ spécifie le nombre de fois où le contenu peut être transféré.

5.9.3.6 Transcode type

Ce champ spécifie le type de transcodage.

Tableau 37 – Interprétation de transcode type

Position des bits	Interprétation
0	Indique que transcode type est à not limited
1	Indique que transcode type est à MPEG-1
2	Indique que transcode type est à MPEG-2
3	Indique que transcode type est à NTSC
4	Indique que transcode type est à H.264
5	Indique que transcode type est à JPEG
6	Indique que transcode type est à GIF
7	Indique que transcode type est à PNG
8	Indique que transcode type est à linear PCM
9	Indique que transcode type est à AAC
10	Indique que transcode type est à MP3
11-30	Réservé
31	Indique que transcode type est à original encoding type (le contenu ne doit jamais être transcodé).

5.9.3.7 Maximum transcode rate

Ce champ spécifie la vitesse du transcodage en kb/s. La valeur 0xffffffff signifie que la vitesse de transcodage maximale n'est pas limitée.

5.9.3.8 Minimum transcode rate

Ce champ spécifie la vitesse du transcodage en kb/s. La valeur 0x00000000 signifie que la vitesse de transcodage minimale n'est pas limitée.

5.9.3.9 Expiration date

Ce champ spécifie la date d'expiration à gérer.

Si la valeur indique "not specified", elle doit alors être 0xffffffff.

5.9.3.10 Sublicense count

Ce champ spécifie le nombre de licences secondaires pouvant être délivrées. Si la valeur est 0x00, cela indique que la fourniture de licences secondaires n'est pas autorisée. Si la valeur est 0xff, cela indique que le nombre de licences secondaires est illimité.

5.9.3.11 Time-line edit

Tableau 38 – Structure de l'indicateur time-line (TF)



Légende

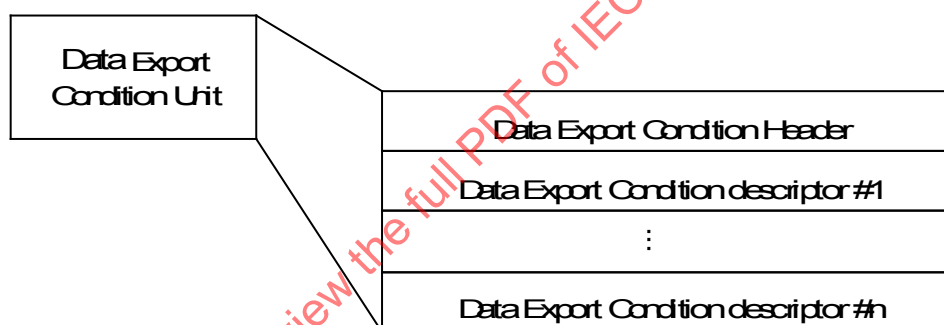
Anglais	Français
Reserved	Réservé

Si la valeur de TF est 1b, cela indique que l'édition du contenu d'origine par rapport à une ligne chronologique et la sauvegarde du contenu résultant sont autorisées. Si la valeur est 0b, cela n'est pas autorisé.

NOTE «Time-line edit» ici défini consiste à éditer la totalité du contenu. Faire attention à la différence par rapport à l'édition d'une liste d'écoute qui est la «lecture éditée d'une ligne chronologique». Voir 5.7.3.2.6.

5.10 Unité data export condition

5.10.1 Structure de l'unité



IEC 699/08

Légende

Anglais	Français
Data Export Condition Unit	Unité Data Export Condition
Data Export Condition Header	En-tête Data Export Condition
Data Export Condition descriptor #1	Descripteur #1 Data Export Condition
Data Export Condition descriptor #n	Descripteur #n Data Export Condition

Figure 7 – Unité data export condition

5.10.2 En-tête de condition d'export des données

5.10.2.1 Structure

Tableau 39 – Structure de l'en-tête de condition d'export de données

RBP (Position d'octet relative, en anglais «Relative Byte Position»)	Longueur en octets	Nom du champ	Contenu
0	1	Data export condition tag	TAG
1	2	Length of data export condition(s)	uimsbf
3	1	Number of data export condition descriptors	uimsbf

5.10.2.2 Data export condition tag

Ce champ doit être mis à 0x15.

5.10.2.3 Length of data export condition(s)

Ce champ spécifie la longueur en octets de la ou des conditions d'export de données.

5.10.2.4 Number of data export condition descriptors

Ce champ définit le nombre de descripteurs data export condition faisant suite à ce champ.

5.10.3 Descripteur data export condition

Le descripteur data export condition spécifie une balise de descripteur, une longueur de descripteur et des conditions d'export.

Tableau 40 – Valeurs de balise de descripteurs

Valeur	Balise
0x00	Réservé
0x01	Descripteur general export
0x02-0xFF	Reserved

5.10.4 Descripteur general export

5.10.4.1 Structure

Tableau 41 – Structure du descripteur general export

Syntaxe	Bits	Identifiant
general_export_descriptor() {		
descriptor_tag	8	uimsbf
descriptor_length	8	uimsbf
storage_media_type	32	bslbf
encoding_type	32	bslbf
protection_type	32	bslbfbslbf
control_type	8	bslbf
move_indicate_flag	1	bslbf
time_period_control_flag	1	bslbf
day_count_control_flag	1	bslbf
date_period_control_flag	1	bslbf
reserved	4	bslbf
if (move_indecate_flag == 0b){		
export_count_parmameter	8	uimsbf
}		
if (time_period_control_flag == 1b) {		
reserved	1	bslbf
time_period_parameter	31	uimsbf
}		
if (day_count_control_flag == 1b) {		
day_count_parameter	8	uimsbf
}		
if (date_period_control_flag == 1b) {		
start_date_parameter	40	imsbf
end_date_parameter	40	imsbf
}		
}		

5.10.4.2 descriptor_tag

Ce champ doit être mis à 0x01.

5.10.4.3 descriptor_length

Ce champ décrit la longueur en octets du descripteur.

5.10.4.4 storage_media_type

Ce champ représente le type autorisé de support de stockage vers lequel le contenu peut être exporté.

Tableau 42 – Interprétation de storage_media_type (SMT)

Position des bits	Interprétation
0	Indique que SMT est à not limited
1	Indique que SMT est à CD
2	Indique que SMT est à DVD
3	Indique que SMT est à HDD
4	Indique que SMT est à flash memory
5	Indique que SMT et à HD-quality opticval disc
6-31	Réservé

5.10.4.5 encoding_type

Ce champ spécifie le type de codage avec lequel le contenu doit être exporté.

Tableau 43 – Interprétation d'encoding_type (ET)

Position des bits	Interprétation
0	Indique qu'ET n'est pas limité
1	Indique qu'ET est à MPEG-1
2	Indique qu'ET est à MPEG-2
3	Indique qu'ET est à NTSC
4	Indique qu'ET est à H.264
5	Indique qu'ET est à JPEG
6	Indique qu'ET est à GIF
7	Indique qu'ET est à PNG
8	Indique qu'ET est à MIC linéaire
9	Indique qu'ET est à AAC
10	Indique qu'ET est à MP3
11-30	Réservé
31	Indique qu'ET est au type de codage d'origine (Le contenu doit être exporté avec le même type de codage que le contenu d'origine. En d'autres termes, le contenu n'est pas transcodé.)

5.10.4.6 protection_type

Ce champ représente le type de protection autorisé selon lequel le contenu doit être exporté.

Tableau 44 – Interprétation de protection_type (PT)

Position des bits	Interprétation
0	Indique que PT est à no protection (Aucune protection de contenu n'est requise.)
1	Indique que PT est à CPRM
2	Indique que PT est à DTCP
3	Indique que PT est à HDCP
4	Indique que PT est à analog copy control
5	Indique que PT est à CGMS
6	Indique que PT est à SAFIA
7	Indique que PT est à AACS
8	Indique que PT est à VCPS
9-31	Réservé

5.10.4.7 control_type

Ce champ représente le contrôle de protection autorisé selon lequel le contenu doit être exporté.

Tableau 45 – Interprétation de control_type (CT)

Valeur	Interprétation
0x00	Indique que CT est à not specified
0x01-0x0F	Réservé
0x11	Indique que CT est à copy never
0x12	Indique que CT est à copy no more
0x13	Indique que CT est à copy once
0x14-0xFF	Réservé

5.10.4.8 move_indicate_flag

Si la valeur est 1b, cela indique que l'export signifie un transfert. Si la valeur est 0b, cela indique que l'export signifie une copie.

5.10.4.9 time_period_control_flag

Si la valeur est 1b, cela indique que le contrôle de période de temps s'applique. Si la valeur est 0b, cela indique qu'il ne s'applique pas.

NOTE Si à la fois time_period_parameter et day_count_paramter sont décrits, time_period_parameter est antérieur.

5.10.4.10 day_count_control_flag

Si la valeur est 1b, cela indique que le contrôle de compte de jours s'applique. Si la valeur est 0b, cela indique qu'il ne s'applique pas.

5.10.4.11 date_period_control_flag

Si la valeur est 1b, cela indique que le contrôle de période de date s'applique. Si la valeur est 0b, cela indique qu'il ne s'applique pas.

5.10.4.12 export_count_parameter

Ce champ spécifie le nombre de fois où le contenu peut être exporté. Si la valeur est 0xff, cela indique que count_period_parameter est illimité.

5.10.4.13 time_period_parameter

Ce champ spécifie le nombre de secondes pendant lesquelles le contenu peut être exporté.

5.10.4.14 day_count_parameter

Ce champ spécifie le nombre jours pendant lesquels le contenu peut être exporté.

5.10.4.15 start_date_parameter

Ce champ spécifie la date de départ à partir de laquelle le contenu peut être exporté. L'unité de valeur est la seconde et la valeur «0» représente le 1er janvier, 1970.00:00:00 UTC.

5.10.4.16 end_date_parameter

Ce champ spécifie la date de fin jusqu'à laquelle le contenu peut être exporté. L'unité de valeur est la seconde et la valeur «0» représente le 1er janvier, 1970.00:00:00 UTC.

Annexe A **(informative)**

Exigences du code d'autorisation pour les serveurs résidentiels et les dispositifs de lecture

A.1 Gestion des codes d'autorisation dans le serveur résidentiel et le dispositif client

Le serveur résidentiel et le dispositif client sont des récepteurs de l'autorisation du détenteur de droits de contenu. Un code d'autorisation est constitué du contenu vendu/distribué et de son autorisation.

Ce qui suit est un ensemble d'exigences de la gestion des codes d'autorisation dans des serveurs résidentiels et des dispositifs clients.

- a) Lorsqu'un serveur résidentiel ou un dispositif client achète des droits d'accès à un contenu, le code d'autorisation doit définitivement atteindre le serveur résidentiel ou le dispositif client sans modification par une tierce partie.
- b) Un code d'autorisation ayant atteint un serveur résidentiel ou un dispositif client doit être conservé à l'intérieur du support avec les droits d'accès jusqu'à ce qu'ils soient détruits par l'utilisateur, invalidés ou perdus en raison d'une destruction du support sur lequel ils résident, etc. En même temps, le contenu du code d'autorisation ne doit jamais être modifié pendant sa possession.
- c) Le serveur résidentiel et le dispositif client doivent être capables de restituer (afficher, imprimer) le contenu conformément au contenu du contrat spécifié dans le code d'autorisation.

Le niveau de sécurité dépend de la mise en œuvre.

Ce qui suit constitue les exigences minimales de mise en œuvre.

- d) Le code d'autorisation doit être incorporé dans la licence et distribué avec la licence.
- e) Le module de mise en œuvre de DRM (Gestion numérique des droits, en anglais «Digital Rights Management») doit comporter une interface permettant aux utilisateurs de référencer en toute sécurité les détails d'autorisation spécifiés par les valeurs dans le code d'autorisation de la licence.
- f) Définir la terminologie exprimant les détails du contrat correspondant à chaque valeur dans le code d'autorisation. Afficher la terminologie définie lors de la présentation des détails du contrat aux utilisateurs.

De plus, ce qui suit est une exigence facultative.

- g) Recueillir des informations permettant de comprendre le niveau d'adhésion au contrat exprimé dans l'autorisation lorsqu'on accède au contenu dans le serveur résidentiel et le dispositif client. Élaborer un système capable d'envoyer ces informations au serveur de licence ou au serveur de gestion d'autorisation comme nécessaire.

A.2 Exemples de gestion de contenu et de codes d'autorisation avec des identifiants de domaine

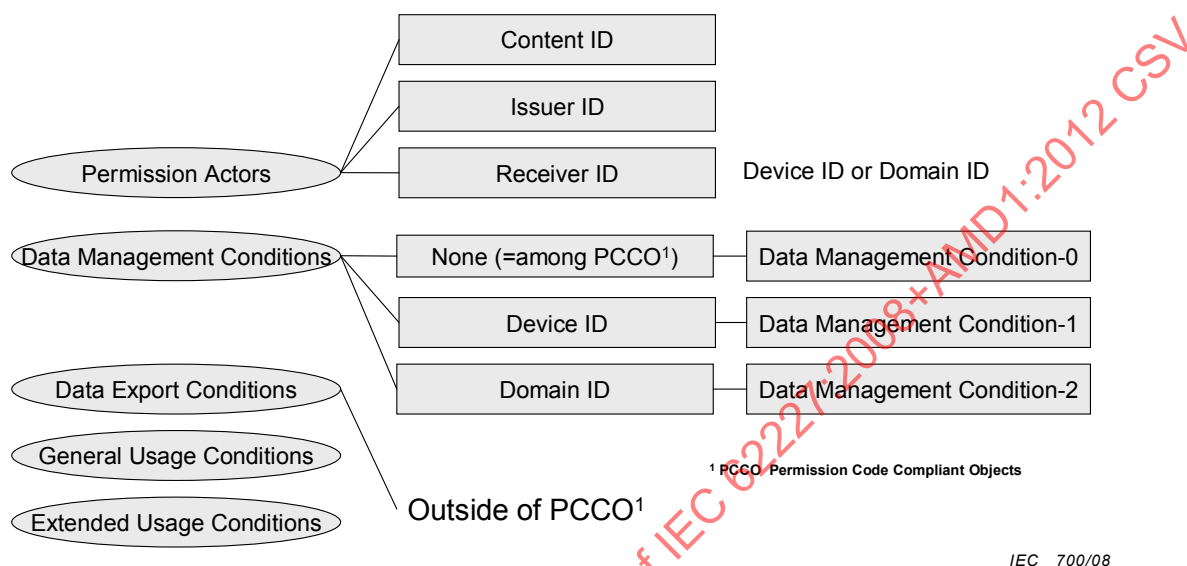
A.2.1 Généralités

Ce paragraphe donne des exemples illustrant la manière dont des dispositifs doivent gérer un contenu et des codes d'autorisation incluant des identifiants de domaine.

A.2.2 Spécification d'identifiants de domaine dans un code d'autorisation

A.2.2.1 Façon dont les domaines apparaissent dans un code d'autorisation

Les domaines apparaissent sous la forme d'identifiants de récepteur et/ou conditions de gestion de données dans des codes d'autorisation comme spécifié dans la présente norme, voir Figure A.1.



Légende

Anglais	Français
Permission Actors	Acteurs d'autorisation
Data Management Conditions	Conditions de gestion de données
Data Export Conditions	Conditions d'export de données
General usage Conditions	Conditions générales d'utilisation
Extended Usage Conditions	Conditions d'utilisation étendues
Content ID	Identifiant de contenu
Issuer ID	Identifiant d'émetteur
Receiver ID	Identifiant de récepteur
None (=among PCCO¹)	Aucun (= parmi PCCO¹)
Device ID	Identifiant de
Domain ID	Identifiant de
Device ID or Domain ID	Identifiant de Identifiant de
Data Management Condition-0	Condition de gestion de données-0
Data Management Condition-1	Condition de gestion de données-1
Data Management Condition-2	Condition de gestion de données-2
Outside of PCCO¹	Extérieur de PCCO¹
PCCO¹ Permission Code Compliant Objects	PCCO¹ Objets conformes au code d'autorisation

Figure A.1 – Code d'autorisation et domaine

A.2.2.2 Lorsqu'un identifiant de domaine est spécifié comme identifiant de récepteur

Lorsqu'un identifiant de domaine est spécifié comme identifiant de récepteur, une autorisation spécifiée dans les conditions générales d'utilisation, les conditions étendues d'utilisation et les conditions d'export de données, est appliquée aux dispositifs et aux supports de stockage

appartenant au domaine. Le dispositif recevant ce code d'autorisation est donc capable de redistribuer la même autorisation à d'autres dispositifs et supports de stockage appartenant à ce domaine.

On suppose que certains mécanismes de prévention sont en place par l'intermédiaire de la gestion des clés de domaine, etc. Ces mécanismes de prévention peuvent empêcher les dispositifs n'appartenant pas au domaine d'usurper l'identifiant de domaine ou empêcher ces dispositifs d'utiliser le contenu même dans le cas peu probable où une licence est reçue après avoir réussi à usurper l'identifiant de domaine.

Dans le cas où le même domaine est également spécifié dans la condition de gestion de données, les conditions de gestion de données ont priorité sur l'identifiant du récepteur.

A.2.2.3 Lorsqu'un identifiant de domaine est spécifié dans les conditions de gestion de données

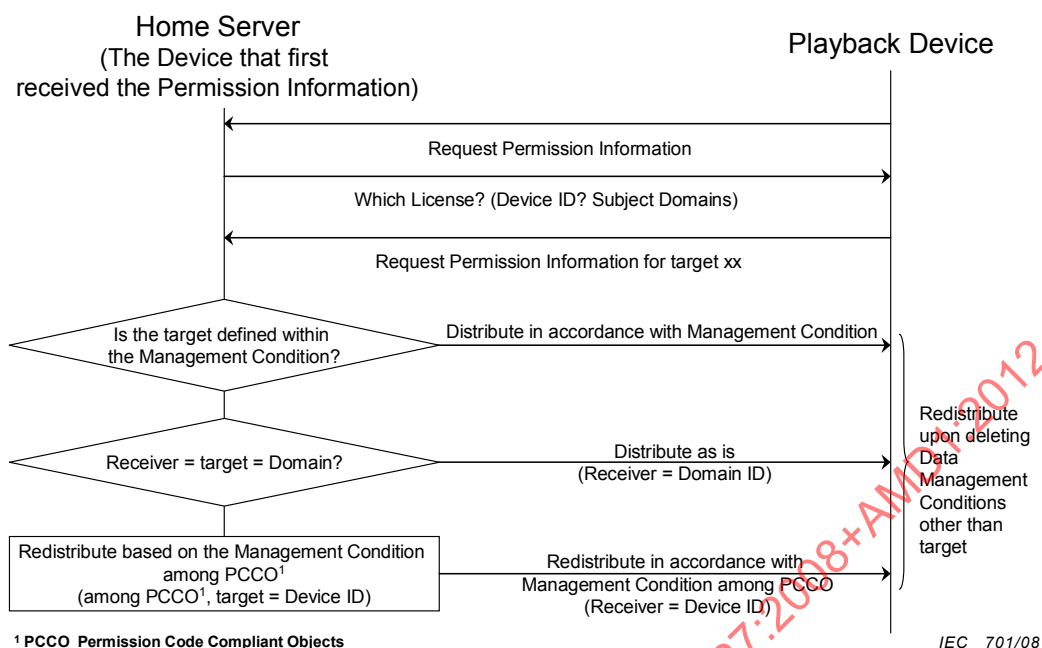
Lorsqu'un identifiant de domaine est spécifié dans les conditions de gestion de données, les conditions sont interprétées comme des règles d'exception ou priorité.

Les conditions générales d'utilisation, les conditions étendues d'utilisation et les conditions d'export de données sont considérées comme des autorisations destinées au dispositif ou au support de stockage ayant reçu le contenu en premier.

A.2.3 Organigramme de la redistribution des informations d'autorisation

La Figure A.2 est un diagramme de la redistribution des informations d'autorisation.

IECNORM.COM : Click to view the full PDF of IEC 62227-2008+A1:2012 CSV



Légende

Anglais	Français
Home Server (The Device that first received the Permission Information)	Serveur résidentiel (Dispositif ayant reçu en premier les informations d'autorisation)
Playback Device	Dispositif de lecture
Request Permission Information	Demande d'informations d'autorisation
Which License? (Device ID? Subject Domains)	Quelle licence? (Identifiant du dispositif ? Domaines sujets)
Request Permission Information for target xx	Demandes d'informations d'autorisation pour la cible xx
Is the target defined within the Management Condition?	La cible est-elle définie dans les conditions de gestion ?
Distribute in accordance with Management Condition	Distribution en conformité avec la condition de gestion
Receiver = target = Domain?	Récepteur = cible = domaine?
Distribute as is (Receiver = Domain ID)	Distribution tel quel (Récepteur = Identifiant de domaine)
Redistribute based on the Management Condition among PCCO¹ (among PCCO¹, target = Device ID)	Redistribution basée sur la condition de gestion parmi les PCCO¹ (parmi les PCCO¹, cible = identifiant de dispositif)
Distribute in accordance with Management Condition among PCCO¹ (Receiver = Device ID)	Distribution en conformité avec la condition de gestion parmi les PCCO¹ (Récepteur = identifiant de dispositif)
Redistribute upon deleting Management Conditions other than target	Redistribution lors de la suppression des conditions de gestion autres que la cible
PCCO¹ Permission Code Compliant Objects	PCCO¹ Objets conformes au code d'autorisation

Figure A.2 – Redistribution des informations d'autorisation

Ce qui suit s'applique à l'organigramme des informations d'autorisation.

- a) Dispositif b, le dispositif demandant la redistribution du code d'autorisation effectuée la requête avec le dispositif a, premier dispositif ayant reçu les informations d'autorisation. Le dispositif b spécifie l'identifiant de dispositif, l'identifiant de support de stockage ou l'identifiant de domaine; l'acteur faisant l'objet de la redistribution d'autorisation.
- b) Si les conditions de gestion du code d'autorisation contiennent un identifiant spécifique, le dispositif a redistribué le code d'autorisation à l'identifiant de récepteur spécifié conformément à la condition de gestion.
- c) Si l'identifiant du premier récepteur du code d'autorisation et l'identifiant spécifié comme objet de la redistribution sont tous deux le même identifiant de domaine, le code d'autorisation est redistribué avec l'identifiant de domaine laissé intact dans l'identifiant de récepteur.
- d) Si aucun des cas ci-dessus ne s'applique, le code d'autorisation est redistribué avec l'identifiant de récepteur comme identifiant spécifié conformément aux conditions de gestion imposées aux dispositifs parmi les objets conformes au code d'autorisation.

Noter que lorsque les codes d'autorisation sont redistribués, les conditions de gestion de données qui concernent les acteurs autres que l'identifiant spécifié comme identifiant de récepteur sont effacées avant redistribution.

A.2.4 Restrictions concernant les comptes

Lors de la redistribution des codes d'autorisation, il convient de prendre soin à ce qui suit lorsque des restrictions concernant les comptes sont impliquées:

- Restrictions sur le compte de copies dans les conditions de gestion de données;
- Restrictions sur le compte d'exports dans les conditions d'export de données;
- Restrictions sur le compte d'utilisations dans les conditions générales d'utilisation.

En ce qui concerne les restrictions des comptes, ce qui suit doit être vrai.

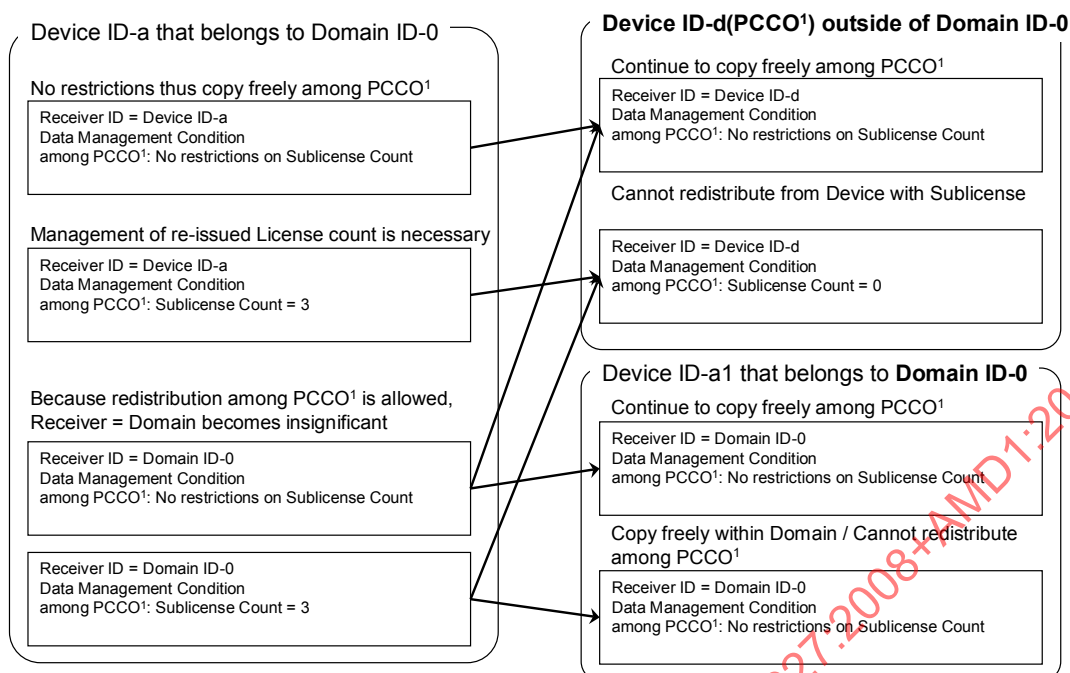
(Compte spécifié dans le code d'autorisation reçu en premier.)

=(compte restant sur le premier dispositif ayant reçu le code d'autorisation)

+(compte spécifié sur le code d'autorisation à redistribuer)

Les codes d'autorisation suivants avec les restrictions de comptes peuvent être redistribués lorsque ce processus est géré en mettant à zéro le compte de licences secondaires spécifié dans le code d'autorisation.

L'exemple ci-dessous illustre les restrictions du compte de copies dans les conditions de gestion de données.



¹ PCCO: Permission Code Compliant Objects

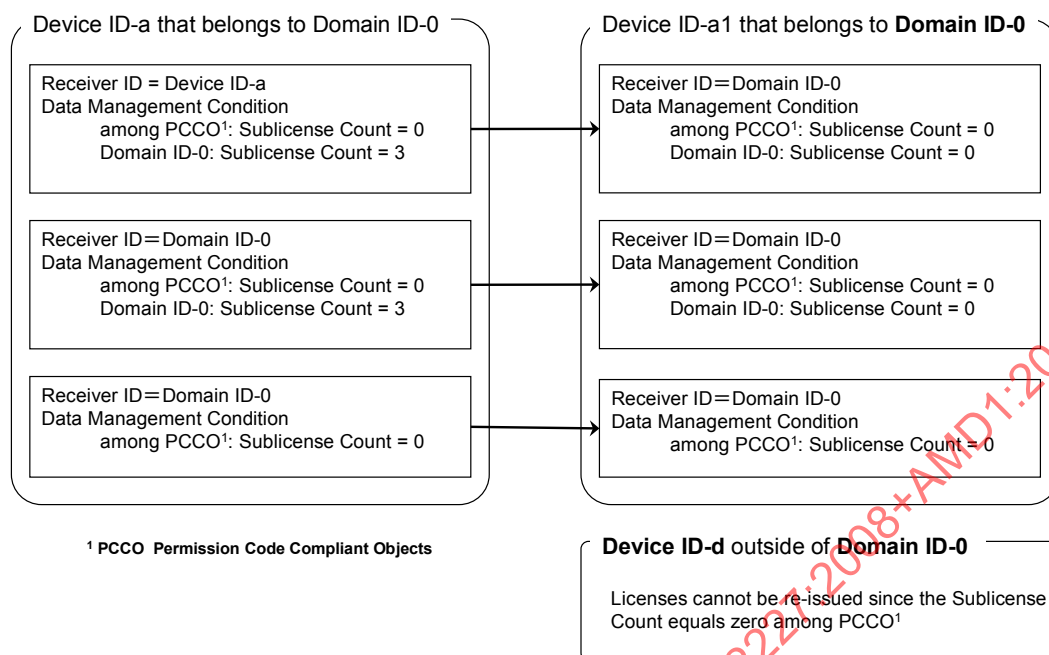
IEC 702/08

Légende

Anglais	Français
Device ID-a that belongs to Domain ID-0	Identifiant de dispositif a appartenant à l'identifiant de domaine-0
No restrictions thus copy freely among PCCO¹	Pas de restrictions, donc copie libre parmi les PCCO¹
Receiver ID = Device ID-a Data Management Condition among PCCO¹. No restrictions on Sublicense Count	Identifiant de récepteur = identifiant de dispositif-a Condition de gestion de données parmi les PCCO¹. Pas de restrictions au compte de licences secondaires
Management of re-issued License count is necessary	La gestion du compte de licences redistribuées est nécessaire
Receiver ID = Device ID-a Data Management Condition among PCCO¹. Sublicense Count = 3	Identifiant de récepteur = identifiant de dispositif-a Condition de gestion de données parmi les PCCO¹. Compte de licences secondaires = 3
Because redistribution among PCCO¹ is allowed, Receiver = Domain becomes insignificant	Puisque la redistribution parmi les PCCO¹ est autorisée, Récepteur = le domaine devient non significatif
Receiver ID = Domain ID-0 Data Management Condition among PCCO¹. No restrictions on Sublicense Count	Identifiant de récepteur = identifiant de domaine-0 Condition de gestion de données parmi les PCCO¹. Pas de restrictions au compte de licences secondaires
Receiver ID = Domain ID-0 Data Management Condition among PCCO¹. Sublicense Count = 3	Identifiant de récepteur = identifiant de domaine-0 Condition de gestion de données parmi les PCCO¹. Compte de licences secondaires = 3
Device ID-d(PCCO¹) outside of Domain ID-0	Identifiant de dispositif d (PCCO¹) extérieur à l'identifiant de domaine-0
Continue to copy freely among PCCO¹	Poursuite de la copie libre parmi les PCCO¹
Receiver ID = Device ID-d	Identifiant de récepteur = identifiant de dispositif-d

Anglais	Français
Data Management Condition among PCCO ¹ . No restrictions on Sublicense Count	Condition de gestion de données parmi les PCCO ¹ . Pas de restrictions au compte de licences secondaires
Cannot redistribute from Device with Sublicense	Ne peut pas redistribuer à partir du dispositif avec une licence secondaire
Receiver ID = Device ID-d Data Management Condition among PCCO ¹ . Sublicense Count = 0	Identifiant de récepteur = identifiant de dispositif-d Condition de gestion de données parmi les PCCO ¹ . Compte de licences secondaires = 0
Device ID-a1 that belongs to Domain ID-0	Identifiant de dispositif a1 appartenant à l'identifiant de domaine-0
Continue to copy freely among PCCO ¹	Poursuite de la copie libre parmi les PCCO ¹
Receiver ID = Domain ID-0 Data Management Condition among PCCO ¹ . No restrictions on Sublicense Count	Identifiant de récepteur = identifiant de domaine-0 Condition de gestion de données parmi les PCCO ¹ . Pas de restrictions au compte de licences secondaires
Copy freely with Domain / Cannot redistribute among PCCO ¹	Copie libre avec domaine/ne peut pas redistribuer parmi les PCCO ¹
Receiver ID = Domain ID-0 Data Management Condition among PCCO ¹ . No restrictions on Sublicense Count	Identifiant de récepteur = identifiant de domaine-0 Condition de gestion de données parmi les PCCO ¹ . Pas de restrictions au compte de licences secondaires
PCCO ¹ Permission Code Compliant Objects	PCCO ¹ Objets conformes au code d'autorisation

**Figure A.3 – La redistribution d'autorisation parmi les objets conformes
au code d'autorisation est autorisée**



IEC 703/08

Légende

Anglais	Français
Device ID-a that belongs to Domain ID-0	Identifiant de dispositif a appartenant à l'identifiant de domaine-0
Receiver ID = Device ID-a Data Management Condition among PCCO ¹ . Sublicense Count = 0 Domain ID-0. Sublicense Count = 0	Identifiant de récepteur = identifiant de dispositif-a Condition de gestion de données parmi les PCCO ¹ . Compte de licences secondaires = 0 Identifiant de domaine-0. Compte de licences secondaires = 0
Receiver ID = Domain ID-0 Data Management Condition among PCCO ¹ . Sublicense Count = 0 Domain ID-0. Sublicense Count = 3	Identifiant de récepteur = identifiant de domaine-0 Condition de gestion de données parmi les PCCO ¹ . Compte de licences secondaires = 0 Identifiant de domaine-0. Compte de licences secondaires = 3
Receiver ID = Domain ID-0 Data Management Condition among PCCO ¹ . Sublicense Count = 0 Domain ID-0. Sublicense Count = 3	Identifiant de récepteur = identifiant de domaine-0 Condition de gestion de données parmi les PCCO ¹ . Compte de licences secondaires = 3 Identifiant de domaine-0. Compte de licences secondaires = 3
Device ID-a1 that belongs to Domain ID-0	Identifiant de dispositif a1 appartenant à l'identifiant de domaine-0
Receiver ID = Device ID-0 Data Management Condition among PCCO ¹ . Sublicense Count = 0 Domain ID-0. Sublicense Count = 0	Identifiant de récepteur = identifiant de dispositif-0 Condition de gestion de données parmi les PCCO ¹ . Compte de licences secondaires = 0 Identifiant de domaine-0. Compte de licences secondaires = 0
Receiver ID = Device ID-0 Data Management Condition among PCCO ¹ . Sublicense Count = 0	Identifiant de récepteur = identifiant de dispositif-0 Condition de gestion de données parmi les PCCO ¹ . Compte de licences secondaires = 0 Identifiant de domaine-0. Compte de licences

Anglais	Français
Domain ID-0. Sublicense Count = 0	secondaires = 0
Receiver ID = Device ID-0 Data Management Condition among PCCO ¹ . Sublicense Count = 0	Identifiant de récepteur = identifiant de dispositif-0 Condition de gestion de données parmi les PCCO ¹ . Compte de licences secondaires = 0
Device ID-d outside of Domain ID-0	Identifiant de dispositif d extérieur à l'identifiant de domaine-0
Licenses cannot be re-issued since the Sublicense Count equals zero among PCCO ¹	Les licences ne peuvent pas être redistribuées car le compte de licences est égal à zéro parmi les PCCO ¹
PCCO ¹ Permission Code Compliant Objects	PCCO ¹ Objets conformes au code d'autorisation

Figure A.4 – La redistribution d'autorisation dans un domaine est autorisée

IECNORM.COM : Click to view the full PDF of IEC 62227:2008+AMD1:2012 CSV