

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 © 2008 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 Varembé
CH-1211 Geneva 20
Switzerland

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

About the IEC

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

About IEC publications

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

Useful links:

IEC publications search - www.iec.ch/searchpub

The advanced search enables you to find IEC publications by a variety of criteria (reference number, text, technical committee,...).

It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

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

Electropedia - www.electropedia.org

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

Customer Service Centre - webstore.iec.ch/csc

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

A propos de la CEI

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

A propos des publications CEI

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

Liens utiles:

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

La recherche avancée vous permet de trouver des publications CEI en utilisant différents critères (numéro de référence, texte, comité d'études,...).

Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

Just Published CEI - webstore.iec.ch/justpublished

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

Electropedia - www.electropedia.org

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

Service Clients - webstore.iec.ch/csc

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

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

PRICE CODE **XB**
CODE PRIX

ICS 33.160.60; 35.240.99

ISBN 978-2-83220-315-6

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.....	8
1 Scope.....	9
2 Normative references	9
3 Terms, definitions and abbreviations	9
3.1 Terms and definitions	9
3.2 Abbreviated terms	15
4 Permission code framework.....	16
4.1 General.....	16
4.2 Assumptions associated with the permission code.....	17
4.2.1 Binary relationships within the content distribution value chain	17
4.2.2 Permission issued for a group of content	17
4.2.3 Common code center for permissions	18
4.2.4 Usage report	18
4.2.5 Application scenario of the permission code	18
4.2.6 Harmonization with DRM systems.....	19
4.3 Components of a permission code.....	19
4.3.1 Permission actor.....	19
4.3.2 Permission classification	22
4.3.3 Content usage	22
4.3.4 Content data handling	23
5 Permission code configuration.....	24
5.1 General.....	24
5.2 Notation	25
5.2.1 Numerical values	25
5.3 Permission code system.....	25
5.4 Version unit.....	26
5.4.1 Structure	26
5.4.2 Version unit tag	26
5.4.3 Reserved.....	27
5.4.4 Version.....	27
5.5 Permission actor unit.....	27
5.5.1 Structure	27
5.5.2 Permission actor unit tag	27
5.5.3 Total bytes of identifiers	27
5.5.4 Content identifier	28
5.5.5 Issuer identifier.....	29
5.5.6 Receiver identifier	31
5.6 Permission classification unit†.....	32
5.6.1 Structure	32
5.6.2 Permission classification unit tag	32
5.6.3 Reserved.....	32
5.6.4 Disclosure class	32
5.6.5 Usage purpose class	33
5.6.6 Charge model class	34
5.6.7 Billing class	34

5.6.8	Application class	35
5.6.9	Sponsor class.....	35
5.6.10	Territory class	36
5.6.11	Usage class.....	36
5.7	General usage condition unit.....	39
5.7.1	Unit structure.....	39
5.7.2	General usage condition header	39
5.7.3	General usage condition descriptor	39
5.8	Extended use condition unit	48
5.9	Data management condition unit	49
5.9.1	Unit structure.....	49
5.9.2	Data management condition header	49
5.9.3	Data management condition	50
5.10	Data export condition unit.....	52
5.10.1	Unit structure.....	52
5.10.2	Data export condition header.....	52
5.10.3	Data export condition descriptor	52
5.10.4	General export descriptor	53
Annex A (informative)	Permission code requirements for home servers and playback devices	57
Annex B (informative)	Use-case scenario.....	62
Annex C (informative)	Issuing a permission code	70
Figure 1	– Permission code environment	17
Figure 2	– Permission code environment	23
Figure 3	– Permission code configuration	26
Figure 4	– Basic structure of permission code unit.....	26
Figure 5	– General usage condition unit.....	39
Figure 6	– Data management condition unit.....	49
Figure 7	– Data export condition unit	52
Figure A.1	– Permission code and domain	58
Figure A.2	– Re-issuing permission information	59
Figure A.3	– Re-issuing permission among permission code compliant objects is allowed	60
Figure A.4	– Re-issuing permission within a domain is allowed	60
Figure A.5	– Other conditions	61
Figure B.1	– Permission code structuring (1/2).....	62
Figure B.2	– Permission code structuring (2/2).....	63
Figure B.3	– Permission code example with respect to FairPlay (1/2).....	63
Figure B.4	– Permission code example with respect to FairPlay (2/2).....	64
Figure B.5	– Permission code example with respect to CPRM (1/2)	65
Figure B.6	– Permission code example with respect to CPRM (2/2)	65
Figure B.7	– Permission code example with respect to SAFIA (1/2)	66
Figure B.8	– Permission code example with respect to SAFIA (2/2)	66
Figure B.9	– Permission code example with respect to PC distribution (streaming)	67

Figure B.10 – Permission code example with respect to PC distribution (download) (1/2).....	68
Figure B.11 – Permission code example with respect to PC distribution (download) (2/2).....	68
Figure B.12 – Permission code example with respect to ringtones (1/2).....	69
Figure B.13 – Permission code example with respect to ringtones (2/2).....	69
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)	70
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)	71
Figure C.3 – The flow of issuing a permission code to grant access to subscription content (for access on a home server)	72
Figure C.4 – The flow of issuing a permission code to grant access to subscription content (for access on a client device)	73
Table 1 – Distinct tag interpretation	25
Table 2 – Structure of version unit	26
Table 3 – Structure of permission actor unit.....	27
Table 4 – Structure of content identifier descriptor	28
Table 5 – Content type code interpretation.....	28
Table 6 – Structure of issuer identifier descriptor	29
Table 7 – Issuer role code interpretation	30
Table 8 – Issuer configuration code interpretation.....	30
Table 9 – Structure of receiver identifier descriptor	31
Table 10 – Receiver role code interpretation.....	31
Table 11 – Receiver configuration code interpretation.....	31
Table 12 – Structure of permission classification unit.....	32
Table 13 – Structure of disclosure class.....	33
Table 14 – disclosure_type (DT) interpretation.....	33
Table 15 – Structure of usage purpose class	33
Table 16 – usage_purpose_type (UPT) interpretation	33
Table 17 – Structure of charge model class	34
Table 18 – charge_model_type (CMT) interpretation.....	34
Table 19 – Structure of billing class	35
Table 20 – billing_type (BT) interpretation	35
Table 21 – Structure of application class.....	35
Table 22 – application_type (AT) interpretation.....	35
Table 23 – Structure of sponsor class	36
Table 24 – Configuration of sponsor_type (ST)	36
Table 25 – Structure of territory class	36
Table 26 – Structure of usage class	37
Table 27 – Usage_type (UT) interpretation.....	37
Table 28 – Configuration of redistribution_Type	38
Table 29 – Structure of general usage condition header	39
Table 30 – Tag values of descriptors	40

Table 31 – Structure of playback usage condition descriptor	40
Table 32 – Structure of print usage condition descriptor	43
Table 33 – Structure of execute usage condition descriptor	46
Table 34 – Structure of data management condition header	49
Table 35 – Structure of data management condition	50
Table 36 – Structure of encryption flag (EF)	50
Table 37 – Transcode type interpretation	51
Table 38 – Structure of time-line flag (TF)	51
Table 39 – Structure of data export condition header	52
Table 40 – Tag values of descriptors	53
Table 41 – Structure of general export descriptor	53
Table 42 – storage_media_type (SMT) interpretation	54
Table 43 – encoding_type (ET) interpretation	54
Table 44 – protection_type (PT) interpretation	55
Table 45 – control_type (CT) interpretation	55

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.

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.

This bilingual version (2012-11) corresponds to the monolingual English version, published in 2008-06.

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

CDV	Report on voting
100/1287/CDV	100/1374/RVC

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

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 this publication will remain unchanged until the maintenance result 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

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.

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

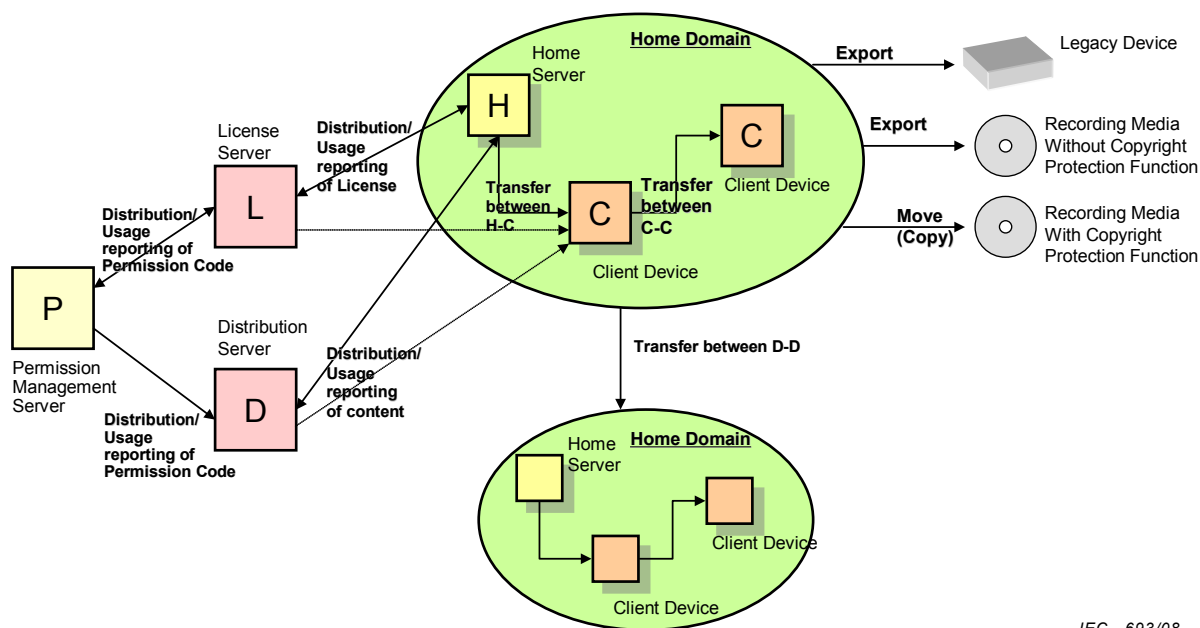
This standard defines permission as “an act by a certain issuing entity to authorize use for content to a certain receiving entity under a certain set of permission classifications, usage conditions, data management conditions and data export conditions”.

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."

permission receiver would be able to extract and compile portions of content as 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

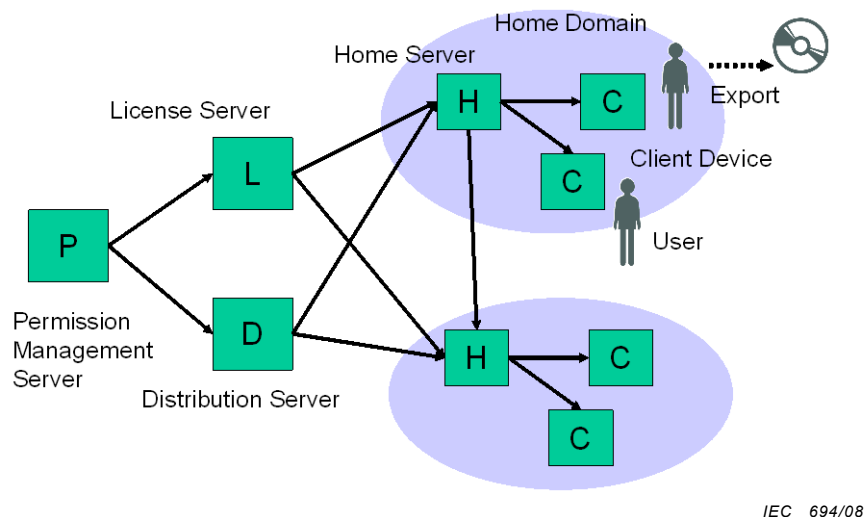


Figure 2 – Permission code environment

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

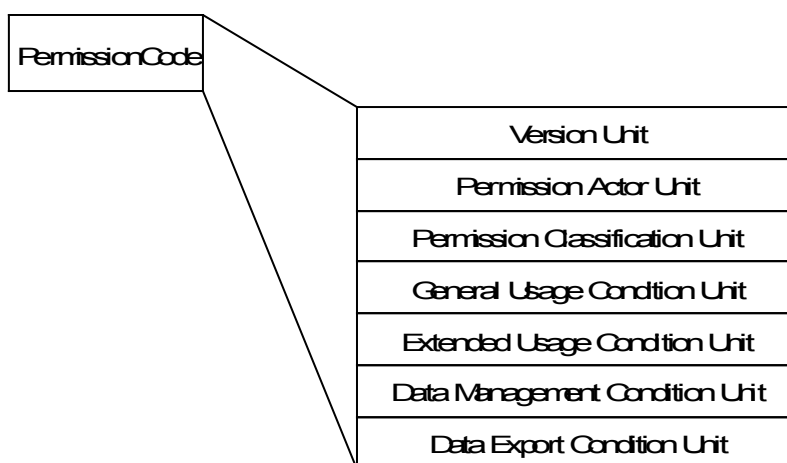
All bits in the reserved fields shall be set to 0b.

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.

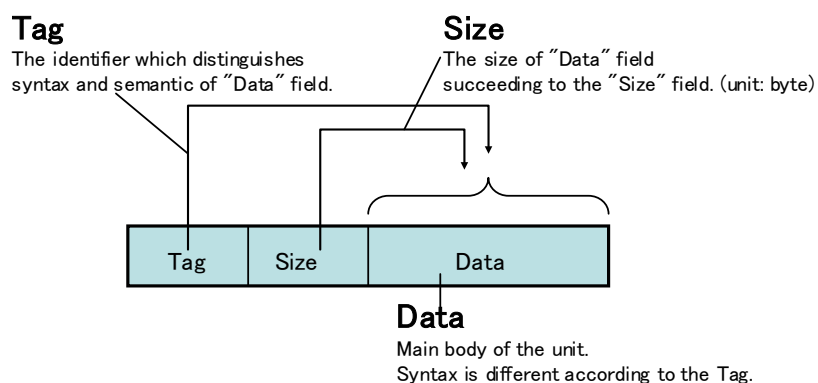
The permission code has a hierarchical structure, tag – length – main data. The top tag determines the main data portion's syntax. Please refer to 5.2.1.6 for more information regarding tags.



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	uimsbf
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
IP	Image Program
II	Image Illustration

Content classification	Interpretation
IC	Image Comic
IM	Image Music
IA	Image Ad
IO	Image Object
PG	Program Game
PS	Program Soft
PM	Program Music
PA	Program Ad
PO	Program Object

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	8	bslbf
if (issuer_role_code == ASCII) {		
Country Code	16	char(2)
Issuer Configuration Code	8	char(1)
ID Center Code	32	char(4)
Unique Code	64	char(8)
} else {		
extended_identifier_length	16	uimbsf
extended_identifier	n	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) uimbsf 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	Sponsor class	bslbf
32	3	Territory class	bslbf
35	13	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
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.

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
}		

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

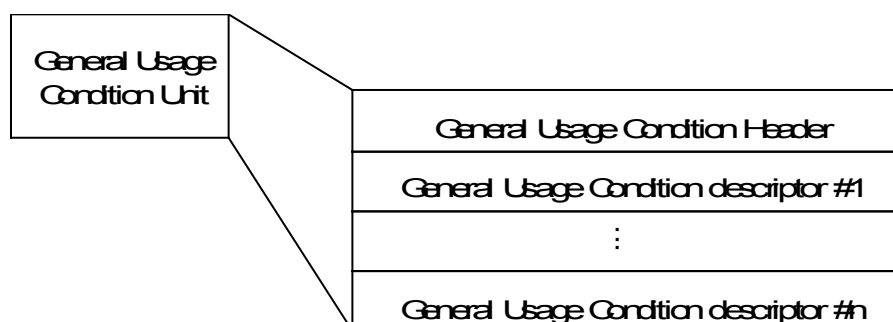
If value is 1b, it indicates the content is permitted to be modified. If value is 0b, it indicates the content is not permitted to be modified.

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	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	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

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.

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
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.

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.