BS EN 62698:2013

BSI Standards Publication

Multimedia home server systems — Rights information interoperability for IPTV

National foreword

This British Standard is the UK implementation of EN 62698:2013. It is identical to IEC 62698:2013.

The UK participation in its preparation was entrusted to Technical Committee EPL/100, Audio, video and multimedia systems and equipment.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2013

ISBN 978 0 580 78655 6

ICS 33.160.60; 35.240.99

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 May 2013.

Amendments issued since publication

Amd. No.	Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 62698

April 2013

ICS 33.160.60; 35.240.99

English version

Multimedia home server systems - Rights information interoperability for IPTV
(IEC 62698:2013)

Systèmes de serveur domestique multimédia -
Interopérabilité d'information des droits pour TVIP
(CEI 62698:2013)

Multimedia-Homeserversysteme -
Interoperabilität von Rechteinformationen für IPTV
(IEC 62698:2013)

This European Standard was approved by CENELEC on 2013-04-15. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

CENELEC
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Management Centre: Avenue Marnix 17, B - 1000 Brussels

Foreword

The text of document 100/1947/CDV, future edition 1 of IEC 62698, prepared by “Technical Area 8 “Multimedia home server systems” of IEC/TC 100 “Audio, video and multimedia systems and equipment” was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 62698:2013.

The following dates are fixed:

• latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2014-01-15
• latest date by which the national standards conflicting with the document have to be withdrawn	(dow)	2016-04-15

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC [and/or CEN] shall not be held responsible for identifying any or all such patent rights.

Endorsement notice

The text of the International Standard IEC 62698:2013 was approved by CENELEC as a European Standard without any modification.

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

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

NOTE When an international publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

Publication	Year	Title	EN/HD	Year
IEC 62227	2008	Multimedia home server systems - Digital rights permission code	EN 62227	2008
IEC/TR 62636	2009	Multimedia home server systems - Implementation of digital rights permission code	-	-
ISO 3166-1	-	Codes for the representation of names of countries and their subdivisions - Part 1: Country codes	EN ISO 3166-1	-
ITU-T Recommendation H.750	2009	High-level specification of metadata for IPTV services	-	-
ITU-T Recommendation X.509	-	Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks	-	-

CONTENTS

INTRODUCTION 6
1 Scope 7
2 Normative references 7
3 Abbreviations and acronyms 7
4 Systems: the RII environment 8
4.1 General 8
4.2 Permission subjects 9
4.3 Permission limit components 9
5 Permission subject identifiers 10
5.1 Permission subject identifiers 10
5.2 Content identifier 10
5.3 Issuer identifier 10
5.4 Receiver identifier 10
6 Permission classification 10
6.1 Permission classification 10
6.2 Disclosure class 11
6.3 Purpose class 11
6.4 Charge model class 11
6.5 Sponsor class 11
6.6 Territory class 12
6.7 Usage class 12
6.8 Compilation class 12
7 Permission limit components 13
7.1 Permission limit components 13
7.2 General usage condition 13
7.2.1 General 13
7.2.2 Quality limits 13
7.2.3 Lifetime limits 13
7.2.4 Permission management system limits 14
7.2.5 Simultaneous output limits 14
7.3 Extended usage condition 15
8 Data management condition 15
9 Data export condition 16
Annex A (informative) SECURITY related issues 18
Annex B (informative) Syntax (encoding) 20
Annex C (informative) Rights information interoperability background 24
Annex D (informative) Two basic technologies for enabling RII 27
Annex E (informative) RII elements corresponding to existing DRM 32
Bibliography 48

Figure A.1 – Example of PkiPath 19
Figure C.1 – Concept – Rights information interoperability 24
Figure D.1 – Common semantics of Metadata 27

Figure D.2 – The necessity of information consolidation for content distribution 28
Figure D.3 – Common semantics for RII 30
Figure D.4 – Core elements and common semantics for RII 31

Table A.1 – Rough composition of distribution format data 18
Table B.1 – Permission actors and permission classifications 21
Table B.2 – Playback usage conditions 22
Table B.3 – Printout usage conditions 22
Table B.4 – Execution usage conditions 22
Table B.5 – Data management conditions 22
Table B.6 – Data output conditions 23
Table E.1 – Marlin BB (broadband) 32
Table E.2 – Marlin IPTV-ES (end-point service), Download license, EXPORT for Copy with Direct Key Delivery 34
Table E.3 – Marlin IPTV-ES, Download license, EXTRACT with Direct Key Delivery, Download 35
Table E.4 – Marlin IPTV-ES, Download license, EXTRACT with Direct Key Delivery, VOD streaming 37
Table E.5 – Marlin IPTV-ES, Broadcast license, EXTRACT with IndirectKey Delivery license, Terrestrial re-distribution/BS (broadcasting satellite) re-distribution 38
Table E.6 – Marlin IPTV-ES, Broadcast license, EXTRACT with DirectKey Delivery license, IP multicast 39
Table E.7 – Marlin IPTV-ES, VOD license, EXTRACT with Simple Key Delivery license 41
Table E.8 – WM-DRM (Windows Media DRM) 42
Table E.9 – OMA DRM v2.0 43
Table E.10 – AACS, basic 45
Table E.11 – AACS, extended 46

INTRODUCTION

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

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

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

MULTIMEDIA HOME SERVER SYSTEMS – RIGHTS INFORMATION INTEROPERABILITY FOR IPTV

1 Scope

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

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

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

2 Normative references

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

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

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

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

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

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

3 Abbreviations and acronyms

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

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

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

4 Systems: the RII environment

4.1 General

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

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

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

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

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

4.2 Permission subjects

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

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

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

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

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

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

4.3 Permission limit components

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

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

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

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

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

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

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

5 Permission subject identifiers

5.1 Permission subject identifiers

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

5.2 Content identifier

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

5.3 Issuer identifier

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

5.4 Receiver identifier

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

6 Permission classification

6.1 Permission classification

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

6.2 Disclosure class

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

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

6.3 Purpose class

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

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

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

6.4 Charge model class

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

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

6.5 Sponsor class

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

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

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

6.6 Territory class

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

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

6.7 Usage class

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

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

Elements required in usage class are listed below.

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

6.8 Compilation class

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

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

7 Permission limit components

7.1 Permission limit components

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

7.2 General usage condition

7.2.1 General

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

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

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

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

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

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

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

7.2.2 Quality limits

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

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

7.2.3 Lifetime limits

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

Elements required in lifetime limits are listed below.

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

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

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

- Day count expresses the number of dates during which the content is permitted to be used (play, print or execute) in target domains and compliance devices. For example, if the value is seven, the content can be used for 7 days after its reception in compliance devices. Possible values are natural values and the unit is day (e.g. 1 day, 7 days).
  - – IEC 62227:2008, 5.7.3.2.14, day_count_parameter, can describe the element with the same meaning on playback usage. 5.7.3.3.12 day_count_parameter can describe the element with the same meaning on print usage. 5.7.3.4.13 day_count_control_parameter can describe the element with the same meaning on excution usage.

- Date period expresses the term limit until which the content is permitted to be used (play, print or execute) in target domain and compliant devices. For example, if the value is from 2010/11/01 to 2010/11/30, the content can be used from 1st November 2010 to 30th November 2010. Possible values are dates (start date and end date) and the unit is date (e.g., period from start date to end date).
  - – IEC 62227:2008, 5.7.3.2.15, start_date_parameter, can describe the element with the same meaning as for playback usage. 5.7.3.3.13, start_date_parameter, can describe the element with the same meaning as for on print usage. 5.7.3.4.14, start_date_parameter, can describe the element with the same meaning as for on playback usage.
  - – IEC 62227:2008, 5.7.3.2.16, end_date_parameter, can describe the element with the same meaning as for on playback usage. 5.7.3.3.14, end_date_parameter, can describe the element with the same meaning as for on print usage. 5.7.3.4.15, end_date_parameter, can describe the element with the same meaning as for on playback usage.

7.2.4 Permission management system limits

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

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

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

7.2.5 Simultaneous output limits

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

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

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

7.3 Extended usage condition

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

8 Data management condition

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

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

Elements required in the data management condition are listed below.

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

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

9 Data export condition

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

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

Elements required in data export condition are listed below.

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

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

Annex A
(informative)

SECURITY related issues

A.1 Tamper detection

A.1.1 General

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

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

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

Table A.1 – Rough composition of distribution format data

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

A.1.2 Authentication

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

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

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

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

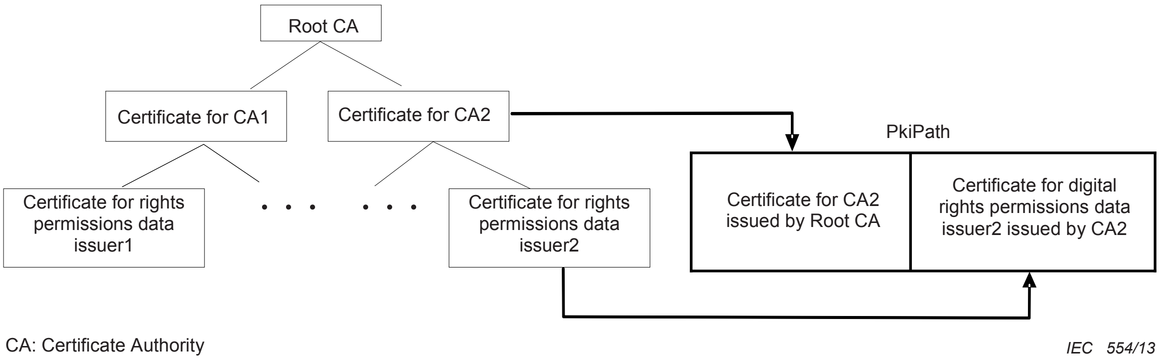

Root CA
Certificate for CA1
Certificate for CA2
Certificate for rights permissions data issuer1
. . . . . .
Certificate for rights permissions data issuer2
PkiPath
Certificate for CA2 issued by Root CA
Certificate for digital rights permissions data issuer2 issued by CA2
CA: Certificate Authority
IEC 554/13

Figure A.1 – Example of PkiPath

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

A.1.3 Signature

The following algorithms are applicable to signature generation and verification.

EC-DSA with SHA

RSA/DSA with SHA

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

A.2 Secret keeping

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

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

Annex B
(informative)

Syntax (encoding)

B.1 General

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

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

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

B.2 DRPC syntaxes tables of the twenty three scenarios

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

In subscription scenario, there are three different permission codes,

a) a parent permission code which represents a permission condition of a subscription contract itself and
b) two children permission codes which represent permission conditions of music contents.

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

Table B.1 – Permission actors and permission classifications

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

Table B.2 – Playback usage conditions

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

Table B.3 – Printout usage conditions

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

Table B.4 – Execution usage conditions

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

Table B.5 – Data management conditions

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

Table B.6 – Data output conditions

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

Annex C
(informative)

Rights information interoperability background

C.1 General

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

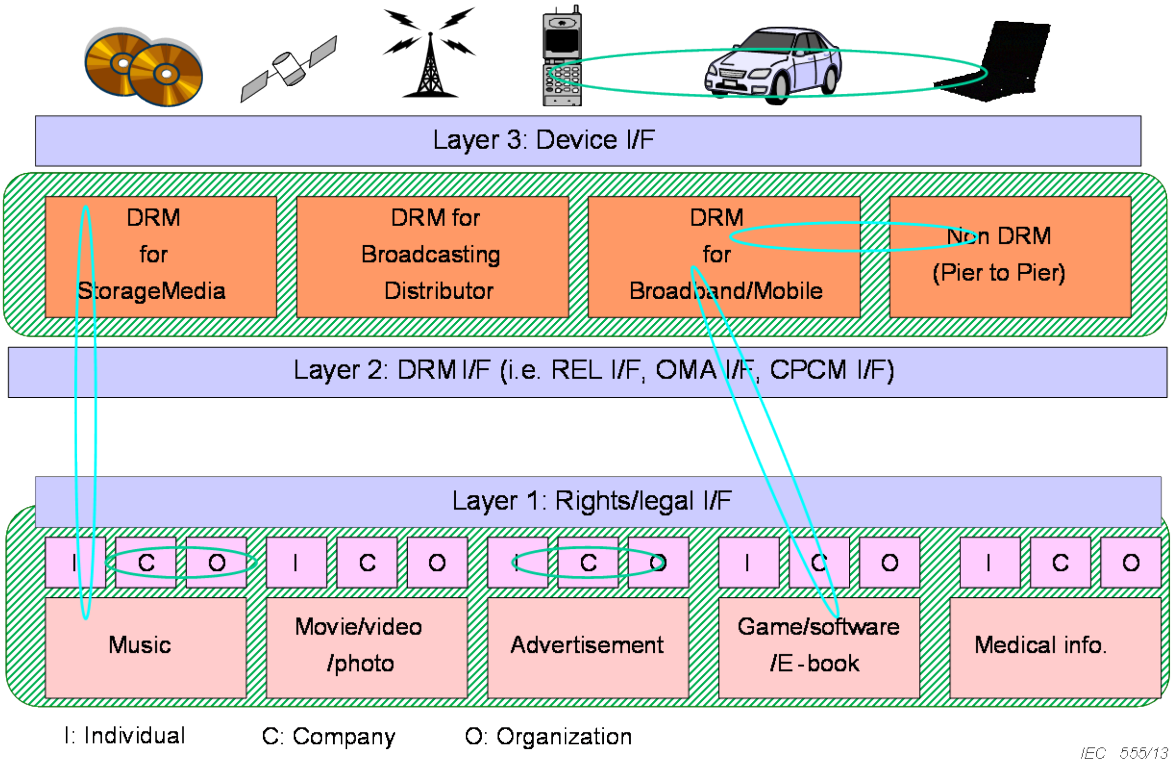


Figure C.1 – Concept – Rights information interoperability

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

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

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

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

C.2 Relationship between rights and digital permissions

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

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

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

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

Specifically,

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

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

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

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

Example

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

↓

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

Streams it?

Downloads it?

Owns recording media?

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

Grant digital rights permissions ⇔ Receive digital rights permissions

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

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

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

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

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

Annex D
(informative)

Two basic technologies for enabling RII

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

D.1.1 General

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

D.1.2 Rights related metadata and simple tag ID code

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

Rights related metadata can be divided roughly into three types.

a) Open metadata

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

b) Closed metadata

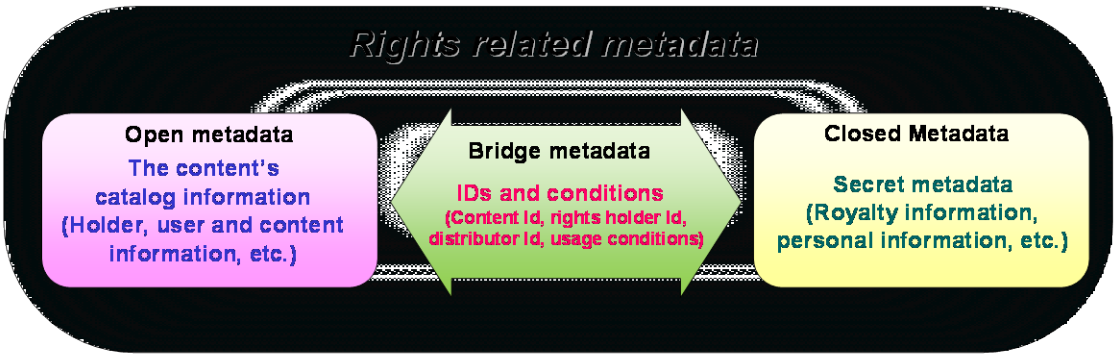
Examples of closed metadata include the auther's real name, bank info, etc.

c) Bridge metadata

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

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

■ Rights Related Metadata is divided into "open metadata" which is made open to the public, "closed metadata" which is only shared by the parties related to those transaction, and "bridge metadata" which relate both types by IDs and Conditions for joint management purposes.


Rights related metadata
Open metadata
The content's catalog information (Holder, user and content information, etc.)
Bridge metadata
IDs and conditions
(Content Id, rights holder Id, distributor Id, usage conditions)
Closed Metadata
Secret metadata
(Royalty information, personal information, etc.)

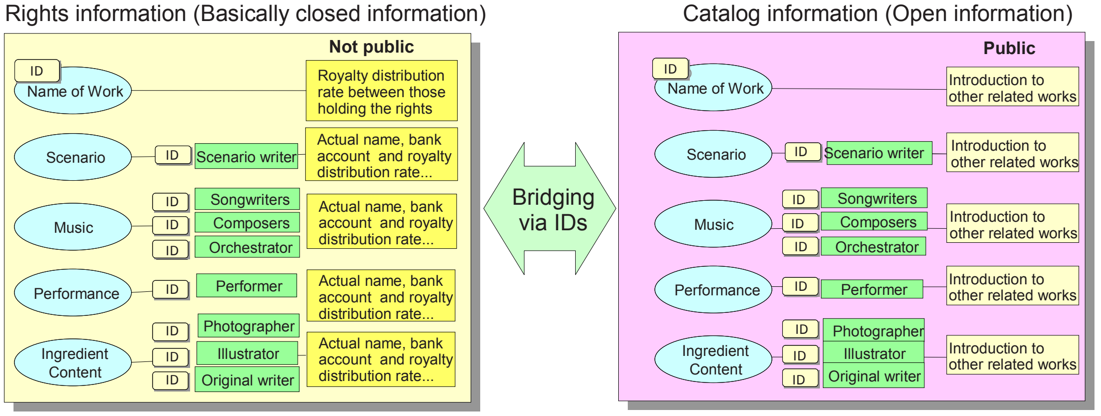
"Metadata": a convenient yet inconvenient term

IEC 556/13

Figure D.1 – Common semantics of Metadata

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

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


Rights information (Basically closed information)
Not public
ID
Name of Work
Royalty distribution rate between those holding the rights
Scenario
ID
Scenario writer
Actual name, bank account and royalty distribution rate...
Music
ID
Songwriters
ID
Composers
ID
Orchestrator
Actual name, bank account and royalty distribution rate...
Performance
ID
Performer
Actual name, bank account and royalty distribution rate...
Ingredient Content
ID
Photographer
ID
Illustrator
ID
Original writer
Actual name, bank account and royalty distribution rate...
Bridging via IDs
Catalog information (Open information)
Public
ID
Name of Work
Introduction to other related works
Scenario
ID
Scenario writer
Introduction to other related works
Music
ID
Songwriters
ID
Composers
ID
Orchestrator
Introduction to other related works
Performance
ID
Performer
Introduction to other related works
Ingredient Content
ID
Photographer
ID
Illustrator
ID
Original writer
Introduction to other related works

IEC 557/13

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

D.1.3 Shared ID system

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

a) Content ID

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

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

b) Business ID

1) Rights holder ID

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

2) User ID

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

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

D.2.1 General

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

D.2.2 Classification

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

a) usage purpose;

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

c) specific usage consumption format;

d) territory of the usage consumption.

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

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

D.2.3 Limit components

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

a) Personal limit component

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

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

b) Transmission and distribution machine setup control component

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

c) Quality limit component

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

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

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

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

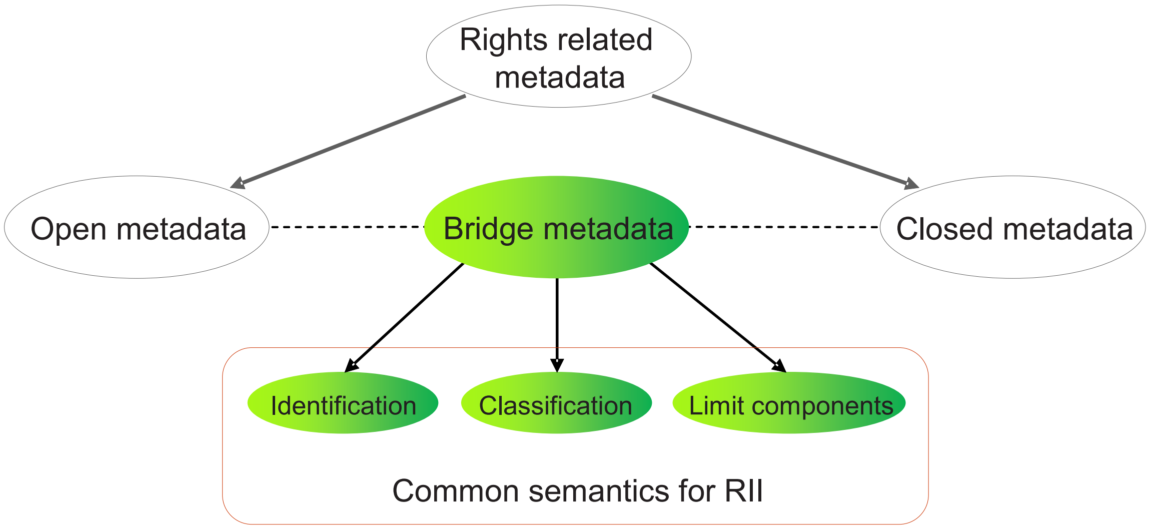
g) Security limit component (watermark, DRM, rights report).

D.3 Common semantics for RII

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

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

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



IEC 558/13

Figure D.3 – Common semantics for RII

D.4 Core elements and common semantics for RII

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

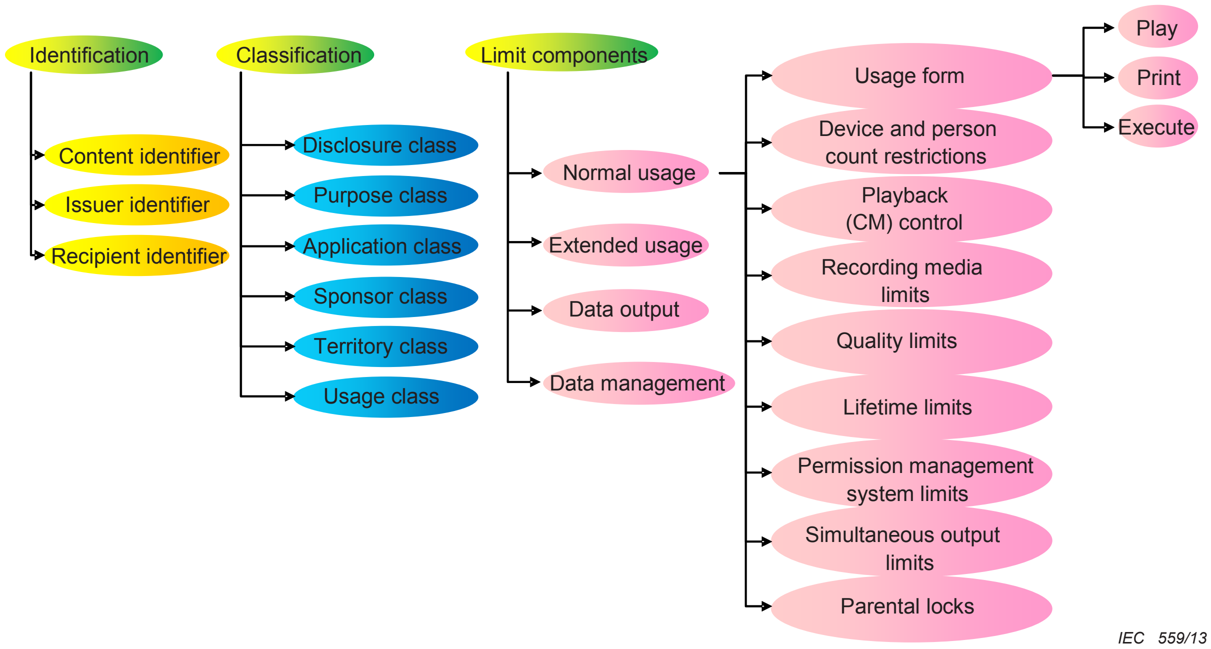


Figure D.4 – Core elements and common semantics for RII

Annex E
(informative)

RII elements corresponding to existing DRM

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

Table E.1 – Marlin BB (broadband)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Table E.9 – OMA DRM v2.0

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

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

Table E.10 – AACS, basic

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

Table E.11 – AACS, extended

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

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

Bibliography

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

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

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

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

____

This page deliberately left blank

British Standards Institution (BSI)

BSI is the independent national body responsible for preparing British Standards and other standards-related publications, information and services. It presents the UK view on standards in Europe and at the international level.

BSI is incorporated by Royal Charter. British Standards and other standardisation products are published by BSI Standards Limited.

Revisions

British Standards and PASs are periodically updated by amendment or revision. Users of British Standards and PASs should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using British Standards would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover. Similary for PASs, please notify BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001

BSI offers BSI Subscribing Members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of British Standards and PASs.

Tel: +44 (0)20 8996 7669 Fax: +44 (0)20 8996 7001
Email: plus@bsigroup.com

Buying standards

You may buy PDF and hard copy versions of standards directly using a credit card from the BSI Shop on the website **www.bsigroup.com/shop.** In addition all orders for BSI, international and foreign standards publications can be addressed to BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001
Email: orders@bsigroup.com

In response to orders for international standards, BSI will supply the British Standard implementation of the relevant international standard, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Knowledge Centre.

Tel: +44 (0)20 8996 7004 Fax: +44 (0)20 8996 7005
Email: knowledgecentre@bsigroup.com

BSI Subscribing Members are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration.

Tel: +44 (0)20 8996 7002 Fax: +44 (0)20 8996 7001
Email: membership@bsigroup.com

Information regarding online access to British Standards and PASs via British Standards Online can be found at **www.bsigroup.com/BSOL**

Further information about British Standards is available on the BSI website at **www.bsi-group.com/standards**

Copyright

All the data, software and documentation set out in all British Standards and other BSI publications are the property of and copyrighted by BSI, or some person or entity that own copyright in the information used (such as the international standardisation bodies) has formally licensed such information to BSI for commerical publication and use. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI. This does not preclude the free use, in the course of implementing the standard, of necessary details such as symbols, and size, type or grade designations. If these details are to be used for any other purpose than implementation then the prior written permission of BSI must be obtained. Details and advice can be obtained from the Copyright & Licensing Department.

Tel: +44 (0)20 8996 7070
Email: copyright@bsigroup.com

BSI

389 Chiswick High Road London W4 4AL UK

Tel +44 (0)20 8996 9001
Fax +44 (0)20 8996 7001
www.bsigroup.com/standards

raising standards worldwide™