

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.751

(03/2013)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

IPTV multimedia services and applications for IPTV –
IPTV metadata

Metadata for rights information interoperability in IPTV services

Recommendation ITU-T H.751



International
Telecommunication
Union

Documents
Document Sharing Hub

ITU-T H-SERIES RECOMMENDATIONS
AUDIOVISUAL AND MULTIMEDIA SYSTEMS

CHARACTERISTICS OF VISUAL TELEPHONE SYSTEMS	H.100–H.199
INFRASTRUCTURE OF AUDIOVISUAL SERVICES	
General	H.200–H.219
Transmission multiplexing and synchronization	H.220–H.229
Systems aspects	H.230–H.239
Communication procedures	H.240–H.259
Coding of moving video	H.260–H.279
Related systems aspects	H.280–H.299
Systems and terminal equipment for audiovisual services	H.300–H.349
Directory services architecture for audiovisual and multimedia services	H.350–H.359
Quality of service architecture for audiovisual and multimedia services	H.360–H.369
Supplementary services for multimedia	H.450–H.499
MOBILITY AND COLLABORATION PROCEDURES	
Overview of Mobility and Collaboration, definitions, protocols and procedures	H.500–H.509
Mobility for H-Series multimedia systems and services	H.510–H.519
Mobile multimedia collaboration applications and services	H.520–H.529
Security for mobile multimedia systems and services	H.530–H.539
Security for mobile multimedia collaboration applications and services	H.540–H.549
Mobility interworking procedures	H.550–H.559
Mobile multimedia collaboration inter-working procedures	H.560–H.569
BROADBAND, TRIPLE-PLAY AND ADVANCED MULTIMEDIA SERVICES	
Broadband multimedia services over VDSL	H.610–H.619
Advanced multimedia services and applications	H.620–H.629
Ubiquitous sensor network applications and Internet of Things	H.640–H.649
IPTV MULTIMEDIA SERVICES AND APPLICATIONS FOR IPTV	
General aspects	H.700–H.719
IPTV terminal devices	H.720–H.729
IPTV middleware	H.730–H.739
IPTV application event handling	H.740–H.749
IPTV metadata	H.750–H.759
IPTV multimedia application frameworks	H.760–H.769
IPTV service discovery up to consumption	H.770–H.779
Digital Signage	H.780–H.789

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T H.751

Metadata for rights information interoperability in IPTV services

Summary

Recommendation ITU-T H.751 defines the common semantics and core elements of rights information interoperability (RII) for Internet Protocol television (IPTV) systems and/or equipment that allow multimedia content to be legally used across different platforms. The rights information includes rights- and security-related metadata that is described in Recommendation ITU-T H.750. This Recommendation describes rights-related information such as content ID, permission issuer ID and permission receiver ID, which are used to bridge between rights-related metadata. It should be noted, however, that rights management and content protection technology are beyond the scope of this Recommendation. This Recommendation is technically aligned with the specification in IEC 62698, *Multimedia home server systems – Rights information interoperability for IPTV*.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T H.751	2013-03-16	16

Keywords

Metadata, permission, rights information.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2013

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

	Page
1 Scope	1
2 References.....	1
3 Definitions	1
3.1 Terms defined elsewhere	1
3.2 Terms defined in this Recommendation.....	3
4 Abbreviations and acronyms	3
5 Conventions	4
6 Introduction: the RII environment	4
6.1 General	4
6.2 Permission subjects	5
6.3 Permission limit components	5
7 Permission subject identifiers	6
7.1 Content identifier	6
7.2 Issuer identifier	6
7.3 Receiver identifier	6
8 Permission classification	6
8.1 Disclosure class	7
8.2 Purpose class	7
8.3 Charge model class.....	7
8.4 Sponsor class	7
8.5 Territory class.....	8
8.6 Usage class	8
8.7 Compilation class	9
9 Permission limit components.....	9
9.1 General usage condition	9
9.2 Extended usage condition.....	11
10 Data management condition	11
11 Data export condition	12
Appendix I – Security-related issues	14
I.1 Tamper detection	14
I.2 Keeping secret	15
Appendix II – Syntax (encoding).....	16
II.1 General	16
II.2 Digital rights permission code syntaxes tables of the 23 scenarios.....	16
Appendix III – Background to rights information interoperability.....	20
III.1 General	20
III.2 Relationship between rights and digital permissions	21

	Page
Appendix IV – Two basic technologies for enabling RII	23
IV.1 Code language technology that carries the shared elements that identify the scattered content and the parties associated with that content.....	23
IV.2 Code language technology that carries the shared elements of the specific content consumer services	25
IV.3 Common semantics for RII	26
IV.4 Core elements and common semantics for RII.....	26
Appendix V – Rights information metadata elements corresponding to existing SCP systems.....	28
V.1 SCP1	28
V.2 SCP System 2, with Download license, EXPORT for Copy with Direct Key Delivery	30
V.3 SCP System 3, with Download license, EXTRACT with Direct Key Delivery, Download	31
V.4 SCP System 4, with Download license, EXTRACT with Direct Key Delivery, VOD streaming.....	32
V.5 SCP System 3, with Download license, EXTRACT with Direct Key Delivery, Download	33
V.6 SCP System 4, with Download license, EXTRACT with Direct Key Delivery, VOD streaming.....	34
V.7 SCP System 5, with, Broadcast license, EXTRACT with IndirectKey Delivery license, Terrestrial re-distribution/BS(Broadcasting satellite) re- distribution.....	35
V.8 SCP System 6, with Broadcast license, EXTRACT with DirectKey Delivery license, IP multicast.....	36
V.9 SCP System 9, for mobile IPTV terminal	38
V.10 SCP System 10, for recording media (e.g., DVD), basic	39
V.11 SCP System 11, for recording media (e.g., DVD), extended.....	40
Appendix VI – Examples of media formats.....	41
Bibliography.....	42

Recommendation ITU-T H.751

Metadata for rights information interoperability in IPTV services

1 Scope

This Recommendation gives the high-level specification of the metadata for rights information interoperability, including representation of the minimum required elements. The rights information interoperability (RII) metadata provide 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.

This Recommendation defines the common semantics and core elements of rights information interoperability for IPTV systems and/or equipment that require multimedia content to be legally used across different platforms.

The rights information includes rights- and security-related metadata that is described in [ITU-T 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 Recommendation. It should be noted, however, that rights management and content protection technology are beyond the scope of this Recommendation.

This Recommendation is technically aligned with the specification in [IEC 62698].

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

- | | |
|---------------|---|
| [ITU-T H.750] | Recommendation ITU-T H.750 (2008), <i>High-level specification of metadata for IPTV services</i> . |
| [IEC 62227] | IEC 62227 (2008), <i>Multimedia home server systems – Digital rights permission code subdivisions</i> . |
| [IEC 62698] | IEC 62698:2013, <i>Multimedia home server systems – Rights information interoperability for IPTV</i> . |
| [ISO 3166-1] | ISO 3166-1 (2009), <i>Codes for the representation of names of countries and their subdivisions – Part 1: Country codes</i> . |

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

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

3.1.2 content export [b-ITU-T X.1191]: Process of exporting securely the IPTV content from the IPTV terminal to another terminal owned by the user entitled to use it.

3.1.3 content protection [b-ITU-T Y.1901]: Ensuring that an end-user can only use the content they have already acquired in accordance with the rights that they have been granted by the rights holder.

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

3.1.5 digital signature [b-ITU-T X.800]: Data appended to, or a cryptographic transformation (see cryptography) of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g., by the recipient.

3.1.6 distribution [b-ITU-T Y.1910]: In the context of IPTV architecture, "distribution" is defined as sending the content to appropriate intermediate locations to enable subsequent delivery.

3.1.7 end user [b-ITU-T Y.1910]: The actual user of the products or services.

NOTE – The end user consumes the product or service. An end user can optionally be a subscriber.

3.1.8 IPTV [b-ITU-T Y.1901]: Multimedia services such as television/video/audio/text/graphics/data delivered over IP-based networks managed to support the required level of QoS/QoE, security, interactivity and reliability.

3.1.9 key [b-ITU-T X.800]: A sequence of symbols that controls the operations of encipherment and decipherment.

3.1.10 metadata [b-ITU-T Y.1901]: Structured, encoded data that describe characteristics of information-bearing entities to aid in the identification, discovery, assessment, and management of the described entities.

NOTE – EPG metadata has many applications and may vary in depth from merely identifying the content package title or information to populate an EPG to providing a complete index of different scenes in a movie or providing business rules detailing how the content package may be displayed, copied, or sold.

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

3.1.12 PkiPath [b-ITU-T X.509]: The data type PkiPath is used to represent a certification path for ITU-T X.509 digital certificates. Within the sequence, the order of public-key certificates is such that the subject of the first certificate is the issuer of the second certificate, etc.

3.1.13 rights [b-ITU-T X.1191]: Referring to the ability to perform a predefined set of utilization functions for a content item; these utilization functions include permissions (e.g., to view/hear, copy, modify, record, excerpt, sample, keep for a certain period, distribute), restrictions (e.g., play/view/hear for multiple number of times, play/view/hear for certain number of hours), and obligations (e.g., payment, content tracing) that apply to the content and provide the liberty of use as granted to the end user.

3.1.14 rights expression [b-ITU-T X.1191]: Syntactic embodiment of rights in concrete, formal form.

3.1.15 service [b-ITU-T Y.101]: A structure set of capabilities intended to support applications.

3.1.16 service and content protection [b-ITU-T X.1191]: A combination of service protection and content protection or the system or implementation thereof.

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

3.1.18 tamper-resistant [b-ITU-T X.1191]: Resistance to tampering by either the personal users/attackers of a product, package, or system with physical/software access to it.

3.1.19 terminal device (TD) [b-ITU-T Y.1901]: An end-user device which typically presents and/or processes the content, such as a personal computer, a computer peripheral, a mobile device, a TV set, a monitor, a VoIP Terminal or an audio-visual media player.

3.1.20 transcoding [b-ITU-T X.1191]: Process of transforming multimedia content such as images, text, audio, and video from the original format to a different format or quality.

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

NOTE – The viewing may occur sometime after the selection of the video content.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 information interoperability: The term used to describe the ability to meaningfully exchange information among separately developed systems, where the separate systems are able to understand the format, meaning and also the quality of the information being exchanged.¹

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AAC	Advanced Audio Coding
CD	Compact Disc
CM	Commercial Message
DRPC	Digital Rights Permission Code
DSA	Digital Signature Algorithm
DVD	Digital Versatile Disk
EC-DSA	Elliptic Curve Digital Signature Algorithm
GC	Group Contents
GIF	Graphic Interchange Format
HD	High Definition
HDD	Hard Disk Drive
ID	Identifier
IPTV	Internet Protocol Television
JPEG	Joint Photographic Experts Group
MP3	MPEG Audio Layer-3

¹ Based on http://www.webopedia.com/TERM/I/information_interoperability.html

MPEG	Moving Picture Experts Group
PCM	Pulse Code Modulation
PNG	Portable Network Graphics
RII	Rights Information Interoperability
RSA	Rivest Shamir Adleman
SCP	Service and Content Protection
SHA	Secure Hash Algorithm
VOD	Video On Demand

5 Conventions

The following conventions are used in this Recommendation:

- The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.
- The keywords "is prohibited from" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.
- The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.
- The keywords "is not recommended" indicate a requirement which is not recommended but which is not specifically prohibited. Thus, conformance with this Recommendation can still be claimed even if this requirement is present.
- The keywords "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with this Recommendation.

6 Introduction: the RII environment

6.1 General

This Recommendation gives the high-level standard of the metadata for rights information interoperability, including representation of the minimum recommended 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. In other words, RII is about conveying rights information in units of groups of context expressions called permissions.

This Recommendation considers the constituent components of permissions. Permissions can encode "what, from whom and to whom" and "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 and to whom" part, and the content usage information that corresponds to the "under what conditions" part.

6.2 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 recommended 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 if 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.

6.3 Permission limit components

One permission limit component is the type of permission (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 types, which indicate:

- whether the permission content being granted is public or not (hereinafter referred to as "the disclosure class");
- the purpose of use being granted (hereinafter referred to as the "purpose class");
- the billing format being granted (hereinafter referred to as the "charge model class");
- the request format being granted (hereinafter referred to as the "request class");
- the sponsor format being granted (hereinafter referred to as the "sponsor class");
- the usage format being granted (hereinafter referred to as the "usage class"); and
- the territory being granted, (hereinafter referred to as the "territory class").

These permissions limit components are included in RII because it is necessary to be able to see the information, even in an offline environment that is not connected to a network. This is so that the terminal can determine what types of permission 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 information that limits 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 permissions limit components are included in RII because it is necessary that the rights they correspond 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 and the encoding method should make use of existing standardized technology. Clause II.2 shows the example of adding context expressions stated using natural language in [IEC 62227].

RII is a set of items to be considered when 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 either an administrative issue or an issue related to service and content protection (SCP) systems. RII does not have an exclusive policy. Implementers of each SCP or content distribution system can choose their own subset and RII usage scheme, based on their necessity and resources. For example, they can limit the application to simply displaying the permissions but not use them for rights management.

7 Permission subject identifiers

There are three permission subject identifiers: Content identifier assigned to the subject content, issuer identifier assigned respectively to each permission issuer, and receiver identifier assigned to each permission receiver.

7.1 Content identifier

The content identifier is information to uniquely identify the content. It is required that a content identifier be assigned to each content that is subject to permission.

7.2 Issuer identifier

The issuer identifier is information to uniquely identify the permission issuer. The 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 reporting and content management.

7.3 Receiver identifier

The receiver identifier is information to uniquely identify the permission receiver. The receiver identifier may be used to identify an end-user, a device or a set of end users.

8 Permission classification

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

8.1 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.

Clause 5.6.4 in [IEC 62227] on disclosure classes specifies a permission classification for signalling and carrying disclosure information. Informative clause B.2 of [b-IEC 62636] addresses permission actors and permission classifications and provides use-case scenarios for implementing disclosure class.

8.2 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.

Clause 5.6.5 of [IEC 62227] addresses usage purpose class and specifies a permission classification for signalling and carrying usage purpose information. Clauses 5 and B.2 (informative) of [b-IEC 62636] provide use-case scenarios for implementing usage purpose class.

8.3 Charge model class

Charge model class defines classification including the charge method such as free-of-charge and for-charge. It might include "pay-per-view" (charged per viewing), and "subscription" (fixed periodic charge) categories. These conditions should not be used at the same time; if one is selected, the other is not used. Possible values are "free of charge", "pay per use", "subscription", and "coupon".

Clause 5.6.6 of [IEC 62227] specifies a permission classification for signalling and carrying charge model information. Informative clause B.2 of [b-IEC 62636] provides use-case scenarios for implementing charge model classes.

8.4 Sponsor class

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

The advertising model describes the condition of viewing ads in the content consumption. The premium, coupon and consumption information disclosure models describe the conditions for the content acquisition. In the premium model there can be a specific advertiser to sponsor a specific content. In the coupon model there can be multiple advertiser to sponsor the content. In the disclosure model, the content can be exchanged for end-user's 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".

Clause 5.6.9 in [IEC 62227] on sponsor classes specifies a permission classification for signalling and carrying sponsor information. Clauses 5.17 and 5.18 in [b-IEC 62636] describe use-case scenarios on download and streaming of free content with advertising that illustrate the implementation of sponsor class.

8.5 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 contents are consumed. Possible values are region code, country code (ISO 3166-1) and postal code.

Clause 5.6.10 in [IEC 62227] specifies a permission classification for signalling and carrying territory information. Clause B.2 of [b-IEC 62636] provides a use-case scenario for implementing territory class.

8.6 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.

Clause 5.6.11 in [IEC 62227] on usage class specifies a permission classification for signalling and carrying usage information. Clause B.2 of [b-IEC 62636] provides a use-case scenario for implementing usage class.

The elements required in the usage class are as follows:

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

8.7 Compilation class

Compilation class includes classification indicating content 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 enable, false if play-list disable and other.

Clause 5.7.3.2.6 in [IEC 62227] specifies the `playlist_parameter` field on permission conditions for signalling and carrying compilation information.

9 Permission limit components

Permission 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.

9.1 General usage condition

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 execution 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 compliant devices.

Clause 5.7.3.2 of [IEC 62227] on playback usage condition descriptor 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 compliant devices.

Clause 5.7.3.3 of [IEC 62227] on print usage condition descriptors 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 compliant devices.

Clause 5.7.3.4 of [IEC 62227] on execute usage condition descriptors specifies a permission constraint for signalling and carrying execution condition.

9.1.1 Quality limits

Component **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":

- Clause 5.7.3.2.4 of [IEC 62227] defines the `quality_parameter` field on quality condition for playback usage (high quality, standard, low quality, and extension).
- Clause 5.7.3.3.4 of [IEC 62227] defines the `quality_parameter` field on quality conditions for print usage (high quality, standard, low quality, and extension).
- Clause 5.7.3.4.4 of [IEC 62227] defines the `service_level_parameter` field on quality conditions for execution usage (full control, standard, trial and extension).