International Telecommunication Union

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

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/.

Table of Contents

Page

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), *High-level specification of metadata for IPTV services*.

[IEC 62227] IEC 62227 (2008), *Multimedia home server systems – Digital rights permission code subdivisions*.

[IEC 62698] IEC 62698:2013, *Multimedia home server systems – Rights information interoperability for IPTV.*

[ISO 3166-1] ISO 3166-1 (2009), *Codes for the representation of names of countries and their subdivisions – Part 1: Country codes*.

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).

9.1.2 Lifetime limits

Component **lifetime limits** includes information indicating the usage lifetime of distributed content. Permission issuers typically specify a time period, a day count or a date range.

Elements required in **lifetime limits** are as follows:

– Time period expresses the number of hours during which use (play, print or execute) of the content is permitted in target domains and compliant devices. For example, if the value is 24, the content can be used for 24 hours after received in a compliant device. Possible values are natural numbers and the unit is hour (e.g., 24 hours, 48 hours).

  - Various clauses of [IEC 62227] apply. Clause 5.7.3.2.13 defines the time_period_parameter field that can be used to describe the element for the same meaning on playback usage. Clause 5.7.3.3.11 defines the time_period_parameter field that can be used to describe the element for the same meaning on print usage. Clause 5.7.3.4.12 defines the time_period_parameter field that can be used to describe the element for the same meaning on playback usage.

– Day count expresses the number of days during which use (play, print or execute) of the content is permitted in target domains and compliant devices. For example, if the value is 7, the content can be used for 7 days after received in a compliant device. Possible values are natural values and the unit is day (e.g., 1 day, 7 days).

  - Various clauses of [IEC 62227] apply. Clause 5.7.3.2.14 defines the day_count_parameter field that can be used to describe the element for the same meaning on playback usage. Clause 5.7.3.3.12 defines the day_count_parameter field that can be used to describe the element for the same meaning on print usage. Clause 5.7.3.4.12 defines the day_count_parameter field that can be used to describe the element for the same meaning on execution usage.

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

  - Various clauses of [IEC 62227] apply. Clause 5.7.3.2.15 defines the start_date_parameter field that can be used to describe the element for the same meaning on playback usage. Clause 5.7.3.3.13 defines the start_date_parameter field that can be used to describe the element for the same meaning on print usage. Clause 5.7.3.4.14 defines the start_date_parameter field that can be used to describe the element for the same meaning on playback usage.
  - Various clauses of [IEC 62227] apply. Clause 5.7.3.2.16 defines the end_date_parameter field that can be used to describe the element for the same meaning on playback usage. Clause 5.7.3.3.14 defines the end_date_parameter field that can be used to describe the element for the same meaning on print usage. Clause 5.7.3.4.15 defines the end_date_parameter field that can be used to describe the element for the same meaning on playback usage.

9.1.3 Permission management system limits

Component **permission management system limits** include 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 compliant device is required to protect the content using a SCP system on its usage time (playing, printing or executing). Possible values are "digital copy protection", "digital watermark" and "rights report". It may take a value of –1 for "other" meaning.

Various clauses of [IEC 62227] apply. Clause 5.7.3.2.5 (permission_management_model_ parameter) can be used to describe the element for the same meaning on playback usage. Clause 5.7.3.3.5 (permission_management_model_parameter) can be used to describe the element for the same meaning on print usage. Clause 5.7.3.4.5 (permission_management_model_parameter) can be used to describe the element for the same meaning on execute usage.

9.1.4 Simultaneous output limits

Component **simultaneous output limits** includes information indicating the permitted number of simultaneous output for each content consumption. For example, if the value is 2, a compliant device is permitted to simultaneously export the content toward two displays during its allowed usage time (playing, printing or executing). Valid values are non-negative integers, and –1 to designate "other".

Clause 5.7.3.2.17 of [IEC 62227] defines the simultaneous_output_parameter field that can be used to describe the element for the same meaning on playback usage.

9.2 Extended usage condition

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

10 Data management condition

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

Permission issuers typically specify encryption flag, copy count, transcode type, expiration date, and other usage condition about the data management.

Elements required in 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 and other.
  - Clause 5.9.3.3 of [IEC 62227] (encryption_flag) can be used to describe the element for the same meaning.

– Copy count expresses the number of times that the content can be permitted to copy in target domains and compliant devices. If the value is 1, there can be two copies including the original one. Possible values are non-negative integers and –1 to designate "other".
  - Clause 5.9.3.4 of [IEC 62227] on copy count can be used to describe the element for the same meaning.

– Move count expresses the number of times that the content can be permitted to mobile in target domains and compliant devices. "Move" usually means a combination of copying the content and deleting the original one. Possible values are non-negative integers and –1 to designate "other".
  - Clause 5.9.3.5 of [IEC 62227] on move count can describe the element for the same meaning.

– Transcode type expresses the type of transcoding in which the content can be permitted to be stored in target domains and compliant devices. Examples of possible values are found in Appendix VI.

  - Clause 5.9.3.6 of [IEC 62227] on transcode type can describe the element for the same meaning.

– Maximum transcode rate expresses the highest bit rate at which the content is permitted to be transcoded for storing in target domains and compliant devices. Possible values are non-negative real numbers and the unit is kbit/s.

  - Clause 5.9.3.7 of [IEC 62227] on maximum transcode rate can describe the element for the same meaning.

– Minimum transcode rate expresses the lowest bit rate at which the content is permitted to be transcoded for storing in target domains and compliant devices. Possible values are non-negative real numbers and the unit is kbit/s.

  - Clause 5.9.3.8 of [IEC 62227] on minimum transcode rate can describe the element for the same meaning.

– Expiration date expresses the limit date until which the content is permitted to be stored in target domains and compliant devices. Possible values are dates, using the date format defined in [ITU-T H.750].

  - Clause 5.9.3.9 of [IEC 62227] on expiration date can describe the element for the same meaning.

– Sublicense count expresses the number of times sub-licenses are permitted to be issued in target domains and compliant devices. Possible values are non-negative integers.

  - Clause 5.9.3.10 of [IEC 62227] on sublicense count can describe the element for the same meaning.

– Time-line edit flag indicates whether editing the content with respect to a time-line (i.e., the content is shortened time-wise) and saving the resulting content is permitted. Possible values are `true` (time-line edit enabled), `false` (time-line edit disabled) and `other`.

  - Clause 5.9.3.11 of [IEC 62227] on time-line edit can describe the element for the same meaning.

11 Data export condition

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

Permission issuers typically specify storage media, encoding type, control type, time period, day count, date period, and other usage conditions regarding content export.

The elements required in data export condition are as follows:

– Encryption flag indicates indicate whether the content needs to be encrypted or not. Possible values are `true` (encryption required), `false` (encryption not required), and `other`.

  - Clause 5.9.3.3 of [IEC 62227] (encryption_flag) can be used to describe the element for the same meaning.

– Copy count expresses the number of times the content can be permitted to be copied in target domains and compliant devices. Possible values are non-negative integers and –1 to designate "other". For example, if the value is 1, there can be two copies, including the original one.

  - Clause 5.9.3.4 of [IEC 62227] on copy count can be used to describe the element for the same meaning.

– Move count expresses the number of times that the content can be permitted to be moved in target domains and compliant devices. "Move" usually means a combination of copying the content and deleting original one. Possible values are non-negative integers and –1 to designate "other".

  - Clause 5.9.3.5 of [IEC 62227] on move count can be used to describe the element for the same meaning.

– Transcode type expresses the type of transcoding in which the content can be permitted to be stored in the target domain and compliant devices. Examples of possible values are found in Appendix VI.

  - Clause 5.9.3.6 of [IEC 62227] on transcode type can be used to describe the element for the same meaning.

– Maximum transcode rate expresses the highest bit rate at which the content may be transcoded for storage in the target domain and compliant devices. Possible values are non-negative real numbers and the unit is kbit/s.

  - Clause 5.9.3.7 of [IEC 62227] on maximum transcode rate can be used to describe the element for the same meaning.

– Minimum transcode rate expresses the lowest bit rate at which the content may be transcoded for storage in target domains and compliant devices. Possible values are non-negative real numbers and the unit is kbit/s.

  - Clause 5.9.3.8 of [IEC 62227] on minimum transcode rate can be used to describe the element for the same meaning.

– Expiration date expresses the limit date until which the content may be stored in target domains and compliant devices. The possible value is date, formatted as defined in [ITU-T H.750].

  - Clause 5.9.3.9 of [IEC 62227] on expiration date can be used to describe the element for the same meaning.

– Sublicense count expresses the number of times for which sub-licenses can be issued in target domains and compliant devices. Possible values are non-negative integers.

  - Clause 5.9.3.10 of [IEC 62227] on sub-license count can be used to describe the element for the same meaning.

– Time-line edit flag indicates whether editing the content with respect to a time-line (i.e., the content is shortened time-wise) and saving the resulting content is permitted. Possible values are true (time-line edit enabled), false (time-line edit disabled) and other.

  - Clause 5.9.3.11 of [IEC 62227] on time-line edit can be used to describe the element for the same meaning.

Appendix I

Security-related issues

(This appendix does not form an integral part of this Recommendation.)

I.1 Tamper detection

I.1.1 General

Since distribution format data representing digital rights permissions require screening to detect whether or not they have been falsified by anyone, they must include a digital signature.

The elliptic curve digital signature algorithm (EC-DSA) with secure hash algorithm (SHA) and the Rivest Shamir Adleman (RSA)/DSA with SHA are given as applicable examples of digital signature algorithms. The concrete standard of the signature is implementation-dependent.

The basic composition of distribution format data is depicted in Table I.1.

Table I.1 – Basic composition of distribution format data

Description	Digital rights permissions data	Digital signature	Certificate or PkiPath
Relevant information: – Position in the PkiPath hierarchy – 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 to authenticate the digital signature.

I.1.2 Authentication

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

The issuer generates the digital signature of the digital rights permissions data by using the above private key, and makes 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 are to comply with [b-ITU-T X.509].

If the certificate contains a certificate chain, PkiPath defined in [b-ITU-T X.509] is used.

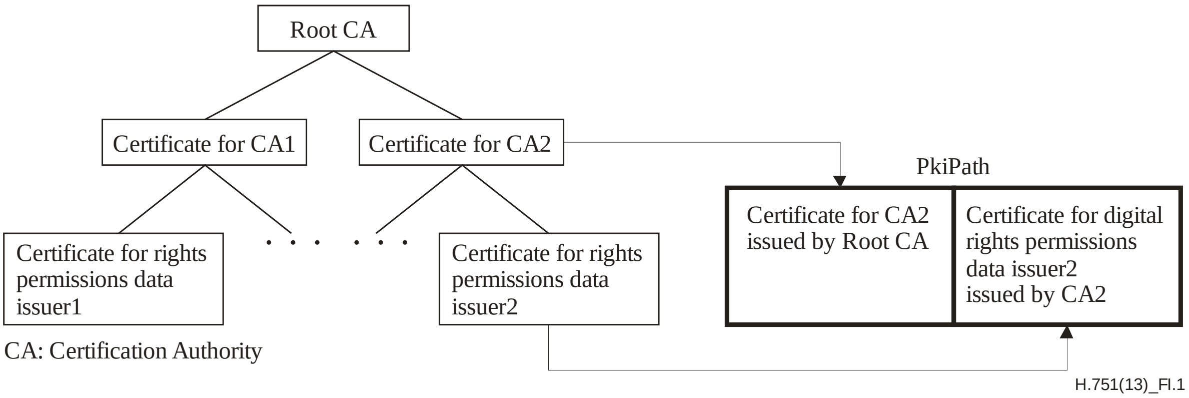

Root CA
Certificate for CA1
Certificate for CA2
Certificate for rights permissions data issuer1
Certificate for rights permissions data issuer2
PkiPath
Certificate for CA2 issued by Root CA
Certificate for digital rights permissions data issuer2 issued by CA2
CA: Certification Authority
H.751(13)_FI.1

Figure I.1 – Example of PkiPath

Figure I.1 shows an example of PkiPath. The depth of the PkiPath hierarchy depends on how each service or system is implemented. This information needs to be specified in the description area of the distribution format data.

I.1.3 Signature

The following algorithms are applicable for signature generation and verification:

- EC-DSA with SHA
- RSA/DSA with SHA

The key lengths and encryption parameters of EC-DSA, RSA/DSA and SHA depend on the implementation of each service or system. This information needs to be specified in the description area of the distribution format data.

I.2 Keeping secret

The decision as to whether distribution format data representing digital rights permissions is to be kept secret is either service or system dependent.

If the digital rights permissions data have to be kept secret, the protection mechanism will be service or system dependent, and is outside the scope of this Recommendation.

Appendix II

Syntax (encoding)

(This appendix does not form an integral part of this Recommendation.)

II.1 General

Considering the implementation of IPTV services, metadata need to be encoded by a common standardized format. Interoperability requires that the representation scheme of rights-related metadata be based on a common syntax. This clause shows the typical 23 use-cases scenarios that are described in [b-IEC 62636]:

- Content purchase
- Rental with time or playback limit
- Subscription
- Two scenarios on direct retrieval of content from a device
- Unlimited play
- Preview
- Multiple permissions for a multipart content format
- Inheritance
- Export of content
- Combinations of constraint elements
- Recordable media
- Ringtones
- Download or streaming of free content with advertising
- Giveaways
- Coupons (discount points)
- Privacy information disclosure
- Copying nine times with unlimited moving
- Subscription games
- Software rental

In the next clause, these scenarios are divided into permission conditions tables using the syntax in [IEC 62227].

II.2 Digital rights permission code syntaxes tables of the 23 scenarios

This clause shows digital rights permission code (DRPC) [IEC 62227] syntax tables of the 23 scenarios above that expand the four main elements (ContentID, IssuerID, Receiver ID and Permission conditions) into the sub-elements that specify the practical value for each element in the scenarios (see Tables II.1 to II.6).

In the subscription example scenario, there are three different permission codes: one parent permission code (which represents a permission condition of a subscription contract itself) and two children permission codes (which represent permission conditions of music contents). Further, it is assumed that Receiver ID has the fixed value "HJPC01000000001".

Table II.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	UJPI010000000101
2	VPJP010000000202	Rental with time or playback limit	Open	Commercial	Fee-based	Individual	Individual	No Sponsor	Reserved	Download	UJPI010000000101
3	SMJP010000000210	Subscription	Open	Commercial	Fee-based, Subscription	Individual	Individual	No Sponsor	Reserved	Download, Reuse, Copy	UJPI010000000101
4	SMJP010000000211	Subscription child 1	Open	Commercial	Fee-based, Subscription	Individual	Individual	No Sponsor	Reserved	Download, Reuse, Copy	UJPI010000000101
5	SMJP010000000212	Subscription child 2	Open	Commercial	Fee-based, Subscription	Individual	Individual	No Sponsor	Reserved	Download, Reuse, Copy	UJPI010000000101
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	UJPI010000000101
9	VPJP010000000302	Preview	Open	Commercial	Fee-based	Individual	Individual	No Sponsor	Reserved	Streaming	UJPI010000000101
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	UJPI010000000101
16	VPJP010000000502	CPRM	Open	Commercial	Fee-based	Individual	Individual	No Sponsor	Reserved	Download, Reuse, Export	UJPI010000000101
17	VPJP010000000503	SAFIA	Open	Commercial	Fee-based	Individual	Individual	No Sponsor	Reserved	Download, Reuse, Copy, Export	UJPI010000000101
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	UJPI010000000101
20	VPJP010000000602	Streaming of content free with advertising	Open	Commercial	Free	Individual	Individual	Time-synchronized Forced Viewing	Reserved	Streaming	UJPI010000000101
21	VPJP010000000603	Giveaways	Open	Commercial	Free	Individual	Individual	Giveaway Model	Reserved	Download, Reuse, Copy	UJPI010000000101
22	VPJP010000000604	Coupons (discount points)	Open	Commercial	Free	Individual	Individual	Coupon Model	Reserved	Download, Reuse, Copy	UJPI010000000101
23	VPJP010000000605	Privacy information disclosure	Open	Commercial	Free	Individual	Individual	Advertising Model	Reserved	Streaming	UJPI010000000101
24	VPJP010000000701	Copying 9 times with unlimited moving	Open	Commercial	Fee-based	Individual	Individual	No Sponsor	Reserved	Fixed Broadcast Delivery, Reuse, Move, Copy	UJPI010000000101
25	PGJP010000000101	Subscription games	Open	Commercial	Fee-based	Individual	Individual	No Sponsor	Reserved	Download	UJPI010000000101
26	PSJP010000000101	Software rental	Open	Commercial	Fee-based	Individual	Individual	No Sponsor	Reserved	Download	UJPI010000000101

Table II.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 II.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 II.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 II.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 II.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			

Appendix III

Background to rights information interoperability

(This appendix does not form an integral part of this Recommendation.)

III.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 service and content protection (SCP) systems have been offered, and various distribution models such as "superdistribution" have been proposed. Even though the technology and infrastructure to support digital distribution are now in place, no mechanisms or rules have been established for flexible digital distribution. Such flexible digital distribution would allow easy exchange of content based on individual commitments between content creators and consumers. 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.

Taking movies as a typical case, content creation is generally a group effort, and responsibilities are shared amongst various individuals. As a result, the financial and personal rights related to the final content, and the compensation that must be shared among those involved, are uncertain. Since no technology has yet been established for managing usage fees based on the volume of content consumed, 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 that possible. Consequently, appropriate permission commitments are not shown and all involved must accept lost opportunities. In addition, the development of technology for the fast-growing market of mobile phones and simple terminals that makes content available to consumers is progressing without interoperability across different service providers. Paradoxically, this results in more inconvenience for the consumer. Moreover, while SCP 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 is technologically possible to improve the user experience.

Rights information interoperability (RII) makes it possible to study measures to resolve these problems from two standpoints. The first standpoint is that of engineering – building the infrastructure for a next generation of digital information distribution systems by developing technology that achieves a combination of interoperability and convenience for the consumer. The second is a legal one – 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 specifies an ideal system that merges the two together and helps make interoperability a reality for groups of existing SCP systems scattered throughout the world (Figure III.1).

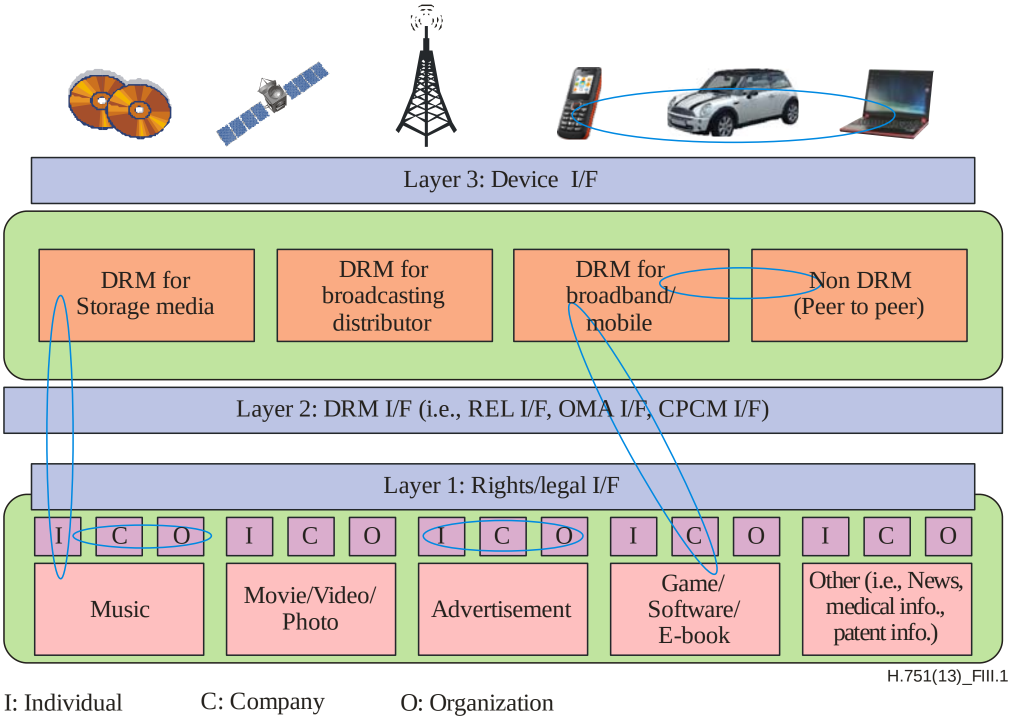

Layer 3: Device I/F
DRM for Storage media
DRM for broadcasting distributor
DRM for broadband/ mobile
Non DRM (Peer to peer)
Layer 2: DRM I/F (i.e., REL I/F, OMA I/F, CPCM I/F)
Layer 1: Rights/legal I/F
I
C
O
Music
Movie/Video/ Photo
Advertisement
Game/ Software/ E-book
Other (i.e., News, medical info., patent info.)
H.751(13)_FIII.1
I: Individual
C: Company
O: Organization

Figure III.1 – Concept: rights information interoperability

III.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 legal prosecution when rights are infringed.

The action of granting digital rights permissions is an action that forms an agreement between (multiple) holders who hold declared rights and (multiple) holders who do not have rights according to copyright law, but who must 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 should include 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. 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 one arrives at the limitations of the law. What compensates for this is technology.

Specifically:

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

Component 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 is synonymous with management of continually updated digital rights permissions information. Components a) and b) above ensure that, as a minimum, all of the rights defined in the existing copyright law are expressed. It shall also assure future extensibility, meaning that it will be technologically possible to express any new, future agreement that it is acceptable to enable specific content consumption services.

III.2.1 Example

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, suppose that rights holder company H, who grants the rights permissions for film content A, enters into a business-to-business content usage license agreement with distributor U, who runs a downloading business; in this situation, it is not possible to capture all of the specific service formats in advance. In particular, if one imagines that services that are not yet known will be enabled in the future, the employees responsible for legal affairs must 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 specific conditions, 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 supported by technology in order to legally manage the forms of consumption targeted to more finely differentiated final consumers.

Several situations may arise:

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

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

   1) cases where it is possible for permissions to be obtained after consumption; and

   2) cases where it is not possible for permissions to be obtained after consumption.

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

Appendix IV

Two basic technologies for enabling RII

(This appendix does not form an integral part of this Recommendation.)

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

IV.1.1 General

In this digital age, digital technology and networked environments are used, and there exists a wide variety of content, content creators and users. 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. RII establishes code language technology that simplifies as much as these pieces of rights-related metadata possible and expresses their common elements.

IV.1.2 Rights related metadata and simple tag ID code

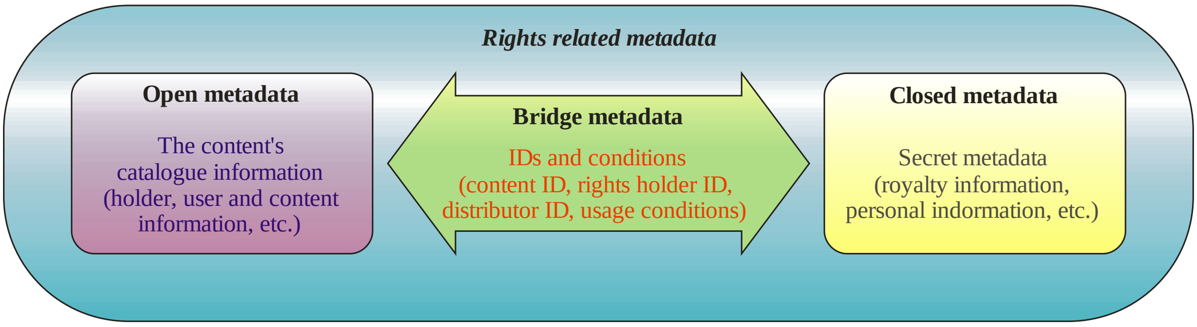
Rights related metadata is a general term for information surrounding and related to an object of consumption and enjoyment (film, music, photos, etc.), which is called content or a product, etc.

Rights related metadata can be divided roughly into three types; the whole relationship is explained in Figure IV.1:

a) Open metadata: This metadata type comprises metadata that is made open to the public. Examples of open metadata include the product name, official author, etc.

b) Closed metadata: This metadata type comprises metadata that is shared only amongst the parties related to the transaction. Examples of closed metadata include the author's real name, royalty rates, 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) for joint management purposes.


Rights related metadata
Open metadata
The content's catalogue 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 indormation, etc.)

H.751(13)_FIV.1

Figure IV.1 – Common semantics of metadata

Figure IV.2 shows a practical usage example of shared IDs in bridge metadata. As various rights holders are involved with content such as audiovisual work, the consolidation of name-list information is needed for determining the actual rights holders and the royalties that are due to them.

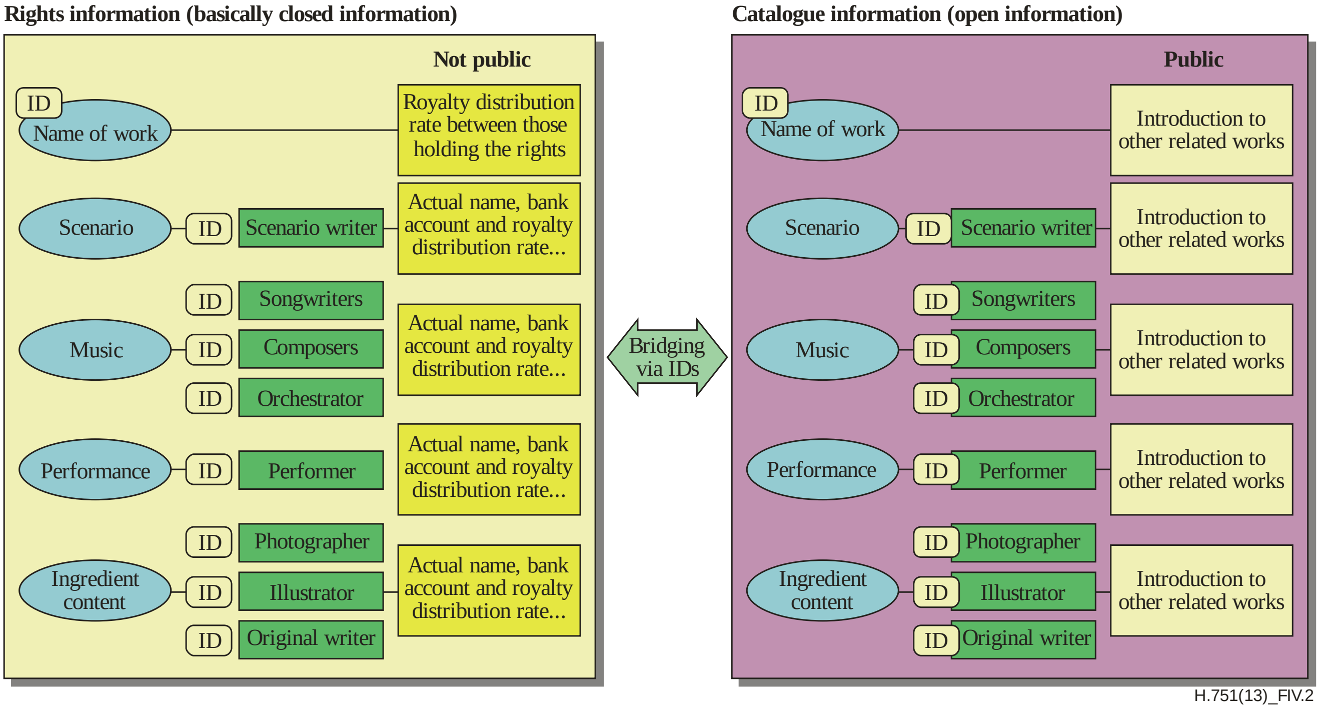

Rights information (basically closed information)
Not public
ID
Name of work
Royalty distribution rate between those holding the rights
Scenario
ID
Scenario writer
Actual name, bank account and royalty distribution rate...
Music
ID
Songwriters
ID
Composers
ID
Orchestrator
Actual name, bank account and 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
Catalogue 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
H.751(13)_FIV.2

Figure IV.2 – Need for information consolidation for content distribution

This name-list information is necessary both in the context of "closed information", information that needs to be shared (e.g., for contracts purposes) only amongst content and rights holders, and of "open information" (e.g., catalogue information for the purpose of gaining a deeper knowledge regarding the content in question) between content holders and users or users and consumers.

For this reason, it is effective to carry out information bridging for both parties, using Holder Rights IDs as a means for association.

IV.1.3 Shared ID system

In order to facilitate content distribution from here on out, it is essential that IDs be commonly used through databases to identify contents, rights holders and users, and that mechanisms be improved for access from the outside. Because of this, a shared ID system is necessary. The assignment of IDs shared between the concerned 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 network. [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 [b-WIPO ST.3] two-letter country codes.

For example, film content created inside Japan is expressed by VPJP, where "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

Clause 5.5.5 of [IEC 62227] specifies the structure of the container carrying the rights holder ID on shared ID system. This ID 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

Clause 5.5.6 of [IEC 62227] specifies the structure of the container carrying the user ID on shared ID system. This ID commonly identifies the distributor, broadcaster, end consumer, device owned by the consumer and service group used by the consumer, using the content identified using the above content ID.

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

IV.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.

IV.2.2 Classification

The classification is comprised of seven items defined from a particular 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 business-to-business rights processing.

IV.2.3 Limit components

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

a) Personal Limit Component:

- Compilation permission (free, by product, by album, compilation within the same artist, compilation within the same company);

NOTE – When using group content distribution services, it is possible to bundle and group content in ways that go beyond content genres.

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 (cf. clause 5.10.4.4 of [IEC 62227], storage_media_type field);

d) Compression Format Standard (cf. clause 5.9.3.6 of [IEC 62227], transcode type);

e) Bit Rate Limit Component (cf. clause 5.9.3.7 of [IEC 62227], maximum transcode rate);

f) Lifetime (Life Control) Limit Component (free, count limit, time period limit, expiration limit);

g) Security Limit Component (watermark, SCP, rights report).

IV.3 Common semantics for RII

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

Bridge metadata are the common semantics for RII, which are organized into three groups:

– "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.

These common semantics for RII are illustrated in Figure IV.3.

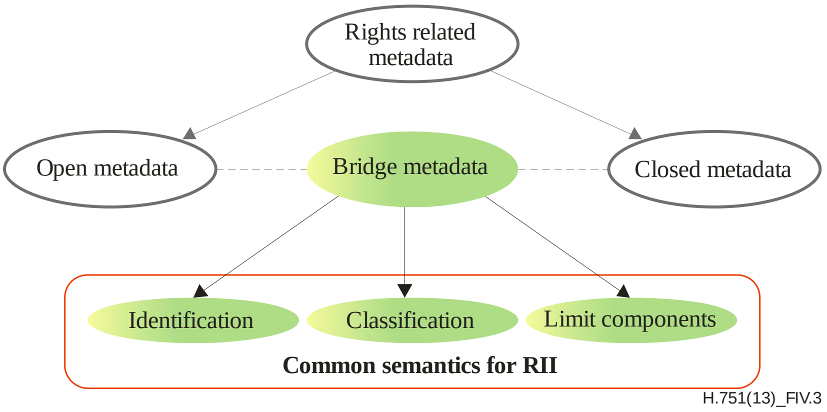


Figure IV.3 – Common semantics for RII

IV.4 Core elements and common semantics for RII

Each component for RII is divided into core elements that specify the details of bridge information. Figure IV.4 shows core elements and common semantics for RII.

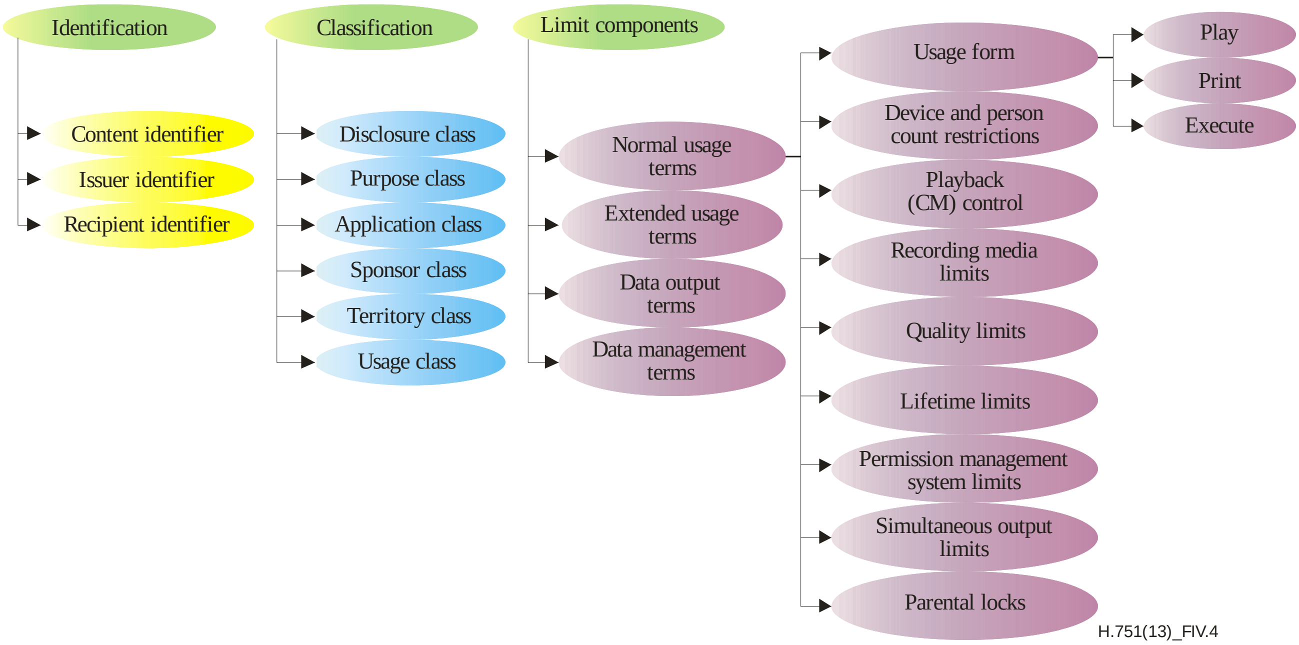


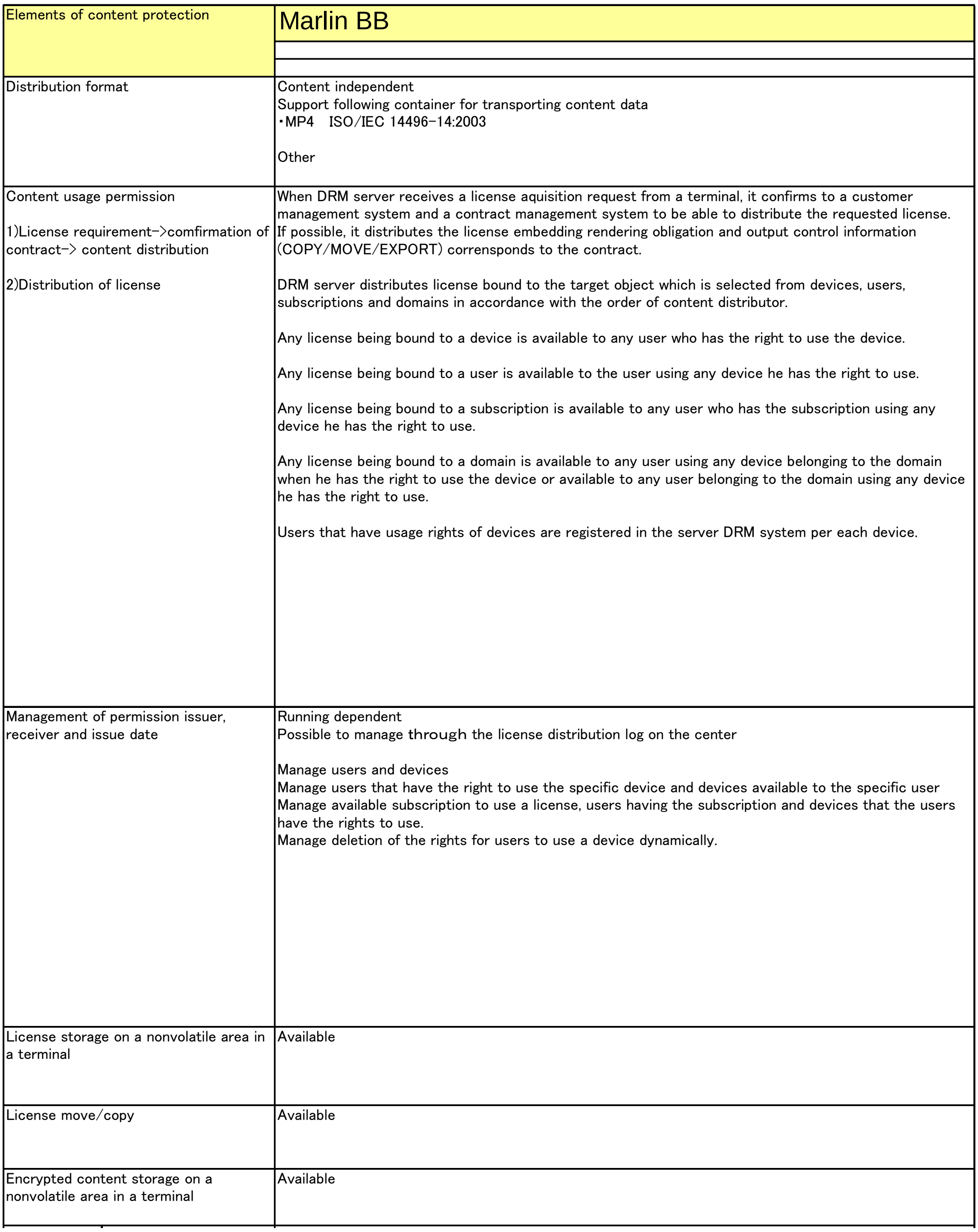
Figure IV.4 – Core elements and common semantics for RII

Appendix V

Rights information metadata elements corresponding to existing SCP systems

(This appendix does not form an integral part of this Recommendation.)

V.1 SCP1



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->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 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. 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 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 per 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

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 being transported from 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 being issued by a certificate authority authorized by MTMO. RSA-DSA (1024bit/2048bit key) with SHA256 Revocation lists of client DRM and server DRM are available..
Communication protection between DRMs		Concealment of communication data RSA 1024bit,2048bit RSA 1.5 | RSA-OAEP AES 128bit Check a tamper of communication data RSA – SHA 1 | RSA – SHA 256 Secret data concealment between DRM system nodes RSA 1024bit,2048bit RSA 1.5 | RSA-OAEP AES 128bit Check a falsification of secret data between DRM system nodes. HMAC – SHA1 RSA – SHA1 | RSA – SHA256

V.2 SCP System 2, with 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 a rights to get the requested license. If possible, it distributes the license embedding playback control information 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		Following elements are available to be specified a playback control information per 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		
Authentication of DRM systems		Authentication of client DRM and server DRM makes by using a public key certificate which is issued by authentication center which is authorized by MTMO. EC-DSA (224bit key) with SHA256 Run revocation lists. Client DRM can be revoked per each device. Server DRM can be revoked per license distribution server.
Communication protection between DRMs		EC-DH (224 bti key) + EC-DSA (224 bit key) + AES (128 bit key) + SHA 256

V.3 SCP System 3, with Download license, EXTRACT with Direct Key Delivery, Download

Elements of content protection		Marlin IPTV-ES
		Download license
		EXTRACT with Direct Key Delivery
Distribution format		Download
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 corresponds to the contract.
Management of permission issuer, receiver and issue date		Running dependent It is possible to manage as a license distribution log on the center
License storage on a nonvolatile area in a terminal		Available
License move/copy		Not available
Encrypted content storage on a nonvolatile area in a terminal		Available
Content usage control	Playback period	NotBefore, NotAfter
	Digital copy control information	DigitalRecordingControlData 11 : Copy never * Follow APS Control Data for analog output
	Serial interface output control	CopyControlType 01 : Serial interface encoding output
	Analog output copy control	APS Control Data 00:Copy free 01:Pseudo-synchronizing pulse 10:Pseudo-synchronizing pulse + two line inverted burst 11:Pseudo-synchronizing pulse + four line inverted burst
	Video quality control information	ImageConstraintToken 1 : unbound
	Decoded content data retention mode	RetentionMode 0 : Permit retention
	Decoded content data retention state	RetentionState 111 : 90 minuite
	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 (128bit key) + SCTE 52
Authentication of DRM systems		Authentication of client DRM and server DRM makes by using a public key certificate which is issued by authentication center that authorized in MTMO. EC-DSA (224bit key) with SHA256 Run revocation lists. Client DRM can be revoked by per each devices. Server DRM can be revoked by per license distribution server.
Communication protection between DRMs		EC-DH (224 bti key) + EC-DSA (224 bit key) + AES (128 bit key) + SHA 256

V.4 SCP System 4, with 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 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 minuite
	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 (128bit key) + SCTE 52
Authentication of DRM systems		Authentication of client DRM and server DRM makes by using a public key certification which is issued by authentication center which authrized by MTMO. EC-DSA (224bit key) with SHA256 Run revocation lists. Client DRM can be revoked per each device. Server DRM can be revoked per license distribution server.
Communication protection between DRMs		EC-DH (224 bti key) + EC-DSA (224 bit key) + AES (128 bit key) + SHA 256

V.5 SCP System 3, with Download license, EXTRACT with Direct Key Delivery, Download

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, 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 are only valid for one generation. It is not possible second generation copy/move) 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.
		A playback control information of broadcasting data succeed ones of terrestrial broadcast and BS broadcast playback control information.
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.
Content usage control	Playback period	NotBefore, NotAfter ＊ There is offset period which is possible to be updated license period from NotAfter.
	Digital copy control information	It succeeds 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 (128bit key) + SCTE 52
Authentication of DRM systems		Authentication of client DRM and server DRM makes by using a public key certification which is issued in authentication center which is authorized by MTMO. EC-DSA (224bit key) with SHA256 Run revocation lists. Client DRM can be revoked per each device. Server DRM can be revoked per license distribution server.
Communication protection between DRMs		EC-DH (224 bti key) + EC-DSA (224 bit key) + AES (128 bit key) + SHA 256

V.6 SCP System 4, with Download license, EXTRACT with Direct Key Delivery, VOD streaming

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, 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 are only valid for one generation. It is not possible second generation copy/move) 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 per 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.
Content usage control	Playback period	NotBefore, NotAfter ＊ There is offset period which is possible to be updated 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 minuite
	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 (128bit key) + SCTE 52
Authentication of DRM systems		Authentication of client DRM and server DRM makes by using a public key certification which is issued in authentication center which is authrized by MTMO. EC-DSA (224bit key) with SHA256 Run revocation lists. Client DRM can be revoked per each device. Server DRM can be revoked per license distribution server.
Communication protection between DRMs		EC-DH (224 bti key) + EC-DSA (224 bit key) + AES (128 bit key) + SHA 256

V.7 SCP System 5, with, Broadcast license, EXTRACT with IndirectKey Delivery license, Terrestrial re-distribution/BS(Broadcasting satellite) re-distribution

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 a rights to get a requested license. If possible, it distributes the license embedding playback control information 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		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 minuite
	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 (128bit key) + SCTE 52
Authentication of DRM systems		Authentication of client DRM and server DRM makes by using a public key certification which is issued in authentication center which is authorized by MTMO. EC-DSA (224bit key) with SHA256 Run revocation lists. Client DRM can be revoked per each device. Server DRM can be revoked per license distribution server.
Communication protection between DRMs		EC-DH (224 bti key) + EC-DSA (224 bit key) + AES (128 bit key) + SHA 256

V.8 SCP System 6, with Broadcast license, EXTRACT with DirectKey Delivery license, IP multicast

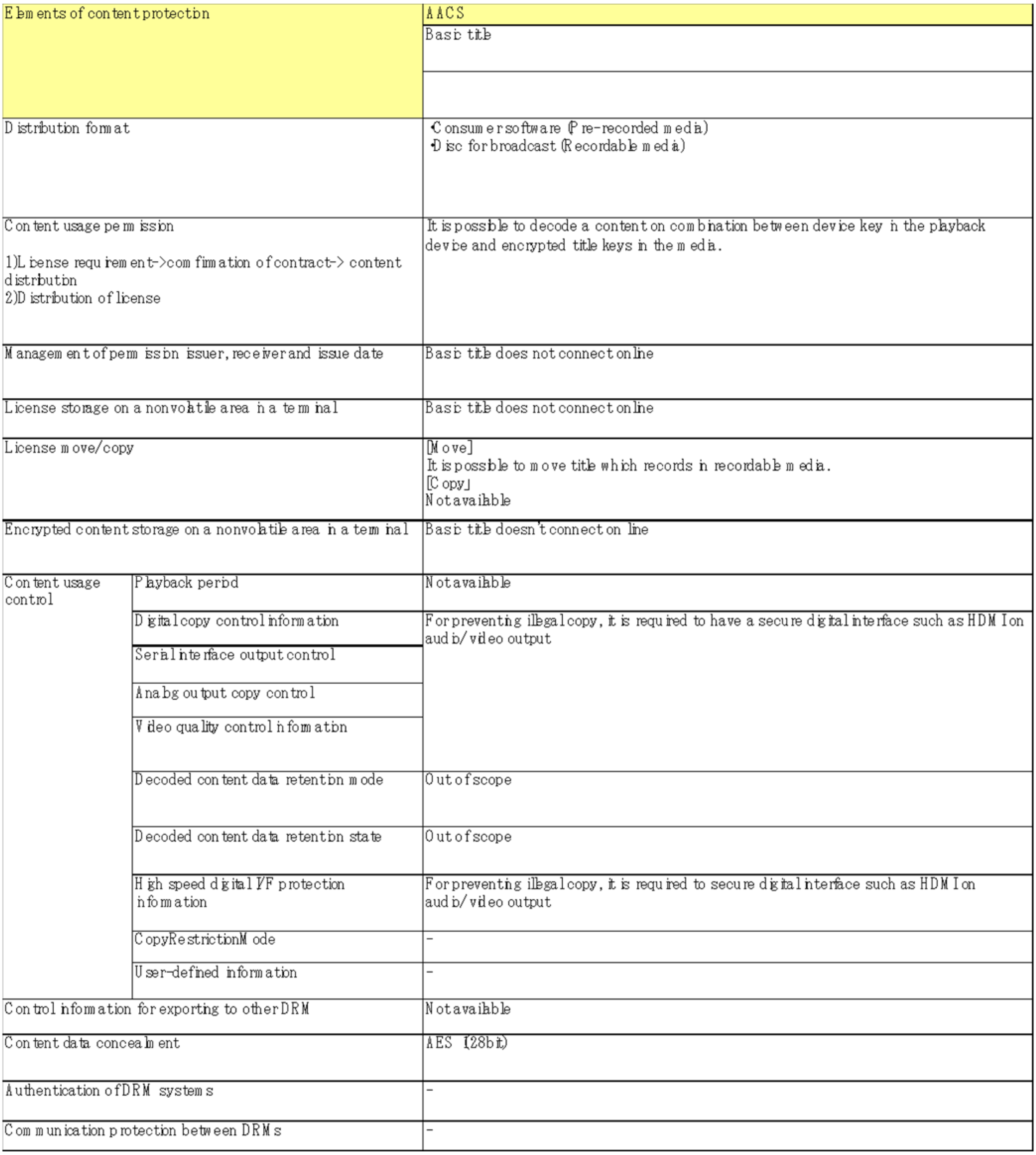
Elements of content protection		WM-DRM
Distribution format		Download
Content usage permission 1)License requirement->comfirmation of contract-> content distribution 2)Distribution of license		A protected content encrypt by using a key which is encrypted in license and relate to a specific terminal. Both 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, 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	Content provider is possible to combine a following constraint alternatively. · As following calendar date, a license can be valid or not. · A license can be revoked after specific time period from first use. · A license can be revoked after specific time period from first install to PCs or devies. As following a playback count condition, a license can be revoked.
	Digital copy control information	<Audio output protection> 1. Non protection 2. Obfuscation（Protect by Secure Audio Path. Permit digital output) Obfuscation 3. Encryption-Low（Protect by Secure Audio Path. Deny digital output) 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 a 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 bit) which use both of ECB and CTR mode
Authentication of DRM systems	By linking each terminal to server indentically, system security becomes high. If there are terminals who are infringed security, they can be identified in licensing process and revoked. It is possible to revoke by a license server.
Communication protection between DRMs	As a network device requirement, there are following encryption technologies. ・2048 bit RSA encryption that can store and protect a private key ・SHA-256 that has 2048 bit RSA encryption and AES OMAC1

V.9 SCP System 9, for mobile IPTV terminal

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 cornensponds to the contract.
Management of permission issuer, receiver and issue date		Content issuer, Rights issuer and DRM agent is defined and it is possible to be managed by rights holder.
License storage on a nonvolatile area in a terminal		Available
License move/copy		If these are the devices in the same domain, content and rights object can be shared. If these are the devices which belong to no common domain, only content can be copied.
Encrypted content storage on a nonvolatile area in a terminal		Available
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)not defined about the way to transport from OMA DRM to other protection mechanisms 3)Permission and restriction of 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(128bit) + CBC 0x2…AES(128bit) + CTR
Authentication of DRM systems		A terminal has own secret/public key and certificate. In a certificate, there are maker name, device type, software version, serial number and determine whether rights holder trust a terminal or not by the certificate.
Communication protection between DRMs		Rights information is protected by rights information acquisition protocol.

V.10 SCP System 10, for recording media (e.g., DVD), 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 on combination between device key in the playback device and encrypted title keys in the media.
Management of permission issuer, receiver and issue date		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 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	For preventing illegal copy, 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 (128bit)
Authentication of DRM systems		-
Communication protection between DRMs		-

V.11 SCP System 11, for recording media (e.g., DVD), 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 authentication server, the content is decoded by 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 has Cacheable attribute are available
License move/copy		[move] Title recorded in recordable medhia can be moved. [Copy] It is managed by managed copy. It is required to authenticate online
Encrypted content storage on a nonvolatile area in a terminal		<AACS Network Download Content> Never Store。Available to record on the media such as BD <AACS On-line Enabled Content> Available to the title that has Cacheable attribute <AACS Streamed Content>
Content usage control	Playback period	Only titles that have 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(128bit)
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

Appendix VI

Examples of media formats

(This appendix does not form an integral part of this Recommendation.)

MPEG-1, MPEG-2, ITU-T H.264, ITU-T H.265, JPEG, GIF, PNG, Linear PCM, AAC, MP3.

Bibliography

[b-ITU-T F.902] Recommendation ITU-T F.902 (1995), *Interactive services design guidelines*.

[b-ITU-T J.148] Recommendation ITU-T J.148 (2003), *Requirements for an objective perceptual multimedia quality model*.

[b-ITU-T M.1400] Recommendation ITU-T M.1400 (2006), *Designations for interconnections among operators' networks*.

[b-ITU-T X.509] Recommendation ITU-T X.509 (2005), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for open systems interconnection for CCITT applications*.

[b-ITU-T X.1191] Recommendation ITU-T X.1191 (2009), *Functional requirements and architecture for IPTV security aspects*.

[b-ITU-T Y.1901] Recommendation ITU-T Y.1901 (2009), *Requirements for the support of IPTV services*.

[b-ITU-T Y.1910] Recommendation ITU-T Y.1910 (2008), *IPTV functional architecture*.

[b-IEC 62636] IEC Technical Report 62636 (2009), *Multimedia home server systems – Implementation of digital rights permission code*.

[b-WIPO ST.3] World Intellectual Property Organization (WIPO) Standard ST.3 (2011), *Recommended standard on two-letter codes for the representation of states, other entities and intergovernmental organizations*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	**Audiovisual and multimedia systems**
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2013