# DRM Rights Expression Language V2.0

Candidate Version 2.0 – 10 Dec 2004

**Open Mobile Alliance**

OMA-DRM-REL-V2_0-20041210-C

# Contents

# Figures

# 1. Scope

Open Mobile Alliance (OMA) specifications are the result of continuous work to define industry-wide interoperable mechanisms for developing applications and services that are deployed over wireless communication networks.

The scope of OMA "Digital Rights Management" [DRM-v2] is to enable the consumption of digital content in a controlled manner. The content is consumed on authenticated devices per the usage rights expressed by the content owners. The OMA DRM work addresses the various technical aspects of this system by providing appropriate specifications for content formats, protocols, and the rights expression language.

The scope for this specification is to define the rights expression language used to describe the rights over DRM Content.

It addresses requirements such as enabling preview, i.e., test-driving, of Content, possibly prior to purchasing, expressing a range of different permissions and constraints. It provides a concise mechanism for expressing rights over DRM Content. It is independent of the Content being distributed, the mechanism used for distributing the Content, and the billing mechanism used to handle the payments.

# 2. References

## 2.1 Normative References


**[ISO8601]** "Representations of dates and times", ISO (International Organization for Standardization), URL:http://www.iso.ch/

**[ODRL]** "Open Digital Rights Language (ODRL)", Version 1.1, 8 August 2002, URL:http://odrl.net/1.1/ODRL-11.pdf or URL:http://www.w3.org/TR/odrl/

**[RFC2119]** "Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997, URL:http://www.ietf.org/rfc/rfc2119.txt

**[RFC2396]** "Uniform Resource Identifiers (URI): Generic Syntax ", T. Berners-Lee, R. Fielding, L. Masinter, August 1998, URL:ftp://ftp.isi.edu/in-notes/rfc2396.txt

**[XML]** "Extensible Markup Language (XML) 1.0 (Second Edition)", W3C Recommendation 6 October 2000, URL:http://www.w3c.org/TR/2000/REC-xml-20001006/

**[XMLENC]** "XML Encryption Syntax and Processing", W3C Candidate Recommendation 10 December 2002, URL:http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/

**[XMLSchema]** "XML Schema Part 2: Datatypes", W3C Recommendation 2 May 2001, URL:http://www.w3.org/TR/xmlschema-2/

**[XMLSIG]** "XML Signature Syntax and Processing", W3C Recommendation 12 February 2002, URL:http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/


## 2.2 Informative References


**[DRM-v2]** "Digital Rights Management", Open Mobile Alliance™, OMA-DRM-DRM-V2_0, URL:http://www.openmobilealliance.org/

**[DRMARCH-v2]** "OMA DRM Architecture Overview", Open Mobile Alliance™, OMA-DRM-ARCH-V2-0, URL:http://www.openmobilealliance.org/

**[DRMCF-v2]** "DRM Content Format", Open Mobile Alliance™, OMA-DRM-DCF-V2_0, URL:http://www.openmobilealliance.org/

# 3. Terminology and Conventions

## 3.1 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

All sections and appendixes, except “Scope” and “Introduction”, are normative, unless they are explicitly indicated to be informative.

## 3.2 Definitions

| | |
|---|---|
| **Constraint** | A restriction on the Permission over DRM Content. |
| **Composite Object** | A Media Object that contains one ore more Media Objects by means of inclusion e.g. DRM messages, zip files. |
| **Content** | One or more Media Objects. |
| **DRM Agent** | The entity in the Device that manages Permissions for Media Objects on the Device. |
| **DRM Content** | Media Objects that are consumed according to a set of Permissions in a Rights Object. |
| **DRM Time** | A secure, non-user changeable time source. The DRM Time is measured in the UTC time scale. |
| **Media Object** | A digital work e.g. a ringing tone, a screen saver, a Java game or a Composite Object. |
| **Permission** | Actual usage or activities allowed (by the Rights Issuer) over DRM Content. |
| **Rights Issuer** | An entity that issues Rights Objects to OMA DRM Conformant Devices. |
| **Rights Object** | A collection of Permissions, Constraints, and other attributes which define under what circumstances access is granted to, and what usages are defined for, DRM Content. All OMA DRM Conformant Devices must adhere to the Rights Object associated with DRM Content. |

## 3.3 Abbreviations

| | |
|---|---|
| **AES** | Advanced Encryption Standard |
| **CEK** | Content Encryption Key |
| **DCF** | DRM Content Format |
| **DRM** | Digital Rights Management |
| **DTD** | Document Type Definition |
| **MIME** | Multipurpose Internet Mail Extensions |
| **OMA** | Open Mobile Alliance |
| **OMNA** | Open Mobile Naming Authority |
| **ODRL** | Open Digital Rights Language |
| **REL** | Rights Expression Language |
| **REK** | Rights Encryption Key |
| **SHA-1** | Secure Hash Algorithm |
| **SMS** | Short Message Service |
| **WAP** | Wireless Application Protocol |
| **XML** | Extensible Markup Language |

# 4. Introduction

Digital Rights Management [DRM-v2] defines the mechanisms to deliver DRM Content and Rights Objects to a consuming device. Rights are used to specify the access a consuming device is granted to DRM Content. The Rights Expression Language (REL) defined in this document specifies the syntax and semantics of rights governing the usage of DRM Content based on the Open Digital Rights Language [ODRL].

This specification defines

1. A subset, i.e., a mobile profile, of ODRL, and
2. A data dictionary defining additional permissions and constraints beyond those provided by ODRL.

DRM Content is consumed according to the specified rights. Therefore, the value is in the rights and not in the Content itself. Rights Objects are specified so that they only become usable on authorized devices.

## 4.1 Goals

The goal of this specification is to define a REL taking into account the special requirements and characteristics of the mobile domain to express consumption rights over DRM Content. Some of the specific goals include

- Light-weight and simple way of expressing rights
- Lowering the entrance barrier for content providers and other players to adopt DRM technologies
- Suitable for specifying rights independently of the content type
- Suitable for specifying rights independently of the transport mechanism
- Enable specification of right to preview, i.e., test-drive, DRM Content enabling users to experience the Content first hand, possibly prior to purchasing it
- Enable specification of constraints to restrict permissions to the number of times Content can be accessed, and time limits and intervals during which Content can be accessed.

## 4.2 Non-goals

OMA Digital Rights Management release 2.0 [DRM-v2] defines a more comprehensive DRM system than release 1.0. The following are not goals of the REL:

- To govern the distribution of DRM Content is not a goal of the REL. Since DRM Content is encrypted it is useless without the corresponding Rights Object, and thus there is no need for the REL to explicitly govern distribution.
- To govern device management permissions such as ‘install’, ‘uninstall’, ‘delete’, etc. Freeing memory capacity on the device is an intrinsic right that every user has to his/her device.

# 5. Structure

This section describes the structure of the rights expression language. The REL is defined as a mobile profile of ODRL v1.1 [ODRL]. Rights are the collection of permissions and constraints defining under which circumstances access is granted to DRM Content. The structure of the rights expression language enables the following functionality:

1. Metadata such as version and content ID
2. The actual rights specification consisting of
    a. Linking to and providing protection information for the content, and
    b. Specification of usage rights and constraints

Models are used to group rights elements according to their functionality, and thus enable concise definition of elements and their semantics. The following models are used throughout this specification:

- Foundation model
- Agreement model
- Context model
- Permission model
- Constraint model
- Inheritance model
- Security model

The rights expression language is defined as a mobile profile, i.e., a subset, of ODRL. Section 5.8 specifies how to handle ODRL models and elements that are not used in this specification.

## 5.1 Foundation Model

The foundation model constitutes the basis for rights. It contains the <rights> element bringing together Meta information and agreement information. The foundation model serves as the starting point for incorporating the agreement model and the context model.

### 5.1.1 Element <rights>

| | |
|---|---|
| Element | <!ELEMENT o-ex:rights (o-ex:context, o-ex:agreement)> |
| Semantics | The <rights> element is the root element of all Rights Objects defined according to this specification. It contains the mandatory <context>, and <agreement> elements linking assets to corresponding permissions. |

# 5.2 Agreement Model

The agreement model expresses the Rights that are granted over an DRM Content. It consists of the <agreement> element connecting a set of Rights with the corresponding DRM Content specified with the <asset> element. The agreement model incorporates the permission model and the security model.

## 5.2.1 Element <agreement>

| | |
|---|---|
| Element | <!ELEMENT o-ex:agreement (o-ex:asset+, o-ex:permission*)> |
| Semantics | The <agreement> element specifies the rights granted over the corresponding DRM Content. It contains one or more <asset> elements and zero or more <permission> elements. |

## 5.2.2 Element <asset>

| | |
|---|---|
| Element | <!ELEMENT o-ex:asset (o-ex:context?, o-ex:inherit?, o-ex:digest?, ds:KeyInfo?)> |
| Semantics | The <asset> element specifies the identity of the DRM Content governed by the containing <agreement> element via the <context> child element.<br><br>The optional <inherit> element instructs the DRM Agent to apply the rights from the inherited Rights Object, specified in the <inherit> element context, to this asset. Note that the <KeyInfo> element SHOULD be omitted if the Rights Object functions as a parent Rights Object in the inheritance case.<br><br>The optional <digest> element provides integrity protection for the reference to the DRM Content.<br><br>The optional <KeyInfo> element provides the functionality to access the DRM content if granted the rights to do so.<br><br>The <asset> element enables expression linking via its “id” and “idref” attributes. This enables reuse of Permissions defined for one asset, for other assets inside the same Rights Object. When the <asset> element is contained in a <permission> element, it MUST contain an “idref” attribute, and MUST be empty, i.e., all its optional child elements MUST be omitted. |

### 5.2.2.1 Attribute “id”

| | |
|---|---|
| Attribute | <!ATTLIST asset o-ex:id ID #IMPLIED> |

| | |
|---|---|
| Semantics | The “id” attribute is the identifier of the <asset> element. It uniquely identifies each <asset>.<br><br>The “id” attribute MUST only be used if the <asset> element is a child element of the <agreement> element. It MUST NOT be used if the <asset> element is child element of the <permission> element.<br><br>It SHOULD be omitted if there is no reference to the <asset> element from elsewhere in the same Rights Object.<br><br>The “id” attribute MUST be unique within the Rights Object, and it MUST NOT be the same as the Content ID specified in the <uid> element. |

#### 5.2.2.2 Attribute “idref”

| | |
|---|---|
| Attribute | <!ATTLIST asset o-ex:idref IDREF #IMPLIED> |
| Semantics | The “idref” attribute refers to the identifier of the <asset> element.<br><br>The “idref” attribute MUST only be used if the <asset> element is a child element of the <permission> element. It MUST NOT be used if the <asset> element is child element of the <agreement> element.<br><br>It SHOULD be omitted if it does not reference another <asset> element inside the same Rights Object. |

## 5.3 Context Model

The context model provides Meta information about the rights. It augments the foundation model, the agreement model, and the constraint model by expressing additional information.

The <context> element is used in the <rights> element, in the <asset> element, and in the <individual> element. As the model’s name already indicates, the semantics of its child elements depend on the context in which it occurs in the rights object.

### 5.3.1 Element <context>

| | |
|---|---|
| Element | <!ELEMENT o-ex:context (o-dd:version?, o-dd:uid*)> |
| Semantics | The <context> element contains the optional <version>, and <uid> elements. As the name already indicates, it provides context sensitive information for use within the context of its parent element.<br><br>The semantics of its child elements depend on the parent element in which the <context> element is used. These are different if the <context> element is a child element of the <rights>, <asset>, <individual>, <system>, or <inherit> element. Please see the corresponding descriptions of the individual child elements.<br><br>A <context> element MUST NOT contain more than one <uid> element unless the <context> element is contained in the <individual> or <system> element. |

### 5.3.2 Element <version>

| | |
|---|---|
| Element | <!ELEMENT o-dd:version (#PCDATA)> |
| Semantics | The <version> element SHOULD only be used if its parent <context> element is included in the <rights> element or the <system> element.<br><br>If its parent <context> element is included in the <rights> element, it then specifies the version of the Rights Object. For this specification its content MUST then be "2.0" (without quotes).<br><br>If its parent <context> element is included in the <system> element, it then specifies the version of the other DRM system or content protection scheme to which the DRM Content and the Rights Objects will be exported. |

### 5.3.3 Element <uid>

| | |
|---|---|
| Element | <!ELEMENT o-dd:uid (#PCDATA)> |
| Semantics | If its parent <context> element is included in the <rights> element, the <uid> element constitutes the Rights Object's identifier.<br><br>If its parent <context> element is included in the <asset> element, the <uid> element specifies the content identifier of the corresponding DRM Content. It contains the ContentURI value of the DCF[[DRMCF-v2]]. The format used for the value MUST conform to [RFC2396]. If the <asset> element is part of a parent Rights Object (see section 5.6) it SHOULD NOT contain the content identifier of an actual DCF, but contain a "virtual" UID denoting, for example, a subscription.<br><br>If its parent <context> element is included in the <individual> element, the <uid> element(s) specifies the individual to which the content is constrained. A <uid> element can contain an IMSI related to the end user's subscription or a WIM identifier, thus effectively binding the consumption of content to the individual.<br><br>In the case of IMSI binding, the format of its value MUST be "IMSI:x" (without the quotes) where x is replaced by the IMSI to which content is bound. If content is bound to multiple IMSI values, then multiple <uid> elements MUST be used.<br><br>In the case of WIM binding, the format of its value MUST be "WIM:x" (without the quotes) where x is replaced by the PKC_Id of the WIM to which content is bound.<br><br>If its parent <context> element is included in the <system> element, the <uid> element specifies the target system to which the logically integral unit of DRM Content and the Rights Object(s) are allowed to be exported / transiently rendered to. Its value MUST be the name of the target system(s) as defined by OMNA.<br><br>If the <export> permission is granted to more than one target system, then these are enumerated by using multiple <uid> elements. In this case, the <count> constraint applies to the combined export transactions of all target systems.<br><br>The only instances when a <context> element MAY contain more than one <uid> element is when the <context> element is contained in an <individual> or <system> element.<br><br>If its parent <context> element is included in the <inherit> element, the <uid> element specifies the UID of the <asset> element in the parent Rights Object from where to inherit Permissions and Constraints (see section 5.6). |

## 5.4 Permission Model

The permission model augments the agreement model. It facilitates the expression of permissions over assets by specifying the access granted to a device. The permission model incorporates the constraint model allowing fine-grained consumption control of DRM Content.

The set of permissions comprises <play>, <display>, <execute>, <print>, and <export>. Usage of the DRM Content MUST only be granted according to the permissions explicitly specified by the corresponding Rights Object(s). A permission that does not contain a <constraint> child element is unconstrained and access according to the respective permission element(s) MUST be granted.

Note that the REL only specifies consumption and export rights and not management rights, e.g., install, uninstall, delete, or distribution rights. This is made possible by the separation of DRM Content and Rights Objects (although DRM Content and Rights Objects may be delivered together) freeing the REL from unnecessary complexity and overhead. Content can be stored; however, it can only be accessed if a corresponding Rights Object is available.

Similarly, encrypted content can be super-distributed without unnecessarily complicating the REL; no separate distribution permissions are necessary, since DRM Content without the decryption key is of no value.

The DRM Agent MUST ignore unknown or unsupported permission elements. The DRM Agent MUST NOT grant alternative, not explicitly specified rights to access Content instead. Known and supported permission elements defined by the same Rights Object MUST remain unaffected and the DRM Agent MUST grant access according to those. A Permission that is not granted due to unknown or unsupported constraints (section 5.5) MUST NOT affect the granting of other permissions.

### 5.4.1 Element <permission>

| Element | <!ELEMENT o-ex:permission (o-ex:constraint?, o-ex:asset*, o-dd:play?, o-dd:display?, o-dd:execute?, o-dd:print?, oma-dd:export?)> |
|---|---|

| | |
|---|---|
| Semantics | The <permission> element contains an optional <constraint> element, zero or more <asset> elements and a set of optional permissions specifying the rights over a piece of Content, such as <play>, <display>, <execute>, <print>, and <export> permission elements.<br><br>The <constraint> element is the top-level constraint. As a sibling element to other permission elements such as <play>, <display> it applies to all sibling permission elements inside the same <permission> element. The DRM Agent MUST honor the top level constraint in addition to honoring possible constraints specified as a child element to a permission element, e.g., <play>, when granting access to content according to such a permission. The <asset> elements specified within the <permission> element enable expression linking allowing its sibling permission elements in the same <permission> element to apply to DRM Content referenced by <asset> elements contained in an <agreement> element (i.e., outside a <permission> element). The link is established through the use of the "id" and "idref" attributes specified in sections 5.2.2.1 and 5.2.2.2.<br><br>Note that the DRM Agent MUST respect both, constraints specified as child elements to a permission element and those specified as top-level constraints in the same Rights Object. I.e., the stricter of two constraints of the same type prevails for a given permission element. Of course, Rights Objects with contradictory constraints should not be issued in the first place.<br><br>When there is a top-level constraint that is otherwise not allowed as a child constraint to a permission, e.g., <count> and <export mode="move">, the child constraint takes precedence over the top-level constraint as applied to this permission. For example, in the move scenario, Content and Rights Object would be moved, and the <count> constraint would accordingly be removed, too.<br><br>A DRM Agent MUST grant access to DRM Content referenced by an <asset> element in the agreement model according to permissions specified inside a <permission> element that is as sibling elements to an <asset> element in the permission model, where the <asset> element referencing the DRM Content and the <asset> element inside the <permission> element are linked by matching "id" and "idref" attributes.<br><br>If no <asset> element is present in a permission element such as <play>, then the permission applies to all <asset> sibling elements in the same Rights Object.<br><br>The <export> permission is associated with all of the DRM Content referenced by <asset> elements within the same Rights Object. A single Rights Object has at most one <export> element within a given <permission> element. |

## 5.4.2 Element <play>

| | |
|---|---|
| Element | <!ELEMENT o-dd:play (o-ex:constraint?)> |

| | |
|---|---|
| Semantics | The <play> element grants the permission to create a transient representation of audio or video Content. It contains an optional <constraint> element. If the <constraint> element is specified the DRM Agent MUST grant play rights according to the <constraint> child element. If no <constraint> element is specified, the DRM Agent MUST grant unlimited play rights.<br><br>A <system> element contained in a <constraint> child element to <play> is used to specify target system that may be used for creating a transient rendering of DRM Content.<br><br>The <play> element has the semantics of rendering the DRM Content into transient audio/video form, for example, audio/midi, video/quicktime. The DRM Agent MUST NOT grant access according to <play> to Content that cannot be rendered in this way.<br><br>Note that the DRM Agent MUST NOT grant access to game content, e.g., Java™ games, based on the <play> permission. In order to specify rights for Java™ games, the <execute> element MUST be utilized instead (section 5.4.4). |

### 5.4.3 Element <display>

| | |
|---|---|
| Element | <!ELEMENT o-dd:display (o-ex:constraint?)> |
| Semantics | The <display> element grants the permission to make a transient visible rendering of the Content. It contains an optional <constraint> element. If the <constraint> element is specified the DRM Agent MUST grant display rights according to the <constraint> child element. If no <constraint> element is specified, the DRM Agent MUST grant unlimited display rights.<br><br>The <display> element has the semantics of rendering the DRM Content onto a visual device, for example, image/gif or image/jpeg. The DRM Agent MUST NOT grant access according to <display> to Content that cannot be rendered in this way.<br><br>A <system> element contained in a <constraint> child element to <display> is used to specify target system that may be used for creating a transient rendering of DRM Content. |

### 5.4.4 Element <execute>

| | |
|---|---|
| Element | <!ELEMENT o-dd:execute (o-ex:constraint?)> |
| Semantics | The <execute> element grants permissions over the primitive computing element execute. It contains an optional <constraint> element. If the <constraint> element is specified the DRM Agent MUST grant execution rights according to the <constraint> child element. If no <constraint> element is specified, the DRM Agent MUST grant unlimited execution rights.<br><br>The <execute> element has the semantics of executing, i.e., invoking, DRM Content, e.g., Java™ games or other applications. Thus, the DRM Agent MUST NOT grant access according to <execute> to Content that cannot be rendered in this way. |

## 5.4.5 Element <print>

| | |
|---|---|
| Element | <!ELEMENT o-dd:print (o-ex:constraint?)> |
| Semantics | The <print> element grants the permission to create a fixed (i.e., static), directly perceivable representation of Content. It contains an optional <constraint> element. If the <print> element is specified the DRM Agent MUST grant print rights according to the <constraint> child element. If no <constraint> element is specified, the DRM Agent MUST grant unlimited print rights.<br><br>The <print> element has the semantics of printing, i.e., creating a hardcopy of, the DRM Content, for example, image/jpeg. The DRM Agent MUST NOT grant access according to <print> to Content that cannot be rendered in this way. |

## 5.4.6 Element <export>

| | |
|---|---|
| Element | <!ELEMENT oma-dd:export (o-ex:constraint)> |
| Semantics | The <export> element grants export rights over DRM Content and corresponding Rights Objects. It contains a mandatory <constraint> element. The DRM Agent MUST grant export rights according to the <constraint> child element.<br><br>The <export> element has the semantics of exporting the DRM Content and corresponding Rights Objects to a target system other than the OMA DRM system.<br><br>The <export> element contains a mandatory <constraint> element, which then contains a mandatory <system> element specifying to which target system(s) the DRM Content and Rights Objects are allowed to be exported.<br><br>The semantics of the <export> element are defined as an operation in which the complete Rights Object and DRM Content are exported, either together or separately, to create a logically integral unit. |

### 5.4.6.1 Attribute “mode”

| | |
|---|---|
| Attribute | <!ATTLIST oma-dd:export oma-dd:mode (move \| copy) #REQUIRED> |

| | |
|---|---|
| Semantics | move:<br><br>When the mode attribute is equal to “move”, the <constraint> element within the <export> element MAY have the <datetime> element, MUST NOT have the <interval> element, MUST NOT have the <count> element, MUST NOT have the <accumulated> element, and MUST NOT have <individual> element.<br><br>When exporting the Rights Object and the mode attribute is equal to “move”, the DRM agent MUST export the original Rights Object excluding <export> element with state information if it is a stateful Rights Object, and MUST make the original Rights Object including the <export> permission permanently unusable on the original device, after exporting is conducted.<br><br>copy:<br><br>When the mode attribute is equal to “copy”, the <constraint> element within the <export> element MAY have the <count> element, MAY have the <datetime> element, MAY have the <interval> element, MUST NOT have the <accumulated> element, and MUST NOT have <individual> element.<br><br>Note that if the <count> element is not specified for an <export> permission whose mode attribute is set to “copy”, the corresponding Rights Object would grant unlimited export to other DRM systems without removing the original Rights Object from the exporting device.<br><br>When the mode attribute is equal to “copy”, the DRM agent MUST export the original Rights Object excluding <export> element without state information if it is a stateful Rights Object, and MUST leave the original Rights Object including the <export> permission unchanged on the original device, after exporting is conducted. Note that, of course, the state needs to be updated on the device from which it is exported. |

# 5.5 Constraint Model

The constraint model enhances the permission model by providing fine-grained consumption control of content.

Constraints are associated with one permission element at a time. For a permission to be granted all its constraints MUST be fulfilled. If a constraint is not understood or cannot be enforced by the consuming device the parent permission is invalid and MUST NOT be granted. If present, a <constraint> element SHOULD contain at least one of its child elements. If a <constraint> element does not contain any constraints such as <count>, <datetime>, etc. it is unconstrained, and a DRM Agent MUST grant unconstrained access according to the permission containing such an unconstrained <constraint> element.

## 5.5.1 Element <constraint>

| | |
|---|---|
| Element | <!ELEMENT o-ex:constraint (o-dd:count?, oma-dd:timed-count?, o-dd:datetime?, o-dd:interval?, o-dd:accumulated?, o-dd:individual?, oma-dd:system*)> |
| Semantics | The <constraint> element is the top most element in the constraint model. It contains the optional <count>, <timed-count>, <datetime>, <interval>, <accumulated>, <individual>, and <system> elements.<br><br>The <constraint> element contains <system> elements only when its parent <permission> element contains the <export>, <play>, or <display> element. |

### 5.5.2 Element <count>

| | |
|---|---|
| Element | <!ELEMENT o-dd:count (#PCDATA)> |
| Semantics | The <count> element specifies the number of times a permission may be granted over an asset. It contains a positive integer value. If its parent <constraint> element is included in the <export> element, the <count> element specifies the number of times an <export> permission may be granted over the DRM Content and the Rights Object itself.<br><br>The DRM Agent MUST NOT grant the corresponding permission to the DRM Content more often than specified by the contained value. Similarly, the DRM Agent MUST NOT grant the corresponding permission to the DRM Content if the contained value is non-positive.<br><br>When used to constrain the <play> permission, the count MUST be decremented immediately upon play.<br><br>When used to constrain the <display> permission, the count MUST be decremented immediately upon display.<br><br>When used to constrain the <print> permission, the count MUST be decremented immediately upon commencement of printing.<br><br>When used to constrain the <execute> permission, the count MUST be decremented upon commencement of execution.<br><br>When used to constrain the <export> permission, the count MUST be decremented upon commencement of an export process.<br><br>Note that when using a stateful constraint such as <count> in a Rights Object that is bound to a domain of Devices, every Device in the domain will be able to access Content according to the containing Permission as often as specified by the value of the <count> element. Note that this might be considered particularly severe in the case that export rights with the copy mode are granted through a Rights Object bound to a domain. |

### 5.5.3 Element <timed-count>

| | |
|---|---|
| Element | <!ELEMENT oma-dd:timed-count (#PCDATA)> |
| Semantics | The semantics of the <timed-count> element are as for the <count> element (5.5.2) with the addition of an optional timer attribute (section 5.5.3.1).<br><br>If the timer attribute is omitted or contains an invalid value, or if the device is not able to measure the time passed as required by the semantics of this element, then the device MUST reduce the state value of the <timed-count > immediately upon beginning to access the content in which case the semantics of the <timed-count > element are identical to those of the <count> element.<br><br>The <timed-count> element MUST NOT occur as a constraint to a <print> or <export> permission. |

#### 5.5.3.1 Attribute "timer"

| | |
|---|---|
| Attribute | <!ATTLIST oma-dd:timed-count oma-dd:timer CDATA #IMPLIED> |
| Semantics | The attribute contains a positive integer value. It specifies the number of seconds after which the count state specified by the value of the <timed-count> element (section 5.5.3) is reduced starting from beginning to render the Content.<br><br>For example, if the timer value is set to "30" (without the quotes) and the <count> constraint value is set to "5" (without the quotes), a corresponding Media Object, may be rendered 5 times, while the number of remaining accesses is decremented after the Content has been rendered for 30 seconds. In other words, if rendering of the Content stops after less than 30 seconds, the state value of the <timed-count> element is not reduced. |

### 5.5.4 Element <datetime>

| | |
|---|---|
| Element | <!ELEMENT o-dd:datetime (o-dd:start?, o-dd:end?)> |
| Semantics | The <datetime> element specifies the time range, respectively the time limit, for a containing permission. It contains the optional <start> and <end> elements.<br><br>If the <start> element is present, its semantics are 'not before' the specified time/date.<br><br>If the <end> element is present, its semantics are 'not after' the specified time/date.<br><br>If both are present, the value of the <start> element MUST be smaller than the value of the <end> element. If the value of the <start> element is greater than the value of the <end> element then the DRM Agent MUST NOT grant access to the DRM Content according to the containing permission.<br><br>If both are absent, the datetime element does not have a meaning and MUST be ignored, i.e., it does not add to the constraints to access the DRM Content according to its parent permission element.<br><br>The DRM Agent of a consuming device without DRM Time MUST NOT grant access to DRM Content according to permissions containing the <datetime> element. |

#### 5.5.4.1 Element <start>

| | |
|---|---|
| Element | <!ELEMENT o-dd:start (#PCDATA)> |

| | |
|---|---|
| Semantics | The <start> element specifies the start time/date. Its semantics are 'not before'. The general format used for specifying time/date values is defined in [ISO8601].<br><br>To increase interoperability and facilitate ease of implementation values MUST conform to a single lexical representation defined in section 3.2.7 of [XMLSchema]. This lexical representation is the extended format CCYY-MM-DDThh:mm:ssZ where CC denotes the century, YY denotes the year, MM denotes the month, DD denotes the day, T is the date/time separator, hh, mm, ss represent the hour, minute, and second respectively, and Z is the mandatory UTC indicator. For example, 2002-12-31T23:59:59Z represents December 31st, 2002, 23:59:59 UTC.<br><br>The DRM Agent MUST NOT grant the corresponding permission to the DRM Content before the time/date specified by the value of the <start> element. |

### 5.5.4.2 Element <end>

| | |
|---|---|
| Element | <!ELEMENT o-dd:end (#PCDATA)> |
| Semantics | The <end> element specifies the end time/date. Its semantics are 'not after'. The general format used for specifying time/date values is defined in [ISO8601].<br><br>To increase interoperability and facilitate ease of implementation values MUST conform to a single lexical representation defined in section 3.2.7 of [XMLSchema]. This lexical representation is the extended format CCYY-MM-DDThh:mm:ssZ where CC denotes the century, YY denotes the year, MM denotes the month, DD denotes the day, T is the date/time separator, hh, mm, ss represent the hour, minute, and second respectively, and Z is the mandatory UTC indicator. For example, 2002-12-31T23:59:59Z represents December 31st, 2002, 23:59:59 UTC.<br><br>The DRM Agent MUST NOT grant the corresponding permission to the DRM Content after the time/date specified by the value of the <end> element. Also, the DRM Agent MUST NOT allow execution of the permission to continue beyond the specified time/date with the following exception:<br><br>If DRM Content is rendered with the purpose of directing the user's attention to an incoming phonecall or message, or to a calendar or other alarm event, the DRM Agent MAY allow access to the DRM Content to continue until the user has taken notice of the event, for example, by answering or rejecting the phone call, or dismissing the calendar or other alarm event. |

### 5.5.5 Element <interval>

| | |
|---|---|
| Element | <!ELEMENT o-dd:interval (#PCDATA)> |
| Semantics | The <interval> element specifies a period of time during which the permissions can be exercised over the DRM Content. The <interval> period MUST begin when the associated permission is first exercised. The permission can then be exercised any number of times within the <interval> period. The DRM Agent MUST NOT grant the corresponding permission to the DRM Content after the period specified by the value of the <interval> element has elapsed. Also, the DRM Agent MUST stop the execution of the permission as soon as possible after the value of the <interval> element has elapsed. This SHOULD happen immediately, with the following exception:<br><br>If DRM Content is rendered with the purpose of directing the user's attention to an incoming phonecall or message, or to a calendar or other alarm event, the DRM Agent MAY allow access to the DRM Content to continue until the user has taken notice of the event, for example, by answering or rejecting the phone call, or dismissing the calendar or other alarm event.<br><br>The general format used for specifying interval values is defined in [ISO8601].<br><br>To increase interoperability and facilitate ease of implementation values MUST conform to a single lexical representation defined in section 3.2.6 of [XMLSchema]. Further, the lexical representation MUST use the restricted duration format PnDTnHnMnS or any reduced precision and truncated representation version thereof as specified in [XMLSchema]. For example, P15DT10H30M20S represents a duration of 15 days, 10 hours, 30 minutes and 20 seconds.<br><br>The specified period SHOULD be greater than zero. If the specified period is equal to zero, then the permission MUST NOT be granted.<br><br>[XMLSchema] allows the number of seconds in the period to include decimal digits to arbitrary precision. However, to ensure interoperability, ROs MUST NOT contain fractional seconds in the period.<br><br>The DRM Agent of a consuming device without a time source MUST NOT grant access to DRM Content according to permissions containing the <interval> element. |

## 5.5.6 Element <accumulated>

| Element | <!ELEMENT o-dd:accumulated (#PCDATA)> |
|---|---|
| Semantics | The <accumulated> element specifies the maximum period of metered usage time during which the rights can be exercised over the DRM Content. The general format used for specifying the period is defined in [ISO8601].<br><br>To increase interoperability and facilitate ease of implementation values MUST conform to a single lexical representation defined in section 3.2.6 of [XMLSchema]. Further, the lexical representation MUST use the restricted duration format PnDTnHnMnS or any reduced version thereof as specified in [XMLSchema]. For example, P15DT10H30M20S represents a duration of 15 days, 10 hours, 30 minutes and 20 seconds.<br><br>The specified period SHOULD be greater than zero. If the specified period is equal to zero, then the permission MUST NOT be granted.<br><br>[XMLSchema] allows the number of seconds in the period to include decimal digits to arbitrary precision. However, to ensure interoperability, ROs MUST NOT contain fractional seconds in the period.<br><br>The <accumulated> period MUST begin when the associated permission is first exercised. The period defined by the <accumulated> element MUST only be metered when rendering the Content, i.e., the <accumulated> period is only consumed / used up while the Content is being rendered. The DRM Agent MUST NOT grant access to the DRM Content after the accumulative period specified by the value of the <accumulated> element has elapsed. Also, the DRM Agent MUST stop the execution of the permission as soon as possible after the value of the <accumulated> element has elapsed. This SHOULD happen immediately, with the following exception:<br><br>If DRM Content is rendered with the purpose of directing the user's attention to an incoming phonecall or message, or to a calendar or other alarm event, the DRM Agent MAY allow access to the DRM Content to continue until the user has taken notice of the event, for example, by answering or rejecting the phone call, or dismissing the calendar or other alarm event.<br><br>The DRM Agent of a consuming device without a time source MUST NOT grant access to DRM Content according to permissions containing the <accumulated> element.<br><br>The <accumulated> element MUST NOT occur as a constraint to a <print> permission. |

## 5.5.7 Element <individual>

| Element | <!ELEMENT o-dd:individual (o-ex:context)> |
|---|---|
| Semantics | The <individual> element specifies the individual to which content is bound. It does so by binding content to the user identity specified via its <context> child element.<br><br>The DRM Agent MUST NOT grant access to the DRM Content unless one of the user identity(s) to which the use of Content is constrained matches the user identity associated with the device. |

### 5.5.8 Element <system>

| | |
|---|---|
| Element | <!ELEMENT oma-dd:system (o-ex:context)> |
| Semantics | The <system> element specifies the target system to which DRM Content and Rights Objects can be exported, described in the mandatory <context> element.<br><br>The <system> element MUST only occur as a constraint to an <export>, <play>, or <display> permission.<br><br>In the case of <export>, it specifies the target system to which DRM Content is copied or moved to. In the case of <play> and <display> it specifies the target system to which DRM Content may be transiently rendered. |

## 5.6 Inheritance Model

This section describes how a parent Rights Object can specify Permissions and Constraints for one or more pieces of DRM Content each governed by a child Rights Object, using a limited subset of the ODRL inheritance model. The DRM Agent MUST NOT accept parent child Rights Objects constellations with more than one level of inheritance (i.e. parent-child). In other words, a parent Rights Object MUST NOT inherit Permissions and Constraints from another Rights Object.

### 5.6.1 Element <inherit>

| | |
|---|---|
| Element | <!ELEMENT o-ex:inherit (o-ex:context)> |
| Semantics | The <inherit> element specifies the inheritance of Permissions and Constraints from one Rights Object to another in order to allow parent/child relationships to be defined. This enables Rights Issuers to efficiently support, for example, subscription business models.<br><br>A parent Rights Object defines Permissions and Constraints for DRM Content which can be inherited by child Rights Objects. Child Rights Objects usually reference DRM Content whereas parent Rights Objects do not reference DRM Content themselves.<br><br>Child Rights Objects inherit from a single corresponding parent Rights Object by including this <inherit> element. The <uid> element of the <context> element in the <inherit> element MUST match the value of the <uid> element of the <context> element of the <asset> element of the corresponding parent Rights Object. If the parent Rights Object referenced by a child Rights Object does not exist, the DRM Agent MUST NOT grant access to the DRM Content according to this child Rights Object.<br><br>When granting access to DRM Content according to a permission element, e.g.,<play>, in a child or parent Rights Object, the DRM Agent MUST enforce all top-level constraints of the parent and child Rights Object as well as possible constraints of the permission according to which access is being granted. Child Rights Objects reference DRM Content as usual, i.e., via the <uid> element in the <context> element of the <asset> element. The <asset> element of a Parent Rights Objects may not reference an actual DCF, but contain a “virtual” UID denoting, for example, the subscription itself.<br><br>Child Rights Objects MUST NOT inherit from more than one parent Rights Object. A parent Rights Object MUST NOT be a child Rights Object at the same time. |

Figure 5.1 depicts the above described relationships between parent Rights Object, child Rights Object, and DRM Content with the example of a subscription model.

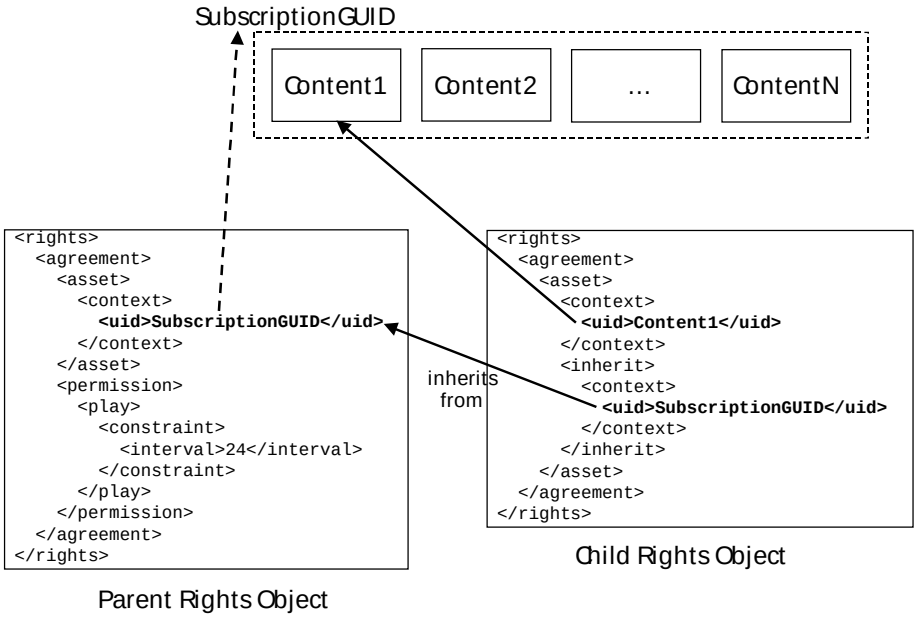


**Figure 5.1. Inheritance.**

Note that the other instances of DRM Content (Content2 through ContentN) would be referenced by separate child Rights Objects each inheriting from the parent Rights Object just like the child Rights Object shown for Content1. Also note that the subscription as well as content references MUST be globally unique.

# 5.7 Security Model

Security constitutes an important part of a DRM system. OMA DRM 2.0 provides

1. Confidentiality for the CEK of Rights Objects
2. Integrity of the association between Rights Objects and DRM Content
3. Rights Object integrity and authenticity

The former two are specified in sections 5.7.1 and 5.7.2 of this specification. The latter is specified in [DRM-v2]. Rights Objects defined in this specification MUST be contained in a <ProtectedRO> element as defined in [DRM-v2] to protect against unauthorized Rights Issuers, or Rights Object replay.

The ODRL security model, which forms the basis for the security model of this specification, is based on [XMLENC] and [XMLSIG].

## 5.7.1 Content Confidentiality

Protecting the confidentiality of Content is an essential part of enforcing consumption control of DRM Content. Enabling an authorized party to consume DRM Content is similar to granting this party access to the confidential Content. In other words, a party authorized to consume DRM Content is let into the exclusive circle of parties deemed trustworthy enough to access the Content.

This concept is realized in [DRM-v2] by i) encrypting the Content thus transforming it into DRM Content [DRMCF-v2], and ii) sharing the key(s) required to decrypt the DRM Content only with those parties that are authorized to consume the Content.

DRM Content is protected by a symmetric algorithm (AES), i.e., the key used for decryption can be derived from the key used for encryption. Thus, henceforth, the key will be referred to as *content encryption key*, or short *CEK*.

Note that the CEK might also be used to wrap another (intermediate) key that in turn encrypts the Content. The DRM Agent can determine whether the CEK wraps the DCF or another key by using the ContentID the <asset> element contains (via its child elements) to retrieve DCFs that match this ContentID. If a DCF contains an OMADRMGroupID box (see [DRMCF-v2]), then the CEK contained in the Rights Object wraps a GroupKey and not the DCF directly.

Encrypting the Content defers Content confidentiality to controlling the confidentiality of the CEK. Now, the security of the DRM system relies on the control of the CEK that must be kept secret from all unauthorized parties. The CEK necessary to decrypt the DRM Content is contained in the Rights Object in encrypted form.

A CEK, $K_{CEK}$, is a randomly generated 128-bit AES key. It is wrapped using a REK, $K_{REK}$, by use of AES-WRAP. $K_{REK}$ keys derived as specified in section 6.4. of [DRM-v2] shall be used as the key-wrapping keys:

$$C = \text{AES-WRAP}(K_{REK}, K_{CEK})$$

After receiving $C$, the DRM Agent decrypts $C$ using $K_{REK}$:

$$K_{CEK} = \text{AES-UNWRAP}(K_{REK}, C)$$

The following URI shall be used to identify this key transport scheme in <EncryptionMethod> elements:

http://www.w3.org/2001/04/xmlenc#kw-aes128

The corresponding XML security elements are described next.

### 5.7.1.1 Element <KeyInfo>

| | |
|---|---|
| Element | <!ELEMENT ds:KeyInfo (xenc:EncryptedKey?, ds:RetrievalMethod?)> |
| Semantics | The <KeyInfo> element has a dual purposes, depending on its parent element.<br><br>1) When it is contained in an <asset> element, it contains the <EncryptedKey> element, making it the starting point for all consumption control, i.e., Content encryption, functionality. Note that the <KeyInfo> element SHOULD NOT be included in the <asset> element if the Rights Object does not reference DRM Content but is used as a parent Rights Object in the inheritance case.<br><br>2) When it is contained in the <EncryptedKey> element, it contains the <RetrievalMethod> element which references the key used to encrypt the CEK, i.e., the REK (see [DRM-v2]). |

### 5.7.1.2 Element <EncryptedKey>

| | |
|---|---|
| Element | <!ELEMENT xenc:EncryptedKey (ds:KeyInfo?, xenc:EncryptionMethod, xenc:CipherData)> |
| Semantics | The <EncryptedKey> element contains the optional <KeyInfo> element, the <EncryptionMethod> element, and the <CipherData element>. |

#### 5.7.1.3 Element <xenc:EncryptionMethod>

| | |
|---|---|
| Element | <!ELEMENT xenc:EncryptionMethod (#PCDATA)> |
| Semantics | The <EncryptionMethod> element is empty. Its attribute identifies the encryption method algorithm used to encrypt the CEK. |

##### 5.7.1.3.1 Attribute "Algorithm"

| | |
|---|---|
| Attribute | <!ATTLIST xenc:EncryptionMethod Algorithm CDATA #FIXED "http://www.w3.org/2001/04/xmlenc#kw-aes128"> |
| Semantics | The "Algorithm" attribute identifies the encryption algorithm used to encrypt the CEK contained in encrypted form in the <CipherValue> element.<br><br>The algorithm MUST be AES128 Key Wrap. |

#### 5.7.1.4 Element <CipherData>

| | |
|---|---|
| Element | <!ELEMENT xenc:CipherData (xenc:CipherValue)> |
| Semantics | The <CipherValue> element contains the <CipherValue> element. |

#### 5.7.1.5 Element <CipherValue>

| | |
|---|---|
| Element | <!ELEMENT xenc:CipherValue (#PCDATA)> |
| Semantics | The <CipherValue> element contains the base64 encoded value of the encrypted CEK. |

#### 5.7.1.6 Element <RetrievalMethod>

| | |
|---|---|
| Element | <!ELEMENT ds:RetrievalMethod (#PCDATA)> |
| Semantics | The <RetrievalMethod> element provides a reference to the key used to encrypt the CEK, i.e., the REK, via its attribute. |

##### 5.7.1.6.1 Attribute "URI"

| | |
|---|---|
| Attribute | <!ATTLIST ds:RetrievalMethod URI CDATA #REQUIRED> |
| Semantics | The "URI" attribute provides a reference to the REK, i.e., the key used to encrypt the CEK (see [DRM-v2]).<br><br>Its value MUST match the value of the "Id" attribute of the <encKey> element. The <encKey> element is a sibling element to the <rights> root element of a Rights Object as defined in this specification. These two elements are both child elements to the <ro> element of type ROPayload as specified in [DRM-v2]. |

## 5.7.2 Rights Object DRM Content Association Integrity

The ability to replace the DRM Content governed by rights amounts to the ability of changing the rights itself. Thus, the integrity of the association between a Rights Object and the corresponding DRM Content must be protected as much as the specified Rights Object itself.

A reference to a piece of DRM Content is established via the <uid> element contained in the <context> element of the <asset> element. Enforcing the integrity of the association between Rights Object and DRM Content is handled similarly to enforcing the integrity of Rights Objects, i.e., by signing Rights Objects utilizing functionality from [XMLSIG]. This prevents tampering with the content identifier in the Rights Objects. It does not, however, prevent from modifying the corresponding identifier in the DRM Content [DRMCF-v2].

It is possible to provide a way of securing the content-end of the Rights Object - DRM Content association without having to sign the DRM Content. Instead, a hash of the DRM Content is included in the Rights Object. Since this hash value is part of the signed Rights Object, it is as safe from being tampered with, as is the <uid> element in the Rights Object referencing the DRM Content. The integrity of the content-end is guaranteed by the very characteristics of the hash itself: any modifications to the DRM Content automatically invalidate the hash value inside the Rights Object. The hash value of the DRM Content in the Rights Object ensures the integrity of the Rights Object DRM Content association as the integrity of the Rights Object is protected also, i.e.,, by signing it.

### 5.7.2.1 Element <digest>

| | |
|---|---|
| Element | <!ELEMENT o-ex:digest (ds:DigestMethod, ds:DigestValue)> |
| Semantics | The <digest> element provides the integrity for the association of the Rights Object with the DRM Content referenced by the <uid> element in the <context> of the same <asset> element. It contains the <DigestMethod> element and the <DigestValue> element.<br><br>The <digest> element SHOULD NOT be present if the Rights Object is a parent Rights Object referencing a ‘virtual’ resource such as a subscription (see section 5.6). |

### 5.7.2.2 Element <DigestMethod>

| | |
|---|---|
| Element | <!ELEMENT ds:DigestMethod (#PCDATA)> |
| Semantics | The <DigestMethod> element indicates the algorithm used to calculate the digest value contained in the <DigestValue> element via its attribute element. The element itself is empty. |

#### 5.7.2.2.1 Attribute “Algorithm”

| | |
|---|---|
| Attribute | <!ATTLIST ds:DigestMethod Algorithm CDATA #FIXED "http://www.w3.org/2000/09/xmldsig#sha1"> |
| Semantics | The “Algorithm” attribute identifies the digest algorithm. It MUST identify the algorithm SHA-1. |

#### 5.7.2.3 Element <DigestValue>

| | |
|---|---|
| Element | <!ELEMENT ds:DigestValue (#PCDATA)> |
| Semantics | The <DigestValue> element contains the base64 encoded value of the digest.<br><br>It contains the base64 encoded hash value of the DRM Content referenced by the <uid> element in the <context> of the same <asset> element. |

### 5.7.3 Rights Object Integrity and Authenticity

Integrity protection prevents illegitimately modifying the Rights Object specified for DRM Content, including but not limited to, adding, deleting, and modifying permissions and constraints for DRM Content, and references to DRM Content itself included in the Rights Object.

Authenticity provides for authentication of the origin of Rights Objects. It enables a DRM Agent to verify the Rights Issuer identity before accepting a Rights Objects.

The functionality employed to provide Rights Object integrity and authenticity are specified in [DRM-v2].

## 5.8 ODRL Compatibility

This specification defines a mobile profile of ODRL v1.1 [ODRL]. This specification takes precedence in case there is any divergence from [ODRL].

The DRM Agent of a device encountering any ODRL [ODRL] elements not defined within this specification MUST proceed as follows:

- Unsupported permissions MUST be ignored. Supported permissions MUST still be granted.
- Permissions containing one or more unsupported constraints MUST NOT be granted.
- Rights objects containing <requirement> elements MUST NOT be granted.
- Rights objects containing <condition> elements MUST NOT be granted.
- Unsupported <rightsholder> elements SHOULD be ignored.
- Unsupported <context> elements SHOULD be ignored.
- Unsupported <offer> elements SHOULD be ignored.
- Unsupported <party> elements within an <asset> element SHOULD be ignored.
- Unsupported <revoke> elements SHOULD be ignored.
- Unsupported elements of the ODRL security model SHOULD be ignored.

Rights Objects SHOULD NOT contain any elements that are not defined in the specification.

## 5.9 Order of Rights Object Evaluation

In order to achieve a uniform user experience across different implementations, the DRM Agent MUST apply the following rules when automatically selecting which Rights Object to apply when accessing content, in case there are multiple Rights Objects for this content.

1. Only Rights Objects valid at the time of requesting content access can be considered, for example, those with a <datetime> constraint whose <begin> date still lies in the future cannot be considered.
2. Rights Objects with no constraints should be used first.
3. Rights Objects containing a <datetime> constraint (and potentially other constraints) should be used to grant access to content before using rights objects that do not contain a <datetime> constraint.
4. If multiple Rights Objects exist that contain <datetime> constraints (and potentially other constraints), then these should be used in the order of ascending <end> dates first, i.e., those that expire first should be utilized first.
5. If multiple Rights Objects exist that do not contain a <datetime> constraint (and potentially other constraints), then those containing an <interval> constraint should be used to grant access to content before using rights objects that do not contain an <interval> constraint.
6. Rights Objects containing a <timed-count> should be used before Rights Objects containing <count>.

Note that the user MAY be allowed to select a Rights Object to apply manually when accessing DRM Content, thus overwriting the DRM Agent's choice.

# 6. Syntax

As described in section 4, this specification defines

3. A subset, i.e., a mobile profile, of ODRL, and
4. A data dictionary defining additional permissions and constraints beyond those provided by ODRL.

The OMA data dictionary is defined in an XML Schema utilizing the extension mechanisms provided by the original ODRL expression language and data dictionary schemas. The document type definition (DTD) defines the set of permissible Rights Objects for DRM Agents. Rights Objects generated according to the DTD validate against the combination of the original ODRL expression language schema and data dictionary schema as well as the OMA data dictionary schema (and those utilized by those, e.g., [XMLSIG] and [XMLENC]).

The subset is contained in section 6.1 and section 6.2 defines the OMA data dictionary utilized in addition to the ODRL data dictionary.

## 6.1 ODRL Subset

Figure 6.1 depicts the syntax of the ODRL mobile profile using XML document type definition [XML]. The document type definition has the public identifier '-//OMA//DTD DRMREL 2.0//EN' and is located at 'http://www.openmobilealliance.org/tech/DTD/drmrel20.dtd'.

A DRM Agent MUST be able to parse all elements defined in the DRM REL DTD. Proprietary elements MAY be added in new namespaces. DRM Agents MAY ignore any element not defined in the DRM REL DTD. This DTD defines the valid subset of Rights Objects for OMA DRM 2.0 that can be generated as jointly defined by the ODRL expression language XML schema, the ODRL data dictionary XML schema and the OMA data dictionary XML schema.

Rights Issuer servers MUST be able to generate Rights Object according to the below DTD.

```
<!ELEMENT o-ex:rights (o-ex:context, o-ex:agreement)>
<!ATTLIST o-ex:rights
    xmlns:o-ex CDATA #FIXED "http://odrl.net/1.1/ODRL-EX"
    xmlns:o-dd CDATA #FIXED "http://odrl.net/1.1/ODRL-DD"
    xmlns:oma-dd CDATA #FIXED "http://www.openmobilealliance.com/oma-dd"
    xmlns:ds CDATA #FIXED "http://www.w3.org/2000/09/xmldsig#"
    xmlns:xenc CDATA #FIXED "http://www.w3.org/2001/04/xmlenc#"
>
<!ELEMENT o-ex:context (o-dd:version?, o-dd:uid*)>
<!ELEMENT o-dd:version (#PCDATA)>
<!ELEMENT o-dd:uid (#PCDATA)>
<!ELEMENT o-ex:agreement (o-ex:asset+, o-ex:permission*)>
<!ELEMENT o-ex:asset (o-ex:context?, o-ex:inherit?, o-ex:digest?, ds:KeyInfo?)>
<!ATTLIST o-ex:asset
   o-ex:id ID #IMPLIED
   o-ex:idref IDREF #IMPLIED
>
<!ELEMENT o-ex:inherit (o-ex:context)>
<!ELEMENT o-ex:digest(ds:DigestMethod, ds:DigestValue)>
<!ELEMENT ds:DigestMethod (#PCDATA)>
<!ATTLIST ds:DigestMethod
    Algorithm CDATA #FIXED "http://www.w3.org/2000/09/xmldsig#sha1"
>
```

```
<!ELEMENT ds:DigestValue (#PCDATA)>
<!ELEMENT ds:KeyInfo (xenc:EncryptedKey?, ds:RetrievalMethod?)>
<!ELEMENT xenc:EncryptedKey (ds:KeyInfo?, xenc:EncryptionMethod, xenc:CipherData)>
<!ELEMENT xenc:EncryptionMethod (#PCDATA)>
<!ATTLIST xenc:EncryptionMethod
    Algorithm CDATA #FIXED "http://www.w3.org/2001/04/xmlenc#kw-aes128"
>
<!ELEMENT xenc:CipherData (xenc:CipherValue)>
<!ELEMENT xenc:CipherValue (#PCDATA)>
<!ELEMENT ds:RetrievalMethod (#PCDATA)>
<!ATTLIST ds:RetrievalMethod
    URI CDATA #REQUIRED
>
<!ELEMENT o-ex:permission (o-ex:constraint?, o-ex:asset*, o-dd:play?, o-dd:display?, o-
dd:execute?, o-dd:print?, oma-dd:export?)>
<!ELEMENT o-dd:play (o-ex:constraint?)>
<!ELEMENT o-dd:display (o-ex:constraint?)>
<!ELEMENT o-dd:execute (o-ex:constraint?)>
<!ELEMENT o-dd:print (o-ex:constraint?)>
<!ELEMENT o-ex:constraint (o-dd:count?, oma-dd:timed-count?, o-dd:datetime?, o-
dd:interval?, o-dd:accumulated?, o-dd:individual?, oma-dd:system*)>
<!ELEMENT o-dd:count (#PCDATA)>
<!ELEMENT oma-dd:timed-count (#PCDATA)>
<!ATTLIST oma-dd:timed-count
    oma-dd:timer CDATA #IMPLIED
>
<!ELEMENT o-dd:datetime (o-dd:start?, o-dd:end?)>
<!ELEMENT o-dd:start (#PCDATA)>
<!ELEMENT o-dd:end (#PCDATA)>
<!ELEMENT o-dd:interval (#PCDATA)>
<!ELEMENT o-dd:accumulated (#PCDATA)>
<!ELEMENT o-dd:individual (o-ex:context)>
<!ELEMENT oma-dd:export (o-ex:constraint)>
<!ATTLIST oma-dd:export
    oma-dd:mode (move | copy) #REQUIRED
>
<!ELEMENT oma-dd:system (o-ex:context)>
```

**Figure 6.1. Syntax.**

## 6.2 OMA Data Dictionary

A DRM Agent MUST be able to parse all elements defined in the below schema.

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema targetNamespace="http://www.openmobilealliance.com/oma-dd"
   xmlns:xsd="http://www.w3.org/2001/XMLSchema"
   xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
   xmlns:o-ex="http://odrl.net/1.1/ODRL-EX"
```

```
   xmlns:o-dd="http://odrl.net/1.1/ODRL-DD"
   xmlns:oma-dd="http://www.openmobilealliance.com/oma-dd"
   elementFormDefault="qualified" attributeFormDefault="qualified"
>
   <xsd:import namespace="http://odrl.net/1.1/ODRL-EX"
schemaLocation="http://odrl.net/1.1/ODRL-EX-11.xsd"/>
   <xsd:element name="export" substitutionGroup="o-ex:permissionElement">
      <xsd:complexType>
         <xsd:complexContent>
            <xsd:extension base="o-ex:permissionType">
               <xsd:attribute name="mode" use="required">
                  <xsd:simpleType>
                     <xsd:restriction base="xsd:NMTOKEN">
                        <xsd:enumeration value="move"/>
                        <xsd:enumeration value="copy"/>
                     </xsd:restriction>
                  </xsd:simpleType>
               </xsd:attribute>
            </xsd:extension>
         </xsd:complexContent>
      </xsd:complexType>
   </xsd:element>
   <xsd:element name="system" type="o-ex:constraintType"
       substitutionGroup="o-ex:constraintElement"/>
   <xsd:element name="timed-count" substitutionGroup="o-ex:constraintElement">
      <xsd:complexType>
         <xsd:simpleContent>
            <xsd:extension base="xsd:positiveInteger">
               <xsd:attribute name="timer" type="xsd:positiveInteger" use="required"/>
            </xsd:extension>
         </xsd:simpleContent>
      </xsd:complexType>
   </xsd:element>
</xsd:schema>
```

**Figure 6.2. OMA Data Dictionary schema**

# Appendix A. Static Conformance Requirements (Normative)

## A.1 Client Conformance Requirements

| Item | Function | Reference | Status | Requirement |
|---|---|---|---|---|
| DRM-REL-GEN-C-001 | <rights> element | 5.1.1 | M | |
| DRM-REL-GEN-C-002 | <agreement> element | 5.2.1 | M | |
| DRM-REL-GEN-C-003 | <asset> element | 5.2.2 | M | |
| DRM-REL-GEN-C-004 | Expression linking | 5.2.2.1, 5.2.2.2 | M | |
| DRM-REL-GEN-C-005 | <context> element | 5.3.1 | M | |
| DRM-REL-GEN-C-006 | <version> element | 5.3.2 | M | |
| DRM-REL-GEN-C-007 | <uid> element | 5.3.3 | M | |
| DRM-REL-GEN-C-008 | Permission Model | 5.4 | M | |
| DRM-REL-GEN-C-009 | <permission> element | 5.4.1 | M | |
| DRM-REL-GEN-C-010 | <play> element | 5.4.2 | M | |
| DRM-REL-GEN-C-011 | <display> element | 5.4.3 | M | |
| DRM-REL-GEN-C-012 | <execute> element | 5.4.4 | M | |
| DRM-REL-GEN-C-013 | <print> element | 5.4.5 | M | |
| DRM-REL-GEN-C-014 | <export> element | 5.4.6, 5.4.6.1 | M | |
| DRM-REL-GEN-C-015 | Constraint Model | 5.5 | M | |
| DRM-REL-GEN-C-016 | <constraint> element | 5.5.1 | M | |
| DRM-REL-GEN-C-017 | <count> element | 5.5.2 | M | |
| DRM-REL-GEN-C-018 | <timed-count> element | 5.5.3, 5.5.3.1 | O | |
| DRM-REL-GEN-C-019 | <datetime> element | 5.5.4 | O | DRM-REL-GEN-C-020 AND DRM-REL-GEN-C-021 |
| DRM-REL-GEN-C-020 | <start> element | 5.5.4.1 | O | |
| DRM-REL-GEN-C-021 | <end> element | 5.5.4.2 | O | |
| DRM-REL-GEN-C-022 | <interval> element | 5.5.5 | O | |
| DRM-REL-GEN-C-023 | <accumulated> element | 5.5.6 | O | |
| DRM-REL-GEN-C-024 | <individual> element | 5.5.7 | O | |
| DRM-REL-GEN-C-025 | <system> element | 5.5.8 | M | |
| DRM-REL-GEN-C-026 | Inheritance model | 5.6, 5.6.1 | M | |
| DRM-REL-GEN-C-027 | <KeyInfo> element | 5.7.1.1 | M | |
| DRM-REL-GEN-C-028 | <EncryptedKey> element | 5.7.1.2 | M | |
| DRM-REL-GEN-C-029 | <EncryptionMethod> element | 5.7.1.3, 5.7.1.3.1 | M | |
| DRM-REL-GEN-C-030 | <CipherData> element | 5.7.1.4 | M | |
| DRM-REL-GEN-C-031 | <CipherValue> element | 5.7.1.5 | M | |
| DRM-REL-GEN-C-032 | <RetrievalMethod> element | 5.7.1.6, 5.7.1.6.1 | M | |
| DRM-REL-GEN-C-033 | <digest> element | 5.7.2.1 | M | |
| DRM-REL-GEN-C-034 | <DigestMethod> element | 5.7.2.2, 5.7.2.2.1 | M | |
| DRM-REL-GEN-C-035 | <DigestValue> element | 5.7.2.3 | M | |
| DRM-REL-GEN-C-036 | ODRL compatibility | 5.8 | M | |
| DRM-REL-GEN-C-037 | Syntax Parsing | 6 | M | |
| DRM-REL-GEN-C-038 | Rights Object evaluation order | 5.9 | M | |

## A.2 Server Conformance Requirements

| Item | Function | Reference | Status | Requirement |
|---|---|---|---|---|
| DRM-REL-GEN-S-001 | Expression linking | 5.2.2.1, 5.2.2.2 | M | |
| DRM-REL-GEN-S-002 | <version> element | 5.3.2 | M | |
| DRM-REL-GEN-S-003 | <uid> element | 5.3.3 | M | |
| DRM-REL-GEN-S-004 | <play> element | 5.4.2 | M | |
| DRM-REL-GEN-S-005 | <export> element | 5.4.6, 5.4.6.1 | M | |
| DRM-REL-GEN-S-006 | <datetime> element | 5.5.4 | M | |

| Item | Function | Reference | Status | Requirement |
|---|---|---|---|---|
| DRM-REL-GEN-S-007 | <start> element | 5.5.4.1 | M | |
| DRM-REL-GEN-S-008 | <end> element | 5.5.4.2 | M | |
| DRM-REL-GEN-S-009 | <interval> element | 5.5.5 | M | |
| DRM-REL-GEN-S-010 | <accumulated> element | 5.5.6 | M | |
| DRM-REL-GEN-S-011 | <system> element | 5.5.8 | M | |
| DRM-REL-GEN-S-012 | Inheritance model | 5.6, 5.6.1 | M | |
| DRM-REL-GEN-S-013 | Security model | 5.7 | M | |
| DRM-REL-GEN-S-014 | <EncryptedKey> element | 5.7.1.2 | M | |
| DRM-REL-GEN-S-015 | Encryption algorithm | 5.7.1.3.1 | M | |
| DRM-REL-GEN-S-016 | REK referencing | 5.7.1.6, 5.7.1.6.1 | M | |
| DRM-REL-GEN-S-017 | Hash algorithm | 5.7.2.2.1 | M | |
| DRM-REL-GEN-S-018 | ODRL compatibility | 5.8 | M | |
| DRM-REL-GEN-S-019 | Syntax Generation | 6 | M | |

# Appendix B. Change History (Informative)

## B.1 Approved Version History

| Reference | Date | Description |
|---|---|---|
| n/a | n/a | No prior version |

## B.2 Draft/Candidate Version 2.0 History

| Document Identifier | Date | Sections | Description |
|---|---|---|---|
| Candidate Version | 16 Jul 2004 | n/a | Candidate version. |
| OMA-DRM-REL-V2_0 | 10 Dec 2004 | 5.4.1 | Namespace correction |
| | | 5.4.2 | Editorial clarifications |
| | | 5.4.3 | Editorial clarifications |
| | | 5.4.6.1 | Editorial clarifications |
| | | 5.5.3.1 | Element name correction |
| | | 5.5.8 | Editorial clarifications |
| | | 5.7.1.3.1 | Namespace corrections |
| | | 5.7.1.6.1 | Namespace corrections |
| | | 5.7.2.2.1 | Namespace corrections |
| | | 6.1 | Namespace corrections |
| | | Appendix C | Namespace corrections |
| | | | TP ref #OMA-TP-2005-0054-INP_Notifcation_of-CRs_to_DRM2 |

# Appendix C. Examples (Informative)

This appendix contains a number of examples to illustrate the use of Rights Objects.

## C.1 Unlimited Play

The rights depicted in this example grant unconstrained permission to play the corresponding DRM Content.

```
<o-ex:rights
 xmlns:o-ex="http://odrl.net/1.1/ODRL-EX"
 xmlns:o-dd="http://odrl.net/1.1/ODRL-DD"
 xmlns:oma-dd="http://www.openmobilealliance.com/oma-dd"
 xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
 xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
 <o-ex:context>
  <o-dd:version>2.0</o-dd:version>
  <o-dd:uid>RightsObjectID</o-dd:uid>
 </o-ex:context>
 <o-ex:agreement>
  <o-ex:asset>
   <o-ex:context>
    <o-dd:uid>ContentID</o-dd:uid>
   </o-ex:context>
   <o-ex:digest>
    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
    <ds:DigestValue>DCFHash</ds:DigestValue>
   </o-ex:digest>
   <ds:KeyInfo>
    <xenc:EncryptedKey>
     <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#kw-aes128"/>
     <xenc:CipherData>
      <xenc:CipherValue>EncryptedCEK</xenc:CipherValue>
     </xenc:CipherData>
    </xenc:EncryptedKey>
    <ds:RetrievalMethod URI="REKReference"/>
   </ds:KeyInfo>
  </o-ex:asset>
  <o-ex:permission>
   <o-dd:play/>
  </o-ex:permission>
 </o-ex:agreement>
</o-ex:rights>
```

Note that the CEK inside the <CipherValue> element is base64 encoded.

## C.2 Preview

The rights depicted in this example grant the right to display the corresponding Content once, thus implementing the functionality to test-drive, i.e., preview, Content.

Note that in this example preview functionality is implemented as displaying the Content once. It is possible to implement any kind of preview through the use of appropriate constraints, e.g., limiting the time range during which Content can be displayed through the use of the <datetime> or <interval> constraints (sections 5.5.4 and 5.5.5).

```
<o-ex:rights
 xmlns:o-ex="http://odrl.net/1.1/ODRL-EX"
 xmlns:o-dd="http://odrl.net/1.1/ODRL-DD"
 xmlns:oma-dd="http://www.openmobilealliance.com/oma-dd"
 xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
 xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
 <o-ex:context>
  <o-dd:version>2.0</o-dd:version>
  <o-dd:uid>RightsObjectID</o-dd:uid>
 </o-ex:context>
 <o-ex:agreement>
  <o-ex:asset>
   <o-ex:context>
    <o-dd:uid>ContentID</o-dd:uid>
   </o-ex:context>
   <o-ex:digest>
    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
    <ds:DigestValue>DCFHash</ds:DigestValue>
   </o-ex:digest>
   <ds:KeyInfo>
    <xenc:EncryptedKey>
     <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#kw-aes128"/>
     <xenc:CipherData>
      <xenc:CipherValue>EncryptedCEK</xenc:CipherValue>
     </xenc:CipherData>
    </xenc:EncryptedKey>
    <ds:RetrievalMethod URI="REKReference"/>
   </ds:KeyInfo>
  </o-ex:asset>
  <o-ex:permission>
   <o-dd:display>
    <o-ex:constraint>
     <o-dd:count>1</o-dd:count>
    </o-ex:constraint>
   </o-dd:display>
  </o-ex:permission>
 </o-ex:agreement>
</o-ex:rights>
```

Note that the CEK inside the <CipherValue> element is base64 encoded.

# C.3 Multiple permissions for a Multipart DCF

This example describes an example of multiple permissions within a single Rights Object for a multipart DCF where each Media Object is assigned an individual Content-ID. The Rights Object contains two permissions. The first one is an

unconstrained permission to display both Media Objects in the DCF, and the second one is an unconstrained permission to print the Media Object. The Rights Object refers to each of the two Media Objects in the multipart DCF by their Content-IDs.

```
<o-ex:rights
 xmlns:o-ex="http://odrl.net/1.1/ODRL-EX"
 xmlns:o-dd="http://odrl.net/1.1/ODRL-DD"
 xmlns:oma-dd="http://www.openmobilealliance.com/oma-dd"
 xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
 xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
 <o-ex:context>
  <o-dd:version>2.0</o-dd:version>
  <o-dd:uid>RightsObjectID</o-dd:uid>
 </o-ex:context>
 <o-ex:agreement>
  <o-ex:asset o-ex:id="Asset-1">
   <o-ex:context>
    <o-dd:uid>ContentID1</o-dd:uid>
   </o-ex:context>
   <o-ex:digest>
    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
    <ds:DigestValue>DCFHash</ds:DigestValue>
   </o-ex:digest>
   <ds:KeyInfo>
    <xenc:EncryptedKey>
     <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#kw-aes128"/>
     <xenc:CipherData>
      <xenc:CipherValue>EncryptedCEK</xenc:CipherValue>
     </xenc:CipherData>
    </xenc:EncryptedKey>
    <ds:RetrievalMethod URI="REKReference"/>
   </ds:KeyInfo>
  </o-ex:asset>
  <o-ex:asset o-ex:id="Asset-2">
   <o-ex:context>
    <o-dd:uid>ContentID2</o-dd:uid>
   </o-ex:context>
   <o-ex:digest>
    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
    <ds:DigestValue>DCFHash</ds:DigestValue>
   </o-ex:digest>
   <ds:KeyInfo>
    <xenc:EncryptedKey>
     <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#kw-aes128"/>
     <xenc:CipherData>
      <xenc:CipherValue>EncryptedCEK</xenc:CipherValue>
     </xenc:CipherData>
    </xenc:EncryptedKey>
    <ds:RetrievalMethod URI="REKReference"/>
   </ds:KeyInfo>
```

```
  </o-ex:asset>
  <o-ex:permission>
   <o-ex:asset o-ex:idref="Asset-1"/>
   <o-ex:asset o-ex:idref="Asset-2"/>
   <o-dd:display/>
  </o-ex:permission>
  <o-ex:permission>
   <o-ex:asset o-ex:idref="Asset-2"/>
   <o-dd:print/>
  </o-ex:permission>
 </o-ex:agreement>
</o-ex:rights>
```

## C.4 Subscription Scenario

The example shown below illustrates the use of a parent and child Rights Object to implement a subscription scenario by which a Rights Issuer can extend the validity of a number of Rights Objects and corresponding DRM Content through issuing a single new Rights Object rather than having to re-issue all Rights Objects.

The parent Rights Object specifies the <play> Permission with a <datetime> constraint that ends on April 30. The child Rights Object specifies that the Permissions and Constraints should be inherited from the identified <asset> referencing the parent Rights Object. Once the subscribed DRM Content is about to expire, the Rights Issuer can efficiently extend the subscription by issuing a single, new parent Rights Object with the same subscription URN and an updated <datetime> Constraint, this time set to, e.g., October 31. No change is required to the child Rights Object; it will inherit the <play> Permission with the updated end date.

```
<o-ex:rights
 xmlns:o-ex="http://odrl.net/1.1/ODRL-EX"
 xmlns:o-dd="http://odrl.net/1.1/ODRL-DD"
 xmlns:oma-dd="http://www.openmobilealliance.com/oma-dd"
 xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
 xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
 <o-ex:context>
  <o-dd:version>2.0</o-dd:version>
  <o-dd:uid>RightsObjectID</o-dd:uid>
 </o-ex:context>
 <o-ex:agreement>
  <o-ex:asset>
   <o-ex:context>
    <o-dd:uid>SubscriptionGUID</o-dd:uid>
   </o-ex:context>
  </o-ex:asset>
  <o-ex:permission>
   <o-dd:play>
    <o-ex:constraint>
     <o-dd:datetime>
      <o-dd:end>2004-04-30T23:59:59Z</o-dd:end>
     </o-dd:datetime>
```

```
    </o-ex:constraint>
   </o-dd:play>
  </o-ex:permission>
 </o-ex:agreement>
</o-ex:rights>
```

**Parent Rights Object referencing DRM Content**

```
<o-ex:rights
 xmlns:o-ex="http://odrl.net/1.1/ODRL-EX"
 xmlns:o-dd="http://odrl.net/1.1/ODRL-DD"
 xmlns:oma-dd="http://www.openmobilealliance.com/oma-dd"
 xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
 xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
 <o-ex:context>
  <o-dd:version>2.0</o-dd:version>
  <o-dd:uid>RightsObjectID</o-dd:uid>
 </o-ex:context>
 <o-ex:agreement>
  <o-ex:asset>
   <o-ex:context>
    <o-dd:uid>ContentID</o-dd:uid>
   </o-ex:context>
   <o-ex:inherit>
    <o-ex:context>
     <o-dd:uid>SubscriptionGUID</o-dd:uid>
    </o-ex:context>
   </o-ex:inherit>
   <o-ex:digest>
    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
    <ds:DigestValue>DCFHash</ds:DigestValue>
   </o-ex:digest>
   <ds:KeyInfo>
    <xenc:EncryptedKey>
     <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#kw-aes128"/>
     <xenc:CipherData>
      <xenc:CipherValue>EncryptedCEK</xenc:CipherValue>
     </xenc:CipherData>
    </xenc:EncryptedKey>
    <ds:RetrievalMethod URI="REKReference"/>
   </ds:KeyInfo>
  </o-ex:asset>
 </o-ex:agreement>
</o-ex:rights>
```

**Child Rights Object referencing the Parent Rights Object**

# C.5 Exporting OMA DRM Content

The examples in this section describe export permission for DRM Content and Rights Object in different scenarios.

## C.5.1 Move

```
<o-ex:rights
xmlns:o-ex="http://odrl.net/1.1/ODRL-EX"
xmlns:o-dd="http://odrl.net/1.1/ODRL-DD"
xmlns:oma-dd="http://www.openmobilealliance.com/oma-dd"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
 <o-ex:context>
  <o-dd:version>2.0</o-dd:version>
  <o-dd:uid>RightsObjectID</o-dd:uid>
 </o-ex:context>
 <o-ex:agreement>
  <o-ex:asset>
   <o-ex:context>
    <o-dd:uid>ContentID</o-dd:uid>
   </o-ex:context>
   <o-ex:digest>
    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
    <ds:DigestValue>DCFHash</ds:DigestValue>
   </o-ex:digest>
   <ds:KeyInfo>
    <xenc:EncryptedKey>
     <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#kw-aes128"/>
     <xenc:CipherData>
      <xenc:CipherValue>EncryptedCEK</xenc:CipherValue>
     </xenc:CipherData>
    </xenc:EncryptedKey>
    <ds:RetrievalMethod URI="REKReference"/>
   </ds:KeyInfo>
  </o-ex:asset>
  <o-ex:permission>
   <o-dd:display/>
   <o-dd:print/>
   <oma-dd:export oma-dd:mode="move">
    <o-ex:constraint>
     <oma-dd:system>
      <o-ex:context>
       <o-dd:version>1.0</o-dd:version>
       <o-dd:uid>XYZ</o-dd:uid>
      </o-ex:context>
     </oma-dd:system>
    </o-ex:constraint>
   </oma-dd:export>
  </o-ex:permission>
 </o-ex:agreement>
```

```
</o-ex:rights>
```

## C.5.2 Multiple Permissions for Multiple Content Objects

```
<o-ex:rights
xmlns:o-ex="http://odrl.net/1.1/ODRL-EX"
xmlns:o-dd="http://odrl.net/1.1/ODRL-DD"
xmlns:oma-dd="http://www.openmobilealliance.com/oma-dd"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
 <o-ex:context>
  <o-dd:version>2.0</o-dd:version>
  <o-dd:uid>RightsObjectID</o-dd:uid>
 </o-ex:context>
 <o-ex:agreement>
  <o-ex:asset o-ex:id="Asset-1">
   <o-ex:context>
    <o-dd:uid>ContentID1</o-dd:uid>
   </o-ex:context>
   <o-ex:digest>
    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
    <ds:DigestValue>DCFHash</ds:DigestValue>
   </o-ex:digest>
   <ds:KeyInfo>
    <xenc:EncryptedKey>
     <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#kw-aes128"/>
     <xenc:CipherData>
      <xenc:CipherValue>EncryptedCEK</xenc:CipherValue>
     </xenc:CipherData>
    </xenc:EncryptedKey>
    <ds:RetrievalMethod URI="REKReference"/>
   </ds:KeyInfo>
  </o-ex:asset>
  <o-ex:asset o-ex:id="Asset-2">
   <o-ex:context>
    <o-dd:uid>ContentID2</o-dd:uid>
   </o-ex:context>
   <o-ex:digest>
    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
    <ds:DigestValue>DCFHash</ds:DigestValue>
   </o-ex:digest>
   <ds:KeyInfo>
    <xenc:EncryptedKey>
     <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#kw-aes128"/>
     <xenc:CipherData>
      <xenc:CipherValue>EncryptedCEK</xenc:CipherValue>
     </xenc:CipherData>
    </xenc:EncryptedKey>
```

```
    <ds:RetrievalMethod URI="REKReference"/>
   </ds:KeyInfo>
  </o-ex:asset>
  <o-ex:permission>
   <oma-dd:export oma-dd:mode="copy">
    <o-ex:constraint>
     <o-dd:count>1</o-dd:count>
     <o-dd:datetime>
      <o-dd:start>2004-01-01T00:00:00Z</o-dd:start>
      <o-dd:end>2004-12-31T23:59:59Z</o-dd:end>
     </o-dd:datetime>
     <oma-dd:system>
      <o-ex:context>
       <o-dd:version>1.0</o-dd:version>
       <o-dd:uid>XYZ</o-dd:uid>
      </o-ex:context>
     </oma-dd:system>
    </o-ex:constraint>
   </oma-dd:export>
  </o-ex:permission>
  <o-ex:permission>
   <o-ex:asset o-ex:idref="Asset-1"/>
   <o-dd:play>
    <o-ex:constraint>
     <o-dd:datetime>
      <o-dd:start>2004-01-01T00:00:00Z</o-dd:start>
      <o-dd:end>2004-12-31T23:59:59Z</o-dd:end>
     </o-dd:datetime>
    </o-ex:constraint>
   </o-dd:play>
  </o-ex:permission>
  <o-ex:permission>
   <o-ex:asset o-ex:idref="Asset-2"/>
   <o-dd:print>
    <o-ex:constraint>
     <o-dd:datetime>
      <o-dd:start>2004-01-01T00:00:00Z</o-dd:start>
      <o-dd:end>2004-12-31T23:59:59Z</o-dd:end>
     </o-dd:datetime>
    </o-ex:constraint>
   </o-dd:print>
  </o-ex:permission>
 </o-ex:agreement>
</o-ex:rights>
```