DRM Rights Expression Language

Approved Version 2.1.1 – 31 May 2011

Open Mobile Alliance

OMA-TS-DRM-REL-V2_1_1-20110531-A

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-v2.1] 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 Organisation for Standardisation), 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
[RFC2392]	"Content-ID and Message-ID Uniform Resource Locators", E. Levinson, August 1998, URL:http://www.ietf.org/rfc/rfc2392.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

[DRMARCH-v2.0]	"DRM Architecture V2.0", Open Mobile Alliance™, OMA-AD-DRM-V2-0, URL:http://www.openmobilealliance.org/
[DRMARCH-v2.1]	"DRM Architecture V2.0", Open Mobile Alliance™, OMA-AD-DRM-V2-1, URL:http://www.openmobilealliance.org/
[DRMCF-v2.0]	"DRM Content Format V2,0", Open Mobile Alliance™, OMA-TS-DRM-DCF-V2_0, URL:http://www.openmobilealliance.org/
[DRMCF-v2.1]	"DRM Content Format V2,1", Open Mobile Alliance™, OMA-TS-DRM-DCF-V2_1, URL:http://www.openmobilealliance.org/
[DRMRELDDXSD-v2.1]	"DRM REL ODRL Mobile profile Data Dictionary ROAP schema V2.1", Open Mobile Alliance™, OMA-TS-DRM-RELDD-V2_1, URL:http://www.openmobilealliance.org/
[DRMRELODDXSD-v2.1]	"DRM REL OMA Data Dictionary schema V2.1", Open Mobile Alliance™, OMA-TS-DRM-RELODD-V2_1, URL:http://www.openmobilealliance.org/
[DRMRELXSD-v2.1]	"DRM REL ODRL Mobile profile Expression Language schema V2.1", Open Mobile Alliance™, OMA-TS-DRM-REL-V2_1, URL:http://www.openmobilealliance.org/
[DRM-v2.0]	"Digital Rights Management V2.0", Open Mobile Alliance™, OMA-TS-DRM-DRM-V2_0, URL:http://www.openmobilealliance.org/

[DRM-v2.1] "Digital Rights Management V2.1", Open Mobile Alliance™, OMA-TS-DRM-DRM-V2_1, 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.
Device	A Device is a user equipment with a DRM Agent. The Device MAY include a smartcard module (e.g. a SIM) or not depending upon implementation.
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.
Meterable Event	A Meterable Event is an event that meets the RI defined criteria for metering.
Metered Content	When DRM Content is accessed via an RO that contains the <tracked> element, the content is said to be Metered Content.
Metering	Recording of usage information (the number of times that the associated DRM Content has been consumed and the accumulated usage time) upon consumption of an RO which contains the <tracked> element. Metering enables a Rights Issuer to collect usage information from Devices for the purpose of royalty collection.
Metering Information	The information that is recorded for purposes of Metering.
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 (see http://www.openmobilealliance.org/tech/omna/index.htm)
ODRL	Open Digital Rights Language
REL	Rights Expression Language
REK	Rights Object Encryption Key

SHA-1	Secure Hash Algorithm
SMS	Short Message Service
WAP	Wireless Application Protocol
XML	Extensible Markup Language

4. Introduction

OMA "Digital Rights Management" (DRM) enables the distribution and consumption of digital content in a controlled manner by enabling Content Issuers to distribute DRM Content and Rights Issuers to issue Rights Objects for the DRM Content.

This specification defines the OMA DRM v2.1 Rights Expression Language (REL v2.1) to construct DRM v2.1 Rights Objects and is one part of a set of OMA DRM 2.1 technical specifications. For a detailed discussion of the overall system architecture, please refer to [DRMARCH-v2.1]. For a detailed discussion of the DRM Content Format in OMA DRM v2.1, please refer to [DRMDCF-v2.1]. For a detailed discussion of the format and semantics of the cryptographic protocol, messages, processing instructions and certificate profiles to enable an end-to-end system for DRM protected content distribution, see the DRM part [DRMDRM-v2.1] of OMA DRM v2.1.

4.1   Version 1.0

The OMA DRM v1.0 specification provides some fundamental building blocks for a DRM system without addressing the complete security necessary for a robust, end-to-end DRM system that takes into account the need for secure distribution, authentication of Devices, revocation and other aspects.

OMA DRM v1.0 does not specify a Rights Expression Language.

4.2   Version 2.0

The main differences between OMA DRM v1.0 and OMA DRM v2.0 are significantly improved security and functionality. One of the important new features of OMA DRM v2.0 is a Rights Expression Language.

The The OMA DRM v2.0 Rights Expression Language (RELV2.0) specifies the syntax and semantics of rights governing the usage of DRM Content based on the Open Digital Rights Language [ODRL]

The REL v2.0 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 authorised Devices.

The goal of the REL v2.0 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 rights 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.

The following are not goals of the REL v2.1 specification:

- 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.

4.2.1   Version 2.0.1

The most important REL changes introduced in DRM v2.0.1 compared with DRM v2.0 are summarized in section 4.2.1 of the REL Specification [DRMREL v2.0] in the DRM 2.0.1 ERP. These changes are considered to require special consideration in implementation. Most of the identified changes are bug fixes which if not implemented correctly may result in interoperability problems between conformant and non-conformant devices. Companies with existing DRM 2.0 implementations should take careful consideration of these changes.

4.3   Version 2.1

OMA DRM v2.1 has been developed as a result of market feedback. The main differences between OMA DRM v2.0 and OMA DRM v2.1 are the addition of several features on top of OMA DRM v2.0, including:

- Metering, primarily intended for information gathering. By means of metering, actual content usage information can be provided to Rights Issuers, thereby enabling royalty collection based on actual usage of content.

- Content differentiation, defining a mechanism to control how content can be consumed. For example, this mechanism can prevent a music track to be used as ringtone.

- RO installation confirmation.

- Additional metadata, such as artist, title and genre

- Support for user editable metadata, in addition to content issuer defined metadata.

- A binary format for ROAP triggers to improve communication efficiency.

- New domain property (noConsumeAfter) to simplify "temporary sharing" business models

- RO upload functionality to enable users to upload Rights from their old device to a Rights Issuer so that these Rights can be downloaded to their new device.

- Improved extensibility for future versions.

The DRM 2.1 features have minimum impact on the DRM 2.0 architecture and are defined in a DRM 2.0 backward compatible manner.

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

- Requirements model

- Inheritance model

- Security model

The rights expression language is defined as a mobile profile, i.e., a subset, of ODRL. Section 5.9 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.

5.1.1.1   Attribute "id"

Attribute	<!ATTLIST o-ex:rights o-ex:id ID #REQUIRED>
Semantics	The o-ex:id attribute of the <rights> element identifies the <rights> element in the context of a protected rights object (see [DRM-v2.1]).
	The value of the o-ex:id attribute MAY be used in the <ds:Reference> element of the <signature> of the <roap:ROPayload> element.

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.
	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.
	The optional <digest> element provides integrity protection for the reference to the DRM Content.
	The optional <KeyInfo> element provides the functionality to access the DRM content if granted the rights to do so.
	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>.
	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.
	It SHOULD be omitted if there is no reference to the <asset> element from elsewhere in the same Rights Object.
	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.
	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.
	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, in the <individual> element, in the <system> element, and in the <inherit> 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.
	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.
	A <context> element MUST NOT contain more than one <uid> element unless the <context> element is contained in the <individual> 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.
	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 "2.1" (without quotes).

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. The value MUST match the "id" attribute of the <ro> element of type ROPayload (see [DRM-v2.1], section 5.3.10).
	If its parent <context> element is included in the <asset> element, the <uid> element specifies a DCF ContentID (see [DRMCF-v2.1]), a DCF GroupID (see [DRMCF-v2.1]), or a "virtual" UID for a parent Rights Object (see section 5.7). The format of the <uid> MUST conform to [RFC2396]. If the <uid> is a DCF ContentID the value MUST be according to the "cid:" Uniform Resource Locator (URL) scheme (defined in [RFC2392]). If the <uid> is a DCF GroupID the value MUST use the URL format of [RFC2392] except the scheme name must be "gid:". If the <uid> element identifies a parent Rights Object the value MUST use the URL format of [RFC2392] except the scheme name must be "pid:". In the case of Parent ROs the <uid> SHOULD NOT contain the content identifier of an actual DCF, but contain a "virtual" UID denoting, for example, a subscription.
	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.
	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.
	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.
	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.
	If the <export> permission is granted to more than one target system, then these are enumerated by using multiple <context> elements, each containing one <uid> element. In this case, the <count> constraint applies to the combined export transactions of all target systems.
	The only instances when a <context> element MAY contain more than one <uid> element is when the <context> element is contained in an <individual> element.
	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 5.7).

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 onExpiredURL attribute, 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.
	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 honour the top level constraint in addition to honouring possible constraints specified as a child element to a permission element, e.g., <play>, when granting access to content according to such a permission.
	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.
	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.
	The <asset> elements specified within the <permission> element enable expression linking allowing its sibling permission elements (e.g. <play>, <display>) 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.
	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.
	If no <asset> element is present in a <permission> element, then the permission applies to all <asset> sibling elements in the same Rights Object.
	The <export> permission is associated with all <asset> elements within the same Rights Object. This implies that there SHOULD only be one <export> element within the Rights Object. Therefore the <permission> element containing an <export> element MUST NOT contain an <asset> element.

5.4.1.1 Attribute <onExpiredURL>

Element	<!ATTLIST o-ex:permission oma-dd:onExpiredURL CDATA #IMPLIED>
Semantics	The value of the onExpiredURL attribute MUST be a URL according to [RFC2396]. Note: See [DRM-v2.1] for DRM Agent behaviour.

5.4.2 Element <play>

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

Semantics	The <play> element grants the permission to create a transient representation of audio or video Content. It contains an optional <constraint> element and an optional <requirement> element.
	If the <requirement> element is specified, the DRM Agent MUST ensure that the requirements specified by this element are fulfilled before using this permission element. If any of the specified requirements is not met, then the DRM Agent MUST NOT use this permission element to grant access to DRM Content.
	If the <constraint> element is specified the DRM Agent MUST grant play rights according to the <constraint> child element and the top-level <constraint> element if any. If no child <constraint> element is specified, the DRM Agent MUST grant play rights according to the top-level <constraint> element if any. If neither child nor top-level <constraint> element is specified, the DRM Agent MUST grant unlimited play rights.
	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.
	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.
	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 utilised instead (section 5.4.4).

5.4.3 Element <display>

Element	<!ELEMENT o-dd:display (o-ex:constraint?, o-ex:requirement?)>
Semantics	The <display> element grants the permission to make a transient visible rendering of the Content. It contains an optional <constraint> element and an optional <requirement> element.
	If the <requirement> element is specified, the DRM Agent MUST ensure that the requirements specified by this element are fulfilled before using this permission element. If any of the specified requirements is not met, then the DRM Agent MUST NOT use this permission element to grant access to DRM Content.
	If the <constraint> element is specified the DRM Agent MUST grant display rights according to the <constraint> child element and the top-level <constraint> element if any. If no child <constraint> element is specified, the DRM Agent MUST grant display rights according to the top-level <constraint> element if any. If neither child nor top-level <constraint> element is specified, the DRM Agent MUST grant unlimited display rights.
	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.
	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?, o-ex:requirement?)>
Semantics	The <execute> element grants permissions over the primitive computing element execute. It contains an optional <constraint> element and an optional <requirement> and element.
	If the <requirement> element is specified, the DRM Agent MUST ensure that the requirements specified by this element are fulfilled before using this permission element. If any of the specified requirements is not met, then the DRM Agent MUST NOT use this permission element to grant access to DRM Content.
	If the <constraint> element is specified the DRM Agent MUST grant execution rights according to the <constraint> child element and the top-level <constraint> element if any. If no child <constraint> element is specified, the DRM Agent MUST grant execution rights according to the top-level <constraint> element if any. If neither child nor top-level <constraint> element is specified, the DRM Agent MUST grant unlimited execution rights.
	The <execute> element has the semantics of executing, i.e., invoking, DRM Content, e.g., Java^{TM} 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?, o-ex:requirement?)>
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 and an optional <requirement> element.
	If the <requirement> element is specified, the DRM Agent MUST ensure that the requirements specified by this element are fulfilled before using this permission element. If any of the specified requirements is not met, then the DRM Agent MUST NOT use this permission element to grant access to DRM Content.
	If the <print> element is specified the DRM Agent MUST grant print rights according to the <constraint> child element and the top-level <constraint> element if any. If no child <constraint> element is specified, the DRM Agent MUST grant print rights according to the top-level <constraint> element if any. If neither child nor top-level <constraint> element is specified, the DRM Agent MUST grant unlimited print rights.
	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. 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. It contains a mandatory <constraint> element.
	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. The DRM Agent MUST grant export rights according to the <constraint> child element and the top-level <constraint> element if any.
	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. During an Export operation all <permission> elements and <asset> elements within the exported enabled Rights Objects are transcribed to the target DRM system per the mapping established by the appropriate governing bodies that are allowing the export.
	If any <asset> elements within an <export> enabled Rights Object refer to a DCF Group ID then the export permission applies to all Content Objects in that Group.
	If the <export> element is contained within a Parent RO then all related Child ROs inherit the export permission, allowing all DRM Content referenced by the Child ROs to be exported.

5.4.6.1   Attribute "mode"

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

Semantics	move:
	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.
	When exporting the Rights Object and the mode attribute is equal to "move", the DRM agent MUST export the original Rights Object <u>with</u> 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.
	copy:
	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.
	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. If the original Rights Object is a stateful RO, this will result in consuming the content without limit.To avoid the risk, the <constraint> element within the <export> element in a stateful RO should have the <count> element, or the <datetime> element, or the <interval> element.
	When the mode attribute is equal to "copy", the DRM agent MUST export the original Rights Object <u>without</u> 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. The state of the <export> permission's constraints MUST be updated on the Device from which it is exported.
	Note that state information refers to the state maintained by the Device when consuming rights and not to the value originally defined in the Rights Object.
	For both "move" and "copy", whether the <export> element is to be transcribed together with the rest of the Rights Object depends on the presence and the value of the "transcribe" attribute, see Section 5.4.6.2.

5.4.6.2   Attribute "transcribe"

Attribute	<!ATTLIST oma-dd:export oma-dd:transcribe (true | false | 1 | 0) "false">
Semantics	The transcribe attribute contains a boolean value. If the value is "false" (the default value) or "0", then the DRM Agent SHALL follow the <export> semantics of [above]. Otherwise, the DRM Agent MUST transcribe the <export> permission and its constraint (together with the other permissions/constraints other than <export> permission) into target DRM system.
	It is RECOMMENDED that Rights Issuers do not include a <count> constraint in an <export> permission if the transcribe attribute is true.

5.5 Requirements Model

The requirement model enhances the permission model by allowing specific pre-conditions that should be fulfilled in order to obtain the related permissions.

Requirements are associated with one permission element at a time. For a permission to be granted all its requirements MUST be fulfilled. If a requirement is not understood or cannot be enforced by the consuming Device the parent permission is invalid and MUST NOT be granted. If present, a <requirement> element SHOULD contain at least one of its child elements. If a <requirement> element does not contain any requirements such as <tracked>, it does not require any specific pre-condition to be fulfilled.

For a given permission element to be allowed, the requirements specified by the permission element specific <requirement> element (if present) MUST be respected.

5.5.1   Element <requirements>

Element	<!ELEMENT o-ex:requirement (o-dd:tracked?)>
Semantics	The <requirements> element contains an optional <tracked> element.
	Requirements are associated with one permission element at a time. For a permission to be granted all its requirements MUST be fulfilled. If a requirement is not understood or cannot be enforced by the consuming Device the associated permission is invalid and MUST NOT be granted.
	If present, a <requirement> element SHOULD contain the <tracked> element. If a <requirement> element does not contain the <tracked> element, it does not require any specific pre-condition to be fulfilled.
	The <requirement> element MUST only be present as a child element to other permission elements such as <play> and <display>, it MUST NOT be present as a top-level requirement. If a DRM Agent receives an RO with a top-level requirement it MUST ignore this requirement.

5.5.2   Element <tracked>

Element	<!ELEMENT o-dd:tracked EMPTY>

Semantics	The `<tracked>` element indicates that DRM Agent is required to record Metering Information.
	The Metering Information SHALL consist of the number of times that the DRM Content has been consumed and the accumulated usage time that the DRM Content has been consumed for.
	Enablement and disablement of Metering is described in Section 11 of [DRM-v2.1].
	If metering is not enabled for the RI who issued the RO and the contentAccessGranted attribute is not present, or it is present and the value is "false" or "0", the DRM Agent MUST NOT grant access to the DRM Content.
	If metering is not enabled for this RI and the contentAccessGranted is present with the value "true" or "1", the DRM Agent MUST grant access to the DRM Content, but MUST NOT store Metering Information associated with the consumption of the associated DRM Content.
	If metering is enabled for this RI and the `<tracked>` element is present in the RO and if the `timed` attribute is not present, or it is present and the value is equal to zero, or if the Device is not able to measure the time since the Device began to access the DRM Content, then the DRM Agent MUST record the appropriate Metering Information immediately upon the Device beginning to access the DRM Content, as referenced via the `<uid>` element in the `<context>` element of the `<asset>` element of the RO.
	If metering is enabled for this RI and the `<tracked>` element is present in the RO and the `timed` attribute is present and its value is bigger than zero and if the Device is still accessing the DRM Content, as referenced via the `<uid>` element in the `<context>` element of the `<asset>` element of the RO, after the number of seconds specified by the value of the `timed` attribute then DRM Agent MUST record the appropriate Metering Information.
	If metering is enabled for this RI and the `<tracked>` element is defined in a parent RO then the DRM Agent MUST record the appropriate Metering Information as defined above for the associated DRM Content as referenced via the `<uid>` element in the `<context>` element of the `<asset>` element of the child RO.

5.5.2.1   Attribute <timed>

Element	`<!ATTLIST o-dd:tracked oma-dd:timed CDATA "0">`
Semantics	The `timed` attribute contains a non-negative integer value. It specifies the number of seconds after which the access to the DRM Content SHALL be considered a Meterable Event. The default value is 0 seconds which implies that the DRM Agent MUST immediately record Metering Information for the DRM Content being consumed.

5.5.2.2   Attribute < contentAccessGranted >

Element	`<!ATTLIST o-dd:tracked oma-dd: contentAccessGranted (true | false | 1 | 0) "false">`

Semantics	The `contentAccessGranted` attribute contains a boolean value. If the value is "true" or "1", the DRM Agent MUST grant the access to the DRM Content even if the metering is not enabled. Otherwise, the DRM Agent MUST NOT grant the access to the DRM Content if the metering is disabled. If the metering is enabled the DRM Agent MUST ignore this attribute.

5.6 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.

5.6.1 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. The <constraint> element contains <system> elements only when its parent <permission> element contains the <export>, <play>, or <display> element.

5.6.1.1 Attribute "id"

Attribute	<!ATTLIST o-ex:constraint o-ex:id ID #IMPLIED>
Semantics	The "id" attribute is the optional identifier of the <constraint> element. It uniquely identifies each <constraint>. When present, the "id" attribute MUST be unique within the Rights Object. This attribute is used when uploading Rights Objects to the RI as specified in [DRM-v2.1]. In the Rights Object Upload protocol the latest state information for each stateful constraint must be uploaded. The "id" attribute is used to associate the updated constraints with the constraints in the original Rights Object. If the Rights Issuer supports the Rights Object Upload protocol, then this attribute MUST be specified if the <constraint> element contains any of the following elements: <count>, <timed-count>, <interval> or <accumulated>.

5.6.2 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.
	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.
	When used to constrain the <play> permission, the count MUST be decremented immediately upon play.
	When used to constrain the <display> permission, the count MUST be decremented immediately upon display.
	When used to constrain the <print> permission, the count MUST be decremented immediately upon commencement of printing.
	When used to constrain the <execute> permission, the count MUST be decremented upon commencement of execution.
	When used to constrain the <export> permission, the count MUST be decremented upon commencement of an export process. If an <export> permission is granted to more than one target system (multiple <context> elements within the system constraint) then any <count> constraint applies to the combined export transactions of all target systems.
	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.

5.6.3   Element <timed-count>

Element	<!ELEMENT oma-dd:timed-count (#PCDATA)>
Semantics	The semantics of the <timed-count> element are as for the <count> element (5.6.2) with the addition of an optional timer attribute (section 5.6.3.1).
	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.
	The <timed-count> element MUST NOT occur as a constraint to a <print> or <export> permission.

5.6.3.1   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 5.6.3) is reduced starting from beginning to render the Content.
	For example, if the timer value is set to "30" (without the quotes) and the <timed-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.

5.6.4 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.
	If the <start> element is present, its semantics are 'not before' the specified time/date.
	If the <end> element is present, its semantics are 'not after' the specified time/date.
	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.
	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.
	The DRM Agent of a consuming Device without DRM Time MUST NOT grant access to DRM Content according to permissions containing the <datetime> element.

5.6.4.1 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].
	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.
	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.

5.6.4.2 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]. 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. 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: 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.

5.6.5 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:

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.

The general format used for specifying interval values is defined in [IS8601].

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.

The specified period SHOULD be greater than zero. If the specified period is equal to zero, then the permission MUST NOT be granted.

[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.

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. |
|---|---|

5.6.6   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]. 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. The specified period SHOULD be greater than zero. If the specified period is equal to zero, then the permission MUST NOT be granted. [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. 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: 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. 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. The <accumulated> element MUST NOT occur as a constraint to a <print> or <export> permission.

5.6.7   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. 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.

5.6.8   Element <system>

Element	<!ELEMENT oma-dd:system (o-ex:context+)>

Semantics	The <system> element MUST only occur as a constraint to an <export>, <play>, or <display> permission. In the case of <export>, the <system> constraint specifies the target system(s) to which DRM Content and Rights Object(s) can be copied or moved. In the case of <play> and <display>, the <system> constraint specifies the target system(s) to which DRM Content may be transiently rendered. The target system(s) are described in the mandatory <context> element(s). If multiple context elements occur these shall be treated exclusively, thereby allowing export/consumption on any of those systems.

5.7   Inheritance Model
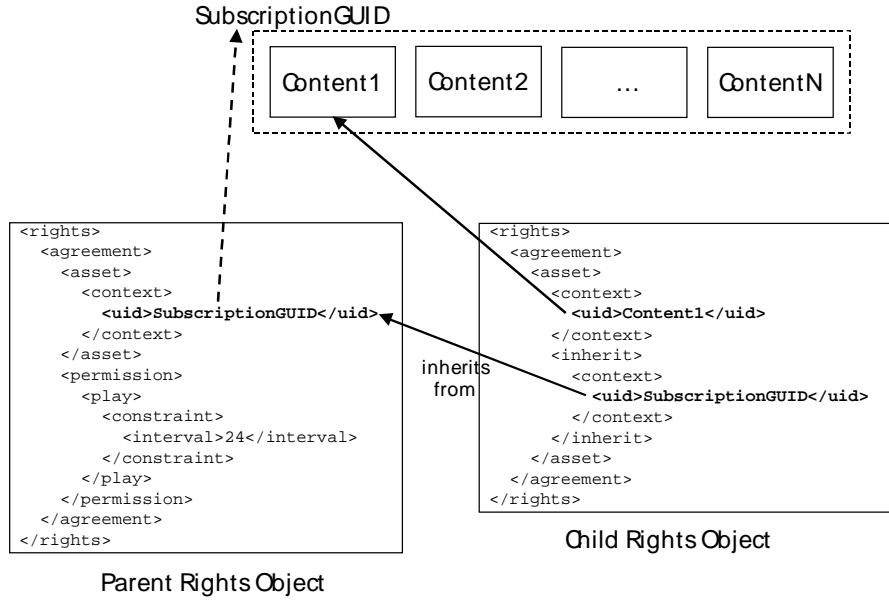
This section describes how a parent Rights Object can specify Permissions and Constraints for one or more pieces of DRM Content each governed by a child Rights Object, using a limited subset of the ODRL inheritance model. The DRM Agent MUST NOT accept parent child Rights Objects constellations with more 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.

5.7.1   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.
	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.
	When exercising permissions, 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 if there are no applicable <permission> elements within the child Rights Object itself. When the child refers to multiple parent Rights Objects, the DRM Agent MUST select exactly one of these from which the child is allowed to inherit permissions and constraints. This selection SHALL be done in accordance with the Rights Objects selection algorithm as defined in section 5.10.
	For each consumption of the DRM Content, the agent MUST select exactly one <permission> element from installed rights objects, according to which access will be granted. Note that it is allowed that the Child Rights Object specifies no <permission> elements. In that case, the <permission> elements inherited from the Parent Rights Object still apply.
	When granting access to DRM Content according to a specific permission element, e.g.,<play> of a <permission> element, the DRM Agent MUST enforce the top-level constraints of that <permission> element as well as possible constraints of the specific permission element 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.
	Child Rights Objects MUST NOT inherit from more than one parent Rights Object simultaneously, the DRM Agent MUST always select one parent Rights Object from which the Child Rights Object may inherit permissions and constraints. A parent Rights Object MUST NOT be a child Rights Object at the same time.

Figure 1 depicts the above described relationships between parent Rights Object, child Rights Object, and DRM Content with the example of a subscription model.

Figure 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.

Access to DRM Content through a child <asset> that has an <inherit> child element requires selection of an appropriate <permission> element from the Child Rights Object or selection of an appropriate <permission> element in a Parent Rights Object. The DRM Agent SHALL use exactly one <permission> element that contains a permission element that is appropriate for the type of requested access. In case both the Child Rights Object as well as the Parent Rights Object contain suitable <permission> elements, then the DRM Agent MUST select the most appropriate <permission> element to use, this selection SHALL be done in accordance with section 5.10.

Note that a parent <asset> is not allowed to inherit permissions and constraints from other parent <asset> elements and therefore it SHOULD NOT contain an <inherit> child element. An <asset> element with an <inherit> child element but without a <ds:KeyInfo> child element is semantically illegal and SHALL NOT be used by the DRM agent to grant access to DRM Content. Such an illegal asset SHALL NOT inherit permissions and constraints, and permissions and constraints SHALL NOT be inherited from it by child <asset> elements.

Note further that a parent <asset> can be distinguished from a child <asset> as the former does not hold a <ds:KeyInfo> element, whereas the latter holds a <ds:KeyInfo> element and an <inherit> element.

5.8 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 5.8.1 and 5.8.2 of this specification. The latter is specified in [DRM-v2.1]. Rights Objects defined in this specification MUST be contained in a <ProtectedRO> element as defined in [DRM-v2.1] to protect against unauthorised 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].

5.8.1 Content Confidentiality

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

This concept is realised in [DRM-v2.1] by i) encrypting the Content thus transforming it into DRM Content [DRMCF-v2.1], and ii) sharing the key(s) required to decrypt the DRM Content only with those parties that are authorised 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 may contain an (intermediate) key that in turn encrypts the Content. . If the ContentID contained in the <asset> element matches the ContentID stored in the Common Headers Box associated with the content item (see [DRMCF-v2.1]), then the CEK contained in the Rights Object was used to encrypt the content directly. If the ContentID matches the GroupID value stored in the OMADRMGroupID box, then the CEK in the Rights Object was used to encrypt the content item's encryption key.

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 unauthorised 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 7.2 of [DRM-v2.1] 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:

<div align="center">

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

</div>

The corresponding XML security elements are described next.

5.8.1.1 Element <KeyInfo>

Element	<!ELEMENT ds:KeyInfo (xenc:EncryptedKey?, ds:RetrievalMethod?)>
Semantics	The <KeyInfo> element has a dual purposes, depending on its parent element. 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. 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-v2.1]).

5.8.1.2 Element <EncryptedKey>

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

5.8.1.3 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.

5.8.1.3.1 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. The algorithm MUST be AES128 Key Wrap.

5.8.1.4 Element <CipherData>

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

5.8.1.5 Element <CipherValue>

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

5.8.1.6 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.

5.8.1.6.1 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-v2.1]). 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-v2.1].

5.8.2   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-v2.1].

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.

5.8.2.1   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. 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 5.7) or if the Rights Object is a group Rights Object.

5.8.2.2   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.

5.8.2.2.1   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.

5.8.2.3   Element <DigestValue>

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

5.8.3   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-v2.1].

5.9   ODRL and Forward Compatibility

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

This specification defines mechanisms that enable future versions of OMA DRM to extend the REL in such a way that correct instances of the future extensions validate against the REL XML Schemas defined in this specification, as described in more detail in Appendix I of [DRM-v2.1].

The DRM Agent of a Device encountering any elements (e.g. from ODRL [ODRL], future versions or proprietary extensions) 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 unsupported <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 <agreement> element SHOULD be ignored.

- Unsupported <revoke> elements SHOULD be ignored.

- Unsupported elements of the ODRL security model SHOULD be ignored.

5.10   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 to apply when accessing content, in case there are multiple rights for this content. This also applies to automatically selecting between multiple applicable Parent Rights Objects if the content is accessed via a Child Rights Object. In this section, the term 'rights' is to be understood to refer to a combination of an <asset> element and an associated <permission> element.

1. Only rights 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. Any rights with no constraints should be used first.
3. Any rights containing a <datetime> constraint (and potentially other constraints) should be used to grant access to content before using rights that do not contain a <datetime> constraint.
4. If multiple rights 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 utilised first.

5. If multiple rights 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. Any rights containing a <timed-count> should be used before rights containing <count>.
7. There is no priority between <accumulated> and <count>. It is up to the agent to consume one prior to the other according to its internal consumption rules.

If the DRM Agent needs to automatically select between two <export> permissions which are equivalent according to the above semantics, then the DRM Agent MUST select <export> permissions with mode of "copy", before <export> permissions with mode of "move".

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

6. Syntax

A DRM Agent MUST be able to parse all elements defined by the combination of [DRMRELXSD-v2.1], [DRMRELDDXSD-v2.1] and [DRMRELODDXSD-v2.1] and MUST handle any valid unknown elements as specified in section 5.9.

As described in section 5.9, this specification defines a subset, i.e., a mobile profile, of ODRL that is forward compatible as described in more detail in Appendix I of [DRM-v2.1]. Jointly [DRMRELXSD-v2.1] and [DRMRELDDXSD-v2.1] define the ODRL subset and also define (in a way that is different from ODRL) the future extensions that DRM Agents must anticipate. The additional permissions and constraints beyond those provided by ODRL are defined in [DRMRELODDXSD-v2.1].

The Rights Objects that are valid in OMA DRM as defined by the combination of [DRMRELXSD-v2.1], [DRMRELDDXSD-v2.1] and [DRMRELODDXSD-v2.1] are also ODRL compatible. This means that they validate against the ODRL schema except for the OMA specific extensions. The OMA specific extensions defined in [DRMRELODDXSD-v2.1] are utilizing the extension mechanisms provided by the original ODRL expression language and schemas and MAY also be used with the original full ODRL Schemas.

The previous version of this specification, part of the OMA DRM 2.0 enabler, used XML document type definition [XML] to specify the ODRL mobile profile for OMA DRM 2.0. This version uses [XMLSchema] to normatively specify the ODRL mobile profile, for reasons of consistency with the other documents in the OMA DRM enabler, particularly in the area of the mechanisms for forward compatibility. However, for convenience, a document type definition of the elements defined in this version of the ODRL mobile profile is also provided. This document type definition has the public identifier '-//OMA//DTD DRMREL 2.1//EN' and is located at 'http://www.openmobilealliance.org/tech/DTD/drmrel21.dtd'. Please note this is an informative document.

6.1   ODRL-Mobile profile Expression Language

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://odrl.net/1.1/ODRL-EX"
xmlns:enc="http://www.w3.org/2001/04/xmlenc#" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:o-ex="http://odrl.net/1.1/ODRL-EX"
elementFormDefault="qualified" attributeFormDefault="qualified" version="1.1">

    <xsd:import namespace="http://www.w3.org/2000/09/xmldsig#"
schemaLocation="http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/xmldsig-core-
schema.xsd"/>
    <xsd:import namespace="http://www.w3.org/2001/04/xmlenc#"
schemaLocation="http://www.w3.org/TR/xmlenc-core/xenc-schema.xsd"/>


    <xsd:element name="rights" type="o-ex:rightsType"/>
    <xsd:complexType name="rightsType">
        <xsd:sequence minOccurs="1" maxOccurs="1">
                <xsd:element ref="o-ex:context" minOccurs="1" maxOccurs="1"/>
                <xsd:element ref="o-ex:agreement" minOccurs="1" maxOccurs="1"/>
                <xsd:any  minOccurs="0" maxOccurs="unbounded" processContents="lax"/>
        </xsd:sequence>
        <xsd:attributeGroup ref="o-ex:IDGroup"/>

    </xsd:complexType>


    <xsd:element name="agreement" type="o-ex:offerAgreeType"/>
    <xsd:complexType name="offerAgreeType">
        <xsd:sequence minOccurs="1" maxOccurs="1">
                <xsd:element ref="o-ex:asset" minOccurs="1" maxOccurs="unbounded"/>
```

```
                    <xsd:element ref="o-ex:permission" minOccurs="0" maxOccurs="unbounded"/>

            </xsd:sequence>
    </xsd:complexType>


    <xsd:element name="context" type="o-ex:contextType"/>
    <xsd:element name="contextElement" abstract="true"/>
    <xsd:complexType name="contextType">
            <xsd:sequence minOccurs="1" maxOccurs="1">
                    <xsd:any  minOccurs="0" maxOccurs="unbounded" processContents="lax"/>
            </xsd:sequence>
            <xsd:attributeGroup ref="o-ex:IDGroup"/>
    </xsd:complexType>


    <xsd:complexType name="inheritType">
            <xsd:sequence minOccurs="1" maxOccurs="1">
                    <xsd:element ref="o-ex:context" minOccurs="1" maxOccurs="1"/>
            </xsd:sequence>
    </xsd:complexType>
    <xsd:element name="inherit" type="o-ex:inheritType"/>


    <xsd:complexType name="assetType">
            <xsd:choice minOccurs="0" maxOccurs="unbounded">
                    <xsd:element ref="o-ex:context"/>
                    <xsd:element ref="o-ex:inherit"/>
                    <xsd:element name="digest">
                            <xsd:complexType>
                                        <xsd:choice minOccurs="0" maxOccurs="unbounded">
                                                    <xsd:element ref="ds:DigestMethod"/>
                                                    <xsd:element ref="ds:DigestValue"/>
                                        </xsd:choice>
                            </xsd:complexType>
                    </xsd:element>
                    <xsd:element ref="ds:KeyInfo"/>
            </xsd:choice>
            <xsd:attributeGroup ref="o-ex:IDGroup"/>
    </xsd:complexType>
    <xsd:element name="asset" type="o-ex:assetType"/>


    <xsd:element name="permission" type="o-ex:permissionType"/>
    <xsd:element name="permissionElement" abstract="true"/>
    <xsd:complexType name="permissionType">
            <xsd:sequence minOccurs="1" maxOccurs="1">
                    <xsd:any  minOccurs="0" maxOccurs="unbounded" processContents="lax"/>
            </xsd:sequence>
            <xsd:attribute name="exclusive" type="xsd:boolean" use="optional"/>
            <xsd:attributeGroup ref="o-ex:IDGroup"/>
    </xsd:complexType>


    <xsd:element name="constraint" type="o-ex:constraintType"/>
    <xsd:element name="constraintElement" abstract="true"/>
```

```
        <xsd:complexType name="constraintType">
            <xsd:sequence minOccurs="1" maxOccurs="1">
                <xsd:any  minOccurs="0" maxOccurs="unbounded" processContents="lax"/>
            </xsd:sequence>
            <xsd:attributeGroup ref="o-ex:IDGroup"/>
            <xsd:attribute ref="o-ex:type"/>
        </xsd:complexType>
        <xsd:attribute name="type" type="xsd:anyURI"/>

        <xsd:element name="requirement" type="o-ex:requirementType"/>
        <xsd:element name="requirementElement" abstract="true"/>
        <xsd:complexType name="requirementType">
            <xsd:sequence minOccurs="1" maxOccurs="1">
                <xsd:any  minOccurs="0" maxOccurs="unbounded" processContents="lax"/>
            </xsd:sequence>
            <xsd:attributeGroup ref="o-ex:IDGroup"/>
        </xsd:complexType>

        <xsd:attributeGroup name="IDGroup">
            <xsd:attribute name="id" type="xsd:ID"/>
            <xsd:attribute name="idref" type="xsd:IDREF"/>
            <xsd:anyAttribute namespace="##other"/>
        </xsd:attributeGroup>
</xsd:schema>
```

Figure 2: ODRL-Mobile profile Expression Language

6.2   **ODRL-Mobile profile 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://odrl.net/1.1/ODRL-DD" xmlns:o-
ex="http://odrl.net/1.1/ODRL-EX" xmlns:o-dd="http://odrl.net/1.1/ODRL-DD"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
attributeFormDefault="qualified" version="1.1">

    <xsd:import namespace="http://odrl.net/1.1/ODRL-EX" schemaLocation="OMADRMREL.xsd"/>


    <!-- Declare all the Permission Elements of ODRL Mobile Profile-->
    <xsd:element name="display" type="o-ex:permissionType" substitutionGroup="o-
ex:permissionElement"/>
    <xsd:element name="print" type="o-ex:permissionType" substitutionGroup="o-
ex:permissionElement"/>
    <xsd:element name="play" type="o-ex:permissionType" substitutionGroup="o-
ex:permissionElement"/>
    <xsd:element name="execute" type="o-ex:permissionType" substitutionGroup="o-
ex:permissionElement"/>

    <!-- Declare all the Requirements Elements of ODRL Mobile Profile-->
    <xsd:element name="tracked" type="o-ex:requirementType" substitutionGroup="o-
ex:requirementElement"/>


    <!-- Declare all the Context Elements of ODRL Mobile Profile-->
```

```
    <xsd:element name="uid" type="o-dd:uriAndOrString" substitutionGroup="o-
ex:contextElement"/>
    <xsd:element name="version" type="xsd:string" substitutionGroup="o-ex:contextElement"/>


    <!-- Declare all the Constraint Elements of ODRL Mobile Profile-->
    <xsd:element name="individual" type="o-ex:constraintType" substitutionGroup="o-
ex:constraintElement"/>
    <xsd:element name="datetime" type="o-dd:dateType" substitutionGroup="o-
ex:constraintElement"/>
    <xsd:element name="accumulated" type="xsd:duration" substitutionGroup="o-
ex:constraintElement"/>
    <xsd:element name="interval" type="xsd:duration" substitutionGroup="o-
ex:constraintElement"/>
    <xsd:element name="count"  substitutionGroup="o-ex:constraintElement">
        <xsd:complexType>
            <xsd:simpleContent>
                <xsd:extension base="xsd:positiveInteger">
                        <xsd:attributeGroup ref="o-ex:IDGroup"/>
              <xsd:attribute ref="o-ex:type"/>
                </xsd:extension>
            </xsd:simpleContent>
        </xsd:complexType>
    </xsd:element>


    <!-- Declare used types  for ODRL Mobile Profile-->
    <xsd:simpleType name="uriAndOrString">
        <xsd:union memberTypes="xsd:anyURI xsd:string"/>
    </xsd:simpleType>


    <xsd:complexType name="dateType">
        <xsd:sequence>
            <xsd:element name="start" type="o-dd:dateAndOrTime" minOccurs="0"/>
            <xsd:element name="end" type="o-dd:dateAndOrTime" minOccurs="0"/>
        </xsd:sequence>
    </xsd:complexType>


    <xsd:simpleType name="dateAndOrTime">
        <xsd:union memberTypes="xsd:date xsd:dateTime"/>
    </xsd:simpleType>
</xsd:schema>
```

Figure 3: ODRL-Mobile profile Data Dictionary

6.3   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"?>
<!--
OMA Data Dictionary V2.0 XML Schema


Copyright Open Mobile Alliance Ltd., 2006
```

```
        All rights reserved

Terms and conditions of use are available from the

Open Mobile Alliance Ltd. web site at

http://www.openmobilealliance.org/useterms.html

-->
<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="OMADRMREL.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:attribute name="transcribe" type="xsd:boolean"
default="false"/>

                    </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>
```

Figure4: OMA Data Dictionary

Appendix A.   Change History   (Informative)

A.1   Approved Version History

Reference	Date	Description
OMA-TS-DRM-REL-V2_1-20081014-A	14 Oct 2008	Status changed to Approved by TP ref# OMA-TP-2008-0382-INP_DRM_V2_1_ERP_for_Final_Approval
OMA-TS-DRM-REL-V2_1_1-20110531-A	31 May 2011	Status changed to Approved by TP ref# OMA-TP-2011-0181-INP_DRM_V2_1_2_ERP_for_notification

Appendix B.   Static Conformance Requirements (Normative)

B.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	5.6.1	M	
DRM-REL-GEN-C-017	<count> element	5.6.2	M	
DRM-REL-GEN-C-018	<timed-count> element	5.6.3, 5.6.3.1	O	
DRM-REL-GEN-C-019	<datetime> element	5.6.4	O	DRM-REL-GEN-C-020 AND DRM-REL-GEN-C-021
DRM-REL-GEN-C-020	<start> element	5.6.4.1	O	
DRM-REL-GEN-C-021	<end> element	5.6.4.2	O	
DRM-REL-GEN-C-022	<interval> element	5.6.5	O	
DRM-REL-GEN-C-023	<accumulated> element	5.6.6	O	
DRM-REL-GEN-C-024	<individual> element	5.6.7	O	
DRM-REL-GEN-C-025	<system> element	5.6.8	M	
DRM-REL-GEN-C-026	Inheritance model	5.7, 5.7.1	M	
DRM-REL-GEN-C-027	<KeyInfo> element	5.8.1.1	M	
DRM-REL-GEN-C-028	<EncryptedKey> element	5.8.1.2	M	
DRM-REL-GEN-C-029	<EncryptionMethod> element	5.8.1.3, 5.8.1.3.1	M	
DRM-REL-GEN-C-030	<CipherData> element	5.8.1.4	M	
DRM-REL-GEN-C-031	<CipherValue> element	5.8.1.5	M	
DRM-REL-GEN-C-032	<RetrievalMethod> element	5.8.1.6, 5.8.1.6.1	M	
DRM-REL-GEN-C-033	<digest> element	5.8.2.1	M	
DRM-REL-GEN-C-034	<DigestMethod> element	5.8.2.2, 5.8.2.2.1	M	
DRM-REL-GEN-C-035	<DigestValue> element	5.8.2.3	M	
DRM-REL-GEN-C-036	ODRL compatibility	5.9	M	
DRM-REL-GEN-C-037	Syntax Parsing	6	M	
DRM-REL-GEN-C-038	Rights Object evaluation order	5.10	M	
DRM-REL-GEN-C-039	<tracked> element	5.5.2, 5.5.2.1, 5.5.2.2	M	

B.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	5.6.4	M	

Item	Function	Reference	Status	Requirement
DRM-REL-GEN-S-007	\<start\> element	5.6.4.1	M	
DRM-REL-GEN-S-008	\<end\> element	5.6.4.2	M	
DRM-REL-GEN-S-009	\<interval\> element	5.6.5	M	
DRM-REL-GEN-S-010	\<accumulated\> element	5.6.6	M	
DRM-REL-GEN-S-011	\<system\> element	5.6.8	M	
DRM-REL-GEN-S-012	Inheritance model	5.7, 5.7.1	M	
DRM-REL-GEN-S-013	Security model	5.8	M	
DRM-REL-GEN-S-014	\<EncryptedKey\> element	5.8.1.2	M	
DRM-REL-GEN-S-015	Encryption algorithm	5.8.1.3.1	M	
DRM-REL-GEN-S-016	REK referencing	5.8.1.6, 5.8.1.6.1	M	
DRM-REL-GEN-S-017	Hash algorithm	5.8.2.2.1	M	
DRM-REL-GEN-S-018	ODRL compatibility	5.9	M	
DRM-REL-GEN-S-019	Syntax Generation	6	M	
DRM-REL-GEN-S-020	\<tracked\> element	5.5.2, 5.5.2.1, 5.5.2.2	M	

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:id="C.1">
 <o-ex:context>
  <o-dd:version>2.1</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"/>
     <ds:KeyInfo>
      <ds:RetrievalMethod URI="REKReference"/>
     </ds:KeyInfo>
     <xenc:CipherData>
      <xenc:CipherValue>EncryptedCEK</xenc:CipherValue>
     </xenc:CipherData>
    </xenc:EncryptedKey>
   </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 5.6.4 and 5.6.5).

```
<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:id="C.2">
 <o-ex:context>
  <o-dd:version>2.1</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"/>
     <ds:KeyInfo>
      <ds:RetrievalMethod URI="REKReference"/>
     </ds:KeyInfo>
     <xenc:CipherData>
      <xenc:CipherValue>EncryptedCEK</xenc:CipherValue>
     </xenc:CipherData>
    </xenc:EncryptedKey>
   </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.

```xml
<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:id="C.3">
 <o-ex:context>
  <o-dd:version>2.1</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"/>
     <ds:KeyInfo>
      <ds:RetrievalMethod URI="REKReference"/>
     </ds:KeyInfo>
     <xenc:CipherData>
      <xenc:CipherValue>EncryptedCEK</xenc:CipherValue>
     </xenc:CipherData>
    </xenc:EncryptedKey>
   </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"/>
     <ds:KeyInfo>
      <ds:RetrievalMethod URI="REKReference"/>
     </ds:KeyInfo>
     <xenc:CipherData>
      <xenc:CipherValue>EncryptedCEK</xenc:CipherValue>
```

```
      </xenc:CipherData>
     </xenc:EncryptedKey>
    </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:id="C.4p">
 <o-ex:context>
  <o-dd:version>2.1</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:id="C.4c">
 <o-ex:context>
  <o-dd:version>2.1</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"/>
     <ds:KeyInfo>
      <ds:RetrievalMethod URI="REKReference"/>
     </ds:KeyInfo>
     <xenc:CipherData>
      <xenc:CipherValue>EncryptedCEK</xenc:CipherValue>
     </xenc:CipherData>
    </xenc:EncryptedKey>
   </ds:KeyInfo>
  </o-ex:asset>
 </o-ex:agreement>
</o-ex:rights>
```

Child Rights Object referencing the Parent Rights Object

C.5 Subscription Scenario with Metering

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. In this scenario the RI requires Metering Information for loyalty collection purposes and so the RI includes the <tracked> element in the Parent RO. When granting access to content using the ParentRO the DRM agent records Metering Information for the DRM Content and returns this to the RI when it receives a Metering Report ROAP Trigger.

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:id="C.4p">
 <o-ex:context>
  <o-dd:version>2.1</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>2006-08-01T23:59:59Z</o-dd:end>
     </o-dd:datetime>
    </o-ex:constraint>
    <o-ex:requirement>
     <o-dd:tracked oma-dd:timed="10" oma-dd:contentAccessGranted="false"/>
    </o-ex:requirement>
   </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:id="C.4c">
<o-ex:context>
 <o-dd:version>2.1</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"/>
    <ds:KeyInfo>
     <ds:RetrievalMethod URI="REKReference"/>
    </ds:KeyInfo>
    <xenc:CipherData>
     <xenc:CipherValue>EncryptedCEK</xenc:CipherValue>
    </xenc:CipherData>
   </xenc:EncryptedKey>
  </ds:KeyInfo>
 </o-ex:asset>
</o-ex:agreement>
</o-ex:rights>
```

Child Rights Object referencing the Parent Rights Object

C.6   Inheritance Scenario

This scenario shows how the inheritance relation works when the Parent RO and the Child RO both have multiple applicable <permission> elements.

The Parent Rights Object has one 'virtual asset', identified by its <uid> which is equal to "ParentAssetUID". There are two permissions applicable to that <asset> element. The first gives 10 <display> or <play> rights, where the <play> is further constrained to the time interval of January 1st, 2006, 00:00:00 UTC to February 1st, 2006, 00:00:00 UTC. The second permission contains 3 <play> rights and a display right both constrained in the time interval February 1st, 2006, 00:00:00 UTC to March 1st, 2006, 00:00:00 UTC.

```
<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:id="C.5p">
<o-ex:context>
 <o-dd:version>2.1</o-dd:version>
 <o-dd:uid>RightsObjectID</o-dd:uid>
</o-ex:context>
<o-ex:agreement>
 <o-ex:asset id="1">
  <o-ex:context>
   <o-dd:uid>ParentAssetUID</o-dd:uid>
  </o-ex:context>
 </o-ex:asset>
 <o-ex:permission>
  <o-ex:constraint>
    <o-dd:count>10</o-dd:count>
  </o-ex:constraint>
  <o-dd:play>
   <o-ex:constraint>
    <o-dd:datetime>
     <o-dd:start>2006-01-01T00:00:00Z</o-dd:start>
     <o-dd:end>2006-02-01T00:00:00Z</o-dd:end>
    </o-dd:datetime>
   </o-ex:constraint>
  </o-dd:play>
  <o-dd:display>
  </o-dd:display>
 </o-ex:permission>
 <o-ex:permission>
  <o-ex:constraint>
    <o-dd:datetime>
     <o-dd:start>2006-02-01T00:00:00Z</o-dd:start>
     <o-dd:end>2006-03-01T00:00:00Z</o-dd:end>
    </o-dd:datetime>
  </o-ex:constraint>
  <o-dd:play>
   <o-ex:constraint>
    <o-dd:count>3</o-dd:count>
   </o-ex:constraint>
  </o-dd:play>
  <o-dd:display>
  </o-dd:display>
 </o-ex:permission>
</o-ex:agreement>
</o-ex:rights>
```

Parent Rights Object (not referencing DRM Content)

The Child Rights Object has two 'asset's, that are linked to the DRM Content with ContentID "cid:media123@oma.com". The asset with 'id' equal to 1 inherits from a Parent Rights Object's asset, identified by "ParentAssetUID". The asset with 'id' equal to 2, does not inherit from a Parent Rights Object.

The Child Rights Object specifies two separate permissions for its asset with 'id' equal to 1. The first permission allows 'play' between January 15th 2006, 00:00:00 UTC and February 15th 2006, 00:00:00 UTC and 'print' between April 15th 2006, 00:00:00 UTC and May 15th 2006, 00:00:00 UTC, but with the total of 'play's and 'print's constrained to 20. The second permission allows 5 'play's, 8 'print's and 30 'display's in the period between February 15th 2006, 00:00:00 UTC and March 15th 2006, 00:00:00 UTC.

For the asset with 'id' equal to 2, it specifies a 'play' that is constrained to a total accumulated time of 2 hours.

```
<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:id="C.5c">
<o-ex:context>
 <o-dd:version>2.1</o-dd:version>
 <o-dd:uid>RightsObjectID</o-dd:uid>
</o-ex:context>
<o-ex:agreement>
 <o-ex:asset id="1">
  <o-ex:context>
   <o-dd:uid>cid:media123@oma.com</o-dd:uid>
  </o-ex:context>
  <o-ex:inherit>
   <o-ex:context>
    <o-dd:uid>ParentAssetUID</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"/>
    <ds:KeyInfo>
     <ds:RetrievalMethod URI="REKReference"/>
    </ds:KeyInfo>
    <xenc:CipherData>
     <xenc:CipherValue>EncryptedCEK</xenc:CipherValue>
    </xenc:CipherData>
   </xenc:EncryptedKey>
  </ds:KeyInfo>
 </o-ex:asset>
 <o-ex:asset id="2">
  <o-ex:context>
   <o-dd:uid>cid:media123@oma.com</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"/>
    <ds:KeyInfo>
     <ds:RetrievalMethod URI="REKReference"/>
    </ds:KeyInfo>
    <xenc:CipherData>
     <xenc:CipherValue>EncryptedCEK</xenc:CipherValue>
    </xenc:CipherData>
   </xenc:EncryptedKey>
  </ds:KeyInfo>
 </o-ex:asset>
 <o-ex:permission>
  <o-ex:asset idref="1"></o-ex:asset>
  <o-ex:constraint>
    <o-dd:count>20</o-dd:count>
  </o-ex:constraint>
  <o-dd:play>
   <o-ex:constraint>
    <o-dd:datetime>
     <o-dd:start>2006-01-15T00:00:00Z</o-dd:start>
     <o-dd:end>2006-02-15T00:00:00Z</o-dd:end>
    </o-dd:datetime>
   </o-ex:constraint>
  </o-dd:play>
  <o-dd:print>
   <o-ex:constraint>
    <o-dd:start>2006-04-15T00:00:00Z</o-dd:start>
    <o-dd:end>2006-05-15T00:00:00Z</o-dd:end>
   </o-ex:constraint>
  </o-dd:print>
 </o-ex:permission>
 <o-ex:permission>
  <o-ex:asset idref="1"></o-ex:asset>
  <o-ex:constraint>
    <o-dd:datetime>
     <o-dd:start>2006-02-15T00:00:00Z</o-dd:start>
     <o-dd:end>2006-03-15T00:00:00Z</o-dd:end>
    </o-dd:datetime>
  </o-ex:constraint>
  <o-dd:play>
   <o-ex:constraint>
    <o-dd:count>5</o-dd:count>
   </o-ex:constraint>
  </o-dd:play>
  <o-dd:print>
```

```
      <o-ex:constraint>
       <o-dd:count>8</o-dd:count>
      </o-ex:constraint>
     </o-dd:print>
     <o-dd:display>
      <o-ex:constraint>
       <o-dd:count>30</o-dd:count>
      </o-ex:constraint>
     </o-dd:display>
    </o-ex:permission>
    <o-ex:permission>
     <o-ex:asset idref="2"></o-ex:asset>
     <o-dd:play>
      <o-ex:constraint>
       <o-dd:accumulated>P0DT2H0M00S</o-dd:accumulated>
      </o-ex:constraint>
     </o-dd:play>
    </o-ex:permission>
   </o-ex:agreement>
  </o-ex:rights>
```

Child Rights Object referencing the Parent Rights Object

In this constellation, when the DRM Agent is asked for access to the DRM Content identified by its ContentID equal to "cid:media123@oma.com", it will compute the following list of possible permissions and permission combinations:

RO id / asset id	Action	Constraint(s) to be satisfied (and updated if selected)	
C5.c / 1	'play'	`<o-dd:count>20</o-dd:count>`	
		and	

		`<o-dd:datetime>`
		`  <o-dd:start>2006-01-15T00:00:00Z</o-dd:start>`
		`  <o-dd:end>2006-02-15T00:00:00Z</o-dd:end>`
		`</o-dd:datetime>`	

C5.c / 1	'print'	`<o-dd:count>20</o-dd:count>`	
		and	

		`<o-dd:datetime>`
		` <o-dd:start>2006-04-15T00:00:00Z</o-dd:start>`
		` <o-dd:end>2006-05-15T00:00:00Z</o-dd:end>`
		`</o-dd:datetime>`	

C5.c / 1	'play'	`<o-dd:datetime>`
		` <o-dd:start>2006-02-15T00:00:00Z</o-dd:start>`
		` <o-dd:end>2006-03-15T00:00:00Z</o-dd:end>`	

		`</o-dd:datetime>`
	and	
		`<o-dd:count>5</o-dd:count>`

C5.c / 1	'print'	`<o-dd:datetime>`
		`  <o-dd:start>2006-02-15T00:00:00Z</o-dd:start>`
		`  <o-dd:end>2006-03-15T00:00:00Z</o-dd:end>`
		`</o-dd:datetime>`

	and	
		`<o-dd:count>8</o-dd:count>`

C5.c / 1	'display'	`<o-dd:datetime>`
		`  <o-dd:start>2006-02-15T00:00:00Z</o-dd:start>`
		`  <o-dd:end>2006-03-15T00:00:00Z</o-dd:end>`
		`</o-dd:datetime>`

	and	
		`<o-dd:count>30</o-dd:count>`
C5.c / 2	'play'	`<o-dd:accumulated>P0DT2H0M00S</o-dd:accumulated>`
C5.p / 1	'play'	`<o-dd:count>10</o-dd:count>`
	and	

		`<o-dd:datetime>`
		`  <o-dd:start>2006-01-01T00:00:00Z</o-dd:start>`
		`  <o-dd:end>2006-02-01T00:00:00Z</o-dd:end>`
		`</o-dd:datetime>`

C5.p / 1	'display'	`<o-dd:count>10</o-dd:count>`

C5.p / 1	'play'	`<o-dd:datetime>`
		`  <o-dd:start>2006-02-01T00:00:00Z</o-dd:start>`
		`  <o-dd:end>2006-03-01T00:00:00Z</o-dd:end>`
		`</o-dd:datetime>`

	and	
		`<o-dd:count>3</o-dd:count>`

C5.p / 1	'display'	`<o-dd:datetime>`
		`  <o-dd:start>2006-02-01T00:00:00Z</o-dd:start>`
		`  <o-dd:end>2006-03-01T00:00:00Z</o-dd:end>`

		`</o-dd:datetime>`

Following the steps from the algorithm defined in section 5.10, the DRM Agent then evaluates these results to find the proper order in which to consider using these permissions.

1. Only valid rights can be considered.

2. Unconstrained rights first.

3. Rights containing a <datetime> constraint are to be considered first.

4. Rights containing a <datetime> constraint should be used first in order of expiration.

For this discussion, suppose the DRM Time in the Device is January 18th, 2006, 13:00:00 UTC. Then a number of possibilities for <permission> elements cannot be satisfied, because of <datetime> constraints that are not valid at that time. These are filtered during step 1 of the evaluation. This leaves the following list:

RO id / asset id	Action	Constraint(s) to be satisfied (and updated if selected)

C5.c / 1	'play'	`<o-dd:count>20</o-dd:count>`
		
		and
		
		`<o-dd:datetime>`
		`  <o-dd:start>2006-01-15T00:00:00Z</o-dd:start>`
		`  <o-dd:end>2006-02-15T00:00:00Z</o-dd:end>`
		`</o-dd:datetime>`

C5.c / 2	'play'	`<o-dd:accumulated>P0DT2H0M00S</o-dd:accumulated>`

C5.p / 1	'play'	`<o-dd:count>10</o-dd:count>`
		
		and
		
		`<o-dd:datetime>`
		` <o-dd:start>2006-01-01T00:00:00Z</o-dd:start>`
		` <o-dd:end>2006-02-01T00:00:00Z</o-dd:end>`
		`</o-dd:datetime>`

C5.p / 1	'display'	`<o-dd:count>10</o-dd:count>`

Since there are no unconstrained rights, step 2 does not eliminate any <permission> elements. Step 3 filters out any <permission> elements that do not have <datetime> constraints, if any of the <permission> elements on the list has such a constraint. This leaves the following list:

RO id / asset id	Action	Constraint(s) to be satisfied (and updated if selected)
C5.c / 1	'play'	`<o-dd:count>20</o-dd:count>` **and**

RO id / asset id	Action	Constraint(s) to be satisfied (and updated if selected)		

		```<o-dd:datetime>```
		``` <o-dd:start>2006-01-15T00:00:00Z</o-dd:start>```
		``` <o-dd:end>2006-02-15T00:00:00Z</o-dd:end>```
		```</o-dd:datetime>```		

C5.p / 1	'play'	```<o-dd:count>10</o-dd:count>```		
		and		

		```<o-dd:datetime>```
		``` <o-dd:start>2006-01-01T00:00:00Z</o-dd:start>```
		``` <o-dd:end>2006-02-01T00:00:00Z</o-dd:end>```
		```</o-dd:datetime>```		

Step 4 of the evaluation algorithm now favours rights with the earliest expiration date. That leaves the only <permission> element that is valid and applicable:

RO id / asset id	Action	Constraint(s) to be satisfied (and updated if selected)
C5.p / 1	'play'	```<o-dd:count>10</o-dd:count>```
		and

		```<o-dd:datetime>```
		``` <o-dd:start>2006-01-01T00:00:00Z</o-dd:start>```
		``` <o-dd:end>2006-02-01T00:00:00Z</o-dd:end>```
		```</o-dd:datetime>```

When actually consumed, the count state of the top-level constraint of this <permission> element (the first in the Parent Rights Object) is decremented by one.

C.7 Exporting OMA DRM Content

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

C.7.1 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:id="C.5.1">
 <o-ex:context>
  <o-dd:version>2.1</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"/>
     <ds:KeyInfo>
      <ds:RetrievalMethod URI="REKReference"/>
     </ds:KeyInfo>
     <xenc:CipherData>
      <xenc:CipherValue>EncryptedCEK</xenc:CipherValue>
     </xenc:CipherData>
    </xenc:EncryptedKey>
   </ds:KeyInfo>
  </o-ex:asset>
  <o-ex:permission>
   <o-dd:display/>
   <o-dd:print/>
   <oma-dd:export oma-dd:mode="move" oma-dd:transcribe="false">
    <o-ex:constraint>
     <oma-dd:system>
      <o-ex:context>
       <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.7.2   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:id="C.5.2">
 <o-ex:context>
  <o-dd:version>2.1</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"/>
   <ds:KeyInfo>
    <ds:RetrievalMethod URI="REKReference"/>
   </ds:KeyInfo>
   <xenc:CipherData>
    <xenc:CipherValue>EncryptedCEK</xenc:CipherValue>
   </xenc:CipherData>
  </xenc:EncryptedKey>
 </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"/>
   <ds:KeyInfo>
    <ds:RetrievalMethod URI="REKReference"/>
   </ds:KeyInfo>
   <xenc:CipherData>
    <xenc:CipherValue>EncryptedCEK</xenc:CipherValue>
   </xenc:CipherData>
  </xenc:EncryptedKey>
 </ds:KeyInfo>
</o-ex:asset>
<o-ex:permission>
 <oma-dd:export oma-dd:mode="copy" oma-dd:transcribe="false">
  <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: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>
```

C.7.3   Mutual Export

The following is an example RO that can be "mutually" exported among Multi-DRM systems.

The following RO allows export of the DCF identified by "ContentID" along with unconstrained display and print permissions. Export is allowed to either DRM_A or DRM_B. When the RO is exported to DRM_A or DRM_B, the <export> permission will also be transcribed such that the content can be exported from DRM_A or DRM_B.

```
<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:id="C.5.1">
 <o-ex:context>
  <o-dd:version>2.1</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"/>
      <ds:KeyInfo>
       <ds:RetrievalMethod URI="REKReference"/>
      </ds:KeyInfo>
      <xenc:CipherData>
       <xenc:CipherValue>EncryptedCEK</xenc:CipherValue>
      </xenc:CipherData>
     </xenc:EncryptedKey>
    </ds:KeyInfo>
   </o-ex:asset>
   <o-ex:permission>
    <o-dd:display/>
    <o-dd:print/>
    <oma-dd:export oma-dd:mode="move" oma-dd:transcribe="true">
     <o-ex:constraint>
      <oma-dd:system>
        <o-ex:context>
         <o-dd:uid>DRM_A</o-dd:uid>
        </o-ex:context>
        <o-ex:context>
         <o-dd:uid>DRM_B</o-dd:uid>
        </o-ex:context>
        <o-ex:context>
         <o-dd:uid>urn:oma:drms:oma-drm:drm-v2.1</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.8   Example – Combinations of Constraint Elements

The rights depicted in this example shows combinations of constraints to play 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>2.1</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>
     <ds:KeyInfo>
      <ds:RetrievalMethod URI="REKReference"/>
     </ds:KeyInfo>
     <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#kw-aes128"/>
     <xenc:CipherData>
      <xenc:CipherValue>EncryptedCEK</xenc:CipherValue>
     </xenc:CipherData>
    </xenc:EncryptedKey>
   </ds:KeyInfo>
  </o-ex:asset>
  <o-ex:permission>
   <o-ex:constraint>
    <oma-dd:timed-count oma-dd:timer=30>10</oma-dd:timed-count>
    <o-dd:datetime>
      <o-dd:start>2004-01-01T00:00:00Z</o-dd:start>
      <o-dd:end>2004-04-30T23:59:59Z</o-dd:end>
    </o-dd:datetime>
   </o-ex:constraint>
   <o-dd:play>
    <o-ex:constraint>
      <oma-dd:timed-count oma-dd:timer=1800>2</oma-dd:timed-count>
      <o-dd:datetime>
       <o-dd:start>2004-03-01T00:00:00Z</o-dd:start>
       <o-dd:end>2004-06-01T23:59:59Z</o-dd:end>
      </o-dd:datetime>
    </o-ex:constraint>
   </o-dd:play>
  </o-ex:permission>
 </o-ex:agreement>
</o-ex:rights>
```

The example contains two constraint elements, both of which have to be satisfied in order for the DRM Agent to grant the given permission to the user. This paragraph briefly explains what the spec means by "*the stricter of two constraints of the same type prevails for a given permission element*".

In the example there are four constraints that have to be applied to the <permission>: two <timed-count> constraints and two <datetime> constraints. All constraints need to be satisfied. This means that access to the content can only be granted during the time when both <datetime> constraints are satisfied, as well as the specific semantics of both timed-count constraints.

Here the first <datetime> constraint specifies a period between January 1st, 2004, 00:00:00 UTC and April 30th, 2004, 23:55:59 UTC. The second <datetime> constraint specifies a period between March 1st, 2004, 00:00:00 UTC and June 1st, 2004, 23:59:59 UTC. The period of overlap is between March 1st, 2004, 00:00:00 UTC and April 30th, 2004, 23:59:59 UTC.

During this overlapping period, if 'play' access to the content is requested, it is granted, and two timers start simultaneously. The first timer is set to expire in 30 seconds, while the second timer is set to expire in 1800 seconds. When any of these timers expires, and the 'play' access to the content is still in effect, then the counter of the <timed-count> element of which the timer has expired is decreased, and the 'play' access remains in effect.

The resulting access can be described as:

- no access before March 1st, 2004, 00:00:00 UTC

- no access after April 30th, 2004, 23:59:59 UTC

- during the period of overlap, March 1st, 2004, 00:00:00 UTC to April 30th, 2004, 23:59:59 UTC

    o 'play' access for a period greater than 1800 seconds is granted at most 2 times.

    o 'play' access for a period greater than 30 seconds is granted at most 10 times,

    o 'play' access for a period of less than 30 seconds is granted without limit,

C.9   Example – Restricting the usage to a Media Player

The rights depicted in this example shows how to restrict the usage of content to the Audio Media Player only (thus prevents the associated content to be installed as a ring-tone).

```
<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>2.1</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>
     <ds:KeyInfo>
      <ds:RetrievalMethod URI="REKReference"/>
     </ds:KeyInfo>
```

```
        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#kw-aes128"/>
        <xenc:CipherData>
         <xenc:CipherValue>EncryptedCEK</xenc:CipherValue>
        </xenc:CipherData>
      </xenc:EncryptedKey>
     </ds:KeyInfo>
   </o-ex:asset>
  <o-ex:permission>
   <o-dd:play>
     <o-ex:constraint>
      <o-dd:system>
          <o-ex:context>
              <o-dd:uid>urn:oma:drms:oma-appl:media-player-consumption-v1.0</o-dd:uid>
          </o-ex:context>
      </oma-dd:system>
     </o-ex:constraint>
   </o-dd:play>
  </o-ex:permission>
</o-ex:agreement>
</o-ex:rights>
```