DRM Rights Expression Language – SCE Extensions

Candidate Version – 09 Dec 2008

Open Mobile Alliance

OMA-TS-SCE_REL-V1_0-20081209-C

Contents

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 Secure Content Exchange (SCE) is to enhance the OMA Digital Rights Management v2.1 (OMA DRM v2.1) specifications to enable the secure exchange of DRM Content among multiple devices. These enhancements include the following:

- New capabilities that enable flexible sharing of purchased content in ways that were not possible using Domains as defined in OMA DRM v2.1. These new features include Copy and Move of Rights between Devices, Lending and sharing in an ad hoc manner.
- Extension of the OMA DRM v2.1 Domain concept to the User Domain concept, which allows different Rights Issuers to generate Rights Objects for the same User Domain.
- The definition of the Import function allows content protected by non-OMA DRM mechanisms to be consumed by SCE Devices. Together with the Export function from OMA DRM v2.1, the Import function allows OMA SCE Devices to securely exchange content with non-OMA DRM devices.
- Enhancements to the OMA DRM specifications to enable consumption of DRM Content contained in an MPEG-2 Transport Stream across a wide variety of user Devices.

This document extends the OMA DRM v2.1 Rights Expression Language (REL) [DRM-REL-v2.1] for SCE specific purposes. New permissions, such as <move> and <adhoc-share>, and new constraints, such as <userDomain> and <proximity> are specified in this document. Normative text from the OMA DRM v2.1 REL document SHALL apply to SCE.

2. References

2.1 Normative References

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

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

[DRM-DCF-v2.1] "DRM Content Format v2.1", Open Mobile Alliance™, OMA-TS-DRM_DCF-V2_1-20070724-C, URL: http://www.openmobilealliance.org/

[DRM-REL-v2.1] "DRM Rights Expression Language v2.1", Open Mobile Alliance™, OMA-TS-DRM_REL-V2_1-20070919-C, URL: http://www.openmobilealliance.org/

[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

[SCE-A2A] "Secure Content Exchange Agent To Agent Transfer", Open Mobile Alliance™, OMA-TS-SCE-A2A-V1_0-20081209-C, URL: http://www.openmobilealliance.org/

[SCE-DRM] "Secure Content Exchange Digital Rights Management", Open Mobile Alliance™,OMA-TS-SCE-DRM-V1_0-20081209-C, URL: http://www.openmobilealliance.org/

[SCE-DOM] "Secure Content Exchange User Domains", Open Mobile Alliance™, OMA-TS-SCE-DOM-V1_0-20081209-C, URL:http://www.openmobilealliance.org/

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

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

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

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

2.2 Informative References

[DRM-v2.1] "Digital Rights Management", Open Mobile Alliance™, OMA-DRM-DRM-V2_1, URL:http://www.openmobilealliance.org/

[DRM-AD-v2.1] "OMA DRM Architecture Overview", Open Mobile Alliance™, OMA-DRM-AD-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

Ad Hoc Domain	A group of Devices that engage in Ad Hoc Sharing that is governed by a Domain Policy.
Ad Hoc Sharing	Sharing that is intended to allow a source Device to share specified Rights with a recipient Device in spontaneous, unplanned situations (e.g. sharing a song with a new group of friends at a party or playing a video on a hotel room TV while travelling).
Composite Object	A Media Object that contains one ore more Media Objects by means of inclusion e.g. DRM messages, zip files.
Constraint	A restriction on the Permission over DRM Content.
Content	One or more Media Objects.
Device	A Device is the entity (hardware/software or combination thereof) within a user equipment that implements a DRM Agent. The Device is also conformant to the OMA DRM specifications. The Device may include a smart card module (e.g. a SIM) (DRM V2.0).
Device Rights Object	A Rights Object that is initially targeted to a specific entity. Subsequently, the Rights Object may be allowed to be targeted to other entities to be consumed, serially or in parallel, independently of membership in a Domain or User Domain.
Domain	A set of v2.x and/or SCE DRM Agents that can consume Domain Rights Objects.
Domain Authority	The entity to specify the Domain Policy for a User Domain or an Ad Hoc Domain.
Domain Enforcement Agent	The entity to enforce the Domain Policy on behalf of the Domain Authority. It may reside in the network as a service or in a User’s device.
Domain Policy	A collection of attributes which defines the policy determining characteristics of the membership of a User Domain or Ad Hoc Domain, as set by the Domain Authority that the Domain Enforcement Agent will enforce.
Domain Rights Object	A Rights Object that is targeted to a specific v2.x Domain. The Rights Object can be consumed independently by each v2.x or SCE DRM Agent that is a member of the Domain.
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.
Lending	Sharing such that the Shared Rights cannot be used on the source Device as long as the recipient Device is able to render the shared Content associated with the Shared Rights
Media Object	A digital work e.g. a ringing tone, a screen saver, a Java game or a Composite Object.
Permission	Actual usage or activities allowed (by the Rights Issuer) over DRM Content.
Rights	The collection of permissions and constraints defining under which circumstances access is granted to DRM Content.
Rights Issuer	An entity that issues Rights Objects to OMA DRM Conformant Devices.
Rights Object	A collection of Permissions, Constraints, and other attributes which define under what circumstances access is granted to, and what usages are defined for, DRM Content. All OMA DRM Conformant Devices must adhere to the Rights Object associated with DRM Content.

Shared Rights	Rights that can be consumed on multiple Devices, where the allowed distribution and consumption of the Rights among the Devices are specified by permissions in the Rights themselves or in the Domain Policy of the Domain for which the Rights were obtained.
Sharing	The act of providing Shared Rights from a source Device to a recipient Device, such that the recipient Device is able to render the shared content associated with the Shared Rights.
User	The human user of a Device. The User does not necessarily own the Device (DRM V2.0).
User Domain	A set of v2.x and/or SCE DRM Agents that can consume User Domain Rights Objects.
User Domain Rights Object	A Rights Object that is targeted to a specific User Domain. Besides requiring membership in the User Domain, consumption may require being targeted to an SCE DRM Agent.

3.3 Abbreviations

AES	Advanced Encryption Standard
CEK	Content Encryption Key
DCF	DRM Content Format
DEA	Domain Enforcement Agent
DER	Distinguished Encoding Rules
DRM	Digital Rights Management
DTD	Document Type Definition
IMSI	International Mobile Subscriber Identity
LRM	Local Rights Manager
MIME	Multipurpose Internet Mail Extensions
OMA	Open Mobile Alliance
OMNA	Open Mobile Naming Authority
ODRL	Open Digital Rights Language
REL	Rights Expression Language
REK	Rights Object Encryption Key
RI	Rights Issuer
RO	Rights Object
ROAP	Rights Object Acquisition Protocol
SCE	Secure Content Exchange
SHA-1	Secure Hash Algorithm
SIM	Subscriber Identity Module
SMS	Short Message Service
UID	Unique Identifier
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
WAP	Wireless Application Protocol
WIM	Wireless Identity Module
XML	Extensible Markup Language

4. Introduction

Secure Content Exchange extends the mechanisms described in Digital Rights Management 2.1 to increase the flexibility of DRM Content usage. Some of these extensions allow the import of non-OMA DRM Content, the exchange of DRM Content among Devices and the implementation of a central domain management function. Rights are used to specify the access a consuming Device is granted to DRM Content. The Rights Expression Language (REL) defined in this document specifies the syntax and semantics of rights governing the usage of DRM Content based on the Open Digital Rights Language [ODRL]. The REL defined in this document extends the semantics as defined in [DRM-REL-v2.1] with some new elements, e.g. permissions and constraints that are needed for implementing OMA SCE use cases.

4.1 Goals

The goal of this specification is to extend the REL semantics defined in OMA DRM REL [DRM-REL-v2.1]. Only additions and modifications to the OMA DRM REL are described in this document.

5. Structure

5.1 Foundation Model

5.1.1 Element <rights>

```
<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>

<element name="moveIndication">
        <complexType>
                <element name="originalIssuer" type="roap:Identifier"/>
                <sequence maxOccurs="unbounded">
                        <element name="riID" type="roap:Identifier"/>
                        <element name="riURL" type="anyURI"/>
                </sequence>
        </complexType>
</element>
```

In the case of an RO with a <userDomain> constraint, the <moveIndication> element includes a list of RI IDs and RI URLs for RIs that the RI or LRM that originally issued the RO allows to provide Move via RI service for the RO. If an RO with a <userDomain> constraint has a <copy> permission, the RO MUST NOT have a <moveIndication> element since an RO that has a <copy> permission SHALL NOT be Moved via an RI.

In the case of a Device RO, the <moveIndication> element includes a list of RI IDs and RI URLs for RIs that the LRM that originally issued the RO allows to provide Move via RI service for the RO. The <moveIndication> element SHALL NOT be used in Device ROs that are originally issued by an RI.

The <originalIssuer> element in the <moveIndication> element contains the ID of the original Issuer of that RO. The ID MUST correspond to a Rights Issuer or LRM if the RO has a <userDomain> constraint. The ID MUST correspond to an LRM if the RO is a Device RO.

An RO with a <userDomain> constraint MAY be Moved via the original Issuer if the original Issuer is an RI and if the original Issuer's ID and URL are included in the list of RI IDs and RI URLs in the <moveIndication> element.

5.2 Agreement Model

The agreement model expresses the Rights that are granted over 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>

```
 <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="1" maxOccurs="unbounded"/>
                <xsd:element ref="o-ex:party" minOccurs="0" maxOccurs="unbounded"/>
        </xsd:sequence>
 </xsd:complexType>
```

The <agreement> element specifies the rights granted over the corresponding DRM Content. It contains zero or more <party> elements, one or more <asset> elements and zero or more <permission> elements.

5.2.2 Element <party>

```
<xsd:element name="party" type="o-ex:partyType"/>

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

A <party> element MAY be included in the <agreement> element to specify to which Device, Domain or User Domain the RO is bound. In this case, the <party> element in the <agreement> element contains a <context> element with a <uid> element that matches a Device ID, Domain ID or User Domain ID, respectively specifying to which Device Domain or User Domain the RO is bound. An SCE Device MUST reject an RO without an <individual> constraint element and without a <party> element which identifies that Device or identifies a non- device-specific collection of Devices (such as a Domain or User Domain), if the RO was received in other ways than through a successful execution of the RO Acquisition Protocol or as a recipient DRM Agent in an OMA DRM-specified transaction, operation or protocol.

When generating User Domain ROs, the RI/LRM MUST include a <party> element to show that the RI or LRM is associated with a particular User Domain and authorized to create (or import) ROs for this User Domain. In this case, the <party> element in the <agreement> element contains a <context> element with a <userDomainAuthorization> element specifying that the RI or LRM was authorized by the DEA to be associated to a specific User Domain and generate ROs for that User Domain (refer to [SCE-DOM] for more details).

When generating Device RO, the RI/LRM MUST include a <party> element that includes <issuerURL> element under the <context> element, if a <contextRequired> constraint is present or a <move> permission that allows “Move via RI” protocol is present. This <issuerURL> element is used for DRM Agent to contact RI/LRM if necessary.

In future versions of SCE, there may be multiple <uid> elements in the <context> element in the <party> element. Therefore, the DRM Agent SHALL be able to process multiple <uid> elements in the <context> element, and SHALL ignore any <uid> elements with values that are not specified in this version of SCE.Note: including the party element may lead to incompatibility with certain OMA DRM 2.0 and OMA DRM 2.1 implementations.

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 <party> element, in the <asset> element, in the <individual> element, in the <system> element, and in the <inherit> element. As the model name already indicates, the semantics of its child elements depend on the context in which it occurs within the Rights Object (RO).

5.3.1 Element <context>

```
<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"/>
        </sequence>
        <xsd:attributeGroup ref="o-ex:IDGroup"/>
</xsd:complexType>
```

The <context> element contains the optional <version>, <uid>, <date>, <userDomainAuthorization> and <issuerURL> 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>, <party>, <asset>, <individual>, <system>, or <inherit> element. Please see the corresponding descriptions of the individual child elements. The descriptions of the <asset>, <individual> and <inherit> elements can be found in [DRM-REL-v2.1], whereas the description of the other elements are in this document.

A <context> element MUST NOT contain more than one <uid> element unless the <context> element is contained in the <individual> element or the <party> element.

The <cekHash> element contains the hash over all the hashed CEKs in this RO. It is used for key confirmation. See section 5.3.5 for more details.

5.3.2 Element <version>

This element is not changed from the [DRM-REL-v2.1].

5.3.3 Element <uid>

<xsd:element name="uid" type="o-dd:uriAndOrString" substitutionGroup="o-ex:contextElement"/>If its parent <context> element is included in the <rights> element, the <uid> element constitutes the RO identifier.

If its parent <context> element is included in the <asset> element, the <uid> element specifies a DCF ContentID (see [DRM-DCF-v2.1]), a DCF GroupID (see [DRM-DCF-v2.1]), or a "virtual" UID for a Parent RO (see [DRM-REL-v2.1], 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 that the scheme name MUST be "gid:". If the <uid> element identifies a Parent RO the value MUST use the URL format of [RFC2392] except that 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 the content is bound. If the 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 the 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 RO(s) are allowed to be exported or/ 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> or <party> 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 RO from where to inherit Permissions and Constraints (see [DRM-REL-v2.1], section 5.7).

If its parent <context> element is included in the <party> element, the <uid> element specifies the Device or the Domain to which the RO is bound:.

- If the RO is a Device RO, the RI/LRM MAY include a <uid> element, in which the value is of the form "device:*x*" (without the quotes) where *x* is replaced by the base64 encoded SHA-1 hash over the concatenation of the ROID and the Device ID (i.e. the SHA-1 hash of the DER-encoded subjectPublicKeyInfo value in its certificate) of the Device to which the RO is initially bound.

- If the RO is a Domain RO the RI MAY include a <uid> element, in which the value is of the form "dom:*x*:*y*" (without the quotes), where *x* is replaced by the RI ID and where *y* is replaced by the base64 encoded SHA-1 hash over the concatenation of the RO ID and the Domain ID of the Domain to which the RO is bound.

5.3.4 Element <date>

```
<xsd:element name="date" type="o-dd:dateType" substitutionGroup="o-ex:contextElement"/>
<xsd:complexType name="dateType">
        <xsd:choice>
                <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:element name="fixed" type="o-dd:dateAndOrTime" minOccurs="0"/>
        </xsd:choice>
 </xsd:complexType>
```

If its parent <context> element is included in the <party> element, the <date> element MAY be included. The <date> element specifies the Rights Issuer's TimeStamp (RITS). The RITS is stored in the <fixed> element. Its form MUST conform to a single lexical representation defined in section 3.2.7 of [XMLSchema] and section 5.6.4.1 of [DRM-REL-v2.1].

The elements <start> and <end> SHALL NOT be included in the <date> element.

The RITS in the <fixed> element in the <date> element MUST be equal to the value in the <timeStamp> element in the <ro> element. This ensures that the RITS is protected by the RI signature, which increases security.

5.3.5 Element <cekHash>

```
<xsd:element name="cekHash" type="xsd:base64Binary" substitutionGroup="o-ex:contextElement"/>
```

The <cekHash> element contains the hash over the hashes of the individual CEKs in the separate Assets. This field MUST be included if the RO contains an <adhoc-share> or <lend> permission.

It is calculated as follows:

- Suppose this RO contains *n* ciphertext CEKs, of form AES-WRAP(REK, CEK). Number the associated plaintext CEKs in order of appearance of their ciphertext. Denote the first plaintext CEK by CEK_1, the second by CEK_2, ..., the n^{th} by CEK_n.
- Calculate for each CEK_i the hash $HCEK_i$ as follows:

$$HCEKi = SHA1(CEKi)$$

- The value CEKhash is calculated by taking the SHA-1 hash over the concatenation of all HCEK*i*:

$$CEKhash = SHA1(HCEK_1 \mid HCEK_2 \mid ... \mid HCEK_n)$$

CEKhash is stored in base64 encoded form in the <cekHash> element.

5.3.6 Element <issuerURL>

```
<xsd:element name="issuerURL" type="xsd:anyURI" substitutionGroup="o-ex:contextElement"/>
```

The <issuerURL> element contains the contact address of RI/LRM that generated this <rights> element and it is expressed as URL.

5.4 Permission Model

5.4.1 Element <permission>

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.

```
 <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>
```

In addition to the semantics as defined in [DRM-REL-v2.1], SCE adds the following optional elements to the <permission> element:

- <move> - allows Moving an RO
- <copy> - allows Copying an RO
- <adhoc-share> - allows Ad Hoc Sharing an RO
- <lend> - allows the Lending of an RO

When <move> or <copy> is present, the parent <permission> element MUST NOT have any <asset> elements.

5.4.2 Element <move>

```
<xsd:element name="move" type="o-ex:permissionType" substitutionGroup="o-ex:permissionElement">
```

The <move> element grants the permission to Move an RO between Devices. It contains an optional <constraint> element and an "allowPartial" attribute.

The <move> element can have an optional <constraint> child element. Not all constraints specified in [DRM-REL-v2.1] are allowed to be present in the <constraint> element. Only the following constraints are allowed: <count>, <system>, <datetime>, <interval>, <userDomain> or <proximity>. The <datetime> and <interval> constraints have the same function as defined in [DRM-REL-v2.1]. The <count> and <system> constraints have the same function as defined in [DRM-REL-v2.1] including some SCE additions described in sections 5.5.2 and 5.5.5. For a description of <userDomain> and <proximity>, please refer to section 5.5.3 and 5.5.4.

If the Move of the RO is limited to a User Domain, a top-level <userDomain> constraint MUST be included.

If the <constraint> element is specified, the DRM Agent MUST grant move 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 move 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 move rights.

If the "allowPartial" attribute is "false" (the default value), the Move of the Partial Rights MUST NOT be performed.

5.4.3 Element <copy>

```
<xsd:element name="copy" type="o-ex:permissionType" substitutionGroup="o-ex:permissionElement"/>
```

The <copy> element grants the permission to Copy an RO between Devices of the same User Domain. It contains an optional <constraint> element.

An RO including a <copy> element MUST have a top-level <userDomain> constraint.

Additionally the <copy> element MAY have an optional <constraint> child element. Not all constraints specified in [DRM-REL-v2.1] are allowed to be present in the <constraint> element. Only the following constraints are allowed: <count>, <system>, <datetime>, <interval>, <userDomain> or <proximity>. The <datetime> and <interval> constraints have the same function as defined in [DRM-REL-v2.1]. The <count> and <system> constraints have the same function as defined in [DRM-REL-v2.1] including some SCE additions described in sections 5.5.2 and 5.5.5. For a description of the new <userDomain> and <proximity> constraints, please refer to section 5.5.3 and 5.5.4.

The DRM Agent MUST grant copy rights according to the child <constraint> element and the top-level <constraint> element.

5.4.4 Element <adhoc-share>

```
<xsd:element name="adhoc-share" type="o-ex:permissionType" substitutionGroup="o-ex:permissionElement"/>
```

The <adhoc-share> element grants the permission to Ad Hoc Share an RO and its corresponding DRM-protected content with other DRM Agents.

The <adhoc-share> element SHOULD contain a <constraint> child element that controls the Ad Hoc Sharing of the Rights Object. All constraints specified in [DRM-REL-v2.1] and in section 5.5.1 can be present under the <constraint> element. The <constraint> element SHOULD contain at least one of the <proximity>, <max-concurrent> or <banning-interval> constraint.

The <adhoc-share> element MUST have at least a <permission> child element that define the set of permissions which are granted to the recipient-side DRM Agent. This <permission> element SHOULD have a <constraint> child element that limits for how long the recipient-side DRM Agent is allowed to use the shared rights.

5.4.5 Element <lend>

```
<xsd:element name="lend" type="o-ex:permissionType" substitutionGroup="o-ex:permissionElement"/>
```

The <lend> element grants the permission to Lend an ROand its corresponding DRM-protected content with other DRM Agents. When an RO is Lent, the source DRM Agent is not allowed to consume the Rights Object while the recipient DRM Agent has the Rights Object.

When an RO is Lent, the recipient DRM Agent respects the permissions and constraints as defined by the permission model in the RO. The RI MUST NOT insert a <lend> permission that has stateful constraints for consumption by the DRM Agent.

The <lend> element MUST NOT contain any additional child permissions.

The <lend> element contains a <constraint> element that controls the Lending of the Rights Object, for example limiting the number of times a lending is allowed. Note that if a stateful constraint like <count> is included as a child of the <lend> permission, it applies only to the DRM Requester. At least, the <lending-interval> constraint element MUST be present under the <constraint> element. The lending interval begins as soon as the transfer takes place.

On the source-side DRM Agent (the DRM Requester, see [SCE-A2A]), the <lending-interval> indicates when the Rights Object can be used again by the DRM Agent (acting as a DRM Requester, see [SCE-A2A]). On the recipient DRM Agent, the <lending-interval> indicates when the Rights Object is no longer useable by the DRM Agent. The recipient DRM Agent MAY release the Rights Object back to the source DRM Agent before the <lending-interval> period is over (see the Lend Release operation in [SCE-A2A]).

The processing of a <lend> element in combination with a <metering> constraint is out-of-scope of this enabler.

5.5 Constraint Model

The constraint model enhances the permission model by providing fine-grained consumption control of content. In addition to the semantics as defined in [DRM-REL-v2.1], SCE adds the optional <userDomain>, <proximity>, <banning-interval>, <max-concurrent>, <lending-interval> and <contextRequired> elements to the <constraint> element.

5.5.1 Element <constraint>

```
<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>
```

The <constraint> element is the top most element in the constraint model. It contains the optional <count>, <timed-count>, <datetime>, <interval>, <accumulated>, <individual>, <system>, <userDomain>, <proximity>, <banning-interval>, <max-concurrent>, <lending-interval> and <contextRequired> elements.

5.5.2 Element <count>

```
<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>
```

In addition to the semantics as defined in [DRM-REL-v2.1], the following applies:

If the parent <constraint> element is a child element of a <move> element, the <count> element specifies the number of times the <move> permission may be granted over the Rights Object itself. When used to constrain the <move> permission, the count MUST be decremented upon commencement of a Move process.

If the parent <constraint> element is a child element of a <copy> element, the <count> element specifies the number of times the <copy> permission may be granted.

5.5.3 Element <userDomain>

```
<xsd:element name="userDomain" type="o-ex:constraintType" substitutionGroup="o-ex:constraintElement"/>
```

If a User Domain RO is <userDomain> constrained, it MUST be used only by Devices that have been targeted by an RI/LRM or Devices that are recipients of an A2A operation or transaction.

The <userDomain> constraint SHALL be in a top-level <constraint> element.

ROs with a <userDomain> constraint SHALL include a <userDomainAuthorization> element in the <context> element in the <party> element to proof that the RI or LRM was authorized by the DEA to generate ROs for that User Domain and to specify to which User Domain the RO is bound.

If a permission is restricted with a <userDomain> constraint, the Device SHALL only grant the permission if it is a member of the User Domain indicated by the <userDomainID> element in the corresponding <userDomainInfo> element in the <udaBody> in the <userDomainAuthorization>. However, the recipient Device of a Move or Copy operation does not need to be in the User Domain when it receives the RO over the A2A operation.

To Move an RO containing a <userDomain> constraint, the RO MUST contain a <move> permission. An RO with a <userDomain> constraint MUST only be Moved by using either the A2A Move RO or Move via RI protocol.

To Copy an RO containing a <userDomain> constraint, the RO MUST contain a <copy> permission and MUST only be Copied by using the A2A Copy RO protocol.

If an RO that was received as part of an Ad-Hoc Sharing or Lending operation contains a <userDomain> constraint, the recipient Device can consume the RO independently of its membership in the User Domain.The <userDomain> constraint also assures that the related permission is only granted to SCE Devices. Since the <userDomain> constraint is not understood by OMA DRM 2.0 or OMA DRM 2.1 Devices, including the <userDomain> constraint disallows the permission to be exercised by OMA DRM 2.0 or OMA DRM 2.1 Devices.

5.5.4 Element <proximity>

```
<xsd:element name="proximity" substitutionGroup="o-ex:constraintElement">
        <xsd:complexType>
                <xsd:complexContent>
                        <xsd:extension base="o-ex:constraintType">
                                <xsd:attribute name="method" type="xsd:anyURI"  use="required"/>
                        </xsd:extension>
                </xsd:complexContent>
        </xsd:complexType>
</xsd:element>
```

The <proximity> element restricts the user of the related permission based on the determination of proximity. The use of proximity is not limited to nearness in space, but also includes nearness in time or relation of the Users of the Devices. The <proximity> element MUST have a method attribute that describes, which proximity method is used for this constraint...

If the Device is not able to process the proximity method as required by the semantics of this element, or does not understand a sub-element of the <proximity> element, then the Device MUST treat the constraint as not met and MUST NOT grant the corresponding permission. The RI/LRM MAY use the DeviceDetails extension in the RegistrationRequest message to find out the Device manufacturer, model and version, from which it can determine which proximity method can be used before issuing the RO.

The method attribute contains a string value that specifies the URN associated with the required proximity method to be evaluated, e.g., method="urn:oma:proximity:pm042_iph:3.14". The <proximity> element MAY contain any number of child elements carrying specific parameters depending on the proximity method.

The child elements SHOULD be given in the name space that is named after the name of the proximity method. For example, if the OMNA registered name of the Proximity Method is urn:oma:{OMAresource}:{ResourceSpecificString}, then the name space for child elements within the <proximity> element should be {ResourceSpecificString}.

5.5.5 Element <system>

```
<xsd:element name="system" type="o-ex:constraintType" substitutionGroup="o-ex:constraintElement"/>
```

In addition to the semantics as defined in [DRM-REL-v2.1], the following applies:

The <system> constraint is allowed to also constrain the <move>, <copy>, <adhoc-share> and <lend> permissions.

In the case of a <move>, <copy>, <adhoc-share> or <lend> permission, the <system> constraint specifies the protocol(s) that MUST be used to respectively Move, Copy, Ad Hoc Share or Lend the ROs. In this case, the <context> elements SHALL contain a <version> element and a <uid> element. The <version> element specifies the minimum version of a protocol that MUST be used, whereas the <uid> element contains the URN to identify the protocol as registered with the OMNA.

5.5.6 Element <banning-interval>

```
<xsd:element name="banning-interval" type="xsd:duration" substitutionGroup="o-ex:constraintElement"/>
```

The <banning-interval> element is only used for <adhoc-share> permission. The <banning-interval> element specifies a minimum value for the period of time that the source DRM Agent MUST NOT conduct Ad Hoc Share with the recipient DRM Agent after conducting Ad Hoc Share with the same recipient DRM Agent.

The format used to specify the value of the <banning-interval> element is of type duration, which has the same format as the <interval> element from [DRM-REL-V2.1] (e.g. the value can be "P1D").

5.5.7 Element <max-concurrent>

```
<xsd:element name="max-concurrent" type="xsd:positiveInteger" substitutionGroup="o-ex:constraintElement"/>
```

The <max-concurrent> element is only used for <adhoc-share> permission. The <max-concurrent> element specifies a maximum number of recipient DRM Agents that can simultaneously do ad hoc share with the source DRM Agent. The value of the <max-concurrent> element MUST be a positive integer.

5.5.8 Element <lending-interval>

```
<xsd:element name="lending-interval" type="xsd:duration" substitutionGroup="o-ex:constraintElement"/>
```

The <lending-interval> element is used for the <lend> permission. The <lending-interval> element specifies the maximum amount of time that an RO can be Lent. The format used to specify the value of the <lending-interval> element is of type duration, which has the same format as the <interval> element from [DRM-REL-V2.1] (e.g. the value can be "P1D").

5.5.9 Element <contextRequired>

```
<xsd:element name="contextRequired" type="o-ex:constraintType" substitutionGroup="o-ex:constraintElement"/>
```

The <contextRequired> constraint is used to restrict consumption of a Device RO received via an A2A Move transaction to Devices that have a current RI/LRM Context corresponding to the source RI/LRM [SCE-DRM]. The <contextRequired> constraint SHALL be in a top-level <constraint> element.

If an RO that was received as part of an Ad-Hoc Sharing or Lending operation contains a <contextRequired> constraint, the recipient Device is not required to have registered with the source RI/LRM in order to consume.

If the <contextRequired> element is included, the <context> element in the <party> element MUST include an <issuerURL> element, indicating the URL to which the Device can register.

5.6 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 [ODRL]

The DRM Agent of a Device encountering any elements (e.g. from [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.
- ROs containing unsupported <requirement> elements MUST NOT be granted.
- ROs containing <condition> elements MUST NOT be granted.
- All other unsupported elements SHALL be ignored.

Appendix A. Change History (Informative)

A.1 Approved Version History

A.2 Draft/Candidate Version 1.0 History

Reference	Date	Sections	Description
Draft Versions OMA-TS-SCE_REL-V1_0-20070924-D	24 Sep 2007		Initial Draft
OMA-TS-SCE_REL-V1_0-20071218-D	18 Dec 2007	5.1, 5.2	Incorporated: OMA-DRM-2007-0536R01-CR_SCE_REL_Move_Permission_and_Constraint
OMA-TS-SCE_REL-V1_0-20080110-D	10 Jan 2008	5.2.3, C.1, C.2	Incorporated: OMA-DRM-2007-0491R01-CR_SCE_Proximity
OMA-TS-SCE_REL-V1_0-20080311-D	11 Mar 2008	5.1, 5.2, 5.3, 5.4, 5.5	Incorporated: OMA-DRM-2008-0027R03-CR_REL_Ad_Hoc_Share_permission OMA-DRM-2008-0068-CR_SCE_REL_Place_for_LRMID OMA-DRM-2008-0070R03-CR_SCE_REL_Elements_for_Pairing
OMA-TS-SCE_REL-V1_0-20080313-D	13 Mar 2008	5.2.4.1	Fixed error in merge of OMA-DRM-2008-0027R03.
OMA-TS-SCE_REL-V1_0-20080320-D	20 Mar 2008	4, 5.2, 5.3	Incorporated: OMA-DRM-2008-0090R01-CR_Partial_Rights_Move_Permission OMA-DRM-2008-0107R01-CR_SCE_REL_Copy_Move_Permission
OMA-TS-SCE_REL-V1_0-20080429-D	29 Apr 2008	Many	Incorporated resolutions to comments REL-003 (partly), REL-006, REL-007, REL-015, REL-016, REL-017, REL-018, REL-021, REL-023, REL-037, REL-046, REL-047, as per OMA-CONRR-SCE_REL-V1_0-20080429-D.
OMA-TS-SCE_REL-V1_0-20080430-D	30 Apr 2008	5.2, 5.3, 5.6.3, 5.6.4	Incorporated: OMA-DRM-2008-0181-CR_SCE_device_binding_in_REL
OMA-TS-SCE_REL-V1_0-20080515-D	15 May 2008	3.2, 3.3	Incorporated:OMA-DRM-2008-0173-CR_SCE_REL_Add_abbreviations OMA-DRM-2008-0174R01-CR_SCE_REL_Add_definitions
OMA-TS-SCE_REL-V1_0-20080528-D	28 May 2008	1, 2.1, 5.2, 5.8	Incorporated: OMA-DRM-2008-0176R01-CR_SCE_Add_text_for_sections_1_and_5.6 OMA-DRM-2008-0184-CR_Proposal_for_Resolving_CONR_Comment_REL026 Changed to the common reference scheme of OMA-DRM-2008-0179R01-INP_SCE_Common_Reference_Scheme.
OMA-TS-SCE_REL-V1_0-20080606-D	06 Jun 2008	2.1, 5.4.6, 5.5, 5.5.1.2, 5.5.6.2, new section 5.5.8, 5.6.3.2	Incorporated: OMA-DRM-2008-0241-CR_Fix_reference_in_REL OMA-DRM-2008-0243R02-CR_SCE_REL_Name_Change_For_Lending_Interval OMA-DRM-2008-0245R02-CR_SCE_REL_Clarfication_of_banning_interval_format
OMA-TS-SCE_REL-V1_0-20080626-D	26 Jun 2008	5.5.2, 5.5.5, 5.5.6, 5.5.7.	Incorporated: OMA-DRM-2008-0246R01-CR_Resolve_REL028_and_REL029 OMA-DRM-2008-0249R01-CR_Decrease_of_copy_counter_in_REL
OMA-TS-SCE_REL-V1_0-20080815-D	15 Aug 2008	5.2.2 5.5.4.2	Incorporated resolution to comments: REL-044, REL-005, REL-020 Acronym REK corrected to "Rights Object Encryption Key" as per AP 976. Inserted agreed definitions from INP 261R03. OMA-DRM-2008-0253R03-CR_Revision_of_text_of_party_element.doc
OMA-TS-SCE_REL-V1_0-20080829-D	29 Aug 2008	5.1.1.1 5.2.1, 5.2.2, 5.4.1, 5.4.2, 5.4.4, 5.4.5, 5.4.6, 5.5.1, 5.5.2, 5.5.3, 5.5.4, 5.5.6, 5.5.7, 5.5.8, 5.5.9, 5.6.1, 5.6.3 C.3	Incorporated: OMA-DRM-2008-0347R01-CR_SCE_REL_TS_example_for_adhoc_share_permission.doc OMA-DRM-2008-0351R01-CR_REL_TS_clean_up.doc

Reference	Date	Sections	Description
OMA-TS-SCE_REL-V1_0-20080923-D	23 Sep 2008	whole document	Incorporated: OMA-DRM-2008-0360R03-CR_SCE_REL_TS_Converged_KMS
OMA-TS-SCE_REL-V1_0-20081016-D	16 Oct 2008	5.3.1 5.3.5 5.6 5.1.1	Incorporated: OMA-DRM-2008-0418R01-CR_REL_fix_CEK_hash_element OMA-DRM-2008-0396R02-CR_SCE_REL_Proposal_for_Resolving_CONR_Comment_LRM016
OMA-TS-SCE_REL-V1_0-20081031-D	31 Oct 2008	5.1.1 5.3.5 5.3.6 5.4.5 5.5 Appendix B	Incorporated: OMA-DRM-2008-0316R03-CR_SCE_REL_TS_SCR_Tables OMA-DRM-2008-0420R01-INP_XMLSchemas OMA-DRM-2008-0430R04-CR_REL_TS_Clarification_of_Move_Indication_Element OMA-DRM-2008-0460R02-CR_REL_TS_contexRequired_Constraint OMA-DRM-2008-0467R01-CR_REL_explanation_of_lending_and_stateful_rights OMA-DRM-2008-0468R01-CR_SCE_REL_issuerURL_in_party_element OMA-DRM-2008-0479R01-CR_SCE_REL_XML_for_CEK_Hash Use common referencing scheme form OMA-DRM-2008-0179R01 Add missing reference [RFC2392] and [SCE-DRM]
Candidate Version OMA-TS-SCE_REL-V1_0-20081209-C	12 Dec 2008	n/a	Status changed to Candidate by TP TP ref# OMA-TP-2008-0475-INP_SCE_V1_0_ERP_for_Candidate_Approval

Appendix B. Static Conformance Requirements (Normative)

B.1 DRM Agent Conformance Requirements

This section enumerates conformance requirements for the DRM Agent. The following table extends Appendix B.1 Client Conformance Requirements in [DRM-REL-v2.1].

Item	Function	Reference	Requirement
SCE-REL-DRMAGENT-C-001-M	<rights> element	5.1.1	
SCE-REL-DRMAGENT-C-002-O	<moveIndication> element	5.1.1	
SCE-REL-DRMAGENT-C-003-M	<agreement> element	5.2.1	
SCE-REL-DRMAGENT-C-004-M	<party> element	5.2.2	
SCE-REL-DRMAGENT-C-005-M	<context> element	5.3.1	
SCE-REL-DRMAGENT-C-006-M	<version> element	5.3.2	
SCE-REL-DRMAGENT-C-007-M	<uid> element	5.3.3	
SCE-REL-DRMAGENT-C-008-M	<date> element	5.3.4	
SCE-REL-DRMAGENT-C-009-O	<CEKHash>	5.3.5	
SCE-REL-DRMAGENT-C-010-M	<permission> element	5.4.1	
SCE-REL-DRMAGENT-C-011-O	<move> element	5.4.2	
SCE-REL-DRMAGENT-C-012-O	<copy> element	5.4.3	
SCE-REL-DRMAGENT-C-013-O	<adhoc-share> element	5.4.4	SCE-REL-LRM-S-009-O AND SCE-REL-DRMAGENT-C-016-O AND SCE-REL-DRMAGENT-C-017-O
SCE-REL-DRMAGENT-C-014-O	<lend> element	5.4.5	SCE-REL-DRMAGENT-C-009-O AND SCE-REL-LRM-S-018-O
SCE-REL-DRMAGENT-C-015-M	<constraint> element	5.5.1	
SCE-REL-DRMAGENT-C-016-O	<count> element	5.5.2	
SCE-REL-DRMAGENT-C-017-O	<userDomain> element	5.5.3	
SCE-REL-DRMAGENT-C-018-O	<proximity> element	5.5.4	
SCE-REL-DRMAGENT-C-019-O	<system> element	5.5.5	
SCE-REL-DRMAGENT-C-020-O	<banning-interval> element	5.5.6	
SCE-REL-DRMAGENT-C-021-O	<max-concurrent> element	5.5.7	
SCE-REL-DRMAGENT-C-022-O	<lending-interval> element	5.5.8	

B.2 Rights Issuer Conformance Requirements

This section enumerates conformance requirements for the Rights Issuer, i.e. an entity with only the oma-kp-RightsIssuer key purpose. The following table extends Appendix B.2 Server Conformance Requirements in [DRM-REL-v2.1].

Item	Function	Reference	Requirement
SCE-REL-RI-S-001-M	<rights> element	5.1.1	
SCE-REL-RI-S-002-O	<moveIndication> element	5.1.1	
SCE-REL-RI-S-003-M	<agreement> element	5.2.1	
SCE-REL-RI-S-004-M	<party> element	5.2.2	
SCE-REL-RI-S-005-M	<context> element	5.3.1	
SCE-REL-RI-S-006-M	<version> element	5.3.2	
SCE-REL-RI-S-007-M	<uid> element	5.3.3	
SCE-REL-RI-S-008-O	<date> element	5.3.4	
SCE-REL-RI-S-009-O	<CEKHash>	5.3.5	
SCE-REL-RI-S-010-M	<permission> element	5.4.1	
SCE-REL-RI-S-011-O	<move> element	5.4.2	
SCE-REL-RI-S-012-O	<copy> element	5.4.3	
SCE-REL-RI-S-013-O	<adhoc-share> element	5.4.4	SCE-REL-LRM-S-009-O AND SCE-REL-RI-S-016-O AND SCE-REL-RI-S-017-O
SCE-REL-RI-S-014-O	<lend> element	5.4.5	SCE-REL-LRM-S-009-O AND SCE-REL-

Item	Function	Reference	Requirement
			RI-S-018-O
SCE-REL-RI-S-015-M	<constraint> element	5.5.1	
SCE-REL-RI-S-016-O	<count> element	5.5.2	
SCE-REL-RI-S-017-O	<userDomain> element	5.5.3	
SCE-REL-RI-S-018-O	<proximity> element	5.5.4	
SCE-REL-RI-S-019-O	<system> element	5.5.5	
SCE-REL-RI-S-020-O	<banning-interval> element	5.5.6	
SCE-REL-RI-S-021-O	<max-concurrent> element	5.5.7	
SCE-REL-RI-S-022-O	<lending-interval> element	5.5.8	

B.3 Local Rights Manager Conformance Requirements

This section enumerates conformance requirements for the Local Rights Manager, i.e. an entity with at least the oma-kp-localRightsManagerDevice key purpose.

Item	Function	Reference	Requirement
SCE-REL-LRMDEV-S-001-M	<rights> element	5.1.1	
SCE-REL-LRMDEV-S-002-O	<moveIndication> element	5.1.1	
SCE-REL-LRMDEV-S-003-M	<agreement> element	5.2.1	
SCE-REL-LRMDEV-S-004-M	<party> element	5.2.2	
SCE-REL-LRMDEV-S-005-M	<context> element	5.3.1	
SCE-REL-LRMDEV-S-006-M	<version> element	5.3.2	
SCE-REL-LRMDEV-S-007-M	<uid> element	5.3.3	
SCE-REL-LRMDEV-S-008-O	<date> element	5.3.4	
SCE-REL-LRMDEV-S-009-O	<CEKHash>	5.3.5	
SCE-REL-LRMDEV-S-010-M	<permission> element	5.4.1	
SCE-REL-LRMDEV-S-011-O	<move> element	5.4.2	
SCE-REL-LRMDEV-S-012-O	<copy> element	5.4.3	
SCE-REL-LRMDEV-S-013-O	<adhoc-share> element	5.4.4	SCE-REL-LRMDEV-S-009-O AND SCE-REL-LRMDEV-S-016-O AND SCE-REL-LRMDEV-S-017-O
SCE-REL-LRMDEV-S-014-O	<lend> element	5.4.5	SCE-REL-LRMDEV-S-009-O AND SCE-REL-LRMDEV-S-018-O
SCE-REL-LRMDEV-S-015-M	<constraint> element	5.5.1	
SCE-REL-LRMDEV-S-016-O	<count> element	5.5.2	
SCE-REL-LRMDEV-S-017-O	<userDomain> element	5.5.3	
SCE-REL-LRMDEV-S-018-O	<proximity> element	5.5.4	
SCE-REL-LRMDEV-S-019-O	<system> element	5.5.5	
SCE-REL-LRMDEV-S-020-O	<banning-interval> element	5.5.6	
SCE-REL-LRMDEV-S-021-O	<max-concurrent> element	5.5.7	
SCE-REL-LRMDEV-S-022-O	<lending-interval> element	5.5.8	

B.4 Local Rights Manager Conformance Requirements

This section enumerates conformance requirements for the Local Rights Manager, i.e. an entity with at least the oma-kp-localRightsManagerDomain key purpose.

Item	Function	Reference	Requirement
SCE-REL-LRMDOM-S-001-M	<rights> element	5.1.1	
SCE-REL-LRMDOM-S-002-O	<moveIndication> element	5.1.1	
SCE-REL-LRMDOM-S-003-M	<agreement> element	5.2.1	
SCE-REL-LRMDOM-S-004-M	<party> element	5.2.2	
SCE-REL-LRMDOM-S-005-M	<context> element	5.3.1	
SCE-REL-LRMDOM-S-006-M	<version> element	5.3.2	
SCE-REL-LRMDOM-S-007-M	<uid> element	5.3.3	

Item	Function	Reference	Requirement
SCE-REL-LRMDOM-S-008-O	<date> element	5.3.4	
SCE-REL-LRMDOM-S-009-O	<CEKHash>	5.3.5	
SCE-REL-LRMDOM-S-010-M	<permission> element	5.4.1	
SCE-REL-LRMDOM-S-011-O	<move> element	5.4.2	
SCE-REL-LRMDOM-S-013-O	<adhoc-share> element	5.4.4	SCE-REL-LRMDOM-S-009-O AND SCE-REL-LRMDOM-S-016-O AND SCE-REL-LRMDOM-S-017-O
SCE-REL-LRMDOM-S-014-O	<lend> element	5.4.5	SCE-REL-LRMDOM-S-009-O AND SCE-REL-LRMDOM-S-018-O
SCE-REL-LRMDOM-S-015-M	<constraint> element	5.5.1	
SCE-REL-LRMDOM-S-016-O	<count> element	5.5.2	
SCE-REL-LRMDOM-S-018-O	<proximity> element	5.5.4	
SCE-REL-LRMDOM-S-019-O	<system> element	5.5.5	
SCE-REL-LRMDOM-S-020-O	<banning-interval> element	5.5.6	
SCE-REL-LRMDOM-S-021-O	<max-concurrent> element	5.5.7	
SCE-REL-LRMDOM-S-022-O	<lending-interval> element	5.5.8	

Appendix C. Examples (Informative)

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

C.1 Play under Proximity Constraint Using Fictive Proximity Method "GPS"

The rights depicted in this example grant permission to play the corresponding DRM Content on another device under the constraint that proximity of the two devices is verified using the (fictive) Proximity Method “GPS” and the distance between the two devices is less than 100 meters. The additional parameter to the Proximity Method is given as additional element in the name space that is named after the registered name of the Proximity Method.

Note that the “play” permission given under the proximity constrained in the example below is applicable in the case of rendering the content on the other device. It does not affect possible other “play” permissions without proximity constraints for the device containing the RO.

```
<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:permission>
   <o-dd:play>
    <o-ex:constraint>
     <oma-dd:proximity method=”urn:oma:proximity:pm001_gps:1.0”>
      <pm001_gps:distance>100</pm001_gps:distance>
     </oma-dd:proximity>
    </o-ex:constraint>
   </o-dd:play>
  </o-ex:permission>
 </o-ex:agreement>
</o-ex:rights>
```

Play Permission under a Proximity Constraint if distance measured with GPS is less than 100 meters.

C.2 Display under Proximity Constraint Using Fictive Proximity Method "ServiceProvider"

The rights depicted in this example grant permission to play the corresponding DRM Content on another device under the constraint that proximity of the two devices is verified using the (fictive) Proximity Method “ServiceProvider” involving a third party. It is assumed that the third party would remotely verify the proximity using additionally provided parameters, such as the URI for the web service to be contacted in order to determine social proximity (e.g., family members) or the position based on the network cell to which the device is attached.

```
<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:permission>
   <o-dd:display>
    <o-ex:constraint>
     <oma-dd:proximity method=”urn:oma:proximity:pm002_sp:1.0”>
      <pm002_sp:URI>https://proximity.coolmno.mobi</pm002_sp:URI>
      <pm002_sp:IMSI>1234567890</pm002_sp:IMSI>
     </oma-dd:proximity>
    </o-ex:constraint>
   </o-dd:display>
  </o-ex:permission>
 </o-ex:agreement>
</o-ex:rights>
```

Play Permission under a Proximity Constraint using remote evaluation by a service provider

C.3 Ad Hoc Share Permission

The rights depicted in this example grants permission to Ad Hoc Share.

From the DRM Requester’s view, the rights cannot be shared with more than one DRM Agent (by max-concurrent constraint), and it cannot be shared with a DRM Agent until one day has been passed after conducting Ad Hoc Share with same DRM Agent (by banning-interval constraint).

From the DRM Agent’s view, the rights cannot be consumed after 10 minutes 20 seconds from it has been started to be consumed (by interval constraint). The DRM Agent can play and print, but it cannot play the shared rights more than 2 times (by count constraint).

```
<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="idforsignature">
 <o-ex:context>
  <o-dd:version>2.1</o-dd:version>
  <o-dd:uid>ROID</o-dd:uid>
 </o-ex:context>
 <o-ex:agreement>
```

```
  <o-ex:permission>
   <o-dd:play/>
   <oma-dd:adhoc-share>

     <!-- constraint for source device -->
     <o-ex:constraint>
       <oma-dd:max-concurrent>1</oma-dd:max-concurrent>
       <oma-dd:banning-interval>P1D</oma-dd:banning-interval>
     </o-ex:constraint>

     <!—permissions/constraints for recipient device -->
     <o-ex:permission>
      <o-ex:constraint>
        <o-dd:interval>P10M20S</o-dd:interval>
      </o-ex:constraint>
      <o-dd:play>
       <o-ex:constraint>
        <o-dd:count>2</o-dd:count>
       </o-ex:constraint>
      </o-dd:play>
      <o-dd:print/>
     </o-ex:permission>

   </oma-dd:adhoc-share>
  </o-ex:permission>
 </o-ex:agreement>
</o-ex:rights>
```