Secure Content Exchange Architecture

Approved Version 1.0 – 05 Jul 2011

Open Mobile Alliance

OMA-AD-SCE-V1_0-20110705-A

Contents

Figures

1. Scope (Informative)

The scope of this document is to define the architecture for enhancements to the OMA Digital Rights Management (DRM) specifications to enable the secure exchange of DRM -protected content among multiple devices. These enhancements include the following:

- The definition of a centralized domain management function, such that users do not have to manage domains for each source of Rights for a domain
- The definition of an Import function that will allow content protected by non-OMA DRM mechanisms to be consumed by OMA DRM devices. Together with the Export function defined in OMA DRM V2.0, the Import function will make it possible for OMA DRM devices to securely exchange content with non-OMA DRM devices.
- The definition of a Move function that will allow Rights to be moved from one DRM Agent to another DRM Agent, either directly between two Devices or via a Rights Issuer. Move can be the complete Rights or a subset of the remaining Rights (Partial Rights).
- The concept of Ad Hoc Sharing that allows Users to exchange Rights (and thus use shared Protected Content) in an ad hoc manner (as permitted by the Rights Issuer).
- Allow a Device to request from the Rights Issuer the permission to Share Rights, in the case where the User's existing Rights do not explicitly permit Sharing.

2. References

2.1 Normative References

None

2.2 Informative References

[DRM-v2]	OMA DRM V2 Enabler, Open Mobile Alliance™, OMA-ERP-DRM-V2_0-20060303-A, http://www.openmobilealliance.org/
[DRMARCH-v2.1]	"DRM Architecture", Open Mobile Alliance™, OMA-AD-DRM-V2_1, http://www.openmobilealliance.org/
[SCE-RD]	"Secure Content Exchange Requirements", Open Mobile Alliance, OMA-RD-SCE-V1_0, http://www.openmobilealliance.org/
[OMNA]	"Open Mobile Naming Authority", Open Mobile Alliance, http://www.openmobilealliance.org/tech/omna/index.htm
[OCSP-MP]	OMA Online Certificate Status Protocol (profile of [OCSP]) V 1.0, http://www.openmobilealliance.org/

3. Terminology and Conventions

3.1 Conventions

This is an informative document, which is not intended to provide testable requirements to implementations.

3.2 Definitions

Most entities and concepts that are relevant for this document have been adequately defined [SCE-RD]. For convenience, these definitions have been copied into the table below.

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).
Constraint	A restriction on a Permission over DRM Content (DRM V2.0).
Consume	To Play, Display, Print or Execute DRM Content on a Device or to render DRM Content on a Render Client.
Content	One or more Media Objects (DRM V2.0).
Content Issuer	The entity making content available to the DRM Agent in a Device (DRM V2.0).
Content Provider	An entity that is either a Content Issuer or a Rights Issuer (DRM V2.0).
Copy	To make Rights existing on a source Device available for use by a recipient Device, without affecting availability on the source Device. Rights may be restricted on the recipient Device. Note: this is different from the V2.0 definition.
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).
Domain	A group of Devices defined by a Rights Issuer such that the Rights Issuer can issue Rights Objects for the group that can be processed by all Devices within the group, and only those Devices (DRM V2.0).
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.
DRM Agent	The entity in the Device that manages Permissions for Media Objects on the Device (DRM V2.0).
DRM Content	Media Objects that are consumed according to a set of Permissions in a Rights Object (DRM V2.0).
DRM Time	A secure, non user-changeable time source. The DRM Time is measured in the UTC time scale (DRM V2.0).
Import	To convert Import-Ready Data into OMA (P)DCFs and ROs.
Imported-Content	OMA (P)DCF(s) resulting from converting Import-Ready Data.
Import-Ready Data	Content and associated Rights derived from Non-OMA DRM-sourced data that can be converted into OMA (P)DCFs and ROs.
Imported-Rights-Object	An OMA RO resulting from converting Import-Ready Data.
Imported-Data	Imported-Content and associated Imported-Rights-Object(s).
Local Rights Manager (LRM)	An entity that is responsible for aspect(s) of Import and it may also manage an Imported-Content for a limited group of OMA DRM Agents.
Media Object	A digital work e.g. a ring tone, a screen saver, or a Java game (DRM V2.0).

Move	To make Rights existing initially on a source Device fully or partially available for use by a recipient Device, such that the Rights or parts thereof that become usable on the recipient Device can no longer be used on the source Device.
Non-OMA DRM	A protection system other than OMA DRM, which may include copy protection mechanisms for storage medium and/or transport mechanisms.
Partial Rights	A subset of a set of Rights, such that the Partial Rights are equally or more restrictive than those in the set.
Permission	Actual usages or activities allowed (by the Rights Issuer) over DRM Content.
Play	To create a transient, perceivable rendition of a resource.
Protected Content	Media Objects that are consumed according to a set of Permissions in a Rights Object (DRM V2.0).
Proximity Method	A method for determining whether a proximity constraint is met and which provides either true or false as a result. The internal working of the method is out of scope of OMA DRM. Any Proximity Method has a unique name registered with the OMNA [OMNA] and is requested for DRM SCE by means of parameters in the Rights Object.
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 (DRM V2.0).
Rights Object	A collection of Permissions and other attributes which are linked to 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.
State Information	A set of values representing current state associated with Rights. It is managed by the DRM Agent only when the Rights contain any of the stateful constraints (e.g. interval, count, timed-count, accumulated, etc.).
Superdistribution	A mechanism that (1) allows a User to distribute DRM Content to other Devices through potentially insecure channels and (2) enables the User of that Device to obtain a Rights Object for the superdistributed DRM Content (DRM V2.0).
User	The human user of a Device. The User does not necessarily own the Device (DRM V2.0).
User Domain	A group of Devices defined by the Domain Enforcement Agent such that, for example Rights Issuers, can issue Rights Objects with Permissions, Constraints and other attributes specifically for the Devices in the group.

3.3 Abbreviations

CI	Content Issuer
DA	Domain Authority
DEA	Domain Enforcement Agent
DCF	DRM Content Format
DRM	Digital Rights Management
LRM	Local Rights Manager
OMA	Open Mobile Alliance
OMNA	Open Mobile Naming Authority
RI	Rights Issuer
RO	Rights Object
SCE	Secure Content Exchange

4. Introduction (Informative)

This architecture builds on the architecture of OMA DRM 2.0 ([DRMARCH-v2.1]). It enables the following additional functionality:

- Import of non-OMA protected content into OMA DRM by introducing the Local Rights Manager (LRM)
- Central management of the User Domain by introducing the Domain Authority (DA), with an integrated Domain Enforcement Agent (DEA)
- The definition of a Move function that will allow Rights to be moved from one DRM Agent to another DRM Agent, either directly between two Devices or via a Rights Issuer. Move can be the complete Rights or a subset of the remaining Rights (Partial Rights).
- The concept of Ad Hoc Sharing that allows Users to exchange Rights (and thus use shared Protected Content) in an ad hoc manner (as permitted by the Rights Issuer). Additionally a Device is able to request from the Rights Issuer the permission to Share Rights, in the case where the User's existing Rights do not explicitly permit Sharing.

An important design goal is to provide for this new functionality as much as possible in a backward compatible way. This means that existing OMA DRM 2.0 devices should be able to take advantage of the new functionality.

4.1 Planned Phases

This document defines architectural extensions to OMA DRM 2.0 specifically to enable new functionality with respect to the secure exchange of DRM -protected content among multiple devices. In parallel tracks, other extensions to OMA DRM 2.0 are being defined. When this architecture and the related technical specifications are completed, the architecture described in this document will be merged with the overall OMA DRM architecture to produce the then next minor version of OMA DRM. For convenience we will call the targeted enabler: “OMA DRM 2.SCE1”.

The DLDRM group will make sure that the architectural extensions described in this document do not conflict with other extensions in preparation and ensure that the envisioned merger is a straightforward clerical process.

This version of SCE does not aim to address all requirements in [SCE-RD].

4.2 Security Considerations

This architecture is fully based on the Trust and Security Model of OMA DRM 2.0 (see [DRMARCH-v2.1], chapter 5), considers the current level of security in OMA DRM 2.0 adequate and does NOT aim to improve the specifications in this direction.

The main new threats compared to OMA DRM 2.0 are:

- Device local creation of RO’s and DCF’s
- Management of the User Domain by an entity other than the Rights Issuer.

These threats will be addressed in this architecture and the technical specifications.

4.3 Proximity

4.3.1 Meaning and Scope

The DRM SCE Enabler allows or disallows the secure content exchange between two Devices 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. For example, proximity between two Users could be interpreted as belonging to the same community (e.g., a project team or a sports club). Since many different ways of determining proximity are possible, the architecture defines the abstract concept of Proximity Methods but leaves the actual specification of those Proximity Methods out of scope. The function of a Proximity Method is to return the result of whether two Devices or two Users are in proximity or not in proximity. Therefore, the SCE enabler will extend the set of OMA DRM protocols to enable secure exchange of content between Devices, building – if needed – on Proximity Methods that are not specified by SCE.

The SCE specified protocols will allow services and Devices to securely communicate the need for proximity measurements between Devices, but the actual Proximity (measurement) Methods and related compliancy and robustness rules are not in scope for OMA DRM. This is analogous to OMA DRM 2.0 which specifies the protocols needed to securely acquire content, but building on a trust and compliancy infrastructure that is not specified by OMA DRM. Therefore the SCE enabler will allow other bodies and standards to specify and mandate implementation of certain proximity measurement methods. The SCE Enabler will provide the functionality to allow services and Devices to communicate when and how these methods must be used to assure the secure exchange of content.

The DRM SCE Enabler uses the Rights Object to determine which Proximity Method (or combination of Proximity Methods) to apply and with what parameters for the respective method(s). A Rights Issuer may mandate one or more Proximity Methods by means of the Rights Object that must all evaluate to true for the Rights Objects to be passed from one DRM Agent to another. If a mandated Proximity Method is not supported by the Device then the proximity constraint is considered not to be met.

4.3.2 Proximity Methods

Proximity Methods test certain conditions to determine whether a proximity constraint is met. The conditions and how they are tested is out of scope of the OMA DRM SCE Enabler. Technically speaking, a Proximity Method is a boolean function which results in either true or false. True means “in proximity” or, in other words, that the proximity constraint is met. A Proximity Method may involve only the two Devices involved to determine whether they are in proximity but may also involve a third Entity. For example, a mobile network operator can determine reliably whether two Devices are within the same network cell. A service provider could determine whether two Users are belonging to the same project team etc.

The DRM SCE Enabler addresses the following types of Proximity Methods:

- Proximity Methods that involve only the two Devices for which the condition of proximity is measured. As an example that could be done using short range wireless network connectivity between the two Devices containing the DRM Agents.
- Proximity Methods using a third party (a proximity verifier) for determining or verifying other aspects of proximity, e.g., a service provider with the ability to verify social proximity or the positions of the wireless network cells the Devices are in.

Each required Proximity Method shall be listed in the Rights Object with its registered name and additional values that parameterize each method and that may be different for different Proximity Methods. Examples for illustration: A Proximity Method named “GPS” could contain a parameter for the maximum distance allowed between Devices, e.g., 100 m; The “ServiceProvider” Proximity Method could contain a URI for the web service to be contacted in order to determine social proximity or the position of the network cell.

Because the actual specification of Proximity Methods is out of scope of the DRM SCE Enabler, Proximity Methods shall be registered by third parties under their respective names with the Open Mobile Naming Authority (OMNA). For more information see http://www.openmobilealliance.org/tech/omna/index.htm.

5. Architectural Model

5.1 Dependencies

This architecture builds on the architecture of OMA DRM 2.0 ([DRMARCH-v2.1]) and on [OCSP-MP]. There are no dependencies on other enablers.

5.2 Architectural Diagram

Figure 1 provides an overview of the architecture

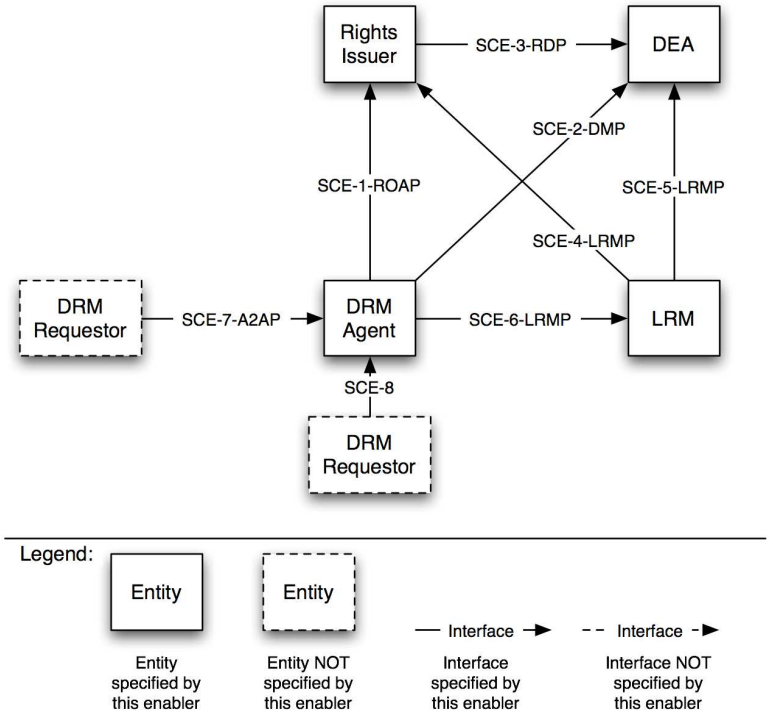

Figure 1: Architecture overview

All entities and protocols are described in subsequent sections.

The SCE requirements require the SCE enabler to allow deployment of the DEA either in the network or on a User's equipment, separate from the DA. This version of the SCE enabler does not address the interface between DA and DEA, whether or not the DEA is in the network.

5.3 Functional Components and Interfaces

5.3.1 DRM Agent

The main responsibility of the DRM Agent is unchanged compared to OMA DRM 2.0:

> A DRM Agent embodies a trusted entity in a device. This trusted entity is responsible for enforcing permissions and constraints associated with DRM Content, controlling access to DRM Content, etc.

Compared to OMA DRM 2.0, new functionalities for the DRM Agent include:

- Handling of User Domain Rights Objects. The DRM Agent will specify during the purchasing process to the RI to which User Domain the Rights should be bound.
- Mutual authentication and establishment of secure authenticated channel between DRM Agents
- Support of new permissions such as Move, Ad-hoc Share and Lend.
- Requesting a Rights Issuer to upgrade existing Rights Objects with additional permissions (e.g. Move, Ad-hoc Share, etc.)

5.3.2 Rights Issuer (RI)

The main responsibility of the Rights Issuer (RI) is unchanged compared to OMA DRM 2.0:

> The rights issuer is an entity that assigns permissions and constraints to DRM Content, and generates Rights Objects. A Rights Object is an XML document expressing permissions and constraints associated with a piece of DRM Content. Rights Objects govern how DRM Content may be used – DRM Content cannot be used without an associated Rights Object, and may only be used as specified by the Rights Object.

Compared to OMA DRM 2.0, the new functionalities for RI's include:

- Providing Rights Objects for a User Domain, as defined by a Domain Authority
- Providing Rights Objects for (P)DCF's created by an LRM from Import-ready data.
- Assisting in Move of Rights from one DRM Agent to another
- Upgrading existing Rights Objects with additional permissions upon request from DRM Agents

5.3.3 Domain Enforcement Agent (DEA)

The main responsibility of the Domain Enforcement Agent (DEA) is to manage a User Domain based on a given User Domain Policy that has been assigned to the DEA by a DA. The DEA ensures that the User Domain conforms to the limits as specified in the User Domain Policy.

The ultimate goal is to enable a User to define a set of Devices (the User Domain) once with the DEA and acquire Rights Objects for this set of Devices from various sources: RI's or LRM's. In this way the User is assured that Content for his/her User Domain can be freely exchanged between his/her Devices and accessed on all of them, regardless of where the Content was purchased or from where it was imported.

5.3.4 Local Rights Manager (LRM)

The main responsibility of the Local Rights Manager (LRM) is to create RO's and (P)DCF's from Import-ready data. The created RO's will only be accessible to a specific device, a specific OMA DRM 2.0 domain or a specific User Domain.

5.3.5 SCE-1-ROAP

The SCE-1-ROAP protocol is an extended version of the ROAP 1.0 protocol as specified in OMA DRM 2.0:

> The Rights Object Acquisition Protocol (ROAP) is the common name for a suite of DRM security protocols between a Rights Issuer (RI) and a DRM Agent in a Device. The protocol suite contains a 4-pass protocol for registration of a Device with an RI and two protocols by which the Device requests and acquires Rights Objects (RO). The 2-pass RO acquisition protocol encompasses request and delivery of an RO whereas the 1-pass RO acquisition protocol is only a delivery of an RO from an RI to a Device (e.g. messaging/push). The ROAP suite also includes 2-pass protocols for Devices joining and leaving a Domain; the Join Domain protocol and the Leave Domain protocol.

As in OMA DRM 2.0, the basic function is to deliver RO's from an RI to a DRM Agent. The extensions are related to being able to request and deliver RO's for a User Domain. The ROAP 1.0 protocols for domain management are still relevant to allow OMA DRM 2.0 devices to join a User Domain.

5.3.6 SCE-2-DMP

The Domain Management Protocol SCE-2-DMP is used by the DEA to manage a User Domain. Using this protocol, the DEA will add and remove Devices to/from the User Domain. Functionally the SCE-2-DMP protocol is quite similar to the domain management protocols in the OMA DRM 2.0-ROAP 1.0 protocol. New functionality may include allowing a DEA to specify to a Device which RI's and LRM's are allowed to provide Rights for the User Domain.

5.3.7 SCE-3-RDP

The RI-DEA Protocol SCE-3-RDP is used by the DEA and RI to enable a Rights Issuer to issue Rights Objects for a User Domain managed by the DEA. Using this protocol, the DEA and RI will agree on a Domain Policy and exchange the secrets the RI needs to create RO's for the User Domain.

5.3.8 SCE-4-LRMP

The Local Rights Manager Protocol SCE-4-LRMP protocol is used to enable an LRM to import Rights to an OMA DRM V2.x-only Device or into an OMA DRM V2.x Domain (that is managed by an RI). Possible robustness rules and backward compatibility issues (see section on Security Considerations) require that such importing of Rights is partly implemented in the LRM and partly implemented in an RI. The Local Rights Manager Protocol SCE-4-LRMP protocol is used to enable the required split in deployment and collaboration between an RI and an LRM.SCE-5-LRMP

The Local Rights Manager Protocol SCE-5-LRMP is used to enable an LRM to import Rights into a User Domain.

5.3.9 SCE-6-LRMP

The SCE-6-LRMP interface is used to transfer Imported-Rights-Objects to a DRM Agent. The interface is typically used by DRM Agents to request Rights for Imported Content. This interface is similar to the SCE-7-A2AP interface.

5.3.10 SCE-7-A2AP

The Agent to Agent SCE-7-A2AP interface is used to exchange Rights and corresponding information to a DRM Agent. The interface is typically used by other DRM Agents. This interface is similar to the SCE-6-LRMP interface.

5.3.11 SCE-8

The SCE-8 interface is used to exchange Rights to a DRM Agent. In contrast to the interfaces SCE-7-A2AP and SCE-6-LRMP, the SCE-8 interface will only provide a Data Specification for the data that is exchanged in this interface. In this way the Content and Rights can be exchanged between Devices via any protocol. The mechanism is similar to the Domain concept in OMA DRM 2.0.

5.4 Flows

By default, the entities exchanging messages in these flows (LRM, RI, DA, DRM Agent) are conformant to the version of OMA DRM as specified by the SCE enabler. In case of interaction with an entity that is conformant to another version of OMA DRM, this is indicated in the text and in name of the entity (e.g. “2.0 DRM Agent”).

5.4.1 Registration of an LRM

Figure 2 depicts the flow of events that is used when a LRM registers with a RI and a DA/DEA.

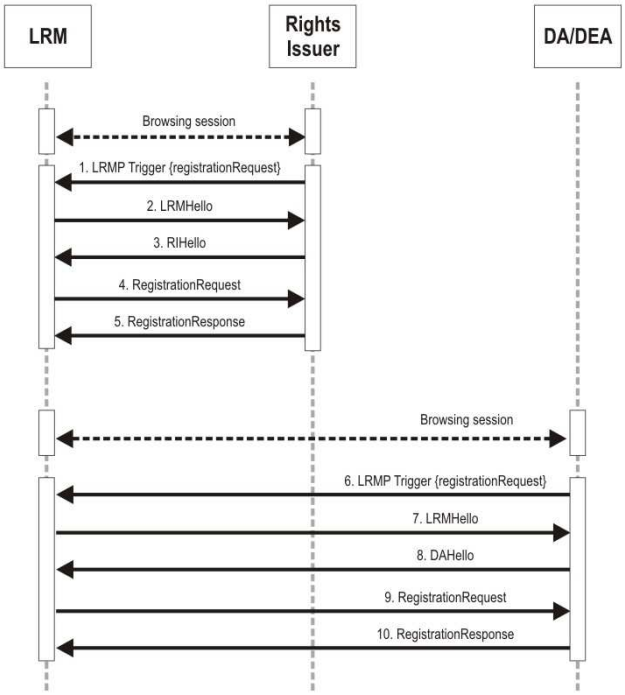

Figure 2: Registration of a LRM

Calls

1-5 The LRM registers with the RI. The involved protocol is similar to Device-RI registration in OMA DRM 2.0. Part of the registration will be a mutual authentication. This protocol is executed the first time the LRM and RI communicate and may be repeated when the registration expires. The protocol is typically preceded by a browsing session, which results in the delivery of a trigger to the LRM.

6-10 The LRM registers with the DA/DEA. The involved protocol is similar to Device-RI registration in OMA DRM 2.0. Part of the registration will be a mutual authentication. This protocol is executed the first time the LRM and DA/DEA communicate and may be repeated when the registration expires. The protocol is typically preceded by a browsing session, which results in the delivery of a trigger to the LRM.

5.4.2 Import for a specific OMA DRM 2.0 Device

Figure 3 depicts the flow of events in case of import for an OMA DRM 2.0 Device with a DRM Agent that is conformant to OMA DRM 2.0 specification (called "2.0 DRM Agent").

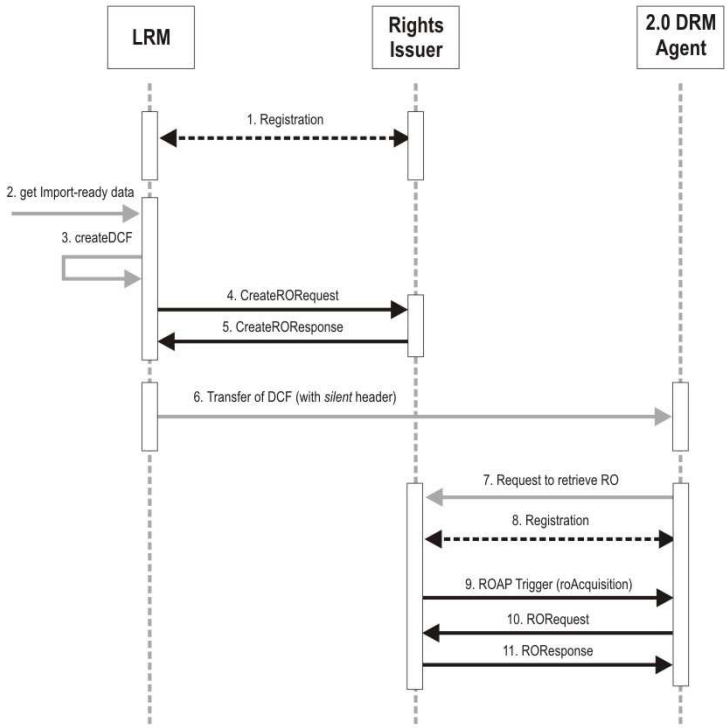

Figure 3: Import for a specific OMA DRM 2.0 Device

Calls:

1 The LRM registers with the RI as described in section 5.4.1.

2-5 The LRM receives Import-ready data from an entity outside of the scope of OMA DRM, creates a DCF from it and requests the creation of an RO for the Import-ready data. In the CreateRORequest/Response-calls, the LRM and RI will exchange the identity of the OMA DRM 2.0 Device for which the RO is to be created, the permissions and restrictions that should be expressed in the RO as well as any necessary key material and other information (e.g. metadata like RightsIssuerURL, SilentURLs etc.). The RI saves the information and prepares for RO creation.. The DCF will contain a silent header, to initiate download of the RO by the Device. The sequence of calls may be somewhat different. In case of streaming content for instance, the LRM may request an RO from initial Import ready data and then create a DCF while still receiving the rest of the Import-ready data.

6 The DCF is transported to the Device, as enabled by OMA DRM 2.0 super distribution.

7-11 Using the silent header information contained in the DCF, the DRM Agent contacts the RI for retrieving the RO. If the RI does not have a valid Device Context with the Device (e.g. the Device has not registered or the existing registration has expired), the RI first requests the DRM Agent to register. The RI creates an OMA DRM 2.0 compatible RO based on the information obtained at step 8 and triggers the DRM Agent to acquire the RO.

Note that the RI may create the RO at step 4 if a valid Device Context for the Device already exists.

Calls 2-11 are repeated for each piece Content that is created from Import-ready data.

5.4.3 Import into a OMA DRM 2.0 Domain

Figure 4 depicts the flow of events in case of import into a OMA DRM 2.0 Domain.

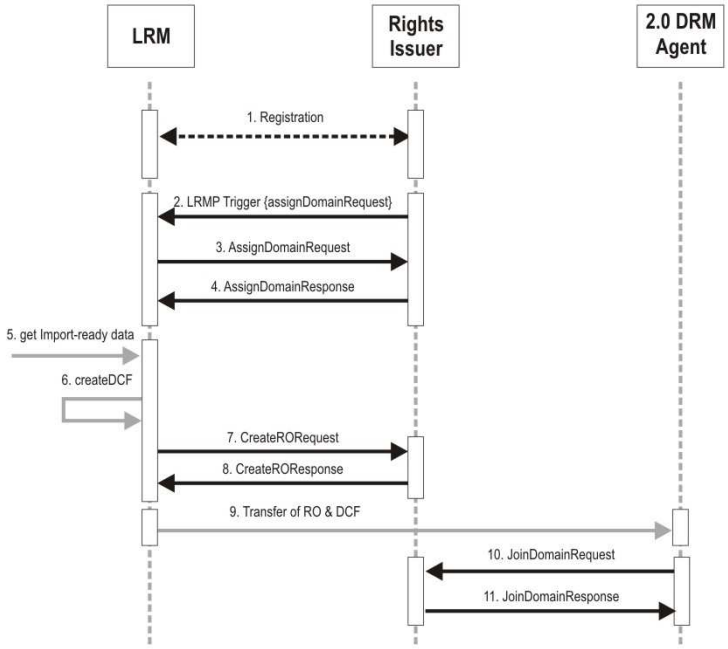

Figure 4: Import into a OMA DRM 2.0 Domain

Calls

1 The LRM registers with the RI as described in section 5.4.1.

2-4 The LRM is assigned to a specific Domain. The involved protocols are similar to the Device join domain protocols as in OMA DRM 2.0. The purpose of these calls is to exchange any additional (domain specific) information and/or keys that are necessary to be exchanged between RI and LRM to create RO's for a (User) Domain. These calls may be repeated e.g. when the domain context expires or when the domain generation is upgraded.

5-8 The LRM receives Import-ready data from an entity outside of the scope of OMA DRM, creates a DCF from it and request the creation of an RO for the Import-ready data. In the CreateRORequest/Response-calls, the LRM and RI will exchange the permissions and restrictions that should be expressed in the RO as well as any necessary key material and other information. The RI creates an OMA DRM 2.0 compatible RO from this information and returns it to the LRM. The sequence of calls may be somewhat different. In case of streaming content for instance, the LRM may request an RO from initial Import ready data and then create a DCF while still receiving the rest of the Import-ready data. These calls are repeated for each piece Content that is created from Import-ready data.

9 The RO and DCF may be transported to other Devices, as enabled by OMA DRM 2.0. This is outside of scope for OMA DRM.

10-11 Using the information contained in the RO, the DRM Agents in other Device may request from the RI to be added to the Domain as specified in OMA DRM 2.0. When the DRM Agent is already part of the Domain, these call are not necessary.

5.4.4 Import into a User Domain – RO created by LRM

Figure 5 depicts the flow of events in case of import into a User Domain.

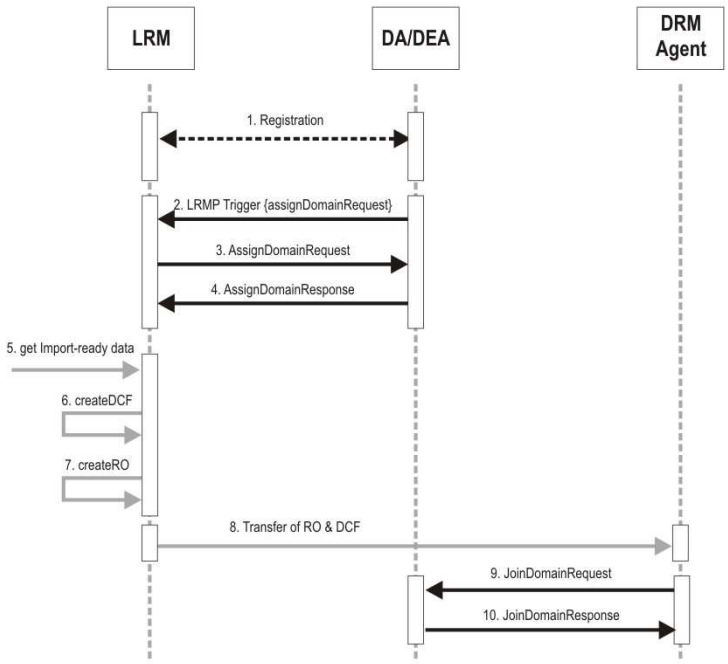

Figure 5: Import into a User Domain (LRM creates RO)

Calls

1 The LRM registers with the DA/DEA as described in section 5.4.1.

2-4 The LRM is assigned to a specific User Domain. The involved protocols are similar to the Device join domain protocols as in OMA DRM 2.0. The purpose of these calls is to exchange any additional (domain specific) information and/or keys that are necessary to be exchanged between RI and LRM to create RO's for a (User) Domain. These calls may be repeated e.g. when the domain context expires or when the domain generation is upgraded.

5-7 The LRM receives Import-ready data from an entity outside of the scope of OMA DRM and creates a DCF and an RO from it. The sequence of calls may be somewhat different. In case of streaming content for instance, the LRM may create an RO from initial Import ready data and then create a DCF while still receiving the rest of the Import-ready data. These calls are repeated for each piece Content that is created from Import-ready data

8 The RO and DCF may be transported to other Devices, as enabled by OMA DRM 2.0. This is outside of scope for OMA DRM.

9-10 Using the information contained in the RO, the DRM Agents in other Devices may request from the DEA to be added to the User Domain. The protocols are very similar to the join domain protocols as specified in OMA DRM 2.0. This may first require registration of the Device with the DA/DEA, described in section 5.4.8. When the DRM Agent is already part of the User Domain, these calls (including the registration) are not necessary.

5.4.5 Import into a User Domain – RO created by RI

Figure 6 depicts an alternative flow for import into a User Domain in which the RI creates RO for imported content. Note that the RI will only create RO for content imported by a LRM that is known (by the RI) to have successfully registered with the DA/DEA and that has been assigned to the target User Domain.

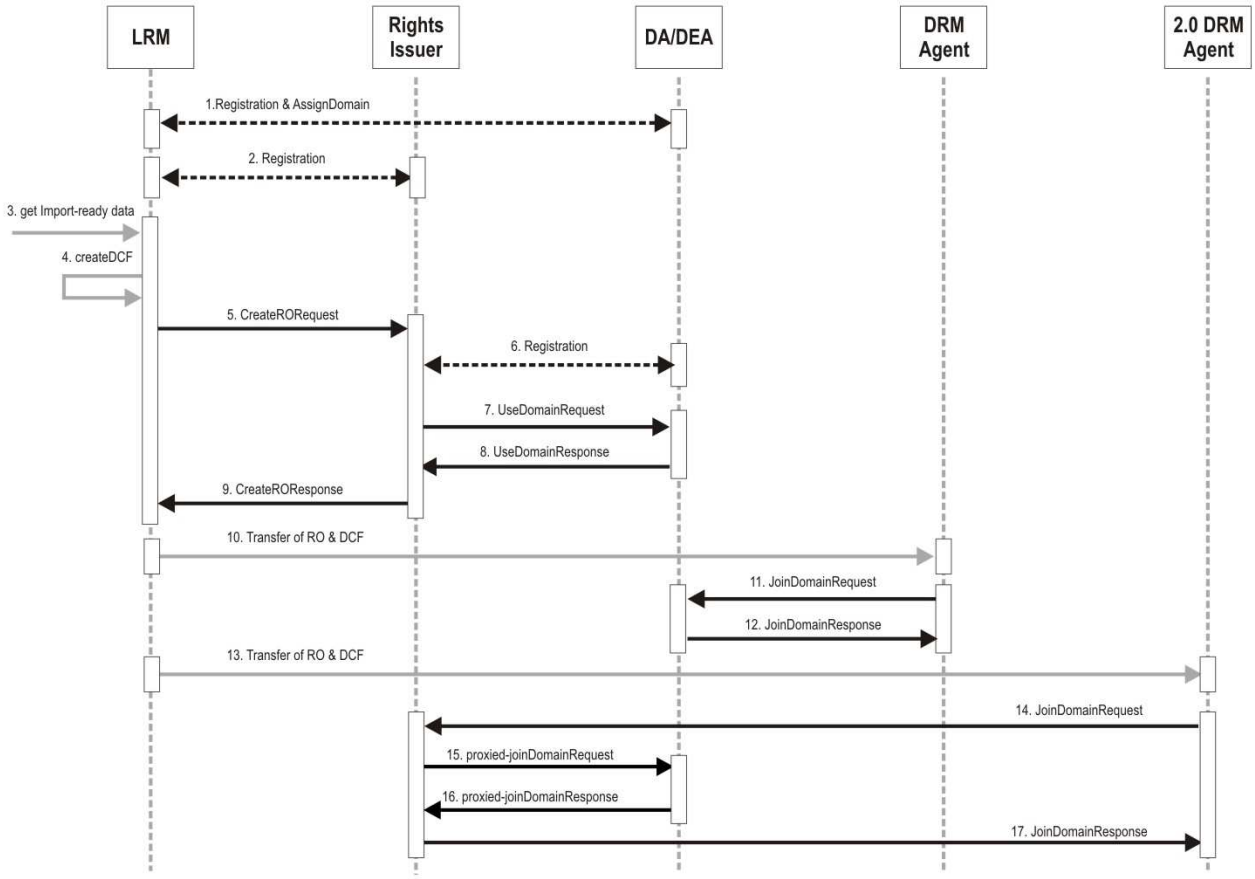

Figure 6: Import into a User Domain (RI creates RO)

Calls

1 The LRM registers with the DA/DEA and joins the User Domain, as described in 5.4.4.

2 The LRM registers with the RI, as described in section 5.4.1.

3-5 The LRM receives Import-ready data from an entity outside of the scope of OMA DRM, creates a DCF from it and requests the creation of an RO for the Import-ready data. In the CreateRORequest call, the LRM specifies the permissions and restrictions that should be expressed in the RO and identifies the User Domain for which the RO should be created. The sequence of calls may be somewhat different. In case of streaming content for instance, the LRM may request an RO from initial Import ready data and then create a DCF while still receiving the rest of the Import-ready data. These calls are repeated for each piece Content that is created from Import-ready data.

6 The DA/DEA registers with the RI. The involved protocols are similar to Device-RI registration in OMA DRM 2.0. Part of the registration will be a mutual authentication. Also see section 5.4.7.

7-8 The RI and the DA/DEA exchange information and key material that enable the RI to create the RO. The RI will use this information to check that it trusts the DA/DEA responsible for this User Domain and that it supports the associated Domain Policy.

9 The RI returns the created RO to the LRM in the CreateROResponse message.

10 The RO and DCF may be transported to other SCE conformant Devices, as enabled by OMA DRM 2.0. This is outside of scope for OMA DRM.

11-12 Using the information contained in the RO, the DRM Agents in other Devices may request from the DA/DEA to be added to the User Domain. The protocols are very similar to the join domain protocols as specified in OMA DRM 2.0. This may first require registration of the Device with the DA/DEA, described in section 5.4.8. When the DRM Agent is already part of the User Domain, these calls (including the registration) are not necessary.

13 The RO and DCF may be transported to DRM 2.0 conformant Devices, as enabled by OMA DRM 2.0. This is outside of scope for OMA DRM.

14-17 The OMA DRM 2.0 conformant DRM Agent is unable to contact a DA/DEA. Instead it uses the information contained in the RO to contact the RI (as specified in OMA DRM 2.0) to register and request to be joined to the domain. The RI acts as proxy for the DA/DEA and forwards the join domain call to the DA/DEA that manages the domain. These calls are executed the first time the 2.0 DRM Agent encounters Content provided by this RI and may be repeated e.g. after the registration or domain context expires. Also see section 5.4.9.

5.4.6 Import and subsequent Move

Figure 7 depicts the flow of events that is used when Import-Ready Data is to be imported for use on a specific Device in the User Domain.

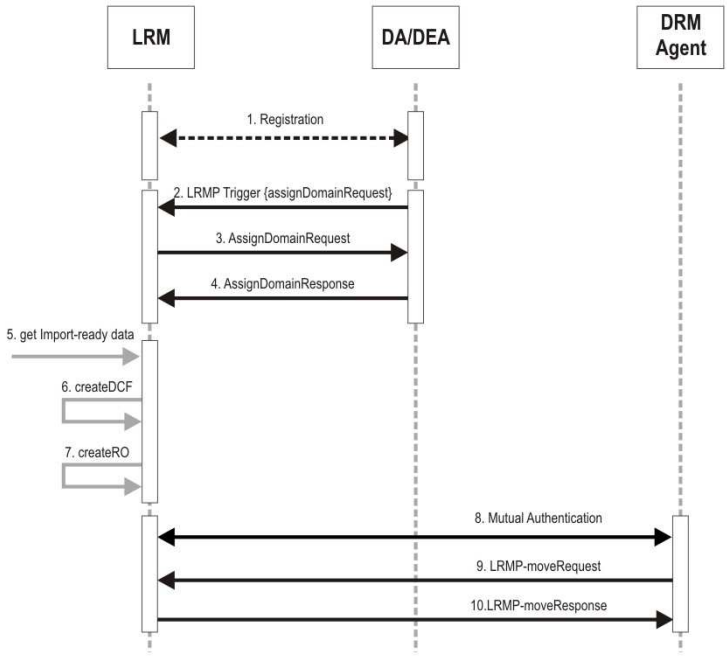

Figure 7: Import to a specific Device in a User Domain

Calls

1-7 These calls are similar to those in Figure 5 of section 5.4.4. Via these calls the DA/DEA authorizes the assignment within the User Domain of specific DRM Agents to the particular LRM.

8 The LRM and DRM Agent complete a mutual authentication. As a result of successful mutual authentication, a session between the LRM and the DRM Agent is established.

9-10 The DRM Agent requests LRM transfers the Rights from to the DRM Agent LRM using a in a A2APLRMP-import importRequest. The DRM Agent LRM processes the A2AP-moveRequest importRequest and then sends a A2APLRMP-moveResponse importResponse to the LRMDRM Agent.

Note that calls 8-10 are similar to calls 3 and 5-6, respectively, in section 5.4.13. Note also (although not shown within Figure 7) that the DRM Agent may use protocols similar to the protocols in section 5.4.13 to subsequently Move the Imported-Rights Object(s) to certain other Devices in the User Domain if allowed and enabled by the LRM. In this flow, unlike a domain in OMA DRM V2.0, all Devices in the User Domain do not necessarily possess common cryptographic means (i.e., shared key material) to decrypt Rights Objects.

5.4.7 Purchase for a User Domain

Figure 8 depicts the flow of events in case of purchase for a User Domain.

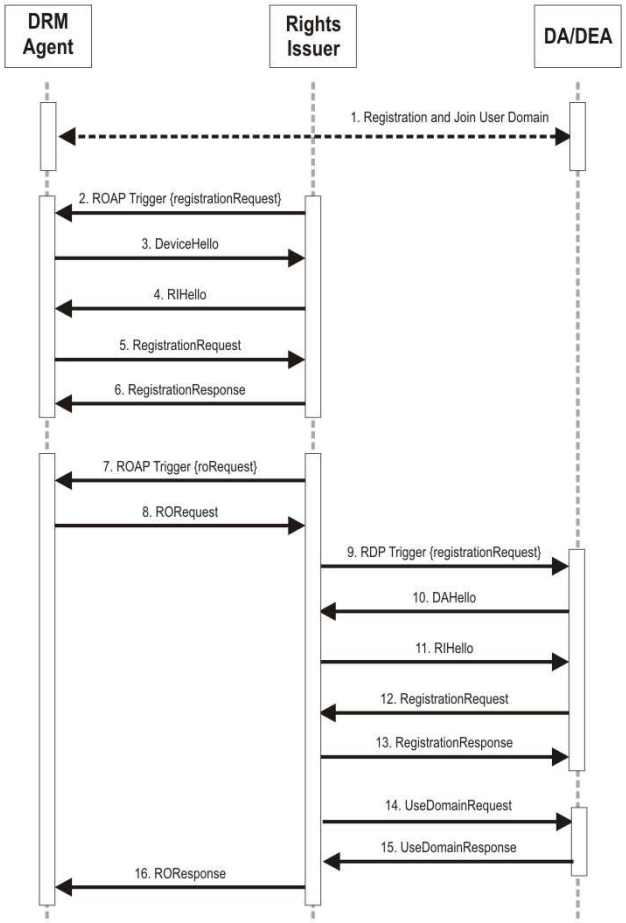

Figure 8: Purchase for a User Domain

Calls

1 The DRM Agent registers with the DA/DEA and joins the User Domain, as described in section 5.4.8.

2-6 The DRM Agent registers with the RI. The involved protocols are similar to Device-RI registration in OMA DRM 2.0. Part of the registration will be a mutual authentication. This protocol is executed when the DRM Agents first starts want to acquire content from a RI and may be repeated when the registration expires.

7-8 The DRM Agent is triggered to request a purchased RO, tied to the selected User Domain. Calls 7 and 8 are similar to the calls in OMA DRM 2.0, extended with the necessary information to request creation of an RO with permission for the User Domain.

9-13 The DA/DEA registers with the RI. The involved protocols are similar to Device-RI registration in OMA DRM 2.0. Part of the registration will be a mutual authentication. This protocol is executed when the RI first contact with the DA/DEA for the User Domain and may be repeated when the registration expires.

14-15 RI and DA/DEA exchange the information and key material that enable the RI to create the RO. The RI will use this information to check that it trusts the DA/DEA responsible for this User Domain and that it supports the associated Domain Policy.

16 The RI sends ROResponse message to the DRM Agent. It is similar to the calls in OMA DRM 2.0, extended with the necessary information to respond to the creation of an RO with permission for the User Domain.

Note: An existing 2.0 DRM Agent can also purchase Rights for a User Domain using a similar flow as described above, if the RI acts as a proxy for the DA (see calls 6-9 in section 5.4.9), and if the user can specify the User Domain (e.g. DomainID, DAID, DAURL, etc.) to the RI.

5.4.8 Management and usage of the User Domain

Figure 9 depicts the flow of events when DRM Agents joins a User Domain.

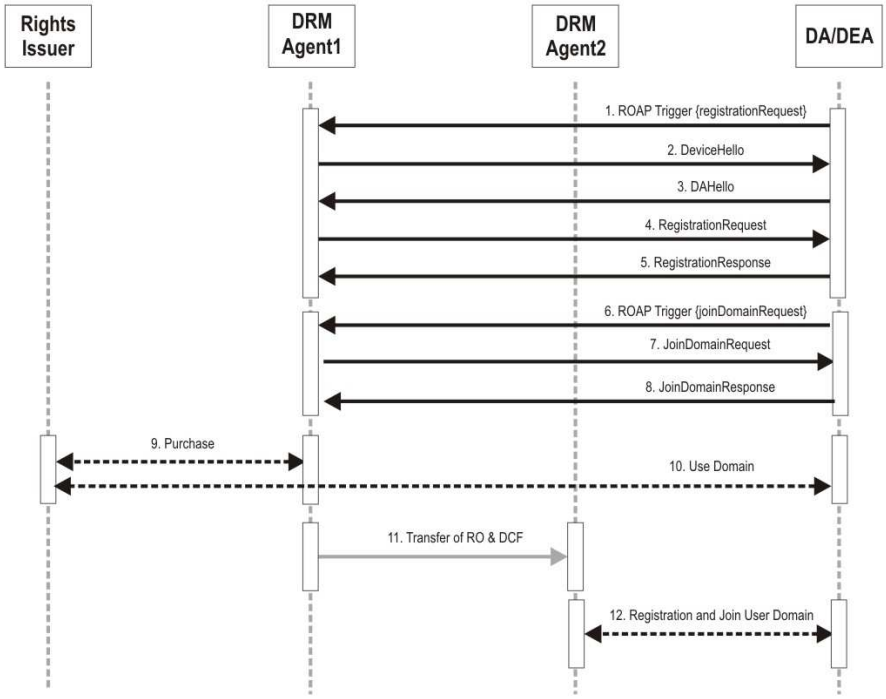

Figure 9: Management and usage of the User Domain

Calls

1-5 DRM Agent1 registers with the DA/DEA . The involved protocols are similar to Device-RI registration in OMA DRM 2.0. Part of the registration will be a mutual authentication. This protocol is executed when the DRM Agents first starts to acquire content for a User Domain managed by the DA/DEA and may be repeated when the registration expires.

6-8 DRM Agent1 is triggered and joins the User Domain. The protocols are very similar to the join domain protocols as specified in OMA DRM 2.0.

9-10 DRM Agent1 acquires a RO as described in section 5.4.7.

11 The RO and DCF is transported to DRM Agent2, as enabled by OMA DRM 2.0. This is outside of scope for OMA DRM.

12 DRM Agent2 registers and join the User Domain as per calls 1-8.

Figure 10 describes the flow of events when DRM Agent 2 is an Unconnected Device

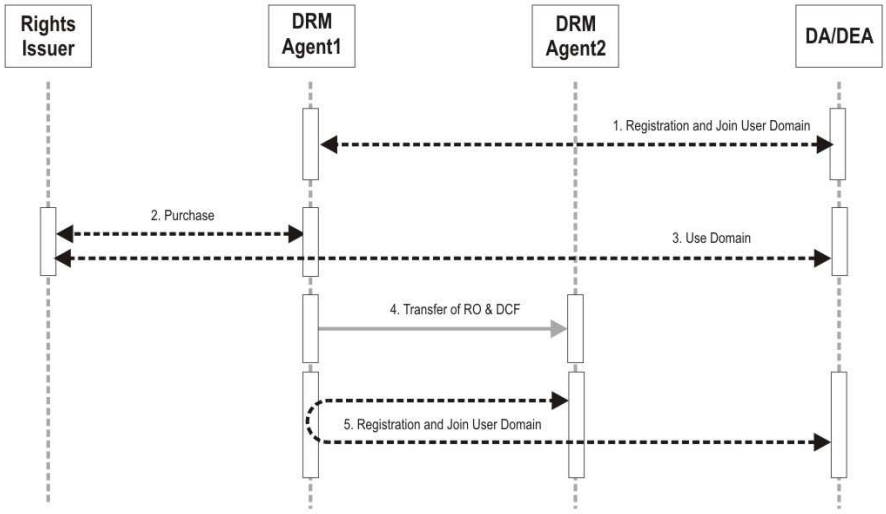

Figure 10: Unconnected Device Support in User Domain

Calls

1. DRM Agent1 registers with the DA/DEA and joins the User Domain as described call 1-8 in Figure 9.

2-3 DRM Agent1 acquires a RO as described in section 5.4.7.

4 The RO and DCF are transported to DRM Agent2, as described call 11 in Figure 9.

5 DRM Agent2 registers and joins the User Domain as per calls 1-8 in Figure 9. DRM Agent 1, Connected Device, can act as an intermediary to assist DRM Agent 2, Unconnected Device, to register and join the User Domain.

5.4.9 User Domain backward compatible usage

Figure 11 depicts the flow of events when DRM Agents acquires Content for a User Domain and transfers this content to a OMA DRM 2.0 conformant DRM Agent ("2.0 DRM Agent").

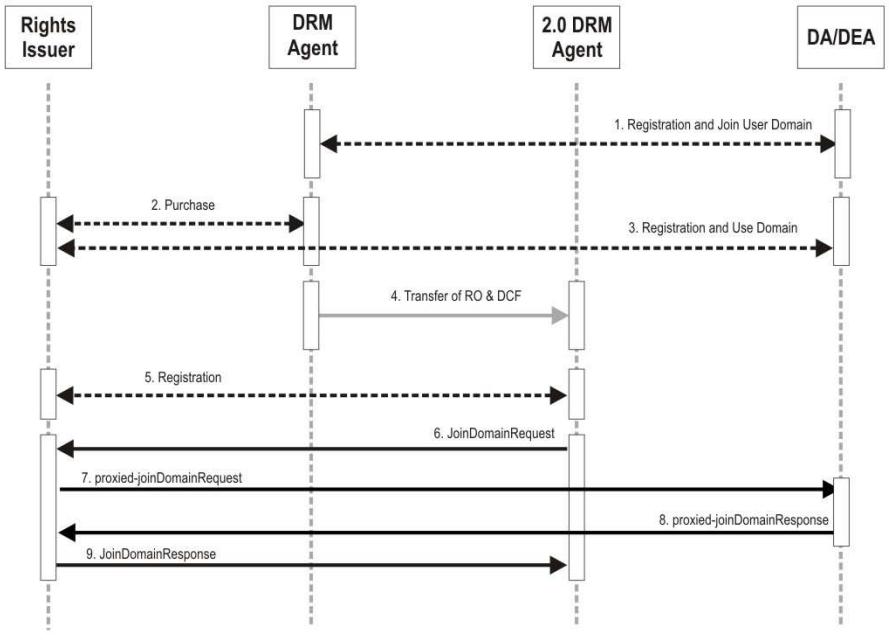

Figure 11: User Domain backward compatible usage

Calls

1 The SCE conformant DRM Agent registers with the DA/DEA and joins the User Domain, as described in section 5.4.8.

2-3 The SCE conformant DRM Agent acquires a RO as described in section 5.4.7. The involved protocols already include the registration phase between the DA/DEA and the RI as described in section 5.4.7.

4 The RO and DCF is transported to the OMA DRM 2.0 conformant DRM Agent, as enabled by OMA DRM 2.0. This is outside of scope for OMA DRM.

5-9 The OMA DRM 2.0 conformant DRM Agent is unable to contact a DA/DEA. Instead it uses the information contained in the RO to contact the RI (as specified in OMA DRM 2.0) to register and request to be joined to the domain. The RI acts as proxy for the DA/DEA and forwards the join domain call to the DA/DEA that manages the domain. These calls are executed the first time the 2.0 DRM Agent encounters Content provided by this RI and may be repeated e.g. after the registration or domain context expires. If the DA/DEA has not registered with the RI, DA-RI registration protocols precede the proxied-joinDomainRequest as described in section 5.4.7.

5.4.10 Mutual Authentication Between Two Devices

Before the transfer of Rights can take place directly between two Devices, they MUST mutually authenticate each other. Figure 12 depicts the flow of events that initiates the mutual authentication between two Devices. The mutual authentication will be used to Moving, Copying and Ad Hoc Sharing. These flows occur over the A2AP-1 interface.

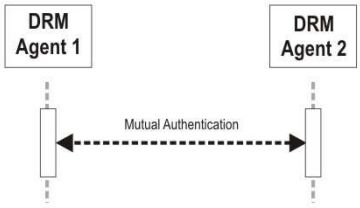

Figure 12: Mutual Authentication between two Devices

Through the mutual authentication process, DRM Agent 1 and 2 may check revocation status of opposite DRM Agent. It is expected that several keys will be established to be used for confidentiality and integrity in later message exchanges. DRM Agent 1 and 2 may also check whether they belong to the same Domain or User Domain.

5.4.11 Obtain Rights for Sharing by RO Upgrade

Figure 13 depicts how Device1 achieves to Share with Device2 the Rights that do not explicitly permit Sharing.

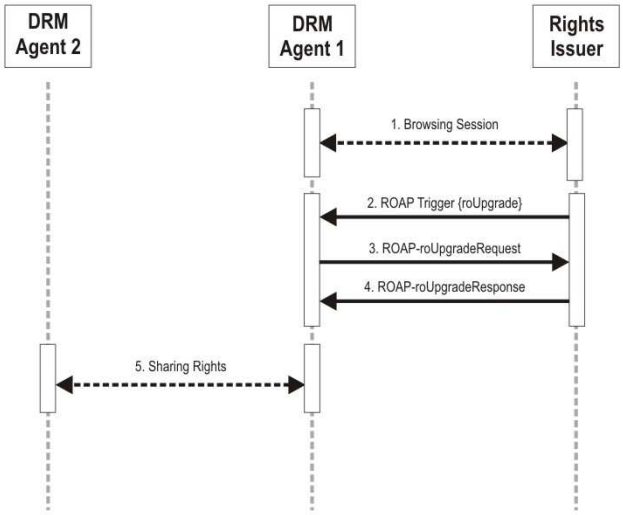

Figure 13: Obtain Rights for Sharing by RO Upgrade

The steps:

1 The user of DRM Agent 1 selects some rights (probably associated with a specific content) that the User wants to share, realizing that the rights are not shareable the User chooses to try to upgrade the rights. This launches a browsing session which allows the user to begin the RO upgrade process.

2-3 DRM Agent1 is triggered to supply to RI enough information for upgrading the User's existing RO, such information may include User's existing RO (and corresponding State Information if it is stateful) and the information about the User's desired permissions/constraints such as identity of the Device with which the User wants to Share Rights. Before sending roUpgrade Request message, DRM Agent1 disables the existing RO.

4 The Rights Issuer send roUpgrade Response message to DRM Agent1. The roUpgrade Response message contains a new RO, which consists of both the permissions/constraints in the existing RO and the User's desired permissions/constraints (which explicitly permit Sharing). DRM Agent1 installs the newly got RO. DRM Agent 1 removes the disabled existing RO and installs the new RO. DRM Agent 1 may enable the disabled existing RO if it does not receive the new RO successfully.

5 DRM Agent1 can now (or some time after this) Share (e.g. Copy, Move, Lend) the existing Rights with DRM Agent2, under the control of the newly got permissions/constraints.

5.4.12 Move Rights via Rights Issuer

Figure 14 depicts the flow of events in the case of Moving Rights via a Rights Issuer. These flows occur over the ROAP-1.1 interface. The steps below correspond to the messages from top to bottom. DRM Agent 1 represents the DRM Agent that sends the Rights. DRM Agent 2 represents the DRM Agent that receives the Rights. The Move has to occur via the Rights Issuer that issued the original Rights.

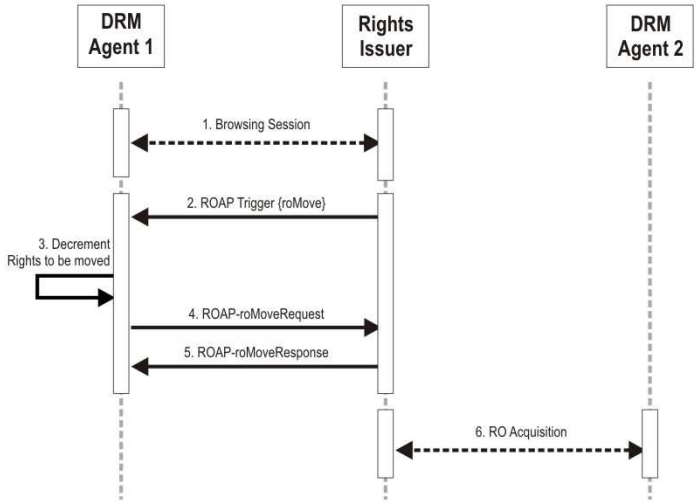

Figure 14: Move Rights via Rights Issuer

One or more Rights Objects were issued to DRM Agent 1 by a Rights Issuer. The User may Move all or a part of the remaining Rights which are in his/her possession.

1. The User of DRM Agent 1 browses the Rights Issuer's portal to inform the Rights Issuer that he/she wants to move Rights in his/her possession to another DRM Agent. This step is out of scope.
2. The Rights Issuer sends ROAP trigger to DRM Agent 1, indicating DRM Agent 1 to start transferring Rights to the Rights Issuer.
3. DRM Agent 1 decrements the Rights to be transferred to the Rights Issuer.
4. DRM Agent 1 sends the ROAP-roMoveRequest to the Rights Issuer. This message contains at least one or more Rights Objects and the information indicating which part of it is available for DRM Agent 2. The Rights Object includes permissions and constraints which are same as the Rights Object initially issued from the Rights Issuer.
5. The Rights Issuer processes the ROAP-roMoveRequest and sends ROAP-roMoveResponse to DRM Agent 1. The processing includes verification of the received Rights Object (and State Information if any) and storing the received Rights Object (and State Information if any).
6. The Rights Issuer conducts existing 1-pass or 2-pass RO Acquisition Protocol to issue the Rights received from Device 1. If 2-pass RO Acquisition Protocol, the Rights Issuer sends a ROAP Trigger to DRM Agent 2, indicating DRM Agent 2 to download the Rights sent by user of DRM Agent 1. Upon receiving ROAP Trigger, if DRM Agent 2 was not registered to the Rights Issuer, DRM Agent 2 registers to the Rights Issuer.

Identification of DRM Agent 2 will occur at Step 1.

5.4.13 Moving Rights Directly Between Devices

Figure 15 depicts the flow of events in the following cases:

- Moving Device bound Rights directly between two Devices
- Moving User Domain bound Rights directly between Devices in the same User Domain.

These flows occur over the A2AP-1 interface. The steps below correspond to the messages from top to bottom. DRM Agent 1 represents the DRM Agent that sends the Rights. DRM Agent 2 represents the DRM Agent that receives the Rights.

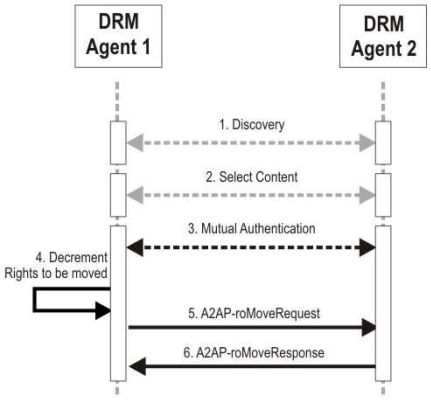

Figure 15: Moving Rights Directly Between Devices

DRM Agent 1 has a Rights Object that is either bound to DRM Agent 1 or a User Domain that DRM Agent 1 belongs to.

1. DRM Agent 1 discovers DRM Agent 2 using a discovery mechanism, e.g. UPnP. The discovery process may include informing of the capability to handle a Move operation. This step is out of scope of OMA.
2. The Users select the Content to move. This step is outside the scope of OMA DRM.
3. DRM Agent 1 and DRM Agent 2 complete the mutual authentication as outlined above. As a result of successful mutual authentication, a session between DRM Agent 1 and DRM Agent 2 is established.
4. DRM Agent 1 decrements the Rights to be moved to DRM Agent 2.
5. DRM Agent 1 transfers the Rights and the information indicating which part of it is available for DRM Agent 2 to DRM Agent 2 in a A2AP-moveRequest.
6. DRM Agent 2 processes the A2AP-moveRequest and then sends A2AP-moveResponse to DRM Agent 1.

5.4.14 Ad Hoc Sharing Directly Between Devices

Figure 16 depicts the flow of events in the case of Ad Hoc Sharing directly between two Devices. These flows occur over the A2AP-1 interface. The steps below correspond to the messages from top to bottom. DRM Agent 1 represents the DRM Agent that sends the Rights. DRM Agent 2 represents the DRM Agent that receives the Rights.

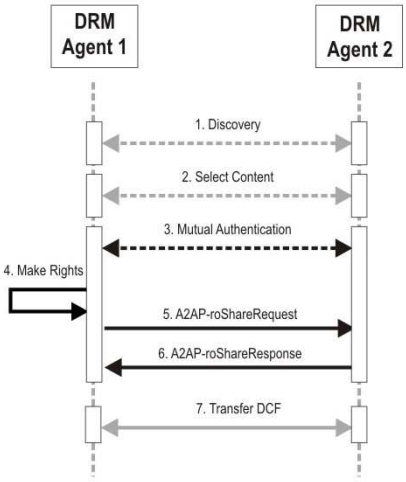

Figure 16: Ad Hoc Sharing Between Two Devices

1. DRM Agent 1 discovers DRM Agent 2 using a discovery mechanism, e.g. UPnP. The discovery process may include informing of the capability to handle Ad Hoc Sharing. This step is out of scope of OMA DRM.
2. The Users select the Content to ad hoc share. This step is outside the scope of OMA DRM.
3. DRM Agent 1 and DRM Agent 2 complete the mutual authentication as outlined above. As a result of successful mutual authentication, a session between DRM Agent 1 and DRM Agent 2 is established.
4. DRM Agent 1 then makes the Rights for DRM Agent 2 based on the current Rights, the permissions set by the Rights Issuer for Ad Hoc Sharing and the current state information (if any). It is expected that the Rights will include at least a <datetime> constraint. If the current Rights are not explicitly permitted to be shared, DRM Agent 1 MUST obtain Rights for sharing by RO upgrade from RI as described in section 5.4.11.
5. DRM Agent 1 sends a A2AP-roShareRequest, which contains the Rights for DRM Agent 2.
6. DRM Agent 2 processes the A2AP-roShareRequest and then sends back an A2AP-roShareResponse.
7. DRM Agent 1 transfers the DCF (corresponding to the shared Rights) to DRM Agent 2. This step is out of scope of OMA DRM. Note that step 7 could take place during step 2.

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
OMA-AD-SCE-V1_0-20110705-A	05 Jul 2011	Status changed to Approved by TP: OMA-TP-2011-0233-INP_SCE_V1_0_ERP_for_Final_Approval