Secure Content Exchange Requirements

Approved Version 1.0 – 05 Jul 2011

Open Mobile Alliance

OMA-RD-SCE-V1_0-20110705-A

Contents

Tables

1. Scope (Informative)

The scope of this document is to define use cases and normative requirements for enhancements to the OMA Digital Rights Management (DRM) specifications to enable the secure exchange of DRM content among multiple devices. These enhancements include the following:

- New capabilities that will enable flexible sharing of purchased content in ways that were not possible using Domains as defined in OMA DRM V2.0. These new features include device-based creation and management of content sharing groups; copying and moving of rights between OMA DRM devices; and sharing between devices in ad hoc groups.
- 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.
- Enhancements to the OMA Digital Rights Management (DRM) specifications to enable consumption of DRM Content contained in an MPEG-2 Transport Stream across a wide variety of user Devices.

2. References

2.1 Normative References

[DRMREQ-v2] OMA DRM Requirements, Open Mobile Alliance™, included in OMA-RD-DRM-V2_1, http://www.openmobilealliance.org/

[MPEG-2 TS] ISO/IEC 13818-1 | ITU-T H.222.0

2.2 Informative References

[DRM-v2] OMA DRM V2.1 Enabler, Open Mobile Alliance™, OMA-RD-DRM-V2_1, 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

Definitions that are copied from [DRM-v2] are marked with (DRM V2.0). Definitions with the same name as in [DRM-v2] but different text are intended to overwrite the definitions from [DRM-v2]. Note, in particular, that some terms may also occur in [DRM-v2] but have new definitions (e.g. Copy).

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).
Backup/Remote Storage	Transferring Rights Objects and Content Objects to another location with the intention of transferring them back to the original Device (DRM V2.0).
Broadcast Program	A logical portion of a Broadcast Service with a distinct start and end time. In the case where the Broadcast Program is not free-to-air, it can be offered individually for purchase, such as “Pay-Per-View”, or as part of a parent service (e.g. subscription service). A Broadcast Program may for example represent a movie, news show or soccer game.
Broadcast Service	A digital broadcast delivered in an MPEG-2 transport stream consisting of a concatenation of Broadcast Programs, as defined in an MPEG-2 Program Map Table (PMT).
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 set of DRM 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 DRM 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 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).
Execute	To execute a software programme (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).
Interaction Channel	A bi-directional channel used to engage in communication protocols (such as DRM v2 ROAP) with other entities. The Interactive Channel can for example be used to request a Rights Object from a Rights Issuer.
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.
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.
Print	To create a fixed and directly perceivable rendition of a resource.
Proximity-Limited Domain	An Ad Hoc Domain in which all member Devices must be in proximity to the device on which the Domain Enforcement Agent resides.
Proximity-Limited Sharing	Ad Hoc Sharing that is possible only when the source and recipient Devices are in proximity.
Render Agent	The entity in a Render Client that manages the secure rendering of Media Objects on the Render Client.
Render Client	The entity (hardware, software or combination thereof) within a user equipment that implements a Render Agent. The Render Client is used to transiently render DRM Content.
Restore	Transferring the Protected Content and/or Rights Objects from an external location back to the Device from which they were backed up (DRM V2.0).
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.
Set-top Box	A device capable of receiving digital broadcast services contained in an MPEG-2 transport stream that may be delivered over cable, satellite, terrestrial, IP or any other medium. To access the digital broadcast services, a Set-top Box (STB) may or may not use a Conditional Access System. A STB may or may not be OMA DRM compliant
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).
Token Agent	The entity in a User Domain Token that manages the secure mutual authentication between User Domain Token and a Device in case of Token based access
Token based access	The act of accessing Content with Rights for a User Domain on a Device that is not a member of that User Domain after successful mutual authentication between the Token Agent of a User Domain Token that is associated with that User Domain and the DRM Agent in the non-member Device. The Domain Authority can specify in the Domain Policy the conditions under which the Device is allowed to access the Content.
User	The human user of a Device. The User does not necessarily own the Device (DRM V2.0).
User Domain	A set of DRM v2.x and/or SCE DRM Agents that can consume User Domain Rights Objects.
User Domain Token	The entity (hardware, software or combination thereof; e.g. a SIM) within a user equipment that implements a Token Agent. A User Domain Token can be associated with one or more User Domains, and enables Token based access to the Content for each User Domain with which it is associated.
User Domain Rights Object	A Rights Object that is targeted to a specific User Domain. Besides requiring membership in the User Domain, consumption of the Rights Objects may require being targeted to an SCE DRM Agent.

3.3 Abbreviations

CAS	Conditional Access System
CI	Content Issuer
DEA	Domain Enforcement Agent
DCF	DRM Content Format
DRM	Digital Rights Management
DVR	Digital Video Recorder
LRM	Local Rights Manager
MDCF	MPEG-2 Transport Stream DRM Content Format

MP3	MPEG-1 Audio Layer 3 (public format for digital music)
OMA	Open Mobile Alliance
PDA	Personal Digital Assistant
RI	Rights Issuer
RO	Rights Object
SCE	Secure Content Exchange
SIM	Subscriber Identity Module
STB	Set-top Box
USB	Universal Serial Bus
UID	User Token
WAN	Wide Area Network
WiFi	also Wi-fi, Wifi, or wifi from _Wi_reless _Fi_delity

4. Introduction (Informative)

The goal of the Secure Content Exchange (SCE) Enabler is to extend OMA DRM v2.0 to enable seamless sharing of purchased content between multiple devices, including all the devices owned by a subscriber (phone, PC, home electronics system, car audio system, etc) and the ad hoc sharing of content with any device the user encounters in unplanned or impromptu situations. Examples of when ad hoc sharing may be applicable include users who want to render their content on a television set at a friend's house or in a hotel room while the user is travelling, or a user who wants to borrow DRM content for a period of time. The Ad Hoc Sharing part of the SCE Enabler enforces temporal and proximity based restrictions that are defined by the RI/DA e.g. content can only be shared with a Device that is in close proximity to the subscriber's Device. Because there is no single DRM system deployed across all these different devices, the SCE Enabler also enhances the interoperability between OMA and non-OMA DRM systems by defining an Import function for OMA DRM. Yet another goal of the Secure Content Exchange Enabler is to extend OMA DRM with the capability of using an MPEG-2 transport stream as a container of DRM Content.

Hence, the SCE Enabler extends DRM v2.0 with the following:

- Flexible rights transfer and DRM domain management, which involves enhancements to OMA DRM v2.0 for flexible sharing of content between OMA DRM conformant devices; and
- DRM interoperability, which addresses content exchange between OMA DRM and non-OMA DRM conformant devices.

These two extensions are complementary, since they address different aspects of secure content exchange, and it is expected that some of the technical solutions developed by the SCE work will be used in both extensions.

The enhancements specified by the SCE Enabler provide the following benefits to subscribers, Content Providers and operators:

- Subscribers benefit from increased flexibility to share and render their content in ways that were previously not possible. They perceive a level of convenience in their digital media service which rivals the user experience offered by physical media such as CDs and DVDs, which can be played on any device available.
- Content providers benefit from an increase in content purchases, while enjoying the protection against content piracy that DRM provides.
- The added appeal of flexible sharing to subscribers makes the operator's mobile digital media service competitive with wireline-based services and physical media, resulting in an increase in the number of service subscribers and content purchases (and hence an increase in operator revenue).

4.1 Flexible Rights Transfer and DRM Domain Management

This extension eliminates restrictions of the current OMA DRM v2.0 to enable more flexible sharing of content and proposes solutions for flexible rights transfer. To understand the current restrictions, it may be helpful to review the current status of OMA DRM.

In OMA DRM v1.0, content could only be purchased for use on a single device. OMA DRM v2.0 relaxes this restriction by introducing domains to enable the purchase of content for use on multiple devices. Each device to be included in a domain registers itself with a Rights Issuer, executes a domain join protocol, and receives a domain key in return. When a subscriber purchases content for a particular domain, they receive a domain rights object that can be used together with the domain key by any device in the domain to render the content.

OMA DRM v2.0 domains have a number of limitations that prevent the kinds of seamless sharing described above:

- Domains must be created at each Rights Issuer from which a subscriber purchases domain content. In cases where subscribers want to buy content from multiple Rights Issuers, they must newly create the domains at each of the Rights Issuers, which requires a great deal of effort.

- Because domains are maintained at Rights Issuers in the network, each device joined to a domain must have wide-area network connectivity to execute the domain join protocol (or have access to a WAN-connected device that can be used as a proxy for communication with the Rights Issuer). This makes it difficult to include unconnected devices in a domain.
- Ad hoc sharing scenarios are typically spontaneous, and the identities of the devices involved are not known in advance. This makes it cumbersome to have each device execute the domain join protocol with a Rights Issuer before sharing can take place.

Thus, this extension eliminates these restrictions and enables more flexible sharing of content by providing the following capabilities:

- Allowing devices to create groups of devices for sharing rights, add members to these groups, and provide rights to group members without the involvement of a Rights Issuer in the network.
- Providing a mechanism for the definition of content sharing policies, so that content providers can specify the extent to which a device is allowed to share a content item (e.g. maximum size of a sharing group, permitted changes to group membership, etc.)
- Enabling users to share content on an ad hoc basis in impromptu situations, subject to certain constraints.
- Allowing users to copy and move rights between devices (e.g., a user purchases 10 plays of a song and gives five of the plays to a friend)

4.1.1 Overview of SCE Content Sharing Features

This section provides a brief overview of the new sharing features that SCE introduces into OMA DRM. As shown in Table 1, these new features (shown in bold text) can be categorized according to their intended uses. *Planned sharing* involves the sharing of rights among a set of devices whose identities are known in advance (e.g. all the devices owned by members of the same family), while *unplanned sharing* refers to situations in which the devices receiving shared rights can be arbitrary OMA DRM-compliant devices. Unplanned sharing can be further categorized based on whether a device shares its own rights or has a separate set of sharing permissions and constraints; in the latter case, sharing can be between a pair of devices or among a group of devices. In addition, SCE adds several sharing support functions that are described at the end of this section.

<table>
<tr><th>Planned Sharing</th><th colspan="3">Unplanned Sharing</th></tr>
<tr><td rowspan="3">User Domain

Domain Split and Join

User Domain Token</td><td></td><td>Device-to-Device Sharing</td><td>Group Sharing</td></tr>
<tr><td>Device Shares Own Rights</td><td>Move, Lending</td><td>N/A</td></tr>
<tr><td>Device Shares Separate Set of Rights</td><td>Ad Hoc Sharing</td><td>Ad Hoc Domain</td></tr>
</table>

Table 1: SCE Sharing Features

SCE provides an enhanced version of OMA DRM V2.0 Domains known as *User Domains* to enable planned sharing of rights among Devices. The main difference between a User Domain and an OMA DRM V2.0 domain is that the User can choose to set up and manage only a single User Domain and subsequently acquire Rights for this User Domain from any Rights Issuer. This means that a User does not have to manage a Domain for each Rights Issuer they acquire Content from.

As with OMA DRM 2.0 Domains, all Devices that belong to the User Domain can access Content with Rights for the User Domain.

SCE introduces the following entities to enable this:

- The *Domain Policy* determines the allowed changes to the User Domain, including its maximum number of Device members and the number of changes in a given time period.
- The *Domain Authority* is the entity that sets the Domain Policy. A Domain Authority can define Domain Policies that are honoured by multiple Rights Issuers. When the User establishes a User Domain that adheres to a Domain Policy, they can then purchase content for that User Domain from these Rights Issuers, without having to create the User Domain at each Rights Issuer, as is required in OMA DRM V2.0.
- The *Domain Enforcement Agent (DEA)* is the entity which ensures that any changes to the User Domain adhere to the Domain Policy. The DEA can reside either in the network or on a user's device. When a DEA is present on the User's Device, the User can perform User Domain management operations locally on the Device, without the need for interaction with a network entity such as a Rights Issuer.
- The *User Domain Token (UDT)* is the entity that allows non-member Devices to render Content bound to the User Domain associated with the UDT.

The user experience that is targeted with this technology is that a User can set up a User Domain, add their Devices to this User Domain, and then purchase Content for the User Domain from any provider. The User is then assured that the Content they have acquired will be accessible on all of their Devices. The SCE enabler extends this experience further by allowing a User to select one or more *User Domain Token(s)* for "his/her" User Domain. This enables a User to access Content bound to the User Domain on any non-member Device after the non-member Device has mutually authenticated the User Domain Token. The User can regard the User Domain Token as the "key" to "his/her" content, "unlocking" it on any Device when needed. The Device can then be regarded as being a "virtual member" of the User Domain(s) associated with the User Domain Token.

Although the SCE enabler provides for this straightforward user experience, the legal aspects and the technical implementation is a little less straightforward. Legally the User will not own the Content, instead Users purchase Rights to access the Content. Also, technically there is no way to prove that all Devices that are members of the User Domain are owned by the same User or that the User Token is actually handled by the User that purchased the Rights. However the Domain Policy defines limits and conditions for the Devices that are allowed to access Content with Rights for the User Domain. These limits and conditions should be chosen such that intended experience as described above is enabled, whereas unintended usage is made difficult. The SCE enabler will enable such conditions and limits but will not specify their value or usage. This is left up to the Domain Authority and/or Trust Authority.

In addition, SCE will allow an existing User Domain to be split into multiple domains, and will also allow multiple User Domains to be joined into a single User Domain, with the rights purchased for each User Domain modified accordingly.

As shown in Table 1, unplanned sharing in SCE is categorized according to whether a source device shares its own rights with recipient devices, or whether the device has a set of rights governing unplanned sharing in addition to its own rights. SCE provides two features, Move and Lending, that allow a device to share its own rights. The Move feature enables a device to share some or all of its rights with a recipient device; for example, a device that has 7 plays of a song remaining can give one of these plays to the recipient and keep the remaining 6 for itself. Lending allows a source device to assign its rights temporarily to a recipient device; the recipient can then consume the rights, which are not usable on the source device until the lending period expires or the recipient returns them.

Move and Lending are somewhat limited in the flexibility of sharing that they allow. For example, it is difficult to use the Move operation when the rights of the source Device are not stateful: if the source Device has unlimited rights, then it cannot share a part of these rights via a Move (since "parts" of unlimited rights can also be unlimited). Ad Hoc Sharing is another form of sharing that is useful in unplanned situations, and which allows a greater variety of sharing scenarios. The rights of a source device in Ad Hoc Sharing include a set of permissions and constraints that determines the sharing that is allowed with recipient devices. These sharing rights are separate in the sense that an instance of Ad Hoc Sharing does not diminish the source device's own rights to render the associated DRM content. Ad Hoc Sharing makes it possible for a rights issuer to specify constraints on the ability of a source device to engage in Ad Hoc Sharing (for example, whether proximity between the source and recipient devices is required for sharing, and limits on the number of times the rights to a particular content

item can be shared), and constraints on the rights that can be granted to a recipient device (for example, the recipient might receive only a single play of a song, and the rights could expire with an hour or two of when they are received).

Ad Hoc Sharing can occur either on a device-to-device basis or among a group of devices. In the latter case, SCE provides the notion of an Ad Hoc Domain to make it easier for a group of devices to share content. Once a device joins an Ad Hoc Domain, it can share rights with any other member of the Domain via Ad Hoc Sharing, without requiring a separate device-to-device interaction for each source device and set of shared rights. Ad Hoc Domains are useful in situations where a group of devices are sharing rights for multiple content items, for example a group of friends at a party that are browsing the content available for sharing on each others' devices. As with User Domains, Ad Hoc Domains are governed by a Domain Policy that is enforced by a DEA.

In addition to the above sharing features, SCE will define the following supporting functions that help to enable seamless sharing among devices:

- Allowing a user to request additional sharing rights from the rights issuer after the initial purchase of a set of rights (this is especially useful a DRM V2.0 user upgrades to SCE and wants to SCE features to share rights purchased under DRM V2.0)
- Enabling a recipient device to browse the rights available for sharing on a source device, and to acquire the associated content file from a content server. This is useful in cases where the source device stores a number of rights objects but does not store the corresponding DRM content files for each one. If the source device's sharing rights allow, the recipient device can also request the DRM content in a format suitable for display on that device.
- Allowing devices with limited capabilities (Render Clients) to render DRM content (even if these devices are not able to process the permissions and constraints in a rights object, they can acquire a content decryption key from a Device by other means and render a DRM content item).

4.2 DRM Interoperability

OMA DRM v2.0 already defines an Export function but has no corresponding Import function. This extension defines an Import function for OMA DRM. As background, it may be helpful to review the current definition of Export in OMA DRM v2.0. After downloading OMA DRM content, a User may wish to render that content on another Device that has a different DRM protection format. Export (from OMA DRM) is an operation in which the DRM content and corresponding Rights Object are transferred to a DRM system or content protection scheme other than the OMA DRM system. Import (into OMA DRM) is the corresponding function, where the DRM content and its corresponding Rights Object (or other form of content rights) are transferred from a DRM system or content protection scheme other than the OMA DRM system. In both Export and Import, the content rights should be transformed securely and consistently and the content should be transferred securely.

Without specifying Import, devices that have different DRM protection formats must implement the entire functions and protocols of an OMA DRM Rights Issuer, and must format content in OMA DRM format, to be able to export to devices that have OMA DRM protection. This requirement may be excessive on the exporting devices and may prohibit inter-operability between OMA DRM and other DRM protection schemes. As an example, the source of content may be a Digital Video Recorder (DVR) with content obtained from cable or satellite provider and locally protected by a non-OMA DRM system. The (non-protected form of this) content may be transcoded such that it can be consumed by a mobile handset. The content protection must also be translated from the non-OMA DRM system to OMA DRM based on the assumption that the handsets support only the OMA DRM system. The transcoding and translation will be performed by a Local Rights Manager (LRM) that receives the original content from the DVR and distributes it to one or more devices within the user's "personal domain" or home network.

4.3 MPEG-2 Transport Stream as a Container for DRM Content

In OMA DRM v2 the use of DCF and PDCF is defined as container for DRM Content. The SCE Enabler defines that also an MPEG-2 Transport Stream can be used as a container of DRM Content. The objective is to allow consumption of received digital broadcast content as DRM Content by OMA DRM Devices, presuming that a Rights Issuer provides an associated Rights Object for such consumption.

5. Use Cases (Informative)

5.1 Use Case 1: Moving Rights

5.1.1 Short Description

This use case describes Moving of DRM Content and its associated Rights from a sender Device to a receiver Device. After Moving the Rights, the Moved Rights are no longer usable in the sender Device.

John enjoys MP3 Content on his mobile phone. John would like to give his friend Jane, who has a portable MP3 player, the latest hot MP3 single as her birthday gift. Using his mobile phone, John downloads the latest MP3 single from his Content Provider. When he sees Jane on her birthday, he transfers the latest hit MP3 Content and its associated Rights from his mobile phone to her portable MP3 player.

At a later point of time, John visits his friend Mike who is interested in viewing a video purchased by John. As John has purchased Rights to view the video for 10 times, John transfers 1 play count of his Rights to Mike's PC so that Mike can view to the video only once. Hence Mike can also listen to the music purchased by John on his MP3 player for 9 times.

5.1.2 Actors

John, Jane and Mike	Users who own Devices and are involved in Moving Content.
Mobile Phone	A Device that belongs to John.
Portable MP3 Player	A Device that belongs to Jane.
PC	A Device that belongs to Mike.
Content Provider	The Rights Issuer that John uses.

5.1.3 Actor Specific Issues

John wants to transfer DRM Content and associated Rights to a friend.

The sender Device and receiver Device may belong to the same User or to different Users.

John may transfer Device Rights or User Domain Rights.

Content Provider wants to restrict unauthorized transfer of the Rights.

5.1.4 Actor Specific Benefits

John is able to buy Content. Some time later he is able to gift the Content to his friends or family.

Jane and Mike can be given Content as a gift without paying for it.

Content Provider benefits from offering a compelling Content download service that attracts users but prevents unauthorized transfer of Content.

5.1.5 Pre-conditions

None.

5.1.6 Post-Conditions

The Receiver Device is able to use the transferred Rights.

After a successful transfer of the Rights to the receiver Device, the sender Device will no longer be able to use the amount of Rights which were transferred. If the transfer is not successful, the receiver Device will not be able to consume the Content.

The receiver Device may move DRM Content and associated Rights further to another Device if the received Rights allow it.

5.1.7 Normal Flow

The following sections explain how Whole and Partial Moves can be done directly between Devices.

5.1.7.1 Whole Move

1. John uses his mobile phone and browses for the latest hit MP3 song from his Content Provider.
2. John indicates that he wants to gift the song.
3. The Rights that the Content Provider creates for the MP3 song include the Move permission.
4. John downloads the latest hit MP3 song and associated Rights.
5. John meets Jane and tells her he is giving her the latest hit MP3.
6. John's mobile phone and Jane's portable MP3 player connect and authenticate each other.
7. John's mobile phone Moves the latest hit MP3 song and its Rights to Jane's portable MP3 player.
8. Jane can now play the latest hit MP3 song on her portable MP3 player but John cannot play it on his mobile phone.

5.1.7.2 Partial Move

1. John uses his mobile phone and browses some videos available from his Content Provider.
2. John selects the video that he wants to buy, indicating that he only wants to view it 10 times but that he might want to share some of the views.
3. The Rights that the Content Provider creates for the video have a render constraint of 10 times and a Move permission.
4. John downloads the video and associated Rights.
5. John views the video once.
6. John visits Mike and tells him about the cool video he has. Mike wants to see the video on his PC.
7. John's mobile phone and Mike's PC connect and authenticate each other.
8. John's mobile phone Moves the video and the Rights for one play of the video to Mike's PC.
9. Mike can now view the video once on his PC. John can now only view it 8 more times.

5.1.8 Alternative Flow

The following sections explain how Whole and Partial Moves can be done via the Content Provider (or Rights Issuer).

5.1.8.1 Whole Move

An alternative to steps 6 and 7 in the Whole Move above is as follows:

6. John's mobile phone connects to John's Content Provider and Moves the Rights to the latest hit MP3 song to the Content Provider.
7. Mary's portable MP3 player connects and identifies itself to John's Content Provider, and downloads the latest hit MP3 song and Rights that John moved to the Content Provider.

5.1.8.2 Partial Move

An alternative to steps 7 and 8 in the Partial Move above is as follows:

7. John's mobile phone connects to John's Content Provider and Moves one play from the Rights to the video to the Content Provider.

8. Mike's PC connects and identifies itself to John's Content Provider, and downloads the video and Rights that John moved to the Content Provider.

5.2 Use Case 2: Import Authorization and Revocation

5.2.1 Short Description

Jacob gets service from a local cable TV provider. The cable TV provider provides content that is protected by a non-OMA DRM system. Jacob informs his cable TV provider that he has one or more Devices from which he wishes to access the content provided by the provider. To access the content, the cable TV provider requires that the Devices obtain authorization from the provider. The cable TV provider explicitly authorizes the ability to make its content available to these Devices via OMA DRM Import.

The non-OMA DRM protected content from the cable TV provider, which has been downloaded to Jacob's set-top box (STB), can now be made available to his authorized Devices. Jacob connects one of his OMA DRM devices to the STB via USB and downloads the Imported-Content on the Device. Jacob can now render the Imported-Content on the Device while adhering to the licensing terms of the original content. Also, Jacob is able to directly share the Imported-Content with his other authorized Devices.

After some time, Jacob loses one of his Devices. Via the STB, Jacob is able to revoke the lost Device's authorization to access Imported-Content on the STB.

5.2.2 Actors

Cable TV Provider	An entity that provides non-OMA DRM content to its subscribers.
STB	A set-top box provided by the Cable TV Provider that renders the non-OMA DRM content received from the Provider. It can also deliver Import-Content to Devices.
Jacob	A User that owns several Devices and receives service from the Cable TV Provider.
Mobile Phone	A Device that belongs to Jacob.
Portable Video Player	A Device that belongs to Jacob.

5.2.3 Actor Specific Issues

Jacob, via the STB, can browse for Imported-Content that is available to be downloaded.

The STB may implement the LRM functions, but the LRM may also be physically separate from the ST.

5.2.4 Actor Specific Benefits

Jacob can use Imported-Content on his authorized Devices.

Upon losing a Device, Jacob is able to prevent the lost Device from further access to new Imported-Content from the STB.

5.2.5 Pre-conditions

Jacob has an STB and gets service from a cable TV provider. The STB has received and stored non-OMA DRM protected content.

Jacob's STB and Devices all support a means of communicating with each other (e.g., USB, WiFi and/or Bluetooth).

5.2.6 Post-conditions

Jacob's Devices are authorized by the Cable TV Provider to access Imported-Content.

Imported-Content is available for download on the Jacob's STB.

Lost Devices can no longer access new Imported-Content stored in the STB.

5.2.7 Normal Flow

5.2.7.1 Authorization

For each Device that Jacob wants to render Imported-Content, he does the following (just once):

1. Connects the Device to the Cable TV Provider
2. Gets authorization from the Cable TV Provider

5.2.7.2 Download

When Jacob wants to render Imported-Content on one of his authorized Devices, he does the following:

1. Jacob saves the non-OMA DRM protected content that he wants to his STB.
2. Jacob, via the STB, browses for content he wants to render on one of his Devices.
3. Jacob connects his Device to the STB via some communications link such as USB or Bluetooth.
4. Jacob downloads the selected Imported-Content to his Device.
5. Jacob renders the Imported-Content on his Device.
6. Jacob is able to directly share the Imported-Content with his other authorized Devices.

5.2.7.3 Revocation

1. Jacob loses one of his authorized Devices.
2. Via the STB, Jacob selects the lost Device and revokes it.

5.2.8 Alternative flow

Alternative 1:

Jacob may have created a User Domain that includes his Devices. The flow becomes as follows:

1. Jacob gets authorization for his User Domain from the Cable TV Provider.
2. Jacob downloads OMA-conformant video clip from STB to his Mobile Phone.
3. Jacob is able to view the video clip on the Mobile Phone.
4. Jacob is able to share directly the video clip with his Portable Video Player.

Alternative 2:

The flow in this alternative assumes that the LRM functions are implemented to be physically separate from the STB:

1. A video protected by non-OMA DRM is downloaded from Upstream Operator into STB.
2. Jacob browses the STB and decides to see video clip on his Mobile Phone.
3. Jacob makes request to Cable TV Provider for authorization to see video on his Devices.
4. Jacob is informed of the Devices' authorization to access non-OMA DRM video.
5. Jacob downloads OMA-conformant video clip from LRM to Mobile Phone.
6. Jacob is able to view the video clip on his Mobile Phone.
7. Jacob is able to share directly the video clip with other devices in the Jacob's group of authorized devices.

5.3 Use Case 3: Sharing in User Domains

5.3.1 Short Description

John owns several Devices, including a networked Home Media Center entertainment system and a number of handheld devices with varying degrees of network connectivity (mobile phone, portable player, etc.) John would like to play any of his content (regardless of where it was purchased) on any of his Devices.

5.3.2 Actors

John	A User that owns a set of Devices on which he want to access his Content.
Content Provider	An entity that provides Content and its associated Rights.
Operator	A Domain Authority that provides Domain Policies.
Cell Phone	A cell phone that is one of John's Devices.
PC	A Personal Computer that is one of John's Devices. The PC also contains a Domain Enforcement Agent.
Portable Player	A portable MP3 player that is one of John's Devices.
Home Media Center	A component that can hold, distribute and render content. It is one of John's Devices.

5.3.3 Actor Specific Issues

The Content Provider would like to offer a compelling content download service but prevent unauthorized use of their content.

John wants as few restrictions as possible on the distribution and consumption of Content on his own Devices. He also wants as little User Domain management tasks as possible.

5.3.4 Actor Specific Benefits

John needs to add his Cell Phone, PC, Portable Player and Home Media Center to his User Domain only once. John may use any Device in his User Domain to purchase Content for his User Domain from any Content Provider and is able to freely share his Content on any of his Devices.

The Content Provider can allow free replication and consumption of Content among the limited set of Devices in a User Domain and limit distribution and consumption to Devices outside the User Domain. This feature increases the attractiveness of the content download service and increases usage rates.

5.3.5 Pre-conditions

John owns a number of Devices. These Devices can communicate with each other to allow User Domain Content to be shared between the Devices.

The Content Provider supports User Domains.

5.3.6 Post-conditions

John has created a User Domain that includes his Cell Phone, PC, Portable Player and Home Media Center.

John has acquired User Domain Content on one (or more) of the Devices in his User Domain.

John is able to share his User Domain Content with to all the Devices in his User Domain.

5.3.7 Normal Flow

5.3.7.1 User Domain Creation

To create his User Domain, John performs the following steps:

1. Via his PC, John browses the Operator's list of Domain Policies.
2. John selects a Domain Policy appropriate for his situation.
3. The Operator provides a Domain Policy to the DEA in John's PC.
4. The PC (via its DEA), creates the John's User Domain, automatically adding itself to the User Domain.
5. John connects his Cell Phone, Portable Player and Home Media Center to his PC and adds them to his User Domain. The PC (via its DEA) makes sure that John cannot add more Devices than are allowed in the Domain Policy.

5.3.7.2 Content Acquisition

To acquire Content for his User Domain, John performs the following steps:

1. John uses his Cell Phone to browse the catalog of a Content Provider.
2. John selects a piece of Content he wishes to purchase.
3. John indicates he wants to purchase the Content for his User Domain and provides his Domain Policy.
4. If the Domain Policy is acceptable to the Content Provider, it provides John with a User Domain Rights Object along with the Content.
5. If the Domain Policy is NOT acceptable to the Content Provider, it informs John and it can give John the option of acquiring a Device Rights Object.

5.3.7.3 Content Sharing

Now that John has acquired User Domain Content, he wants to share it with his other Device in his User Domain. He has the following two options:

1. He can connect his Cell Phone to each of his other Devices and transfer the Content and its corresponding User Domain Rights Object to each Device.
2. He can upload the Content and its corresponding User Domain Rights Object on a common server such as the PC or Home Media Server. John then connects the other Devices to the PC (or Home Media Server) and downloads the Content and User Domain RO.

5.3.8 Alternative Flow

None.

5.4 Use Case 4: Ad Hoc Sharing of Content

5.4.1 Short Description

Jacob, John and Mary are attending a party at Mike's house with some other friends. Mike has a big-screen TV and a Home Media Center. The friends would like to see John's videos on the big-screen TV and listen to Jacob and Mary's audio files on Home Media Center. Jacob and Mary bring their mobile phones, each containing several audio files, to the party. Creating a User Domain that includes all the Devices at the party seems overkill. John, Jacob, Mary and Mike would like to take

advantage of the Ad Hoc Sharing feature offered by their Content Providers that enables them to share their Content with their friends.

5.4.2 Actors

Jacob, John, Mary, Tom, Jill and Ted	Users with Devices who are attending Mike's party.
Mike	A User who owns several Devices and is throwing a party.
Phyllis	A User who owns a mobile phone. She cannot come to the party because she is sick.
Mobile Operator	An entity that provides mobile phone service and a Content download service to its subscribers. It serves as a proxy to the Content Provider
Content Provider	An entity that provides Content and its associated Rights.
Mobile Phone	A portable Device and phone that can render audio and video. John, Jacob and Mary all own mobile phones.
Big Screen TV	One of Mike's Devices that can render and store video Content.

5.4.3 Actor Specific Issues

Jacob, John, Mary and Mike would like to make use of their purchased Content with as few restrictions as possible on how they can share and render it.

The mobile operator would like to offer a compelling content download service to its subscribers.

The content provider would like to encourage increased content purchases while preventing unauthorized use of its content.

5.4.4 Actor Specific Benefits

John is able to share his purchased content with friends in a variety of situations.

The Ad Hoc Sharing feature increases the attractiveness of the mobile operator's content download service and increases service subscription.

Mobile Operator benefits by offering a compelling service that includes phone and Content download.

Content Provider benefits by offering a compelling Content download service that attracts users but prevents unauthorized transfer of Content.

5.4.5 Pre-conditions

Jacob, John, Mary and Mike's Devices support short-range connectivity allows each Device to browse the available sharable Content on the other Devices.

The mobile operator and content provider support the Ad Hoc Sharing of Content.

5.4.6 Post-conditions

All the friends are able to browse and render the Content on each other's Devices.

5.4.7 Normal Flow

1. Mike has invited Jacob, John and Mary to a party he is giving. He acquires a music video that is stored on his Big Screen TV. The music video has the Rights that allow it to be shared on an ad hoc basis.
2. Jacob purchases an audio file from his Mobile Operator. His Rights to the audio file include the ability to share it on an ad hoc basis with other Devices.
3. On his way to the party at Mike's house, John purchases a music video on his Mobile Phone. He selects a set of Rights that allows him to share the video on an ad hoc basis with other Devices (his Device can provide Rights to play the video for two hours to at most three other Devices at a time).
4. Jacob and John arrive at the party, where Mary is also a guest.

5. Mary's Mobile Phone discovers the Devices of her friends at the party and is authenticated to enable Ad Hoc Sharing of Content.
6. Mary's Mobile Phone browses the sharable Content available to be rendered on all the guest's devices.
7. She chooses John's new music video to be displayed on the Mike's Big Screen TV.
8. Jacob is outside on the balcony when his Mobile Phone discovers Mike's Big Screen TV. He browses and discovers the Mike's music video.
9. Jacob plays Mike's music video on his Mobile Phone.
10. Jacob leaves the party. Mike's music video can no longer be played his Mobile Phone.

5.4.8 Alternative flow

When Jacob leaves the party, he can play the Mike's music video on his Mobile Phone for a limited time, as allowed by the rights granted to the Big Screen TV when sharing was initiated.

In Step 1, after sharing his video with Mary, John shares it with Tom and Jill. When John tries to share it with Ted, his attempt is rejected, since there are already three other guests sharing the video. John sees Ted at the party a few hours later, after the shared rights of Mary, Tom and Jill have expired; John is able to share the video with Ted at that time.

In step 1, after sharing his video with Mary, John exchanges instant messages with his friend Phyllis, who is sick and not able to attend the party. She also wants to share his video. Since the Ad Hoc Sharing rights that John purchased for the video do not include a proximity constraint, John's Mobile Phone is able to provide Phyllis's Mobile Phone with Rights to play the video for two hours.

5.5 Use Case 5: Play Outside of User Domain

5.5.1 Short Description

John has created a User Domain that includes his Mobile Phone and he has associated his User Identity Module (UIM) as a User Domain Token for his User Domain. He also owns an Internet connected Home Media Center. In his rented car, he would like to render the content from his Mobile Phone to the Car Stereo. While staying in a hotel room that has an Internet connected, OMA DRM-enabled television, John would like to render videos on this television that he purchased for his User Domain and which he has stored on his Home Media Center.

5.5.2 Actors

John	The User that interacts with the Devices to request rendering of Content.
Car Stereo	A Render Client used to render the Content stored on the Mobile Phone
Home Media Center	A component that stores Content and Rights Objects and from which the content can be accessed via Internet. The Home Media Center is not a Device in this Use Case.
User Identity Module (UIM)	A User Doman Token that belongs to John. When the UIM is in proximity to a non-member Device, any User Domain Content can be rendered on that Device (regardless of where the Content is stored).
Hotel Television	A Device used to render video's stored on the Home Media Center after interaction with a User Domain Token.
Mobile Phone	A Device that belongs to the User Domain and hosts the UIM.

5.5.3 Actor Specific Issues

The Car Stereo does not have the resources to implement a full OMA DRM Agent and does not have the means to access the Internet.

5.5.4 Actor Specific Benefits

John is able to enjoy his Content where ever he goes.

5.5.5 Pre-conditions

John has created a User Domain, that includes his Mobile Phone, and has associated to his UIM to his User Domain. John's Domain Policy allows for Token based access.

John has downloaded User Domain Content to his Mobile Phone and stored some of the Content on his Home Media Center.

5.5.6 Post-conditions

John is able to render the videos on the television in his hotel room from both his Mobile Phone and his Home Media Center.

John is able to render the music stored on his Mobile Phone on the Car Stereo.

5.5.7 Normal Flow

1. John uses his Mobile Phone to discover the Car Stereo and establish a connection.
2. John interacts with the Mobile Phone to request transport and rendering of an audio track (stored on the Mobile Phone) to the Car Stereo.
3. The Car Stereo renders the audio.
4. In his hotel room, John remembers that he has a video stored on his Home Media Center (but not on his Mobile Phone) that he would like to play on the Hotel Television.
5. John uses his Mobile Phone to discover the Hotel Television and establish a connection.
6. The Hotel Television mutually authenticates with the UIM in John's Mobile Phone. The Hotel Television is now enabled to temporarily access John's User Domain Content that is stored either on his Mobile Phone or on his Home Media Center at home.
7. John interacts with the Hotel Television to connect via the Internet to his Home Media Center at home.
8. John interacts with the Hotel Television to request transport and rendering of a video that is stored on his Home Media Center.
9. The video is streamed over the Internet from the Home Media Center to the Hotel Television, which renders the video.

5.5.8 Alternative Flow

Alternative Step 1: The discovery and connection set-up is initiated by the Car Stereo.

Alternative Step 3: The Mobile Phone determines that for the selected piece of content it is NOT allowed to render outside the User Domain via local connectivity. The user is notified.

5.6 Use Case 6: Sharing of Content Between Family Members and their Friends

5.6.1 Short Description

The Smith family owns several OMA DRM enabled components which are networked and belong to a User Domain. Emma, the wife, buys a movie online and stores it on their networked home entertainment system. That evening Emma and her husband John watch the movie on their entertainment system. Since the movie is long they decide to watch the end in their

bedroom. In the bedroom, Emma turns on the TV and selects the movie they were watching. Emma and John continue watching the end of the movie.

The next day their son Adam wants to watch the movie on his PC, so he connects to the home entertainment system and watches the movie on his PC monitor.

Later that day Adam's friend Michael visits and he shows off his newest OMA DRM enabled gaming console. To check the quality of the device they decided to watch a part of the movie that was bought by Emma. However, Emma did not purchase rights for the movie that would allow it to be shared on devices not owned by Emma and her family members. Adam contacts the Rights Issuer for the movie and requests an additional permission that allows him to lend the movie to another Device, and he then lends the movie to Michael. Michael connects the device to the in-house wireless network and fetches the content from the media center and plays a part.

5.6.2 Actors

Emma, John, Adam	Members of the Smith family who share Content via a User Domain that includes all of their Devices.
Michael	A friend of Adam who owns a portable Device.
Home Entertainment System	One of the family's Devices that belongs to their User Domain.
Bedroom TV	One of the family's Devices that belongs to their User Domain.
PC	One of Adam's Devices that belongs to the family User Domain.
Gaming Console	A portable Device that belongs to Michael. It does not belong to the Smith family User Domain.

5.6.3 Actor Specific Issues

John, Emma and Adam would like to purchase content that they can render on any of the Devices that the family owns.

Adam wants to share family content occasionally with his friends.

Content provider wants to offer their subscribers the flexibility to share content on multiple devices, while protecting against piracy and unauthorized distribution of content and rights.

5.6.4 Actor Specific Benefits

It will be possible for family members to render purchased OMA DRM Contents at any of their Devices without any interaction with the Rights Issuer.

The sharing functionality provided by OMA DRM allows for flexible application of DRM to different scenarios without interaction with the user, making DRM transparent to use and as such lowers the barrier for consumers whilst at the same time upholding the specific requirements set by the content owner.

Rights Issuer can control whether and how rights are shared.

5.6.5 Pre-conditions

The Smith family, consisting of John, Emma and Adam, have a number of Devices that can communicate with each other over a home network.

A User Domain has been created that includes all of the family's Devices.

Michael has a gaming console that supports OMA DRM.

5.6.6 Post-conditions

A movie purchased by Emma can be rendered on any Device in the family's User Domain.

Adam is able to lend the movie to his friend Michael.

5.6.7 Normal Flow

1. Emma purchases a movie for the User Domain, and she and John watch it on the HD television set in their living room. Later, they continue to watch it on the TV set in their bedroom.
2. The next day, Adam accesses the movie from his PC and plays it.
3. Adam's friend Michael comes over to visit with his gaming console. Michael wants to play the movie purchased by Emma on his gaming console.
4. Adam realizes that the rights purchased by Emma for the movie do not include permission to share the movie with devices outside the family User Domain. He contacts the Rights Issuer and views the available options for purchase of additional sharing permissions for the movie.
5. Adam chooses to add a permission that allows him to lend to the movie to another Device outside the User Domain. Adam lends the movie to Michael for a period of two hours. During this period, Adam is not able to watch the movie on his PC.
6. Michael downloads the content file containing the movie from the family's media server and attempts to play the movie on his gaming console. However, his console does not support the video media type contained in the file.
7. Fortunately, the rights package purchased for the movie by Emma includes a permission that allows the acquisition and rendering of the movie in several different media formats. Michael contacts a content server via the family's home network and is able to download a version of the movie in a format that is compatible with his gaming console.
8. Michael plays the movie. Two hours later, the lending period terminates; Michael is no longer able to render the movie on his gaming console, and Adam is once again able to watch the movie on his PC.

5.6.8 Alternative Flow

In Step 8, Michael explicitly returns the Rights to Adam before the two-hour period has ended. Once Adam receives the returned Rights from Michael, Adam can immediately watch the movie on his PC.

5.7 Use Case 7: Long Term Ownership

5.7.1 Short Description

John, his brother Richard and sister Harriet build up a library of music as they grow up on their PCs, phones and portable music players. When John goes off to university he still has access to the library. After a year at university John moves into a shared house and forms a new library with his housemates, incorporating all his home music and adding in new music from his housemates. When John goes back home, Richard and Harriet can listen to John's housemates' music while John is at home but it is not added into the home library and they can't listen to it when John goes back to university. Similarly, John can listen to the new music that Richard and Harriet have bought since he left home while he is at home, but it is not permanently added into his university library.

5.7.2 Actors

John	The user.
Richard & Harriet	The user's siblings.
Home Domain	A Domain established by family members so that they can share their content.
New Domain	A new Domain "spawned" from possibly multiple different Home Domain(s).
Service Provider	The entity that provides Domain and other content services to the user.

5.7.3 Actor Specific Issues

5.7.4 Actor Specific Benefits

5.7.5 Pre-conditions

The members of the Home Domain have established a Domain so that they can purchase, consume and share music and other content.

5.7.6 Post-conditions

When John leaves home he still has access to the content that belongs to the Home Domain.

When John spawns a new Domain, New Domain he is able to incorporate all his content from his Home Domain and also add new content from other sources.

When John returns home, the members of the Home Domain can consume the content from the New Domain while the John is at home but it is not permanently added into the Home Domain and it can not be consumed when John is not at home.

When John is at home he can listen to any content that has been added to the Home Domain since he spawned his new Domain but it is not added into his New Domain.

5.7.7 Normal Flow

1. John, Richard and Harriet have formed a home Domain and built up lots of songs over the years.
2. When John goes off to university, his phone and laptop are still in the home Domain and he can still listen to all the music collection he built up with Richard and Harriet. They synchronise devices over the Internet and can all listen to the new music that has been added.
3. After a year at university, John and his new house mates contact the service providers who controls their Home Domain(s) and asks them to "spawn" a new Domain from their Home Domain(s). As members of this New Domain John and his housemates all have access to the content from all of their Home Domain(s). John and his housemates pay their service providers various charges for forming this New Domain. John and his housemates have effectively left their Home Domain(s) in so much that they can not consume any content that is added after they spawned the New Domain, but they collectively still have access to all the music that was in their Home Domain(s) at the moment that the New Domain was spawned.
4. Meanwhile Richard and Harriet continue to build up their collection at home.
5. When John returns home, the members of the Home Domain can consume the content from the New Domain while the John is at home but it is not permanently added into the Home Domain and it can not be consumed when John is not at home.
6. When John is at home he can also listen to any content that has been added to the Home Domain since he spawned his new Domain but it is not permanently added into his New Domain.

5.7.8 Alternative flow

None.

5.8 Use Case 8: Consumption of Digital Broadcast Content on a portable player

5.8.1 Short Description

In this use case, John has a subscription for a Digital broadcast service delivered over cable to John's home. For this purpose, John has a Set-top Box (STB) with a Recorder, which allows playback at the STB. John regularly records movies, and in this use case he can play those movies also on his OMA DRM portable media player.

5.8.2 Actors

John	User who owns Devices and wants to transfer DRM Content across his Devices.
Set-top Box	A product that belongs to John for receiving and recording Digital broadcast content received over cable
Portable Media Player	A Device that belongs to John on which he can watch movies
Broadcaster	The provider of the Digital broadcast content to John's STB
Rights Issuer	The entity that issues the Rights to consume broadcast content on John's portable media player
Interaction Channel	A bi-directional communication path between John and the Rights Issuer

5.8.3 Actor Specific Issues

John wants the movies that he records on his Digital TV STB to play on his Portable Media Player.

The Broadcaster allows John to record the movies from the Digital broadcast service on his STB, and the Rights Issuer allows him to consume those recorded movies on his Portable Media Player.

5.8.4 Actor Specific Benefits

John is not only able to play the movie on his STB, but also on his Portable Media Player.

The Broadcaster has the option not only to sell his Digital TV broadcast content for use at John's STB, but also the Rights for play back at John's Portable Media Player.

5.8.5 Pre-conditions

John records a movie from the Digital broadcast service at his STB and transfers, for example copies, the recorded movie to his Portable Media Player.

The Rights Issuer provides the Rights to John to play the movie at his Portable Media Player.

Within the Digital broadcast service, the Broadcaster inserted information required for playback of the movie in John's Portable Media Player.

5.8.6 Post-Conditions

The Portable Media Player is able to use the Rights provided by the Rights Issuer to play the movie.

5.8.7 Normal Flow

The following explains how John can play a recorded movie on his Portable Media Player.

9. John records a movie on his STB, and transfers this movie to his Portable Media Player.
10. Via an Interaction Channel, John requests the Rights Issuer in order to play this movie on his Portable Media Player.

11. The Rights Issuer provides those Rights via the Interaction Channel.
12. John can now play the movie on his Portable Media Player, as permitted by the Rights he received from the Rights Issuer.

6. Requirements (Normative)

The requirements in Section 6 are in addition to the requirements in [DRMREQ-v2]. In cases where the requirements in Section 6 contradict the requirements in [DRMREQ-v2], the requirements in Section 6 take precedence.

6.1 High-Level Functional Requirements

Label	Description	Enabler Release
SCE-HL-001	It SHALL be possible for a Device to send DRM Content to a Render Client Device, such that the DRM Content may be rendered there, if usage permissions allow.	SCE V1.0
SCE-HL-002	The SCE enabler SHALL allow a Device to Move Rights to another Device.	SCE V1.0
SCE-HL-003	The SCE Enabler SHALL allow a Device to request from the Rights Issuer the permission to share Rights (e.g. move Rights, copy Rights, lend Rights and so on), in the case where the user's existing Rights do not explicitly permit sharing; the SCE Enabler SHALL allow the Rights Issuer to respond by including newly generated (Domain, User Domain, or Device) Right Objects to be used by intended Move recipient Device(s).	SCE V1.0
SCE-HL-MDCF-001	The SCE Enabler SHALL allow to use an MPEG-2 Transport Stream as a container of DRM Content	SCE V1.0

Table 2: High-Level Functional Requirements

6.1.1 Security

Label	Description	Enabler Release
SCE-SEC-001	The SCE Enabler SHALL allow Rights Issuer to provide authorization for moving the Rights from one Device to another Device.	SCE V1.0
SCE-SEC-002	The SCE enabler SHALL allow Rights Issuers to require that the integrity of DRM Content and associated Content Encryption Key(s) be verified against an RI-generated Rights Object by recipient Devices.	SCE V1.0
SCE-SEC-003	The SCE Enabler SHALL allow a Domain Enforcement Agent to provide authorization for the membership of Devices in a User Domain.	SCE V1.0
SCE-SEC-004	The SCE enabler SHALL enable authentication of a User to a Device based on a User Token (e.g. SIM) that represents the User.	SCE V1.0
SCE-SEC-005	The SCE enabler SHALL provide a mechanism for mutual authentication between two Devices before Moving Rights directly between the Devices.	SCE V1.0
SCE-SEC-006	Devices SHALL be able to use revocation information as part of mutual authentication between Devices	SCE V1.0
SCE-SEC-007	The SCE enabler SHALL provide a secure mechanism to Move Rights between Devices.	SCE V1.0
SCE-SEC-008	The SCE enabler SHALL ensure the confidentiality of Content Encryption Key(s) during transfer to recipient Devices.	SCE V1.0
SCE-SEC-009	Devices SHALL digitally sign appropriate critical elements when moving Rights to recipient Devices. Such information MAY be used by a trust authority to securely determine which Devices have been involved in a (potentially unauthorized) moving of the Rights.	SCE V1.0

SCE-SEC-010	The SCE enabler SHALL ensure that Devices verify that received Rights were generated using knowledge of the embedded Content Encryption Key(s).	SCE V1.0
SCE-SEC-011	The SCE enabler SHALL ensure that message replay does not result in duplicate operation(s) by a recipient Device.	SCE V1.0
SCE-SEC-012	The SCE enabler SHALL ensure that source Devices that Move Rights do not locally re-enable such Rights without assurance that the Rights are not enabled on the intended recipient Device.	SCE V1.0

Table 3: High-Level Functional Requirements – Security Items

6.1.2 Charging

No charging requirements have been identified.

6.1.3 Administration and Configuration

No administration or configuration requirements have been identified.

6.1.4 Usability

No usability requirements have been identified.

6.1.5 Interoperability

No interoperability requirements have been identified.

6.1.6 Privacy

No privacy requirements have been identified.

6.2 Overall System Requirements

Label	Description	Enabler Release
SCE-SYS-001	It SHALL be possible for a DRM Agent on the Device to verify that for a Render Client a proximity constraint is met.	SCE V1.0
SCE-SYS-002	The SCE enabler SHALL allow a Device to verify that a User Domain Token is in proximity.	Future Release
SCE-SYS-003	The SCE enabler SHALL provide a mechanism for Unconnected Devices that support DRM Time to make use of Rights received from Unconnected Devices that support DRM Time.	Future Release
SCE-SYS-004	The SCE enabler SHALL permit a Device to use local discovery mechanisms (e.g. UPnP), in a mechanism-independent manner, to browse the Content and Rights available on other Devices for Sharing, if authorized by other Device through a non-OMA DRM mechanism.	SCE V1.0
SCE-SYS-005	The SCE enabler SHALL include the means for a Device receiving Shared Rights to acquire a version of the associated DRM Content in a format suitable for rendering on that Device.	SCE V1.0
SCE-SYS-006	The SCE enabler SHOULD provide all operations, permissions and restrictions that are available for Device bound Rights also for User Domain bound Rights and Domain bound Rights	SCE V1.0

Table 4: Overall System Requirements

6.3 Rights Move Requirements

Label	Description	Enabler Release
SCE-MOVE-001	The SCE enabler SHALL allow Moving Partial Rights to another Device.	SCE V1.0
SCE-MOVE-002	The SCE enabler SHALL allow Moving of Rights to another Device via Rights Issuer.	SCE V1.0
SCE-MOVE-003	It SHALL be possible for the Device initiating a Move of Rights to specify a unique identity of the recipient Device for which it intends to Move the Rights.	SCE V1.0
SCE-MOVE-004	The SCE enabler SHALL allow Moving Rights directly between two Devices without contacting Rights Issuer for each Move.	SCE V1.0
SCE-MOVE-005	The SCE enabler SHALL allow a Rights Issuer to specify in Rights Object the conditions under which it is allowed for the Device to Move Rights to another Device(s).	SCE V1.0
SCE-MOVE-006	The SCE enabler SHALL allow Devices to Move Rights Objects and its associated State Information, in case Rights Object is stateful.	SCE V1.0
SCE-MOVE-007	The SCE enabler SHALL allow functionality of Moving Rights regardless of geographical locations of the originating Device and the recipient Device.	SCE V1.0
SCE-MOVE-008	The SCE enabler SHALL allow a Rights Issuer to specify how many times the Rights can be Moved.	SCE V1.0
SCE-MOVE-009	The SCE enabler SHALL allow a Device to reduce the number of times that Rights can be Moved as a result of successfully Moving those Rights.	SCE V1.0

Table 5: Rights Move Requirements

6.4 Import Requirements

Label	Description	Enabler Release
SCE-IMP-001	The SCE enabler SHALL allow Devices to have the capability to receive Imported-Data.	SCE V1.0
SCE-IMP-002	The SCE enabler SHALL allow the Import of data from various Non-OMA DRM systems.	SCE V1.0
SCE-IMP-003	The SCE enabler SHALL allow Imported-Data to be OMA DRM v2.0 conformant.	SCE V1.0
SCE-IMP-004	The SCE enabler SHALL allow the Imported-Data to be bound to a unique Device or to a unique Domain or User Domain, such that the Imported-Rights-Object can only be processed by the intended Device(s).	SCE V1.0

Table 6: Import Requirements

6.5 User Domain Requirements

Label	Description	Enabler Release
SCE-DOM-001	The SCE enabler SHALL enable a Rights Issuer to specify usage permissions for consumption of Rights on and transfer of Rights between Devices that are members of the same User Domain. It SHALL at least be possible to include play, copy and move permissions.	SCE V1.0
SCE-DOM-002	The SCE enabler SHALL enable a Rights Issuer to specify usage permissions for consumption of Rights on and transfer of Rights between Devices that are NOT members of the same User Domain. It SHALL at least be possible to include copy and move permissions.	SCE V1.0
SCE-DOM-003	It SHALL be possible for a Device to request Rights from a Rights Issuer with permissions for a certain User Domain.	SCE V1.0

SCE-DOM-004	It SHALL be possible for the Rights Issuer to indicate to a Device that the Domain Policy associated with the User Domain for which Rights are requested, is not supported.	SCE V1.0
SCE-DOM-005	The SCE enabler SHALL enable a Domain Authority to define limits on the size of the User Domain: the Domain Policy.	SCE V1.0
SCE-DOM-006	The SCE enabler SHALL allow a Domain Authority to specify in its Domain Policy that DRM Content that may be rendered in the User Domain may also be rendered from a Device that is a User Domain member, to any Render Client if a proximity constraint for that Render Client is met.	SCE V1.0
SCE-DOM-007	Domain Policies for User Domains, issued by a Domain Authority, SHALL support constraints such as: • the number of Devices in the User Domain • the number of changes in membership within a time period • the number of User Domain Tokens associated with the User Domain • the number of changes in associations of User Domain Tokens within a time period • the lifetime of the Token based access.	SCE V1.0
SCE-DOM-008	The Domain Enforcement Agent SHALL be able to use local device discovery mechanisms (e.g. UpnP) to facilitate the designation of devices for the User Domain.	SCE V1.0
SCE-DOM-009	The SCE enabler SHALL require that a Device be authenticated before it is added to a User Domain by the Domain Enforcement Agent.	SCE V1.0
SCE-DOM-010	The SCE enabler SHALL enable the Domain Enforcement Agent to enforce the Domain Policy and to perform User Domain management according to the Domain Policy specified by the Domain Authority. Management includes the adding and removing of Devices to/from the User Domain.	SCE V1.0
SCE-DOM-011	The SCE enabler SHALL allow a Domain Authority to replace the Domain Enforcement Agent with another Domain Enforcement Agent upon the request of the User, so that the new Domain Enforcement Agent can manage the User Domain instead of the former Domain Enforcement Agent, i.e. the adding and removing of Devices and the enforcement of the Domain Policy.	SCE V1.0
SCE-DOM-012	The SCE enabler SHALL enable mutual authentication of a Device and a Domain Enforcement Agent.	SCE V1.0
SCE-DOM-013	Devices and Domain Enforcement Agents SHALL be able to use revocation information as part of mutual authentication between Devices and Domain Enforcement Agents.	SCE V1.0
SCE-DOM-014	The SCE enabler SHALL enable mutual authentication of Domain Authority and Domain Enforcement Agent.	Future Release
SCE-DOM-015	Domain Authorities and Domain Enforcement Agents SHALL be able to use revocation information as part of mutual authentication between Domain Authorities and Domain Enforcement Agents.	Future Release
SCE-DOM-016	The SCE enabler SHALL enable a Device in a User Domain to provide acquired Rights to other members of the User Domain to render the associated Content.	SCE V1.0
SCE-DOM-017	The SCE enabler SHALL enable Token based access.	Future Release
SCE-DOM-018	The SCE enabler SHALL enable a User to associate User Domain Token(s) with his/her User Domain.	Future Release

SCE-DOM-019	A Device that is not a member of a User Domain SHALL NOT be able to Consume DRM Content based on Rights Objects that were issued for that User Domain.	SCE V1.0
SCE-DOM-020	The SCE enabler SHALL allow a Device to be member of more than one User Domain at the same time.	SCE V1.0
SCE-DOM-021	The SCE enabler SHALL enable mutual authentication of a DRM Agent and a Render Agent.	SCE V1.0
SCE-DOM-022	The SCE enabler SHALL support only one Domain Policy per User Domain.	SCE V1.0

Table 7: Domain Requirements

6.6 Ad Hoc Sharing Requirements

Label	Description	Enabler Release
SCE-SHR-001	The SCE enabler SHALL make it possible for a Device that acquires DRM Content to request from the Rights Issuer the ability to share that Content within an Ad Hoc Domain.	SCE V1.0
SCE-SHR-002	The SCE Enabler SHALL allow a source Device to generate Shared Rights only when Rights Issuer has given the permission for the source Device to do so.	SCE V1.0
SCE-SHR-003	The SCE enabler SHALL allow Rights Issuer to define the Rights or parts thereof that can be shared during Ad Hoc Sharing.	SCE V1.0
SCE-SHR-004	Devices that engage in Proximity-Limited Sharing SHALL be able to reliably determine if they are in proximity to each other.	SCE V1.0
SCE-SHR-005	The Domain Enforcement Agent SHALL allow a Device to participate in a Proximity-Limited Domain only when that Device is in proximity to the device on which the Domain Enforcement Agent resides.	Future Release
SCE-SHR-006	The SCE enabler SHALL allow a Device to participate in Ad Hoc Sharing with another Device.	SCE V1.0
SCE-SHR-007	The SCE enabler SHALL make it possible for Rights acquired for a User Domain to include Permissions for Ad Hoc Sharing.	SCE V1.0
SCE-SHR-008	The SCE enabler SHALL provide a means for Devices to mutually authenticate each other, and if this mutual authentication fails then Ad Hoc Sharing between these Devices MUST NOT be enabled.	SCE V1.0
SCE-SHR-009	The SCE enabler SHALL allow Ad Hoc Sharing between Devices that are not members of an Ad Hoc Domain.	SCE V1.0
SCE-SHR-010	The SCE enabler SHALL allow successful initiation of Ad Hoc Sharing, in an Ad Hoc Domain, to be dependent upon communications with a Domain Enforcement Agent.	Future Release
SCE-SHR-011	Domain Policies for Ad Hoc Domains, issued by a Domain Authority, SHALL support constraints such as the number of Devices in the Ad Hoc Domain, the number of changes in membership within a time period and the lifetime of the Ad Hoc Domain.	Future Release
SCE-SHR-012	It SHALL be possible for Devices to use Rights acquired via Ad Hoc Sharing for restricted usage following initiation of the Ad Hoc Sharing, without requiring communication between the Devices.	SCE V1.0
SCE-SHR-013	The SCE enabler SHALL allow Rights to be granted to the recipient of shared Content via Ad Hoc Sharing, independently of the Rights on the source Device.	SCE V1.0

SCE-SHR-014	The SCE enabler SHALL allow initiation of Ad Hoc Sharing of Content by a source Device to be conditional upon previously initiated Ad Hoc Sharing of that Content, e.g. by specifying limits on the number of recipients that can simultaneously share the Content within a specific period of time.	SCE V1.0
SCE-SHR-015	Shared Rights (without time Constraints) SHALL NOT be backed up.	SCE V1.0

Table 8: Ad Hoc Sharing Requirements

6.7 Local Rights Manager Requirements

Label	Description	Enabler Release
SCE-LRM-001	The SCE enabler SHALL allow Devices to verify the identifiers of Local Rights Manager(s) that created Imported-Rights-Object.	SCE V1.0
SCE-LRM-002	The SCE enabler SHALL allow a Local Rights Manager to create Imported-Rights-Objects for Devices, Domains, or User Domains.	SCE V1.0
SCE-LRM-003	A Local Rights Manager that creates an Imported-Rights-Object SHALL associate Imported-Content with that Imported-Rights-Object.	SCE V1.0
SCE-LRM-004	The SCE enabler SHALL allow Devices to have the capability to confirm the association between Imported-Rights-Object(s) and Imported-Content.	SCE V1.0
SCE-LRM-005	A Local Rights Manager that creates an Imported-Rights-Object SHALL identify itself within the Imported-Rights-Object as the source of the Imported-Rights-Object.	SCE V1.0

Table 9: Local Rights Manager Requirements

6.8 Lending Requirements

Label	Description	Enabler Release
SCE-LEN-001	The SCE enabler SHALL enable Rights Issuer to specify the conditions under which the Device is allowed to share DRM Content using Lending.	SCE V1.0
SCE-LEN-002	The SCE enabler SHALL make it possible for a Device to share Content with another Device using Lending.	SCE V1.0
SCE-LEN-003	It SHALL be possible to define a time limitation on the lent Rights so that after the specified time the Rights are no longer valid on the recipient Device but are valid on the source Device.	SCE V1.0
SCE-LEN-004	It SHALL be possible to return lent Rights so that they are no longer valid on the recipient Device but are valid on the source Device.	SCE V1.0
SCE-LEN-005	The SCE Enabler SHALL NOT allow a recipient Device to Move the Shared Rights received from a source Device by Lending, to any other Device except the Device which they came from.	SCE V1.0

Table 10: Lending Requirements

6.9 Long Term Ownership Requirements

Label	Description	Enabler Release
SCE-LTO-001	It SHALL be possible to split an existing User Domain (the original User Domain) into two (or more) separate User Domains (the resultant User Domains).	Future Release
SCE-LTO-002	It SHALL be possible to define if a Domain Enforcement Agent is allowed to create new User Domains from existing User Domains (i.e. split an existing User Domain) within the Domain Policy.	Future Release

SCE-LTO-003	It SHALL be possible to define the rules that the Domain Enforcement Agent MUST enforce when splitting a User Domain within the Domain Policy. Example rules include, but are not limited to: • If User Domain Splitting is allowed for this User Domain. • The number of User Domains that the existing User Domain can be split into • The Domain Policy(s) for the resultant User Domains • If the creation of new ROs (see SCE-LTO-004) requires additional payments to the RI • The constraints that specify the conditions when members of the original User Domain can consume ROs bound to any of the resultant User Domains. E.g. o Only when they are in proximity to Devices belonging to the resultant User Domains (see SCE-LTO-006) o Always o Never o etc • If the original User Domain should still exist after it has been split. • If it will be possible to acquire Rights for the original User Domain after it has been split.	Future Release
SCE-LTO-004	It SHALL be possible to create new ROs that are bound to the resultant User Domains as a result of splitting a User Domain; depending on the Domain Policy this may involve additional payments to the RIs that issued the original ROs.	Future Release
SCE-LTO-005	It SHALL be possible to specify the domain membership for User Domains (i.e. the resultant User Domains) that are created as a result of splitting an existing User Domain (i.e. the original User Domain).	Future Release
SCE-LTO-006	It SHALL be possible for members of the original User Domain to consume ROs bound to any of the resultant User Domains (created as a result of splitting a User Domain) when they are in proximity of a Device from any of the other resultant User Domains.	Future Release
SCE-LTO-007	It SHALL be possible to merge two (or more) existing User Domains into a single User Domain (merged User Domain).	Future Release
SCE-LTO-008	It SHALL be possible to define if a Domain Enforcement Agent is allowed to merge existing User Domains into a single User Domain within the Domain Policy.	Future Release

SCE-LTO-009	It SHALL be possible to define the rules that the Domain Enforcement Agent MUST enforce when merging User Domains within the Domain Policy. Example rules include, but are not limited to: • If Domain Merging is allowed for this User Domain • The semantics for creating the Domain Policy for the merged User Domain from the Domain Policies of the User Domains to be merged. • If the creation of new ROs (see SCE-LTO-010) requires additional payments to the RI • If the User Domains that are to be merged should still exist as separate and valid User Domains after they have been merged. • If it will be possible to acquire Rights for the User Domains that are to be merged after they have been merged • Rules for defining the Domain membership of the merged User Domains e.g. o If all members of the User Domains to be merged will automatically become members of the merged User Domain or not.	Future Release
SCE-LTO-010	It SHALL be possible to create new ROs that are bound to the merged User Domain as a result of merging a User Domain; depending on the Domain Policy this may involve additional payments to the RIs that issued the original ROs.	Future Release

Table 11: Long Term Ownership Requirements

6.10 MPEG-2 Transport Stream Container Requirements

The following requirements have been identified for the use of an MPEG-2 transport stream as a container of DRM Content.

Label	Description	Enabler Release
SCE-MDCF-0010	DRM content protection within an MPEG-2 Transport Stream SHALL be possible per single Broadcast Program such as a sport event, news show or movie.	SCE V1.0
SCE-MDCF-0011	DRM content protection within an MPEG-2 Transport Stream SHALL be possible per single Broadcast Service, consisting of a concatenation of multiple “broadcast programs” within one “MPEG-2 PMT.	SCE V1.0
SCE-MDCF-0012	DRM content protection within an MPEG-2 Transport Stream, when applied in an existing broadcast service, SHALL allow simulcrypt of CAS defined messages with OMA DRM defined messages without requiring re-transmission of the (protected) content.	SCE V1.0
SCE-MDCF-0013	It SHALL be possible to use an OMA DRM 2.0 or an OMA DRM 2.1 Rights Object to access DRM Content in an MPEG-2 Transport Stream.	SCE V1.0
SCE-MDCF-0014	It SHALL be possible to store DRM Content contained in an MPEG-2 Transport Stream on commonly deployed storage systems for MPEG-2 Transport Streams without requiring any re-encryption, re-formatting or transcoding.	SCE V1.0
SCE-MDCF-0015	By using existing or extended DRM v2 protocols, and based on information contained in the MPEG-2 Transport Stream, it SHALL be possible to retrieve an OMA DRM Rights Object over an interaction channel to access DRM Content within that MPEG-2 Transport Stream.	SCE V1.0
SCE-MDCF-0016	It SHALL be possible to signal in an MPEG-2 transport stream whether DRM Content is contained.	

Table 12: MDCF Requirements

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
OMA-RD-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