DRM Architecture

Draft Version 2.0 – 20 August 2004

Open Mobile Alliance
OMA-DRM-ARCH-V2_0-20040820-C

Contents

Figures

1. Scope

The scope of OMA "*Digital Rights Management*" is to enable the controlled consumption of digital media objects by allowing content providers the ability, for example, to manage previews of DRM Content, to enable superdistribution of DRM Content, and to enable transfer of content between DRM Agents. The OMA DRM specifications provide mechanisms for secure authentication of trusted DRM Agents, and for secure packaging and transfer of usage rights and DRM Content to trusted DRM Agents.

2. References

2.1 Normative References

None

2.2 Informative References

[DRMREQ] OMA DRM Requirements Version 2.0. Open Mobile Alliance™. OMA-DRM-REQ-V2_0-20030425-d

[OMADRM] OMA DRM Specification V 2.0. Open Mobile Alliance™. OMA-DRM-DRM-V2_0-2003xxxx-d

[OMADCF] OMA DRM Conent Format V 2.0. OMA Open Mobile Alliance™. OMA-DRM-DCF-V2_0-2003xxxx-d

[OMAREL] OMA DRM Rights Expression Language V 2.0. Open Mobile Alliance™. OMA-DRM-REL-V2_0-2003xxxx-d

[MPEG21 RDD] ISO/IEC CD 21000-Part 6 - Rights Data Dictionary (RDD) (2002-07-26)

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

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

Actor	An actor is an external entity that carries out use cases.
Backup/Remote Storage	Transferring Rights Objects and Content Objects to another location with the intention of transferring them back to the original Device.
Billing Service Provider	The entity responsible for collecting payment from a User.
Composite Object	A Media Object that contains one or more Media Objects by means of inclusion.
Connected Device	A Connected Device is a Device that is capable of directly connecting to a Rights Issuer using an appropriate protocol over an appropriate wide area transport/network layer interface. E,g, HTTP over TCP-IP.
Content	One or more Media Objects
Content Issuer	The entity making content available to the DRM Agent.
Content Provider	An entity that is either a Content Issuer or a Rights Issuer.
Device	A Device is a user equipment with a DRM Agent. In the case where functionality is specific to either Connected Devices or Unconnected Devices the explicit terminology (i.e Unconnected Device or Connected Device) will be used, in all other cases the term Device generically applies to both Connected Devices and Unconnected Devices.
DRM Agent	The entity in the Device that manages Permissions for Media Objects on the Device.
DRM Content	Media Objects that are consumed according to a set of Permissions in a Rights Object.
DRM Time	A secure, non-user changeable time source. The DRM Time is in the UTC time format.
Functional Entity	Internal building block of the architecture.
Integrity	The property that data has not been altered or destroyed in an unauthorised manner. (ISO 7498-2)
Media Object	A digital work e.g. a ringing tone, a screen saver, a Java game or a Composite Object.
Network Service Provider	The entity providing network connectivity for a mobile Device.
Network Store	An entity remote to the device and controlled by a service provider which can store DRM Content and encrypted Rights Objects on behalf of a Device for Backup.
OMA DRM Conformant Device	A Device that will work interoperably with other OMA DRM Conformant Devices and some or all of the following; Billing Service Providers, Content Providers and Network Service Providers. It will also enable DRM Content on the Device only if the Device possesses a valid Rights Object for that instance of DRM Content and only according to the Permissions defined in the Rights Object for that instance of DRM Content.
Permission	Actual usages or activities allowed (by the Rights Issuer) over DRM Content (From [ODRL 1.1])
Restore	Transferring the DRM Content and/or Rights Objects from an external location back to the Device from which they were backed up.

Revoke	Process of declaring a Device or Rights Issuer certificate as invalid.
Rights Issuer	An entity that issues Rights Objects to OMA DRM Conformant Devices.
Rights Object	A collection of Permissions and other attributes which are linked to DRM Content.
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.
Transfer	To relocate DRM Content or a Rights Object from one place to another.
Unconnected Device	An Unconnected Device is a Device that is capable of connecting to a Rights Issuer via a Connected Device using an appropriate protocol over a local connectivity technology. E.g. OBEX over IrDA, Bluetooth or USB. An Unconnected Device may support DRM Time.
User	The human user of a Device. The User does not necessarily own the Device.

3.3 Abbreviations

3GPP	3rd Generation Partnership Project
CD	Compact Disc
CEK	Content Encryption Key
DCF	DRM Content Format
DRM	Digital Rights Management
DVD	Digital Versatile Disc
HTTP	HyperText Transfer Protocol
ISO	International Organization for Standardization
LAN	Local Area Network
MMS	Multimedia Messaging Service
MPEG	Motion Picture Expert Group
MP3	MPEG audio layer 3; coding scheme for audio compression
OMA	Open Mobile Alliance
OS	Operating System
PC	Personal Computer
PDA	Personal Digital Assistant
PKI	Public Key Infrastructure
REK	Rights Encryption Key
RFC	Request For Comments
RI	Rights Issuer
RO	Rights Object
SCR	Static Conformance Requirement
SIM	Subscriber Identity Module
SMS	Short Messaging Service
UI	User Interface
URI	Uniform Resource Indicator

4. Introduction

The role of DRM in distribution of content is to enable business models whereby the consumption and use of content is controlled. As such, DRM extends beyond the physical delivery of content into managing the content lifecycle. When a user buys content, she may agree to certain constraints - for example by choosing between a free preview version or a full version at cost, or she may agree to pay a monthly fee. DRM allows this choice to be translated into permissions and constraints, which are then enforced when the user accesses the content.

4.1 Actors and Functional Entities

An actor is defined here as an external entity involved in carrying out use cases. There exist a large number of possible actors in a DRM system. Examples range from content owners, content developers and content distributors, via network service providers and billing service providers, to manufacturers of network equipment and devices, and finally consumers of content. Depending on deployment scenario, different actors can play different roles in the system.

In the OMA DRM architecture, functional entities are used to embody specific roles in the DRM system. This makes it possible to decompose the tasks involved in digital rights management, separately from what actors perform each task in a certain deployment.

The functional entities are logical and need not represent physical network nodes (servers, etc). Depending on configuration, different functional entities may be implemented by the same or different physical nodes, and be operated by the same or different actors. Different deployments may incorporate some or all of the functional entities depending on the required functionality in each deployment setting.

From the point of view of digital rights management, the following functional entities have been identified in the architecture:

- DRM Agent

  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.

- Content Issuer

  The content issuer is an entity that delivers DRM Content. OMA DRM defines the format of DRM Content delivered to DRM Agents, and the way DRM Content can be transported from a content issuer to a DRM Agent using different transport mechanisms. The content issuer may do the actual packaging of DRM Content itself, or it may receive pre-packaged content from some other source.

- Rights Issuer

  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.

- User

  A user is the human user of DRM Content. Users can only access DRM Content through a DRM Agent.

- Off-device Storage

  DRM Content is inherently secure, and may be stored by users off-device - for example in a network store, a PC, on removable media or similar. This may be used for backup purposes, to free up memory in a device, and so on. Similarly, Rights Objects that only contain stateless permissions may be stored off-device.

4.2 Functional Architecture

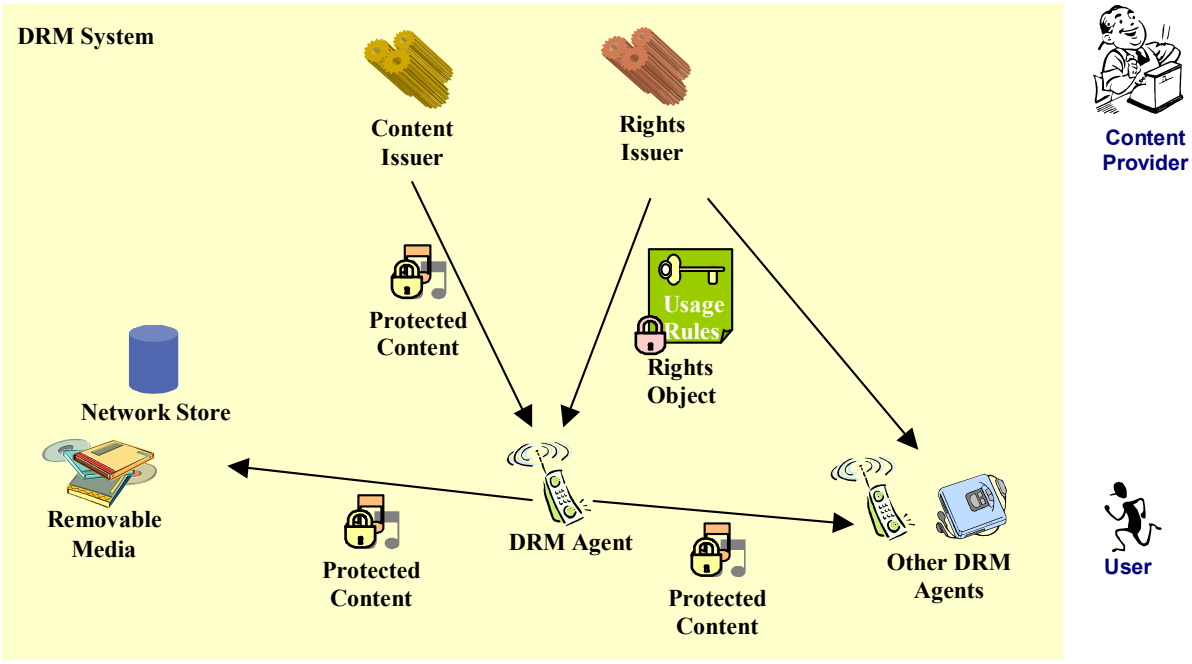

Figure 1. Functional architecture.

Before content is delivered, it is packaged to protect it from unauthorised access. A content issuer delivers DRM Content, and a rights issuer generates a Rights Object. The content issuer and rights issuer embody roles in the system. Depending on deployment they may be provided by the same or different actors, and implemented by the same or different network nodes. For example, in one deployment, content owners may pre-package DRM Content, which is then distributed by a content distributor acting as both content issuer and rights issuer.

A Rights Object governs how DRM Content may be used. It is an XML document specifying permissions and constraints associated with a piece of DRM Content. DRM Content cannot be used without an associated Rights Object, and may only be used according to the permissions and constraints specified in a Rights Object.

OMA DRM makes a logical separation of DRM Content from Rights Objects. DRM Content and Rights Objects may be requested separately or together, and they may be delivered separately or at the same time. For example, a user can select a piece of content, pay for it, and receive DRM Content and a Rights Object in the same transaction. Later, if the Rights Object expires, the user can go back and acquire a new Rights Object, without having to download the DRM Content again.

Rights Objects associated with DRM Content have to be enforced at the point of consumption. This is modelled in the OMA DRM specifications by the introduction of a DRM Agent. The DRM Agent embodies a trusted component of a device, responsible for enforcing permissions and constraints for DRM Content on the device, controlling access to DRM Content on the device, and so on.

A Rights Object is cryptographically bound to a specific DRM Agent, so only that DRM Agent can access it. DRM Content can only be accessed with a valid Rights Object, and so can be freely distributed. This enables, for example, superdistribution, as users can freely pass DRM Content between them. To access DRM Content on the new device, a new Rights Object has to be requested and delivered to a DRM Agent on that device.

If rights issuers support it, a Rights Object may optionally be bound to a group of DRM Agents. This is known in the OMA DRM specifications as a Domain. DRM Content and Rights Objects distributed to a domain can be shared and accessed off-line on all DRM Agents belonging to that domain. For example, a user may purchase DRM Content for use on both her phone and her PDA.

The OMA DRM specifications define the format and the protection mechanism for DRM Content, the format (expression language) and the protection mechanism for the Rights Object, and the security model for management of encryption keys. The OMA DRM specifications also define how DRM Content and Rights Objects may be transported to devices using a range of transport mechanisms, including pull (HTTP Pull, OMA Download), push (WAP Push, MMS) and streaming. Any interaction between network entities, e.g. between rights issuer and content issuer, is out of scope.

4.3 Technical Use Cases

OMA DRM is designed to be flexible and support a wide variety of different business and usage models. This section outlines some technical use cases covered by the specifications. It is not an exhaustive list.

4.3.1 Basic Pull Model

A user selects content to download by browsing to some web site, and confirms the terms of the purchase. The content issuer identifies and protects content (packaging). Device capabilities can be detected using advertised MIME-type support, UAProf, etc.

The rights issuer generates a Rights Object for the content and the target DRM Agent. A Rights Object includes permissions appropriate for the transaction and the content encryption key.

Finally, the Rights Object is protected in a way that makes it accessible only to the target DRM Agent.

DRM Content and the protected Rights Object are then delivered to the DRM Agent.

4.3.2 Push of DRM Content

The basic scenario outlined above is based on a user initiated pull model. An alternative distribution model is to push content directly to a device using MMS, WAP Push or similar, without a preceding discovery process. There are two basic variations on this model:

- Content Push

  The content issuer/rights issuer may have some previous knowledge of a user and a particular DRM Agent, so that content and a Rights Object can be correctly formatted and packaged for delivery. For example, the user may have registered to receive a daily background image to her phone, or the hit song of the week. In this case the process would go through the same steps as above, but delivery of DRM Content and Rights Objects would be over WAP Push or MMS.

- Push-initiated Pull

  In this case, the content issuer/rights issuer has no previous knowledge of a user or the target DRM Agent, but still wishes to send content. For example, one user may buy some content as a gift to another user. In this case, the content provider does not yet know what content is suitable for the receiving device, how trusted the receiving DRM Agent is, and so on. Instead of pushing DRM Content directly, a link to the content can be sent. Following the link will take the receiving user to a specific location, and then the procedure continues as in the basic pull model.

4.3.3 Streaming of DRM Content

The two previous examples assume that content is packaged and delivered in its entirety. Alternatively, content may be packetised and delivered as a stream.

In this case, the stream itself is protected (encrypted). OMA DRM does not specify formats for encrypted streams as other standards bodies are specifying this. Streams may be protected with encryption schemes which are different from those specified by OMA for Download, to address possible packet loss, etc.

Once the stream has been encrypted, access to it can be controlled through the same procedure as described earlier for discrete content. A Rights Object is generated, the encryption key(s) to access the encrypted stream is put in the RO just like a CEK would, and the RO is then bound to a DRM Agent. Without the Rights Object, the protected stream cannot be accessed.

4.3.4 Domains

The basic model of OMA v2 DRM involves binding Rights Objects and content encryption keys to a specific DRM Agent. Domains expand this notion, allowing a rights issuer to bind rights and content encryption keys to a group of DRM Agents instead of just a single DRM Agent. Users may then share DRM Content off-line between all DRM Agents belonging to the same domain.

Using this feature a rights issuer may provide new services such as enabling users to access DRM Content from several devices that they own. Other new scenarios enabled by the Domain concept include support for Unconnected Devices where users purchase DRM Content and rights via one device (e.g. a PC) for later use on another device (e.g. a portable player with no wide area network connectivity).

It is entirely up to the rights issuer if they wish to provide services based on domains, and it is entirely under rights issuer control what DRM Agents form part of a particular domain.

4.3.5 Backup

DRM Content can be stored safely on removable media, in a network store, or in some other form of storage. DRM Content is stored in encrypted form, and so can only be accessed by a particular target DRM Agent using an associated Rights Object.

Rights Objects can be stored for backup purposes if the Rights Object only contains stateless permissions. The security model ensures that the Rights Object is protected and can only be accessed by the intended DRM Agent – even if a Rights Object is stored off-device, it will still only allow the intended DRM Agent to access associated DRM Content.

Some permissions require maintenance of state by the DRM Agent, for example a limited number of plays. Such Rights Objects cannot be stored off-device, as this might result in loss of state information - e.g. current number of plays. A lost or damaged Rights Object may still be restored via the rights issuer by requesting a new Rights Object.

4.3.6 Super Distribution

DRM Content can be safely copied and transferred to other DRM Agents, for example a user sending DRM Content to a friend. In order to access DRM Content, the friend is taken to the rights issuer, by way of a link in the DRM Content package, to acquire a Rights Object. The rights issuer controls whether to release a new Rights Object or not to the new DRM Agent.

4.3.7 Export

DRM Content may be exported to other DRM systems, for use on devices that are not OMA DRM compliant but support some other DRM mechanism – e.g. export to copy protected media. The rights issuer may limit export only to specific external DRM systems.

The OMA DRM architecture allows rights issuers to, if they wish, express permission for DRM Agents to perform conversions to specific other DRM systems. It is expected that other DRM systems will specify how such a conversion is done.

Devices supporting export to other DRM systems must ensure that the content remains protected throughout the export process.

4.3.8 Unconnected Device Support

OMA DRM enables a Connected Device to act as an intermediary to assist an Unconnected Device to purchase and download content and Rights Objects. This functionality enables, for example, a portable, mobile device that does not have inherent network connectivity to acquire DRM Content and associated Rrights Objects. This functionality builds on the Domain concept as described in section 4.3.4..

For example, a user has an OMA DRM compliant portable device (Unconnected Device) that has no wide area network connectivity, and an OMA DRM compliant mobile device (Connected Device) that has wide area network connectivity. She uses the Connected Device to browse and purchase DRM Content, and download the DRM Content to the Connected Device.

If the user wishes to render the DRM Content on the Unconnected Device then the DRM Agent on the Connected Device requests and downloads a Domain Rights Object from the rights issuer. The DRM Agent on the Connected Device then embeds the Domain Rights Object in the DCF. The DCF (with embedded Domain RO) can then be transferred to the Unconnected Device using an appropriate protocol over a local connectivity technology e.g. OBEX over IrDA, Bluetooth or USB.

Using intermediaries in this way can be useful if the Unconnected Device has a limited UI. Both the Connected and Unconnected Device must be OMA DRM compliant. Since the Unconnected Device support is built upon the Domain concept then the Unconnected Device must also belong to the same Domain as the Connected Device. In order to join the Domain the Connected Device can provide network connectivity to enable the Unconnected Device to perform the steps required to join a Domain.

5. Trust and Security Model

The fundamental challenge facing any DRM solution is how to ensure that permissions and constraints associated with DRM Content are enforced. The main threat comes from unauthorised access to DRM Content beyond what is stipulated by the associated Rights Objects, or creation of illegal copies and redistribution of valuable content such as music and games.

Rights Objects and DRM protection are enforced at the point of consumption. This is modelled in the OMA DRM specifications by the introduction of a DRM Agent. The DRM Agent embodies a trusted environment within which DRM Content can be securely consumed. Its role is to enforce permissions and constraints and to control access to DRM Content.

5.1 Overview

The basic steps for distributing DRM Content can be summarised as follows:

1. Content packaging: Content is packaged in a secure content container (DCF). DRM Content is encrypted with a symmetric content encryption key (CEK). Content can be pre-packaged, i.e. content packaging does not have to happen on the fly.

   Although not required by the OMA DRM specifications or the OMA DRM architecture, it is recommended that the same CEK is not used for all instances of a piece of content. Using the same CEK for all content instances would pose a greater risk if a single device was to be hacked and a CEK stored on that device exposed. Using a different CEK for different deliveries or different devices will limit this risk.

2. DRM Agent authentication: All DRM Agents have a unique private/public key pair and a certificate. The certificate includes additional information, such as maker, device type, software version, serial numbers, etc. This allows the content and rights issuers to securely authenticate a DRM Agent. Any privacy aspects with releasing such information are addressed in the technical specifications.

3. Rights Object generation: A Rights Object is an XML document, expressing the permissions and constraints associated with the content. The Rights Object also contains the CEK – this ensures that DRM Content cannot be used without an associated Rights Object.

4. Rights Object protection: Before delivering the Rights Object, sensitive parts are encrypted (e.g. the CEK), and the Rights Object is then cryptographically bound to the target DRM Agent. This ensures that only the target DRM Agent can access the Rights Object and thus the DRM Content

   In addition, the RI digitally signs the RO.

5. Delivery: The RO and DCF can now be delivered to the target DRM Agent. Since both are inherently secure, they can be delivered using any transport mechanism (e.g. HTTP/WSP, WAP Push, MMS). They can be delivered together, e.g. in a MIME multipart response, or they can be delivered separately.

5.2 Trust Model

The DRM Agent has to be trusted by the rights issuer, both in terms of correct behaviour and in terms of a secure implementation. In OMA DRM, each DRM Agent is provisioned with a unique key pair, and an associated certificate, identifying the DRM Agent and certifying the binding between the agent and this key pair. This allows rights issuers to securely authenticate the DRM Agent using standard PKI procedures.

The information in the certificate enables the Rights Issuer to apply a policy based on its business rules, the value of its content, etc. For example, a rights issuer may trust certain manufacturers, or it may keep an updated list of DRM Agents that are known to be good or bad according to some criteria defined by the rights issuer. It is also possible for a group of stakeholders to establish a joint authority identifying trusted DRM Agents, with legally binding compliance rules.

Revocation in this model amounts to not distributing content any more to DRM Agents that are no longer considered trusted. What constitutes a trusted DRM Agent depends on the policy and business model of rights issuers. For example, if a hack or a fault compromises a whole class of devices, a rights issuer may decide to stop distributing new content to all devices of that type or class. This is a worst-case scenario. At the other end of the spectrum, maybe there is a known bug in devices of a

certain type, but the risk of content leaking is relatively small. In such cases, content and rights issuers may choose to continue to deliver content to existing devices, and instead let manufacturers correct the problems in future versions. Either way, the secure mechanism for authenticating DRM Agents enables rights issuers to enforce such policies.

5.3 Content Protection

The DRM Content Format (DCF) is a secure content package for encrypted content, with its own MIME content type. In addition to the encrypted content it contains additional information, such as content description (original content type, vendor, version, etc.), rights issuer URI (a location where a Rights Object may be obtained), and so on. This additional information is not encrypted and may be presented to the user before a Rights Object is retrieved.

Since a DCF is inherently secure, it can be transported using any transport protocol, e.g. in an HTTP response or in an MMS message. It can be stored for back-up on any kind of storage, e.g. removable media or a networked PC. It can be copied and sent to another DRM Agent, where a Rights Object may be acquired for use on the receiving device (superdistribution).

The content encryption key needed to unlock DRM Content inside a DCF is contained within a Rights Object. Thus it is not possible to access DRM Content without a Rights Object. DRM Content can only be used as specified in a Rights Object.

OMA DRM includes a mechanism allowing a DRM Agent to verify the integrity of a DCF, protecting against modification of the content by some unauthorised entity.

5.4 Rights Object

Rights Objects are used to specify consumption rules for DRM Content. The Rights Expression Language (REL) defined by OMA DRM specifies the syntax (XML) and semantics of permissions and constraints governing the usage of DRM Content. An instance of a rights document is called a Rights Object, and has its own MIME content type.

Rights Objects are made up of permissions (e.g. play, display and execute) and constraints (e.g. play for a month, display ten times) – see [OMA REL]. Rights Objects may also include constraints that require a certain user (user identity) to be present when the content is used. These permissions and constraints, along with other information embodied in the Rights Object, (e.g. copyright information) may be presented to the user. The Rights Object also governs access to DRM Content by including the content encryption key (CEK).

A single Rights Object may be associated with multiple pieces of DRM Content. Further, it is possible to assign different permissions to different components of a composite object.

Conversely, a single piece of DRM Content may be associated with multiple Rights Objects. If there are multiple Rights Objects associated with a piece of DRM Content, each Rights Object is treated individually – Rights Objects are not combined. This means that at any one time, there may be more than one Rights Object whose constraints are satisfied. When this is the case, the DRM Agent selects one to enforce. This selection may be made automatically by the DRM Agent based on some selection criteria, e.g. picking the least restrictive Rights Object, or it may be done based on user interaction.

5.5 Rights Object Protection

A Rights Object is protected using a rights encryption key (REK). The REK is used to encrypt sensitive parts of the Rights Object, such as the CEK. In addition, the RO is digitally signed by the RI.

During delivery, the REK is cryptographically bound to the target DRM Agent. In this way only the target DRM Agent can access the Rights Object, and thus the CEK.

Since a protected Rights Object is inherently secure, it can be copied and stored off-device for backup purposes. Some permissions require maintenance of state by the DRM Agent, for example a limited number of plays. Rights Objects containing such permissions cannot be copied or stored off-device, if this would result in loss of state information - e.g. current number of plays.

5.6 Other Security Aspects

The building blocks described above address the main security issues of protecting content and Rights Objects from unauthorised access. In addition, OMA DRM addresses a number of other security aspects, including:

- Rights Issuer Authentication

  Rights issuers are required to authenticate themselves to the DRM Agent during delivery of Rights Objects. This gives some level of assurance about the authenticity of the rights issuer.

- Rights Object Replay Protection

  An example of Rights Object replay would be if an intermediary intercepts a Rights Object with a limited number of plays during delivery to the DRM Agent. When the rights run out on the DRM Agent, the intercepted Rights Object might be delivered again (replayed) from the intermediary. OMA DRM prevents this and similar attacks from occurring.

- DRM Time

  Some constraints (absolute time constraints), as well as some aspects of the delivery protocol for Rights Objects, rely on the DRM Agent having a secure time source. DRM Time in the context of the OMA DRM specifications means accurate as well as not changeable by users. Since users are not able to change the DRM AgentTime, the OMA DRM specifications provide mechanisms for the DRM Time to be synchronised when necessary, e.g. if DRM Time is lost after prolonged power failure. Due to the limited capabilities of some Unconnected Devices, Unconnected Device may not support a real time clock and therefore will not support DRM Time. Within OMA DRM Connected Devices must support DRM Time.

6. Use Cases

The DRM Trust Model required by this specification is based on the Public Key Infrastructure (PKI). In this model, typically, there are groups of principals, verifiers and one or more authentication authorities recognized and trusted by both. A single entity can play both as a principal and a verifier depending on the needs of the solution being crafted. The overall purpose of the infrastructure is to enable a verifier to authenticate the identity and other attributes of a principal when they communicate over an open, unsecured network. In such a system, typically, the verifier does not have to maintain any sensitive information about the principals it interacts with, for the purposes of authentication. In addition, the CA is not directly involved in transactions between principal and the verifier.

The primary entities of the trust model as it is specified in this specification are the CAs, Devices and Rights Issuers. The authentication and key transfer protocols developed require Rights Issuer to be able to authenticate the Device and the Device to be able to authenticate the Rights Issuer. Mutual authentication is accomplished by the Rights Object Acquisition Protocol (ROAP).

- It is assumed that devices are provisioned (either at manufacturing time or later) with Device public and private keys and associated certificates signed by an appropriate CA. A Device manufacturer could be a CA by itself in order to sign the certificates.
- The Device can be provisioned with more than one certificate. Based on the certificate preferences expressed by the Rights Issuer, the Device has to provide an appropriate certificate.
- It is also required that the Device stores the private keys in local storage with integrity and confidentiality protection.
- The Rights Issuers are also provided with public and private keys and certificates. The certificates would be signed by a CA. The certificate chain is presented to the Device at the time of the authentication protocol so that the Device can validate the certificate path.
- There could be multiple CAs in this system. This specification does not mandate a specific trust model such as a hierarchical trust model or a bridge trust model. The exact nature of these trust models is left up to the marketplace decisions.
- The ROAP protocol also requires that the CA who signs the Rights Issuer certificates runs an OCSP responder for use during the execution of the protocol.
- The CAs are also required to define the appropriate certificate policies to govern the use of the issued certificates.

Irrespective of the deployment configurations, the Media Objects are packaged and delivered to users in a protected and controlled manner. The content issuer delivers DRM Content from a portal to the Device. The Rights Issuer authenticates the Device and provides the necessary Rights Objects so that the content can be used. The DRM Agent on the Device participates in the authentication protocol and implements the necessary security and trust elements so that the Rights Objects are utilized in a conforming manner.

The Rights Objects govern the usage of the DRM Content by specifying the permissions and constraints as needed. These Rights Objects are also protected by encryption such that only the target devices obtain access to the DRM Content.

Within the OMA DRM, the DRM Content and Rights Objects are separate entities. But, they are logically associated with each other and this association is protected. The DRM Content and Rights Objects can arrive at the Device in a number of ways – over the air, through local connectivity, through both push and pull mechanisms, etc. The system does not specify any ordering or sequence for the delivery of these objects to the Device either.

One of the fundamental functions of the DRM Agent is to enforce the permissions specified in the Rights Object during content usage. It is required that the secrets and keys that are part of the system security are protected and handled such that un-authorized use is avoided.

The OMA DRM specifies the content formats, rights expression language, authentication/authorization protocols, and protection mechanisms. OMA DRM also specifies how DRM Content and Rights Objects can be transported to devices using a number of transport mechanisms. The following sections describe some example models for content distribution and consumption that are supported by these specifications.

6.1 Basic Download

One model for content distribution is using OMA OTA Download mechanisms. The client would launch a browser and connect to a Content Issuer portal. The user would evaluate the content offerings from this portal and make a decision on specific items of content to be downloaded. Once the DRM Content is downloaded, the client can connect to the Rights Issuer portal and engage in the Rights Object Acquisition Protocol to acquire the associated rights. Another model is based on subscription. The subscriber can get DRM Content and Rights Objects pushed to the Device on a regular interval. The third model shown in this picture is one of subscription with the Device invoking the rights acquisition silently as needed. The flow of events between the significant actors of the scenarios is illustrated below.

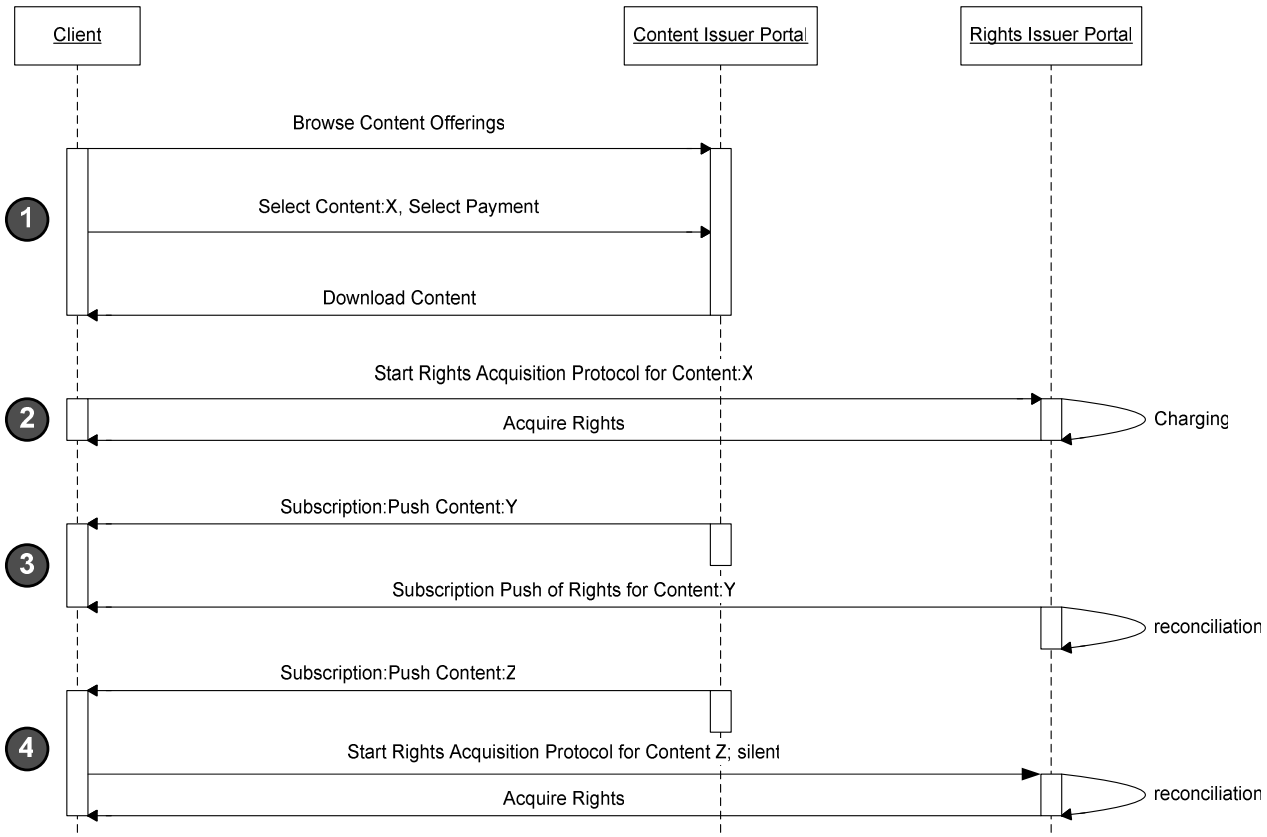

Figure 2: Basic Download - Pull and Push Models

1. The client initiates a browsing session with the Content Portal. The client selects the specific content from the content offerings on the portal. In addition, the client may select the payment mode during this session. Subsequently, the client downloads the DRM Content from the portal to local storage.

2. The client looks up the Rights Issuer URL within the DRM Content headers and initiates a connection to the Rights Issuer portal. And engages in the Rights Object Acquisition Protocol. The client, at the successful completion of this protocol, acquires the Rights Object associated with the DRM Content.

3. Another scenario shown in this picture is the subscription push of both content and rights. In this model, the client has an established subscription and charging agreement with the Rights Issuer in place. As a result of this, the Rights Issuer can push both DRM Content and Rights Objects to the clients on a regular interval.

4. Another scenario shown in this picture is the subscription based push that in turn initiates a pull of the Rights Object from the Rights Issuer Portal. The DRM Content is delivered with the 'silent' header ("in-advance") and the Client, on reception of the content, connects to the Rights Issuer to trigger the Rights Object Acquisition Protocol. On completion of this protocol successfully, the Rights Object is issued to the client.

6.2 Super Distribution

A given client who has downloaded content from a Content Issuer can in turn distribute this DRM Content to other devices using various networked links as well as removable media. This DRM Content is encrypted and is not usable by the receiving device/user until the associated rights are acquired for the content. The device that receives this super-distributed content will discover the Rights Issuer URL within the DRM Content headers and use this information to connect to the Rights Issuer portal to acquire the rights. The interaction diagram below illustrates this model of content distribution and the related flow of events amongst the significant actors.

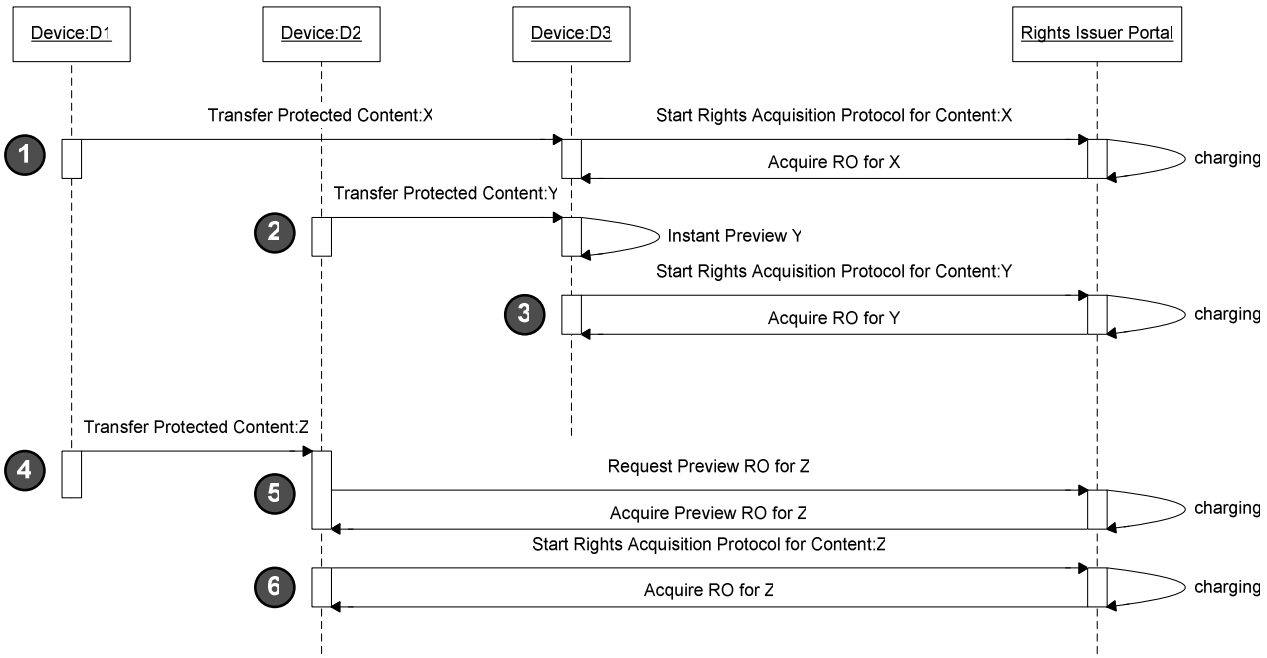

Figure 3: Super Distribution

1. Device D1 has previously received some DRM Content and has it stored locally. Device D1 wants to share this DRM Content with Device D3, and as a result, transfers this to D3 using local connectivity or removable media. Device D3, on reception of this DRM Content, discovers the Rights Issuer URL from the DRM Content headers and initiates a Rights Object Acquisition Protocol session with the Rights issuer. On completion of this protocol and appropriate payment arrangements, the device D3 obtains the Rights Object associated with DRM Content X. Now, the user of device D3 is able to use this content.

2. Device D2 transfers DRM Content Y to device D3. This DRM Content Y has the 'preview' headers and is able to provide an 'instant preview' for the content within it. The device D3 can make the 'preview' available to the user and the user can make a decision regarding the content purchase.

3. Once the user of device D3 has decided to purchase the rights for content Y, it initiates the Rights Object Acquisition Protocol with the Rights Issuer. On successful completion of this protocol, the device D3 obtains the Rights Object for DRM Content Y.

4. Device D1 transfers DRM Content Z to device D2.

5. On reception of this DRM Content Z, the device D2 discovers that this content can provide a preview if the device obtains a preview Rights Object. As a result, the device D2 connects to the Rights Issuer and obtains the Rights Object to enable a preview. Rights Objects provided are full-fledged Rights Objects, the only difference being that the permissions and constraints are specified to just enable a preview. This may or may not result in charging, depending on the business model.

6. Once the user decides to purchase the rights, the device D2 starts a Rights Object Acquisition Protocol session to acquire rights for content Z. On successful completion of the protocol, the Rights Object for Z is obtained by the device.

6.3 Streaming Media

For distributing protected streams, the streaming token[1] is acquired from the Content Issuer portal and the access to the streams is governed by the associated Rights Object. The client, after receiving the session headers, can connect to the Rights Issuer and acquire the necessary Rights Object, which in turn will provide the necessary information for the client to be able to decode the streams and render the content. The interaction diagram below illustrates the flow of events and the technical elements necessary for this solution.

[1] A streaming token is a piece of data that the streaming player uses to determine the location of streaming media, possibly also to determine properties of the streaming session or streams, and to set up and start the delivery of streaming media. For the 3GPP Packet-Switched Streaming Service for example, this can either be a SMIL presentation, an SDP session description, or an RTSP URL.

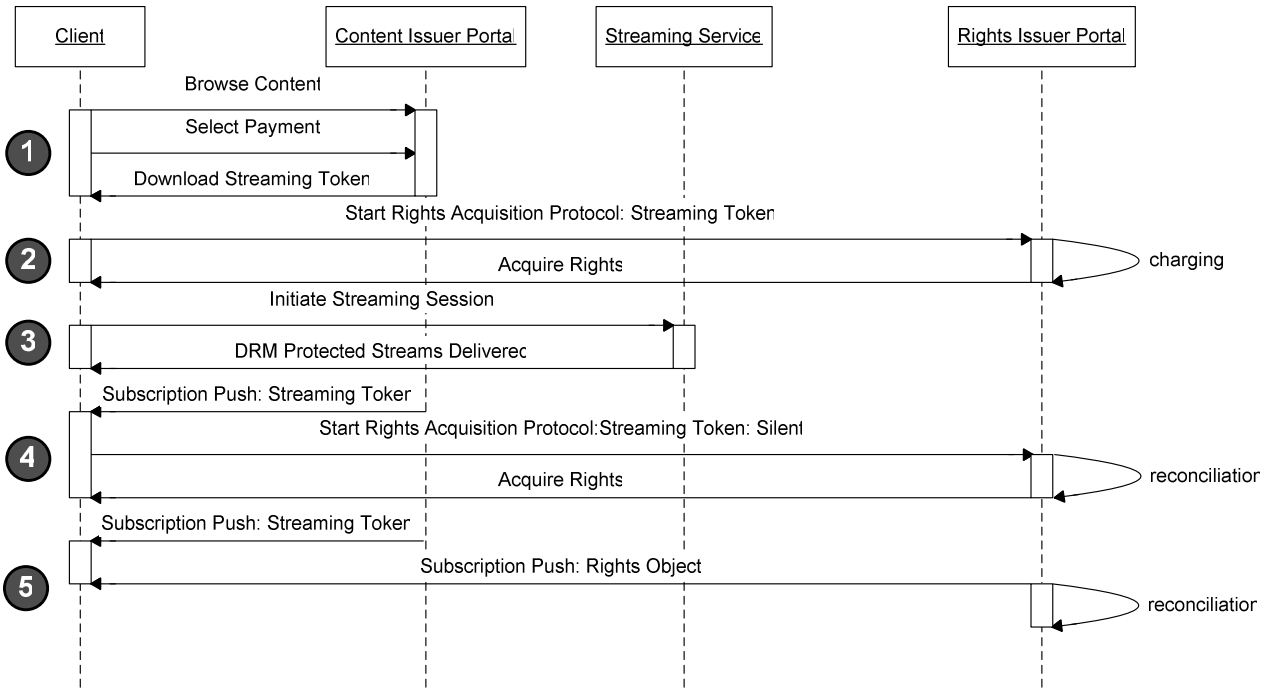

Figure 4: DRM Protected Streaming Service

1. The client connects to the Content Issuer portal and browses for content of interest. Client selects the streaming service of interest, possibly indicates the payment mode, and downloads the streaming token.

2. The Client requests rights by connecting to the Rights Issuer and initiating the Rights Object Acquisition Protocol to acquire the rights for the streamed content. On successful completion of the protocol, the client obtains the Rights Object for the streaming service.

3. The Client connects to the Streaming server and initiates the streaming session. After the stream is initiated, the Client will have the stream properties available. The DRM properties will be included in these stream properties (except for the case of an SDP description token, where the properties are already contained in the token).

4.

5. The client connects to the Streaming server and resumes the streaming session. And, the Protected Streams are delivered to the client.

Push rights

1. Another mode of delivering streaming services is when the rights are delivered in advance or along side the streaming token.

2. The client can then connect to the streaming server and initiate the streaming session. The DRM Agent will have rights so the client will be able to immediately start the streaming session instead of going through step 3 above.

6.4 Domains

This specification also allows the distribution of content to a group of devices that are enrolled in a domain, which is created, managed and administered by a Rights Issuer. Once the domain is formed and the devices are enrolled in the domain, content and rights distributed to any of the devices in the domain can be shared among the other devices in the domain without connecting back to the Rights Issuer. Alternatively, a device can join a desired domain on reception of content that is targeted for a domain.

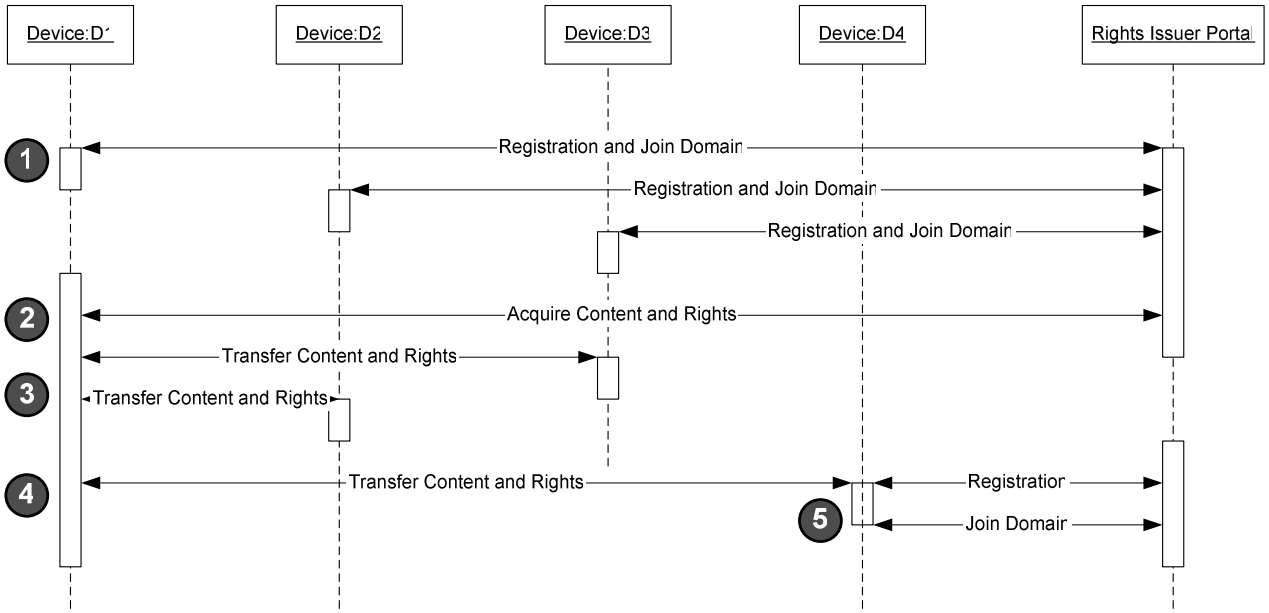

Figure 5: Domains

1. In the scenario illustrated above, each of the devices D1, D2, and D3 connect to the RI and complete the registration and join a domain DM1.
2. At a later time, device D1 connects to the RI and acquires content DCF1 and the associated domain RO for the DCF, DRO1. Now since the device D1 is part of the domain DM1, the content and rights are usable on this device.
3. Subsequently, the device D1 forwards the content and the associated domain RO to the other devices D2, & D3.
4. Since D2 & D3 are part of the domain DM1, the content and associated rights are immediately usable on those devices without connecting to the RI.
5. At a later time, content is also forwarded to device D4. This device D4 has not joined the domain DM1. As a result, the content is not usable on this device. The user can choose to connect to the RI and join the domain DM1 to gain access to this content. Since the domain management is conducted by the RI, the RI can explicitly decide on the composition of the domain and decide on whether D4 can join the domain or not.

6.5 Export

DRM Content may be exported to some other DRM system, for use on devices that are not OMA DRM compliant but support some other DRM mechanism – e.g. export to copy protected media. The rights issuer may limit export only to specific external DRM systems.

The capabilities of the other DRM system can be provided to the Content Portal so the downloaded content and rights are compatible with the target DRM system. This downloaded content is stored and managed on the original device for later

export to a consuming device. OMA DRM does not define how to translate from OMA DRM to other protection mechanisms. It merely allows Rights Issuers to, if they wish, express permission for DRM Agents with such a capability to do so.

The interaction diagram below illustrates the flow of content and rights in this model.

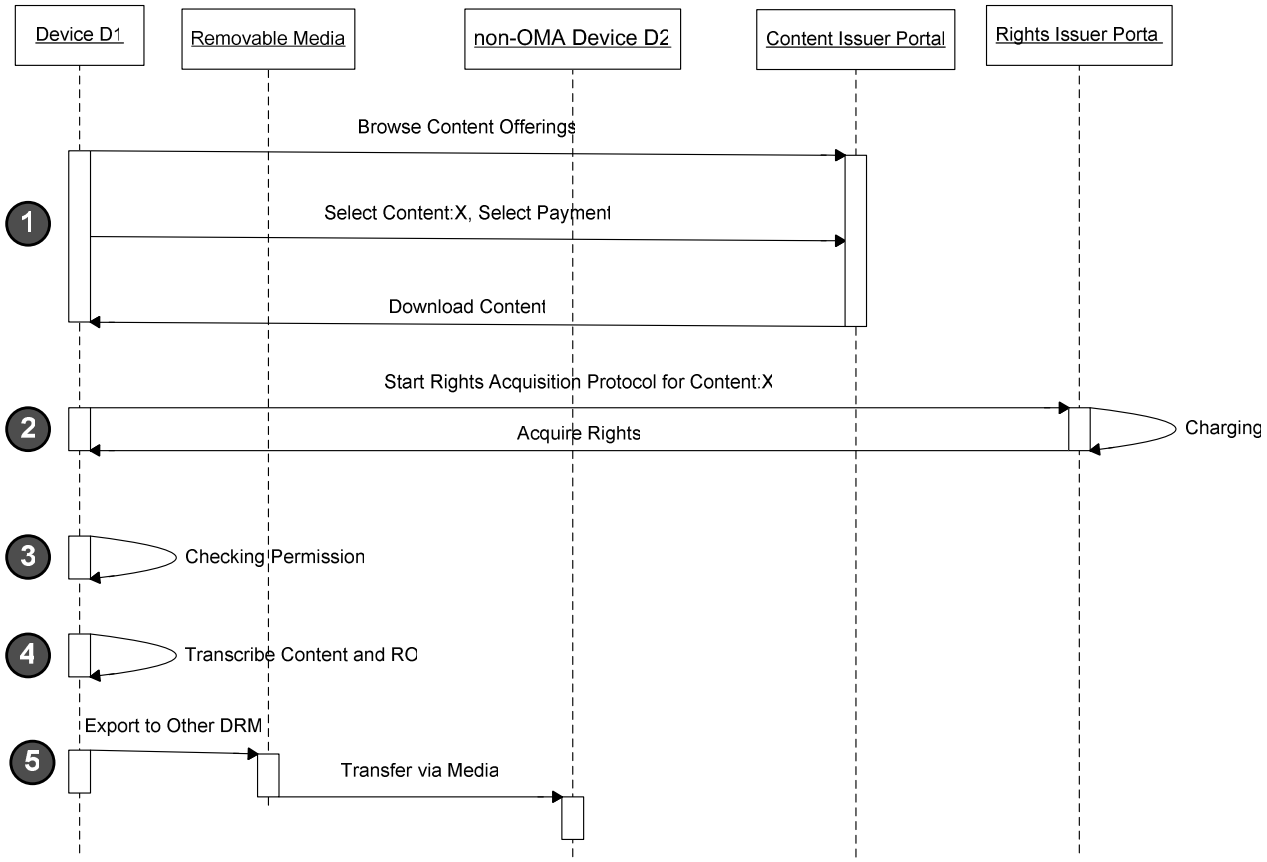

Figure 6: Export

1. The client initiates a browsing session with the Content Portal. The client selects the specific content for future export from the content offerings on the portal. The content should be suitable for the target DRM system. Subsequently, the client downloads the DRM Content from the portal to local storage.
2. Device D1 now connects to the RI to acquire the rights for the content. The rights issued are compatible with the usage rules of the target DRM system.
3. The User wants to transfer the DRM Content to Device D2 that has a different (non-OMA) DRM system using local connectivity or removable media. The OMA DRM Agent checks the permissions described in the Rights Object to determine whether the Rights Issuer allows the content to be exported to the target DRM system, whether its content type is appropriate, and whether its usage rules are compatible with the target DRM system.
4. The OMA DRM Agent transfers the decrypted content and Rights Object to the other (non-OMA) DRM Agent. The other DRM Agent transcribes the compatible rights to the other DRM usage rules according to the specific rules defined by the Rights Issuer and the other DRM system to maintain consistency with the original Rights Object.
5. The User is now able to securely use this content on Device D2.

6.6 Unconnected Device Support

DRM Content and Rights Objects can be distributed to Unconnected Devices using a Connected Device. In this model both the Connected Device and the Unconnected Device need to belong to the same Domain. A Connected Device such as a mobile device with wide area network connectivity can connect to a Content Issuer's portal using available network connections and download DRM Content in the form of a DCF. Once the DRM Content is downloaded Domain Rights Object can be purchased. The downloaded DCF and associated Domain Rights Object are stored and managed on the Connected Device for later transfer to the consuming Unconnected Device. The Connected Device can embed the Domain RO in the DCF to enable other Devices within the Domain to access the content once they receive the DCF.

At a later point in time the DCF can be transferred to an Unconnected Device. At this point no connection to the Rights Issuer is required in order for the Unconnected Device to render the content, since the DCF contains a Domain RO for the DRM Content

The interaction diagram below illustrates the flow of content and rights in this model.

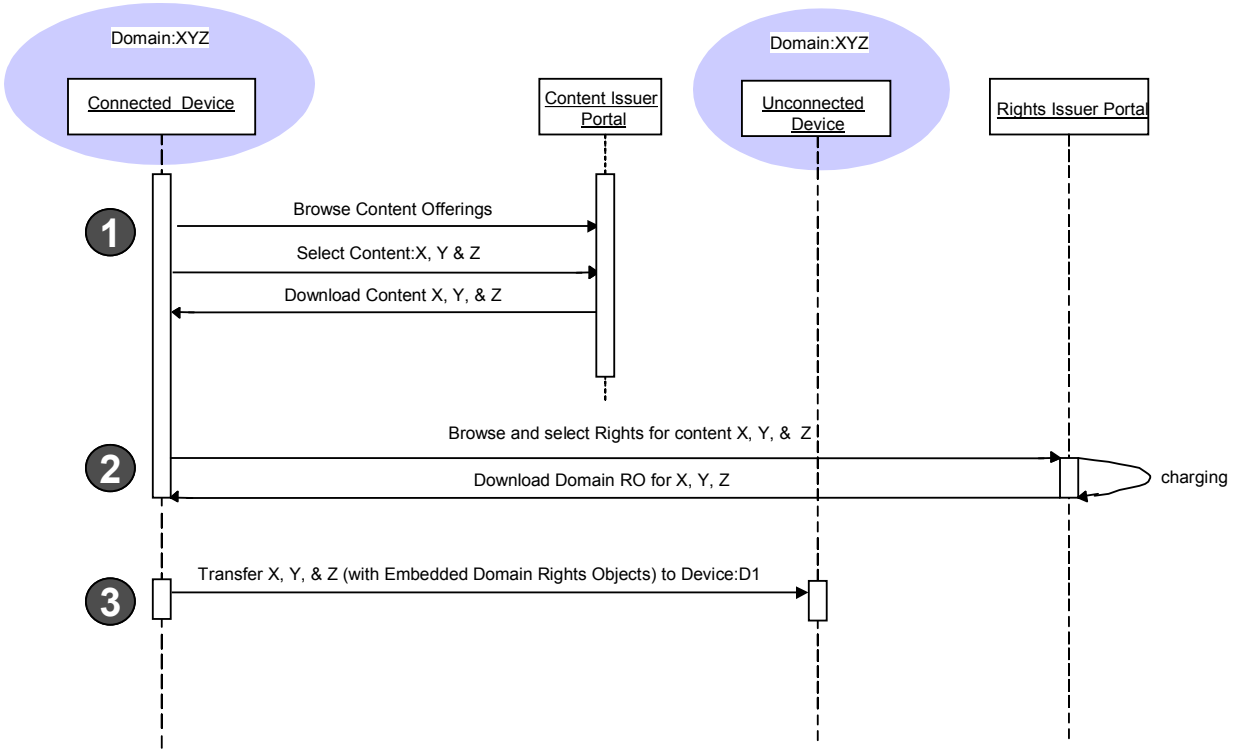

Figure 7: Store & Forward

1. The Connected Device connects to the Content Issuer portal. After a browsing session to select the content, The DRM Content X, Y, & Z are downloaded to the Connected Device.

2. The Connected Device now connects to the RI to acquire Domain Rights Objects for the content X, Y, & Z. The Connected Device embeds the Domain Rights Objects inside the corresponding DCF.

3. At a later time, the Connected Device transfers the DRM Content X, Y, & Z (with embedded Domain Rights Objects) to Unconnected Device over a local connection.

Appendix A. Change History (Informative)

A.1 Approved Version History

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

A.2 Draft/Candidate Version 2.0 History

Document Identifier	Date	Sections	Description
Candidate Versions OMA-DRM-ARCH-V2_0	20 August 2004		Initial candidate version