OMA DRM Requirements

Version 2.0

Version 15-May-2003

Open Mobile Alliance

OMA-DRM-REQ-v2_0-20030515-C

A list of errata and updates to this document is available from the OMA ™ Web site, http://www.openmobilealliance.org/, in the form of SIN documents, which are subject to revision or removal without notice.

The Open Mobile Alliance™ assumes no responsibility for errors or omissions in this document. In no event shall the Open Mobile Alliance be liable for any special, indirect or consequential damages or any damages whatsoever arising out of or in connection with the use of this information.

Open Mobile Alliance™ members have agreed to use reasonable endeavors to disclose in a timely manner to the Open Mobile Alliance the existence of all intellectual property rights (IPR's) essential to the present document. However, the members do not have an obligation to conduct IPR searches. The information received by the members is publicly available to members and non-members of the Open Mobile Alliance and may be found on the “OMA IPR Declarations” list at http://www.openmobilealliance.org/ipr.htm. Essential IPR is available for license on the basis set out in the schedule to the Open Mobile Alliance Application Form.

No representations or warranties (whether express or implied) are made by the Open Mobile Alliance™ or any Open Mobile Alliance member or its affiliates regarding any of the IPR's represented on this “OMA IPR Declarations” list, including, but not limited to the accuracy, completeness, validity or relevance of the information or whether or not such rights are essential or non-essential.

This document is available online in PDF format at http://www.openmobilealliance.org/.

Known problems associated with this document are published at http://www.openmobilealliance.org/.

Comments regarding this document can be submitted to the Open Mobile Alliance™ in the manner published at http://www.openmobilealliance.org/documents.htm.

Document History	
OMA-DRM-REQ-v2_0-20030515-C-C	Current

Contents

1. Scope

A number of DRM specifications have already been defined within the OMA. See [DRM], [DRMCF] and [DRMREL]. These existing specifications are referred to within this document as “release 1”.

This document defines the requirements for a further release of DRM specification within OMA that is referred to as “release 2”. It was stated in [DLARCH], “A complete DRM technology is, however, **not** in scope of WAP Download”. This statement reflects the comparably low level of security of OMA DRM Release 1 due to the lack of a key management infrastructure. Release 2 does not claim to be “complete”. However, release 2 will provide the security that was left out of release 1 and will also address additional user requirements.

Both Release 1 and Release 2 requirements in this document are requirements on Release 2 implementations.

Requirements on mobile Devices that support the processing of Protected Content are defined.

Requirements on servers that MAY distribute Protected Content to mobile Devices are stated with respect to their correct functioning when communicating with mobile Devices supporting DRM only.

2. References

2.1 Normative References

[CREQ] “Specification of WAP Conformance Requirements”. Open Mobile Alliance™. WAP-221-CREQ. http://www.openmobilealliance.org/

[RFC2119] “Key words for use in RFCs to Indicate Requirement Levels”. S. Bradner. March 1997.http://www.ietf.org/rfc/rfc2119.txt

[RFC2234] “Augmented BNF for Syntax Specifications: ABNF”. D. Crocker, Ed., P. Overell. November 1997. http://www.ietf.org/rfc/rfc2234.txt

[RFC2396] “Uniform Resource Identifiers (URI): Generic Syntax”, T. Berners-Lee, R. Fielding, U.C. Irvine, L. Masinter. August 1998. http://www.ietf.org/rfc/rfc2396.txt

[DRM] “Digital Rights Management”, Open Mobile Alliance™, OMA-Download-DRM-v1_0, http://www.openmobilealliance.org/

[DRMCF] “DRM Content Format”, Open Mobile Alliance™, OMA-Download-DRMCF-v1_0, http://www.openmobilealliance.org/

[DLARCH] OMA-Download-DLARCH-V1_0

[DRMREL] “DRM Rights Expression Language”, Open Mobile Alliance™, OMA-Download-DRMREL-v1_0, http://www.openmobilealliance.org/

[3GPP PSS] Transparent end-to-end packet switched streaming service (PSS); 3GPP 26.234; Protocols and codecs - Release 5. http://www.3gpp.org/

[BT AVDTP] Bluetooth Audio/Video Distribution Transport Protocol, Version 1.00

[BT AVCTP] Bluetooth Audio/Video Control Transport Protocol, Version 1.00

[BT GAVDP] Bluetooth Generic Audiovisual Distribution Profile, Version 1.00

2.2 Informative References

[WAPARCH] “WAP Architecture”. Open Mobile Alliance™. WAP-210-WAPArch. http://www.openmobilealliance.org/

[3GPPDRM] “Digital Rights Management; Proposed Stage 1”. 3rd Generation Partnership Program, 3G TS 22.242. Version 1.0.0. http://www.3gpp.org/

[ISO 7498-2]] ISO/IEC 7498: Information processing systems -- Open Systems Interconnection -- Basic Reference Model - Part 2: Security Architecture

[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 (2002-08-08), http://odrl.net

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, except appendices, "Scope", and "Introduction" are normative, unless they are explicitly indicated to be informative.

3.2 Definitions

Backup Defines an action for duplicating a Media Object and/or Rights Object and transferring them to another location that is not a Device.

Billing Service Provider The entity responsible for collecting payment from a User.

Combined Delivery A Release 1 method for delivering Protected Content and Rights Object. The Rights Object and Protected Content are delivered together in a single entity, the DRM Message.

Composite Object A Media Object that contains one or more Media Objects by means of inclusion e.g. DRM messages, zip files.

Confidentiality The property that information is not made available or disclosed to unauthorised individuals, entities or processes. (From [ISO 7498-2])

Content One or more Media Objects

Content Issuer The entity making content available to the DRM Agent; the entity whose Content is being Protected.

Content Provider An entity that is either a Content Issuer or a Rights Issuer.

Content subscription A subscription that a User has with a Content Provider for the purposes of paying for Protected Content purchased from that Content Provider and played on a Users Device.

Copy To make a perfect reproduction of Protected Content or a Rights Object.

Device A Device is a user equipment with a DRM Agent. The Device MAY include a smartcard module (e.g. a SIM) or not depending upon implementation.

DRM Agent The entity in the Device that manages Permissions for Media Objects on the Device.

DRM Message A message containing a Media Object and optionally, a Rights Object. Media objects received inside a DRM Message must not leave the Device. The optional Rights Object defines Permissions for the Media Object.

Enable To make a resource (Media Object) capable of being interacted with. When applied to a digital resource, Enable results in a change in an existing resource such that it becomes capable of being read, written to or executed. Enabling MAY be partial and/or contextual. (From [MPEG21 RDD])

Execute To execute a software programme

Forward Lock A special case of the Combined Delivery method where the DRM Message includes only the Media Object and not a Rights Object at all. A set of default Permissions applies to the Media Object.

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 Protected Content and encrypted Rights Objects on behalf of a Device for Backup.

OMA DRM Conformant A Device that will work interoperably with other OMA DRM Conformant Devices and some or all

Device of the following; Billing Service Providers, Content Providers and Network Service Providers. It will also enable Protected Content on the Device only if the Device possesses a valid Rights Object (or implied Rights Object i.e. forward lock) for that instance of Protected Content and only according to the Permissions defined in the Rights Object for that instance of Protected Content.

Permission Actual usages or activities allowed (by the Rights Issuer) over Protected Content (From [ODRL 1.1])

Play To create a transient, perceivable rendition of a resource (From [MPEG21 RDD])

Print To create a fixed and directly perceivable rendition of a resource (From [MPEG21 RDD])

Protected Content Media Objects that are consumed according to a set of Permissions in a Rights Object.

Restore Defines an action for duplicating a Media Object and/or Rights Object, transferring it back to the Device from which it was Backed up and then deleting the Rights Object from the backup location if applicable. .

Revoke A Device has been Revoked by a particular Rights Issuers if that Rights Issuers has decided it does not wish to issue Rights Objects to that Device (for example, because it has concerns about the robustness of the Device's implementation).

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 Protected Content.

Separate Delivery A Release 1 method for delivering Protected Content and Rights Object. The Rights Object and Protected Content are delivered separately, over different transport mechanisms..

Superdistribution A mechanism that (1) allows a User to distribute Protected Content to other Devices through potentially insecure channels and (2) enables the User of that Device to obtain a Rights Object for the superdistributed Protected Content.

Transfer To relocate Protected Content or a Rights Object from one place to another.

Unprotected Content Content which is not Protected Content.

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
DRM	Digital Rights Management
DVD	Digital Versatile Disc
HTTP	HyperText Transfer Protocol
ISO	International Standards Organisation
LAN	Local Area Network
MMS	Multimedia Messaging Service
MPEG	Moving 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
RFC	Request For Comments
SCR	Static Conformance Requirement
SIM	Subscriber Identity Module
SMS	Short Messaging Service
URI	Uniform Resource Indicator

4. Introduction

Digital Rights Management (DRM) enables the consump tion by Users of protected content by allowing Content Providers to express Permissions, e.g., the ability to preview Protected Content, and by specifying how Devices should observe these Permissions.

This requirements specification document builds on the work in the release 1 DRM specifications and in total provides:

- The scenarios that we wish to enable with release 2 (section 5)
- The high level market requirements derived from the scenarios (section 6)
- The security requirements applying to the technical solution (section7.1)
- The charging requirements applying to the technical solution (section 7.2)
- The requirements relating to streaming applying to the technical solution (section 7.3)
- The requirements relating to superdistribution applying to the technical solution (section 7.4)
- The requirements relating to storage and back up of rights and content applying to the technical solution (section 7.5)
- The requirements relating to rights applying to the technical solution (section 7.6)
- The requirements relating to User privacy applying to the technical solution (section 7.7)
- The requirements relating to terminals and smartcards (that are not covered implicitly or explicitly elsewhere in the document) applying to the technical solution (section 7.9)
- The requirements relating to usability applying to the technical solution (section 7.12)
- The requirements relating to interoperability and backwards compatibility applying to the technical solution (section 7.13)

5. Description (Informative)

5.1 Introduction

This section is intended to describe in the form of user scenarios the types of services which customers will require when they come to have access to a wider range of content. The scenarios are based upon a student although many of the principles will apply to older users and potentially to younger ones as well. The examples given try not to relate to any particular mobile operator, Content Provider or Device manufacturer (although several are mentioned) and are given to help understand the actual way in which users MAY want to deal with content distributed to mobile Devices in the future. Some of the user cases MAY be seen as being too difficult or MAY mandate a particular business model. This is not intentional and MAY lead to the scenarios changing to reflect an easier solution or an enlarged business solution.

Simply, the purpose of this section is:

- To provide a better understanding of the functionality that the OMA DRM Release 2 solution should provide.
- To offer high level descriptions of different OMA scenarios against which the formal requirements for OMA-DRM Release 2 can be checked
- To be a public document that can help to explain what OMA-DRM Release 2 is about.

5.2 Usage Scenarios

Jo is an active teenager in 2003. She has many friends both in her real and virtual worlds. She belongs to several virtual communities and likes to share experiences with them. Her friends in her real world enjoy interacting socially when they meet and also using other messaging techniques such as email, instant messaging and even short messaging when they cannot talk.

Jo owns a range of different electronic Devices including a digital camera that can take still pictures and short video clips. She has in effect become a Content Provider herself and would like to be able to control the content which she sends both to her friends and that she places onto a personalised web site.

The other Devices that she owns have a range of communications mechanisms including Bluetooth and wireless LAN. Her iMac has Bluetooth connectivity, her PDA is Bluetooth enabled, her tablet PC which she uses to take notes in lectures is connected with 802.11 technology. Some Devices MAY have network connectivity built into them (e.g. mobile phone), some MAY have intermittent connectivity (e.g. a PDA with Bluetooth) and some MAY never have any connectivity with the network (e.g. an MP3 player).

She owns a number of CDs and DVDs with content from well-known record and film companies.

She has subscriptions with several Content Providers, both her mobile operator and Internet-based Content Providers, which enables her to download and stream songs to her PC and mobile Devices..

Note: Discussions regarding content types are for example only. Other content types MAY be considered.

In the user cases described below, it is important to note that the facilities offered to Jo and her friends are made only if appropriate Rights Objects have been specified by the Content Provider, allowing her to do this.

Scenario 1: Using content on multiple devices

Jo purchases and downloads a protected music track to her mobile phone. She sends a copy of the track to her DRM compliant portable music player by:

a. using a Bluetooth connection with the player, or

b. copying the track to a removable memory card, and moving the card to her music player.

Jo can listen to the track on both her phone and on the music player. She can do this because when she bought the track, she agreed to a purchase agreement on the transaction, which explicitly allows her to use the track on another, specified OMA DRM Conformant Device. However, depending on the purchase agreement, she may only be able to listen to the track on one of devices at one time, or may be able to listen to the tracks on both devices at the same time.

Scenario 2 – Buying Rights Objects for another user

Jo hears about a great song and wants to send it to her mother. She uses a service from her Rights Issuer to buy the Rights Object to the song for her mother and enables her mother to receive the content (and Rights Object) on her Device and play the song.

Scenario 3 – Restoration of Rights Object and content using a secure portable user identity

Jo drops her mobile Device resulting in a catastrophic failure, she calls her Network Service Provider who replaces the Device (under her insurance agreement). The embedded portable smartcard Device carries her identity in a secure way. The smartcard has not been damaged and she is able to insert it in the replacement Device and use this as an authenticated identity which allows her to download the Protected Content and Rights Object previously purchased from the Content Providers.

Scenario 4 –Backup of Protected Content and Rights Object from a Service Provider

Jo loses her mobile Device which contains many Protected Content files and related Rights Object. She calls her Network Service Provider who replaces the Device (under her insurance agreement). The Device is only set up to her default subscription. Luckily, her Content Provider maintains a record of the content which Jo owns, and she is able to login to her Content Provider who automatically downloads the Protected Content and related Rights Object which she has previously purchased to her new Device.

There is no specified method of storing information relating to the state of stateful Rights Objects outside the Device to which the Rights Objects apply.

The Rights Issuer can Revoke the old Device (preventing it from future access to OMA DRM services) to prevent possible fraud.

Scenario 5 – Local Device Backup of content and Rights Object

Jo has a mobile Device with a removable media slot. She makes a Backup of her Media Objects and stateless Rights Objects , which she has previously purchased, on a removable media, and leaves it at home. Then Jo drops her mobile Device resulting in a catastrophic failure, She calls her Network Service Provider who replaces the Device (under her insurance agreement). The removable media is safe, so she is able to insert it in the replacement Device, restore all the objects to the Device and continue to use the Media Objects once new Rights Objects have been re-issued to the replacement Device. She cannot restore the stateless Rights Objects on the new Device, as the Rights Objects could only have been restored to the old Device.

The Rights Issuer can Revoke the old Device (preventing it from future access to OMA DRM services) to prevent possible fraud.

Scenario 6 – Protecting user generated content

Jo would like to create content (photo etc.) and send it to her friend. However, she does not wish her friend to forward it to anybody else. Her Device provides the capability to give her content a “forward lock”. The transport for her content is unspecified, but could be MMS.

Scenario 7 – Export of Protected Content and Rights Objects to other DRM systems and/or transfer to copy-protected storage medium/transport

Jo purchases and downloads an OMA DRM protected music track to her mobile phone. She plays the music on her mobile phone for several days, and then decides she would prefer to play it on another music player that has a different DRM protection format.

Jo can choose between the following mechanisms to render the track on a different player. In all cases, the Content Provider can specify whether the alternative rendering mechanism is allowed or not.

1. She exports the music and its (stateless) Rights Object (or its equivalent in the exported-to DRM) to the other player using a Bluetooth connection or via removable media. Now she cannot play the music on her mobile phone but can play it on the other DRM-compliant music player.

2. She transfers the music track to a copy protected storage medium. Jo can now play the track on any player that supports this storage medium. The copy protection mechanism of the storage medium prevents copying of the tracks from the medium.

3. She streams the music tracks from her mobile phone to a rendering device for immediate playback. An example of such a rendering device is a headphone. The transmission protocol between her mobile phone and the rendering device incorporates copy protection so that the track cannot be copied.

Scenario 8 - Multiple Contents Scenario

Jo subscribes to a music service where she can download favourite songs for karaoke. Each karaoke song is delivered as a package that includes the music and lyrics for the song as well as associated images and links to related content. She can play and sing the songs with her mobile karaoke player. A single Rights Object for this package can specify different Permissions for the individual components. The content provider wants to promote the song so it allows the lyrics, images, and other information to be copied for free so Jo can share them with her friends. Through this promotion, the content provider hopes to stimulate sales of the music.

The package of music, lyrics and pictures might be sent by MMS.

Although the package contains several parts, Jo may only have a single Rights Object associated with that content package.

Scenario 9 - Basic download

Jo browses a content provider’s portal and decides to acquire downloadable content. She completes the required browsing, ordering and payment transactions. She downloads the content object to her Device and receives the Rights Object that is sent to her Device, and is subsequently able to play the content subject to the terms described in the Rights Object. The content is protected against use or misuse that does not comply with the Rights Object set by the Content Provider.

The types of Permission she may have are:

- Time based Rights Object allowing her to listen to the song until a particular date .

- Metered usage time based rights allowing her to listen to the song as long as the metered usage time is less than a specified time, whilst ensuring that she cannot alter the accumulated time to give herself additional usage.

Scenario 10 - Subscription

Jo has subscribed to a Internet music service that she accesses through her mobile Device. The mobile Device has removable storage and music playing capability. The service allows Jo:

- music streaming to her mobile Device for on-demand listening with play control (pause, resume, etc.).

- music download to her mobile Device. The music can be listened to, as long as the subscription is active (even when the Device is out of coverage), either when the Device is connected to or disconnected from the Internet site.

Scenario 11 - Basic streaming

Jo browses a Content Provider’s portal and decides to see an audiovisual stream showing a concert of her favourite group. She completes the required browsing, ordering and payment transactions. She downloads some information for the streaming player to her Device and receives the Rights Object. The Rights Object describes Jo’s Permissions concerning setting up, receiving and playing the streams. She is subsequently able to set up the audio and video streams and play them subject to the terms described in the Rights Object.

Scenario 12 - Multicast streaming under subscription

Jo has a paid subscription with an Internet radio service that she accesses through her mobile Device. The service allows Jo to select one of number of multicast radio channels and listen to the multicast stream on that channel.. The music can be listened month after month, as long as the membership is active, either when the Device is connected to or disconnected from the Internet site.

Scenario 13 - Backwards compatibility

Jo receives many forms of content from various service providers. When her new Device receives content from service providers only utilising the release 1 DRM mechanism, her new Device handles these requests according to the requirements specified for release 1 compliant Devices, without causing Jo any problems.

Scenario 14 - Preview Rights Object

Jo receives a music clip of a band she has never heard of before by superdistribution. She is issued preview Rights Object allowing her to listen once to the music, or allowing unlimited playback of a small section of the music before she decides to buy the full set of rights. In the case of allowing unlimited playback of a segment of the file, Jo is able to preview while the remainder of the file is being downloaded. This type of Rights Object may also apply to a clip at the start of streamed data.

The types of possible permissions within the Rights Object that Jo may receive either:

- state that the Media Object can only be played once, or
- describe the starting and finishing times of the free preview clip

Scenario 15 - Superdistribution

Jo has received Protected Content via a local link (e.g. Bluetooth, IrDA, ...) from her friend. She wants to acquire Rights Object to get access to that content and follows the appropriate reference provided for that purpose in the Protected Content. Jo explores the offer to obtain new Rights Object. Before Jo is charged for the new Rights Object she expects that

- the integrity of the Protected Content is verified to avoid buying Rights Object for content that isn't usable,
- the properties of the Protected Content are validated to be suitable for Jo's Device,
- the process of acquiring new Rights Object provides the same user experience as the process of purchasing new Protected Content with associated Rights Object.
- the Rights Object issuer has been authenticated.

Scenario 16 – Revoke Device

The Content Provider wishes to prevent Jo from being able to acquire new content for her Device, for example, because Jo has illegally shared her content with friends in the past. The Content Provider therefore revokes Jo’s Device and Jo no longer receives Protected Content or Rights Objects from that Content Provider.

Scenario 17 – Binding Rights Objects to User Identity

Jo has two phones but only one SIM – she puts her SIM in the phone she wants to use. Jo has a game that she wants to be able to play on both her phones but does not want to buy it twice. Jo’s Rights Issuer therefore issues both of Jo’s phones with a Rights Object for the game. The Rights Object is tied to the presence of Jo’s SIM so she can only play the game on the phone with her SIM in. When she lends one of her phones to Bob, who puts his SIM in, the Rights Object cannot be used.

Scenario 18 – Basic (silent) auto-renewal of Right Objects

A Rights Object on Jo's mobile phone expires. Jo goes to play the associated Protected Content. Instead of immediately notifying Jo that her Rights Object have expired, the DRM Agent on the phone first contacts to the DRM service provider to request renewal. Only if the Content Provider refuses does the DRM Agent alert Jo that she needs to go and re-acquire Rights Object.

Scenario 19 – Redirection to Rights Issuers from Content Provider

Jo's Rights Object have expired. Jo's mobile Devices attempted to acquire Rights Object from the Content Provider. The Content Provider refuses but returns a message stating that Rights Object can be bought from a named (set of) alternative Rights Issuers. Jo can select the link to initiate a browser connection to one of the Rights Issuers. Jo re-purchases the Rights Object. The chosen Rights Issuer updates the Content Provider of the newly acquired Rights Object.

Scenario 20 – Hacked DRM Solution

OMA DRM solution becomes a very widely adopted DRM standard, and hence becomes the focus of attention for an attempt at cracking the cryptographic implementation.

The Rights Issuer identifies that the Device is insecure, notifies Jo and adds the Device identity (DRM agent, SW version, Device equipment number…) to a black list for Protected Content download.

Scenario 21 –Operation with Varying Cryptographic Strengths

Jo is using a Device which is legally prohibited from using the highest strength ciphers supported by OMA DRM. Content Providers and Rights Issuers are able to discover which ciphers are supported by Jo's Device before sending encrypted data to it.

6. Market Requirements

Release 1

1. It SHALL be possible to precisely identify Protected Content such that Rights Object may be unambiguously associated with it.
2. It SHALL be possible for Rights Issuers to send Rights Objects to Devices .
3. The Permissions in a Rights Object SHALL be enforced by an OMA DRM Conformant Device.
4. It SHALL NOT be possible for a DRM Agent to use Protected Content unless appropriate Rights Object have been associated with that Protected Content and the DRM Agent possesses the required Rights Object.
5. It SHALL be possible to separate Rights Object and Protected Content physically, but not logically.
6. It SHALL be possible for Rights Objects and Protected Content to be delivered via the same or different transport mechanisms. Delivery SHALL be possible using any transport mechanism.
7. Protected Content may contain Media Objects of any Content Type.
8. It SHALL be possible for the Device to identify whether it can play a certain item of Protected Content before requesting the Rights Object for that item of Protected Content.
9. It SHALL be possible for a Rights Issuer to discover whether a Device can play a certain item of Protected Content before issuing the Rights Object (for that item of Protected Content) to the Device.
10. Permissions within the Rights Object SHALL enable the following capabilities. All Permissions SHALL be explicitly stated:
    a. It SHALL be possible to specify Permissions for the following rendering types:
        i. Play
        ii. Execute
        iii. Display
        iv. Print
    b. It SHALL be possible to specify the following Constraints on usage:
        i. Time/date based
        ii. Count based

Release 2

11. Permissions within the Rights Object SHALL enable the following capabilities. All Permissions SHALL be explicitly stated:
    a. It SHALL be possible to export both Rights Objects and Protected Content from a Device to another DRM system, to transfer to a copy protected storage medium or to stream over a copy protected transport mechanism.
    b. It SHALL be possible to specify the following Constraints on usage:
        i. Metered time based (i.e. that the Device can Play the Protected Content as long as the metered usage time is less than a specified time)
        ii. User identity based (i.e. that the Device can only Play the Protected Content when being used by a specified User)

12. It SHALL be possible to Backup both Protected Content and stateless Rights Objects from a Device.
13. It SHALL be possible for the Rights Issuer to reliably identify the Device for the purpose of either issuing or refusing a Rights Object to that Device.
14. It SHALL be possible for Rights Issuers to protect Rights Objects intended for a particular Device such that the Rights Object can only be processed by that Device.
15. It SHALL be possible for Rights Objects and Protected Content to be delivered at the same or different times and to be received in any order.
16. It SHALL be possible for the Device to forward lock a Media Object created on that Device, such that when distributed, the recipient cannot redistribute it.
17. It SHALL be possible for a Device which receives super-distributed Protected Content to be able to validate its integrity .
18. It SHALL be possible to package multiple items of Protected Content and download this package to a user, whilst assigning different Permissions for each item of that Composite Object.
19. Devices that support the requirements of release 2 SHALL also comply with all SCR for release 1 in an interoperable manner.
20. The Release 2 OMA DRM standard SHALL be implemented to prevent Release 1 OMA DRM Conformant Devices from failure conditions which might occur if Release 2 Protected Content or Rights Objects are sent to that release 1 Device.
21. It SHALL not be possible for a Release 1 Device to play Release 2 Protected Content unless the Rights Issuer has issued a Release 1 Rights Object for the Protected Content.
22. It SHALL be possible for a Device to play Protected Content which has been restored from a Backup. .

7. Engineering Requirements

7.1 Security

Release 1

1. It SHALL be possible for the Confidentiality of the Protected Content to be protected, between the Content Provider and the Device.

Release 2

2. The Rights Issuer SHALL be able to authenticate, prior to delivery of Rights Objects to the intended Device, some or all of the following:
   a. The identity of the User of the Device;
   b. The identity of the subscriber (relating to the Network Service Provider) associated with the Device;
   c. The identity of the Content Subscription (relating to the Content Provider) associated with the Device;
   d. The identity of the Device (for example: serial number; Device manufacturer; model number; software version);
   e. The identity of any smartcard inserted in the Device.
3. It SHALL be possible for Rights Issuers to protect Rights Objects for a particular Device such that the Rights Object can only be processed by the intended Device
4. The Rights Issuer SHALL be able to conduct the authentication described in requirement (2) of this sub-section without any explicit relationship (contractual or otherwise) with the Device manufacturer.
5. It SHALL be possible for the Confidentiality of the Protected Content to be protected, in a manner independent of the transport mechanism, between the Content Provider and the DRM Agent on the Device.
6. It SHALL be possible for the Confidentiality of the Protected Content to be protected, in a manner independent of the transport mechanism, between the DRM Agent on a Device and the DRM Agent on any other Device to which the content is transferred.
7. It SHALL be possible for the integrity of the Protected Content to be protected, in a manner independent of the transport mechanism, between the DRM Agent on a Device and the DRM Agent on any other Device to which the Protected Content is transferred.
8. It SHALL be possible for the Confidentiality of any content encryption key (CEK) in a Rights Object to be protected, in a manner independent of the transport mechanism, between the Content Provider and the DRM Agent on the Device, such that the CEK can only be read by the Device for which the Rights Object is intended.
9. It SHALL be possible for the Content Provider to encrypt each instance of a particular piece of Protected Content with a different CEK and for superdistribution of that Protected Content to still be possible.
10. It SHALL be possible for the integrity of the Rights Object to be protected, in a manner independent of the transport mechanism, between the Content Provider and the DRM Agent on the Device for which the Rights Object is intended.
11. It SHALL be possible for the Confidentiality of sensitive information within the Rights Object, for example, user identities, to be protected, in a manner independent of the transport mechanism, between the Content Provider and the DRM Agent on the Device, such that this sensitive information in the Rights Object can only be read by the Device for which the Rights Object is intended.
12. It SHALL be possible for the Device to authenticate the identity of the source of the Rights Object.

13. It SHALL be possible for entities other than the Device manufacturer to provide trusted assertions to Content Providers concerning some or all of the identities listed in requirement (2) within this sub-section.

14. It SHALL be possible for individual components of a composite object to be encrypted with different keys.

15. It SHALL be possible for some components of a composite object to be encrypted and some not.

7.2 Charging

This sub-section will not specify any particular billing mechanism, merely enablers for billing.

Release 1

1. It SHALL be possible for the following charging mechanisms to be supported:

   a. A single Device subscription basis. That is, it SHALL be possible for the Content Provider to deliver to a Device associated with a particular subscription, a defined or unlimited amount of Protected Content with associated Rights Objects over a fixed duration, free of charge, other than the cost of the content subscription.

   b. A pre-pay basis. That is, it SHALL be possible for the Content Provider to deliver to a Device, an amount of Protected Content with associated Rights Objects, valued up to and including a particular financial sum (which is the current balance of the pre-pay account associated with that Device).

   c. A per event basis. That is, it SHALL be possible for the Content Provider to deliver to a Device, an item of Protected Content with associated Rights Object and to make a charge for that piece of content as part of the content delivery transaction.

Release 2

2. It SHALL be possible for the following charging mechanisms to be supported:

   a. A multiple Device subscription basis. That is, it SHALL be possible for the Content Provider to deliver to any subset of a number of Devices associated with a particular subscription, a defined or unlimited amount of Protected Content (with associated Rights Objects) over a fixed duration, free of charge, other than the cost of the content subscription.

   b. A multiple Device pre-pay basis. That is, it SHALL be possible for the Content Provider to deliver to any subset of a number of Devices associated with a pre-pay account, an amount of Protected Content (with associated Rights Objects) valued up to and including a particular financial sum (which is the current balance of the pre-pay account associated with that collection of Devices).

   c. A multiple Device per event basis. That is, it SHALL be possible for the Content Provider to deliver to a any subset of a specified number of Devices, an item of Protected Content (with associated Rights Object) and to make a charge for that piece of Protected Content as part of the content delivery transaction.

3. It SHALL be possible for a Content Provider to obtain payment from a Billing Service Provider even if the Content Provider and Billing Service Provider are operated by separate organisations.

7.3 Streaming

Release 1

1. It SHALL be possible to protect the confidentiality of a description of a media streaming session, between the Content Provider and the Device.

2. It SHALL be possible to associate a Rights Object with a description of a media streaming session.

Release 2

3. It SHALL be possible to stream (play in real time) Protected Content from the Content Provider to the DRM Agent on a single Device. The requirement applies (but not exclusively) to the following real time protocols :

    a. 3GPP transparent end-to-end packet switched streaming service, see [3GPP PSS]

4. DRM protection of streamed Protected Content SHALL NOT prevent the playing of the Protected Content if there are errors introduced into the content by the transport.

5. It SHALL be possible to stream (play in real time) protected content from the Content Provider to a number of DRM Agents on a set of Devices (in both broadcast and multicast modes).

6. It SHALL be possible to apply protection between DRM Agents on different Devices to Protected Content that is played in real time such as streaming media. The requirement applies (but not exclusively) to the following real time protocols :

    a. Bluetooth Generic Audio-visual Distribution Profile, [BT GAVDP]

    b. Bluetooth Audio-visual Distribution Transport Protocol, [BT AVDTP]

    c. Bluetooth Generic Audio-visual Control Transport Protocol, [BT AVCTP]

7.4 Superdistribution

Release 1

1. It SHALL be possible for Devices to send Protected Content to other Devices in a transport independent manner, and for Devices receiving Protected Content in such a manner to be able to obtain the Rights Object corresponding to the received Protected Content.

2. It SHALL be possible for a Device which has received Protected Content from another Device to find out if the Protected Content can be played on the Device before obtaining a Rights Objects for that Protected Content.

3. It SHALL be possible to use the same download mechanism for the acquisition of a Rights Object as for the acquisition of the Protected Content and the Rights Object from a Content Provider in order to enable the same user experience.

7.5 Storage and Backup

Release 1

1. It SHALL be possible for the Device to Backup and Restore Protected Content.

Release 2

2. It SHALL be possible for the Device to Backup stateless Rights Objects .

3. It SHALL only be possible to Restore Backed up stateless Rights Objects to the Device for which the Rights Object were originally issued.

4. It SHALL be possible for the Device to copy Protected Content and encrypted Rights Objects to another Device, that does not necessarily have network access e.g. from a phone to a portable media player.

7.6 Rights

Release 1

1. It SHALL be possible to specify Rights Objects for any content type.

2. It SHALL be possible to specify Rights Objects for encrypted and unencrypted content.

3. It SHALL be possible to specify Rights Objects to enable the following rendering types:
    a. Play
    b. Execute
    c. Display
    d. Print
4. It SHALL be possible to specify Rights Objects containing the following Constraints on usage
    a. Time/date based
    b. Count based
5. It SHALL be possible to specify content identities within Rights Objects using standard identification schemes. In particular it SHALL be possible to support the use of:
    a. URI (RFC 2396)

Release 2

6. It SHALL be possible to specify Rights Objects containing the metered usage time constraints on usage, for example, it SHALL be possible to specify that the Device can Play the Protected Content as long as the metered usage time is less than the specified time.
7. It SHALL be possible to specify that the Rights Object is bound to a particular User identity, i.e., that a Device can only Play the Protected Content when being used by that User.
8. It SHALL be possible to specify within the Rights Objects associated with Protected Content whether or not the Rights Object and Protected Content can be exported to another DRM system, and to which DRM systems.
9. It SHALL be possible to specify within the Rights Objects associated with Protected Content whether or not the Rights Object and Protected Content can be transferred to copy protected storage media, and to which copy protected storage media.
10. It SHALL be possible to specify within the Rights Objects associated with Protected Content whether or not the Rights Object and Protected Content can be transferred to a rendering device over a copy protected transport mechanism, and over which copy protected transport mechanisms.
11. It SHALL be possible to specify Rights Objects associated with Protected Content where the Protected Content is a Composite Object.
12. It SHALL be possible to independently specify Rights Objects for each individual component of a Composite Object.
13. It SHALL be possible to specify, within the Rights Object, text information provided by the Rights Issuer (e.g. title, author, copyrights). This information, if provided, SHALL be available for display to the User.

7.7 Privacy

1. User and Device specific information SHALL NOT be disclosed to the Content Provider and/or to other parties without the explicit consent of that User.
2. User and Device specific information SHALL NOT be disclosed by the Content Provider to any 3rd party without the explicit consent of the User.
3. It SHALL be possible for Confidentiality to be maintained when User specific information such as the User identity is sent from the Device.

7.8 Administration and configuration

No requirements identified.

7.9 Terminal Devices and smartcards

7.9.1 Terminal Devices

Requirements are stated elsewhere in this document.

7.9.2 Smartcards

1. The Device SHALL be able to use the smart card to provide User identification and authentication when obtaining and verifying Rights Objects.

7.9.3 Removable Media Cards

Requirements stating the use of removable media cards by Devices are stated elsewhere in this document. However, this document does not make any requirements on removable media cards themselves.

7.10 Platforms

No requirements identified.

7.11 Network interfaces

No requirements identified.

7.12 Usability

1. It SHALL be possible for the User to delete an instance of Protected Content, but to keep the Rights Objects associated with that content (so that he/she could restore the Protected Content on the Device later without having to obtain new Rights Objects).

2. It SHALL be possible for a User to view a description of the Protected Content without retrieving the Rights Object.

3. It SHALL be possible for the User to view information, e.g. copyright information, available Permissions, regarding Rights Objects on the Device.

7.13 Interoperability and backward compatibility

1. Devices that support the requirements of release 2 SHALL also comply with all SCR for release 1 in an interoperable manner.

2. The supported DRM version SHOULD be exposed.

Change History (Informative)

Type of change	Date	Section	Description
First version in correct template	23-10-02	All	
Minor changes	25-10-02	All	
Additions of new user scenarios	02-11-02	All	
Major changes following discussion at Hamburg meeting and review by IFPI/RIAA.	22-12-02	All	
Minor clean up prior to review by OMA Requirements group	31-12-02	All	
Minor changes following Redwood City meeting	06-02-03	All	
Major changes reflecting architectural decisions and second review by OMA Requirements group	21-03-03	All	
Major changes following Braunschweig meeting	04-04-03	All	
Minor changes following post-Braunschweig conference calls	22-04-09	All	
Minor changes	25-4-03	All	