Implementation Best Practices For OMA DRM release 1

Version 1.1
20th August 2003

Change History:

Version	Date	Author	Comments:
1.0	29th July	Companies who have undersigned	First version for review.
1.1	20th August	As above	Updated also to have <interval> constraints (in addition to <datetime>) to be allowed for automated content and made some other clarifications and editorial changes.

1. INTRODUCTION

This document aims to increase the interoperability of implementations adhering to the OMA DRM release 1 specifications by clarifying parts of the specifications where there is an opportunity for divergent implementations. The text of the document is meant to be a basis for interpretation of the OMA specifications, and does not preclude differentiation or requirements built on top of this understanding. This document does not address integration with other technologies. However, a further document clarifying the integration of Java and DRM is planned, and the usage of DRM content types within the MMS environement is specified in the MMS Conformance Document from the Open Mobile Alliance.

2. REFERENCES

DRM	"Digital Rights Management", Open Mobile Alliance™, OMA-Download-DRM-v1_0, http://www.openmobilealliance.org/
DRMREL	"DRM Rights Expression Language", Open Mobile Alliance™, OMA-Download-DRMREL-v1_0, http://www.openmobilealliance.org/
OMADL	"Generic Content Download Over The Air Specification", Open Mobile Alliance™, OMA-Download-OTA-v1_0, http://www.openmobilealliance.org/
[MMSCONF]	"MMS Conformance Document", Open Mobile Alliance™, OMA-MMS-CONF-v1_2, http://www.openmobilealliance.org

3. CLARIFICATIONS TO OMA DRM RELEASE 1 SPECIFICATIONS

3.1 Cardinality

3.1.1 Media object – DRM message / DCF

Any DRM message or DCF contains a single media object at a time, for example, a ringing tone or operator logo. Note that a DRM message may also contain a DCF[1] [DRM; page 11].

3.1.2 DRM message – Rights object

For any given DRM message, there can be at most a single rights object.

If the DRM message is utilized according to the combined delivery mechanism [DRM; page 10], then it contains the single rights object.

If the DRM message is utilized according to the forward-lock mechanism [DRM; page 10], then it does not contain any rights object.

3.1.3 DCF – Rights object

For any given DCF, there can be multiple rights objects [DRM; page 12]. Each rights object is treated individually. Content can be rendered according to any associated rights object that is valid.

[1] Only when used as forward-lock and not when used in combined delivery

3.1.4 Rights object - Permissions

A rights object can contain multiple permissions, i.e., <play>. <display>, <execute>, and <print>. Access granted to content according to one permissions is independent from all other permissions in the same rights object [DRMREL; page 11].

3.1.5 Permissions – Constraints

In order for access to be granted according to a permission, all its constraints (if any) must be fulfilled [DRMREL; page 13].

3.2 Constraints

Constraints limit the use of content according to specified permissions. The following constraints are defined by the OMA DRM release 1 specifications: <count>, <interval>, and <datetime>.

In order to increase interoperability and to ensure a consistent user experience, the following clarifications and measures are provided:

3.2.1 <count>

The number of 'counts' specified by a rights object is decremented whenever the user initiates rendering of the media object. This number is not decremented when the intention of the rendering is only to show the user a sample of what the file actually contains. Examples of such samples are the thumbnail of an image is used in a list of available images, or when a single frame of a video is used as a thumbnail in a list of available videos.

3.2.2 <interval>

The <interval> constraint specifies the time frame during which the media object can be rendered. The interval period begins on first usage of the rights object (and not from when the rights object was received).

Note that once the rendering of content according to a permission constrained by an <interval> element has started, the <interval> element can logically be interpreted as a <datetime> element with the <start> element containing the time the rendering has started and the <end> element containing the time when the rendering will stop (which is equal to the start time plus the time defined by the interval document).

3.2.3 <datetime>

The <datetime> constraint specifies a <start> and an <end> time in between which the media object can be rendered [DRMREL; page 13]

3.2.4 Usage of Constraints

Constraints can be applied to all Media Objects for user-initiated rendering transactions. However – for automated use, Media objects (e.g. ringing tones and operator logos) are installed only if there exists at least one corresponding rights object without a <count> constraint. Even though these media objects without such rights object cannot be installed for automated use, they can be rendered by corresponding applications as initiated by the terminal user.

For media objects with corresponding <interval> constraints, if these are to be installed for automated use (eg as a ringtone or screensaver) the start of the interval period will be established at the first usage as specified in 3.2.2, i.e. at the first rendering (either user-initiated or automated), not at reception of the content nor at installation for automated use.

For discussing the rendering of constrained media objects, we introduce the concept of a ”rendering session.” A rendering session generally refers to the single exercise of a permission. For instance, the permission to play a MIDI song would consist of the start of the play through to its completion (e.g. by coming to the end of the song, or by having the user manually abort the play).

For automated use, the rendering session may comprise several renderings of a media object. For example, ringtone constraints will only be checked once per phone call or periodically, not each time the phone rings per phone call.

Constraints are validated at the beginning of the rendering session. At the beginning of the rendering session, the renderer will ensure (based on which constraints are specified in the rights object):

- There is at least one count left, and/or
- The interval time has not been exceeded, and/or
- The end time has not passed.

The renderer is not required to validate constraints during the rendering session. For example, if the end time in the <datetime> constraint occurs during the rendering session, the rendering session will not abort prematurely when the <end> time is reached.

Note that this does not imply any specific implementation and manufacturers are free to choose the most efficient scheme for their architecture, but all implementations must ensure that a rendering session cannot be initiated when there are no valid permissions.

3.3 Order of evaluation of rights objects

As described in section 3.1.3, for any DCF, there can be multiple rights objects. According to the OMA DRM release 1 specifications, the selection of which rights object is to be used for granting access to the content (out of multiple valid rights objects) should favor the terminal user [DRM; page 12]. As this might not be immediately clear from the specifications, the order of evaluation required to favor the terminal user is explicitly spelled out below in the following rules:

1. Only rights objects valid at the time of requesting content access can be considered.[2]
2. Rights objects with no constraints should be used first.
3. Rights objects containing a <datetime> constraint (and potentially other constraints) should be used to grant access to content before using rights objects that do not contain a <datetime> constraint.

[2] For example, those with a <datetime> constraint whose <begin> date still lies in the future cannot be considered.

4. If multiple rights objects exist that contain <datetime> constraints (and potentially other constraints), then these should be used in the order of ascending <end> dates first, i.e., those that expire first should be utilized first.

5. If multiple rights objects exist that do not contain a <datetime> constraint (and potentially other constraints), then those containing an <interval> constraint should be used to grant access to content before using rights objects that do not contain an <interval> constraint.

4. DELIVERY VERTICALS

The OMA DRM release 1 standard is designed as a content and transport agnostic protection system. The following sections provide guidelines and recommendations regarding the distribution of OMA DRM protected content using different mechanisms.

4.1 MMS

When distributing forward-locked and combined delivery content via MMS, special care should be taken by the MMS service provider to prevent DRM messages from being made available on, e.g., Web pages, to support non-MMS terminals.

DCFs can be distributed via MMS without any problem since they are inherently secure due to being encrypted.

4.1.1 OMA MMS Conformance Document

The OMA MMS Conformance Document version 1.2 introduces MMS message classes. OMA DRM forward lock is supported by message class Image/Rich and higher. For more information on applying OMA DRM in MMS messages, see Appendix A of [MMSCONF].

4.1.2 Separate delivery header

In case an MMS message includes content using separate delivery, the separate delivery header ‘X-Oma-Separate-Delivery’ may be used to inform the MMS UA of the pending rights object. The ‘X-Oma-Separate-Delivery’ header must be located in the headers section of the corresponding MMS body part.

Note that the ‘X-Oma-Separate-Delivery’ header is only an indiciation of when rights should arrive to the terminal and cannot be relied on as trusted.

4.2 OMA Download

Both, DRM messages and DCFs, can be transported using OMA Download as specified in [OMADL].

4.3 Email

DRM messages contain media objects in unencrypted form unless the media object itself has been encrypted beforehand, e.g., by embedding it in a DCF. Due to the low level of security of the combination of email and DRM message, content providers are advised not

to utilize email to deliver commercial content contained in DRM messages.[3] Rather, the use of DCF is recommended when distributing commercial content via Email.

[3] Transport encryption such as TLS can be utilized to protect against eavesdropping by unauthorized parties.