Enabler Release Definition for DRM

Draft Version 2.0 – 1 April 2004

Open Mobile Alliance
OMA-ERELD-DRM-V2_0-20040401-D

Contents

1. Scope

The scope of this document is limited to the Enabler Release Definition of Digital Rights Management according to OMA Release process and the Enabler Release specification baseline listed in section 5.

2. References

2.1 Normative References

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

[DRMREQ-v2] "OMA DRM Requirements". Open Mobile Alliance™. OMA-DRM-REQ-V2_0. http://www.openmobilealliance.org/

[DRM-v2] "OMA DRM". Open Mobile Alliance™. OMA-DRM-DRM-V2_0. http://www.openmobilealliance.org/

[DRMCF-v2] "OMA DRM Content Format". Open Mobile Alliance™. OMA-DRM-DCF-V2_0. http://www.openmobilealliance.org/

[DRMREL-v2] "OMA DRM Rights Expression Language". Open Mobile Alliance™. OMA-DRM-REL-V2_0. http://www.openmobilealliance.org/

2.2 Informative References

[DRMARCH-v2] "OMA DRM Architecture". Open Mobile Alliance™. OMA-DRM-ARCH-V2_0. http://www.openmobilealliance.org/

[DRMETR-v2] "OMA DRM Enabler Test Requirements". Open Mobile Alliance™. OMA-DRM-ETR-V2_0. http://www.openmobilealliance.org/

3. Terminology and Conventions

3.1 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

All sections and appendixes, except “Scope” and “Introduction”, are normative, unless they are explicitly indicated to be informative.

The formal notation convention used in sections 8 and 9 to formally express the structure and internal dependencies between specifications in the Enabler Release specification baseline is detailed in [CREQ].

3.2 Definitions

Enabler Release	Collection of specifications that combined together form an enabler for a service area, e.g. a download enabler, a browsing enabler, a messaging enabler, a location enabler, etc. The specifications that are forming an enabler should combined fulfil a number of related market requirements.
Minimum Functionality Description	Description of the guaranteed features and functionality that will be enabled by implementing the minimum mandatory part of the Enabler Release

3.3 Abbreviations

DCF	DRM Content Format
DRM	Digital Rights Management
DTD	Document Type Definition
ERDEF	Enabler Requirement Definition
ERELD	Enabler Release Definition
OMA	Open Mobile Alliance
REL	Rights Expression Language
XML	eXtensible Markup Language

4. Introduction

This document outlines the Enabler Release Definition for DRM V2.0 and the respective conformance requirements for clients and servers implementing claiming compliance to it as defined by Open Mobile Alliance across the specification baseline.

OMA "Digital Rights Management" (DRM) enables the distribution and consumption of digital content in a controlled manner. The content is distributed and consumed on authenticated devices per the usage rights expressed by the content owners. OMA DRM work addresses the various technical aspects of this system by providing appropriate specifications for content formats, protocols, and rights expression languages.

This scope for the OMA DRM 2.0 enabler release is to define the protocols, messages and mechanisms necessary to implement the DRM system in the mobile environment. Builds upon the OMA DRM 1.0 enabler release to address the specific requirements enumerated in the OMA DRM 2.0 Requirements document.

There is a growing need for a rights management system in the mobile industry so that the operators and content providers can make digital content available to consumers in a controlled manner. Digital Rights Management is a set of technologies that provide the means to control the distribution and consumption of the digital media objects. OMA has already published release 1 of the DRM specifications. The release 1 specifications provide some fundamental building blocks for a DRM system. But, they lack the complete security necessary for a robust, end-to-end DRM system that takes into account the need for secure distribution, authentication of Devices, revocation and other aspects. This specification addresses these missing aspects of the OMA DRM.

The OMA DRM enables content providers to grant permissions for media objects that define how they should be consumed. The DRM system is independent of the media object formats and the given operating system or run-time environment. The media objects controlled by the DRM can be a variety of things: games, ring tones, photos, music clips, video clips, streaming media, etc. A content provider can grant appropriate permissions to the user for each of these media objects. The content is distributed with cryptographic protection; hence, the Protected Content is not usable without the associated Rights Object on a Device. Given this fact, fundamentally, the users are purchasing permissions embodied in Rights Objects and the Rights Objects need to be handled in a secure and un-compromising manner.

The Protected Content can be delivered to the Device by any means (over the air, LAN/WLAN, local connectivity, removable media, etc.). But the Rights Objects are tightly controlled and distributed by the Rights Issuer in a controlled manner. The Protected Content and Rights Objects can be delivered to the Device by downloading them together, or by sending them separately. The system does not imply any order or "bundling" of these two objects. It is not within the scope of the DRM system to address the specific payment methods employed by the Rights Issuers.

OMA DRM 2.0 consists of a set of specifications developed by OMA to address the need for digital rights management. For a detailed discussion of the overall system architecture, please refer to [DRMARCH-v2]. And, for a detailed discussion of the Rights Expression Language that is used to construct the Rights Objects, please refer to [DRMREL-2]. The DRM Content Format is specified in the [DRMDCF-2] specification. The [DRM-v2] specification defines the format and semantics of the cryptographic protocol, messages, processing instructions and certificate profiles that will, together enable an end-to-end system for protected content distribution. This includes the Rights Object Acquisition Protocol messages, the Key Management protocols, the domains functionality (sharing of content and rights among a set of Devices enrolled into a Domain), super distribution, transport mappings for ROAP, binding rights to user identities, & exporting to other DRMs, the certificate profiles, and application to other services like MMS and streaming.

5. Enabler Release Specification Baseline

This section is normative.

The Enabler comprises the following specifications:

- OMA-DRM-REQ-V2_0: Defines the requirements for the DRM 2.0 specifications.
- OMA-DRM-ARCH-V2_0: Defines the overall architecture for DRM 2.0 including informative descriptions of the technologies and their uses.
- OMA-DRM-DRM-V2_0: Defines the the format and semantics of the cryptographic protocol, messages, processing instructions and certificate profiles , including the Rights Object Acquisition Protocol (ROAP) messages, the domains functionality , transport mappings for ROAP, binding rights to user identities, exporting to other DRMs, the certificate profiles, and application to other services..
- OMA-DRM-REL-V2_0: Defines the rights expression language used to describe the permissions and constraints governing the usage of DRM protected media objects.
- OMA-DRM-DCF-V2_0: Defines the content format for DRM protected (encrypted) media objects.

The enabler comprises the following XML documents:

- XML Schemas for the Rights Object Acquisition Protocol (ROAP) protocol data units as defined in OMA-DRM-DRM-V2_0, Appendix A.
- XML Schema for the Rights Object Acquisition Protocol trigger media type as defined in OMA-DRM-DRM-V2_0, Section 5.2.8.
- XML Schema / DTD for the Rights Expression Language as defined in OMA-DRM-REL-V2_0, Section 6.2.

6. Minimum Functionality Description for DRM

<<This section is informative and should list which mandatory features (on a high level) that the enabler releases consists of, as well as what other dependencies it has towards other specifications, such as transport protocols and security. Optional features may also be listed here to the extent that is deemed to be useful, e.g. if two protocols can be used and both are optional. This chapter should be a high-level introduction to an implementor who intends to implement the Enabler. >>

This section is informative.

The minimum mandatory functionality for the DRM specifications includes:

- to be added when SCR tables of DRM, DCF, REL are ready -

The DRM specifications also define the following optional functionality:

- to be added when SCR tables of DRM, DCF, REL are ready -

7. Conformance Requirements Notation Details

This section is informative

The tables in following chapters use the following notation:

Item:
Entry in this column MUST be a valid ScrItem according to [CREQ].

Feature/Application:
Entry in this column SHOULD be a short descriptive label to the **Item** in question.

Status:
Entry in this column MUST accurately reflect the architectural status of the **Item** in question.
- M means the **Item** is mandatory for the class
- O means the **Item** is optional for the class
- NA means the **Item** is not applicable for the class

Requirement:
Expression in the column MUST be a valid TerminalExpression according to [CREQ] and it MUST accurately reflect the architectural requirement of the **Item** in question.

8. ERDEF for DRM - Client Requirements

This section is normative.

Table 1 ERDEF for DRM Client-side Requirements

Item	Feature / Application	Status	Requirement
OMA-ERDEF-DRM-C-001	DRM 2.0 Client	M	DRM:MCF, REL:MCF, DCF:MCF

9. ERDEF for DRM - Server Requirements

This section is normative.

Table 2 ERDEF for DRM Server-side Requirements

Item	Feature / Application	Status	Requirement
OMA-ERDEF-DRM-S-001	DRM 2.0 Server	M	DRM:MSF, REL:MSF, DCF:MSF

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
Draft Versions OMA-ERELD-DRM-V2_0	16 Dec 2003		Initial version