Enabler Release Definition for DRM V2.1.2

Approved Version 2.1.2 – 31 May 2011

Open Mobile Alliance
OMA-ERELD-DRM-V2_1_2-20110531-A

© 2011 Open Mobile Alliance Ltd. All Rights Reserved.

Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document. [OMA-Template-ERELD-20110101-I]

Contents

Tables

1. Scope

The scope of this document is limited to the Enabler Release Definition of Digital Rights Management 2.1 according to OMA Release process and the Enabler Release specification baseline listed in section 5.

2. References

2.1 Normative References

[IOPPROC]	"OMA Interoperability Policy and Process", Version 1.10, Open Mobile Alliance™, OMA-IOP-Process-V1_10, URL:http://www.openmobilealliance.org/
[DRMREQ-v2.1]	"OMA DRM Requirements", Version 2.1, Open Mobile Alliance™, OMA-DRM-REQ-V2_1, URL:http://www.openmobilealliance.org/
[DRM-v2.1.1]	"OMA Digital Rights Management", Version 2.1, Open Mobile Alliance™, OMA-TS-DRM-DRM-V2_1.1, URL:http://www.openmobilealliance.org/
[DRMCF-v2.1]	" OMA DRM Content Format" Version 2.1. Open Mobile Alliance™, OMA-TS-DRM-DCF-V2_1, URL:http://www.openmobilealliance.org/
[DRMREL-v2.1.1]	"OMA DRM Rights Expression Language", Version 2.1.1, Open Mobile Alliance™, OMA-TS-DRM-REL-V2_1.1, URL:http://www.openmobilealliance.org/
[DRMERELD-v2.1]	"Enabler Release Definition for DRM", Version 2.1, Open Mobile Alliance™, OMA-DRM-ERELD-V2_1, URL:http://www.openmobilealliance.org/
[DRMROAPXSD-v2.1]	"OMA Right Object Acquisition Protocol (ROAP) XML Schema" Version 2.1, Open Mobile Alliance™, OMA-DRM-ROAP-V2_1, URL:http://www.openmobilealliance.org/

2.2 Informative References

[DRMARCH-v2.1]	"OMA DRM Architecture" Version 2.1, Open Mobile Alliance™, OMA-AD-DRM-V2_1, URL:http://www.openmobilealliance.org/
[DRMETR-v2.1]	"Enabler Test Requirements for DRM V2.1", Version 2.1, Open Mobile Alliance™, OMA-DRM-ETR-V2_1, URL:http://www.openmobilealliance.org/
[DRMDTD-v2.1.2]	"DRM Rights Expression Language ", Version 2.1.2, Open Mobile Alliance™, OMA-SUP-DTD_DRM_REL-V2_1_2, URL:http://www.openmobilealliance.org/ Note: this file is for convenience provided in the enabler package
[DRMXSD-v2.1]	"OMA Data Dictionary XML Schema", Version 2.1, Open Mobile Alliance™, OMA-SUP-XSD_DRM_RELODD-V2_1, URL:http://www.openmobilealliance.org/ Note: this file is for convenience provided in the enabler package

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 [IOPPROC].

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
HTTP	HyperText Transfer Protocol
IMSI	International Mobile Subscriber Identity
MAC	Message Authentication Code
OBEX	IrDA Object Exchange Protocol
OCSP	Online Certificate Status Protocol
OMA	Open Mobile Alliance
PDCF	Packetized DRM Content Format
PDU	Protocol Data Unit
PKI	Public Key Infrastructure
REL	Rights Expression Language
RI	Rights Issuer
RO	Rights Object
ROAP	Rights Object Acquisition Protocol
WIM	Wireless Identity Module
XML	eXtensible Markup Language

4. Release Version Overview

This document outlines the Enabler Release Definition for DRM V2.1 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 by enabling Content Issuers to distribute DRM Content and Rights Issuers to issue Rights Objects for the DRM Content.

The OMA 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 system include but are not limited to: 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 Protected Content can be delivered to the Device by any means (over the air, LAN/WLAN, local connectivity, removable media, etc.). It is possible to deliver Protected Content and the associated Rights Object together, but it is also possible to send 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.

4.1   Version 1.0 Functionality

The OMA DRM v1.0 specification provides some fundamental building blocks for a DRM system without addressing 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.

The most important OMA DRM v1.0 functionality is listed below:
- ✓ Forward Lock to prevent forwarding of content if delivered in a DRM Message;
- ✓ Support for the "Content-Transfer-Encoding" and "Content-ID" headers in the DRM Message;
- ✓ Support for the combined delivery of rights and content;
- ✓ Support for separate delivery of rights and content, including superdistribution of said content;
- ✓ Control of content usage based on the specified rights and constraints.

4.2   Version 2.0 Functionality

The main differences between OMA DRM v1.0 and OMA DRM v2.0 are significantly improved security and functionality. Improved security is for example achieved by providing bilateral authorization between Rights Issuer and Device, based on PKI certificates and by confidentiality and integrity protecting Rights Objects. Improved functionality and usability is for example achieved by providing preview functions, mechanisms for sharing of content within a registered community of devices, called a domain, and by enabling devices without a wide-area network connection (unconnected devices) to participate in the system, and consume DRM Content.

The OMA DRM v2.0 specification enables content providers to grant permissions for media objects that define how they should be consumed. A content provider can grant appropriate permissions to the user for each of these media objects. A Rights Object is bound to a Device, by protecting it with the device public key, or to small domains of devices, by protecting it with a domain key. The content is distributed with cryptographic protection; hence, the DRM 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.

OMA DRM v2.0 contains a set of technical specifications, in particular:

- The REL specification defining the Rights Expression Language that is used to construct the Rights Objects.

- The DCF specification defining the DRM Content Formats.

- The DRM specification defining the format and semantics of the cryptographic protocol, messages, processing instructions and certificate profiles to enable an end-to-end system for DRM protected content distribution.

4.2.1   Version 2.0.1 Functionality

The most important changes introduced in DRM v2.0.1 compared with DRM v2.0 are summarized in the sections 4.2.1 of the DRM, DCF and REL Specifications in the DRM 2.0.1 ERP. These changes are considered to require special consideration in implementation. Many of the identified changes are bug fixes which if not implemented correctly may result in interoperability problems between conformant and non-conformant devices. Companies with existing DRM 2.0 implementations should take careful consideration of these changes.

4.3   **Version 2.1 Functionality**

OMA DRM v2.1 has been developed as a result of market feedback. The main differences between OMA DRM v2.0 and OMA DRM v2.1 are the addition of several features on top of OMA DRM v2.0, including:

- Metering, primarily intended for information gathering. By means of metering, actual content usage information can be provided to Rights Issuers, thereby enabling royalty collection based on actual usage of content.

- Content differentiation, defining a mechanism to control how content can be consumed. For example, this mechanism can prevent that a music track is used as ringtone.

- RO installation confirmation.

- Additional metadata, such as artist, title and genre

- Support for user editable metadata, in addition to content issuer defined metadata.

- A binary format for ROAP triggers to improve communication efficiency.

- New domain property (noConsumeAfter) to simplify "temporary sharing" business models

- RO upload functionality to enable users to upload Rights from their old device to a Rights Issuer so that these Rights can be downloaded to their new device.

- Improved extensibility for future versions.

The DRM 2.1 features have minimum impact on the DRM 2.0 architecture and are defined in a DRM 2.0 backward compatible manner.

5. Document Listing for DRM 2.1.2

This section is normative.

Doc Ref	Permanent Document Reference	Description
Requirement Document		
[DRMREQ-v2.1]	OMA-RD-DRM-V2_1-20081014-A	Defines the requirements for the DRM 2.1 specifications
Architecture Document		
[DRMARCH-v2.1]	OMA-AD-DRM-V2_1-20081014-A	Defines the overall architecture for DRM 2.1 including informative descriptions of the technologies and their uses
Technical Specifications		
[DRM-v2.1.1]	OMA-TS-DRM-DRM-V2_1_1-20100406-A	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, metering, installation confirmation, the binary encoding for ROAP triggers, RO upload functionality, the certificate profiles, and application to other services
[DRMREL-v2.1.1]	OMA-TS-DRM_REL-V2_1_1-20110531-A	Defines the rights expression language used to describe the permissions and constraints governing the usage of DRM protected media objects including additions to support metering and content differentiation. Note: in the enabler package, this document is accompanied by the informative support files [DRMDTD-v2.1.2] and [DRMXSD-v2.1]
[DRMDCF-v2.1]	OMA-TS-DRM-DCF-V2_1-20081014-A	Defines the content format for DRM protected (encrypted) media objects.
Supporting Files		
[DRMROAPXSD-v2.1]	OMA-SUP-XSD_DRM_ROAP-V2_1-20081014-A	Defines the ROAP XML schema Working file in Schema directory: file: drm_roap-v1_1.xsd path: http://www.openmobilealliance.org/tech/profiles/
[DRMRELDTD-v2.1.2]	OMA-SUP-DTD_DRM_REL-V2_1_2-20110531-A	DTD for the Rights Expression Language as defined in [DRMREL-v2.1.1]. Working file in DTD directory: file: drm_rel_dtd-v2_1.dtd path: http://www.openmobilealliance.org/tech/dtd/
[DRMRELXSD-v2.1]	OMA-SUP-XSD_DRM_REL-V2_1-20081014-A	Defines the ODRL Mobile profile Expression Langage. Working file in Schema directory: file: drm_rel_ex-v2_1.xsd http://www.openmobilealliance.org/tech/profiles
[DRMRELDDXSD-v2.1]	OMA-SUP-XSD_DRM_RELDD-V2_1-20081014-A	Defines the ODLR Mobile profile Data Dictionary Working file in Schema directory: file: drm_rel_dd-v2_1.xsd http://www.openmobilealliance.org/tech/profiles
[DRMRELODDXSD-v2.1]	OMA-SUP-XSD_DRM_RELODD-V2_1-20081014-A	Defined the OMA Data Dictionary Working file in Schema directory: file: drm_rel_odd-v2_1.xsd http://www.openmobilealliance.org/tech/profiles

Table 1: Listing of Documents in DRM 2.1.2 Enabler

6. Minimum Functionality Description for DRM

This section is informative.

There exist two different types of OMA DRM 2.1 clients: Unconnected Devices and Connected Devices (for a definition, see [DRM-v2.1.1], section 3.2.). The minimum mandatory client functionality for the DRM specifications includes:

1. For Unconnected and Connected Devices:

- ROAP schema parsing and processing

- Storage of RI context information

- Certain hash, MAC, Signature, and Key Wrapping algorithms

- Certificate checking including OCSP response validation

- Key management

- The DCF and RO formats, including RO (REL) fields expressing permissions and constraints

- Replay Protection for ROs

- DCF integrity protection

- Content Differentiation

- User Editable Metadata

- RO Installation Confirmation

- Binary encoding for ROAP Triggers

2. For Connected Devices the functionality above under 1. and additionally

- DRM Time and DRM Time synchronisation

- Support for connectivity to Rights Issuers

- HTTP Transport Mapping

- Capability signalling

- Transaction Tracking

- Metering

3. For Unconnected Devices the functionality above under 1. and additionally

- Support for utilizing connectivity provided by a connected device, for example via OBEX

4. For Unconnected Devices that support DRM Time the functionality above under 3. and additionally

- Metering

The DRM specifications also define the following optional client functionality:

- Domains

- Export to other DRMs

- PDCF

- IMSI and WIM binding

- RO Upload

The minimum mandatory server functionality for the DRM specifications includes:

- ROAP schema parsing and processing

- Certificate processing, including OCSP validation

- The ROAP protocol PDUs

- ROAP Trigger support

- Certain hash, MAC, Signature, and Key Wrapping algorithms

- Key management

- The RO format, including RO fields expressing m\permissions and constraints

- Parent Rights Objects

- Domains

- Transaction Tracking

- Metering

- Content Differentiation

- User Editable Metadata

- RO Installation Confirmation

The DRM specifications also define the following optional server functionality:

- Hash Chain support for Domain Key Generation

- RO Upload

- Binary encoding for ROAP Triggers

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 [IOPPROC].

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 [IOPPROC] and it MUST accurately reflect the architectural requirement of the **Item** in question.

8. ERDEF for DRM - Client Requirements

This section is normative.

Table 2: ERDEF for DRM Client-side Requirements

Item	Feature / Application	Status	Requirement
OMA-ERDEF-DRMv2.1-C-001	DRM 2.1 Client	M	OMA-ERDEF-DRMv2.1-C-002 OR OMA-ERDEF-DRMv2.1-C-003
OMA-ERDEF-DRMv2.1-C-002	Connected Device	O	DRM-v2.1:MCF AND DRM-CLI-CMN-024 AND DRM-CLI-CD-053 AND DRM-CLI-CD-054 AND DRM-CLI-CD-057 AND DRM-CLI-CD-058 AND DRM-CLI-CD-061 AND DRM-CLI-CD-062 AND DRM-CLI-CD-063 AND DRM-CLI-CD-069 AND DRM-CLI-CMN-071 AND DRM-CLI-CMN-072 AND DRM-CLI-CMN-073 AND DRM-CLI-CMN-074 AND DRMREL-v2.1:MCF AND DRM-REL-GEN-C-018 AND DRM-REL-GEN-C-019 AND DRM-REL-GEN-C-020 AND DRM-REL-GEN-C-021 AND DRM-REL-GEN-C-022 AND DRM-REL-GEN-C-023 AND DRMCF-v2.1:MCF
OMA-ERDEF-DRMv2.1-C-003	Unconnected Device	O	DRM-v2.1:MCF AND DRM-CLI-CMN-015 AND DRM-CLI-UD-065 AND DRM-CLI-UD-066 AND DRM-CLI-UD-067 AND DRM-CLI-UD-068 AND DRMREL-v2.1:MCF AND DRMCF-v2.1:MCF

Note: A DRM 2.1 client is either a Connected Device, with mandatory requirements as stated in the second row, or an Unconnected Device, with mandatory requirements as stated in the third row.

9. ERDEF for DRM - Server Requirements

This section is normative.

Table 3: ERDEF for DRM Server-side Requirements

Item	Feature / Application	Status	Requirement
OMA-ERDEF-DRMv2.1-S-001	DRM 2.1 Server	M	DRM-v2.1:MSF AND DRMREL-v2.1:MSF

Appendix A.   Change History   (Informative)

A.1   Approved Version History

Reference	Date	Description
OMA-ERELD-DRM-V2_1-20081014-A	10 Oct 2008	Status changed to Approved by TP ref# OMA-TP-2008-0382-INP_DRM_V2_1_ERP_for_Final_Approval
OMA- ERELD-DRM -V2_1_1-20100406-A	06 Avr 2010	Status changed to Approved by TP ref# OMA-TP-2010-0135-INP_DRM_V2_1_1_ERP_for_Candidate_re_approval
OMA- ERELD-DRM -V2_1_2-20110531-A	31 May 2011	Status changed to Approved by TP ref# OMA-TP-2011-0181-INP_DRM_V2_1_2_ERP_for_notification