Enabler Release Definition for DRM V2.0

Candidate Version 2.0 – 07 Dec 2004

Open Mobile Alliance

OMA-ERELD-DRM-V2_0-20041207-C

Contents

Figures

Tables

1. Scope

The scope of this document is limited to the Enabler Release Definition of Digital Rights Management 2.0 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 1.1, Open Mobile Alliance™, OMA-IOP-Process-V1_1, URL:http://www.openmobilealliance.org/

[DRMREQ-v2] "OMA DRM Requirements V2.0". Open Mobile Alliance™. OMA-DRM-REQ-V2_0. http://www.openmobilealliance.org/

[DRM-v2] "OMA DRM V2.0". Open Mobile Alliance™. OMA-DRM-DRM-V2_0. http://www.openmobilealliance.org/

[DRMCF-v2] "OMA DRM Content Format V2.0". Open Mobile Alliance™. OMA-DRM-DCF-V2_0. http://www.openmobilealliance.org/

[DRMREL-v2] "OMA DRM Rights Expression Language V2.0". Open Mobile Alliance™. OMA-DRM-REL-V2_0. http://www.openmobilealliance.org/

[DRMERELD-v2] "Enabler Release Definition for DRM V2.0". Open Mobile AllianceTM. OMA-DRM-ERELD-V2_0. http://www.openmobilealliance.org/ *[this document]*

2.2 Informative References

[DRMARCH-v2] "OMA DRM Architecture V2.0". Open Mobile Alliance™. OMA-DRM-ARCH-V2_0. http://www.openmobilealliance.org/

[DRMETR-v2] "Enabler Test Requirements for DRM V2.0". Open Mobile Alliance™. OMA-DRM-ETR-V2_0. http://www.openmobilealliance.org/

[DRMDTD-v2] Informative support file to [DRMREL-v2], filename "DRMREL20.dtd", containing the REL DTD file

Note: this file is for convenience provided in the enabler package

[DRMXSD-v2] Informative support file to [DRMREL-v2], filename "OMA-DD.xsd", containing the Data Dictionary V2.0 XML Schema

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. 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 a rights expression language.

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. It builds upon the OMA DRM 1.0 enabler release, but extends it 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 1.0.

The main differences between OMA DRM 1.0 and OMA DRM 2.0 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 online revocation check of them, and by confidentiality and integrity protecting rights objects. A Rights objects 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.

Improved functionality and usability is for example achieved by 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 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 Formats are 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:

"DRM Architecture V2.0"	[DRMARCH-v2]	Defines the overall architecture for DRM 2.0 including informative descriptions of the technologies and their uses
"DRM Specification V2.0"	[DRM-v2]	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
"DRM Rights Expression Language V2.0"	[DRMREL-v2]	Defines the rights expression language used to describe the permissions and constraints governing the usage of DRM protected media objects Note: in the enabler package, this document is accompanied by the informative support files [DRMDTD-v2] and [DRMXSD-v2]
"DRM Content Format V2.0"	[DRMCF-v2]	Defines the content format for DRM protected (encrypted) media objects
"DRM Requirements V2.0"	[DRMREQ-v2]	Defines the requirements for the DRM 2.0 specifications

The mentioned specifications comprising the DRM V2.0 enabler include the following XML documents:

- XML Schemas for the Rights Object Acquisition Protocol (ROAP) protocol data units as defined in [DRM-v2], Appendix A.
- XML Schema for the Rights Object Acquisition Protocol trigger media type as defined in [DRM-v2], Section 5.2.1.
- XML Schema / DTD for the Rights Expression Language as defined in [DRMREL-v2], Section 6.2.

6. Minimum Functionality Description for DRM

This section is informative.

There exist two different types of OMA DRM 2.0 clients: Unconnected Devices, and Connected Devices (for a definition, see [DRM-v2], 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

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

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

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

The DRM specifications also define the following optional client functionality:

- Domains
- Export to other DRMs
- PDCF
- IMSI and WIM binding

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

The DRM specifications also define the following optional server functionality:

- Hash Chain support for Domain Key Generation

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 1 ERDEF for DRM Client-side Requirements

Item	Feature / Application	Status	Requirement
OMA-ERDEF-DRMv2-C-001	DRM 2.0 Client	M	OMA-ERDEF-DRMv2-C-002 OR OMA-ERDEF-DRMv2-C-003
OMA-ERDEF-DRMv2-C-002	Connected Device	O	DRM-v2:MCF AND DRM-CLI-CMN-024 AND DRM-CLI-CD-053 AND DRM-CLI-CD-054 AND DRM-CLI-CD-056 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 DRMREL-v2: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:MCF
OMA-ERDEF-DRMv2-C-003	Unconnected Device	O	DRM-v2:MCF AND DRM-CLI-UD-065 AND DRM-CLI-UD-066 AND DRM-CLI-UD-067 AND DRM-CLI-UD-068 AND DRMREL-v2:MCF AND DRMCF-v2:MCF

Note: A DRM 2.0 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 2 ERDEF for DRM Server-side Requirements

Item	Feature / Application	Status	Requirement
OMA-ERDEF-DRMv2-S-001	DRM 2.0 Server	M	DRM-v2:MSF AND DRMREL-v2: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	1 April 2004	n/a	Initial version
	15 April 2004	n/a	Incorporating comments from REL Chair Change to current ERELD template
	20 April 2004	n/a	Version for consistency review Introduction of unconnected and connected device classes Bug fixes and clerical changes Extended functional description
	17 June 2004	n/a	Version incorporating resolutions on comments from the consistency review, and reflecting changes in the static conformance requirements of the specifications comprising the enabler
Candidate Version OMA-ERELD-DRM-V2_0	15 Jul 2004	n/a	Status changed to Candidate by TP TP ref # OMA-TP-2004-0229-DRM-V2_0-for-candidate-approval
	07 Dec 2004	None	Update for new public specification release after incorporation of a series of change requests into [DRM-v2], [DRMCF-v2] and [DRMREL-v2]. Note: although the requirements tables in this documents have not changed, please note that some of the referred requirements have changed in [DRM-v2] (DRM-CLI-CMN-021, DRM-SERVER-009) and [DRMCF-v2] (DRM-DCF-CLI-9). TP ref #OMA-TP-2005-0054-INP_Notifcation_of-CRs_to_DRM2