Enabler Validation Plan for DRM

Candidate Version 2.2 – 06 Dec 2011

Open Mobile Alliance

OMA-EVP-DRM-V2_2-20111206-C

Contents

Figures

Tables

1. Scope

This document details the Validation plan for the DRM 2.2 Enabler Release. The successful accomplishment of the validation activities will be required for the Enabler to be considered for Approved status.

The validation plan for the DRM 2.2 Enabler Release specifications is based on testing expectations in the Enabler Test Requirements (ETR). While the specific test activities to be performed are described in the Enabler Test Specification (ETS) the test environment is described in this plan. This test environment details infrastructure, operational and participation requirements identified for the needed testing activities.

The list of specifications, defining the scope of DRM 2.2, as stated in [ERELD] is according to the following:

- DRM Requirements V2.2 [DRMREQ-v2.2]
- DRM Architecture V2.2 [DRMARCH-v2.2]
- DRM Specification V2.2 [DRM-v2.2]
- DRM Rights Expression Language V2.2 [DRMREL-v2.2]
- DRM Content Format V2.2 [DRMCF-v2.2]
- DRM ROAP Schema V2.2 [DRMROAPXSD-v2.2]

In addition to the mentioned specifications comprising the DRM V2.2 enabler a data dictionary (DTD) for the Rights Expression Language as defined in [DRMREL-v2.2], Section 6.2.

1.1 Assumptions

None

1.2 Exclusions

None

2. References

2.1 Normative References

[DRMCF-v2.2] "OMA DRM Content Format V2.2", Open Mobile Alliance™, OMA-DRM-DCF-V2_2, http://www.openmobilealliance.org/

[DRMERELD-v2.2] "Enabler Release Definition for DRM V2.2", Open Mobile Alliance™, OMA-DRM-ERELD-V2_2. http://www.openmobilealliance.org/

[DRMETR-v2.2] "OMA DRM Enabler Test Requirements V2.2", Open Mobile Alliance™, OMA-DRM-ETR-V2_2. http://www.openmobilealliance.org/

[DRMREL-v2.2] "OMA DRM Rights Expression Language V2.2", Open Mobile Alliance™. OMA-DRM-REL-V2_2, http://www.openmobilealliance.org/

[DRMREQ-v2.2] "OMA DRM Requirements V2.2", Open Mobile Alliance™, OMA-DRM-REQ-V2_2, http://www.openmobilealliance.org/

[DRMROAPXSD-v2.2] "DRM ROAP schema V2.2", Open Mobile Alliance™, OMA-SUP-XSD_DRM_ROAP-V2_2, http://www.openmobilealliance.org/

[DRM-v2.2] "OMA DRM V2.2", Open Mobile Alliance™, OMA-DRM-DRM-V2_2, http://www.openmobilealliance.org/

[IOPPROC] "OMA Interoperability Policy and Process", Version 1.11, Open Mobile Alliance™, OMA-ORG-IOP_Process-V1_11, URL:http://www.openmobilealliance.org/

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

2.2 Informative References

[DRMETS-v2.2] "OMA DRM Enabler Test Specification for DRM Enabler", Open Mobile Alliance™. OMA-ETS-DRM-V2_2, 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”, are normative, unless they are explicitly indicated to be informative.

3.2 Definitions

Content	One or more Media Objects
Content Issuer	The entity making content available to the DRM Agent in a Device.
Device	A Device is the entity (hardware/software or combination thereof) within a user-equipment that implements a DRM Agent. The Device is also conformant to the OMA DRM specifications.
DRM Agent	A user agent in the device that enforces the rights and controls the consumption of DRM content on the device.
Media Object	A digital work e.g. a ringing tone, a screen saver, a Java game or a Composite Object.
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.
ROAP Trigger	An XML document including a URL that, when received by the Device, initiates the ROAP.

3.3 Abbreviations

DCF	DRM Content Format
DRM	Digital Rights Management
OCSP	Online Certificate Status Protocol
OMA	Open Mobile Alliance
PLMN	Public Land Mobile Network
PPG	Push Proxy Gateway
REL	Rights Expression Language
RI	Rights Issuer
RO	Rights Object
ROAP	Rights Object Acquisition Protocol
SCR	Static Conformance Requirement
WAP	Wireless Application Protocol

4. Enabler Validation Description

It is intended that TestFests will be the primary validation method for OMA DRM 2.2. Please refer to section 5 for further information.

5. TestFest Activities

5.1 Enabler Test Guidelines

A full description of DRM 2.2 can be found in [DRMERELD-v2.2] and related specifications.

DRM is essentially the means by which the management of rights to digital content, including its confinement to authorized usage, users and distribution, is controlled.

DRM 2.0, in addition to the basic functionality provided by DRM 1.0, addresses the complete security necessary for a robust, end-to-end DRM system that takes into account the needs for secure distribution, authentication of Devices, revocation and other aspects.

DRM 2.1 is a minor extension of DRM 2.0 enabling new functionality such as Metering, Confirmed Rights Object Acquisition protocols, Device Identification protocol and Rights Object uploading (optional).

OMA DRM v2.2 has been developed as a result of market feedback. The main differences between OMA DRM v2.2 and OMA DRM v2.1 are the addition of the new features, including:

- Advertisement management that provides support for various advertisement-based content acquisition and consumption models (see [DRMARCH-v2.2]) and incorporates the following functionality:
    - Enforced Advertising, a mechanism to enforce mandatory rendering of Advertisements while normal content is consumed. The advertisement content can be delivered along with the normal DRM content or separately from the advertising source. The rules of enforced rendering are contained either in the RO (see [DRMREL-v2.2]) or in DCF (see [DRMDCF-v2.2]).
    - Extension of metering for advertising, that specifies the metrics for advertisement content that can be collected and reported to the RI.
- Key management extension for multicast streaming protection support (see section 7.4).
- OMA DRM protection of MPEG2 Transport Streams as defined in [DRMDCF-v2.2].
- Extended support of games and executables as defined in [DRMREL-v2.2]

The DRM 2.2 features have minimum impact on the DRM 2.1 architecture and are defined in a backward compatible manner.

5.1.1 Minimal Test Configuration

The minimal (hardware and software) configuration for testing DRM 2.2 is:

- **Public Key Infrastructure** – at least two Certificate Authorities each with an associated OCSP Responder.
- **Client implementation** – at least two devices (mobile phone, PC, or other) that implement a DRM Agent. The devices must be able to transfer content from one device to another via any available means. Client implementations must be able to consume/render DRM Content to allow evaluation of the test case pass criteria.
- **Server implementation** – at least one server consisting of both a Content Issuer and a Rights Issuer. It is expected that server vendors attending OMA DRM 2.1 Test Fests are capable of acting as both Content Issuers and Rights Issuers and their product will contain an appropriate WEB and/or WAP portal to fulfill these tasks. If the pre-requisite for a test case is that there is a DCF stored on the terminal, then these DCFs will be packaged and delivered by the server vendors. It is recommended that the Content Issuer support several delivery models using both HTTP and OMA Download OTA as defined in Appendix G.2 and G.3 of [DRM-v2.2].
- **Streaming Server** – optionally the Server Implementation may be combined with a MPEG2 streaming server.

PKI Provisioning – both DRM Agents and Rights Issuers must be provisioned with certificates and keys issues by the Trust Anchors,

5.1.2 Minimal Participation Guidelines

Minimum Client Participants: 1

Minimum Server Participants: 1

In addition to these minimum participation requirements it is suggested that the ratio of Server to Client implementations be limited to a maximum of 2:1. For example if four server implementations are available no more than eight client implementations should be permitted to participate.

5.1.3 Optimal TestFest Achievement Guidelines

The ETS Test Cases listed below represent a subset of all the Test Cases for the Enabler that it is thought can be executed in a test session at an OMA TestFest. This list is intended to facilitate maximum test coverage of the functionality of the enabler within a test session. It is not intended to be the only tests executed at a TestFest, and teams are encouraged to execute more tests if they are able to do in the time allowed.

The list includes:

Test Case ID	Test Case Title
DRM-2.2-int-001	<playout> requirement
DRM-2.2-int-002	<displayout> requirement
DRM-2.2-int-003	<executeout> requirement
DRM-2.2-int-004	<playout> requirement with <enforcement-count> parameter
DRM-2.2-int-005	<discrete> constraint
DRM-2.2-int-006	<access> permission with <access-code> requirement
DRM-2.2-int-007	Requesting RO for MPEG2DCF
DRM-2.2-int-008	Descrambling MPEG2DCF
DRM-2.2-int-009	Enforced advertisements in MPEG2DCF via access criteria descriptor in KSM
DRM-2.2-int-010	Enforced advertisements in MPEG2DCF via Enforced Advertising Service ECM
DRM-2.2-int-011	Metering for advertisements

5.2 Enabler Test Requirements

Testing requirements for DRM are specified in [DRMETR-v2.2], which divides the test requirements into 3 major parts:

- DRM test requirements
- DRM Content Format test requirements
- DRM Rights Expression Language test requirements

The testing assertions shall reflect all possible high-level functionality of the mentioned areas, both in a normal and error flow.

5.2.1 Test Infrastructure Requirements

To prove interoperability of implementations it is essential to conduct the testing in an end-to-end environment. The environment has to be configured to allow clients under test easy access to the servers under test. It is desirable that the test environment allows for all methods (HTTP, WAP Push, MMS) of delivery of rights objects to the DRM client. The requirements on the testing environment are itemized as follows:

- **Local Area Network (LAN)** – providing connection between PC client implementations and server implementations as well as providing an interface between the server implementation and other infrastructure components.
- **Public Internet Access** – enabling connection to: remotely hosted server implementations and remotely hosted OCSP responders,
- **PLMN** (mobile telephony network) with an aired interface over GSM, UMTS or CDMA.
- A **Push Proxy Gateway** (PPG).

- **Multimedia Messaging Service Center (MMSC)** – optionally the Server Implementation may be integrated with an MMSC to deliver DRM Content and ROAP Triggers via MMS.
- Two **Trust Anchors** (Certificate Authorities) each providing an **OCSP Responder**.
- **SIM cards** for all GSM/UMTS mobile phone based client implementations.

Server Implementations may be hosted either within the TestFest Local Area Network or hosted remotely and accessed via the Internet. In the following conceptual figure, all involved elements of the test fest and all used protocols are depicted.

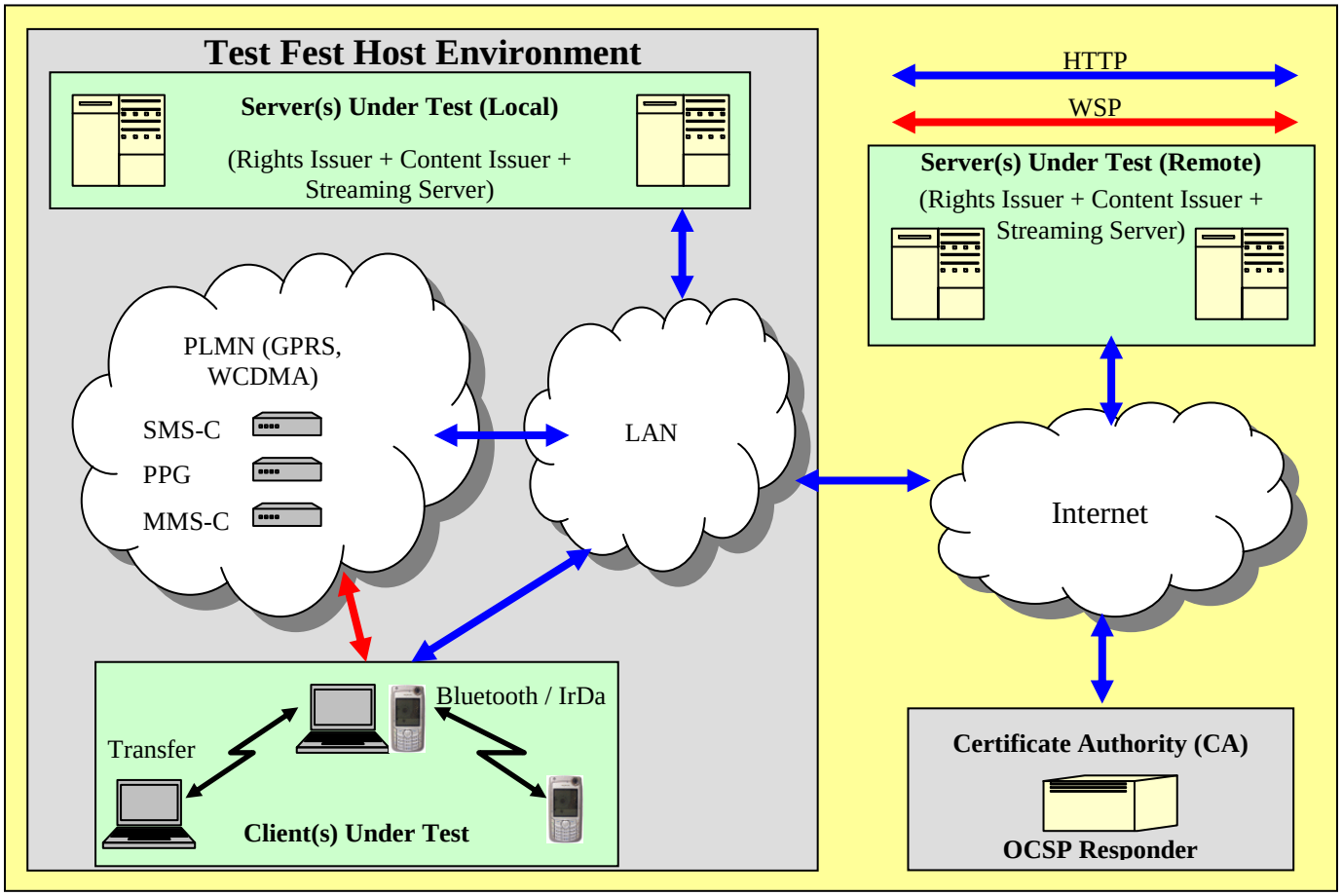

Figure 1 – DRM Testing Infrastructure

5.2.2 Public Key Infrastructure

In order to successfully conduct conformance and interoperability tests, Server and DRM Agent have to agree upon some system parameters, generally referred to as Public Key Infrastructure (PKI). Normally this PKI is defined by the Trust Anchor.

For the purpose of Conformance and Interoperability Tests the default PKI model (see PKI Model A below) shall always be available. In the default model only the RI certificate in the RI certificate chain is revocable. Other PKIs models may also be used if they are available.

5.2.2.1 PKI Model A

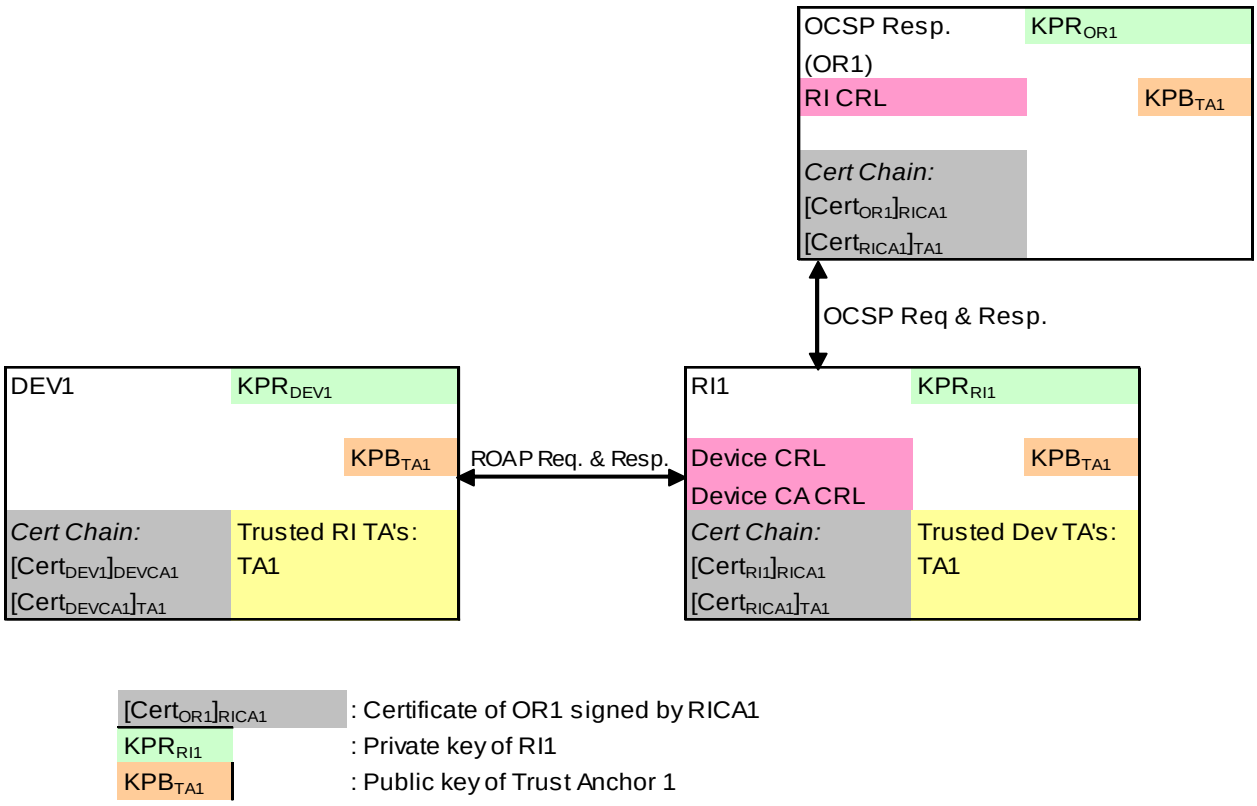

Figure 2 – PKI for conformance and IOP tests

The characteristics of this PKI are:

- It features one Trust Anchor (TA1) thus,
    - the device holds one Certificate chain , one private key and the certificate of one Trust Anchor and it has one entry in the Trusted RI Authority list : TA1
    - the RI holds one Certificate chain , one private key and the certificate of one Trust Anchor and it has one entry in the Trusted Device Authority List : TA1
- The Certificate chain of the Device contains the Device certificate and the certificate of one intermediate Device CA
- The Certificate chain of the RI contains RI certificate and the certificate of one intermediate RI CA
- The Certificate chain of the OCSP responder contains the Responder certificate and the certificate of the intermediate RI CA
- The RI CA has delegated the OCSP response authority (OCSP certificate with **id-kp-OCSPSigning** extension**)**
- OCSP certificate is not revocable (OCSP certificate with **id-pkix-ocsp-nocheck** extension**)**
- The RI holds a Device CRL that it uses to determine revocation status of devices
- The RI holds a Device CA CRL that it uses to determine the revocation status of Device CA's
- The OCSP responder holds a RI CRL that it uses to determine the revocation status of RI's

- The RI CA is not revocable.

All data structures in Device, RI and OCSP responder are loaded in this system with out-of-band tools.

5.2.3 Enabler Execution Flow

DRM interoperability testing is limited to high-level DRM functionality testing of DRM Agent (client) and Rights Issuer (server) implementations. The testing shall cover:

- Client/server protocols (ROAP)
- Implementation of DRM restrictions
- Correct processing of file formats (e.g. format of content and rights objects)

The following sub-sections detail the principle execution flows covered by the interoperability tests of OMA DRM 2.2. These demonstrate the interactions between clients, servers and the requisite network infrastructure (PPG and OCSP Responder).

Most client-server communication in OMA DRM 2.2 is defined to use HTTP. The HTTP protocol can be implemented over any IP bearer such as a mobile WAP network, or a Local Area Network (LAN).

5.2.3.1 ROAP Trigger

The majority of client-server interactions are initiated via a ROAP Trigger object. The following sequence diagram depicts the use of the ROAP Trigger to initiate the majority of ROAP protocols. All ROAP communication is over HTTP.

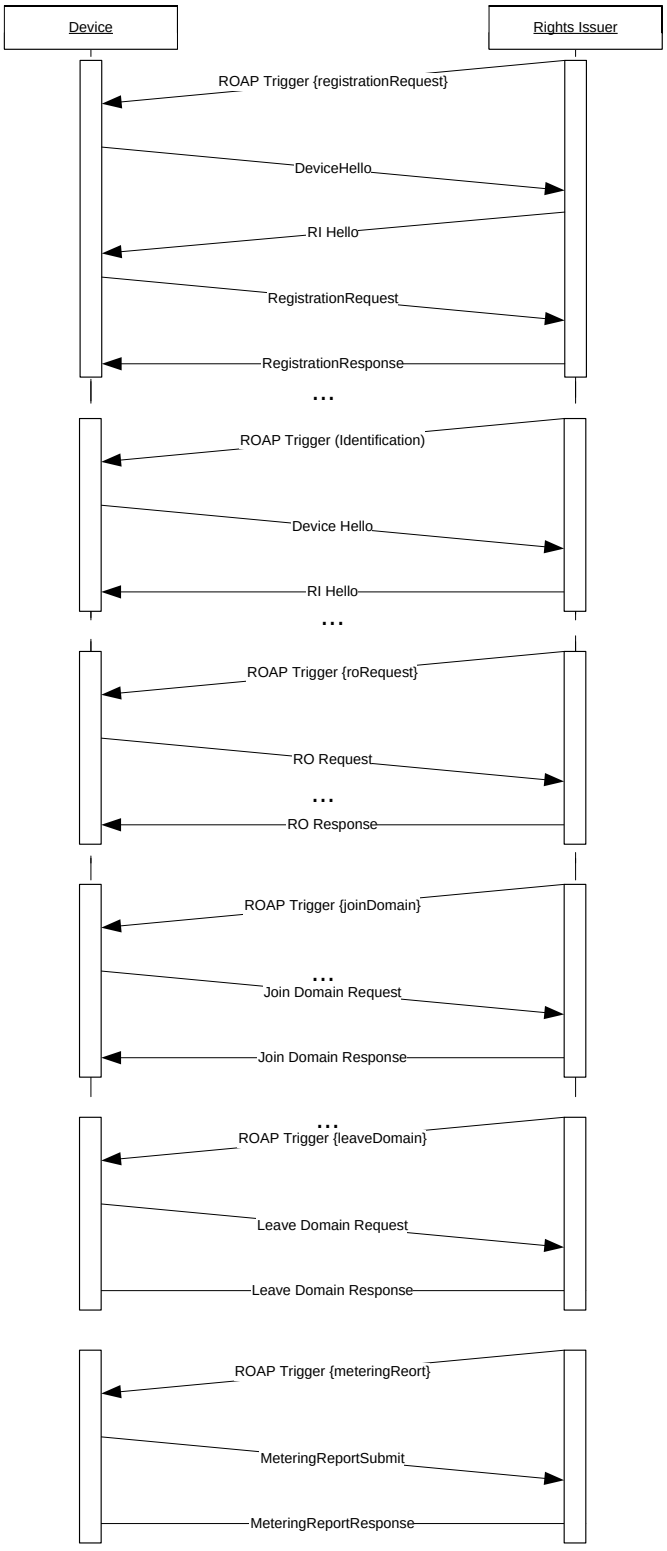

Figure 3 – ROAP Trigger

5.2.3.2 OCSP Responder Interaction

During ROAP communication between the DRM Agent and the Rights Issuer, the RI may initiate a HTTP request to the OCSP Responder as shown in the following sequence diagram depicting the ROAP 4-Pass RO Acquisition Protocol.

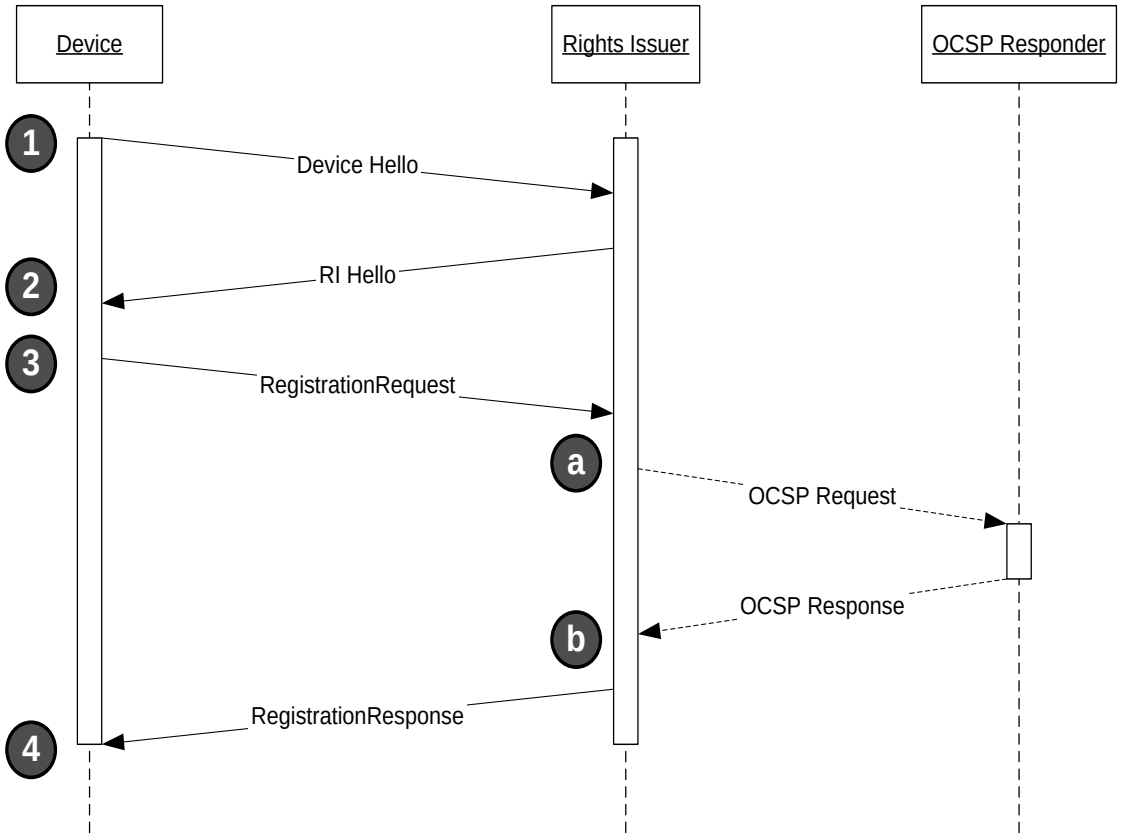

Figure 4 – ROAP 4-Pass RO Acquisition

5.2.4 Test Content Requirements

Server Implementations (Content Issuers) are expected to support DCF packaging of arbitrary media formats and should allow Client Implementers to provide their own content for the purpose of testing. It is recommended that Content Issuers by default host at least the following Media Types:

- audio/mp4
- audio/mpeg
- audio/x-wav
- image/png
- image/gif
- image/jpeg
- image/bmp
- application/java-archive

OMA provides reference test content that are free of copy rights and can be used during TestFests:
http://www.openmobilealliance.org/testfest/docs/DRM/OMA-ETS-DRM-Test-Content-V2_0-20050829-A.zip

PDCF test cases require 3GPP media files (audio/3gpp and video/3gpp).

5.2.5 Test Limitations

5.2.5.1 Physical

None

5.2.5.2 Resources

Each interoperability test session (client + server) is expected to take 4 to 5 hours.

5.2.6 Test Restrictions

None

5.2.7 Test Tools

Client and Rights Issuer Conformance Test Tools may be provided for DRM 2.2.

5.2.7.1 Existing Tools to be Used

None

5.2.7.2 Test Tool Requirements

None

5.2.8 Resources Required

It is required that there is at least one dedicated human tester onsite at a Test Fest for each implementation tested.

Server teams may be asked to test multiple client implementations during a single test session but only if the server test team has a tester assigned to each client implementation.

Typically one tester per implementation is sufficient for mature implementations. However be aware that Interoperability test cases defined for OMA DRM 2.2 are extensive and to complete all test cases in a single test session is only possible if all test cases run without any problems. Therefore early implementations are recommended to assign at least two engineers for each implementation under test. This allows when engineer to run tests while another is investigating the cause of any problems.

5.3 Tests to be Performed

The following sections describe the tests related to the formal TestFest validation activities.

5.3.1 Entry Criteria for TestFest

Implementations entering a test fest must support all Mandatory SCRs as identified in [DRMERELD-v2.2].

5.3.2 Interoperability Test Cases

The following test cases from [DRMETS-v2.2] should be supported by implementations participating in a test fest based on the functional groups. Though all of the test cases of DRM 2.2 Enabler are optional, implementations of the functionality in the same functional group must support all of the high-priority test cases within the group.

Functional Group	Test Case	Section	Title	Priority
Advertisement management	DRM-2.2-int-1	6.1	<playout> requirement	High
	DRM-2.2-int-2	6.2	<displayout> requirement	Low
	DRM-2.2-int-3	6.3	<executeout> requirement	Low
	DRM-2.2-int-4	6.4	<playout> requirement with <enforcement-count> parameter	High
	DRM-2.2-int-5	6.5	<discrete> constraint	High
	DRM-2.2-int-11	6.11	Metering report for enforced advertisements	High
MPEG2DCF	DRM-2.1-int-7	6.7	Request RO for MPEG2DCF	High
	DRM-2.1-int-8	6.8	Descrambling of MPEG2DCF	High
	DRM-2.1-int-9	6.9	Advertisement enforcement using KSM access criteria descriptor	Low
	DRM-2.1-int-10	6.10	Advertisement enforcement using Enforced Advertising Service ECM	Low
Executables	DRM-2.2-int-6	6.6	<access> permission with <access-code> requirement	High

Table 1: IOP Test Cases

5.3.3 Pre-testing to be performed at TestFest

During Pre-Testing and connectivity tests at an OMA Test Fests participant teams must demonstrate correct execution of the following test cases:

- DRM-2.0-int-1 “Forward Lock”
- DRM-2.0-int-4 “ROAP Registration and RO Acquisition”

5.3.4 Testing to be Performed at TestFest

All tests defined in [DRMETS-v2.2] should be performed at a test fest.

5.3.4.1 Testing backwards compatibility with DRM 2.1

Since DRM 2.2 uses backwards compatibility mechanisms defined in DRM 2.0 and 2.1, there are no test cases or requirements related to backwards compatibility.

5.4 Enabler Test Reporting

5.4.1 Problem Reporting Requirements

Normal Reporting, no special reporting required.

5.4.2 Enabler Test Requirements

Normal Reporting, no special reporting required.

6. Alternative Validation Activities

Any results from bi/multi-lateral testing where OMA DRM 2.2 test cases have been used can be used to validate the enabler.

7. Approval Criteria

Normal Approval Criteria

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description

A.2 Draft/Candidate Version 2.2 History

Document Identifier	Date	Sections	Description
Draft Versions OMA-EVP-DRM-V2_2	27 Jun 2011	all	First Agreed draft baseline
	22 Nov 2011	6	Added other mechanisms for validation and history
Candidate Versions OMA-EVP-DRM-V2_2	06 Dec 2011	n/a	Status changed to Candidate by TP TP Ref# OMA-TP-2011-0422-INP_DRM_v2_2_EVP_for_Candidate_Approval

Appendix B. DRM Test Tool Requirements

The requirements in this section are derived from the initial test tool requirements developed for DRM 2.0.

B.1 Introduction

Currently there is an issue regarding the amount of time and resources that are consumed at our organized test events to establish the readiness of products. The ability to pre-test these products would drastically improve the overall quality of the test fest and would address the issue of conformance to the DRM-2.1 EICS prior to an event. In order to address this issue, the application of a test tool, which has the ability to automatically exercise the mandatory requirements in the DRM-2.1 enabler [DRMERELD-v2.2], is recommended by the working group.

Another issue is specific for DRM systems. In contrast to non-DRM systems (like most of the OMA Enablers), a DRM system has two types of requirements: Inter-operability Requirements and Security Requirements. In this context, security is related to measures that make sure that a user can only access content he or she is legitimate to access.

- **Inter-operability Requirements**

  Inter-operability Requirements are those requirements that make sure that the system works in cases that it should work. If not all of these requirements are met, one or more normal use cases will fail. Example of an Inter-operability Requirement in [DRM-v2.2]:

  "The following algorithms and associated RIs MUST be supported by all Devices and RIs:

  - SHA-1,
  - HMAC-SHA-1,
  - RSA-PSS-Default,
  - RSAES-KEM-KDF2-KW-AES128 and
  - AES-WRAP

- **Security Requirements**

  Security Requirements are those requirements that make sure that the system does NOT work in cases that it shall not work. If not all of these requirements are met, one or more illegal use cases will NOT fail. Examples of security Requirements in [DRM-v2.2] :

  - "The RI MUST verify the signature on the ROAP-RegistrationRequest message."
  - "If the Session ID of the ROAP-RegistrationResponse does not equal the Session ID of the corresponding ROAP-RIHello, the Device MUST terminate the protocol."

The traditional OMA conformance tests are related to Inter-operability Requirements. Since OMA-DRM 2.1 is a DRM system, special attention must be paid to Security Requirements. If this issue would not be addressed, implementations of the enabler (and even the specification itself) might suffer security problems. This, in turn might cause legal claims and might make content owners reluctant to provide high-value content for this system.

The Test Tool will be used for testing both Inter-operability Requirements and Security Requirements. The working group has collected and detailed the requirements for such a tool in this document.

The Test Tool can be used during the complete development process, until market introduction to automatically test compliance with the DRM-2.2 specification [DRMERELD-v2.2].

The objects to be tested are:

- OMA DRM Client as defined in [DRMERELD-v2.2]
- OMA DRM Rights Issuer as defined in [DRMERELD-v2.2]

The test tool allows conducting the conformance tests that have been specified in the conformance test section of [DRMETS-v2.2].

B.2 Requirements for Test Tool

B.2.1 Compliance

Wherever applicable the Test Tool and the data structures produced by it SHALL comply to [DRM-v2.2], [DRMCF-v2.2] and [DRMREL-v2.2].

B.2.2 PKI generator

The PKI generator SHALL support all PKI's as defined in the section 5.2.2.

B.2.3 Transport

The Test Tool SHALL use HTTP as default transport mechanism for ROAP, OCSP and content delivery.

B.2.4 Test Automation

All components of the Test Tool have a HTTP API. The Test Operator can use a WEB site for manual control of the Test Tool . Alternatively, the Test Operator can send HTTP messages, generated by a script generator to run automated tests.

B.2.5 Packaging

The Test Tool supports 'real time' generation of Right Objects included in a (P)DCF.

B.2.6 User Interface

The Test operator uses a WEB based Test User Interface for controlling the Test Tool and to retrieve test results.

The Test provides a means for the test operator to be prompted when manual action is required by a test.

The Test Tool provides a means for the test operator to enter observations/result information into the Test Tool when prompted.

The Test Tool logs all transactions and results.

The Test Tool present results and logs to the operator.

The Test Tool provides the operator with management tools for test tool configuration and parameterisation, test selection etc.

B.2.7 Operating Environment

There are no specific requirements for the hardware platform and operating that is used for the Test tool.

B.2.8 Multi Session Capability

The Test Tool supports the test of only one IUT simultaneously.