Enabler Validation Plan for DRM

Candidate Version 2.1 – 07 Aug 2007

Open Mobile Alliance

OMA-EVP-DRM-V2_1-20070807-C

Contents

Figures

Tables

1. Scope

This document details the Validation plan for the DRM 2.1 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 2.1 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 2.1, as stated in [ERELD] is according to the following:

- DRM Requirements V2.1 [DRMREQ-v2.1]
- DRM Architecture V2.1 [DRMARCH-v2.1]
- DRM Specification V2.1 [DRM-v2.1]
- DRM Rights Expression Language V2.1 [DRMREL-v2,1]
- DRM Content Format V2.1 [DRMCF-v2,1]
- DRM ROAP schema V2.1 [DRMROAPXSD-v2.1]

In addition to the mentioned specifications comprising the DRM V2.1 enabler a data dictionary (DTD) for the Rights Expression Language as defined in [DRMREL-v2.1], Section 6.2.

1.1 Assumptions

None

1.2 Exclusions

None

2. References

2.1 Normative References

[DRMCF-v2.1] "OMA DRM Content Format V2.1", Open Mobile Alliance™, OMA-DRM-DCF-V2_1, http://www.openmobilealliance.org/

[DRMEICS-C-v2.1] "OMA DRM Enabler Implementation Conformance Statement for Clients V2.1", Open Mobile Alliance™, OMA-EICS-DRM-Client-V2_1. http://www.openmobilealliance.org/

[DRMEICS-S-v2.1] "OMA DRM Enabler Implementation Conformance Statement for Servers V2.1", Open Mobile Alliance™, OMA-EICS-DRM-Server-V2_1, http://www.openmobilealliance.org/

[DRMERELD-v2.1] "Enabler Release Definition for DRM V2.1", Open Mobile Alliance™, OMA-DRM-ERELD-V2_1. http://www.openmobilealliance.org/

[DRMETR-v2.1] "OMA DRM Enabler Test Requirements V2.1", Open Mobile Alliance™, OMA-DRM-ETR-V2_1. http://www.openmobilealliance.org/

[DRMREL-v2.1] "OMA DRM Rights Expression Language V2.1", Open Mobile Alliance™. OMA-DRM-REL-V2_1, http://www.openmobilealliance.org/

[DRMREQ-v2.1] "OMA DRM Requirements V2.1", Open Mobile Alliance™, OMA-DRM-REQ-V2_1, http://www.openmobilealliance.org/

[DRMROAPXSD-v2.1] "DRM ROAP schema V2.1", Open Mobile Alliance™, OMA-TS-DRM-ROAP-V2_1, http://www.openmobilealliance.org/

[DRM-v2.1] "OMA DRM V2.1", Open Mobile Alliance™, OMA-DRM-DRM-V2_1, http://www.openmobilealliance.org/

[IOPPROC] "OMA Interoperability Policy and Process", Version 1.4, Open Mobile Alliance™, OMA-ORG-IOP_Process-V1_4, URL:http://www.openmobilealliance.org/

[IOPTFG] "OMA TestFest Participation Guidelines", Version 1.1, Open Mobile Alliance™, OMA-IOP-TestFest-Participation-Guidelines-V1_1, 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-CON-C-v2.1] "OMA DRM Enabler Test Specification for Client Conformance V2.1", Open Mobile Alliance™. OMA-ETS-DRM-CON-Client-V2_1, http://www.openmobilealliance.org/

[DRMETS-CON-S-v2.1] "OMA DRM Enabler Test Specification for Server Conformance V2.1", Open Mobile Alliance™, OMA-ETS-DRM-CON-Server-V2_1, http://www.openmobilealliance.org/

[DRMETS-IOP-v2.1] "OMA DRM Enabler Test Specification for Interoperability V2.1", Open Mobile Alliance™, OMA-ETS-DRM-INT-V2_1, 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 2.1. Please refer to section 5 for further information.

5. TestFest Activities

5.1 Enabler Test Guidelines

A full description of DRM 2.1 can be found in [DRMERELD-v2.1] 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 enabling a Rights Issuer to collect usage information (Metering Information) from Devices for the purpose of royalty collection.
- Confirmed Rights Object Acquisition protocols, providing Rights Issuers with notification of successful installation of ROs.
- Device Identification protocol, enabling a Content Issuer to identify the DRM properties of a device before issuing content or rights.
- [Optional] Rights Object uploading enabling a device to move a rights object to a server repository, possibly for the purpose of re-issue to a new device.

A conceptual picture of a DRM system, according to [DRMARCH-v2.1], is depicted in the following figure:

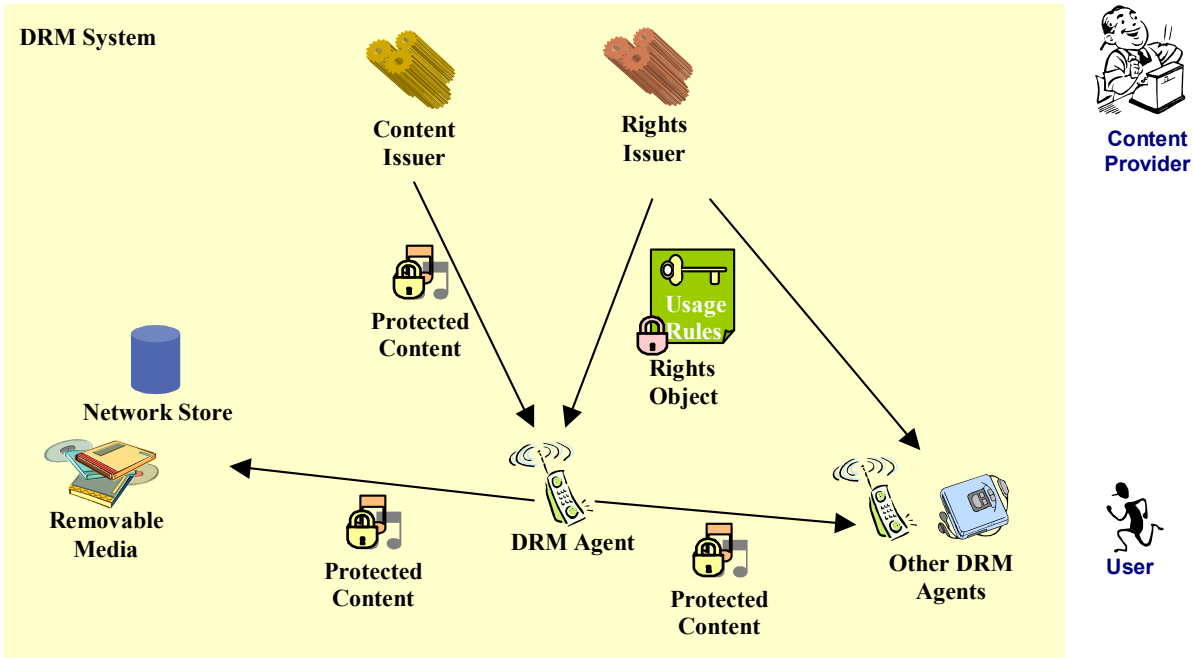

Figure 1 - DRM 2.1 Architecture

5.1.1 Minimal Test Configuration

The minimal (hardware and software) configuration for testing DRM 2.1 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-v2.1].
- **Streaming Server** – optionally the Server Implementation may be combined with a 3GP (or 3GP2) streaming server.
- **PKI Provisioning** – both DRM Agents and Rights Issuers must be provisioned with certificates and keys issues by the Trust Anchors,

To enable backwards compatibility testing Client and Server participants are requested to provide a previously tested DRM 2.0 implementation of their Client or Server. The DRM 2.0 implementations will be used only to execute the backwards compatibility tests defined in [DRMETS-IOP-v2.1].

5.1.2 Minimal Participation Guidelines

Minimum Client Participants: 3

Minimum Server Participants: 3

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-2.1-int-4	DRM 2.0 Registration and RO Acquisition
DRM-2.1-int-5	DRM 2.0 Join Domain and RO Acquisition
DRM-2.1-int-6	Domain RO Superdistribution
DRM-2.1-int-7	DRM 2.0 Leave Domain
DRM-2.1-int-8	Registration and RO Acquisition
DRM-2.1-int-13	RO Acquisition with confirmation (4-pass) with exiting RI context
DRM-2.1-int-14	RO acquisition with confirmation (3-pass) with existing RI context
DRM-2.1-int-15	RO Acquisition for multiple ROs
DRM-2.1-int-16	Device Identification
DRM-2.1-int-17	Device Time Synchronization
DRM-2.1-int-18	RO Upload for stateless ROs
DRM-2.1-int-19	RO Upload for stateful ROs
DRM-2.1-int-20	RO Upload for multiple ROs
DRM-2.1-int-21	Trigger initiated RO Upload
DRM-2.1-int-23	Rights Object for Group ID DCFs
DRM-2.1-int-30	Referencing Multipart Objects – CID mechanism

Test Case ID	Test Case Title
DRM-2.1-int-31	Referencing Multipart Objects – Content Location mechanism
DRM-2.1-int-33	RO Acquisition with TransactionID
DRM-2.1-int-37	Interval constraint
DRM-2.1-int-39	Individual constraint
DRM-2.1-int-40	System constraint
DRM-2.1-int-41	Multiple constraints
DRM-2.1-int-42	Top-level constraints
DRM-2.1-int-43	Expression Linking
DRM-2.1-int-44	Metering Reporting for a single DCF
DRM-2.1-int-45	REL <tracked> contentAccessGranted attribute
DRM-2.1-int-46	REL <tracked> timed attribute
DRM-2.1-int-47	Metering Report initiated via onExpiredURL
DRM-2.1-int-48	Metering Report initiated via a Parent Rights Object
DRM-2.1-int-50	Preview Header – In the Domain Name Whitelist
DRM-2.1-int-53	Multiple Parent Rights Objects
DRM-2.1-int-55	Domain join without existing RI Context
DRM-2.1-int-56	Domain No Consume After
DRM-2.1-int-57	New Domain RO delivered before domain upgrade
DRM-2.1-int-61	Sharing a DCF containing a RO between devices in the same domain
DRM-2.1-int-63	3GPP User Data
DRM-2.1-int-64	User Editable Meta Data
DRM-2.1-int-65	WBXML RO Acquisition Trigger
DRM-2.1-int-66	WBXML Leave Domain Trigger
DRM-2.1-int-72	Device with two certificates
DRM-2.1-int-76	One-track encrypted PDCF
DRM-2.1-int-77	Multi-track encrypted PDCF
DRM-2.1-int-78	PDCF Super Distribution (Transaction Tracking)
DRM-2.1-int-80	Group RO for PDCF
DRM-2.1-int-83	SDP initiated RO acquisition
DRM-2.1-int-84	Multi-track PDCF
DRM-2.1-int-85	Multipart/related delivery of DCF and ROAP Trigger
DRM-2.1-int-86	OMA Download Separate Delivery Method
DRM-2.1-int-87	OTA Download Combined Delivery Method

5.2 Enabler Test Requirements

Testing requirements for DRM are specified in [DRMETR-v2.1], 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. Since DRM basic functions are specified in DRM 1.0 and DRM 2.0, it's essential that the testing session cover backward compatibility of device, server, and content interactions.

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.

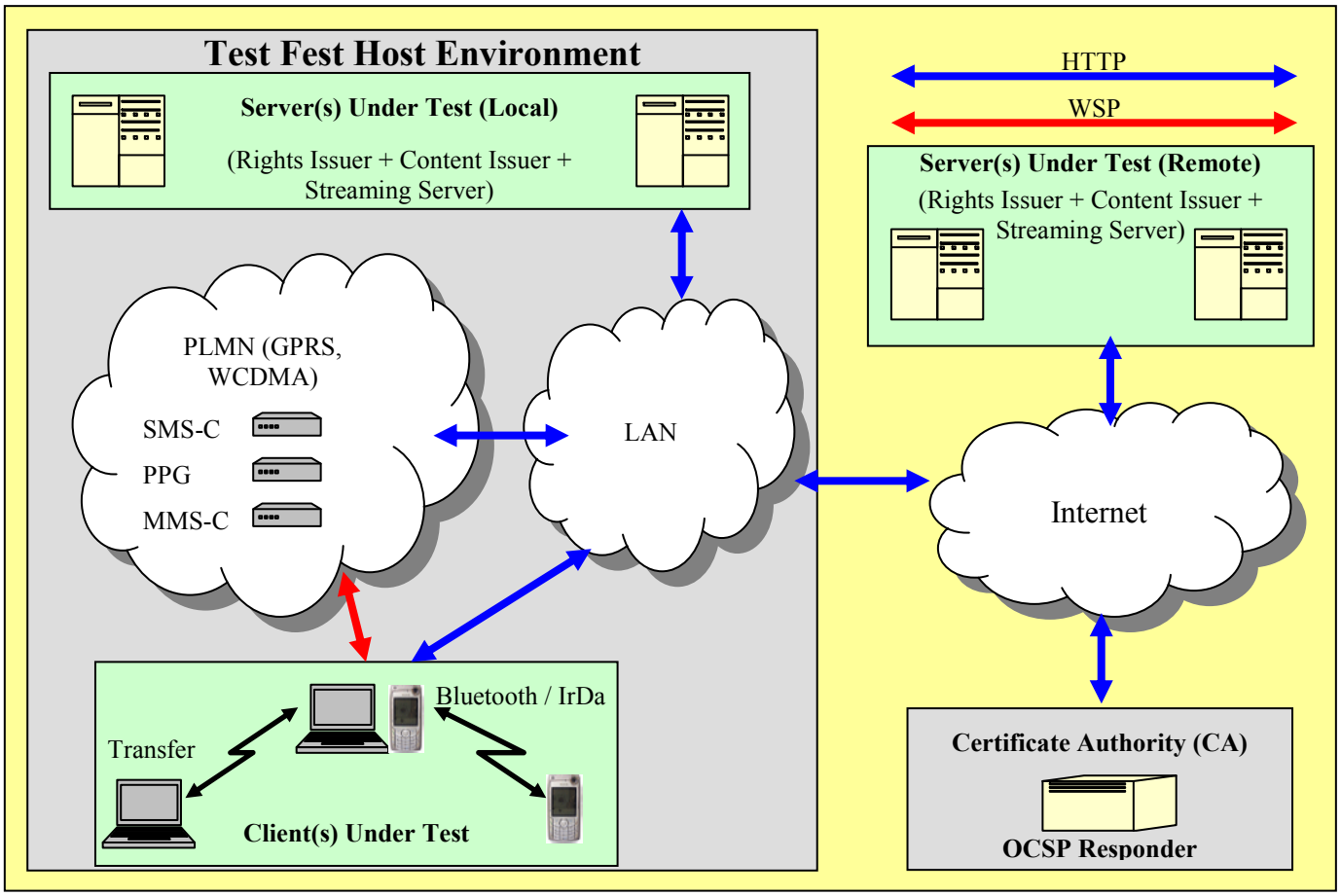

Figure 2 - DRM Testing Infrastructure

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

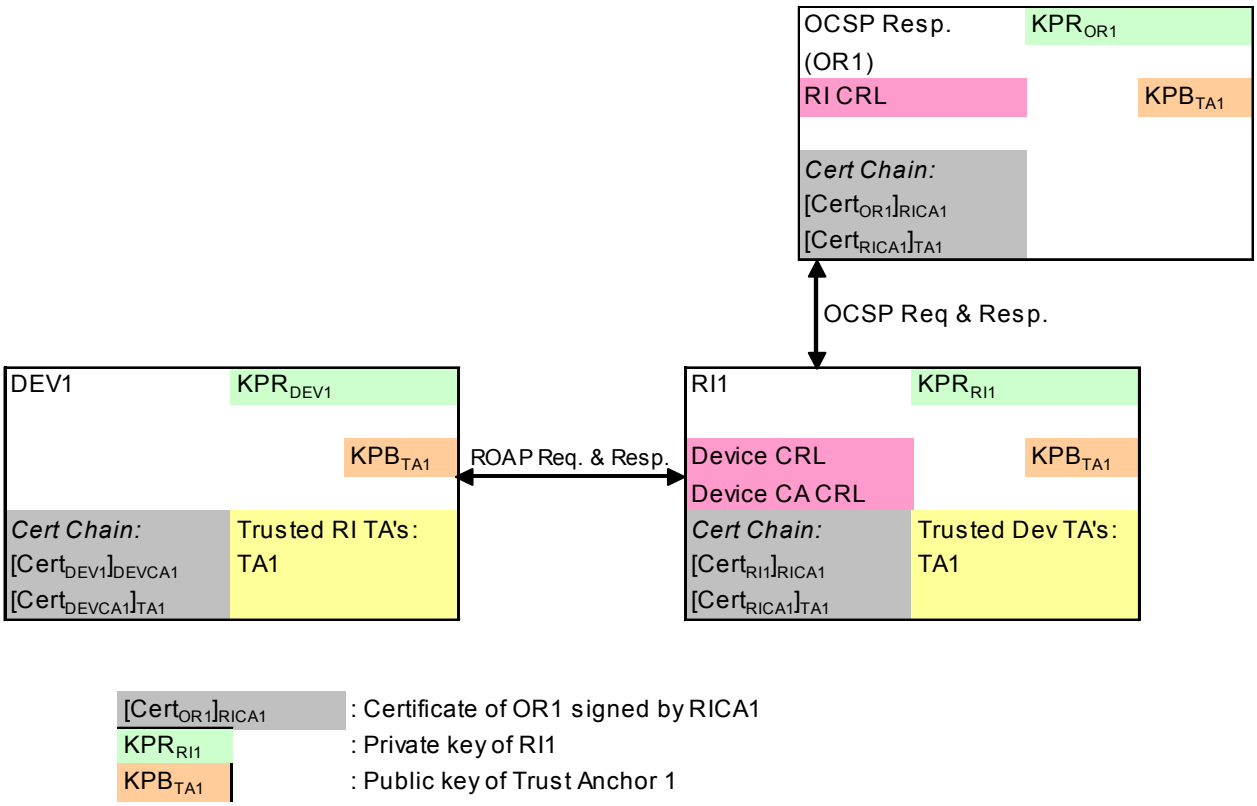

Figure 3: PKI for conformance and IOP tests

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:

- Backwards compatibility with DRM 2.0 and DRM 1.0
- Client/server protocols (ROAP)
- Implementation of DRM restrictions
- Correct processing of file formats (e.g. format of content and rights objects)
- Correct implementation of unconnected devices behaviours

The following sub-sections detail the principle execution flows covered by the interoperability tests of OMA DRM 2.1. These demonstrate the interactions between clients, servers and the requisite network infrastructure (PPG and OCSP Responder).

Most client-server communication in OMA DRM 2.1 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 DRM 1.0 Separate Delivery

DRM 1.0 Separate Delivery is tested as part of backwards compatibility testing. The interaction between the client and server is principally over HTTP for Content Delivery and relies on WAP Push for Rights Object delivery.

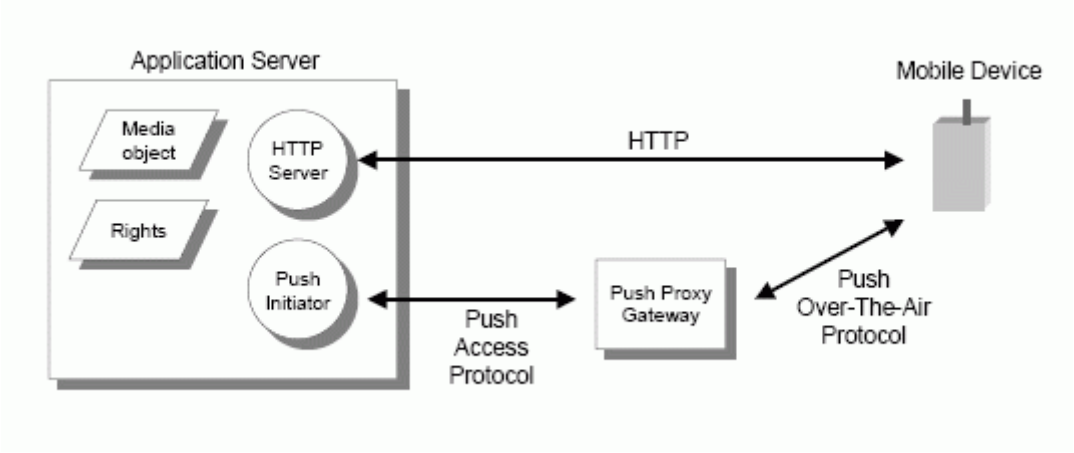

Figure 4 - DRM 1.0 Separate Delivery Architecture

5.2.3.2 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.

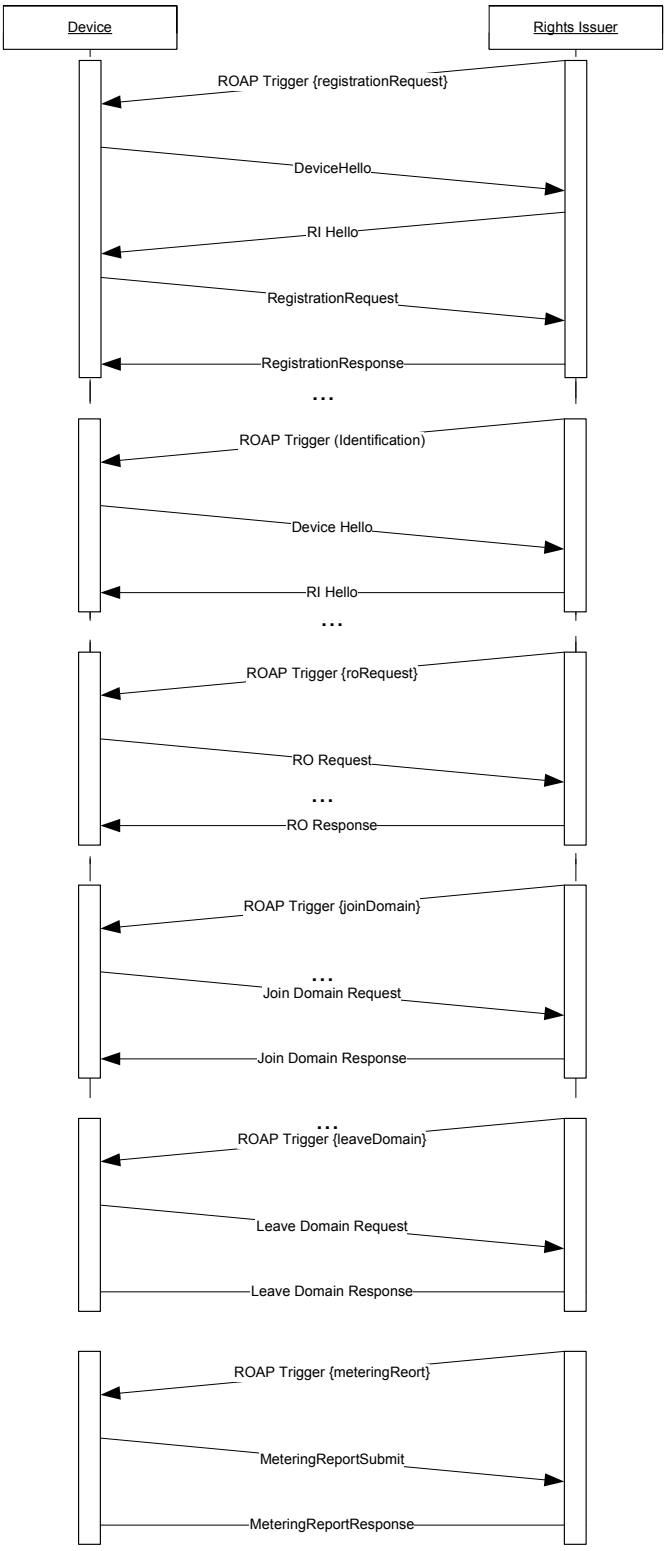

Figure 5 - ROAP Trigger

5.2.3.3 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.

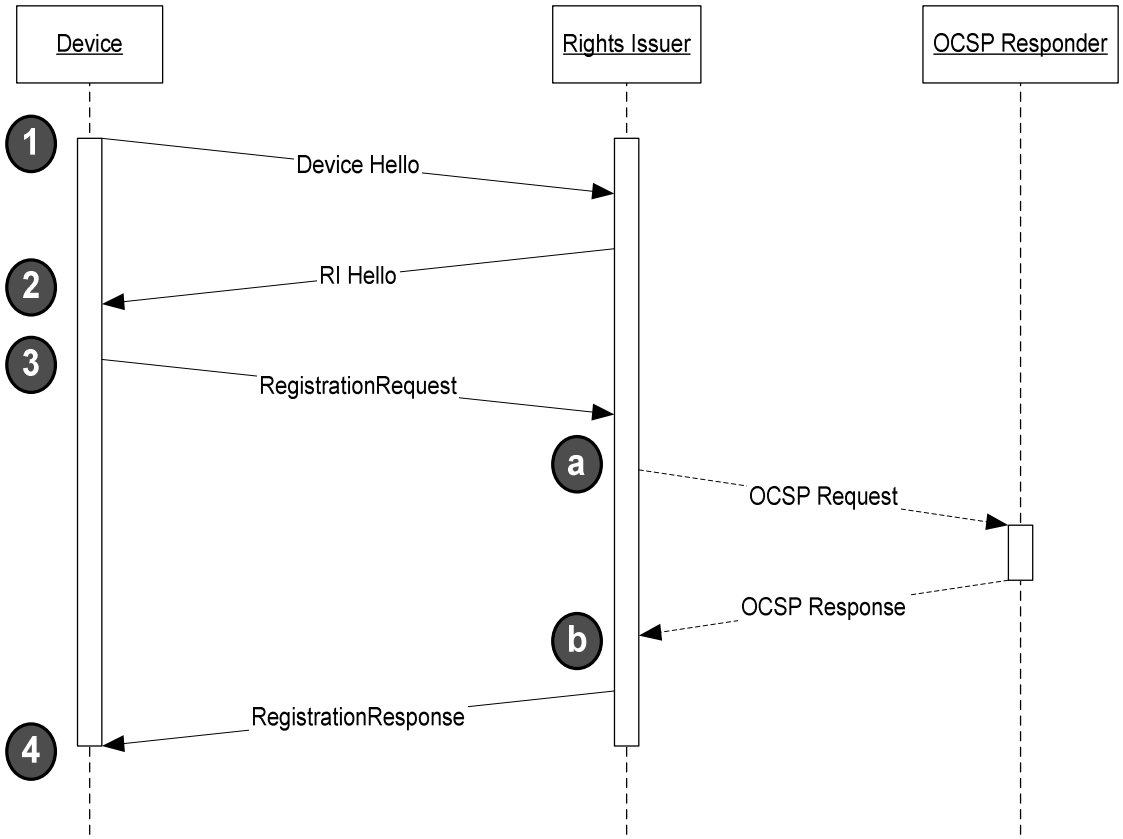

Figure 6 - ROAP 4-Pass RO Acquisition

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 should be provided for DRM 2.1.

5.2.7.1 Existing Tools to be Used

The Client Conformance Test Tool (CTT) for DRM 2.0 may be used to test backwards compatibility of DRM 2.1 implementations. Further information on the CTT can be found here:

http://www.openmobilealliance.org/testfest/IOP_Tools_DRM20.html

DRM 2.1 implementations should be fully compatible with the DRM 2.0 test tool and should be fully execute the DRM 2.0 test tool; and produce complete test reports.

5.2.7.2 Test Tool Requirements

The DRM 2.0 Client Conformance Test Tool should be extended to support additional test cases defined in [DRMETS-CON-C-v2.1].

A DRM 2.1 Rights Issuer Conformance Test Tool should be developed in accordance with the test tool requirements highlighted in Appendix B.

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 2.1 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

The following tests need to be performed and passed by implementations by members wishing to participate in the TestFest. This ensures minimal requisite capability of the implementations.

5.3.1.1 Client Implementations

Client implementations must execute and pass the following subset of tests from [DRMETS-CON-C-v2.1].

Test Case Id	Test Case Title
1a	ROAP trigger with expired RI context
5a, 5b, 5c	Missing Status attribute in ROAP Response
6a, 6b, 6c	Status != Success in ROAP Response
8a, 8b	Invalid Signature in ROAP Response
11a	Invalid signature in certificate chain of ROAP resonse
14a	RI Trusted Anchor not in DRM Agent's Trusted Authorities
16a, 16b	OCSP Handling / Missing OCSP response in ROAP response
18a	OCSP Handling / Invalid signature in OCSP response
23a	OCSP Handling / Recovation Status OCSP response = 'revoked'
30a	Invalid Session ID in registration response
32a	Invalid Device ID in ROAP response; 2 pass RO acquisition and Join Domain.
35a	Missing Device Nonce in ROAP response
38a	Invalid RI ID in ROAP response
39a	DRM Time Synchronise Triggered by Reg. Response
40a	Install Device RO from RO Response; Invalid Signature
48a	Install Device RO from DCF; Invalid MAC element
68a	Replay protection – Stateful RO with RITS; In Replay cache
74a	Wrong permissions for an image object
83a	Instant Preview
85a	Erroneous Count Constraint
86a	Erroneous Timed-Count Constraint
87a	Erroneous Datetime Constraint
88a	Erroneous Interval Constraint
89a	Erroneous Accumulated Constraint
90a	Error in inheritance model: Reference to non-existing Parent rights object.

Table 1: Mandatory tests for execution against DRM 2.0 CTT

Mandatory tests for execution against the DRM 2.1 CTT are yet to be defined.

5.3.1.2 Rights Issuer Implementations

No test fest entry criteria are defined for Rights Issuers.

5.3.2 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”

5.3.3 Testing to be Performed at TestFest

All tests defined in [DRMETS-IOP-v2.1] should be performed at a test fest.

5.3.3.1 Testing backwards compatibility with DRM 2.0

A number of the test cases in [DRMETS-IOP-v2.1] are intended to test interoperability between DRM 2.0 clients and DRM 2.1 Rights Issuers; as well as interoperability between DRM 2.1 clients and DRM 2.0 Rights Issuers. To enable testing of these test cases TestFest participants for DRM 2.1 are requested to provide an additional implementation of DRM 2.0. For example, a server vendor could bring a previously tested DRM 2.0 implementation for the purpose of testing backwards compatibility.

It is optional for participants to provide a previous implementation; but please remember backwards compatibility of DRM 2.1 with DRM 2.0 is critical to the success of DRM 2.1.

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

There is no need for alternative validation activities for OMA DRM 2.1.

7. Approval Criteria

Normal Approval Criteria

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
n/a	n/a	No prior version –or- No previous version within OMA

A.2 Draft/Candidate Version 2.1 History

Document Identifier	Date	Sections	Description
Draft Versions OMA-EVP-DRM-V2_1	21 Jun 2007	All	Created based on: OMA-IOP-BRO-2007-0015R02-INP_DRM_2.1_ETG
	12 Jul 2007	2, 3	Editorial corrections of text styles and sorting of ref, def and abbr lists.
Candidate Versions OMA-EVP-DRM-V2_1	07 Aug 2007	All	Status changed to Candidate by TP TP ref # OMA-TP-2007-0299- INP_EVP_BCAST_V1_0_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-v2.1], 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-v2.1]:

  "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-v2.1] :

  - "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-2.1 specification [DRMERELD-v2.1].

The objects to be tested are:

- OMA DRM Client as defined in [DRMERELD-v2.1]
- OMA DRM Rights Issuer as defined in [DRMERELD-v2.1]

The test tool allows conducting the conformance tests that have been specified in the conformance test section of [DRMETS-CON-C-v2.1] and [DRMETS-CON-S-v2.1].

B.2 OMA DRM Test Tool; Overview

The OMA DRM Test Tool can be used for conformance testing of both the DRM Client and the Rights Issuer. In practical implementations, it can be one tool featuring conformance tests of both the DRM Client and the Rights Issuer or two tools; one Test Tool for the DRM Client and another Test Tool for the Rights Issuer.

For sake of readability, the DRM Client Test Tool and the RI Test Tool have been described separately in the sections below.

B.2.1 OMA DRM Client Test Tool; Overview

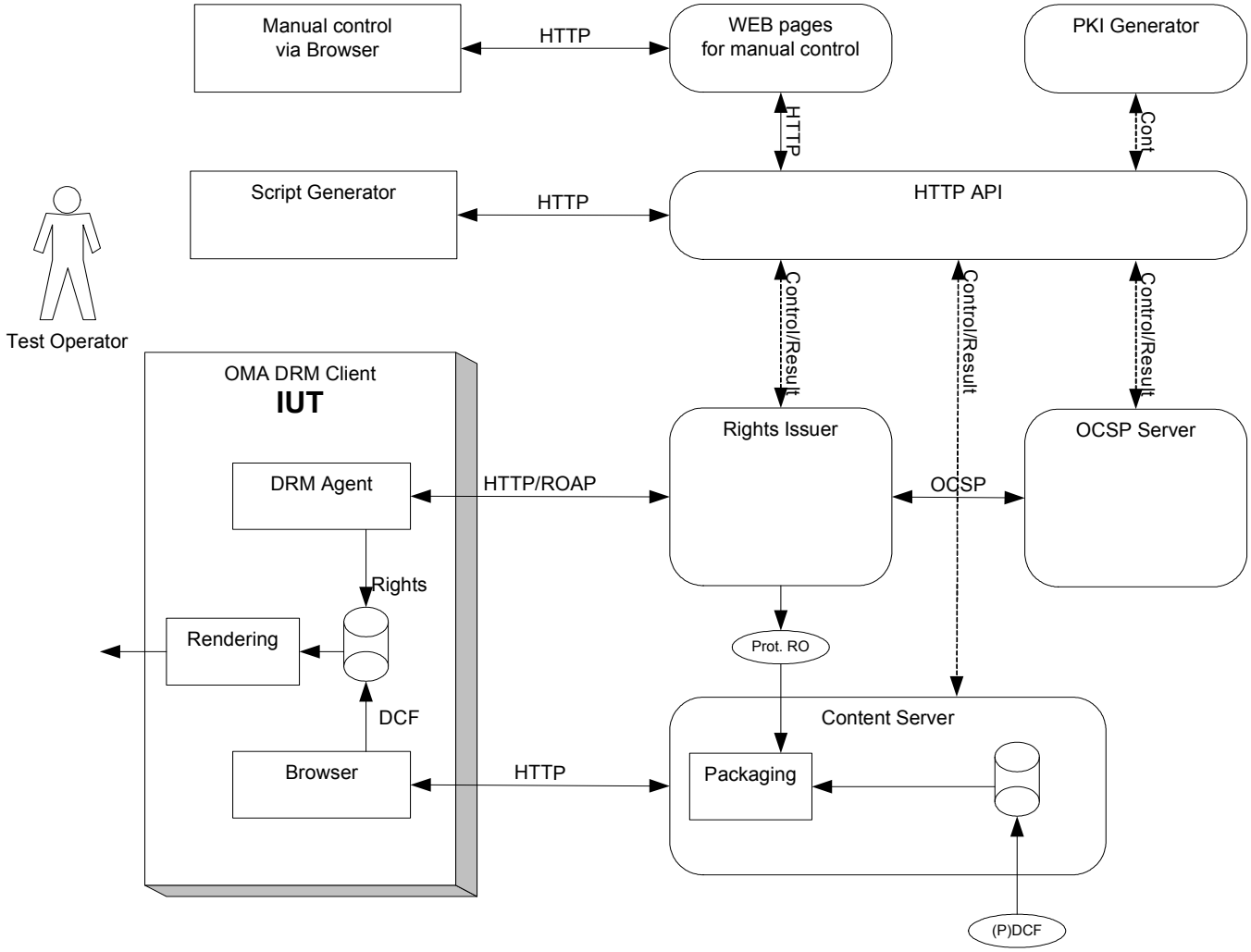

Figure 7 **Overview of the Test Tool for DRM Client Conformance tests**

An overview of the Test Tool for an OMA DRM Client is depicted in

Figure 7. The round-cornered boxes are part of the Test Tool. Detailed requirement for the Test Tool are defined in section B.3.

In this case the IUT is a DRM Client that is expected to hold at least three components:

- A DRM Agent as defined in [DRMERELD-v2.1], handling the ROAP protocol with Rights Issuer.
- A Browser capable of downloading (P)DCF files from a content server
- A rendering system that allows for rendering the (P)DCF files.

The DRM client can be either a Connected Device or an Unconnected Device (as defined in [DRMDRM-2.0]) connected to the Test Tool via a Connected Device.

In general, the DRM Client will not be able to render any type of (P)DCF. For that reason, the Test Tool allows the operator to choose a specific type from a limited set (e.g. MP3 audio, AAC audio, JPEG). This set is yet to be defined and can be expanded in the future.

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.

The Test Tool will:

- interpret test scripts that define the test purpose, test steps and pass/fail criteria
- construct and send all ROAP messages (including OCSP responses) to the client under test.
- Receive ROAP messages from the client under test
- Construct and send (P)DCF files, possibly including Rights objects to the DRM client
- Inject errors into transmitted protocol or content as defined by test scripts and analyze the responses
- Provide a means for the test operator to be prompted when manual action is required by a test
- Provide means for the test operator to enter observations/result information into the Test Tool when prompted
- Log all transactions and results
- Present results and logs to the operator
- Provide the operator with management tools for test tool configuration and parameterisation, test selection etc
- Generate PKI data structures. See section B.2.3.

Note that the Test Tool can be remote from the IUT and from the test operator.

B.2.2 Rights Issuer Test Tool; Overview

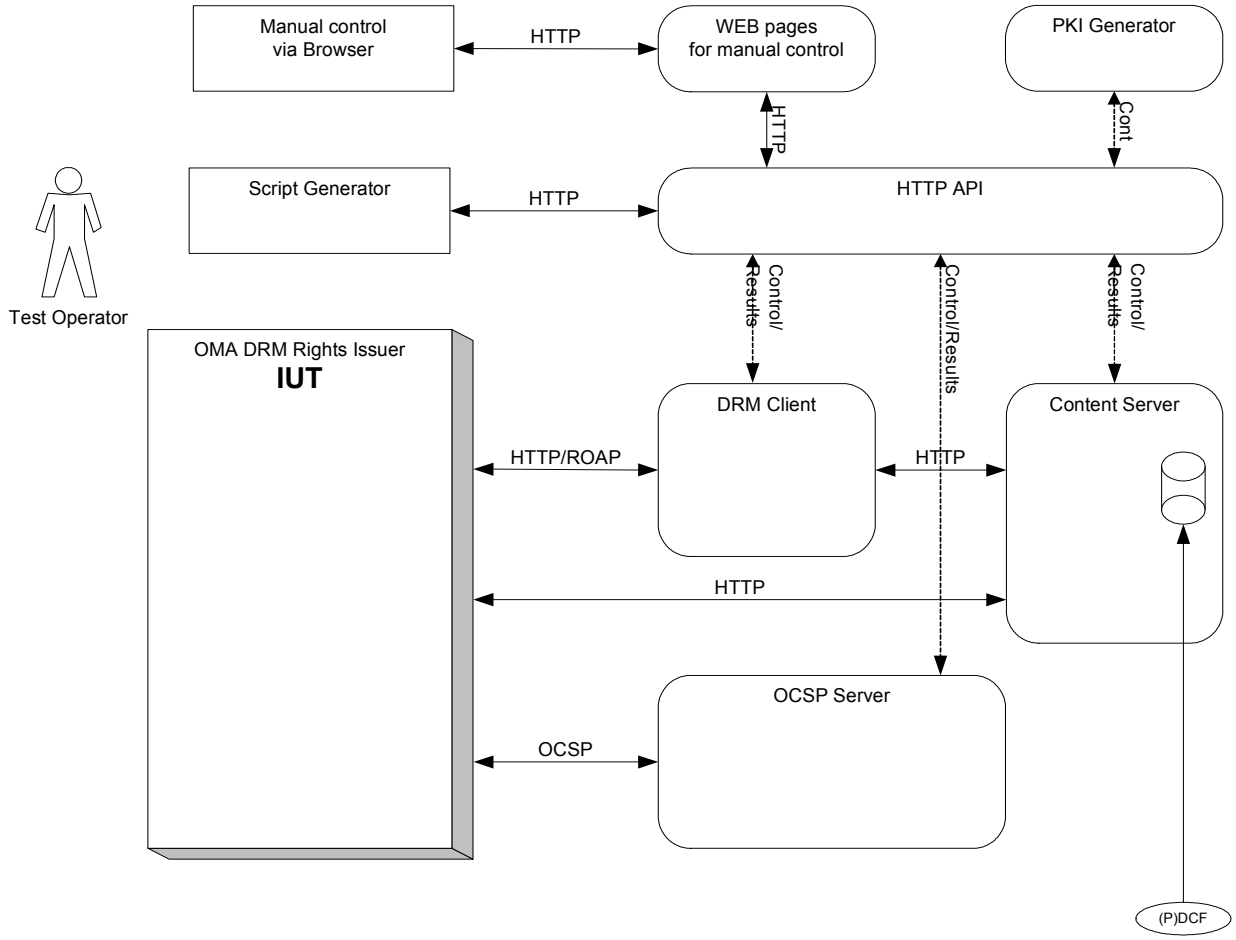

Figure 8 **Overview of the Test Tool for RI Conformance tests**

An overview of the Test Tool for an OMA DRM Rights Issuer is depicted in

Figure 8. The round-cornered boxes are part of the Test Tool. Detailed requirement for the Tool are defined in section B.3. In this case the IUT is a DRM Rights Issuer.

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.

The Test Tool will:

- interpret test scripts that define the test purpose, test steps and pass/fail criteria
- construct and send all ROAP messages to the RI Server (IUT).
- Receive ROAP messages from the RI Server (IUT)
- Send and receive OCSP messages to/from the RI server (IUT).
- Inject errors into transmitted protocol or content as defined by test scripts and analyze the responses
- Provide a means for the test operator to be prompted when manual action is required by a test

- Provide means for the test operator to enter observations/result information into the Test Tool when prompted
- Log all transactions and results
- Present results and logs to the operator
- Provide the operator with management tools for test tool configuration and parameterisation, test selection etc
- Generate PKI data structures. See section B.2.3.

B.2.3 PKI generator; Overview

In order to successfully conduct conformance tests, the DRM Agent, the Rights issuer and the OCSP responder need to agree upon some system parameters, generally referred to as Public Key Infrastructure (PKI). Normally this PKI is defined by the Trust Anchor. The default PKI used for testing is defined in section 5.2.2. A PKI is characterized by:

- A certificate chains and key pairs for the DRM Client, Rights Issuer and OCSP responder
- Trust Authority's Public key for DRM Client, Rights Issuer and OCSP responder
- List of trusted RI Authorities for the DRM Client
- List of trusted Device Authorities for the Rights Issuer
- Device CRL for the Rights Issuer
- Possibly one or more Device CA CRL's for the Rights Issuer
- RI CRL for the OCSP responder
- Possibly one or more RI CA CRL's for the OCSP responder

The test Tool features a PKI generator that allows for generation of these data structures. The PKI data structures for the IUT are provided to the Test operator. Other PKI data structures are automatically downloaded in several components of the Test.

B.3 Requirements for Test Tool

B.3.1 Compliance

Wherever applicable the Test Tool and the data structures produced by it SHALL comply to [DRM-v2.1], [DRMCF-v2.1] and [DRMREL-v2.1].

The Test Tool is capable of performing all tests as defined in the conformance test section of [DRMETS-CON-C-v2.1] and [DRMETS-CON-S-v2.1].

B.3.2 PKI generator

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

B.3.3 Transport

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

B.3.4 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.3.5 Packaging

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

B.3.6 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.3.7 Operating Environment

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

B.3.8 Multi Session Capability

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