Enabler Validation Plan for Secure Removable Media

Candidate Version 1.0 – 06 Nov 2008

Open Mobile Alliance

OMA-EVP-SRM-V1_0-20081106-C

© 2008 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.

Use of this document is subject to all of the terms and conditions of the Use Agreement located at http://www.openmobilealliance.org/UseAgreement.html.

Unless this document is clearly designated as an approved specification, this document is a work in process, is not an approved Open Mobile Alliance™ specification, and is subject to revision or removal without notice.

You may use this document or any part of the document for internal or educational purposes only, provided you do not modify, edit or take out of context the information in this document in any manner. Information contained in this document may be used, at your sole risk, for any purposes. You may not use this document in any other manner without the prior written permission of the Open Mobile Alliance. The Open Mobile Alliance authorizes you to copy this document, provided that you retain all copyright and other proprietary notices contained in the original materials on any copies of the materials and that you comply strictly with these terms. This copyright permission does not constitute an endorsement of the products or services. The Open Mobile Alliance assumes no responsibility for errors or omissions in this document.

Each Open Mobile Alliance member has agreed to use reasonable endeavors to inform the Open Mobile Alliance in a timely manner of Essential IPR as it becomes aware that the Essential IPR is related to the prepared or published specification. However, the members do not have an obligation to conduct IPR searches. The declared Essential IPR is publicly available to members and non-members of the Open Mobile Alliance and may be found on the "OMA IPR Declarations" list at http://www.openmobilealliance.org/ipr.html. The Open Mobile Alliance has not conducted an independent IPR review of this document and the information contained herein, and makes no representations or warranties regarding third party IPR, including without limitation patents, copyrights or trade secret rights. This document may contain inventions for which you must obtain licenses from third parties before making, using or selling the inventions. Defined terms above are set forth in the schedule to the Open Mobile Alliance Application Form.

NO REPRESENTATIONS OR WARRANTIES (WHETHER EXPRESS OR IMPLIED) ARE MADE BY THE OPEN MOBILE ALLIANCE OR ANY OPEN MOBILE ALLIANCE MEMBER OR ITS AFFILIATES REGARDING ANY OF THE IPR'S REPRESENTED ON THE "OMA IPR DECLARATIONS" LIST, INCLUDING, BUT NOT LIMITED TO THE ACCURACY, COMPLETENESS, VALIDITY OR RELEVANCE OF THE INFORMATION OR WHETHER OR NOT SUCH RIGHTS ARE ESSENTIAL OR NON-ESSENTIAL.

THE OPEN MOBILE ALLIANCE IS NOT LIABLE FOR AND HEREBY DISCLAIMS ANY DIRECT, INDIRECT, PUNITIVE, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE USE OF DOCUMENTS AND THE INFORMATION CONTAINED IN THE DOCUMENTS.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms set forth above.

Contents

1. SCOPE 5
1.1 ASSUMPTIONS 5
1.2 EXCLUSIONS 5
2. REFERENCES 6
2.1 NORMATIVE REFERENCES 6
2.2 INFORMATIVE REFERENCES 6
3. TERMINOLOGY AND CONVENTIONS 7
3.1 CONVENTIONS 7
3.2 DEFINITIONS 7
3.3 ABBREVIATIONS 7
4. ENABLER VALIDATION DESCRIPTION 9
5. TESTFEST ACTIVITIES 10
5.1 ENABLER TEST GUIDELINES 10
5.1.1 Minimal Test Configuration 11
5.1.2 Minimal Participation Guidelines 11
5.1.3 Optimal TestFest Achievement Guidelines 11
5.2 ENABLER TEST REQUIREMENTS 12
5.2.1 Test Infrastructure Requirements 12
5.2.2 Public Key Infrastructure 13
5.2.3 Enabler Execution Flow 15
5.2.4 Test Content Requirements 20
5.2.5 Test Limitations 20
5.2.6 Test Restrictions 21
5.2.7 Test Tools 21
5.2.8 Resources Required 21
5.3 TESTS TO BE PERFORMED 22
5.3.1 Entry Criteria for TestFest 22
5.3.2 Mandatory Interoperability Test Cases 22
5.4 ENABLER TEST REPORTING 23
5.4.1 Problem Reporting Requirements 23
5.4.2 Enabler Test Requirements 23
6. ALTERNATIVE VALIDATION ACTIVITIES 24
6.1 BILATERAL TESTING 24
7. APPROVAL CRITERIA 25
7.1 ENABLER VALIDATION TEST CASES 25
7.2 NON-COVERED ETR REQUIREMENTS 26
APPENDIX A. CHANGE HISTORY (INFORMATIVE) 28
A.1 APPROVED VERSION HISTORY 28
A.2 DRAFT/CANDIDATE VERSION 1.0 HISTORY 28

Figures

Figure 1 - SRM 1.0 Architecture 10
Figure 2 - SRM Testing Infrastructure 13
Figure 3: PKI for IOP tests 14
Figure 4 – SRM Hello 15

© 2008 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-EnablerValidationPlan-20070308-I]

Figure 5 – MAKE process **16**

Figure 6 - Rights Movement from a Device to an SRM **17**

Figure 7 - Rights Movement from an SRM to a Device **18**

Figure 8 - Local Rights Consumption **19**

Figure 9 – SRM Utilities: Handle List Query **20**

Tables

Table 1: Mandatory IOP Test Cases **22**

Table 2: Enabler Validation Test Cases **26**

Table 3: Non-Covered ETR Requirements **27**

© 2008 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-EnablerValidationPlan-20070308-I]

1. Scope

This document details the Validation plan for the SRM 1.0 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 SRM 1.0 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 SRM 1.0, as stated in [ERELD] is according to the following:

- SRM Requirements V1.0 [SRM-RD]
- SRM Architecture V1.0 [SRM-AD]
- SRM Specification V1.0 [SRM-TS]
- DRM Specification V2.0 [OMADRMv2]
- DRM Specification V2.1 [OMADRMv2.1]

1.1 Assumptions

None

1.2 Exclusions

None

© 2008 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.

2. References

2.1 Normative References

[SRM-ERELD] "Enabler Release Definition for Secure Removable Media", Version 1.0, Open Mobile Alliance™, OMA- ERELD-SRM-V1_0. URL:http://www.openmobilealliance.org/

[SRM-ETR] "OMA Enabler Test Requirements for Secure Removable Media", Version1.0, Open Mobile Alliance™, OMA-ETR-SRM -V1_0. URL:http://www.openmobilealliance.org/

[SRM-AD] "OMA Secure Removable Media Architecture", Version 1.0, Open Mobile Alliance™, OMA-AD-SRM-V1_0, URL:http://www.openmobilealliance.org/

[SRM-TS] "OMA Secure Removable Media Specification", Version 1.0, Open Mobile Alliance™, OMA-TS-SRM-V1_0, URL:http://www.openmobilealliance.org/

[OMADRMv2] "Digital Rights Management", Version 2.0, Open Mobile Alliance™, OMA-DRM-DRM-V2_0, URL:http://www.openmobilealliance.org/

[OMADRMv2.1] "Digital Rights Management", Version 2.1, Open Mobile Alliance™, OMA-DRM-DRM-V2_1, URL:http://www.openmobilealliance.org/

[IOPPROC] "OMA Interoperability Policy and Process", Version 1.6, Open Mobile Alliance™, OMA-ORG-IOP_Process-V1_6, 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

[SRMETS-v1.0] "OMA SRM Enabler Test Specification" Version 1.0, Open Mobile Alliance™, OMA-ETS-SRM- V1_0, URL:http://www.openmobilealliance.org/

© 2008 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.

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 Issuer	The entity making content available to the DRM Agent in a Device.
Device	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. The Device may include a smartcard module (e.g. a SIM) or not depending upon implementation
DRM Agent	Entity in the Device that manages permissions for media objects
DRM Content	Media objects that are consumed according to a set of permissions in Rights
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.
Rights	Collection of permissions and constraints defining under which circumstances access is granted to DRM Content. Rights may include the associated state information
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.
Secure Removable Media	A removable media that implements means to protect against unauthorized access to its internal data and includes an SRM Agent (e.g. secure memory card, smart card)
SRM Agent	A trusted entity embodied in Secure Removable Media. This entity is responsible for storing and removing Rights in Secure Removable Media, for delivering Rights from/to a DRM Agent in a secure manner, and for enforcing permissions and constraints, including securely maintaining state information for stateful rights. The SRM Agent is a part of Secure Removable Media

3.3 Abbreviations

AD	Architecture Document
CRL	Certificate Revocation List
DRM	Digital Rights Management
ERDEF	Enabler Requirement Definition
ERELD	Enabler Release Definition
ETSI	European Telecommunications Standards Institute
MAC	Message Authentication Code
MMCA	MultiMediaCard Association
OMA	Open Mobile Alliance
RD	Requirements Document
RI	Rights Issuer
RO	Rights Object

© 2008 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-EnablerValidationPlan-20070308-I]

SD	Secure Digital
SDA	SD Card Association
SIM	Subscriber Identity Module
S-MMC	Secure MultiMediaCard
SRM	Secure Removable Media
USIM	Universal Subscriber Identity Module

© 2008 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.

4. Enabler Validation Description

It is intended that TestFests will be the primary validation method for OMA SRM 1.0. Please refer to section 5 for further information.

© 2008 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-EnablerValidationPlan-20070308-I]

5. TestFest Activities

5.1 Enabler Test Guidelines

A full description of SRM 1.0 can be found in [SRM-ERELD] and related specifications.

The OMA SRM is to enable the use of Secure Removable Media by allowing users the ability, for example, to transfer Rights to and from a trusted SRM, and to consume Rights from the SRM. This enabler extends the OMA DRM version 2.0 to provide mechanisms for the secure transfer of Rights between a DRM Agent and an SRM Agent including their mutual authentication.

A conceptual picture of a DRM system, according to [SRM-AD], is depicted in the following figure:

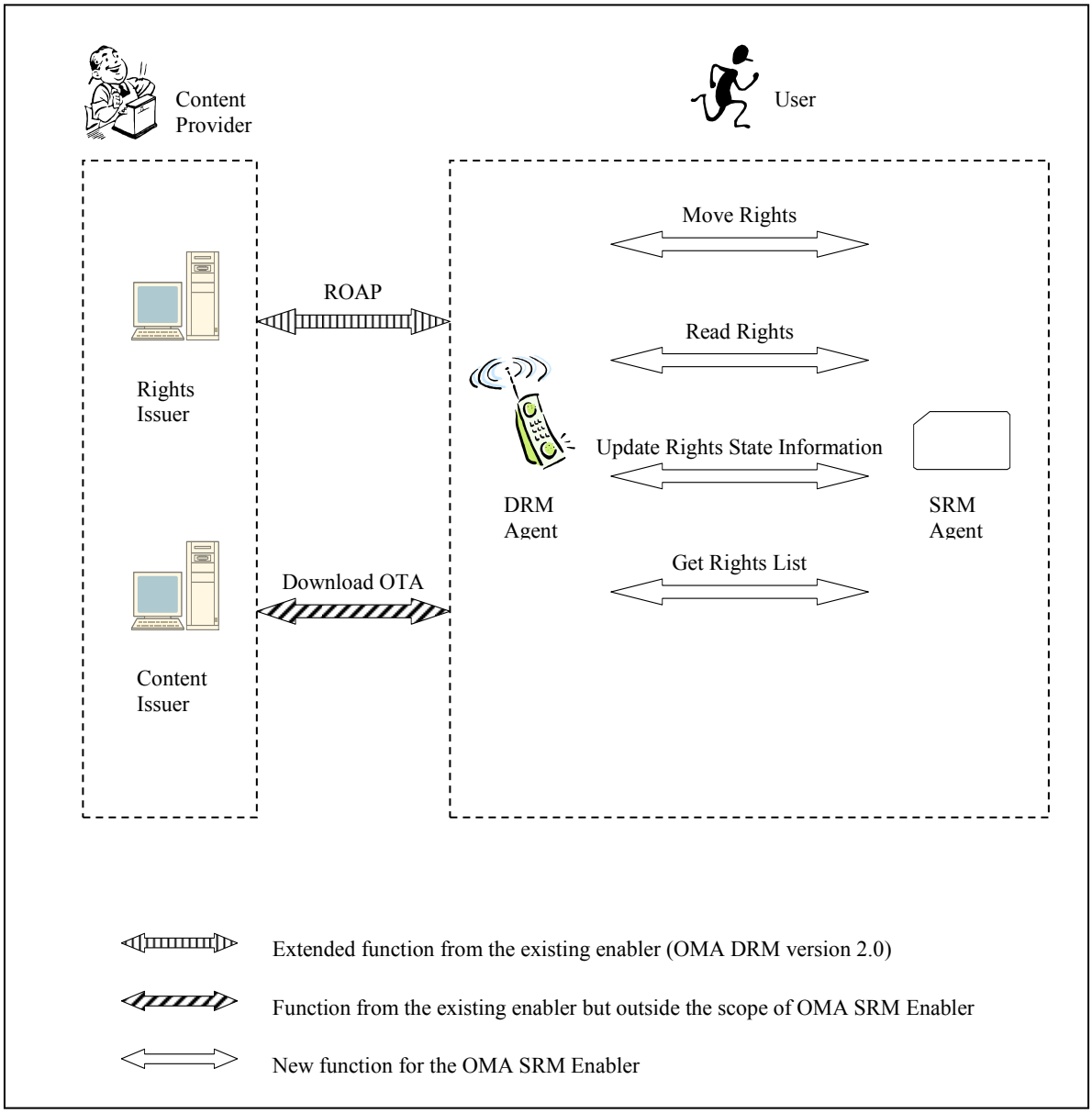

Figure 1 - SRM 1.0 Architecture

© 2008 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.

5.1.1 Minimal Test Configuration

The minimal (hardware and software) configuration for testing SRM 1.0 is:

- **Public Key Infrastructure** – at least one Certificate Authority, which is for CRL download and optionally with an associated OCSP Responder.
- **Client implementation** – at least one device (mobile phone, PC, or other) that implements a DRM Agent. The device must be able to transfer Rights Objects from the device to an SRM via the SRM protocol. Client implementations must be able to consume/render DRM Content to allow evaluation of the test case pass criteria.
- **Server implementation** – at least one SRM that implements an SRM Agent. The SRM must be able to transfer Rights Objects from the SRM to a device via the SRM protocol.
- **Rights Issuer and Content Issuer Server** –at least one server that implements a Rights Issuer server. It is expected that the server is capable of acting as both Content Issuer and Rights Issuer.
- **PKI Provisioning** – both DRM Agents and SRM Agents must be provisioned with certificates and keys issued by the Trust Anchor.

5.1.2 Minimal Participation Guidelines

Minimum Client Participants: 2

Minimum Server Participants: 2

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.

In case there is a need to prioritize testing during the TestFest, due time constraints or otherwise, the following prioritization should be used

The list includes:

Test Case ID	Test Case Title	Priority
SRM-1.0-int-001	SRM Hello	High
SRM-1.0-int-002	Mutual Authentication and Key Exchange: MAKE	High
SRM-1.0-int-003	Key Derivation Function	High
SRM-1.0-int-004	MAC key update	High
SRM-1.0-int-006	CRL Number Exchange	High
SRM-1.0-int-007	CRL Delivery from Device to SRM	High
SRM-1.0-int-008	CRL Delivery from SRM to Device	High
SRM-1.0-int-011	Rights Move from Device to SRM	High
SRM-1.0-int-012	Rights Move from SRM to Device	High
SRM-1.0-int-013	Move Permission	High
SRM-1.0-int-014	REK Query	High
SRM-1.0-int-015	State Information Update	High
SRM-1.0-int-016	Handle List Query	High
SRM-1.0-int-017	Rights Information Query	High
SRM-1.0-int-019	Handle Removal	High
SRM-1.0-int-020	Rights Enablement	High
SRM-1.0-int-021	Rights Removal	High

© 2008 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-EnablerValidationPlan-20070308-I]

Test Case ID	Test Case Title	Priority
SRM-1.0-int-024	Store RI Certificate Chain	High

Priority levels are defined as follows:

- **High** – Passed less than 5 times or Failures in two or more TestFests
- **Medium** – Passed between 6 to 20 times
- **Low** – Passed more than 20 times

5.2 Enabler Test Requirements

Testing requirements for SRM are specified in [SRM-ETR].

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. The requirements on the testing environment are itemized as follows:

- **Local Area Network (LAN)** – providing connection between PC DRM Agent (client) implementations as well as providing an interface between other infrastructure components.
- **Public Internet Access** – enabling connection to: remotely hosted RI Servers, CRL download servers, and OCSP responders,
- **PLMN** (mobile telephony network) with an air interface over GSM, UMTS or CDMA for mobile phone based DRM Agent (client) implementations.
- **Trust Anchor** (Certificate Authority) providing CRLs and (optionally) an OCSP Responder. Prior to testing, DRM Agents and SRM Agents must be provisioned with a certificate chain issued by the CA.
- **SIM cards** for all GSM/UMTS mobile phone based DRM Agent (client) implementations.
- **Rights Issuer and Content Issuer 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.

© 2008 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-EnablerValidationPlan-20070308-I]

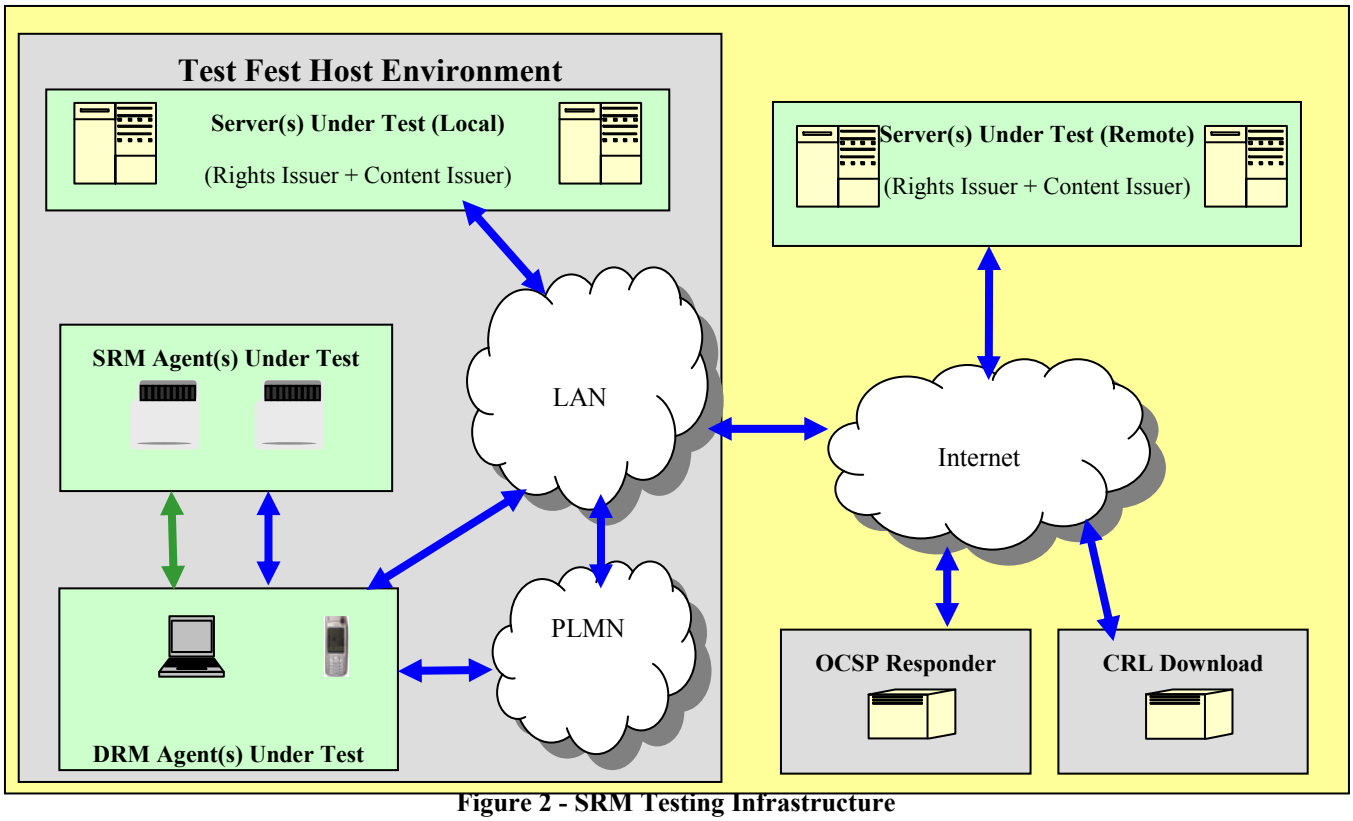

Figure 2 - SRM Testing Infrastructure

5.2.2 Public Key Infrastructure

In order to successfully conduct interoperability tests, SRM Agent, DRM Agent, and Rights Issuer / Content Issuer Server 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 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.

© 2008 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.

5.2.2.1 PKI Model A

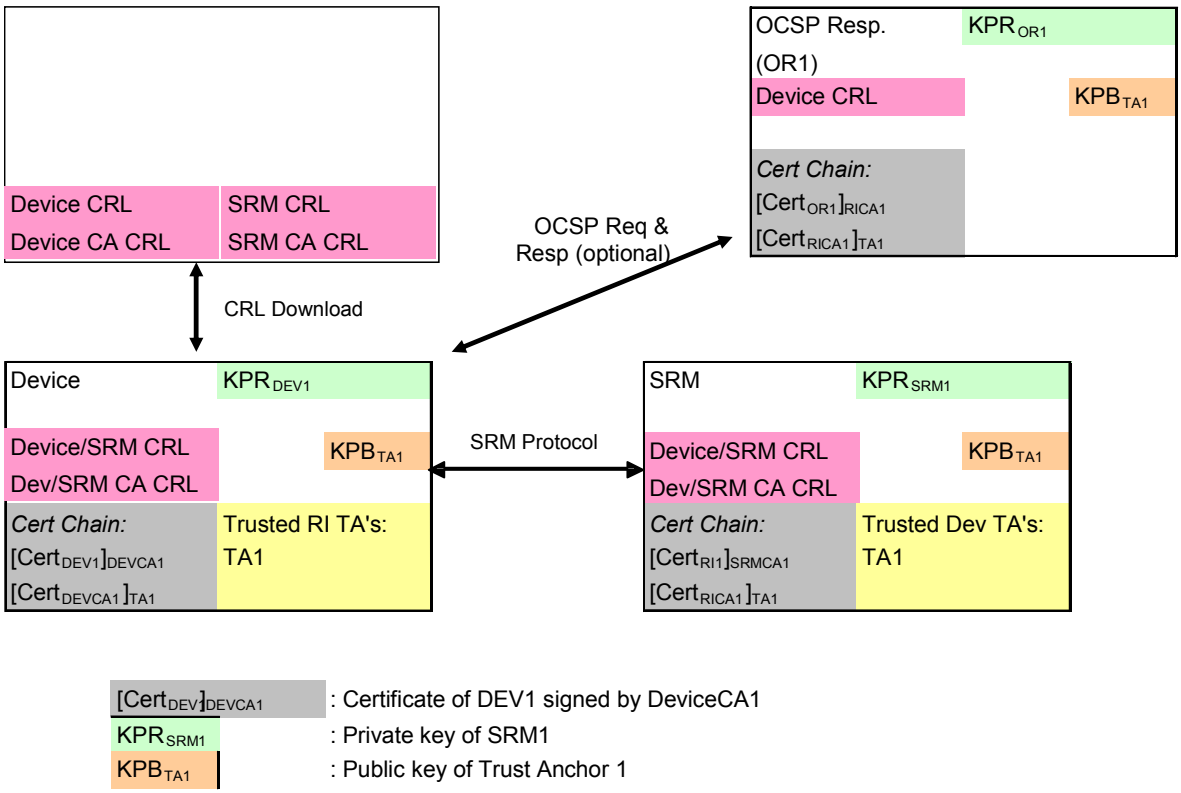

Figure 3: PKI for IOP tests

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 Trust Anchor And Device ID Pair List
  - the SRM holds one Certificate chain , one private key and the certificate of one Trust Anchor and it has one entry in the Trust Anchor And SRM ID Pair List
- The Certificate chain of the Device contains the Device certificate and the certificate of one intermediate Device CA
- The Certificate chain of the SRM contains the SRM certificate and the certificate of one intermediate SRM CA
- The Certificate chain of the OCSP responder contains the Responder certificate and the certificate of the intermediate Device CA
- The Device 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 SRM holds a Device CRL that it uses to determine revocation status of devices
- The SRM holds a Device CA CRL that it uses to determine the revocation status of Device CAs
- The Device holds an SRM CRL that it uses to determine revocation status of SRMs

© 2008 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.

- The Device holds an SRM CA CRL that it uses to determine the revocation status of SRM CAs
- The OCSP responder holds a Device CRL that it uses to determine the revocation status of Devices

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

5.2.3 Enabler Execution Flow

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

- Client/server protocols (SRM protocol)
- Correct processing of file formats (e.g. format of rights information)

The following sub-sections detail the principle execution flows covered by the interoperability tests of OMA SRM 1.0. These flows demonstrate the interactions between a client and a server.

5.2.3.1 SRM Hello and MAKE

The communication between a Device and an SRM starts with the MAKE (Mutual Authentication and Key Exchange) process following the SRM Hello. The DRM Agent sends the SRM Hello message to the SRM Agent to exchange information about each other. After a successful receipt of SRM Hello, the DRM Agent and the SRM Agent mutually authenticate by exchanging Authentication and Key Exchange messages.

Figure 4 – SRM Hello

© 2008 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.

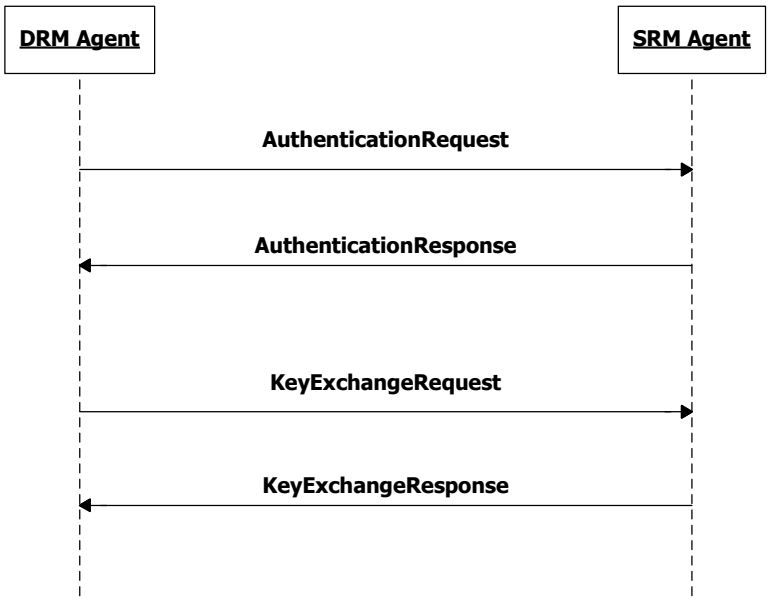

Figure 5 – MAKE process

5.2.3.2 Rights Movement between a Device and an SRM

A Rights Object is moved from a Device to an SRM, and vice versa via the SRM protocol.

© 2008 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.

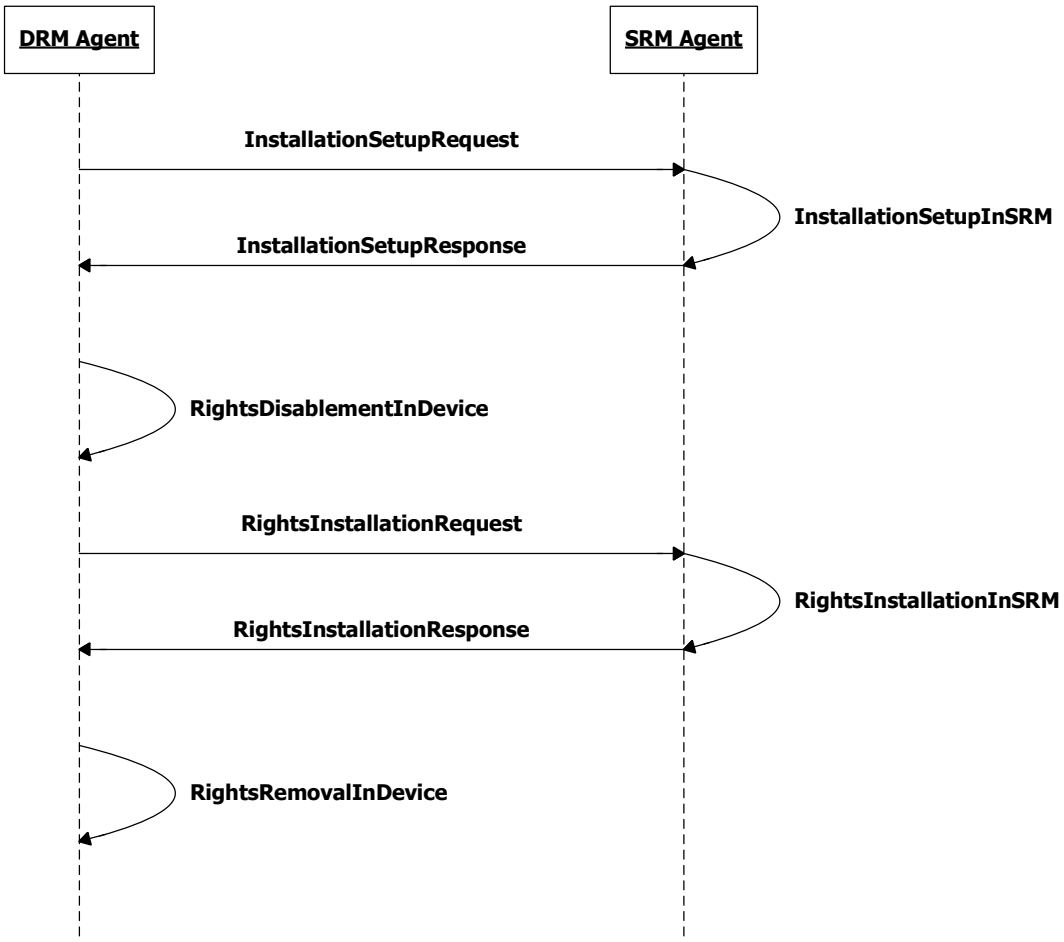

Figure 6 - Rights Movement from a Device to an SRM

© 2008 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.

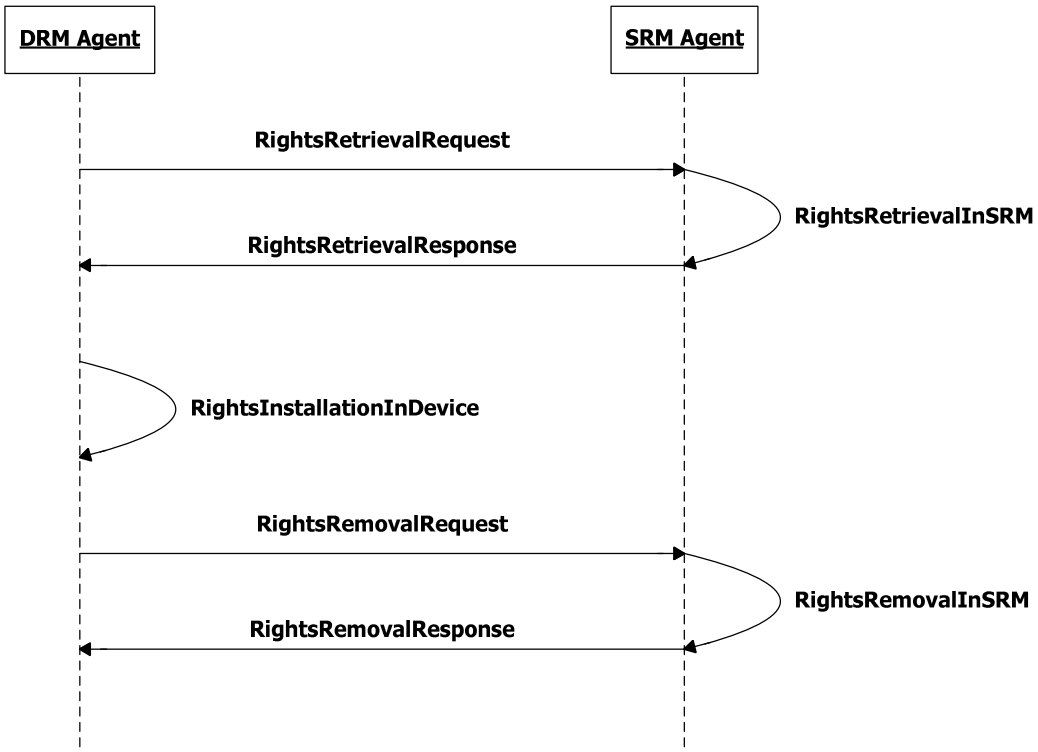

Figure 7 - Rights Movement from an SRM to a Device

5.2.3.3 Local Rights Consumption

A Rights stored in the SRM can be consumed when its associated DRM content is used. At this time the DRM Agent may collect Rights Information associated with the content, from the SRM.

© 2008 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.

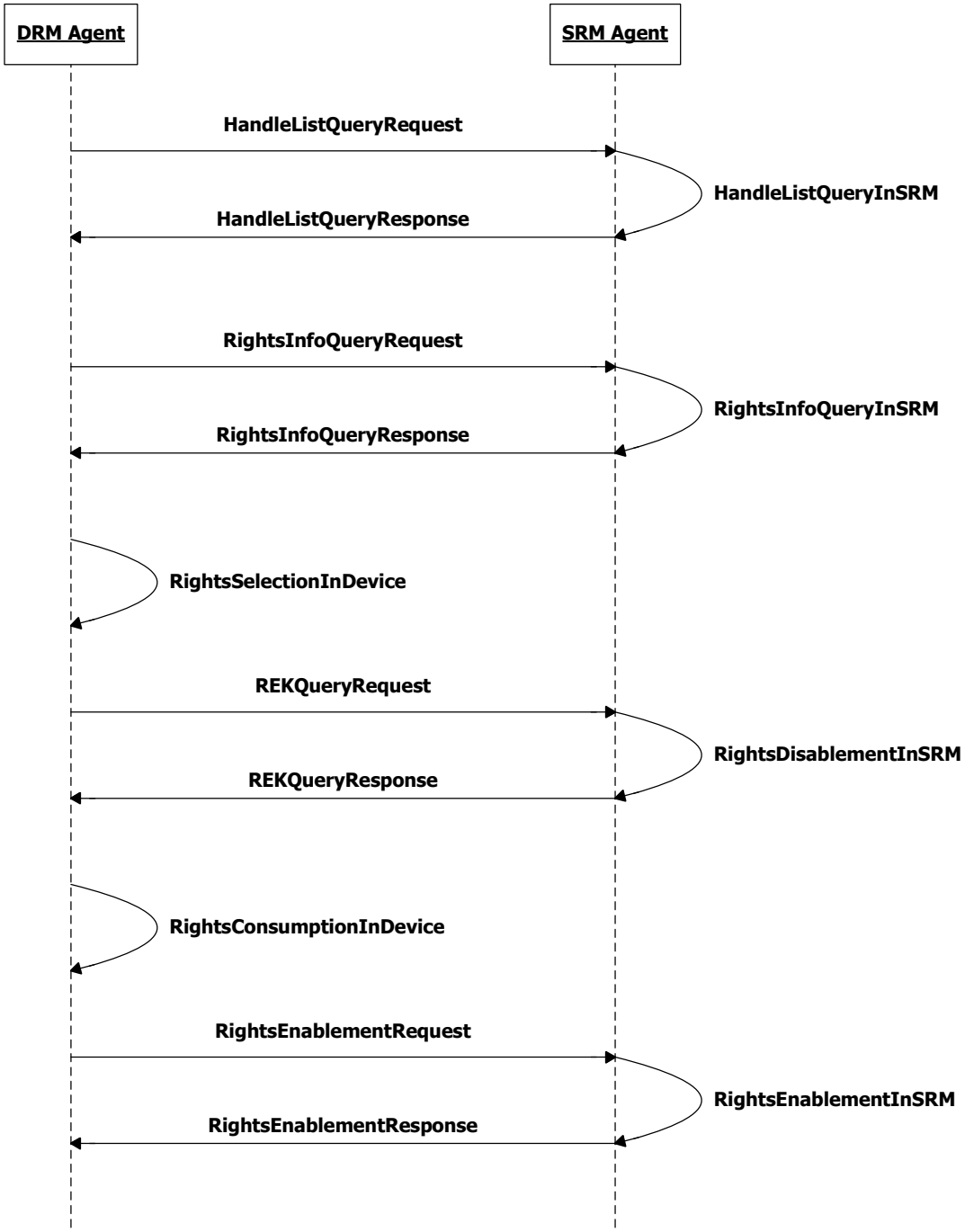

Figure 8 - Local Rights Consumption

5.2.3.4 SRM Utilities

There are a number of protocols that are necessary for the Rights Movement and Local Rights Consumption.

© 2008 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-EnablerValidationPlan-20070308-I]

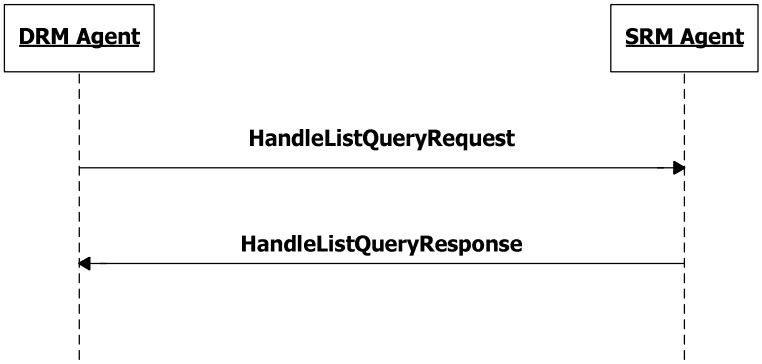

Figure 9 – SRM Utilities: Handle List Query

5.2.4 Test Content Requirements

Content Issuers are expected to support DCF packaging of arbitrary media formats and should allow DRM Agents (Client) 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 to be consistent with DRM 2.0:

- 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).

Rights Issuers are expected to include the Move permission in Rights Objects which should be moved to SRMs, as described in Appendix G of [SRM-TS].

5.2.5 Test Limitations

5.2.5.1 Physical

None

5.2.5.2 Resources

SRM Enabler specifies the Application layer. Other layers are defined by external organisations (e.g., ETSI, MMCA, and SDA) related to each type of SRM (SIM, S-MMC, SD). Each type of SRM typically has a different physical interface that must be supported by the Device. Communication interface options are:

© 2008 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-EnablerValidationPlan-20070308-I]

- HTTP: mapping defined in Appendix D of [SRM-TS]
- SRM API (Application Programming Interface): defined in Appendix E of [SRM-TS]
- Others: mutually agreed for bilateral testing

Each participating SRM Agent must identify its interface requirements when registering for the test fest, and provide any necessary modules to the participating DRM Agents. Also, it is recommended that DRM Agents support either HTTP or the SRM API. Other interfaces can be used in bilateral testing.

5.2.6 Test Restrictions

The SRM IOP testing can be done at the following locations:

- OMA TestFest (http://www.openmobilealliance.org/tf/index.asp)
- Bilateral testing by contracted companies: results should be reported back to OMA IOP

5.2.7 Test Tools

.

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 SRM 1.0 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 one engineer to run tests while another is investigating the cause of any problems.

© 2008 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-EnablerValidationPlan-20070308-I]

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 [SRM-ERELD].

5.3.2 Mandatory Interoperability Test Cases

The following test cases from [SRMETS-v1.0] must be supported by implementations participating in a test fest. There are three unique implementation types that may participate in a test fest: SRM Agent (SA), DRM Agent (DA), and Rights Issuers (RI). The following tables identifies whether a test case is Mandatory (M), Optional (O) or Not Applicable (NA) to each implementation type. If a test case is marked Mandatory then that implementation must not mark that test case as "Not Supported" on the test fest Test Session Report.

Functional Group	Test Case	Section	Title	SA	DA	RI
SRM Hello and MAKE	SRM-1.0-int-001	6.1.1	SRM Hello	M	M	NA
	SRM-1.0-int-002	6.1.2	Mutual Authentication and Key Exchange: MAKE	M	M	NA
	SRM-1.0-int-003	6.1.3	Key Derivation Function	M	M	NA
	SRM-1.0-int-004	6.1.4	MAC key update	M	M	NA
	SRM-1.0-int-005	6.1.5	Change SAC	O	O	NA
CRL and OCSP	SRM-1.0-int-006	6.2.1	CRL Number Exchange	M	M	NA
	SRM-1.0-int-007	6.2.2	CRL Delivery from Device to SRM	M	M	NA
	SRM-1.0-int-008	6.2.3	CRL Delivery from SRM to Device	M	M	NA
	SRM-1.0-int-009	6.2.4	OCSP Nonce generation	O	O	NA
	SRM-1.0-int-010	6.2.5	OCSP Response processing and validation	O	O	NA
Rights Movement between a Device and an SRM	SRM-1.0-int-011	6.3.1	Rights Move from Device to SRM	M	M	NA
	SRM-1.0-int-012	6.3.2	Rights Move from SRM to Device	M	M	NA
	SRM-1.0-int-013	6.3.3	Move Permission	NA	M	M
Local Rights Consumption	SRM-1.0-int-014	6.4.1	REK Query	M	M	NA
	SRM-1.0-int-015	6.4.2	State Information Update	M	M	NA
SRM Utilities	SRM-1.0-int-016	6.5.1	Handle List Query	M	M	NA
	SRM-1.0-int-017	6.5.2	Rights Information Query	M	M	NA
	SRM-1.0-int-018	6.5.3	Rights Information List Query	O	O	NA
	SRM-1.0-int-019	6.5.4	Handle Removal	M	M	NA
	SRM-1.0-int-020	6.5.5	Rights Enablement	M	M	NA
	SRM-1.0-int-021	6.5.6	Rights Removal	M	M	NA
	SRM-1.0-int-022	6.5.7	WBXML Dynamic Code Page Query	O	M	NA
	SRM-1.0-int-023	6.5.8	WBXML Dynamic Code Page Update	O	O	NA
	SRM-1.0-int-024	6.5.9	Store RI Certificate Chain	O	O	NA
	SRM-1.0-int-025	6.5.10	Get RI Certificate Chain	O	O	NA
	SRM-1.0-int-026	6.5.11	Remove RI Certificate Chain	O	O	NA

Table 1: Mandatory IOP Test Cases

© 2008 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-EnablerValidationPlan-20070308-I]

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.

© 2008 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-EnablerValidationPlan-20070308-I]

6. Alternative Validation Activities

6.1 Bilateral Testing

Bi-lateral testing organized by any mutually agreed companies can be an alternative to validate the SRM 1.0 enabler. During bilateral testing, all the test requirements must be compliant with 5.2 in this document. Also, all of the test cases described in 5.1.3 and 5.3.2 must be supported. All the reports required for TestFests must be submitted to the OMA Trusted Zone.

© 2008 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-EnablerValidationPlan-20070308-I]

7. Approval Criteria

The SRM 1.0 Enabler can be put in the Approved state when:

- The Enabler has been tested successfully at 2 Test Fests or
- There has been at least 2 successful bi-lateral test sessions that have reported results and any issues to OMA.
- No open PRs exist.

7.1 Enabler Validation Test Cases

The following table lists the set of tests that are used for validation of the SRM enabler.

Test Case Id	ETR Requirement Id	ETR Status	Notes
SRM-1.0-int-001	HEL01	M	
	HEL02	M	
SRM-1.0-int-002	SAC01	M	
	SAC04	M	
	CRT01	M	
	CRT02	M	
	CRT03	M	
	CRT04	M	
	CRT05	M	
	CRT06	M	
	CRT07	M	
	CRL04	M	
	CRL08	M	
SRM-1.0-int-003	SAC02	M	
	SAC05	M	
SRM-1.0-int-004	SAC03	M	
	SAC06	M	
SRM-1.0-int-005	SAC07	O	
	SAC08	O	
SRM-1.0-int-006	CRL01	M	
	CRL05	M	
SRM-1.0-int-007	CRL02	M	
	CRL06	M	
SRM-1.0-int-008	CRL03	M	
	CRL07	M	
SRM-1.0-int-009	OCSP01	O	
SRM-1.0-int-010	OCSP02	O	
	OCSP03	O	
	OCSP04	O	
	OCSP06	O	

© 2008 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.

Test Case Id	ETR Requirement Id	ETR Status	Notes
SRM-1.0-int-011	MOV01	M	
	MOV04	M	
	MOV05	M	
	CAC01	M	
SRM-1.0-int-012	MOV02	M	
SRM-1.0-int-013	MOV03	M	
	MPRI	M	
SRM-1.0-int-014	LRC01	M	
	LRC03	M	
SRM-1.0-int-015	LRC02	M	
	LRC04	M	
SRM-1.0-int-016	UTL01	M	
	UTL06	M	
SRM-1.0-int-017	UTL05	M	
	UTL07	M	
	MOV06	M	
SRM-1.0-int-018	UTL11	O	
	UTL12	O	
SRM-1.0-int-019	UTL02	M	
	UTL08	M	
SRM-1.0-int-020	UTL03	M	
	UTL09	M	
SRM-1.0-int-021	UTL04	M	
	UTL10	M	
SRM-1.0-int-022	None	-	
SRM-1.0-int-023	None	-	
SRM-1.0-int-024	RICE02	O	
	RICE05	O	
SRM-1.0-int-025	RICE03	O	
	RICE06	O	
SRM-1.0-int-026	RICE04	O	
	RICE07	O	

Table 2: Enabler Validation Test Cases

7.2 Non-Covered ETR Requirements

The table below shows the ETR requirements that are not covered in the test cases used for validation of the SRM enabler.

ETR Requirement Id	ETR Status	Notes
LOG01	M	Error logging conformance is not tested
EXP01	M	Exception recovery conformance is not tested
EXP02	M	Exception recovery conformance is not tested
EXP03	M	Exception recovery conformance is not tested
EXP04	M	Exception recovery conformance is not tested
OCSP05	O	Conformance requirements are not tested

© 2008 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-EnablerValidationPlan-20070308-I]

ETR Requirement Id	ETR Status	Notes
RICER01	M	Conformance requirements are not tested
SRMRMV	O	Conformance requirements are not tested
IOP01	O	Requires a full DRM 2.0 client and Rights Issuer server. Impractical to test as part of an SRM test event.

Table 3: Non-Covered ETR Requirements

© 2008 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.

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 1.0 History

Document Identifier	Date	Sections	Description
Draft Versions OMA-EVP-SRM V1_0	21 Jan 2008	All	Initial draft
	28 Mar 2008	5.1.2, 5.1.3, 5.3.2, 5.4	CR incorporated: OMA-IOP-BRO-2008-0055
Candidate Versions OMA-EVP-SRM V1_0	28 Apr 2008	n/a	TP approved ref# OMA-TP-2008-0178-INP_SRM_1.0_EVP_for_Candidate_Approval
Draft Versions OMA-EVP-SRM V1_0	22 Sep 2008	7.1, 7.2	CR incorporated: OMA-IOP-BRO-2008-0134
Candidate Versions OMA-EVP-SRM V1_0	30 Sep 2008	n/a	TP approved ref# OMA-TP-2008-0368-INP_SRM_1.0_EVP_for_notification
Draft Versions OMA-EVP-SRM V1_0	03 Nov 2008	5.1.3	Incorporated CR: OMA-IOP-BRO-2008-0171
Candidate Versions OMA-EVP-SRM V1_0	06 Nov 2008	n/a	TP approved ref# OMA-TP-2008-0437-INP_SRM_1.0_EVP_for_notification

© 2008 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-EnablerValidationPlan-20070308-I]