OMA Secure Removable Media Architecture

Candidate Version 1.0 – 28 Jan 2008

Open Mobile Alliance

OMA-AD-SRM-V1_0_0-20080128-C

Contents

Figures

Tables

1. Scope (Informative)

The scope of OMA *"Secure Removable Media"* 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 specifications to provide mechanisms for the secure transfer of Rights between a DRM Agent and an SRM Agent including their mutual authentication.

2. References

2.1 Normative References

[OSE] "OMA Service Environment"
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

[OMA-DICT] "OMA Dictionary", Open Mobile Alliance™, OMA-Dictionary-V1_0-20031014-A,URL:http://www.openmobilealliance.org/

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

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

[SRM-RD] "OMA Secure Removable Media Requirements", Open Mobile Alliance™, OMA-RD_SRM-V1_0, URL:http://www.openmobilealliance.org/

3. Terminology and Conventions

3.1 Conventions

This is an informative document, which is not intended to provide testable requirements to implementations.

3.2 Definitions

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. The Device may include a smartcard module (e.g. a SIM) or not depending upon implementation
DRM Agent	The entity in the device that manages Permissions for Media Objects on the device. (From [OMADRMv2])
DRM Content	Media Objects that are consumed according to a set of Permissions in a Rights Object
Interface	See [OMA-DICT].
Rights	Rights are the 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. (From [OMADRMv2])
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 Objects in Secure Removable Media, for delivering Rights Objects 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

CA	Certificate Authority
CEK	Content Encryption Key
CRL	Certificate Revocation List
DRM	Digital Rights Management
OCSP	Online Certificate Status Protocol
OMA	Open Mobile Alliance
PKI	Public Key Infrastructure
ROAP	Rights Object Acquisition Protocol
R-UIM	Removable User Identity Module
SD	Secure Digital
S-MMC	Secure MultiMediaCard
SIM	Subscriber Identity Module
SRM	Secure Removable Media
USIM	Universal Subscriber Identity Module

4. Introduction (Informative)

Secure Removable Media is a removable media that implements means to protect against unauthorized access to its internal data and includes an SRM Agent. Example of Secure Removable Media (referred to as SRM hereinafter) may be the secure memory card and the smart card.

The secure memory card has an embedded microprocessor and is capable of storing Rights or DRM Content in a secure manner (e.g. S-MMC, SD). The smart card also has an embedded microprocessor and is capable of storing access codes, user subscription information, secret keys, DRM Content, Rights etc (e.g. SIM, USIM, R-UIM). If a user uses devices with a physical interface to connect an SRM, the user can use the SRM as a means of increasing storage space for DRM Content and portability of Rights. Differently from the secure memory card, the smart card enables users to make a telephone call by using the devices and is issued by a mobile network operator.

OMA DRM with SRM can provide a mechanism to write, read, delete and update Rights in SRM in a secure manner to realize the use cases defined in the OMA SRM Requirements Document [SRM-RD]. While OMA DRM version 2.0 provides a general framework for downloading Rights and sharing Rights in the domain, the OMA SRM enabler extends OMA DRM version 2.0 to allow users to transfer Rights between the device and the SRM and to consume Rights stored in the SRM without generating and managing complex groups of devices in a domain.

4.1 Use Cases

The OMA SRM Requirements Document [SRM-RD] defines the following new use cases;

- Use Case 1: Upgrade from old Devices to new Devices by using the Secure Removable Media
- Use Case 2: Provisioning of Rights Object in the Smart Card
- Use Case 3: Using Contents in Multiple Devices by using the Secure Removable Media
- Use Case 4: Transfer Contents and Rights Objects among OMA Conformant Devices by using the Secure Removable Media
- Use Case 5: Direct Rendering of DRM Contents by using the Secure Removable Media
- Use Case 6: Backup of Rights Object in the Smart Card
- Use Case 7: Pre-Loading of Rights Objects by using the Smart Card

Details of these new use cases are specified in [SRM-RD].

4.2 Requirements

Requirements that satisfy the use cases listed in chapter 4.1 are defined in the OMA SRM Requirements Document [SRM-RD].

4.3 Security Considerations

Based on security considerations of the OMA DRM v2.0, this section defines security issues needed for OMA SRM enabler. Detailed security solutions for the OMA SRM enabler are specified by the OMA SRM technical specification.

4.3.1 Overview

Mutual Authentication: The DRM Agent and the SRM Agent can authenticate each other (i.e. mutual authentication) based on credentials that are securely provisioned in each. The result of this mutual authentication allows the DRM Agent and SRM Agent to establish a secure channel for the exchange and sharing of secret elements.

Message Transaction: Based on the mutual authentication, a Rights Object and its state information (i.e. Rights) or any necessary messages can be securely delivered between the DRM Agent and SRM Agent regardless of lower layer communication (e.g. SD, S-MMC, Smart Card). The secret elements are used to guarantee the confidentiality and integrity of the Rights. A symmetric encryption or keyed hash function may be used.

Replay of message transactions will not result in any action being taken by the receiver that was unintended by the original transmitter of those messages.

Rights Protection: A Rights Object stored in a device is cryptographically bound to the DRM Agent in the device. While moving the Rights Object and its state information, the result of the mutual authentication can be used to protect the confidentiality of sensitive parts (e.g. CEK) and, integrity of the Rights Object itself and state information. After the move operation, the Rights Object is still securely bound to a trusted entity: DRM Agent or SRM Agent.

Protection of Rights Consumption: To consume the Rights, the SRM Agent sends CEK to the DRM Agent. The device decrypts a DRM Content with the CEK. The result of the mutual authentication can be used to protect the confidentiality of the CEK. If the mutual authentication becomes invalid, the transferred CEK has to be invalidated to the DRM Agent.

4.3.2 Trust Model

The trust model required by this enabler is based on the Public Key Infrastructure (PKI) and is an extension of the trust model described in [DRMARCH-v2.0]. The primary entities of the trust model in this enabler are the Certificate Authorities (CA), SRMs, Devices and Rights Issuers. There could be multiple CAs in this system. This enabler does not mandate a specific trust model. The exact nature of any trust model is left up to marketplace decisions.

The SRM Agent has to be trusted by the DRM Agent, in terms of authorization, data protection, and root of trust. Only an authorized DRM Agent can access data stored in the SRM and the SRM Agent has to guarantee the integrity and the confidentiality of the data. The SRM Agent is also trusted enough to hide security elements (e.g. private key) from other entities. What constitutes a trusted DRM Agent or SRM Agent depends on the business policies of the underlying trust model.

Each SRM Agent is provisioned with a unique key pair and an associated certificate signed by an appropriate CA. The certificate identifies the SRM Agent and certifies the binding between the SRM Agent and the key pair. This allows DRM Agents to securely authenticate the SRM Agent. The DRM Agent is also provisioned with a unique key pair and an associated certificate as defined in [OMADRMv2]. This allows SRM Agents to securely authenticate the DRM Agent.

The information in the certificate of the SRM Agent enables the DRM Agent to trust the SRM Agent and send the sensitive data of the Rights Object and its state information to the SRM Agent. The information in the certificate of the DRM Agent also enables the SRM Agent to trust the DRM Agent and send the sensitive data of the Rights Object and its state information to the DRM Agent. Both the SRM and the Device can be provisioned with more than one certificate. Based on the certificate preferences expressed by the SRM Agent, the DRM Agent has to provide an appropriate certificate.

The SRM enabler also assumes that the CA who signs the Device and SRM certificates issues CRLs indicating their revocation status. The CA may also run an OCSP responder for use during the execution of the protocol.

4.3.3 Other Considerations

4.3.3.1 Rights Replay Protection

If Rights in the device is backed up to a remote place and the Rights is moved to the SRM, restoring the Rights causes unexpected Rights duplication. If the Rights in the SRM is backed up, it is possible to assume the same security problem. Another example of Rights replay attack would be interception of Rights by an intermediary while delivering it from a Rights Issuer to the DRM Agent. If the Rights is moved to the SRM and the originally intercepted Rights is installed in the device again, it also causes unexpected Rights duplication. OMA SRM enabler prevents this and similar attacks from occurring.

4.3.3.2 DRM Time for SRM

The SRM (e.g. SD, S-MMC, Smart Card) cannot have a clock inside, therefore will not support DRM Time. The OMA SRM enabler allows proper DRM time related operations for using Rights stored in the SRM even in case of severe hardware restrictions of the SRM.

4.3.3.3 Aborted Transaction Recovery

If transaction fails during Rights consumption, there is possibility for Rights not to be updated properly. If transaction between the device and the SRM is failed during Rights Move operation, there is also possibility for users to lose their Rights. There are two examples of abnormal Move failure:

In case of Rights Move from Device to SRM

> Rights is removed from the device immediately after the Rights has been moved to the SRM. If the transaction is failed before the moved Rights is reached to the SRM, users lose the Rights.

In case of Rights Move from SRM to Device

> Rights is removed from the SRM immediately after the Rights has been moved to the device. If the transaction is failed before the moved Rights is reached to the device, users lose the Rights.

If the Rights is removed from an originated entity after the Rights have reached the other side successfully, the transaction failure may cause another security problem - unexpected duplication of the Rights.

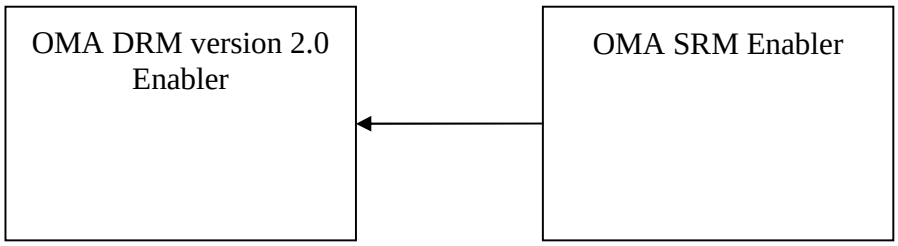
The transaction failure may occur by unstable communication between the device and the SRM which happens rarely or by unexpected physical disconnection of the SRM from the device. To prevent the above problems, OMA SRM enabler has to provide with ways to recover the transaction failure.

5. Architectural Model

5.1 Dependencies

The OMA SRM enabler defines the format and the protection mechanism of the Rights in the SRM and the security model for managing encryption keys in the SRM. It also defines the protection mechanism for transferring Rights and DRM Content between devices and SRM(s) and consuming Rights in the SRM(s). To achieve these functions, the OMA SRM enabler uses OMA DRM version 2.0 [OMADRMv2] as its foundation. The architecture defined in this document takes precedence over those specified by the foundation documents, thus creating the OMA SRM enabler.

The relationship between the enablers is illustrated in Figure 1.



A → B Indicates that the enabler A uses functions of the enabler B.

Figure 1: OMA SRM Enabler Dependencies

5.2 Architectural Diagram

Figure 2 shows the architectural diagram of OMA SRM.

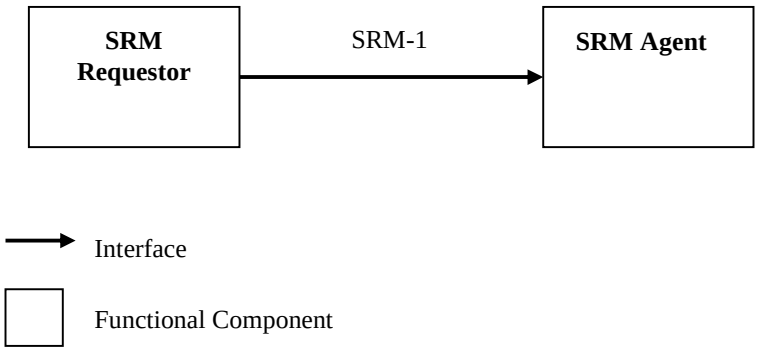


Figure 2: Architectural Model

Figure 3 shows the functional architecture of OMA SRM.

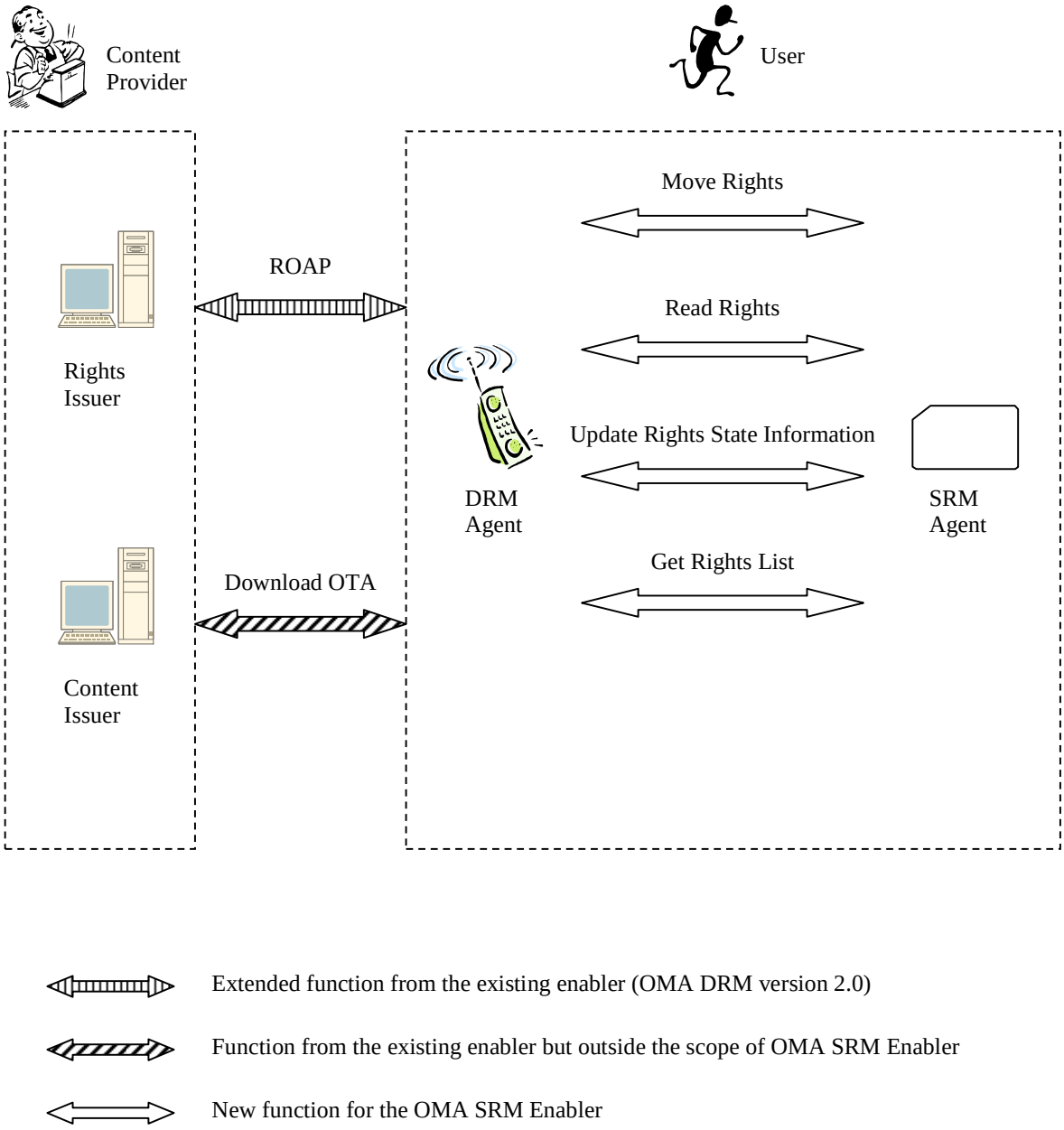


Figure 3: Functional Architecture

5.3 Functional Components and Interfaces

5.3.1 Functional Components

This section describes the OMA SRM functional components. Some of these components are existing entities whose details are defined in [OMADRMv2].

- **Rights Issuer**

  The Rights Issuer is an entity that assigns permissions and constraints to DRM Content, and generates Rights Objects. Rights Objects govern how DRM Content may be used – DRM Content cannot be used without an associated Rights Object, and may only be used as specified by the Rights Object. The Rights Issuer specifies in the Rights Object the usage of the SRM to store Rights.

- **DRM Agent**

  A DRM Agent embodies a trusted entity in a device. This trusted entity is responsible for enforcing permissions and constraints associated with DRM Content, controlling access to DRM Content, etc. The DRM Agent securely communicates with the SRM Agent to control and manage the Rights stored in the SRM.

- **SRM Agent**

  A SRM Agent is a trusted entity embodied in Secure Removable Media. This trusted entity is responsible for storing and removing Rights Objects in Secure Removable Media. It also securely transfers Rights Objects and associated information to and from a DRM Agent,

5.3.2 Interfaces

The OMA SRM interfaces are defined in Table 1.

Interfaces	Description
SRM-1	This interface supports Requests to transfer Rights Objects and associated state information Requests to read the list of Rights in the SRM Requests to transfer Rights in the SRM Requests to consume Rights The use of this interface can involve mutual authentication, confidentiality, and integrity.

Table 1: Interface descriptions

5.4 Flows

Functions between each component which constitutes the functional architecture in **Error! Reference source not found.** are explained in this chapter.

- **Move Rights**

  This function moves a Rights Object and its associated state information (i.e. Rights) from the SRM to the DRM agent (or vice versa). After the move, the Rights Object and its associated state information is present in the destination and deleted from the source and it is guaranteed that duplication or loss of Rights is not possible.

- **Read Rights**

  The DRM agent reads the Rights Object and its associated state information (i.e. Rights) from the SRM and can use it (i.e. locally consume) if and only if the same SRM agent is securely connected to the DRM agent.

- **Update Rights State Information**

  The DRM agent updates the state information of SRM's Rights that are locally consumed by the DRM agent.

- **Get Rights List**

  The DRM Agent retrieves a list of Rights identifiers from the SRM Agent. The SRM Agent can provide this list identifying Rights Objects that are associated with a specific DRM Content.

- **ROAP**

  The ROAP (RO Acquisition Protocol) in the OMA DRM version 2.0 provides the format, the protection mechanism and the transport mechanism for the Rights Object and the security model for managing of content encryption keys. The OMA SRM enabler provides the extended mechanisms and security model to enable the Rights Object to be stored in the SRM.

- **Download OTA**

  This is out of the scope of the OMA SRM enabler. It provides the transport mechanism to deliver DRM Content from the content issuer to the DRM Agent.

5.5 Service Scope

The OMA SRM enabler supports three functional services based on the architecture defined in this document. The services are shown in following sub chapters.

5.5.1 Service 1 - Basic Model

A Rights Issuer issues Rights bound to a Device as defined in [OMADRMv2] with the permission to move. The Rights can be moved from the Device to an SRM. The moved Rights can also be used by multiple Devices for rendering its associated DRM Content. The Rights can be moved to the original Device or other Devices.

Figure 44 shows components and interfaces for the basic model and Table 2 specifies actions on the interfaces. The actions can be permitted or restricted by a permission or constraint stated in the Rights.

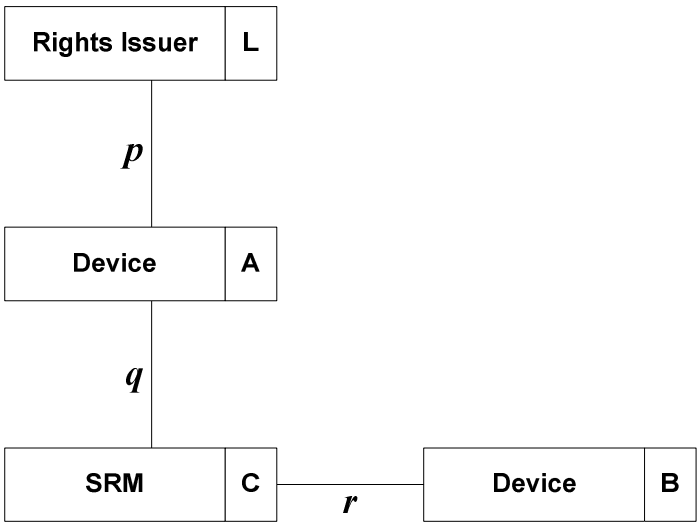


Figure 44: Components and Interfaces in Service 1

Interfaces	Actions
p	The "Rights Issuer – L" issues a Rights to the "Device – A". The issued Rights can be used by the "Device – A"
q	The Rights in the "Device – A" can be moved from the "Device – A" to the "SRM – C" (Refer to chapter **Error! Reference source not found.**) The Rights in the "SRM – C" can be moved from the "SRM – C" to the "Device – A" (Refer to chapter **Error! Reference source not found.**) The Rights in the "SRM – C" can be consumed by the "Device – A" as stored in the "SRM – C" (Refer to chapter **Error! Reference source not found.**)
r	The Rights in the "Device – B" can be moved from the "Device – B" to the "SRM – C" (Refer to chapter 6.1.1) The Rights in the "SRM – C" can be moved from the "SRM – C" to the "Device – B". (Refer to chapter **Error! Reference source not found.**)

	The Rights in the "SRM – C" can be consumed by the "Device – B" as stored in the "SRM – C" (Refer to chapter **Error! Reference source not found.**)

Table 2: Actions in Service 1

Using the interfaces provided by "q" and "r", the Rights in the "Device – A" can be moved to "Device – B" via "SRM – C". Before the move from "SRM – C" to "Device – B", the Rights in "SRM – C" may or may not have been consumed.

Although not directly shown in Figure 4, interfaces "q" and "r" can also be used to move the Rights from one (source) SRM to another (sink) SRM via a Device. Before the move from the Device to the sink SRM, the Device may or may not have consumed the Rights.

5.5.2 Service 2 - Preloaded Rights in SRM

A Rights can be installed in an SRM during manufacturing the SRM. The preloaded Rights in the SRM can be used by Devices for rendering its associated DRM Content.

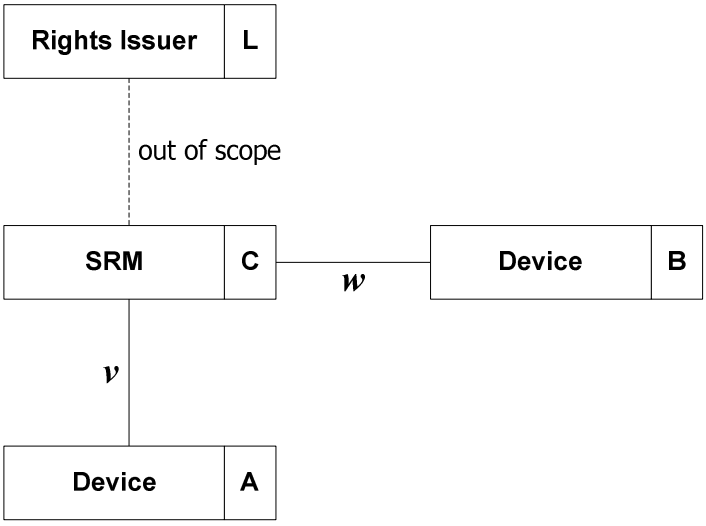


Figure 5 shows components and interfaces for the preloaded Rights service and Table 3 specifies actions on the interfaces. The actions can be permitted or restricted by a permission or constraint stated in the Rights.

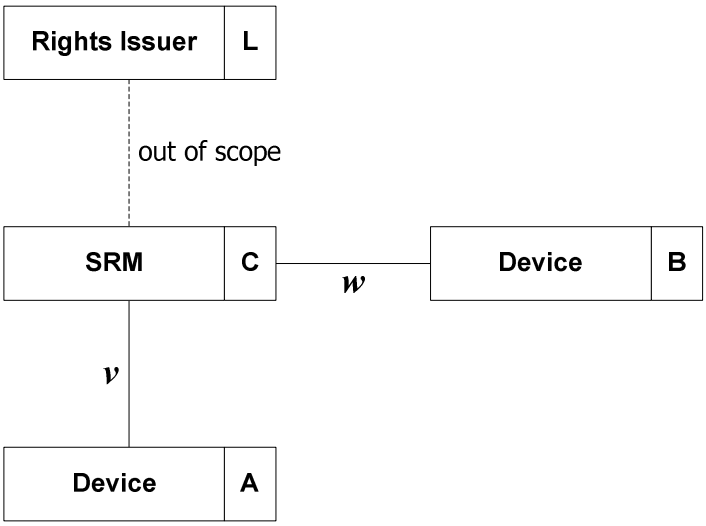


Figure 5: Components and Interfaces in Service 2

Interfaces	Actions
v	The Rights in the "SRM – C" can be used by the "Device – A" as stored in the "SRM – C" (Refer to chapter **Error! Reference source not found.**) The Rights in the "SRM – C" can be moved from the "SRM – C" to the "Device – A". (Refer to chapter **Error! Reference source not found.**) After this action, the moved Rights can be used by the "Device – A"
w	The Rights in the "SRM – C" can be used by the "Device – B" as stored in the "SRM – C" (Refer to chapter **Error! Reference source not found.**) The Rights in the "SRM – C" can be moved from the "SRM – C" to the "Device – B". (Refer to chapter **Error! Reference source not found.**) After this action, the moved Rights can be used by the "Device – B"

Table 3: Actions in Service 2

The interface between the Rights Issuer and the "SRM – C" is out of scope.

5.5.3 Service 3 – On-Line Rights Issue into SRM

A Rights Issuer issues Rights to an SRM Agent by online. The Rights can be used by Devices for rendering its associated DRM Content.

Figure 6 shows components and interfaces for the Rights issue service and Table 4 specifies actions on the interfaces. The actions can be permitted or restricted by a permission or constraint stated in the Rights.

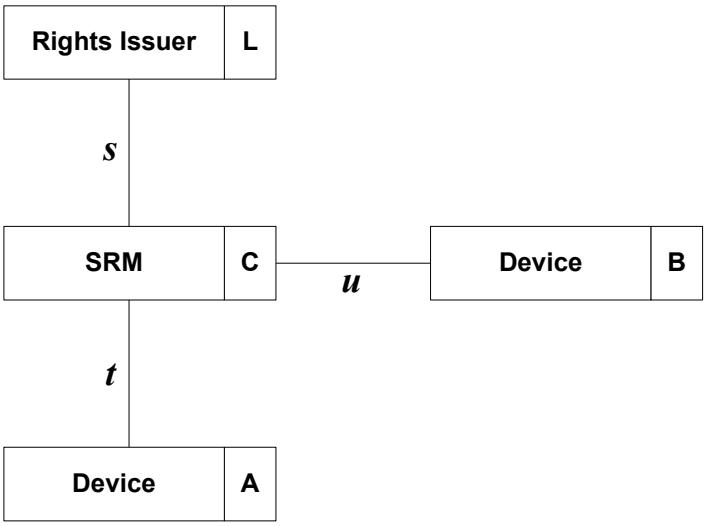


Figure 6: Components and Interfaces in Service 3

Interfaces	Actions
s	The "Rights Issuer – L" issues a Rights to the "SRM Agent – C" by online. (Refer to chapter **Error! Reference source not found.**)
t	The Rights in the "SRM – C" can be used by "Device – A" as stored in the "SRM – C" (Refer to chapter **Error! Reference source not found.**) The Rights in the "SRM – C" can be moved from the "SRM – C" to the "Device – A". (Refer to chapter **Error! Reference source not found.**) After this action, the moved Rights can be used by the "Device – A"
u	The Rights in the "SRM Agent – C" can be used by "Device – B" as stored in the "SRM – C" (Refer to chapter **Error! Reference source not found.**) The Rights in the "SRM – C" can be moved from the "SRM – C" to the "Device – B". (Refer to chapter **Error! Reference source not found.**) After this action, the moved Rights can be used by the "Device – B"

Table 4: Actions in Service 3

6. Example Flow of Technical Use Cases (Informative)

The use cases defined in the OMA SRM Requirements Document [SRM-RD] can be classified into the following technical use cases. This chapter provides the definition of the technical use cases and shows how to achieve the use cases and the requirements in [SRM-RD]. Figure 7 shows an example implementation of the SRM architecture.

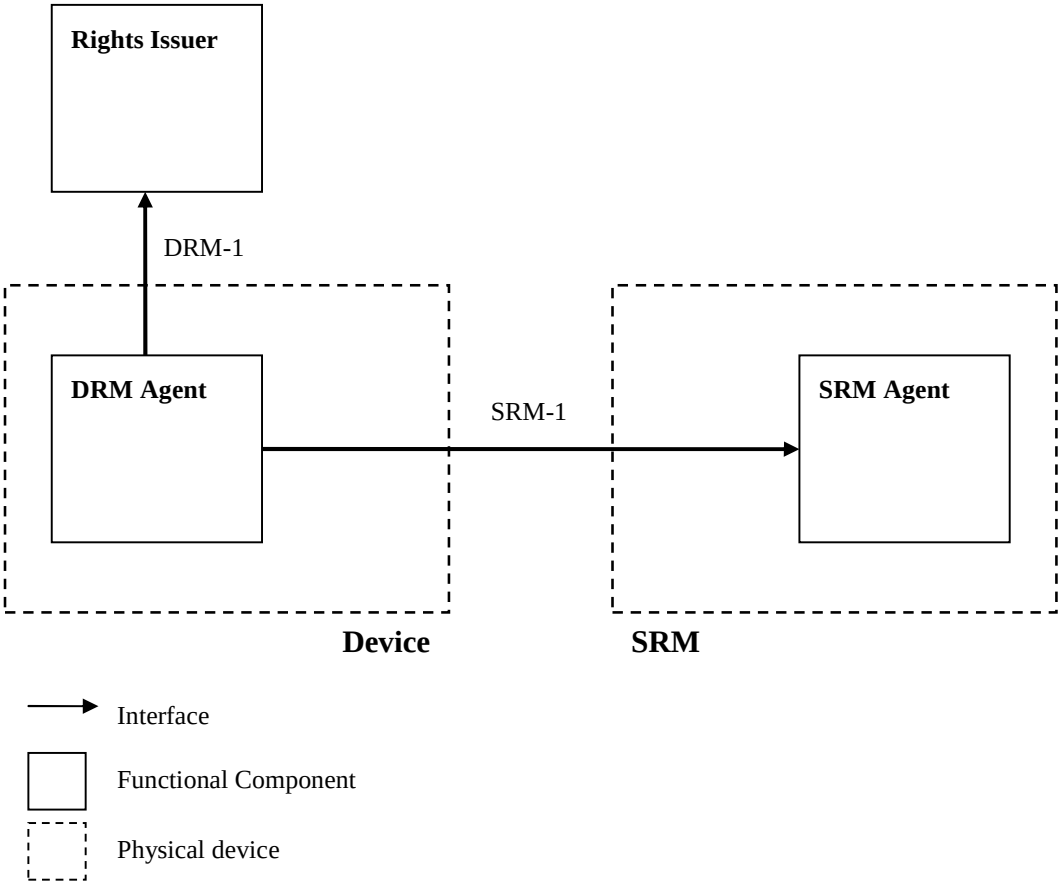


Figure 7: Example Implementation of SRM Architecture

Note: The DRM-1 interface in Figure 7 carries transactions and data to the DRM Agent and is shown for reference. The specification for this interface is contained in OMA DRM v2.0.

6.1 Flow

6.1.1 Rights Move from Device to SRM

This technical use case describes the basic functionality of OMA SRM. Rights are moved from the Device to the SRM. Users can store her or his Rights in the SRM by this use case. This move procedure includes relocating and removing the Rights from the Device.

Action:

1. The DRM Agent selects Rights stored in the Device.
2. The DRM Agent moves the selected Rights to the SRM Agent and the SRM Agent stores it in the SRM. The selected Rights are removed immediately from the Device after it is moved.

Figure 8: Sequence Diagram – Rights Move from Device to SRM

6.1.2 Rights Move from SRM to Device

This technical use case describes the case when Rights is moved from the SRM to the Device. This transfer procedure includes relocating and removing the Rights from the SRM.

Action:

1. The DRM Agent requests the SRM Agent to retrieve a list of Rights identifiers in the SRM and the SRM Agent sends the list to the DRM Agent.
2. The DRM Agent selects Rights in the SRM by referring to the list of Rights identifiers.
3. The DRM Agent requests the SRM Agent to move the selected Rights to the Device. On receiving the request, the SRM Agent moves the selected Rights to the DRM Agent and the DRM Agent stores it in the Device. The selected Rights are removed immediately from the SRM after it is moved.

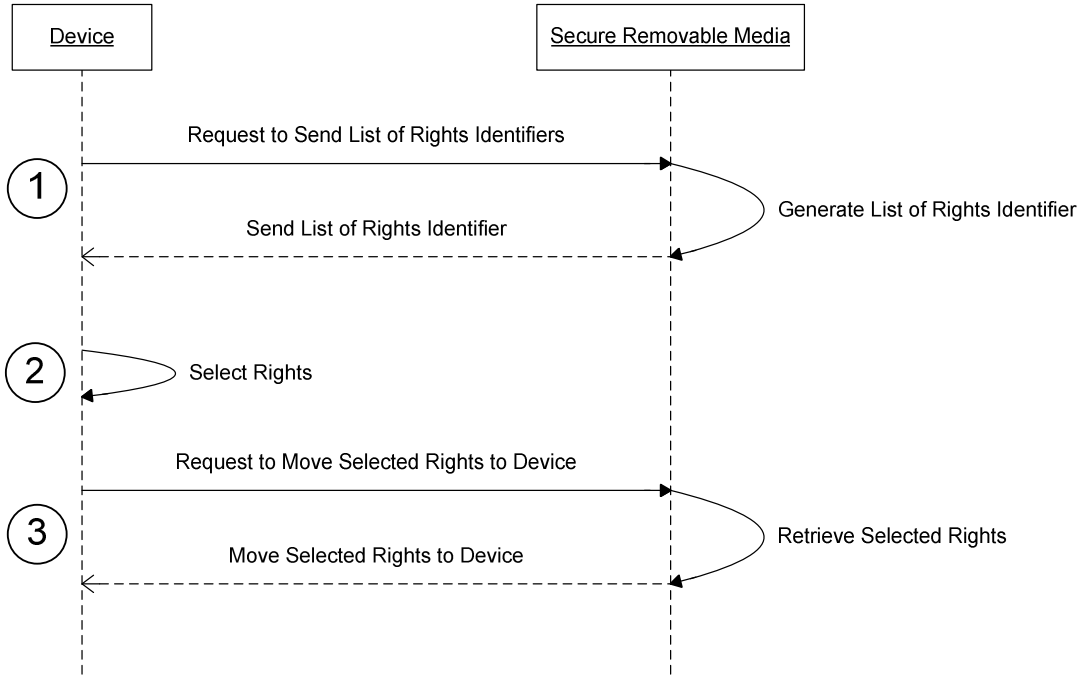


Figure 9: Sequence Diagram – Rights Move from SRM to Device

6.1.3 Rights Consumption in SRM

This technical use case illustrates the case when Rights stored in the SRM is consumed by the DRM Agent to use DRM Content. The consumption is realized by reading and updating state information of the Rights stored in the SRM.

If the DRM Agent once reads the Rights, the Rights are stored in the buffer of the device temporarily. It cannot be used if the SRM Agent from which the Rights were retrieved is not securely connected to the DRM Agent.

Action:

1. The DRM Agent requests the SRM Agent to retrieve a list of Rights identifiers in the SRM and the SRM Agent sends the list to the DRM Agent.
2. The DRM Agent selects Rights by referring to the list of Rights identifiers.
3. The DRM Agent requests the SRM Agent to read the selected Rights (i.e. Rights Object and its state information) in the SRM.
4. While DRM Content is being used, the DRM Agent requests the SRM Agent to update the state information of the selected Rights in the SRM and the SRM Agent updates it. The SRM Agent returns the result of the state information update to the DRM Agent. If some errors occur during the consumption process, the DRM Agent and the SRM Agent should ensure the state information has been updated correctly.

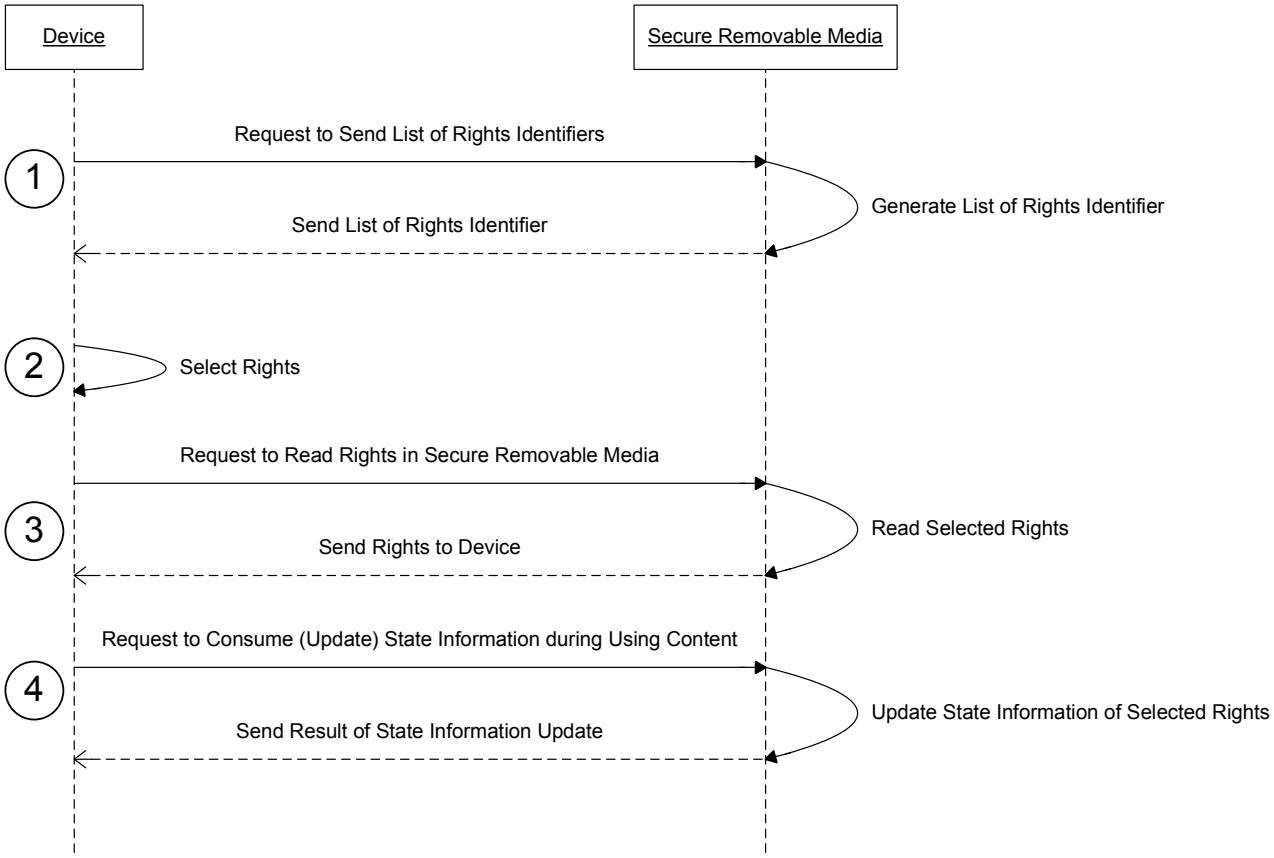


Figure 10: Sequence Diagram – Rights Consumption in SRM

6.1.4 Provisioning of Rights Object in the Secure Removable Media

The technical use case illustrates Provisioning of Rights Object in the Secure Removable Media where the Rights Issuer issues a Rights Object for installation on the SRM. For the actions below, the Device interacts with the Secure Removable Media and fetches the SRM info. The SRM info contains information which is used by the Rights Issuer to uniquely identify the Secure Removable Media.

Action:

1. Rights Issuer sends ROAP Trigger to the Device, to initiate the download of the Rights Object to be stored on the Secure Removable Media.
2. Device sends RO Request to Rights Issuer. Rights Issuer sends RO Response to the Device with Rights Object to be installed in Secure Removable Media.
3. Device transfers Rights Object to Secure Removable Media and the SRM Agent installs the Rights Object.

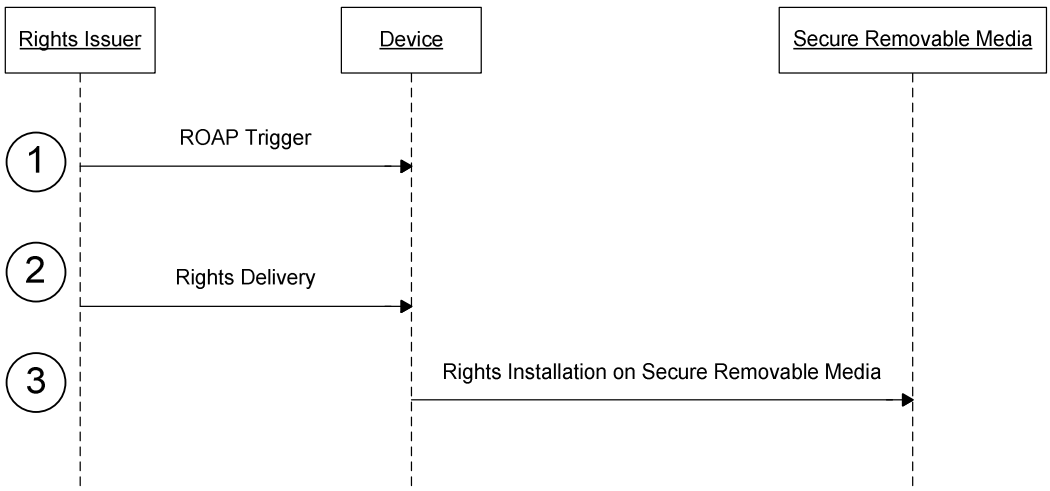


Figure 11: Sequence Diagram – Provisioning of Rights Object in Secure Removable Media

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 History

Document Identifier	Date	Sections	Description
OMA-AD-SRMProfile-V1_0_0_20060406-D	6 April 2006	All	First Draft
	6 April 2006	6.x	Adds technical use cases agreed into OMA-DLDRM-2006-0120R01-SRMProfile-AD-Technical-UseCase during Vancouver meeting (3rd-7th April 2006)
OMA-AD-SRMProfile-V1_0_0_20060609-D	9 June 2006	4.3, 5.3, 6.x	Add Security Considerations text as agreed in OMA-DLDRM-2006-0177R03 Add text for functional components and interfaces and removed some technical use cases as agreed in OMA-DLDRM-2006-0186R01
OMA-AD-SRMProfile-V1_0_0_20060629-D	29 June 2006	1 3.x 6.1.x	Revise scope as agreed at Osaka meeting Define AD as an Informative document; update abbreviations Add technical use case flow as agreed in OMA-DLDRM-2006-0184R03
OMA-AD-SRM-V1_0_0_20060830-D	30 Aug 2006	4.3.3.1 5.5 6.1.x	Revise text as agreed in OMA-DLDRM-2006-0322R01 Add Service Scope section as agreed in OMA-DLDRM-2006-0323R02 Revise technical use cases as agreed in OMA-DLDRM-2006-0211R01 and OMA-DLDRM-2006-0304R01
OMA-AD-SRM-V1_0_0_20061109-D	09 Nov 2006	5.4 6.1.x 6.2	Removed "Get Rights Information" Removed sections 6.1.4 and 6.1.5. Revised text in 6.1.6 as agreed in OMA-DLDRM-2006-0464R02 Removed section 6.2
OMA-AD-SRM-V1_0_0_20070131-D	31 Jan 2007	3.2 4.3.3.4 Fig 3 5.3.2 5.5.x	Add new definitions Removed section 4.3.3.4 as agreed in ADRR Revised figure 3 architecture diagram as agreed in ADRR Revise description of SRM-IF1 as agreed in ADRR Revised service 1 and removed service 4 as agreed in OMA-DLDRM-2006-0483R02
OMA-AD-SRM-V1_0_0_20070214-D	14 Feb 2007	5.2 5.3.2	Revise figure 2 and interface descriptions as agreed in OMA-DLDRM-2007-003R2
OMA-AD-SRM-V1_0_0_20070316-D	16 Mar 2007	5.2 5.3.2 6	Revise figure 2 and interface descriptions, add figure 7 as agreed in OMA-DRM-2007-115.
OMA-AD-SRM-V1_0_0_20071029-D	29 Oct 2007	4.1 2,2, 3.3, 4.2.3	Revise use case names as agreed in OMA-DRM-439R01 Revise description of trust model as agreed in OMA-DRM-2007-479
Candidate Versions OMA-AD-SRM-V1_0-20080128-C	28 Jan 2008	n/a	Status changed to Candidate by TP TP ref# OMA-TP-2007-0508-INP_SRM_V1_0_ERP_for_Candidate_Approval.