OMA Secure Removable Media Architecture

Candidate Version 1.1 – 18 May 2010

Open Mobile Alliance

OMA-AD-SRM-V1_1-20100518-C

© 2010 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.

© 2010 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms set forth above.

Contents

© 2010 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.

Figures

Tables

© 2010 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.

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.

© 2010 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

[OSE] "OMA Service Environment"
URL: http://www.openmobilealliance.org/

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

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

[OMASCEv1.0] "Secure Content Exchange", Open Mobile Alliance™, OMA-DRM-SCE-V1_0,
URL:http://www.openmobilealliance.org/

[SRM-ADv1.0] "OMA Secure Removable Media Architecture", version 1.0, Open Mobile Alliance™, OMA-AD_SRM-V1_0,
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

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

[DRMXBS] "OMA DRM v2.0 Extensions for Broadcast Support", Open Mobile Alliance™, OMA-TS-DRM_XBS-V1_0-20081120,

URL: http://www.openmobilealliance.org/

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

[OMABCASTv1.1] "OMA Broadcasting", version 1.1, Open Mobile Alliance™, OMA-BCAST-V1_1, URL:
http://www.openmobilealliance.org/

[OMASRMv1.0] "Secure Removable Media", Open Mobile Alliance™, OMA-DRM-SRM-V1_0,
URL:http://www.openmobilealliance.org/

[SRM-RDv1.1] "OMA Secure Removable Media Requirements", Open Mobile Alliance™, OMA-RD_SRM-V1_1, URL:http://www.openmobilealliance.org/

© 2010 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 (Normative)

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 appendices, except “Scope” and “Introduction”, are normative, unless they are explicitly indicated to be informative.

3.2 Definitions

Device	A Device is the entity (hardware/software or combination thereof) within user equipment that implements a DRM Agent. The Device is also conformant to the OMA DRM specifications.
DRM Agent	The entity that manages Permissions for Media Objects
DRM Content	Media Objects that are consumed according to a set of Permissions in a Rights Object. (From [SRM-ADv1.0])
Interface	See [OMA-DICT].
Local Rights Consumption	Operations in which Rights stored in SRMs are transferred for use by the recipient Device for a limited period of time for rendering purposes.
Move	To make Rights existing initially on a source Device or SRM fully or partially available for use by a recipient Device or SRM, such that the Rights or parts thereof that become usable on the recipient Device or SRM can no longer be used on the source Device or SRM.
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. (From [SRM-ADv1.0])
Rights Issuer	An entity that issues Rights Objects to OMA DRM conformant Devices. (From [SRM-ADv1.0])
Rights Object	A collection of Permissions and other attributes which are linked to Protected Content. (From [OMADRMv2])
Secure Removable Media	A removable media that possesses means to protect against unauthorized access to its internal data and implements and SRM Agent. (e.g. secure memory card, smart card).
SRM Agent	The entity responsible for storing and removing Rights Objects, 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.

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
SCE	Secure Content Exchange

© 2010 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.

SD	Secure Digital
S-MMC	Secure MultiMediaCard
SIM	Subscriber Identity Module
SRM	Secure Removable Media
S2S	SRM to SRM
USIM	Universal Subscriber Identity Module

© 2010 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. 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 SIM and related cards (e.g. USIM, R-UIM) 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-RDv1.1]. While OMA DRM version 2.0 provides a general framework for downloading Rights and sharing Rights in the domain, the OMA SRM version 1.1 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.

The SRM 1.1 conforms to the OMA DRM 2.1 and is backward compatible to the SRM 1.0.

4.1 Version 1.0

Apart from defining the SRM Agent, OMA SRM 1.0 provides the following list of major features that constitute the general framework of the OMA SRM enabler (please note that this is not the exhaustive list):

- Mutual Authentication and Key Exchange between SRM Agent and DRM Agent.
- Format and the protection mechanism of the Rights in the SRM.
- Security model for managing encryption keys in the SRM.
- SRM to Device Rights Move and vice versa.
- Local Rights Consumption.
- Compatibility and Supports for OMA DRM v2.0 [OMADRMv2] and OMA DRM 2.1 [OMADRMv2.1].

4.2 Version 1.1

The followings are the main features of the OMA SRM 1.1 release:

- Direct Provisioning of Rights to the SRM.
- Rights Move between two SRMs.
- SRM Rights Upgrade.
- Compatibility and Supports for the OMA DRM 2.1 [OMADRMv2.1] and the OMA SCE 1.0 [OMASCEv1.0].
- Backward Compatibility to the OMA SRM 1.0 [OMASRMv1.0].
- SRM Extensions for BCAST v1.1 [OMABCASTv1.1].

© 2010 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. Architectural Model (Normative)

The architecture model is based on the requirements defined in [SRM-RDv1.1].

Since Rights in SRM will only be stored, used and managed by DRM Agent via the interface between DRM Agent and SRM Agent, and the Rights is issued from RI or Moved from DRM Agent, SRM enabler SHALL have close dependency on DRM enablers defined in OMA DRM2.1, OMA SCE and OMA BCAST.

As for the security mechanism, the security measures for the interface between SRM Agent and DRM Agent will be defined in SRM 1.1 TS. The security mechanisms for the interface between DRM Agent and RI will be defined in the dependent enablers or are defined in SRM TS for the extensions to the corresponding part in the dependent enablers.

SRM 1.1 enabler security mechanism SHALL be completely kept consistent to SRM 1.0 enabler security mechanism.

5.1 Dependencies

The OMA SRM version 1.1 enabler depends on OMA DRM version 2.0 [OMADRMv2] and OMA DRM version 2.1 [OMADRMv2.1] as its foundation. The architecture defined in this document takes precedence over those specified by the foundation documents, thus creating the OMA SRM v1.1 enabler.

Among other features, SRM v1.1 provides functionalities which may be used by OMA BCAST [OMABCASTv1.1]. These functionalities only depend on OMA DRM v2.0, such that they can be used without implementing OMA DRM v2.1.

SRM v1.1 also provides functionalities which may be used by OMA Secure Content Exchange (SCE) version 1.0 [OMASCEv1.0].

The OMA SRM 1.1 enabler dependencies are illustrated in Figure 1.

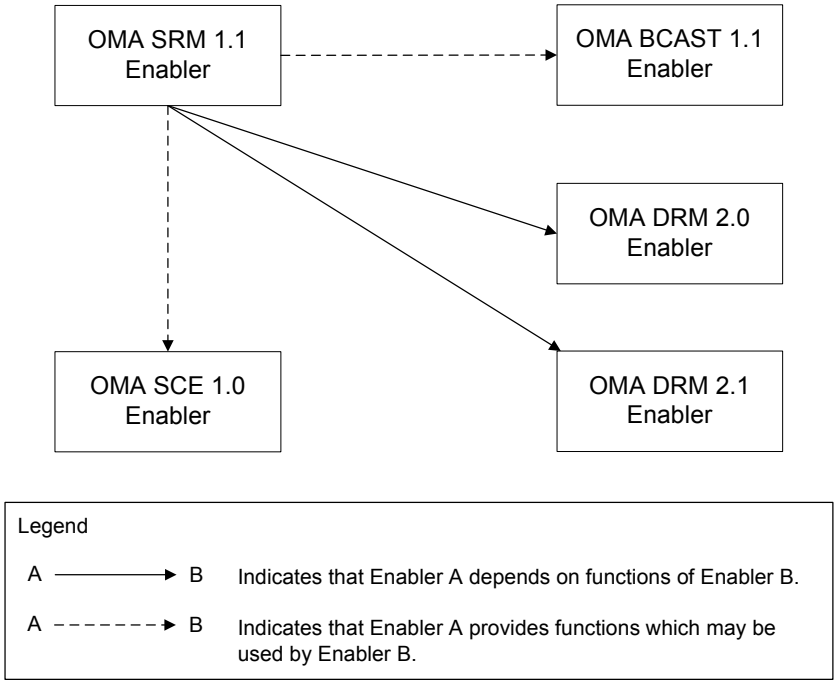

Figure 1: OMA SRM 1.1 Enabler Dependencies

© 2010 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 Architectural Diagram

Figure 2 shows the architectural diagram of OMA SRM v1.1.

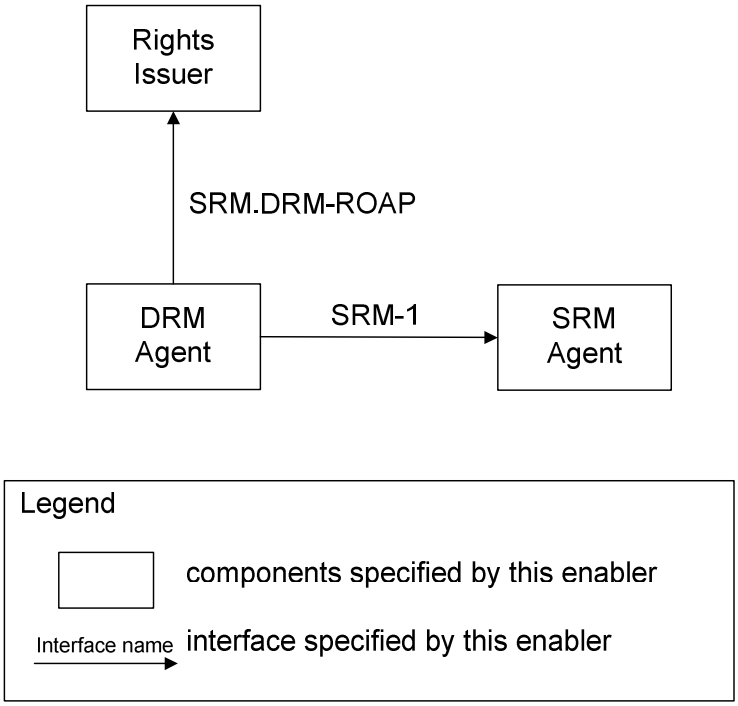

Figure 2: Architectural Diagram

© 2010 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.

5.3 Functional Components and Interfaces

5.3.1 Functional Components

This section describes the OMA SRM v1.1 functional components. Some of these components are existing entities whose details are defined in [OMADRMv2.1].

- **Rights Issuer (RI)**

  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.

  Compared to OMA DRM v2.1, new functionalities for the RI SHALL include:

  - Providing a Rights Object to be downloaded and installed to an SRM.
  - Upgrading an existing Rights Object with additional permissions.

- **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.

  Compared to OMA DRM v2.1, new functionalities for the DRM Agent SHALL include:

  - Mutual authentication and establishment of secure authenticated channel with an SRM Agent.
  - Support of new permissions such as Move.
  - Requesting a Rights Issuer to issue a Rights Object to an SRM.
  - Requesting a Rights Issuer to upgrade an existing Rights Object with additional permissions.

- **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 SHALL support 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. Requests to transfer Tokens and associated token information. Requests to read Tokens in the SRM.

© 2010 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.

	Requests to consume Tokens. The use of this interface can involve mutual authentication, confidentiality, and integrity.
SRM.DRM-ROAP	The SRM.DRM-ROAP interface is an extended version of the ROAP interface as specified in OMA DRM v2.1. This interface SHALL support Issuing a Rights Object to the SRM. Upgrading an existing Rights Object with additional permissions.

Table 1: Interface descriptions

© 2010 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.

5.4 Security Considerations

Based on security considerations of the OMA DRM v2.1 [OMADRMv2.1], this section defines security issues needed for OMA SRM 1.1 enabler. Detailed security solutions for the OMA SRM 1.1 enabler are specified by the OMA SRM v1.1 Technical Specification [OMASRMv1.1].

5.4.1 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 and the 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.

For the secure delivery (e.g. Direct Provisioning of Rights to the SRM, SRM Rights Upgrade) of Rights from the Rights Issuer to the SRM Agent, the REK is cryptographically bound to the SRM Agent, so that only the SRM Agent can access the Rights.

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.

Broadcast Rights Protection: A Broadcast Rights Object stored in a Device or SRM is cryptographically bound to the DRM Agent or SRM Agent in the Device or SRM respectively. A session key established as a result of DRM and SRM Agent's mutual authentication is used to protect confidentiality and/or integrity of the BCRO, BCRO assets (e.g. Service Encryption Key) and BCRO state information while moving them from the SRM to the Device and back.

In order to allow Broadcast Rights consumption, the SRM Agent sends BCRO assets to the DRM Agent encrypting them under the session key. SRM protocol implements a number of mechanisms to avoid Broadcast Rights duplication on multiple Devices as well as maintaining consistency in BCRO state information.

Token Protection: Tokens are securely stored in a Device or SRM, and the integrity protection mechanism is applied during transfer of Tokens between these two entities, similarly to (Broadcast) Rights move protection mechanism. In order to consume Tokens, the DRM Agent has to receive them from the SRM Agent via the move or the local token consumption transaction. Similar to (Broadcast) Rights consumption protection, SRM protocol implements mechanisms to avoid Token duplication on multiple Devices and to maintain integrity and consistency of Token information.

5.4.2 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-v2.1]. 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.

© 2010 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 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.

While SRM v1.0 only defines the protocols for the moving Rights between the DRM Agent and SRM Agent, SRM v1.1 defines the method to deliver the RO(s) directly from the RI to the SRM Agent via the DRM Agent. Therefore the RI should know SRM certificate information in advance for RO protection and applicable other purposes. To know SRM certificate information offline registration and/or online registration can be used between RI and SRM Agent via DRM Agent. The SRM 1.1 enabler will provide the online registration method.

Since the Trust Model can vary from DRM Agent to DRM Agent, the SRM Agent may implement multiple Trust Models. Hence SRM v1.1 protocol for transporting RO between RI and SRM should reflect that RI/DRM Agent/SRM Agent may support different Trust Model(s).

5.4.3 Other Considerations

5.4.3.1 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.

5.4.3.2 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.

5.4.3.3 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:

© 2010 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.

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.

The SRM v1.1 TS defines recovery measures for the newly defined transactions in a way similar to the recovery mechanism in SRM v1.0.

© 2010 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
OMA-TS-SRM-V1_0-20090310-A	10 Mar 2009	Initial document to address the basic starting point Ref TP Doc# OMA-TP-2009-0099-INP_SRM_V1_0_ERP_for_Notification_and_Final_Approval

A.2 Draft/Candidate Version History

Document Identifier	Date	Sections	Description
Draft Versions OMA-AD-SRM-V1_1-20090211-D	11 Feb 2009	6.1.6	Incorporates input to committee: OMA-DRM-2009-0035R01-INP_SRM_AD_SRM_rights_Upgrade
Draft Versions OMA-AD-SRM-V1_1-20090302-D	02 Mar 2009	5.2, 5.4, 5.5.4, 6.1.5	Incorporates input to committee: OMA-DRM-2009-0034R01-INP_SRM_AD_S2S_Move
Draft Versions OMA-AD-SRM-V1_1-20090310-D	10 Mar 2009	6.1.4	Incorporates input to committee: OMA-DRM-2009-0040R02-CR_SRMv1.1_AD_Direct_Provisioning_of_Rights
Draft Versions OMA-AD-SRM-V1_1-20090413-D	13 Apr 2009	4.1 6.1.4	Incorporates input to committee: OMA-DRM-2009-0060-CR_SRM11_AD_Add_use_cases_in_section_4.1 OMA-DRM-2009-0052R02-CR_SRM_AD_Direct_Provision_on_Push_Model
Draft Versions OMA-AD-SRM-V1_1-20090429-D	29 Apr 2009	4 5.1 5.2 5.3 5.4 B. B.7	Incorporates input to committee: OMA-DRM-2009-0065R01-CR_SRMv1_1_AD_Introduction OMA-DRM-2009-0066R01-CR_SRMv1_1_AD_Dependencies OMA-DRM-2009-0067R01-CR_SRMv1_1_AD_Architectural_Diagram OMA-DRM-2009-0068R01-CR_SRMv1_1_AD_Functional_Components_and_Interfaces OMA-DRM-2009-0069-CR_SRMv1_1_AD_Security_Considerations OMA-DRM-2009-0070-CR_SRMv1_1_AD_Example_Flows OMA-DRM-2009-0049R04-CR_SRM_extensions_for_BCAST_in_SRM_1.1_AD
Draft Versions OMA-AD-SRM-V1_1-20090608-D	08 Jun 2009	B.5 5.2 5.3.2	Incorporates input to committee: OMA-DRM-2009-0090R01-CR_Indicate_new_functionality_in_SRM11_AD OMA-DRM-2009-0088R02-CR_modify_the_SRM_to_SRM_Move OMA-DRM-2009-0100R01-CR_SRMv1_1_AD_Reflection_of_informal_review_comments
Draft Versions OMA-AD-SRM-V1_1-20090612-D	12 Jun 2009	B.7.1	Incorporates input to committee: OMA-DRM-2009-0096R01-CR_Update_SRM_Ping_protocol_in_SRM11_AD

© 2010 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.

Document Identifier	Date	Sections	Description
Draft Versions OMA-AD-SRM-V1_1-20090901-D	01 Sep 2009	5.4 5.3 4 4.4, 4.5, 5 5.1 5.1 5 5.4.3.3	Incorporates input to committee: OMA-DRM-2009-0139R03-CR_SRMv1_1_AD_Resolution_for_ADRR_A007 OMA-DRM-2009-0140R01-CR_SRMv1_1_AD_Resolution_for_ADRR_A043 OMA-DRM-2009-0143-CR_SRMv1.1_AD_Resolution_for_ADRR_A015_A016 OMA-DRM-2009-0144-CR_SRMv1.1_AD_Resolution_for_ADRR_A017_A049 OMA-DRM-2009-0145-CR_SRMv1.1_AD_Resolution_for_ADRR_A018_A019_A052 OMA-DRM-2009-0150-CR_SRMv1.1_AD_Resolution_for_ADRR_A024 OMA-DRM-2009-0153R04-CR_Resolution_to_AD_comments_A025_A026_A053 OMA-DRM-2009-0154R01-CR_SRM1.1_Resolution_to_AD_comments_A029_A030_A031_A032 OMA-DRM-2009- 0155R01-CR_SRM1.1_Resolution_to_AD_comments_A038
Candidate Version OMA-AD-SRM-V1_1-20090929-C	29 Sep 2009	N/A	Status changed to Candidate by TP TP ref# OMA-TP-2009-0432-INP_SRM_V1_1_AD_for_Candidate_Approval
Draft Versions	01 Mar 2010	B.1, B.2, B.3	Incorporates input to committee: OMA-DRM-2009-0167R02-CR_Change_the_rights_move_protocol
Candidate Version OMA-AD-SRM-V1_1-20100518-C	05 May 2010	N/A	Status changed to Candidate by TP TP ref# OMA-TP-2010-0206-INP_SRM_V1_1_ERP_for_Candidate_Approval

© 2010 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 B. Flows (Informative)

The use cases defined in the OMA SRM Requirements Document [SRM-RDv1.1] 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-RDv1.1].

B.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 move her or his Rights from the Device to 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 sends the selected Rights to the SRM Agent and the SRM Agent installs them in the SRM. After the successful operation, SRM Agent sends acknowledgment of the successful installation to the DRM Agent.
3. On receiving the response, the selected Rights are immediately deleted from the Device.

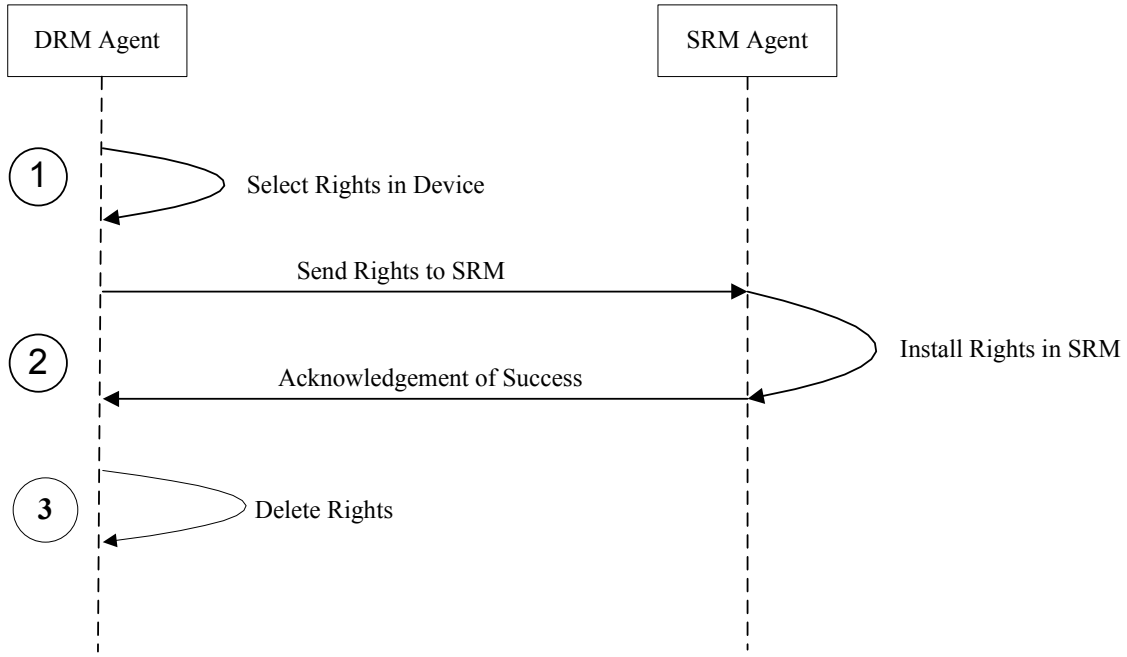

Figure 3: Sequence Diagram – Rights Move from Device to SRM

© 2010 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.

B.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 send the selected Rights to the Device. On receiving the request, the SRM Agent sends the selected Rights to the DRM Agent and the DRM Agent installs them in the Device. The selected Rights are removed immediately from the SRM after it is sent.
4. DRM Agent sends acknowledgment of successful installation to the SRM Agent. On receiving the acknowledgement, the SRM Agent immediately deletes the selected Rights.

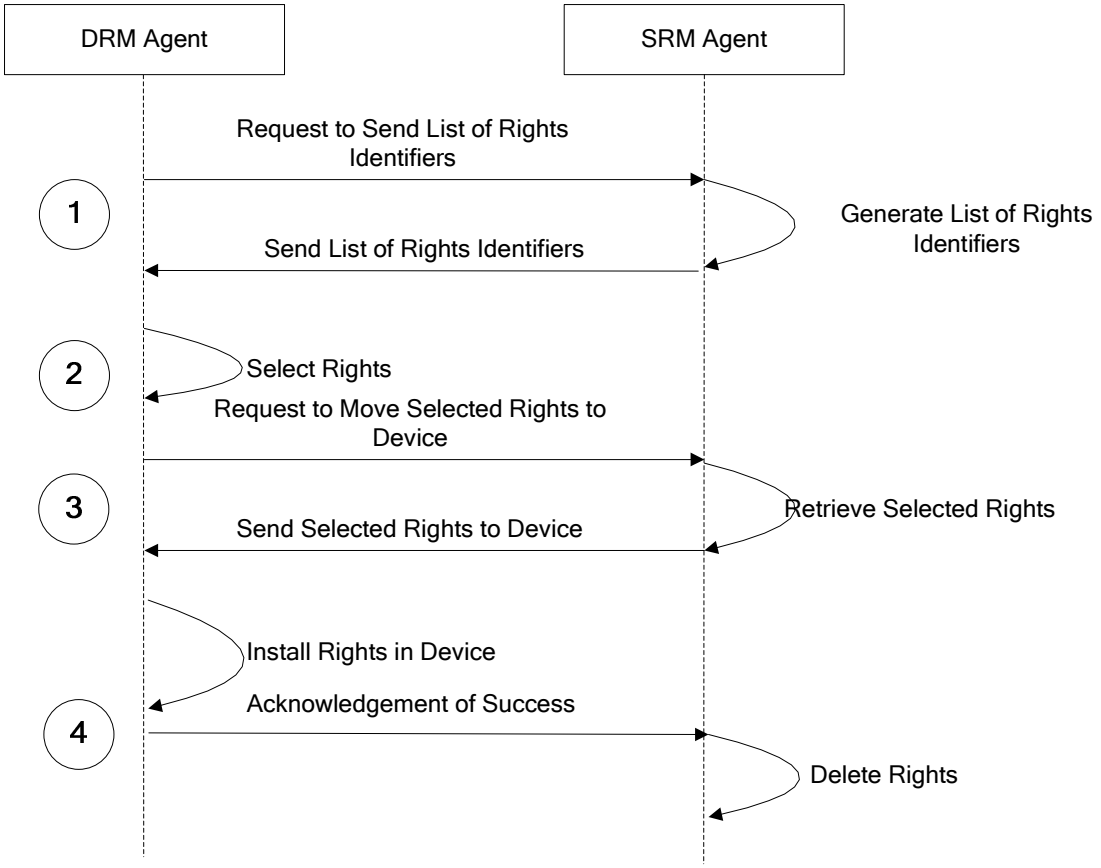

Figure 4: Sequence Diagram – Rights Move from SRM to Device

© 2010 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.

B.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.

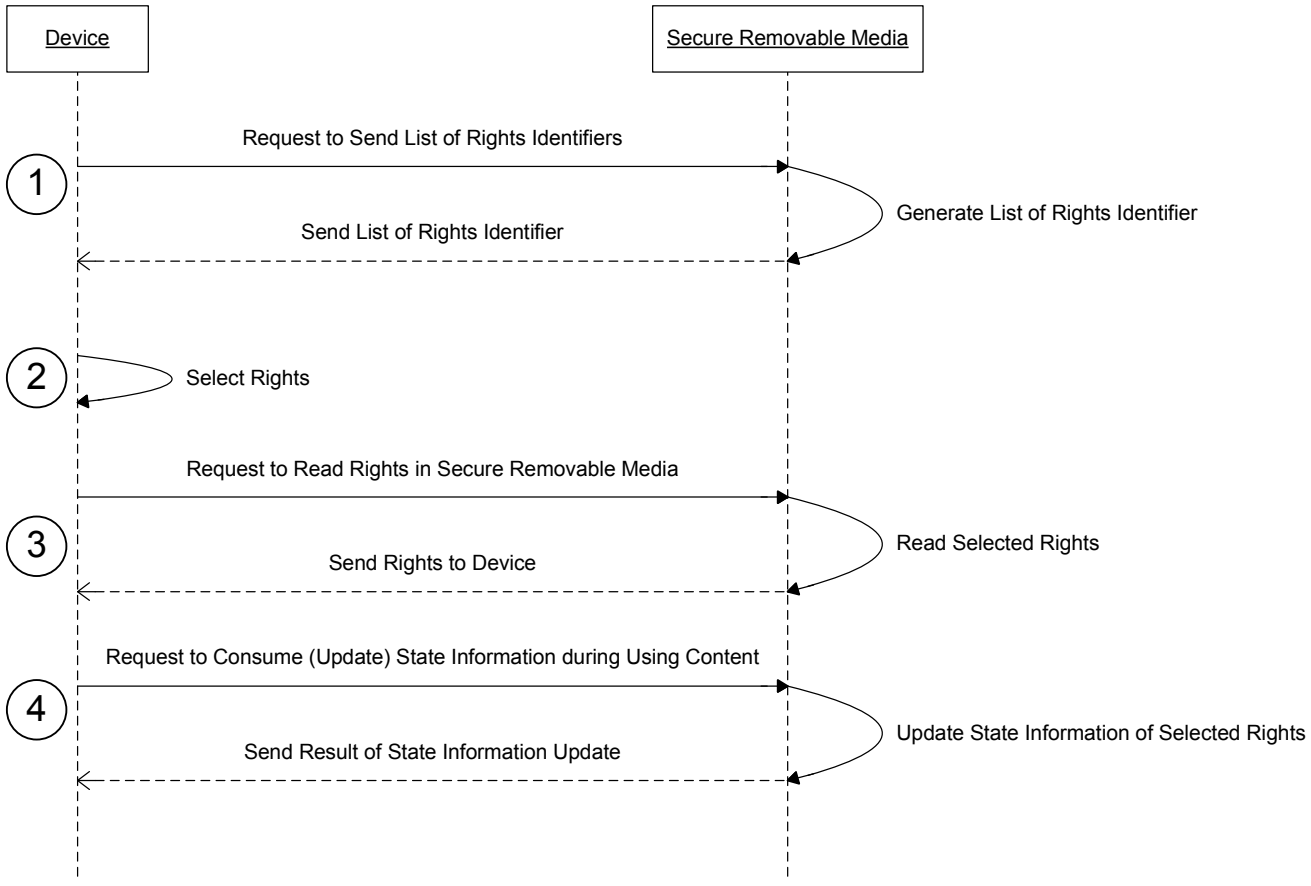

Figure 5: Sequence Diagram – Rights Consumption in SRM

© 2010 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.

B.4 Direct Provisioning of Rights to the SRM

The technical use case illustrates Direct Provisioning of Rights to the SRM where the Rights Issuer issues a Rights Object to SRM. For the actions below, the DRM Agent interacts with the SRM Agent and requests the signature of the SRM Agent. The Rights Object to be downloaded and installed is cryptographically bound to the SRM Agent.

Action on Pull model of RO issuing:

1. Optionally, Rights Issuer sends ROAP Trigger to the DRM Agent, indicating in the Trigger that the Rights Object is to be issued for the SRM Agent.
2. DRM Agent generates body of the RO Request for Rights installation to SRM Agent. At the time the DRM Agent needs a signature of the SRM Agent.
3. DRM Agent sends Signature Request to SRM Agent with message body of RO Request which needs the signature of the SRM Agent.
4. SRM Agent sends Signature Response to DRM Agent with the signature of the SRM Agent.
5. DRM Agent sends RO Request to Rights Issuer with the signature of the SRM Agent which signified that RO is requested by the SRM Agent.
6. Rights Issuer sends RO Response to the DRM Agent with Rights Object that was bound to SRM Agent.
7. DRM Agent sends Rights Provisioning Request to SRM Agent with the Rights for installation.
8. SRM Agent verifies the Rights. If verification of the Rights is successful, the SRM Agent installs the Rights and sends Rights Provisioning Response to DRM Agent.

It is assumed that the DRM Agent performs necessary authentication and validation procedures prior to communicating with the SRM Agent. It also assumes that the Rights Object is signed by the Rights Issuer.

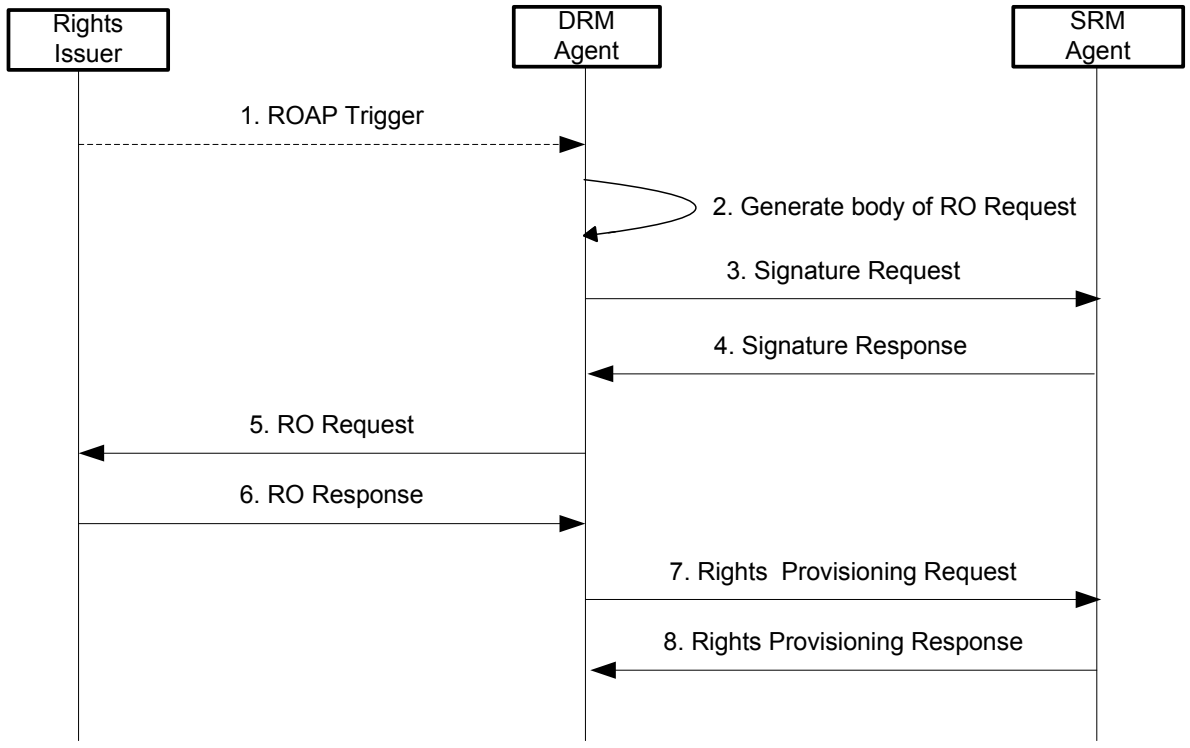

Figure 6: Sequence Diagram – Direct Provisioning of Rights to SRM on Pull Model

© 2010 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.

Action on Push model of RO issuing:

Another scenario for Direct Provision shown in Figure 14 is the subscription based push of rights. In this model, the RI has an established subscription and charging agreement with DRM Agent for the SRM which is bound to that DRM Agent. As a result of this, the Rights Issuer can push both DRM Content and Rights Objects to the clients on a regular interval.

Following is the general description:

1. RO Subscription is made for SRM which is bound to DRM Agent. Optionally, DRM Agent makes subscription via the portal of RI and registers the information of target SRM which is inserted in that DRM Agent.
2. Rights Issuer sends RO Response to the DRM Agent with Rights Object that was bound to SRM Agent.
3. DRM Agent sends Rights Provisioning Request to SRM Agent with the Rights for installation.
4. SRM Agent verifies the Rights. If verification of the Rights is successful, the SRM Agent installs the Rights and sends Rights Provisioning Response to DRM Agent.

It is assumed that the DRM Agent performs necessary authentication and validation procedures prior to communicating with the SRM Agent. It also assumes that the Rights Object is signed by the Rights Issuer.

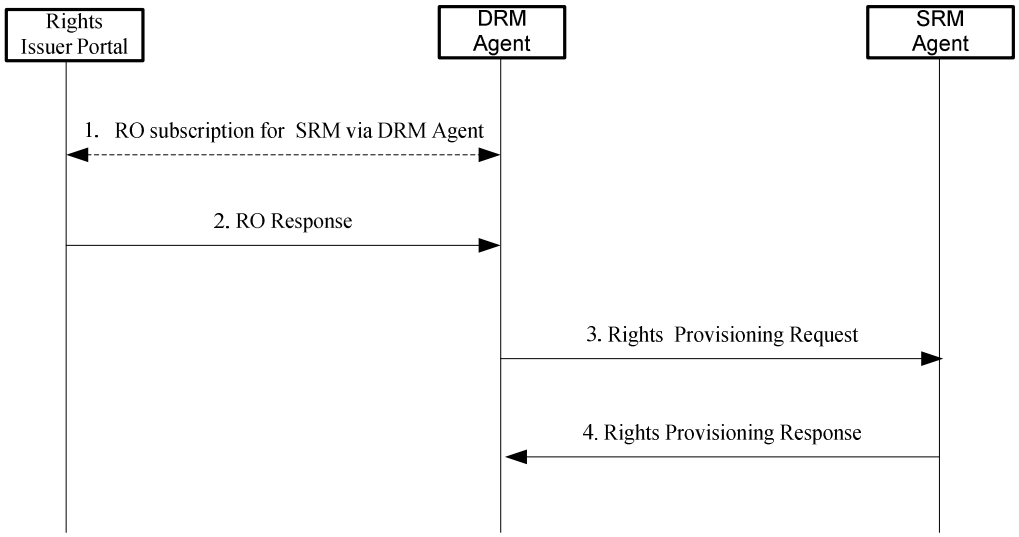

Figure 7: Sequence Diagram – Direct Provisioning of Rights to SRM on Push Model

B.5 SRM to SRM Move

This technical use case describes the case when Rights is moved from a SRM to another SRM.

Action:

1. The DRM Agent accesses the SRM-1.
2. The DRM Agent select Rights and requests the SRM Agent to move that selected Rights to another SRM Agent in SRM-2.
3. SRM Agent in SRM-1 sets the selected Rights as disabled.

© 2010 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. SRM Agent sends the RO and its associated state information to DRM Agent. (Refer to "rights retrieval" procedure from SRM1.0)
5. DRM Agent subtracted the move count in the state information by 1 and sends the updated state information and the RO to SRM Agent in SRM-2. (Refer to "rights removal" procedure from SRM1.0)
6. SRM Agent in SRM-2 installs received rights.
7. SRM Agent in SRM-2 sends result of installation to DRM Agent.
8. DRM Agent requests SRM Agent in SRM-1 to do the End Process. (Refer to "rights removal" procedure from SRM1.0)
9. SRM Agent in SRM-1 does the end process. If the right has been successfully installed in SRM-2, than rights is deleted from SRM-1, else rights is re-enabled. (Refer to "rights removal" procedure from SRM1.0)

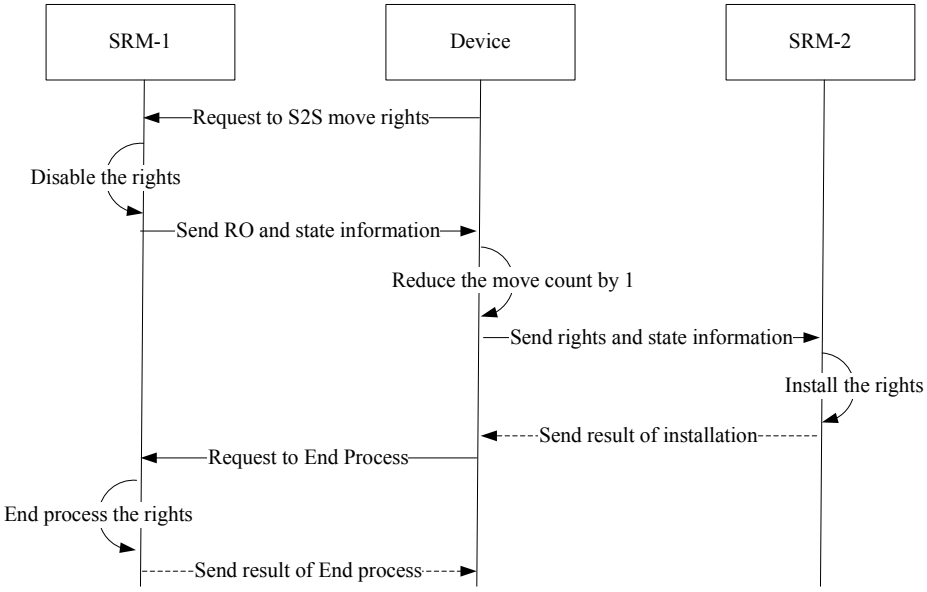

Figure 8: Sequence Diagram – SRM to SRM Move

B.6 SRM Rights upgrade

This technical use case describes the case that existing rights in SRM is upgraded.

The basic flow is as follows:

1. The DRM Agent accesses the SRM（Not shown in this diagram）.
2. The DRM Agent selects Rights and requests the SRM Agent to upgrade that existing Rights selected.
3. SRM Agent sets the selected Rights as disabled.
4. SRM Agent sends the existing Rights (including the associated state information) to DRM Agent.
5. DRM Agent sends the existing Rights information (e.g. RO and its associated state information) to RI and requests for the upgraded Rights. Note: this step is out of SRM's scope.
6. RI sends the upgraded Rights to DRM Agent. Note: this step is out of SRM's scope.
7. DRM Agent sends the upgraded Rights to SRM Agent.
8. SRM Agent upgrades the existing Rights with the upgraded Rights.

© 2010 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.

9. SRM Agent sends the result of the upgrade process to DRM Agent.

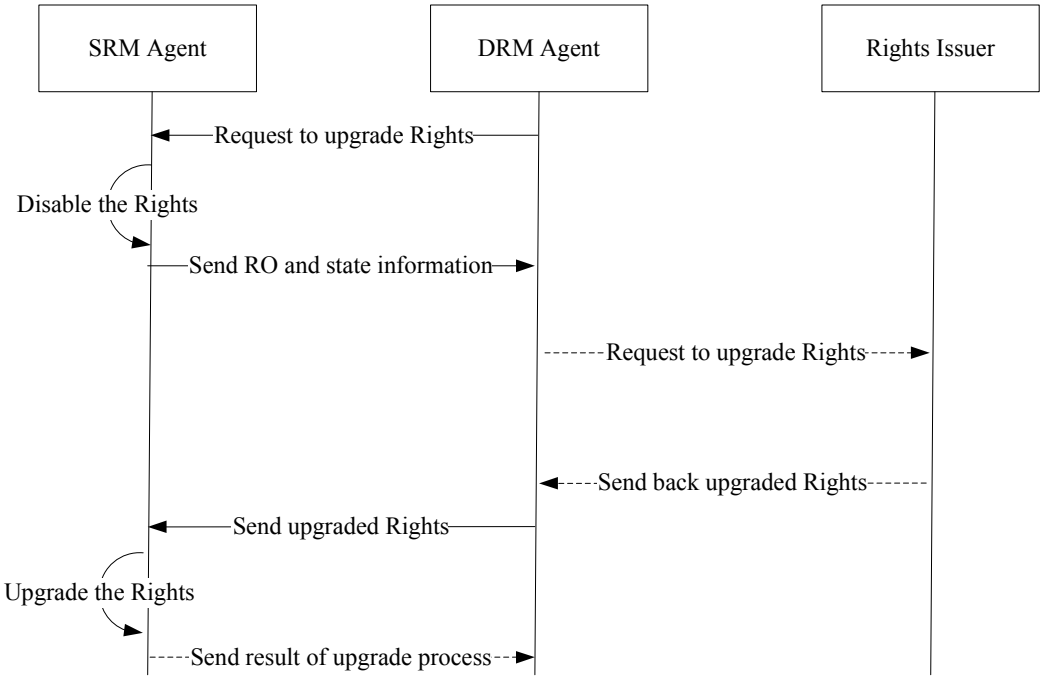

Figure 9: Sequence Diagram – SRM Rights upgrade

B.7 SRM extensions for BCAST service support

B.7.1 Consumption of service requiring presence of SRM

The following flow implements the use case when service consumption is not allowed by the DRM Agent if SRM containing necessary Rights is not present in the Device. Although a copy of the Rights is stored by the DRM Agent, physical presence of the SRM card in the Device is required.

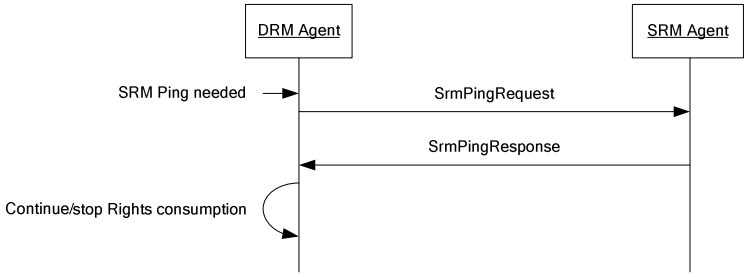

Figure 10: Sequence Diagram - Consumption of Rights Requiring Presence of SRM

Action flow:

© 2010 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.

1. The Device performs Rights Consumption of the Rights bound to particular SRM (not shown in the diagram).
2. While consuming the Rights, the DRM Agent has to check for the presence of the SRM.
3. The DRM Agent sends an SRM Ping request to the SRM Agent challenging it to provide a proper response.
4. The SRM Agent responds with an SRM Ping response, providing an acknowledgement which needs to be properly authenticated and contains all necessary information requested by the DRM Agent.

   Note: DRM Agent and SRM Agent need to perform mutual authentication in case they do not share any active security association prior to initiating presence checking procedure.

5. If the DRM Agent receives and successfully validates a response from the SRM Agent, it can continue to consume the Rights. Otherwise, it stops consuming the Rights.

Note that this example will be an optional feature of SRM 1.1 Enabler, and it is up to the implementer to use another vendor-specific presence checking solution.

B.7.2 Broadcast RO Move from Device to SRM

The following flow represents the use case when Broadcast Right Object (BCRO) is moved to SRM from Device.

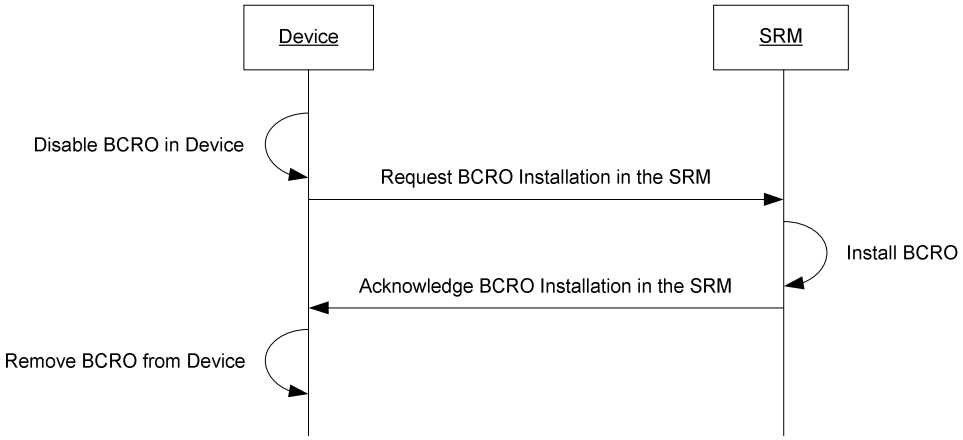

Figure 11: Sequence Diagram – BCRO Move from Device to SRM

Action flow:

1. The DRM Agent disables BCRO in the Device.
2. The DRM Agent requests the SRM Agent to install BCRO in the SRM.
3. The SRM Agent installs BCRO in the SRM.
4. The SRM Agent acknowledges BCRO installation in the SRM.
5. The DRM Agent removes disabled BCRO from the Device.

Note that Rights Move from Device to SRM procedures and messages in SRM 1.0 can be reused for this procedure.

B.7.3 Broadcast RO Move from SRM to Device

The following flow represents the use case when Broadcast Right Object (BCRO) is moved to SRM from Device.

© 2010 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.

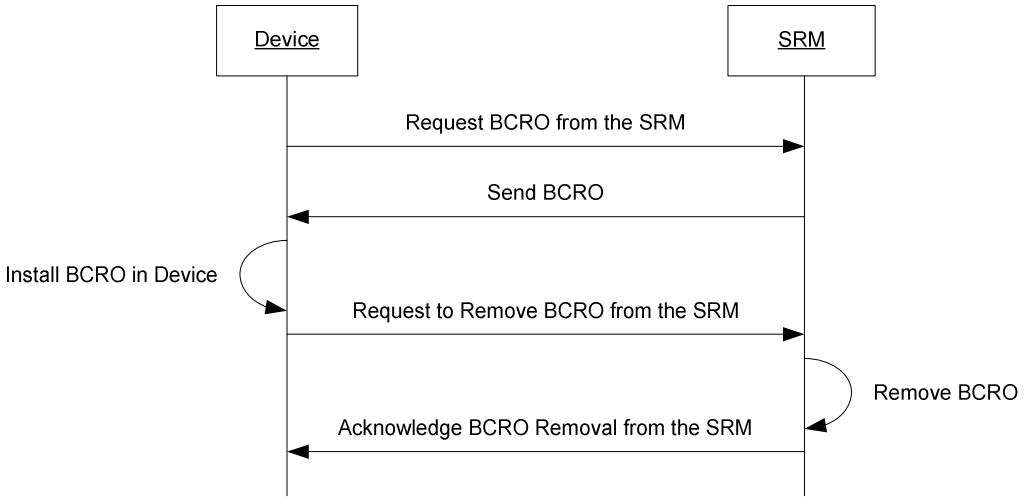

Figure 12: Sequence Diagram – BCRO Move from SRM to Device

Action flow:

1. The DRM Agent sends a request to the SRM Agent to acquire BCRO from the SRM.
2. The SRM Agent replies with the message containing BCRO.
3. The DRM Agent installs BCRO in the Device.
4. The DRM Agent requests the SRM Agent to remove BCRO from the SRM.
5. The SRM Agent removes BCRO from the SRM.
6. The SRM Agent sends acknowledgement of BCRO removal to the DRM Agent.

Note that Rights Move from SRM to Device procedures and messages in SRM 1.0 can be reused for this procedure.

B.7.4 Token Management

Token is a credit which can be exchanged for temporary access to a service as defined in [SRM-RDv1.1]. In scope of this specification, definition of token is extended to include a set of parameters governing the usage of associated amount of credits, and it is further referred as *Token*.

Tokens can be acquired by a Device from the Rights Issuer using Token Request Protocol as defined in [DRMXBS], or installed in SRM at the time of SRM manufacturing. Note that, Token provisioning is out of scope of SRM enabler. Acquired or pre-provisioned Tokens are then used by Device for Rights consumption and can be transferred between multiple Devices using SRM card.

Informational note 1: OMA DRM V2.0 Extensions for Broadcast Support specification [DRMXBS] defines additions to the OMA DRM 2.0 REL to accommodate management of tokens. A Device can receive tokens from multiple RIs and use them to consume DRM content whose usage is defined as token-based in the RO associated with the DRM content. In particular, this RO will contain <token-based> element which specifies what kind of stateful consumption will be governed by token availability.

Informational note 2: Token management is not applicable in case of broadcast-only Devices (see [DRMXBS]).

© 2010 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.

B.7.4.1 Token Move from Device to SRM

The following flow shows an example of Token move from Device to SRM.

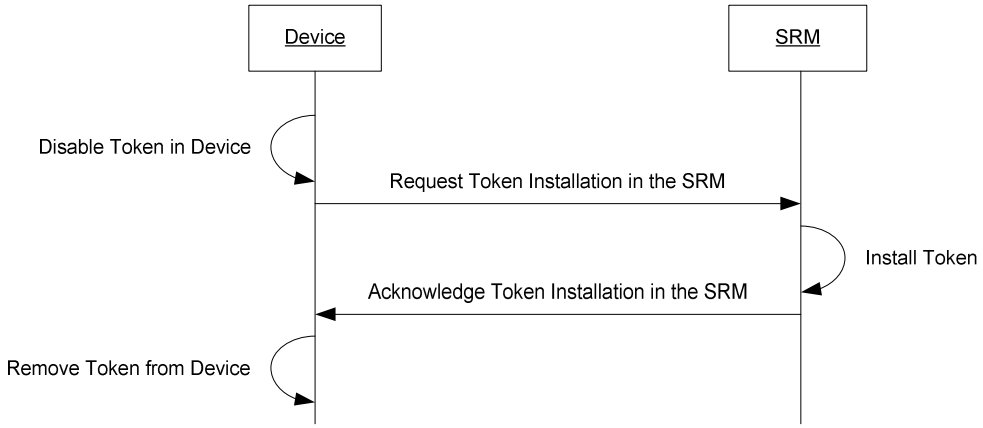

Figure 13: Sequence Diagram – Token Move from Device to SRM

Action flow:

1. The DRM Agent disables Token in the Device.
2. The DRM Agent requests the SRM Agent to install Token in the SRM.
3. The SRM Agent installs received Token in the SRM.
4. The SRM Agent sends Token installation acknowledgement to the DRM Agent.
5. The DRM Agent removes disabled Token from the Device.

B.7.4.2 Token Move from SRM to Device

The following flow shows an example of Token move from SRM to Device.

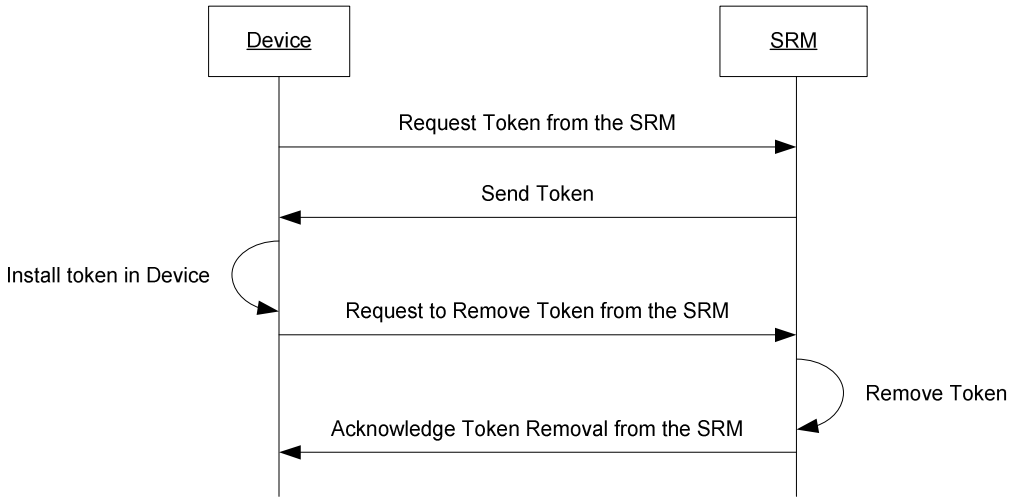

Figure 14: Sequence Diagram – Token Move from SRM to Device

Action flow:

© 2010 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.

1. The DRM Agent sends a request to the SRM Agent to acquire Token from the SRM.
2. The SRM Agent replies with the message containing Token and Token related information.
3. The DRM Agent installs Token in the Device.
4. The DRM Agent requests the SRM Agent to remove Token from the SRM.
5. The SRM Agent removes Token from the SRM.
6. The SRM Agent sends acknowledgement of Token removal to the DRM Agent.

B.7.4.3 Local Token Consumption by the Device

The following flow shows an example of Token consumption by the Device while Tokens are stored at SRM.

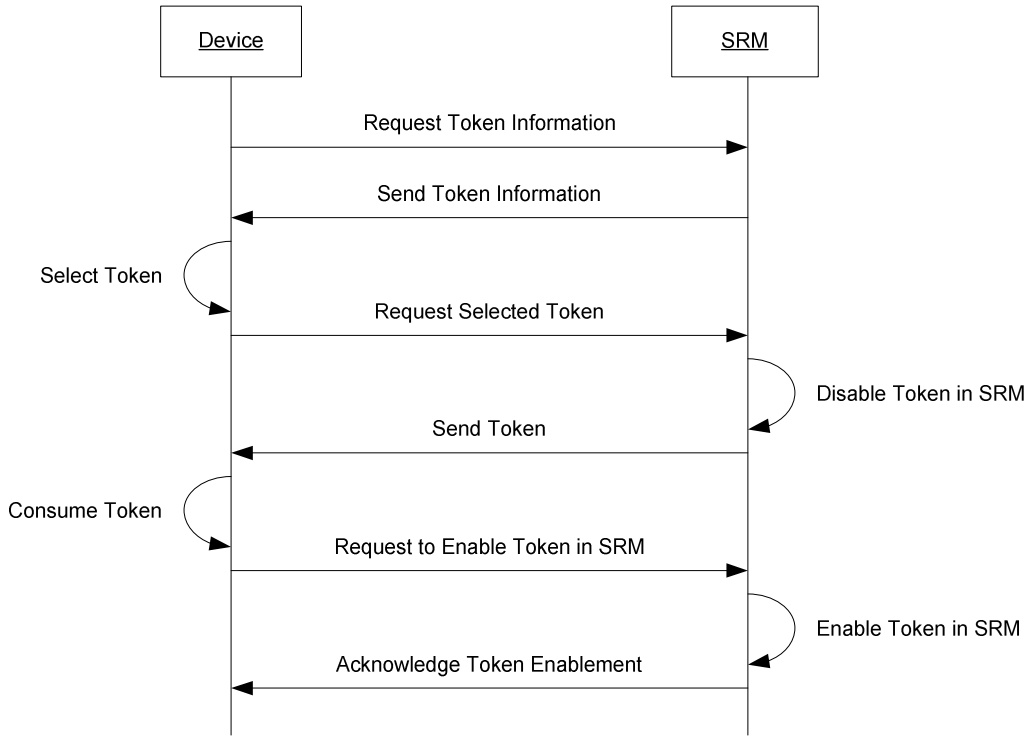

Figure 15: Sequence Diagram – Local Token Consumption

Action flow:

1. The DRM Agent acquires information about Tokens stored on SRM (e.g. list of Token identifiers, amount of available credits, etc.) from the SRM Agent.
2. The SRM Agent sends this information to the DRM Agent.
3. The DRM Agents selects Tokens for consumption.
4. The DRM Agent requests Tokens for consumption from the SRM Agent.
5. The SRM Agent disables Tokens in SRM.
6. The SRM Agent sends Tokens to the DRM Agent.
7. Tokens are then consumed on the Device.
8. When consumption is stopped, the DRM Agent requests the SRM Agent to enable Tokens in SRM. The request includes Token status information (e.g. remaining amount of credits).

© 2010 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.

9. The SRM Agent enables Tokens.
10. The SRM Agent sends a response to the DRM Agent to acknowledge Token enablement.

© 2010 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.