OMA Secure Removable Media Requirements

Candidate Version 1.0 – 10 Oct 2006

Open Mobile Alliance

OMA-RD-SRM-V1_0-20061010-C

Contents

1. SCOPE (INFORMATIVE) ... 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 ... 8
3.3 ABBREVIATIONS ... 9

4. INTRODUCTION (INFORMATIVE) ... 10

5. USE CASES (INFORMATIVE) ... 11

5.1 USE CASES OVERVIEW ... 11
5.1.1 Actors ... 11
5.2 SCENARIO 1: UPGRADE FROM OLD DEVICES TO NEW DEVICES BY USING THE SECURE REMOVABLE MEDIA ... 12
5.2.1 Short Description ... 12
5.2.2 Actors ... 12
5.2.3 Pre-conditions ... 12
5.2.4 Post-conditions ... 13
5.2.5 Normal Flow ... 13
5.2.6 Alternate flow ... 13
5.3 SCENARIO 2: PROVISIONING OF RIGHTS OBJECT IN THE SMART CARD ... 13
5.3.1 Short Description ... 13
5.3.2 Actors ... 13
5.3.3 Pre-conditions ... 14
5.3.4 Post-conditions ... 14
5.3.5 Normal Flow ... 14
5.3.6 Alternate flow ... 14
5.4 SCENARIO 3: USING CONTENTS IN MULTIPLE DEVICES BY USING THE SECURE REMOVABLE MEDIA ... 14
5.4.1 Short Description ... 14
5.4.2 Actors ... 14
5.4.3 Pre-conditions ... 15
5.4.4 Post-conditions ... 15
5.4.5 Normal Flow ... 15
5.4.6 Alternate flow ... 16
5.5 SCENARIO 4: TRANSFER CONTENTS AND RIGHTS OBJECTS AMONG OMA CONFORMANT DEVICES BY USING THE SECURE REMOVABLE MEDIA ... 16
5.5.1 Short Description ... 16
5.5.2 Actors ... 16
5.5.3 Pre-conditions ... 16
5.5.4 Post-conditions ... 16
5.5.5 Normal Flow ... 16
5.5.6 Alternate flow ... 17
5.6 SCENARIO 5: DIRECT RENDERING OF DRM CONTENTS BY USING THE SECURE REMOVABLE MEDIA ... 17
5.6.1 Short Description ... 17
5.6.2 Actors ... 17
5.6.3 Pre-conditions ... 17
5.6.4 Post-conditions ... 17
5.6.5 Normal Flow ... 17
5.6.6 Alternate flow ... 17
5.7 SCENARIO 6: BACKUP OF RIGHTS OBJECT IN THE SMART CARD ... 18
5.7.1 Short Description ... 18
5.7.2 Actors ... 18

5.7.3 Pre-conditions ... 18
5.7.4 Post-conditions ... 18
5.7.5 Nomal Flow ... 18
5.7.6 Alternate flow ... 19
5.8 SCENARIO7: PRE-LOADING OF RIGHTS OBJECTS BY USING THE SMART CARD ... 19
5.8.1 Short Description ... 19
5.8.2 Actors ... 19
5.8.3 Pre-conditions ... 19
5.8.4 Post-conditions ... 19
5.8.5 Normal Flow ... 19
5.8.6 Alternate flow ... 20
6. REQUIREMENTS (NORMATIVE) ... 21
6.1 HIGH-LEVEL FUNCTIONAL REQUIREMENTS ... 21
6.1.1 Security ... 22
6.1.2 Interoperability ... 22
APPENDIX A. CHANGE HISTORY (INFORMATIVE) ... 23
A.1 APPROVED VERSION HISTORY ... 23
A.2 DRAFT/CANDIDATE VERSION 1.0 HISTORY ... 23

Figures

Error! No table of figures entries found.

Tables

Table 1: High-Level Functional Requirements ... 21

Table 2: High-Level Functional Requirements – Security Items ... 22

Table 3: High-Level Functional Requirements – Interoperability Items ... 22

1. Scope (Informative)

Open Mobile Alliance (OMA) specifications are the result of continuous work to define industry-wide interoperable mechanisms for developing applications and services that are deployed over wireless communication networks.

The scope of OMA “Digital Rights Management” (DRM) is to enable the distribution and consumption of digital content in a controlled manner. The content is distributed and consumed on authenticated Devices per the usage rights expressed by the content owners.

This specification defines the requirement for the OMA DRM based Secure Removable Media to extend the OMA DRM 2.0 to enable the use of OMA DRM based Secure Removable Media.

OMA DRM with Secure Removable Media enables the protection and consumption of digital content and its usage rights in Secure Removable Media in a secure manner. This specification is not stand-alone; it must be interpreted in the context of the existing OMA DRM v2.0 suite of specifications.

2. References

2.1 Normative References

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

[OMADRMv2] OMA DRM v2 enabler, Open Mobile Alliance, http://www.openmobilealliance.org

2.2 Informative References

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].

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

3.2 Definitions

Backup
Defines an action for duplicating a Media Object and/or Rights Object and transferring them to another location that is not a Device.

Billing Service Provider
The entity responsible for collecting payment from a User.

Composite Object
A Media Object that contains one or more Media Objects by means of inclusion e.g. DRM messages, zip files.

Consume
To Play, Display, Print or Execute DRM Content on a Device.

Content
One or more Media Objects

Constraint
A restriction on the Permission over DRM Content

Content Issuer
The entity making content available to the DRM Agent; the entity whose Content is being Protected.

Content Provider
An entity that is either a Content Issuer or a Rights Issuer.

Copy
To make a perfect reproduction of DRM Content or a Rights Object, or to make Rights existing on a source Device or SRM available for use by a recipient Device or SRM, without affecting availability on the source Device or SRM. Rights may be restricted on the recipient Device or SRM.

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.

Direct Rendering
Operations in which Rights stored in SRMs are transferred for use by the recipient Device for a limited period of time for rendering purposes.

DRM Agent
The entity in the Device that manages Permissions for Media Objects on the Device.

DRM Content
Media Objects that are consumed according to a set of Permissions in a Rights Object.

Enable
To make a resource (Media Object) capable of being interacted with. When applied to a digital resource, Enable results in a change in an existing resource such that it becomes capable of being read, written to or executed. Enabling MAY be partial and/or contextual. (From [MPEG21 RDD])

Execute
To execute a software programme

Media Object
A digital work e.g. a ringing tone, a screen saver, a Java game or a Composite Objec*t*.

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.

Network Service Provider
The entity providing network connectivity for a mobile Device.

OMA DRM Conformant Device
A Device that will work interoperably with other OMA DRM Conformant Devices and some or all of the following; Billing Service Providers, Content Providers and Network Service Providers. It will also enable DRM Content on the Device only if the Device possesses a valid Rights Object (or implied Rights Object) for that instance of DRM Content and only according to the Permissions defined in the Rights Object for that instance of DRM Content.

Permission
Actual usages or activities allowed (by the Rights Issuer) over DRM Content.

Play
To create a transient, perceivable rendition of a resource (From [MPEG21 RDD])

Restore
Transferring the Protected Content and/or Rights Objects from an external location back to the Device from which they were backed up.

Rights
Rights are the collection of permissions and constraints defining under which circumstances access is granted to DRM Content.

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 DRM Content.

Secure Memory Card A portable tamper resistant Device with an embedded microprocessor chip and a secure storage area. A Secure Memory Card is used for securely storing data (e.g. contents, rights etc.) and for performing security related operations like encryption and authentication.

Secure Removable Media A removable media that implements means to protect against unauthorized access to its internal

Data and includes a SRM Agent (e.g. Secure Memory Card, Smart Card)

Smart Card A portable tamper resistant Device with an embedded microprocessor chip and a secure storage area. A Smart Card is used for securely storing data (e.g. access codes, user subscription information, secret keys, contents, rights etc.) and performing security related operations like encryption and authentication. A Smart Card may contain one or more network authentication applications like the SIM, USIM, R-UIM.

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.

Stateless Rights Stateless Rights are Rights Objects for which the Device does not have to maintain state information.

Stateful Rights Stateful Rights are Rights Objects for which the Device has to explicitly maintain state information, so that the constraints and permissions expressed in the RO can be enforced correctly. An RO containing any of the following constraints is considered Stateful Rights: <interval>, <count>, <timed-count>, or <accumulated>. Additionally an RO with <export> permission and mode attribute of "move" is Stateful Rights.

User The human user of a Device. The User does not necessarily own the Device.

3.3 Abbreviations

DRM	Digital Rights Management
ISO	International Standards Organisation
MMC	Multi Media Card
MPEG	Moving Picture Expert Group
MP3	MPEG audio layer 3; coding scheme for audio compression
OMA	Open Mobile Alliance
PC	Personal Computer
ROAP	Rights Object Acquisition Protocol
RUIM	Removable User Identity Module
SD	Secure Digital
SIM	Subscriber Identity Module
SRM	Secure Removable Media
UFD	USB Flash Drive
USIM	Universal Subscriber Identity Module

4. Introduction (Informative)

Digital Rights Management (DRM) with Secure Removable Media (SRM) enables to use SRMs to store and distribute DRM Contents and Rights Objects in a secure manner. Note: Some Secure Removable Media may not support storage of DRM Contents. OMA Digital Rights Management 2.0 [OMA DRM 2.0] defines mechanisms to deliver DRM Contents and Rights Objects to consuming Devices. To extend the existing mechanisms, this specification defines requirements to deliver Rights Objects between a consuming Device and SRM and to consume Rights Objects as being stored in SRM. Secure Removable Media includes the removable media such as MMC, Smart Card, SD, and UFD.

As defined above, the Secure Removable Media (SRM) is a portable Device containing a SRM Agent and a secure storage area protected against unauthorized reading, writing.

Examples of SRM Devices may be:

- **Secure Memory Card**
- **Smart Card**

This requirements specification document builds on the work in OMA DRM 2.0 specifications and in total provides:

- The scenarios that we wish to enable with SRM (section 5)
- The high level market requirements derived from the scenarios (section 6)
- The security requirements applying to the technical solution (section 6.1.1)

5. Use Cases (Informative)

This section is intended to describe in the form of user scenarios the types of services which customers will require when they come to use OMA DRM based Secure Removable Media. The scenarios are based upon a teenager although many of the principles will apply to older users and potentially to younger ones as well.

Simply, the purpose of this section is:

- To provide a better understanding of the functionality that the OMA DRM based Secure Removable Media should provide.
- To be a public document that can help to explain what OMA SRM Document Package provides.

5.1 Use Cases overview

Alice is an active teenager in 2006. She is an active user of mobile Devices and enjoys the multimedia services on her mobile phone and also at her home entertainment systems such as home theatre and PC. She uses Secure Removable Media in her mobile phone since the embedded memory at her mobile phone is not large enough to store all of her multimedia Contents and Rights Objects. Secure Removable Media is her number 1 choice to carry the data since Secure Removable Media provides easy and secure data transfer and storage.

Scenario 1: Easy upgrade and transfer of Contents and/or Rights Objects by using SRM

Alice would like to transfer her digital music collection from her old Device to the new one using Secure Removable Media (Secure Memory Card, Smart Card).

Scenario 2: Easy Transfer of existing Rights Objects by using Smart Card

Alice upgrades her mobile phone that does not have a Secure Memory Card. She would like to transfer her rights from her old phone to the new one using her Smart Card.

Scenario 3: Sharing Contents among friends by using SRM

Bob would like to borrow some mp3 files from Alice for his party on Saturday.

Scenario 4: Using Contents among Devices by using SRM

Chris has acquired content on his PC and would like to transfer it to his Device.

Scenario 5: Direct Rendering Contents by using SRM

Deborah would like to watch an OMA DRM protected movie that’s stored on her Secure Removable Media on her friend’s big plasma-screen.

Scenario 6: Backup of Smart Card Rights Objects

Alice will be allowed to select which Rights Objects to keep in the Smart Card and which to extract, while doing the Backup, in order to free some space for new Rights Objects.

Scenario 7: Pre-loaded Rights Objects into the Smart Card

A mobile network operator is using the Smart Card to pre-load Rights Objects that will be bound to exclusive DRM Contents (ringtones, games, wallpapers …) when a user is subscribing to new services and got a new Smart Card.

5.1.1 Actors

The following entities will be introduced:

- SRM Agent

  See definition in the section 3.2.

- DRM Agent (from [OMADRMv2])

  A DRM Agent embodies a trusted entity in a Device. This entity is responsible for enforcing permissions and constraints associated with DRM Contents, controlling access to DRM Contents, etc. In this specification, the DRM Agent is also responsible for enforcing permissions and constraints of Rights Objects in Secure Removable Media by interfacing with SRM Agent.
- Rights Issuer (from [OMADRMv2])

  The rights issuer is an entity that assigns permissions and constraints to DRM Contents, and generates Rights Objects. A Rights Object is an XML document expressing permissions and constraints associated with a piece of DRM Contents. Rights Objects govern how DRM Contents 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 Object can also govern how the Rights Object itself is moved from a DRM Agent to a SRM Agent and vice versa.
- Content Issuer (from [OMADRMv2])

  The content issuer is an entity that delivers DRM Content. OMA DRM defines the format of DRM Content delivered to DRM Agents, and the way DRM Content can be transported from a content issuer to a DRM Agent using different transport mechanisms. The content issuer may do the actual packaging of DRM Content itself, or it may receive pre-packaged content form other source. The DRM Content can be delivered to Secure Removable Media also.
- User (based on [OMADRMv2])

  A user is the human user of DRM Content. Users can only access DRM Content though a DRM Agent. Users can choose Secure Removable Media as a secondary storage of their Devices and enable the flexibility of moving and consuming of DRM Content or Rights Objects in other Devices.

5.2 Scenario 1: Upgrade from old Devices to new Devices by using the Secure Removable Media

5.2.1 Short Description

Alice has collected various music files and music video clips since she had purchased her old . She buys a new mobile phone and would like to transfer her digital music collection from her old phone to the new one using Secure Removable Media.

Once she has done this, Alice can enjoy her digital music collection on her new mobile phone.

5.2.2 Actors

DRM Agent	See actors in the section 5.1.1
SRM Agent	See actors in the section 5.1.1
User	See actors in the section 5.1.1

5.2.2.1 Actor Specific Issues

The DRM Agent and the SRM Agent interact with each other to transfer DRM Contents and Rights Objects.

5.2.2.2 Actor Specific Benefits

It is possible for a user to Consume previously acquired DRM Contents and Rights Objects on the User's new Device using the Secure Removable Media.

5.2.3 Pre-conditions

The User has acquired various DRM Contents and Rights Objects, these are installed on the User's old Device.

The User's old Device and User's new Device support Secure Removable Media.

5.2.4 Post-conditions

DRM Contents and Rights Objects can be Consumed on the User's new Device.
The user can't access its DRM Contents on its old phone anymore.

5.2.5 Normal Flow

1. The User has purchased and downloaded DRM Content that is stored in the User's old Device, the associated Rights Objects are installed on User's old Device. The User's old Device supports Secure Removable Media.
2. User has purchased new Device embedding a DRM Agent with SRM Agent support.
3. The DRM Content stored on the old Device is transferred from the User's old Device to the Secure Removable Media.
4. The DRM Agent on the User's old Device transfers Rights Objects to the SRM Agent only after the successful mutual authentication between DRM Agent and SRM Agent.
5. The DRM Content stored on the Secure Removable Media is transferred from the Secure Removable Media to the User's new Device.
6. The SRM Agent transfers Rights Objects to the user's new Device only after the successful mutual authentication between DRM Agent and SRM Agent.
7. The User can Consume the transferred DRM Content according to the specified Rights in the Rights Objects.

5.2.6 Alternate flow

If there are no remaining Rights or the Rights have expired for the transferred DRM Content, the User can not Consume DRM Content which was transferred from the user's old Device.

If the mutual authentication is failed, the transfer of Rights Objects SHALL be prevented.

5.3 Scenario 2: Provisioning of Rights Object in the Smart Card

5.3.1 Short Description

Alice owns a state of the art mobile phone and is a faithful subscriber enjoying the multitude of services that her Network Service Provider offers. Alice wants to use the advanced features of her mobile phone but is reluctant to learn complicated technical topics. She wants a service that allows her to download music, and the associated Rights, in a seamless manner. In fact, Alice does not know what Rights Objects are and does not want to know how to “move” these “Rights Objects”. She wants to surf to her Network Service Provider's portal, choose the music that she likes, download it, pay for the transaction and then just use it with the minimum of ease.

Alice accepts that her Smart Card, which includes all her telecom account details, can be used to store Rights . Alice acquires a new mobile phone and wants to have her existing Rights transferred to the new mobile phone along with her account details. She just wants to be able to plug her Smart Card in her mobile phone, or any new mobile phone in the future, and immediately be able to Consume the music for which she has acquired the Rights.

5.3.2 Actors

DRM Agent	See actors in the section 5.1.1
SRM Agent	See actors in the section 5.1.1
User	See actors in the section 5.1.1

5.3.2.1 Actor Specific Issues

The DRM Agent and the SRM Agent interact with each other to transfer Rights Objects.

5.3.2.2 Actor Specific Benefits

The User can purchase DRM Content, along with the associated Rights Objects, and know that she can use this DRM Content as long as her Smart Card is plugged in her mobile phone. When she wants to change to a new or different mobile phone she just needs to plug her Smart Card in the new mobile phone.

5.3.3 Pre-conditions

The User has acquired various DRM Contents and Rights Objects using her mobile phone.

5.3.4 Post-conditions

DRM Content is delivered to the OMA conformant mobile phone while the Rights Objects are delivered directly to her Smart Card that is plugged in the mobile phone.

5.3.5 Normal Flow

1. The User has purchased and downloaded DRM Content using her mobile phone that contains a Smart Card (e.g. SIM with SRM Agent embedded)

2. The downloaded Rights Objects are installed directly in the user's Smart Card or are seamlessly transferred by the mobile phone DRM Agent, only after successful mutual authentication between DRM Agent and SRM Agent, to the Smart Card.

3. The User can Consume the acquired DRM Content according to the specified Rights in the Rights Objects installed in her Smart Card.

5.3.6 Alternate flow

If there are no remaining Rights or Rights have expired for the DRM Content on the Smart Card, the User cannot Consume the corresponding DRM Content.

If mutual authentication has failed the Consumption of DRM Content SHALL be prevented.

5.4 Scenario 3: Using Contents in Multiple Devices by using the Secure Removable Media

5.4.1 Short Description

Alice has music files in the form of DRM Content on her Device. David would like to borrow these music files from Alice for his party on weekend.

The DRM Content can be Consumed immediately on the other OMA DRM conformant Devices using the Secure Removable Media when the Permissions to do so are included in the associated Rights Object.

5.4.2 Actors

DRM Agent	See actors in the section 5.1.1
SRM Agent	See actors in the section 5.1.1
User	See actors in the section 5.1.1

5.4.2.1 Actor Specific Issues

The DRM Agent and the SRM Agent interact with each other to transfer DRM Contents and Rights Objects.

5.4.2.2 Actor Specific Benefits

It is possible for a User to allow a friend to use their DRM Contents by using the Secure Removable Media.

5.4.3 Pre-conditions

The User has acquired various DRM Content that is stored on the User's Device, the associated Rights Objects are installed in the User's Device. The User has transferred the Rights Objects and DRM Contents to the Secure Removable Media to allow their friends to borrow the DRM Contents.

The User's Device and the User's friend's Device support Secure Removable Media and both Devices are OMA DRM conformant.

5.4.4 Post-conditions

DRM Contents can be Consumed on the friend's Device.

5.4.5 Normal Flow

Up-to 4th step, case 1 and case 2 has the same flow. After the 4th step, the DRM Contents and Rights Objects are stored/installed on the Secure Removable Media. Case 1 and case 2 differ in how the DRM Contents and Rights Objects are Consumed.

Case 1:

1. The User has purchased and downloaded DRM Content that is stored in the User's Devicen the associated Rights Objects are installed in User's Device which supports the Secure Removable Media.
2. The DRM Content is transferred from the User's Device to the User's Secure Removable Media.
3. The DRM Agent on the User's device transfers the Rights Objects to the User's SRM Agent only after the successful mutual authentication between DRM Agent and SRM Agent.
4. The User's friend borrows the User's Secure Removable Media.
5. The DRM Contents are transferred from the Secure Removable Media to the User's friend's Device.
6. The SRM Agent transfers Rights Objects to the User's friend's DRM Agent only after the successful mutual authentication between DRM Agent and SRM Agent.
7. The User's friend can Consume the DRM Content on the Secure Removable Media according to the Rigths specified in the Rights Objects which are installed on the User's Secure Removable Media.

Case 2:

1. The User has purchased and downloaded DRM Content that is stored in the User's Device, the associated Rights Objects are installed in the User's Device which supports the Secure Removable Media.
2. The DRM Content is transferred from the User's Device to the User's Secure Removable Media.
3. The DRM Agent on the User's Device transfers the Rights Objects to the SRM Agent only after the successful mutual authentication between DRM Agent and SRM Agent.
4. The User's friend borrows the User's Secure Removable Media.
5. The SRM Agent allows DRM Content to be rendered immediately by the User's friend's Device only after the successful mutual authentication between DRM Agent and SRM Agent.
6. The User's friend can Consume the DRM Contents on the Secure Removable Media according to the Rights specified in Rights Objects which are installed on the User's Secure Removable Media.

5.4.6 Alternate flow

If there are no remaining Rights or Rights have expired for the DRM Content on the Secure Removable Media, the User's friend can not Consume the corresponding DRM Content.

If the mutual authentication between the User's SRM Agent and the friend's DRM Agent fails, the User's friend can not Consume the DRM Contents which are stored on the User's Secure Removable Media.

5.5 Scenario 4: Transfer Contents and Rights Objects among OMA Conformant Devices by using the Secure Removable Media

5.5.1 Short Description

Alice has acquired DRM Content and Rights Objects on her PC and would like to transfer them to her Device using the Secure Removable Media.

5.5.2 Actors

DRM Agent	See actors in the section 5.1.1
SRM Agent	See actors in the section 5.1.1
User	See actors in the section 5.1.1

5.5.2.1 Actor Specific Issues

The DRM Agent and the SRM Agent interact to each other to transfer DRM Contents and Rights Objects.

5.5.2.2 Actor Specific Benefits

It is possible for the User to Consume purchased DRM Contents on any OMA conformant Device using the Secure Removable Media.

5.5.3 Pre-conditions

The User has acquired various DRM Content that is stored on the User's PC, the associated Rights Objects are installed in the User's PC.

The User's Device and PC support the Secure Removable Media and both Devices are OMA DRM conformant.

5.5.4 Post-conditions

The DRM Contents can be Consumed on the User's Devices.

5.5.5 Normal Flow

1. The User has purchased and downloaded DRM Content that is stored in the User's PC, the associated Rights Objects are installed in User's PC. The User's PC supports Secure Removable Media..

2. The DRM Contents are transferred from the User's PC to the Secure Removable Media.

3. The DRM Agent on the User's PC transfers Rights Objects to the SRM Agent only after the successful mutual authentication between DRM Agent and SRM Agent.

4. The DRM Contents are transferred from the Secure Removable Media to the User's Device.

5. The SRM Agent transfers Rights Objects to the User's DRM Agent only after the successful mutual authentication between DRM Agent and SRM Agent.

6. The User can Consume the transferred DRM Content according to the Rights specified in the transferred Rights Objects.

5.5.6 Alternate flow

If there are no remaining Rights or the Rights have expired for the DRM Content on the Secure Removable Media, the User can not Consume the corresponding DRM Content.

If the mutual authentication is failed, the transfer of Rights Objects SHALL be prevented.

5.6 Scenario 5: Direct Rendering of DRM Contents by using the Secure Removable Media

5.6.1 Short Description

Alice would like to view a movie that's stored on her Secure Removable Media (in the form of DRM Content) on her friend's big plasma-screen.

5.6.2 Actors

DRM Agent	See actors in the section 5.1.1
SRM Agent	See actors in the section 5.1.1
User	See actors in the section 5.1.1

5.6.2.1 Actor Specific Issues

The DRM Agent and the SRM Agent interact to each other to enable the User to Consume the DRM Contents directly on User's friend's rendering Device.

5.6.2.2 Actor Specific Benefits

It is possible for the User to Consume the purchased DRM Contents on other OMA conformant rendering Devices using the Secure Removable Media.

5.6.3 Pre-conditions

The User has acquired various DRM Contents that are stored on the User's Secure Removable Media, the associated Rights Objects are installed on the to the User's Secure Removable Media.

The User's friend's Device that will render has transferred DRM Contents and Rights Objects to the secure removable media.

5.6.4 Post-conditions

OMA DRM conformant rendering Devices can render the DRM Contents which is stored on the Secure Removable Media.

5.6.5 Normal Flow

1. The SRM Agent allows DRM Contents to be Consumed immediately by other OMA DRM conformant rendering Devices only after the successful authentication between DRM Agent and SRM Agent.

5.6.6 Alternate flow

If there are no remaining Rights or Rights have expired for the DRM Content on the Secure Removable Media, the User can not Consume the corresponding DRM Content.

If the authentication between the Secure Removable Media and the rendering Device fails, the DRM Content can not be Consumed by the rendering Device.

5.7 Scenario 6: Backup of Rights Object in the Smart Card

5.7.1 Short Description

Alice owns a state of the art mobile phone and is a faithful subscriber enjoying the multitude of service that her Network Service Provider offers. Alice has purchased DRM content and the associated Rights Objects are installed in her Smart Card. She has subscribed to an operator's a service that allows her to Backup her Rights Object automatically with just a press of a key.

Alice accepts that her Smart Card can be used to hold her music Rights Object because it already contains all her telecom account details. She will never use a "move" operation of these Rights Objects but she wants to be able to Backup them in the case that she looses her mobile phone. The Backup operation will allow her to choose which Rights Objects to keep in the Smart Card and which to extract, while doing the Backup, in order to free some space for new Rights Objects.

5.7.2 Actors

DRM Agent	See actors in the section 5.1.1
SRM Agent	See actors in the section 5.1.1
User	See actors in the section 5.1.1

5.7.2.1 Actor Specific Issues

The DRM Agent and the SRM Agent interact with each other to transfer Rights Objects. The Rights Objects installed in the Smart Card are marked as non-movable to other Devices, but can be Backed up and extracted in a protected manner. These Rights Objects can then only be Restored to the same Smart Card.

5.7.2.2 Actor Specific Benefits

Users can purchase DRM Content and the associated Rights Objects, and know that they can Backup all their Rights Objects. If they loose their Device, their Network Service Provider can provide her another Smart Card to which the Backed up Rights Objects can be Restrored.

5.7.3 Pre-conditions

The User has acquired various DRM Contents these are stored on her mobile phone, the associated Rights Objects are installed in her Device. She is doing regular Backup of her Rights Objects with a service that is offered by her Network Service Provider or with a PC software that is provided by her Network Service Provider. She can decide which Rights Objects she wants to keep in the Smart Card and which ones she wants to extract in order to free some space.

5.7.4 Post-conditions

The user is able to Restore the Backed up Rights Objects to the same Smart Card or to a new one that her Network Service Provider may provide her in the future.

5.7.5 Nomal Flow

1. The User has purchased and downloaded DRM Content and the associated Rights Objects using her mobile phone that contains a Smart Card (e.g. SIM). The Rights Objects for this DRM Content are installed in the Smart Card.

2. The User is doing regular Backups of her Rights Objects using a simple user interface or a PC software provided by her Network Service Provider.

3. The User can Backup the Rights Objects or can Backup the Rights Objects while extracting them from the Smart Card to free some space.

4. The User is able to Restore the Backed up Rights Objects in her Smart Card, or to a new one that her Network Service Provider may provide in the future

5.7.6 Alternate flow

If there are no remaining Rights or the Rights have expired for the DRM Content on the Smart Card, the User cannot Consume the corresponding DRM Content.

If mutual authentication fails the Consumption of DRM Contents/Rights Objects SHALL be prevented.

5.8 Scenario7: Pre-Loading of Rights Objects by using the Smart Card

5.8.1 Short Description

A Network Service Provider is providing a brand new music services for teenagers when they purchase a new network subscription.

In order to deploy exclusive contents, the Network Service Provider provisions DRM Content on the mobile phone or a removable media if available (e.g. MMC, Smart Card …). Finally, the corresponding set of Rights Objects are installed in the Smart Card at the factory during the personalization.

Wendy subscribes to this new service, she puts the Smart Card into her handset, switches on the handset and enjoys her new content without any network interaction.

For sure, this new use case is not replacing the standard way to provision Rights Objects by using OTA (Over The Air) process through ROAP.
This is just a way that can be used by a Network Service Provider to attract new subscribers by promoting free and DRM contents.

5.8.2 Actors

DRM Agent	See actors in the section 5.1.1
SRM Agent	See actors in the section 5.1.1
User	See actors in the section 5.1.1

5.8.2.1 Actor Specific Issues

The DRM Agent and the SRM Agent interact with each other to transfer DRM Contents and Rights Objects.

5.8.2.2 Actor Specific Benefits

It is possible for the Device issuer (e.g. a Network Service Provider) to deploy exclusive contents and Rights Objects to new Users by simply using the Smart Card.

5.8.3 Pre-conditions

The User has acquired new services and in doing so gains access to various DRM Content and Rights Objects.

The User's new mobile phone supports the Smart Card.

5.8.4 Post-conditions

The DRM Content can be used at the User's new mobile phone.

5.8.5 Normal Flow

1. The service issuer (e.g. a Network Service Provider) is willing to deploy new services with exclusive contents to attract new customers.

2. The service issuer (e.g. a Network Service Provider) is offering DRM Content stored into the mobile phone or a removable media is available (e.g. MMC, Smart Card, …)

3. The service issuer (e.g. a Network Service Provider) has provisioning Rights Objects in the Smart Card during the personalization phase
4. The User has purchased a new service subscription and their mobile phone supports the Smart Card.
5. The User is switches the mobile phone on
6. The SRM Agent transfers Rights Objects to the user's new mobile phone DRM Agent after mutual authentication between the DRM Agent and the SRM Agent.
7. The User can Consume transferred Rights Objects.
8. The User enjoys the exclusive DRM Contents provided by the Network Service Provider.

5.8.6 Alternate flow

If there are no Rights Objects provisioned in the Smart Card for the DRM Content, then the User can download them according to the information stored into the DRM Content.

If there are no remaining Rights or the Rights have expired for the transferred DRM Content, the User cannot Consume the Protected Content.

If mutual authentication fails, the transfer of Rights Objects SHALL be prevented.

6. Requirements (Normative)

6.1 High-Level Functional Requirements

Label	Description	Enabler Release
REQ-FCT-1	The DRM Agent SHALL be able to transfer Rights to the SRM Agent.	SRM 1.0
REQ-FCT-2	The SRM Agent SHALL be able to transfer Rights to the DRM Agent.	SRM 1.0
REQ-FCT-3	The DRM Agent SHALL be able to use Rights which are transferred from the SRM Agent.	SRM 1.0
REQ-FCT-4	The DRM Agent SHALL be able to use Rights that are stored in the SRM and update state information in the SRM for stateful rights.	SRM 1.0
REQ-FCT-5	SRM enabler SHALL ensure that only one instance of the Rights Object is usable at any time.	SRM 1.0
REQ-FCT-6	The DRM agent on the Device SHALL ensure that Rights that are Moved from the Device to a SRM can no longer be used on the Device.	SRM 1.0
REQ-FCT-7	Rights Issuer SHALL be able to indicate that the Rights MUST be stored in the Secure Removable Media.	SRM 1.0
REQ-FCT-8	Rights Issuer SHALL be able to restrict the number of times the Rights are transferred between the Device and Secure Removable Media.	SRM 1.0
REQ-FCT-9	The communication protocol between the Device and the SRM Agents (Memory Card, Smart Card …) SHALL be independent of the physical layer.	SRM 1.0
REQ-FCT-10	It SHALL be possible for the user to Backup Stateless Rights Objects from the SRM to a local PC, a remote server or other local mass memory media, and subsequently restore these Rights Objects for usage to the user's SRM	SRM 1.0
REQ-FCT-11	The DRM Agent SHALL be able to read Rights from the Secure Removable Media after the successful mutual authentication with the SRM Agent.	SRM 1.0
REQ-FCT-12	The DRM Agent SHALL be able to write Rights on the Secure Removable Media after the successful mutual authentication with the SRM Agent.	SRM 1.0
REQ-FCT-13	The DRM Agent SHALL be able to remove Rights from the Secure Removable Media after the successful mutual authentication with the SRM Agent.	SRM 1.0
REQ-FCT-14	The DRM Agent SHALL be able to update Rights Object states on the Secure Removable Media after the successful mutual authentication with the SRM Agent.	SRM 1.0

Table 1: High-Level Functional Requirements

6.1.1 Security

Label	Description	Enabler Release
REQ-SEC-1	The DRM Agent SHALL be able to authenticate the SRM Agent.	SRM 1.0
REQ-SEC-2	The SRM Agent SHALL be able to authenticate the DRM Agent.	SRM 1.0
REQ-SEC-3	A Backed Up Rights Object SHALL NOT be Moved.	SRM 1.0
REQ-SEC-4	The mutual authentication between the SRM Agent and a DRM Agent SHALL be secure, e.g. against replay attacks.	SRM 1.0
REQ-SEC-5	Rights or parts thereof in use by a Device SHALL NOT simultaneously be available for use by a SRM that provided such Rights to that Device.	SRM 1.0
REQ-SEC-6	If an SRM Agent provides Rights to a DRM Agent, then any reverting back of the Rights or parts of the Rights to the SRM Agent SHALL be accomplished via a secure method.	SRM 1.0
REQ-SEC-7	Protocol between the DRM Agent and the SRM Agent SHALL allow recovery from an unexpected communication interrupt.	SRM 1.0
REQ-SEC-8	Rights Object SHALL not be exposed unless upon request from the SRM agent.	SRM 1.0
REQ-SEC-9	The SRM enabler SHALL ensure the Confidentiality of any Content Encryption Key (CEK) in the Rights Object, in a manner independent of the transport mechanism between the SRM Agent and the DRM Agent such that the CEK can only be used by the DRM Agent.	SRM 1.0
REQ-SEC-10	The SRM enabler SHALL ensure the Integrity of the Rights Object, in a manner independent of the transport mechanism between the SRM Agent and the DRM Agent.	SRM 1.0
REQ-SEC-11	Devices and SRM SHALL be able to use revocation information as part of ensuring a secure mechanism between DRM Agents and SRM Agents.	SRM 1.0

Table 2: High-Level Functional Requirements – Security Items

6.1.2 Interoperability

Label	Description	Enabler Release
REQ-IOP-1	The SRM enabler SHALL be backward compatible with OMA DRM v2.0.	SRM 1.0

Table 3: High-Level Functional Requirements – Interoperability Items

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-RD-SRMProfile-V1_0_0-D	28/10/05	5.x	Add Use cases agreed during the Sydney'05 Meeting
OMA-RD-SRMProfile-V1_1_0-D	11/11/05	6.1.x	Add first set of requirements
OMA-RD-SRMProfile-V1_2_0-D	24/11/05	6.1.x	Remove requirements, an IC will be submitted during Athens meeting
OMA-RD-SRMProfile-V1_3_0-D	15/12/05	6.1.x	Add Requirements agreed into OMA-DLDRM-2005-0390R03-Requirements-for-SRMProfile-1.doc during Athens meeting (12-15 Dec. 2005)
OMA-RD-SRMProfile-V1_4_0-D	10/02/06	3.2, 4, 5.x, 6.x	Include modifications on Definitions, Use Cases and Requirements agreed into OMA-DLDRM-2006-0036-CR-SRM-RD-Use-Case-Modification & OMA-DLDRM-2006-0046R02-Requirements-for-SRM & OMA-DLDRM-2006-0047R03-New-Req-for-SRM & OMA-DLDRM-2006-0062R01-SRM-RD-Definition during Paris meeting (6th-10th Jan. 2006)
OMA-RD-SRMProfile-V1_4_1-D	27/02/06	3.3, 4	A few typos and editorial changes and new abbreviations
OMA-RD-SRM-V1_0-	02/05/06	All	Updates according RDRR
	22/05/06	All	Update security requirements according to Doc 93R03 Update doc according to Orange/viacess RDRR comments Update Stateful Rights definition according to new DRM v2 spec (March release) Updates according to the final RDRR
	14/06/06	Chapter 6	Fix enabler release: Change 1.0 with "SRM 1.0"
	14 Sep 2006	All	Editorial fixes: cross-references, 2006 template (copyright, styles)
Candidate Versions OMA-RD-SRM-V1_0	10 Oct 2006	All	Status changed to Candidate by TP: OMA-TP-2006-0317R01-INP_SRM_V1_0_RD_for_Candidate_approval