Secure Removable Media Requirements

Candidate Version 1.1 – 26 May 2009

Open Mobile Alliance

OMA-RD-SRM-V1_1-20090526-C

Contents

Tables

1. Scope (Informative)

This document defines specifies the requirements and related use cases for the OMA DRM based Secure Removable Media (SRM) 1.1 with the goal to extend the OMA DRM enabler to allow use of the Secure Removable Media for managing DRM protected contents and the Rights in a secure manner consistent to other OMA DRM technologies.

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

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

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

[SCE 1.0] "OMA Secure Content Exchange Specification", Open Mobile Alliance™, OMA-ERP-SCE-V1_0, 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/

2.2 Informative References

[OMADICT] "Dictionary for OMA Specifications", Version x.y, Open Mobile Alliance™, OMA-ORG-Dictionary-Vx_y, URL:http://www.openmobilealliance.org/

3. Terminology and Conventions

3.1 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

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

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 Provisioning of Rights	Issuing, downloading and installing the Rights from a Rights Issuer to a SRM. The Rights are issued from the Rights Issuer and cryptographically bound to SRM.
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.
Token	Token is a credit which can be exchanged for temporary access to a service. Tokens are purchased by user from a service provider and stored at user's device. Token management is explained in [DRMXBS]

3.3 Abbreviations

OMA	Open Mobile Alliance
MMC	Multi Media Card
MPEG	Moving Picture Expert Group
PC	Personal Computer
ROAP	Rights Object Acquisition Protocol
SIM	Subscriber Identity Module
SRM	Secure Removable Media
USIM	Universal Subscriber Identity Module

4. Introduction (Informative)

The Secure Removable Media (SRM) is a the portable Device medium such as memory card or smart card complete with secure storage area that is protected against unauthorized access. By specifying the SRM Agent, which is a trusted entity embedded in the SRMs, and related protocols, the OMA "Secure Removable Media" (SRM) addresses the user's demands for DRM portability through the SRMs: it enables the SRMs to acquire, move, and consume the Rights Objects in a secure manner.

Finally, the SRM 1.1 will strive to keep track of the latest OMA DRM technologies and maintain backward compatibility with the SRM 1.0 technical specifications.

5. SRM1.1 release description (Informative)

The purpose of this section is to provide overall descriptions for each OMA SRM release in terms of its functions, usability, and compatibility with other releases and DRM technical specifications.

In OMA SRM 1.0, the framework for the OMA SRM enabler has been provided, in a manner compatible with other OMA DRM technologies, by specifying the SRM Agent and various interfaces between the SRM and device. With the framework, the OMA SRM 1.0 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.

While OMA SRM 1.0 provides the framework enabling the portability of Rights through the SRM, it was not possible for the Content Provider to issue the Rights to the SRM in the first place, the use case so called "Direct Provisioning of Rights." Delivering technical specifications to realize this unfulfilled use case is the primary objective of the OMA SRM 1.1.

This new function is depicted in the following figure, together with those provided by OMA SRM 1.0. In figure 1, the Rights is issued to the SRM being cryptographically bound to the SRM, and then consumed on the hosting device or transferred to other devices.

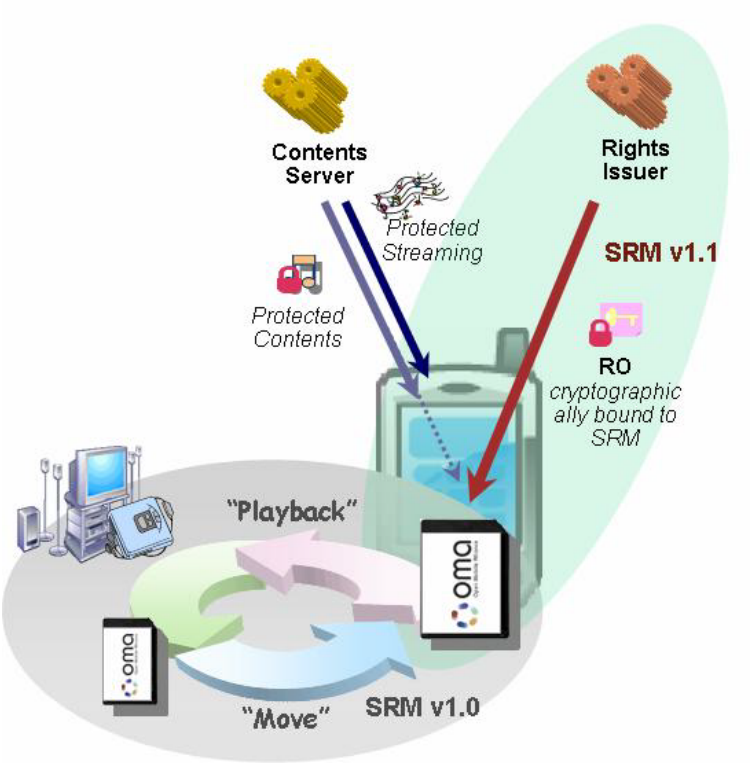


Figure 1: Direct Provisioning of Rights and its overall relationship with the OMA SRM 1.0 functions.

Also in OMA SRM 1.1, some other new functions such as Rights transfer between two SRMs and the SRM Rights Upgrade will be provided. See the following sub-sections for more details.

5.1 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 and Device

- SRM to Device Rights Move and vice versa
- Local Rights Consumption
- Compatibility and Supports for the OMA DRM 2.0 [DRM 2.0].

5.2 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 [DRM 2.1] and the OMA SCE 1.0 [SCE 1.0]
- Backward Compatibility to the OMA SRM 1.0 [SRM 1.0]

6. Requirements (Normative)

6.1 Modularisation

This section depicts the whole release as a collection of different functional modules where each one is a group of requirements identified as related with the offering of functionality.

The defined functional modules are as follows:

- **SRM to SRM Rights Move:** the functional module to Move the Rights directly from one SRM to another SRM .
- **Provisioning:** the functional module to provision the Rights directly into the SRM.
- **SRM Rights Upgrade:** the functional module for upgrading the Rights on SRM.
- **Local Rights Consumption:** the functional module to consume the SRM Rights on the Device without incurring Move of the Rights.
- **Broadcast RO Move:** the functional module for Moving the Broadcast RO between SRM and Device.
- **Token Management:** the functional module to facilitate Token management including but not limited to Token transfer and Token consumption.
- **Rights Move between SRM and Device:** the functional module for Moving the Rights between SRM and Device.
- **General:** Some requirements are intended to affect all the functional modules, and therefore are marked in the functional module column of the requirement's table as “General”.

6.2 High-Level Functional Requirements

Label	Description	Release	Functional module
SRM-HLF-001	The DRM Agent SHALL be able to transfer Rights to the SRM Agent.	SRM V1.0	Rights Move between SRM and Device
SRM-HLF-002	The SRM Agent SHALL be able to transfer Rights to the DRM Agent.	SRM V1.0	Rights Move between SRM and Device
SRM-HLF-003	The DRM Agent SHALL be able to use Rights which are transferred from the SRM Agent.	SRM V1.0	Rights Move between SRM and Device
SRM-HLF-004	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 V1.0	Local Rights Consumption
SRM-HLF-005	SRM enabler SHALL ensure that only one instance of the Rights Object is usable at any time.	SRM V1.0	General
SRM-HLF-006	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 V1.0	Rights Move between SRM and Device
SRM-HLF-007	Rights Issuer SHALL be able to indicate that the Rights MUST be stored in the Secure Removable Media.	SRM V1.0	Provisioning
SRM-HLF-008	Rights Issuer SHALL be able to restrict the number of times the Rights are transferred between the Device and Secure Removable Media.	SRM V1.0	Rights Move between SRM and Device

SRM-HLF-009	The communication protocol between the Device and the SRM Agents (Memory Card, Smart Card …) SHALL be independent of the physical layer.	SRM V1.0	General
SRM-HLF-010	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	Future	General
SRM-HLF-011	The DRM Agent SHALL be able to read Rights from the Secure Removable Media after the successful mutual authentication with the SRM Agent.	SRM V1.0	Rights Move between SRM and Device
SRM-HLF-012	The DRM Agent SHALL be able to write Rights on the Secure Removable Media after the successful mutual authentication with the SRM Agent.	SRM V1.0	Rights Move between SRM and Device
SRM-HLF-013	The DRM Agent SHALL be able to remove Rights from the Secure Removable Media after the successful mutual authentication with the SRM Agent.	SRM V1.0	Rights Move between SRM and Device
SRM-HLF-014	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 V1.0	General
SRM-HLF-015	The SRM enabler SHALL allow the direct Rights transfer from one SRM Agent to another SRM Agent.	SRM V1.1	SRM to SRM Rights Move
SRM-HLF-016	It SHALL be possible to support the subscription model for DRM contents service based on the SRMs, i.e. subscriber cards.	SRM V1.1	Provisioning
SRM-HLF-017	It SHALL be possible for the User to access the DRM contents service continuously and seamlessly from different host Devices as long as the SRM is attached to the Device. **Informational Note:** It includes not just contents consumption, but also contents purchase from different Devices using the same subscription or billing information stored in the SRM.	SRM V1.1	Provisioning
SRM-HLF-018	It SHALL be possible to issue the Rights for the SRMs, download and install it into the SRMs directly.	SRM V1.1	Provisioning
SRM-HLF-019	When the User purchases contents, the Content Provider MUST be able to determine whether it is going to create the Rights for the SRM and trigger subsequent acquisition procedures.	SRM V1.1	Provisioning
SRM-HLF-020	Both separate delivery and combined delivery for the Contents and Rights SHALL be supported.	SRM V1.1	Provisioning
SRM-HLF-021	The solution SHALL be easily, widely applicable to the media with severe resource constraints, such as computing power and memory.	SRM V1.1	Provisioning
SRM-HLF-022	SRM enabler SHALL allow Rights Issuer to create upgraded Rights for SRM corresponding to the request.	SRM V1.1	SRM Rights Upgrade
SRM-HLF-023	SRM enabler SHALL allow a Device to transmit to RI the request for upgrading the rights installed in SRM.	SRM V1.1	SRM Rights Upgrade
SRM-HLF-024	SRM enabler SHALL allow a Device to transmit the upgraded rights to SRM.	SRM V1.1	SRM Rights Upgrade
SRM-HLF-025	It SHALL be possible to upgrade the existing Rights installed in SRM with the upgraded Rights issued by RI.	SRM V1.1	SRM Rights Upgrade
SRM-HLF-026	The SRM enabler SHALL allow certain Rights Objects to be consumed only when the SRM containing those Rights Objects is present in the device.	SRM V1.1	Local Rights Consumption

SRM-HLF-027	The SRM enabler SHALL enable an indication in Rights Objects that mandates that they can be consumed only when the SRM containing those Rights Objects is presented in the device.	SRM V1.1	Local Rights Consumption
SRM-HLF-028	The SRM enabler SHALL enable restricting Move of certain Rights Objects in the SRM.	SRM V1.1	Local Rights Consumption
SRM-HLF-029	The SRM enabler SHALL enable the DRM Agent to Move Broadcast RO (BCRO) to the SRM. Informational note: BCRO is defined in [DRMXBS].	SRM V1.1	Broadcast RO Move
SRM-HLF-030	The SRM enabler SHALL enable the SRM Agent to Move BCRO to the Device.	SRM V1.1	Broadcast RO Move

Table 1: High-Level Functional Requirements

6.2.1 Security

Label	Description	Release	Functional module
SRM-SEC-001	The DRM Agent SHALL be able to authenticate the SRM Agent.	SRM V1.0	General
SRM-SEC-002	The SRM Agent SHALL be able to authenticate the DRM Agent.	SRM V1.0	General
SRM-SEC-003	A Backed Up Rights Object SHALL NOT be Moved.	SRM V1.0	General
SRM-SEC-004	The mutual authentication between the SRM Agent and a DRM Agent SHALL be secure, e.g. against replay attacks.	SRM V1.0	General
SRM-SEC-005	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 V1.0	General
SRM-SEC-006	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 V1.0	General
SRM-SEC-007	Protocol between the DRM Agent and the SRM Agent SHALL allow recovery from an unexpected communication interrupt.	SRM V1.0	General
SRM-SEC-008	Rights Object SHALL not be exposed unless upon request from the SRM agent.	SRM V1.0	General
SRM-SEC-009	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 V1.0	General
SRM-SEC-010	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 V1.0	General
SRM-SEC-011	Devices and SRM SHALL be able to use revocation information as part of ensuring a secure mechanism between DRM Agents and SRM Agents.	SRM V1.0	General
SRM-SEC-012	The SRM enabler SHALL ensure the Integrity of the Rights Object, in a manner independent of the transport mechanism between the SRM Agent and another SRM Agent.	SRM V1.1	SRM to SRM Rights Move
SRM-SEC-013	Both SRMs SHALL be able to use revocation information as part of ensuring a secure mechanism for SRM to SRM rights Move.	SRM V1.1	SRM to SRM Rights Move
SRM-SEC-014	The SRM 1.1 enabler SHALL ensure the confidentiality of the Rights Object, in a manner independent of the transport mechanism between the SRM Agent and the Rights Issuer.	SRM V1.1	Provisioning

SRM-SEC-015	The SRM 1.1 enabler SHALL ensure the integrity of the Rights Object, in a manner independent of the transport mechanism between the SRM Agent and the Rights Issuer.	SRM V1.1	Provisioning
SRM-SEC-016	It SHALL be possible for the Rights Issuer to authenticate the identity of the SRM Agent that is requesting the Rights Object.	SRM V1.1	Provisioning

Table 2: High-Level Functional Requirements – Security Items

6.2.1.1 Authentication

Label	Description	Release	Functional module
SRM-SEC-ATT-001	The Rights Issuer MUST be able to authenticate the Rights acquisition request using the SRM's certificate.	SRM V1.1	Provisioning
SRM-SEC-ATT-002	It SHALL be possible to authenticate on the recipient side the Rights and message transmitted by the Rights Issuer.	SRM V1.1	Provisioning

Table 3: High-Level Functional Requirements – Authentication Items

6.2.1.2 Data Integrity

Label	Description	Release	Functional module
SRM-SEC-DIT-001	SRM 1.1 MUST provide the mechanism to protect data integrity over the course of the Rights acquisition to the SRM from the Rights Issuer.	SRM V1.1	Provisioning

Table 4: High-Level Functional Requirements – Data Integrity Items

6.2.1.3 Confidentiality

Label	Description	Release	Functional module
SRM-SEC-CON-001	The Rights issued for the SRMs SHALL be cryptographically bound to the SRMs.	SRM V1.1	Provisioning
SRM-SEC-CON-002	Over the course of the Rights acquisition to the SRM from the Rights Issuer, the contents keys SHALL NOT be exposed to the intermediaries.	SRM V1.1	Provisioning

Table 5: High-Level Functional Requirements – Confidentiality Items

6.2.2 Charging

Label	Description	Release	Functional module
SRM-CHG-001	It MUST be possible to charge based on the services provided to the SRM.	SRM V1.1	Provisioning

Table 6: High-Level Functional Requirements – Charging Items

6.2.3 Administration and Configuration

Label	Description	Release	Functional module
SRM-ADM-001	When the host Device is changed, it MUST be possible that the system be automatically set up so as to provide the User with continuous access to the service from the User's new Device without requiring the User's intervention, e.g. manually inform the Contents Provider of the Device change.	SRM V1.1	Provisioning

Table 7: High-Level Functional Requirements – Administration and Configuration Items

6.2.4 Usability

Label	Description	Release	Functional module
SRM-USE-001	When the User attaches the SRM to a different host Device, the User SHALL be able to access the services seamlessly without manual re-configuration or registration of the new Device to the portal.	SRM V1.1	Provisioning

Table 8: High-Level Functional Requirements – Usability Items

6.2.5 Interoperability

Label	Description	Release	Functional module
SRM-INT-001	The SRM enabler SHALL be backward compatible with OMA DRM v2.1, SRM v1.0.	SRM V1.1	SRM to SRM Rights Move
SRM-INT-002	The SRM enabler SHALL be able to Move Rights Object that is consistent to SCE REL.	SRM V1.1	SRM to SRM Rights Move
SRM-INT-003	The Rights acquisition for the direct provisioning of the Rights MUST be backward compatible with SRM 1.0 and DRM 2.1.	SRM V1.1	Provisioning
SRM-INT-004	The SRM enabler SHOULD provide extensibility mechanisms in messages and data structures to be used by future specifications extending SRM v1.1.	SRM V1.1	General
SRM-INT-005	The upgrade for SRM rights SHALL be backward compatible with RO upgrade protocol from SCE 1.0.	SRM V1.1	SRM Rights Upgrade

Table 9: High-Level Functional Requirements – Interoperability Items

6.2.6 Token management

Label	Description	Release	Functional module
SRM-TMN-001	The DRM Agent SHALL be able to transfer tokens and the related token information to the SRM Agent.	SRM V1.1	Token Management
SRM-TMN-002	The SRM Agent SHALL be able to transfer tokens and the related token information to the DRM Agent.	SRM V1.1	Token Management
SRM-TMN-003	The SRM enabler SHALL ensure that each token is used by only one Device at one time.	SRM V1.1	Token Management

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 <current version> History

Document Identifier	Date	Sections	Description
Draft Versions OMA-RD_SRM-V1_1	17 Dec 2008	all	Baseline for version 1.1 of this RD
	30 Dec 2008	6 Appendix B	Use cases agreed during Cancun meeting ,2008 OMA-DRM-2008-0521R01-INP_SRM_RD_Requirements_and_Usecase OMA-DRM-2008-0513R01-INP_SRM1.1_Security_Requirements OMA-DRM-2008-0512-INP_SRM_Seamless_Service_Access OMA-DRM-2008-0511-INP_SRM_DRM_Subscription_through_Cards OMA-DRM-2008-0509R02-INP_SRM_Interoperability OMA-DRM-2008-0508R01-INP_SRM_Usability OMA-DRM-2008-0507R02-INP_SRM_ADM OMA-DRM-2008-0506R01-INP_SRM_SEC OMA-DRM-2008-0504R01-INP_SRM_HLFR
	24 Jan 2009	1,4, 5 6	Scope, Introduction, and Release Description, changed in 2009 OMA-DRM-2009-0001-CR_New_Scope_Text_for_SRM_1_1 OMA-DRM-2009-0002R02-CR_New_Introduction_Text_for_SRM_1_1 OMA-DRM-2009-0003R01-CR_Release_Section_SRM_1_1 Changed Requirements, OMA-DRM-2008-0505R01-INP_SRM_Charging OMA-DRM-2009-0004R01-CR_SRM_1_1_Extensibility_requirement
	10 Feb 2009	2,3,6, Appendix B	Agreed CRs in Macro meeting, OMA-DRM-2009-0016R01-CR_Unused_Acronyms OMA-DRM-2009-0015R02-CR_Missing_References OMA-DRM-2009-0010R02- CR_SRM_RD_Requirements_and_Usecase_to_SRM_rights_upgrade The figures in OMA-DRM-2008-0511-INP_SRM_DRM_Subscription_through_Cards and OMA-DRM-2008-0512-INP_SRM_Seamless_Service_Access that have been neglected in previous version of SRM RD1.1 have been added in the B.9 and B.10 respectively.
	27 Feb, 2009	2,3,6 Appendix B	Agreed CR in the CC in 26 Feb, OMA-DRM-2009-0037R03- CR_SRM_extensions_for_BCAST_in_SRM_requirements
	28 Feb 2009	3	Agreed CR in Macro meeting OMA-DRM-2009-0031R02-CR_SRMv1.1_RD_Add_Definitions
	2 Apr, 2009	6	OMA-DRM-2009-0051R03-CR_SRM_RD_Function_Modularisation
	20 Apr, 2009	6.2	OMA-DRM-2009-0062-CR_Missing_requirement_regarding_BCRO_Move
	30 Apr, 2009	A2 B8	Editorial changes according to the comments in REQ CC: 1. Remove the yellow box below the A.2 title; 2. Remove the bracket of the title of B.8. 3. Template 2009
Candidate Versions OMA-RD-SRM-V1_1	26 May 2009	All	Status changed to Candidate by TP OMA-TP-2009-0204-INP_SRM_V1_1_RD_for_Candidate_Approval

Appendix B. 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.

For the Use Cases within this section, 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.

B.1 Upgrade from old Devices to new Devices by using the Secure Removable Media

B.1.1 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.

B.1.2 Actors

B.1.2.1 Actor Specific Issues

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

B.1.2.2 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.

B.1.3 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.

B.1.4 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.

B.1.5 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.

B.1.6 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.

B.2 Provisioning of Rights Object in the Smart Card

B.2.1 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.

B.2.2 Actors

B.2.2.1 Actor Specific Issues

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

B.2.2.2 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.

B.2.3 Pre-conditions

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

B.2.4 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.

B.2.5 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.

B.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.

B.3 Using Contents in Multiple Devices by using the Secure Removable Media

B.3.1 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.

B.3.2 Actors

B.3.2.1 Actor Specific Issues

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

B.3.2.2 Actor Specific Benefits

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

B.3.3 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.

B.3.4 Post-conditions

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

B.3.5 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.

B.3.6 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.

B.4 Transfer Contents and Rights Objects among OMA Conformant Devices by using the Secure Removable Media

B.4.1 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.

B.4.2 Actors

B.4.2.1 Actor Specific Issues

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

B.4.2.2 Actor Specific Benefits

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

B.4.3 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.

B.4.4 Post-conditions

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

B.4.5 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.

B.4.6 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.

B.5 Direct Rendering of DRM Contents by using the Secure Removable Media

B.5.1 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.

B.5.2 Actors

B.5.2.1 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.

B.5.2.2 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.

B.5.3 Pre-conditions

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

B.5.4 Post-conditions

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

B.5.5 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 s.

B.5.6 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

B.6 Backup of Rights Object in the Smart Card

B.6.1 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.

B.6.2 Actors

B.6.2.1 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.

B.6.2.2 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.

B.6.3 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.

B.6.4 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.

B.6.5 Normal 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

B.6.6 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

B.7 Pre-Loading of Rights Objects by using the Smart Card

B.7.1 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.

B.7.2 Actors

B.7.2.1 Actor Specific Issues

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

B.7.2.2 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.

B.7.3 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.

B.7.4 Post-conditions

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

B.7.5 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

B.7.6 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

B.8 SRM to SRM Rights Move

For the Devices inserted with dual or multiple SRMs,in this Use Case, User can move rights between two SRMs.

B.8.1 Short Description

Xiaoming is a modern college student. His mobile phone has two SRM slots.

Formerly, Xiaoming just has one SRM in his mobile phone. With his gradually buying many ROs, this SRM is almost fully occupied. So he inserts the seconcd SRM into the mobile phone.

Two SRMs(SRM-1 and SRM-2) inside the mobile phone are accessible by the host mobile phone simultaneously.

Xiaoli is Xiaoming's girlfriend and will go back home for the summer vacation. She askes Xiaoming give her some digital songs, along with the associated Rights Objects, to enjoy during the vacation. So Xiaoming just transfers some ROs between his two SRMs. Some songs and their associated ROs are moved from SRM-1 to SRM-2. Then Xiaoming pulls out SRM-2 from his mobile phone and gives it to Xiaoli.

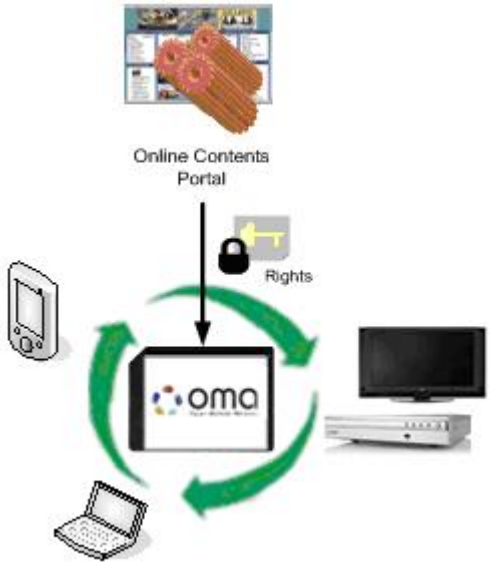
Xiaoli inserts SRM-2 into her own mobile phone and plays the songs in SRM-2 at home.

B.8.2 Market benefits

The rights Move between two SRMs ("S2S Move") is a very popular operation as well as the Move between SRM and Device

This operation would be similar as the file transfer between two U-disks in a PC and would be much convenient to the User. So the User would more like to use SRM and would more like to buy the SRM product and service.

B.9 Seamless Service Access from Multiple Devices



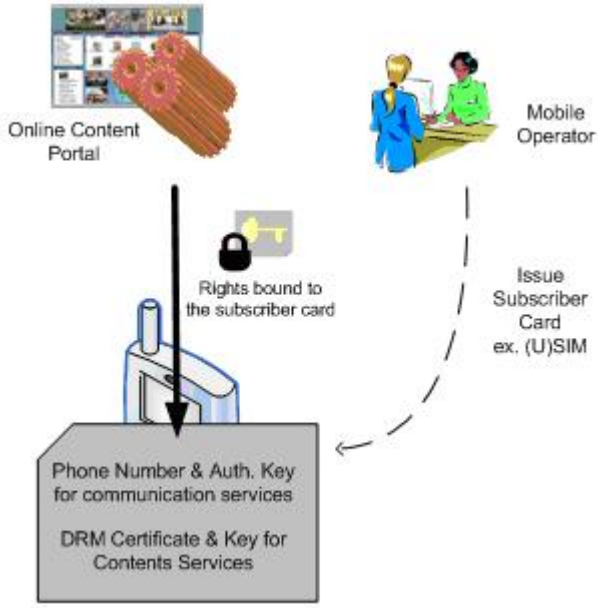
B.9.1 Short Description

Joe subscribes to an online contents service, from which he watches or purchases various contents including films and music. A day before his business trip to Paris, he bought and downloaded several movies and music into the SRM that is attached to the Set-Top-Box, watching one of them on TV. On his business trip, he is carrying the SRM with him. On the airplane he inserts the SRM into his laptop and watches the other movies he bought the other day. Now he is sitting in a nice restaurant in Paris. Over the wireless he accesses the service portal and watches his favourite TV show on his laptop. Next morning in the hotel fitness centre, he is listening to the music bought the other day from his music phone as he runs on the treadmill. He downloads some more free songs from his phone. Although free to download, those songs are DRM protected.

B.9.2 Market Benefits

- It allows the User to seamlessly and continuously access the online contents service from any Devices and from anywhere as long as he carries the SRM, thereby enhancing the user experience and increasing the number of service access.
- It provides the DRM contents portability through the SRM as the Rights moves along with the SRM.
- It supports the subscription model and DRM contents portability at the same time through the SRM for so called triple screen services.

B.10 DRM Service Subscription through the Cards



B.10.1 Short Description

Jane subscribes to a mobile operator for various services including the contents service, and receives the subscriber card with the necessary subscription information already stored. Jane attaches the subscriber card to his music phone, and using them she accesses the online contents portal to download some free contents, DRM protected, and purchases her favourite songs. In the mean time, the Rights for the DRM contents are delivered and installed into her subscriber card. After enjoying the service from her music phone for quite a while, Jane wants to use the movie service provided by the same operator. She buys a state-of-the-art multimedia phone that supports movie downloads and streaming. Jane attaches her subscriber card into her new phone, and she is all set to access the same content portal to use its movie services. Besides, the old DRM contents she purchased from her old music phone are immediately available at her new phone as soon as they are copied to her new phone or memory card.

B.10.2 Market Benefits

- It supports the subscription model through the subscriber card for the mobile operator's converged services including the DRM contents services as bundled with the other mobile operator services.
- It provides the DRM contents portability from one Device to another enabling seamless access to the subscribed contents services and the painless, continuous use of the old DRM contents on her new Device as the subscriber switches her mobile phone.
- It provides improved functionality and flexibility compared to the Conditional Access System (CAS).

B.10.3 Issues

- The DRM contents or services can be offered on a subscription basis to the subscriber who holds the subscriber cards.
- Without the subscriber cards, the DRM contents service must not be provided.
- The solution must be applicable to the resource stricken media, such as ordinary smartcards widely available in the market, in order for the solution to be readily adopted by the market.

- For strong data confidentiality and minimal security risks, the contents keys or service keys must not be exposed to the intermediaries over the course of the Rights provisioning to the subscriber card as well as during the contents migration from the old Device to the new one.

B.11 SRM Rights Upgrade

B.11.1 Short Description

Xiaoming owns a mobile phone which is inserted with a SRM. All the rights he bought for songs are installed on the SRM.

Xiaoming's friend Xiaoli finds a song she favourites much when playing Xiaoming's mobile phone, therefore Xiaoming decides to give it to her as a gift.

But right then, the rights of that song can not be Moved since Xiaoming has not ever purchased the Move permission for it. Xiaoming at once applies the Move permission from service provider for rights of that song. After successful application, the rights of that song is upgraded with new Move permission Xiaoming pulls SRM out from his mobile phone and subsequently inserts it in Xiaoli's mobile phone.

That song and its rights as well are Moved successfully from Xiaoming's SRM to Xiaoli's mobile phone.

B.11.2 Market benefits

This kind of flexible consuming experience is very helpful for the users and content providers.

B.12 SRM extensions for BCAST service support

B.12.1 Short description of use case 1

Alice possesses the SRM card which contains rights and permissions (i.e. Rights Object) for consuming BCAST services. Alice inserts the card in her mobile device and starts viewing BCAST contents. She may continue consuming the service until the Rights Object permits her to do so and while SRM card is inserted in the device. In the event she removes SRM card, device will stop rendering broadcast contents.

In the above description, Rights Object will have the following properties:

- It is cryptographically bound to the SRM card.
- It cannot be moved or copied to a device's internal memory or another SRM card.
- It can be pre-provisioned on the card at the moment of buying the card.
- It can be directly provisioned from the Rights Issuer.

B.12.2 Short description of use case 2

Alice subscribed for BCAST service using her broadcast-only device (as defined in [DRMXBS]). She buys a new device and would like to continue enjoing broadcast contents but on that new device. For that, she inserts her SRM card to the old device and moves BCAST service associated rights (i.e. Broadcast Rights Objects, BCRO) to the card. Then Alice inserts this card to the new device, accesses rights stored on the card and starts consuming BCAST service on her new device.

B.12.3 Short description of use case 3

Tokens are the kind of electronic money that can be used for purchasing of rights for accessing broadcast services. Alice buys tokens from a service provider and stores them on her mobile device. In order to transfer tokens between her devices, Alice first moves them to her SRM card. Then she can acquire necessary amount of tokens from SRM on any device. SRM card can be used as the permanent storage of Alice's tokens.

B.12.4 Market benefits

- First scenario meets business rules of some content providers by binding the rights to a physical medium.
- Second scenario provides rights portability for BCAST service, and allows enjoying broadcast contents on any device anywhere, where SRM card is carried.
- Third scenario introduces a concept of SRM-based electronic wallet, which (together with rights portability) greatly benefits to user experience and brings additional revenue to service and content providers:
    i. User will perform token-based service consumption on any device, anywhere by carrying his SRM card with him and while he has enough number of tokens (credits) on the card.
    ii. Service providers will sell SRM cards with pre-provisioned number of tokens on it.
    iii. User will be able to increase a number of tokens stored on the card by purchasing additional tokens from service provider and transferring.them to device
    iv. User will be able to give tokens to his relatives or friends (as a gift) using his SRM card.