DRM Specification V2.0

Draft Version 2.0 – 20 April 2004

Open Mobile Alliance

OMA-DRM-DRM-V2_0-20040420-D

CONTENTS

FIGURES

TABLES

1. Scope

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. OMA DRM work addresses the various technical aspects of this system by providing appropriate specifications for content formats, protocols, and a rights expression language.

A number of DRM specifications have already been defined within the OMA. See [DRM], [DRMCF] and [DRMREL]. These existing specifications are referred to within this document as “release 1”.

This scope for this specification is to define the protocols, messages and mechanisms necessary to implement the DRM system in the mobile environment. This specification assumes that a PKI is available to facilitate the appropriate transactions between relying parties and it is outside the scope of this specification to define the specifics of such PKI.This specification addresses the specific requirements enumerated in the Release 2 Requirements document [DRMREQ-v2].

2. References

2.1 Normative References

[3GPP PSS] Transparent end-to-end packet switched streaming service (PSS); 3GPP TS-26.234; Protocols and codecs – Release 6. http://www.3gpp.org/

[3GPP TS 24.008] Technical Specification Group Core Network; Mobile radio interface layer 3 specification; Core Network Protocols; Stage 3(Release 5)

[3GPP TS 31.102] Technical Specification Group Terminals; Characteristics of the USIM Application (Release 5).

[3GPP TS 510.11] Specification of the Subscriber Identity Module –Mobile Equipment (SIM – ME) interface (Release 5)

ftp://ftp.3gpp.org/specs/latest/Rel-4/51_series/

[3GPP2 C.S0023-A] http://www.3gpp2.org/Public_html/specs/C.S0023-A_v2.0_021004.pdf

[AES] NIST FIPS 197: Advanced Encryption Standard (AES). November 2001.

URL:http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[AES-WRAP] Advanced Encryption Standard (AES) Key Wrap Algorithm. RFC 3394, J. Schaad and R. Housley, September 2002.

[Bluetooth SDP] Assigned Numbers – Service Discovery Protocol (SDP), Bluetooth SIG, August 2003.

[CP] OMA Certificate and CRL Profiles, draft version 2003-02-16

[DRM] "Digital Rights Management", Open Mobile Alliance™, OMA-Download-DRM-v1_0, http://www.openmobilealliance.org/

[DRMARCH] DRM Architecture Specification, Open Mobile Alliance, OMA-Download_DRMARCH_v1_0

http://www.openmobilealliance.org/

[DRMCF] "DRM Content Format", Open Mobile Alliance™, OMA-Download-DRMCF-v1_0, http://www.openmobilealliance.org/

[DRMCF-v2] DRM Content Format, OMA, v2

[DRMREL] "DRM Rights Expression Language", Open Mobile Alliance™, OMA-Download-DRMREL-v1_0, http://www.openmobilealliance.org/

[DRMREL-v2] DRM Rights Expression Language, OMA, v2

[DRMREQ-v2] DRM Requirements Specification, OMA, v2

[HMAC] RFC 2104: HMAC: Keyed-Hashing for Message Authentication. H. Krawczyk, M. Bellare, and R. Canetti. Informational, February 1997.

http://www.ietf.org/rfc/rfc2104.txt

[HTTP] RFC 2616. Hypertext Transfer Protocol – HTTP/1.1. J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee. June 1999. http://www.ietf.org/rfc/rfc2616.txt

[IETF-KEM] Kaliski B., "Use of the RSA-KEM Key Transport Algorithm in CMS", IETF work in progress, 2003.

[IOPPROC] "OMA Interoperability Policy and Process", Version 1.1, Open Mobile Alliance(tm), OMA-IOP-Process-V1_1, URL:http://www.openmobilealliance.org/

[ISO/IEC 18033] ISO/IEC 18033-2, Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers. CD3, January 2004.

[MIME] RFC 2045. Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies. N. Freed & N. Borenstein. November 1996.

http://www.ietf.org/rfc/rfc2045.txt

[OBEX] IrDA Object Exchange Protocol (OBEX), Version 1.3, January 2003.

[OCSP] Online Certificate Status Protocol, http://www.ietf.org/rfc/rfc2560.txt

[OCSP-MP] OMA Online Certificate Status Protocol (profile of [OCSP]) V 1.0, http://www.openmobilealliance.org/

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

[RFC2045] "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", N. Freed & N. Borenstein, November 1996, http://www.ietf.org/rfc/rfc2045.txt

[RFC2234] "Augmented BNF for Syntax Specifications: ABNF". D. Crocker, Ed., P. Overell. November 1997. URL:http://www.ietf.org/rfc/rfc2234.txt

[RFC2387] "The MIME Multipart/Related Content-type", E. Levinson, 1998, http://www.ietf.org/

[RFC2396] "Uniform Resource Identifiers (URI): Generic Syntax". T. Berners-Lee, R. Fielding, L. Masinter. August 1998. http://www.ietf.org/rfc/rfc2396.txt

[RFC 2965] "HTTP State Management Mechanism". D. Kristol, L. Montulli, October 2000

http://www.ietf.org/rfc/rfc2965.txt.

[X9.44] Draft ANSI X9.44, Public Key Cryptography for the Financial Services Industry – Key Establishment Using Integer Factorization Cryptography. Draft 6, 2003.

[XC14N] Exclusive XML Canonicalization: Version 1.0, John Boyer, Donald E. Eastlake 3rd and Joseph Reagle, W3C Recommendation 18 July 2002. This document is http://www.w3.org/TR/xml-exc-c14n/.

[XML-DSIG] XML-Signature Syntax and Processing. D. Eastlake, J. Reagle, and D. Solo. W3C Recommendation, February 2002.

http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/

[XML-Encryption] XML Encryption Syntax and Processing. D. Eastlake and J. Reagle. W3C Candidate Recommendation, December 2002.

http://www.w3.org/TR/2002/CR-xmlenc-core-20021210/

[XML-Schema] XML Schema Part 1: Structures D. Beech, M. Maloney, and N. Mendelsohn. W3C Recommendation, May 2001.

http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/

XML Schema Part 2: Datatypes. P. Biron and A. Malhotra. W3C Recommendation, May 2001.

http://www.w3.org/TR/2001/REC-xmlschema-2-20010502/

[WAPWIM] "Wireless Application Protocol Architecture Specification", Open Mobile Alliance™. OMA-WAP-WIM-v1_1-20021024-C

[WAPCertProf] "WAP Certificate Profile Specification". WAP Forum™, WAP-211-WAPCert-20010522-a http//www.openmobilealliance.org

2.2 Informative References

[DLOTA] "OMA Download version 1.0." Open Mobile Alliance™. OMA-Download-OTA-V1_0. www.openmobilealliance.org/documents.html

[DRMARCH-v2] "OMA DRM Architecture", Open Mobile Alliance™. OMA-DRM-ARCH-V2_0. www.openmobilealliance.org/documents.html

[PUSHOTA] "Push OTA Protocol Specification." Open Mobile Alliance™. WAP-235-PushOTA. www.openmobilealliance.org/wapdownload.html

[UICC] "Smart cards; UICC-Terminal interface; Physical and logical characteristics (release 5)", ETSI 102.221 , http://www.etsi.org

[TS26.244] "Transparent end-to-end Packet-switched Streaming Service (PSS); File Format", Version 1.2.0,

The Third Generation Partnership Project, TS-26.244, URL:http://www.3gpp.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.

This specification uses schema documents conforming to W3C XML Schema [SCHEMA] and normative text to describe the syntax and semantics of XML-encoded ROAP messages.

Listing of Rights Object Acquisition Protocol (ROAP) schemas appear like this.

The following typographical conventions are used in the body of the text: **<XML Element>**, ***XMLAttribute***, **XMLType**, `ASN.1ValueOrType`.

3.2 Definitions

Backup/Remote Storage	Transferring Rights Objects and Content Objects to another location with the intention of transferring them back to the original Device.
Billing Service Provider	The entity responsible for collecting payment from a User.
Combined Delivery	A Release 1 method for delivering Protected Content and Rights Object. The Rights Object and Protected Content are delivered together in a single entity, the DRM Message.
Composite Object	A content object that contains one or more Media Objects by means of inclusion.
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities or processes. (From [ISO 7498-2])
Connected Device	A Connected Device is a Device that is capable of directly connecting to a Rights Issuer using an appropriate protocol over an appropriate transport/network layer interface. E,g, HTTP over TCP-IP.
Content	One or more Media Objects
Content Issuer	The entity making content available to the DRM Agent in a Device.
Content Provider	An entity that is either a Content Issuer or a Rights Issuer.
Content subscription	A subscription that a User has with a Content Provider for the purposes of paying for Protected Content purchased from that Content Provider and played on a Users Device.
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. In the case where functionality is specific to either Connected Devices or Unconnected Devices the explicit terminology (i.e Unconnected Device or Connected Device) will be used, in all other cases the term Device generically applies to both Connected Devices and Unconnected Devices.
Device Revocation	The process of an RI indicating that a Device is no longer trusted to acquire ROs.
Device Rights Object	An RO dedicated for a particular Device by means of the Device Public Key.
Domain	A set of Devices, which are able to share Domain Rights Objects. Devices in a Domain share a Domain Key. A Domain is defined and managed by an RI.
Domain Identifier	A unique string identifier of the Domain Key
Domain Key	A 128 bit symmetric cipher key
Domain Generation	A Counter reflecting the number of times the Domain has been upgraded. The Domain Generation is a part of the Domain Identifier (the last two digits).
Domain Context	The Domain Context consists of information necessary for the Device to install Domain Rights Objects, such as Domain Key, Domain Identifier and Expiry Time.
Domain Context Expiry Time	An absolute time after which the Device is not allowed to install ROs for this Domain. Usage of ROs installed before the expiry time are not affected by the expiry.

Domain Revocation	The process of an RI indicating that a Domain Key is not trusted for protection of Domain ROs.
Domain Rights Object	An RO that is dedicated to Devices in a particular Domain by means of a Domain Key.
DRM Agent	The entity in the Device that manages Permissions for Media Objects on the Device.
DRM Message	An OMA DRM Release 1 term defined in [DRM]
DRM Time	A secure, non user-changeable time source. The DRM Time is measured in the UTC time scale.
Forward Lock	An OMA DRM Release 1 term defined in [DRM]
Hash Chains	A Method of derivation of Domain Keys of different Domain Generations.
Integrity	The property that data has not been altered or destroyed in an unauthorized manner. (ISO 7498-2)
Join Domain	The process of an RI including a Device in a Domain.
Leave (De-Join) Domain	The process of an RI excluding a non-revoked Device from a Domain.
Media Object	A digital work e.g. a ringing tone, a screen saver, a Java game or a Composite Obje*ct*.
Permission	Actual usages or activities allowed (by the Rights Issuer) over Protected Content (From [ODRL 1.1])
Play	To create a transient, perceivable rendition of a resource (From [MPEG21 RDD])
Protected Content	Media Objects that are consumed according to a set of Permissions in a Rights Object.
Restore	Transferring the Protected Content and/or Rights Objects from an external location back to the Device from which they were backed up.
Revoke	Process of declaring a Device or Rights Issuer certificate as invalid.
Rights Issuer	An entity that issues Rights Objects to OMA DRM Conformant Devices.
RI Context	RI Context (Rights Issuer Context) consists of information that was negotiated with a given Rights Issuer, during the 4-pass Registration Protocol such as RI ID, RI certificate chain, version, algorithms and other information. This RI Context is necessary for a Device to successfully participate in all the protocols of the ROAP suite, except the Registration Protocol.
Rights Object	A collection of Permissions and other attributes which are linked to Protected Content.
Rights Object Acquisition Protocol (ROAP)	A protocol defined within this specification. This protocol enables Devices to request and acquire Rights Objects from a Rights Issuer.
ROAP Trigger	A URL that, when received by the Device, initiates the ROAP.
Separate Delivery	A Release 1 term defined in [DRM].
Stateless Rights	Stateless Rights are Rights Objects for which the Device does not have to maintain state information. An RO containing <interval>, <count> or <accumulated> constraint is considered Stateful Rights because the Device needs to keep track of the uses of the associated content. An RO containing <export> permission is also considered Statefule Rights.
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. For example, a RO containing the <interval> constraints are considered Stateful Rights because the Device needs to keep track of the first use of the associated content.
Superdistribution	A mechanism that (1) allows a User to distribute Protected Content to other Devices through potentially insecure channels and (2) enables the User of that Device to obtain a Rights Object for the superdistributed Protected Content.
Unconnected Device	An Unconnected Device is a Device that is capable of connecting to a Rights Issuer via a Connected Device using an appropriate protocol over a local connectivity technology. E.g. OBEX over IrDA, Bluetooth or USB. An Unconnected Device may support DRM Time.
User	The human user of a Device. The User does not necessarily own the Device.

3.3 Abbreviations

3GPP	3rd Generation Partnership Project
3GPP PSS	3rd Generation Partnership Project Packet-switched Streaming Service
CA	Certification Authority
CEK	Content Encryption Key
CI	Content Issuer

DCF	DRM Content Format
DD	Download Descriptor
DRM	Digital Rights Management
GUID	Globally Unique Identifier
HTTP	HyperText Transfer Protocol
ISO	International Standards Organization
IMSI	International Mobile Subscriber Identity
LAN	Local Area Network
ME	Mobile Equipment
MMS	Multimedia Messaging Service
MPEG	Moving Picture Expert Group
OMA	Open Mobile Alliance
OMNA	Open Mobile Naming Authority (see http://www.openmobilealliance.org/tech/omna/index.htm)
OCSP	Online Certificate Status Protocol
OTA	Over The Air (i.e. transfer over a wireless connection)
PC	Personal Computer
PDA	Personal Digital Assistant
PDCF	Packetized DRM Content Format
PDU	Protocol Data Unit
PKI	Public Key Infrastructure
PKC	Public Key Certificate
PKC-ID	PKC Identifier: the hash of the Public Key Certificate
PSS	Probabalistic Signature Scheme
REK	Rights Encryption Key
RFC	Request For Comments
RI	Rights Issuer
RO	Rights Object
ROAP	Rights Object Acquisition Protocol
RSA	Rivest-Shamir-Adelman public key algorithm
SCR	Static Conformance Requirement
SHA-1	Secure Hash Algorithm
SIM	Subscriber Identity Module
SMIL	Synchronized Multimedia Integration Language
USIM	Universal Subscriber Identity Module
SMS	Short Messaging Service
TLS	Transport Layer Security
UA	User Agent
URI	Uniform Resource Indicator
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
WIM	Wireless Identity Module
WLAN	Wireless Local Area Network

4. Introduction

There is a growing need for a rights management system in the mobile industry so that the operators and content providers can make digital content available to consumers in a controlled manner. Digital Rights Management is a set of technologies that provide the means to control the distribution and consumption of the digital media objects. OMA has already published release 1 of the DRM specifications. The release 1 specifications provide some fundamental building blocks for a DRM system. But, they lack the complete security necessary for a robust, end-to-end DRM system that takes into account the need for secure distribution, authentication of Devices, revocation and other aspects. This specification addresses these missing aspects of the OMA DRM.

The OMA DRM enables content providers to grant permissions for media objects that define how they should be consumed. The DRM system is independent of the media object formats and the given operating system or run-time environment. The media objects controlled by the DRM can be of a wide variety: games, ring tones, photos, music clips, video clips, streaming media, etc. A content provider can grant appropriate permissions to the user for each of these media objects. The content is distributed with cryptographic protection; hence, the Protected Content is not usable without the associated Rights Object on a Device. Given this fact, fundamentally, the users are purchasing permissions embodied in Rights Objects and the Rights Objects need to be handled in a secure and un-compromising manner.

The Protected Content can be delivered to the Device by any means (over the air, LAN/WLAN, local connectivity, removable media, etc.). But the Rights Objects are tightly controlled and distributed by the Rights Issuer in a controlled manner. The Protected Content and Rights Objects can be delivered to the Device by downloading them together, or by sending them separately. The system does not imply any order or “bundling” of these two objects. It is not within the scope of the DRM system to address the specific payment methods employed by the Rights Issuers.

This specification is one part of a set of specifications developed by OMA to address the need for digital rights management. For a detailed discussion of the overall system architecture, please refer to [DRMARCH-v2]. And, for a detailed discussion of the Rights Expression Language that is used to construct the Rights Objects, please refer to [DRMREL-2]. The DRM Content Format is specified in the [DRMDCF-2] specification.

This specification defines the format and semantics of the cryptographic protocol, messages, processing instructions and certificate profiles that will, together enable an end-to-end system for protected content distribution. Section 5 specifies the Rights Object Acquisition Protocol messages, message syntax and processing instructions. Section 6 describes the Key Management protocols utilized in this specification. Section 7 describes the domains functionality – sharing of content and rights among a set of Devices enrolled into a Domain. The specific issues surrounding the processing of Domain keys, Domain RO processing rules, and the Domain upgrade implications are discussed here. Section 8-16 deal with the various other aspects of this system: super distribution, transport mappings for ROAP, binding rights to user identities, & exporting to other DRMs. Finally, the appendices describe the certificate profiles, application to other sevices and related normative as well as informative topics.

5. The Rights Object Acquisition Protocol (ROAP) Suite

5.1 Overview

The Rights Object Acquisition Protocol (ROAP) is the common name for a suite of DRM security protocols between a Rights Issuer (RI) and a DRM Agent in a Device. The protocol suite contains a 4-pass protocol for registration of a Device with an RI and two protocols by which the Device requests and acquires Rights Objects (RO). The 2-pass RO acquisition protocol encompasses request and delivery of an RO whereas the 1-pass RO acquisition protocol is only a delivery of an RO from an RI to a Device (e.g. messaging/push). The ROAP suite also includes 2-pass protocols for Devices joining and leaving a Domain; the Join Domain protocol and the Leave Domain protocol.

5.1.1 The 4-pass Registration Protocol

The Registration protocol is a complete security information exchange and handshake between the RI and the Device and is generally only executed at first contact, but may also be executed when there is a need to update the exchanged security information, or when DRM Time in the Device is deemed inaccurate by the Rights Issuer. This protocol includes negotiation of protocol parameters and protocol version, crytptographic algorithms, exchange of certificate preferences, optional exchange of certificates, mutual authentication of Device and RI, integrity protection of protocol messages and optional Device DRM Time synchronization.

Successful completion of the Registration protocol results in the establishment of an RI Context in the Device containing RI-specific security related information such as agreed protocol parameters, protocol version, and certificate preferences. An RI Context is necessary for execution of the other protocols in the ROAP suite: to acquire and install Device ROs and to join/leave Domains.

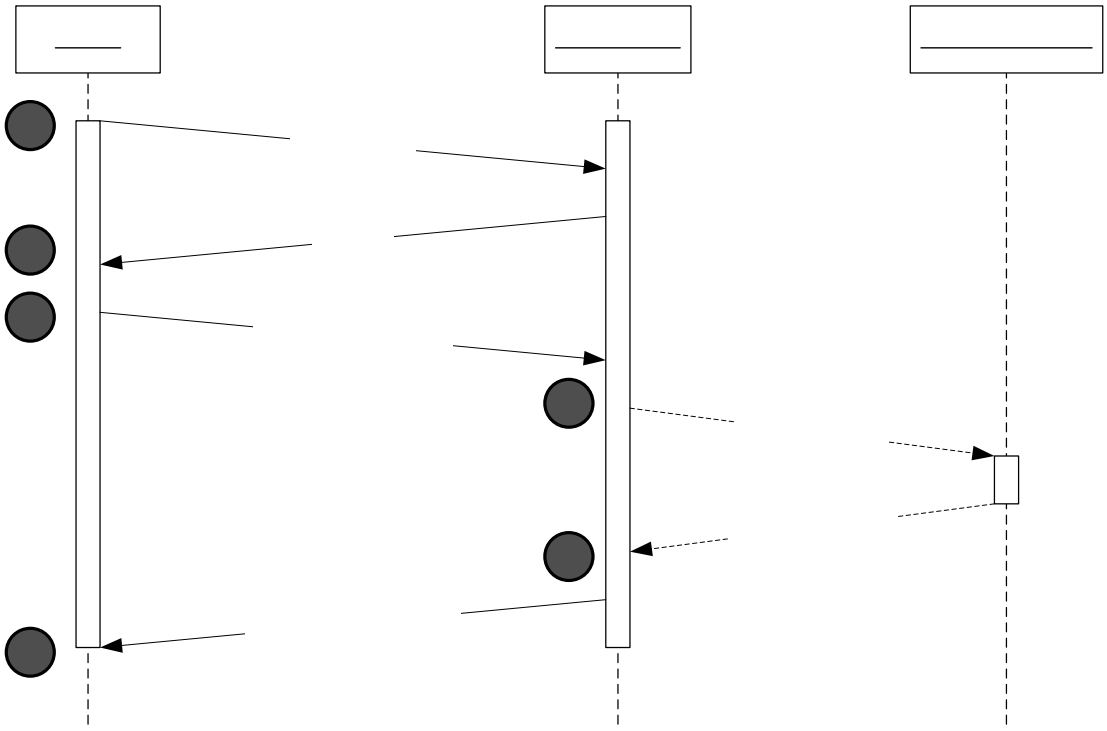

Figure 1: The 4-pass Registration Protocol

As indicated in the figure above, the RI may optionally perform a nonce-based OCSP request for its own certificate (using a nonce supplied by the Device) during the registration protocol, and then provide the Device with the returned OCSP response. The RI will perform this nonce-based OCSP request if it determines that the Device DRM Time is inaccurate. A Device will then be able to adjust its DRM Time based on the time in the OCSP response. If the Device is an Unconnected Device that does not support DRM Time, the RI MUST perform a nonce-based OCSP request for its own certificate (using a nonce supplied by the Device) during the registration protocol. An Unconnected Device might not support DRM Time because it is considered too onerous for a limited functionality Device, but, in order to maximize the security of the overall OMA DRM Version 2 system, implementers are encouraged to implement Unconnected Devices supporting DRM Time whenever possible.

5.1.2 The 2-pass Rights Object Acquisition Protocol

The 2-pass RO acquisition protocol is the protocol by which the Device acquires Rights Objects. This protocol includes mutual authentication of Device and RI, integrity-protected request and delivery of ROs, and the secure transfer of cryptographic keying material necessary to process the RO. The successful execution of this protocol assumes the Device to have a pre-established RI Context with the RI.

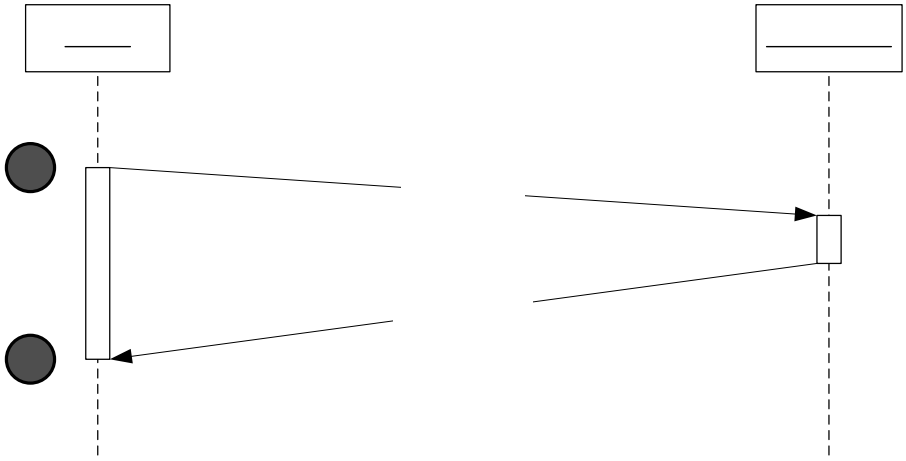

Figure 2: The 2-pass Rights Object Acquisition Protocol

5.1.3 The 1-pass Rights Object Acquisition Protocol

The 1-pass RO acquisition protocol is designed to meet the messaging/push use case. Its successful execution assumes the Device to have an existing RI Context with the sending RI. In contrast to the 2-pass RO acquisition protocol, it is initiated unilaterally by the RI and requires no messages to be sent by the Device. One use case is distribution of Rights Objects at regular intervals, e.g. supporting a content subscription. The 1-pass protocol is essentially the last message of the 2-pass variant.

Figure 3: The 1-pass Rights Object Acquisition Protocol

5.1.4 The 2-pass Join Domain Protocol

The Join Domain protocol is a Device initiated request/response protocol whereby a Device requests to join an RI-defined Domain and receives in the response the Domain Key and other information needed to share ROs in this Domain (if successful) or an error message (if not successful). The protocol assumes an existing RI context with the RI.

Successful completion of the Join Domain protocol results in the establishment of a Domain Context in the Device containing Domain-specific security related information including a Domain Key. A Domain Context is necessary for the Device to be able to install and utilize Domain ROs.

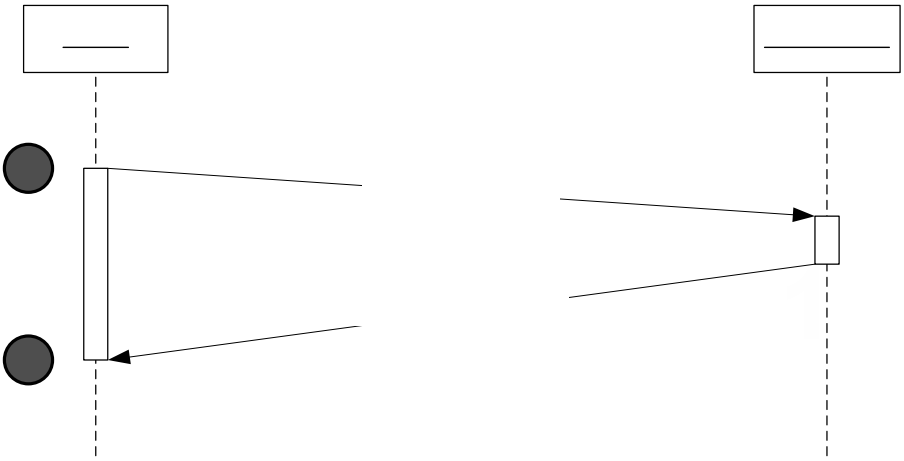

Figure 4: The 2-pass Join Domain Protocol

5.1.5 The 2-pass Leave Domain Protocol

The Leave Domain protocol is a Device initiated request/response protocol whereby a Device that has removed a Domain Context sends a request to the RI to update the Domain membership status, and receives confirmation from the RI that it has updated the Domain membership status or an error message.

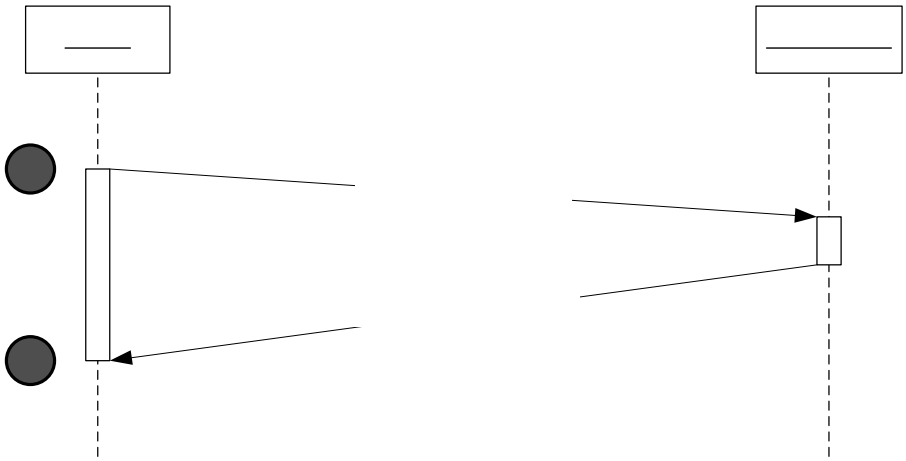

Figure 5: The 2-pass Leave Domain Protocol

5.1.6 The ROAP Trigger

Device

All protocols included in the ROAP suite except the 1-pass RO acquisition protocol are initiated using a ROAP Trigger. The Rights Issuer sends the ROAP Trigger to the Device to trigger a ROAP protocol exchange. When the Device receives the ROAP Trigger it immediately initiates the ROAP protocol exchange. An appropriate user consent MUST have been obtained prior to initiating any ROAP protocols as a result of a ROAP Trigger. Since the ROAP comprises several protocols, the ROAP Trigger includes an indication of the actual protocol (Registration, RO acquisition, Join Domain, or Leave Domain) to be started by the Device.

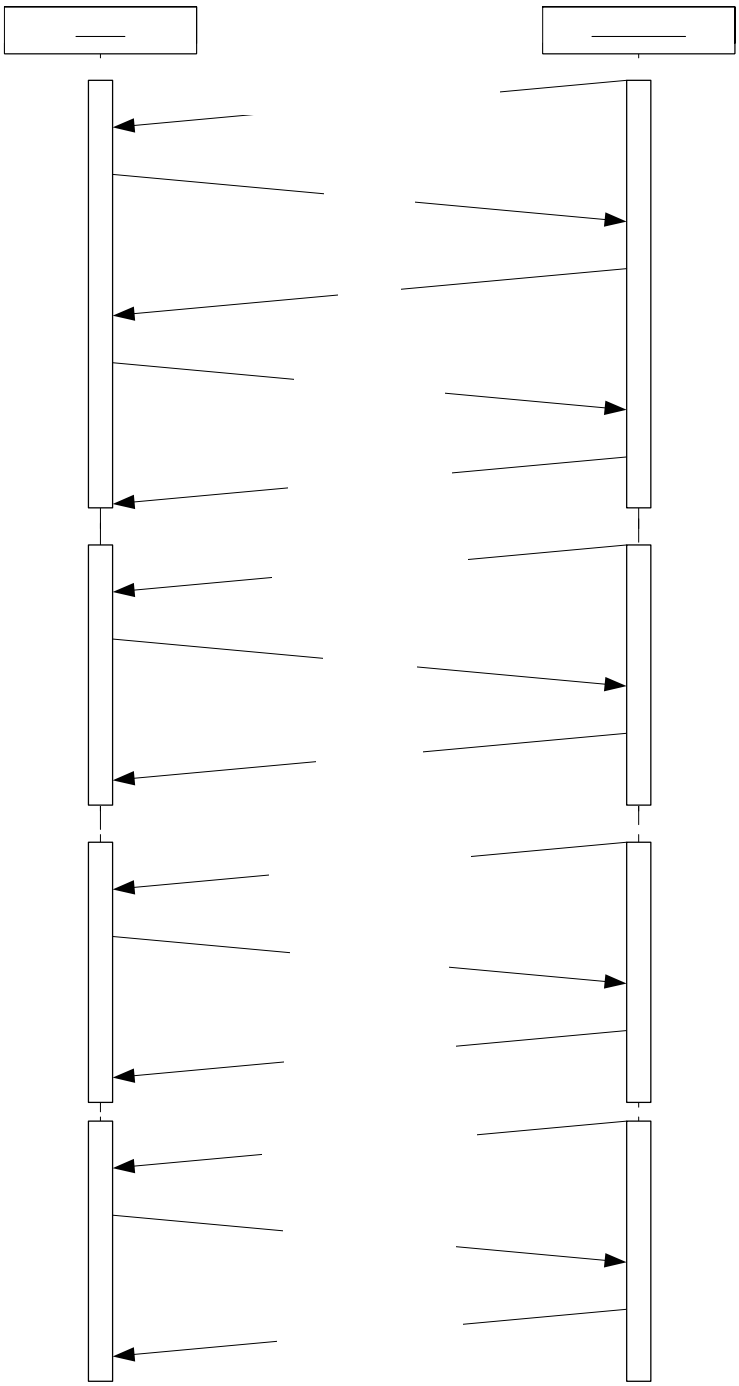

Figure 6: ROAP Trigger

5.2 Initiating the ROAP

As discussed in section 5.1.6, the protocols in the ROAP suite (except for the 1-pass ROAP-ROResponse) are initiated when the ROAP Trigger XML document is received by the Device, or when the Device receives a DCF with a Silent or Preview headers.

5.2.1 The ROAP Trigger

When the ROAP Trigger is received, the Device must initiate an appropriate ROAP protocol as described in this section.

The MIME type for the ROAP Trigger is “application/vnd.oma.drm.roap-trigger+xml”.

The schema for the ROAP Trigger is as follows:

```
<schema
 targetNamespace="urn:oma:bac:dldrm:roap-trigger-20040420"
 xmlns="http://www.w3.org/2001/XMLSchema"
 xmlns:roap-trigger="urn:oma:bac:dldrm:roap-trigger-20040420"
 xmlns:roap="urn:oma:bac:dldrm:roap-1.0"
 xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
 xmlns:xenc=http://www.w3.org/2001/04/xmlenc#
 elementFormDefault="unqualified"
 attributeFormDefault="unqualified">

<import namespace="urn:oma:bac:dldrm:roap-1.0" schemaLocation="roap.xsd"/>

<import namespace="http://www.w3.org/2000/09/xmldsig#"
      schemaLocation="http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/xmldsig-core-
schema.xsd"/>

<import namespace="http://www.w3.org/2001/04/xmlenc#"
      schemaLocation="http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/xenc-schema.xsd"/>

<complexType name="RegistrationRequestTrigger">
 <sequence>
  <element name="riID" type="roap:Identifier"/>
  <element name="roapURL" type="anyURI"/>
 </sequence>
 <attribute name="id" type="ID"/>
</complexType>

<complexType name="ROAcquisitionTrigger">
 <sequence>
  <element name="riID" type="roap:Identifier"/>
  <element name="roapURL" type="anyURI"/>
  <element name="domainID" type="roap:DomainIdentifier"
        minOccurs="0"/>
  <element name="roID" type="ID" maxOccurs="unbounded"/>
 </sequence>
 <attribute name="id" type="ID"/>
</complexType>

<complexType name="DomainTrigger">
 <sequence>
  <element name="riID" type="roap:Identifier"/>
  <element name="roapURL" type="anyURI"/>
  <element name="domainID" type="roap:DomainIdentifier"/>
 </sequence>
 <attribute name="id" type="ID"/>
</complexType>

<!-- ROAP trigger -->
<element name="roapTrigger" type="roap-trigger:RoapTrigger"/>
```

```
<complexType name="RoapTrigger">
  <annotation>
    <documentation xml:lang="en">
      Message used to trigger the device to initiate a Rights Object Acquisition Protocol.
    </documentation>
  </annotation>
  <sequence>
    <choice>
      <element name="registrationRequest" type="roap-trigger:RegistrationRequestTrigger"/>
      <element name="roAcquisition" type="roap-trigger:ROAcquisitionTrigger"/>
      <element name="joinDomain" type="roap-trigger:DomainTrigger"/>
      <element name="leaveDomain" type="roap-trigger:DomainTrigger"/>
    </choice>
    <element name="mac" type="ds:SignatureType" minOccurs="0"/>
    <element name="encKey" type="xenc:EncryptedKeyType" minOccurs="0"/>
  </sequence>
  <attribute name=”proxy” type=”Boolean”/>
</complexType>
</schema>
```

The **<riID>** element MUST uniquely identify the Rights Issuer. For triggers besides the **<registrationRequest>**, the DRM Agent MUST use this value to verify that it has a valid RI Context with the Rights Issuer. If the DRM Agent does not have a valid RI Context with the identified Rights Issuer then the DRM Agent MUST initiate the Registration Protocol before initiating the protocol indicated in the **<roapTrigger>** element.

The **<domainID>** element MAY be included in certain ROAP triggers. If included, the Device MUST incorporate the **<domainID>** in the ROAP PDU that is sent in response to the trigger.

One or several **<roID>** elements MAY be included in the **<roAcquisition>** trigger to identify the ROs to be acquired. The RI MAY specify more than one **<roID>** element to initiate download of multiple ROs. The DRM Agent MUST include all received <**roID**> elements in the **<roInfo>** portion of the subsequent ROAP-RORequest PDU.

If present the ***proxy*** attribute indicates that the ROAP Trigger is not for the Connected Device but is intended for an Unconnected Device. Upon receipt of a ROAP Trigger containing the ***proxy*** attribute with the value set to “**true**” a Connected Device that supports the functionality to provide connectivity for Unconnected Devices (as specified in section 14) MUST start the procedures specified in section 11.5.4. If the ***proxy*** attribute is present but the value is set to “**false**” then Connected Devices MUST treat the ROAP Trigger as if it did not contain the ***proxy*** attribute.

The DRM Agent MUST use the URL specified by the **<roapURL>** element when initiating the ROAP transaction. The **<roapURL>** is used in conjuction with the protocol indicated in the **<roapTrigger>** element as described below to determine which ROAP PDU to send:

- If the **<roapTrigger>** element carries a **<registrationRequest>** element, the PDU MUST be a ROAP-DeviceHello PDU.
- If the **<roapTrigger>** element carries an **<roAcquisition>** element, the PDU MUST be a ROAP-RORequest PDU.
- If the **<roapTrigger>** element carries a **<joinDomain>** element, the PDU MUST be a ROAP-JoinDomain PDU.
- If the **<roapTrigger>** element carries a **<leaveDomain>** element, the PDU MUST be a ROAP-LeaveDomain PDU.

In the case where a DRM Agent receives a ROAP Trigger where the **<roapTrigger>** element carries a **<registrationRequest>** element, the DRM Agent MUST use the value of the **<riID>** element to verify that it has a valid RI Context with the Rights Issuer. If the DRM Agent does not have a valid RI Context with the identified Rights Issuer then the DRM Agent MUST have user consent to connect to the RI. If the DRM Agent has a valid

RI Context with the identified Rights Issuer then the DRM Agent MUST send a ROAP-DeviceHello PDU, this MAY be without acquiring consent from the user.

The Rights Issuer MAY authenticate the ROAP Trigger by including a MAC of the trigger in the **<mac>** element. The RI MUST include a **<mac>** element if a **<leaveDomain>** element is present. If a MAC is included in the ROAP Trigger, the Device MUST verify it prior to initiating the ROAP. If the Device cannot verify the MAC, the Device SHOULD inform the user and MUST discard the ROAP Trigger. Likewise, a Device SHOULD inform the user and MUST discard any unauthenticated ROAP Triggers containing a **<leaveDomain>** element.

The **<ds:Reference>** element of the **<ds:SignedInfo>** child element of the **<mac>** shall reference a **DomainTrigger** element by using the same value for the **URI** attribute as the value for the ROAP Trigger's ***id*** attribute. The **<ds:KeyInfo>** child element of the **<mac>** element shall use its ***URI*** attribute of the **<ds:RetrievalMethod>** element to reference a wrapped MAC key in the **<encKey>** element.

The **<encKey>** element shall be present when the **<mac>** element is present and shall, in the case of a "LeaveDomain" ROAP trigger, contain a MAC key wrapped with the current Domain key. The value of the ***Id*** attribute of this element shall equal the value of the ***URI*** attribute of the **<ds:RetrievalMethod>** child element of the **<mac>** element as specified above.

A Connected Device MUST support HTTP for transporting ROAP PDUs as described in section 11.1.

Connected Devices MAY support other ROAP transport mappings. Additionally Connected Devices MAY support the functionality to provide connectivity for an Unconnected Device as described in section 14.

An Unconnected Device SHALL support the functionality to use connectivity provided by a Connected Device, as described in section 14.

5.2.2 Silent and Preview Headers

If the DRM Agent receives a DCF with a Silent header with a specified silent-url or a Preview header with method “preview-rights” and a specified preview URL, the DRM Agent MUST behave as follows:

If the DRM Agent does not already have a valid RI Context with the RI, as indicated by the riID in the DCF headers, the DRM Agent MUST not attempt to silently acquire the RO for the DCF but MUST obtain user consent prior to acquiring an RO for the DCF. Once the user has given consent, the DRM Agent MUST send a ROAP-DeviceHello to the indicated URL to complete the registration and establish a valid RI Context. Subsequently, the Device MUST attempt to acquire the Rights Object by sending a ROAP-RORequest to the indicated URL

If the DRM Agent does already have an RI Context with the RI that issued the DCF, as indicated by the riID, the DRM Agent MUST compare the domain name of the specified URL with the list of authorized domain names already stored by the DRM Agent for that RI. The DRM Agent MUST be capable of extracting a fully qualified domain name from URLs that follow the format defined in RFC2396. For the purpose of domain name comparison, the DRM Agent MUST use the mechanism described in Section 1 of [RFC 2965]. If the domain name in the specified URL is in the list of authorized domain names already stored by the DRM Agent for that RI, the DRM Agent MUST silently attempt to acquire the RO for the DCF by sending RO-Request to the specified URL. If the domain name in the specified URL is not in the list of authorized domain names stored by the DRM Agent for that RI, the DRM Agent MUST not attempt to silently acquire the RO for the DCF but MUST ask the user if they wish to acquire an RO for the DCF. If the user agrees, the DRM Agent MUST send an RO-Request to the indicated URL. If the user does not agree, the DRM Agent MUST not attempt to acquire an RO for the DCF. The DCF does not have to be deleted at this point.

If this RO request cannot be reconciled to a prior purchase transaction, the RI server MUST return an error. The Device can take further action based on this error indication. In this case, if the context is a user-initiated session, it is recommended that the Device start a browsing session with the RI URL. If the context is a DRM- Agent initiated session to acquire rights silently and automatically, then it is better for the client to abandon the rights acquisition effort.

On any occasion where the DRM Agent successfully retrieves and installs a RO acquired as a result of a Silent header or Preview header (with method preview-rights) in a DCF, the DRM Agent MUST add the domain name in the URL in the Silent or Preview header to the list of authorized domain names for that RI, if the domain name is not already present. As specified in section 5.4.2.4, a DRM Agent must be capable of storing a minimum of 5

domain names for each RI Context. In the case where a new domain name is to be added to the list and the number of domain names is currently equal to 5 then the last domain name SHOULD be deleted. The remaining domain names each at position x, SHOULD be moved to position x=x+1 and the new domain name to be added SHOULD be stored in the first position.

5.3 ROAP XML Schema Basics

5.3.1 Introduction

Core parts of the XML schema for ROAP, found in Appendix A, are explained in this section. Specific protocol message elements are defined in the Section 5.4. Examples are found in Appendix B.

The XML format for ROAP messages have been designed to be extensible. However, it is possible that the use of extensions will harm interoperability and therefore any use of extensions should be carefully considered.

XML Types defined in this sub-section are not ROAP messages; rather they provide building blocks that are used by ROAP messages.

5.3.2 A note on comparison of ROAP values

Some ROAP exchanges rely on the parties being able to compare received values with stored values. Unless otherwise noted, all elements in this document that have the XML Schema "string" type, or a type derived from it, MUST be compared using an exact binary comparison. In particular, ROAP implementations MUST NOT depend on case-insensitive string comparisons, normalization or trimming of white space, or conversion of locale-specific formats such as numbers.

The ROAP specification does not define a collation or sorting order for attributes or element values. ROAP implementations MUST NOT depend on specific sorting orders for values.

5.3.3 The Request type

All ROAP requests are defined as extensions to the abstract **Request** type.

```
<complexType name="Request" abstract="true"/>
```

5.3.4 The Response type

All ROAP responses are defined as extensions to the abstract **Response** type. The elements of the **Response** type therefore apply to all ROAP responses. All responses contain a ***status*** attribute that indicates whether the preceding request was successful or not. Responses MAY optionally include a ***riURL*** attribute that indicates the URL that the Device SHOULD use in a subsequent ROAP session that is triggered as a result of receiving a specific error message. In the case of a ROAP-RegistrationResponse message the ***riURL*** attribute indicates the URL that MUST be stored in the RI Context. The value of the ***riURL*** attribute MUST be a URL according to [RFC2396], and MUST be an absolute identifier.

```
<complexType name="Response" abstract="true">
   <attribute name="status" type="roap:Status" use="required"/>
   <attribute name=”riURL” type=”anyURI”/>
</complexType >
```

5.3.5 The Status type

The **Status** simple type enumerates all possible error messages.

```
<simpleType name="Status">
                <restriction base="string">
                                <enumeration value="Success"/>
                                <enumeration value="UnknownError"/>
```

```
                        <enumeration value=”Abort”/>
                        <enumeration value="NotSupported"/>
                        <enumeration value="AccessDenied"/>
                        <enumeration value="NotFound"/>
                        <enumeration value="MalformedRequest"/>
                        <enumeration value="UnknownRequest"/>
                        <enumeration value="UnknownCriticalExtension"/>
                        <enumeration value="UnsupportedVersion"/>
                        <enumeration value="UnsupportedAlgorithm"/>
                        <enumeration value="NoCertificateChain"/>
                        <enumeration value="InvalidCertificateChain"/>
                        <enumeration value="TrustedRootCertificateNotPresent"/>
                        <enumeration value=”SignatureError”/>
                        <enumeration value="DeviceTimeError"/>
                        <enumeration value="NotRegistered"/>
                        <enumeration value="InvalidDCFHash"/>
                        <enumeration value="InvalidDomain"/>
                        <enumeration value="DomainFull"/>
                </restriction>
</simpleType>
```

Upon transmission or receipt of a message for which Status is not "Success", the default behaviour, unless explicitly stated otherwise below, is that both the RI and the Device SHALL immediately close the connection and terminate the protocol. RI systems and Devices are required to delete any session-identifiers, nonces, keys, and/or secrets associated with a failed run of the ROAP protocol.

When possible, the Device SHOULD present an appropriate error message to the user.

UnknownError indicates an internal RI system error.

Abort indicates that the RI rejected the Device’s request for unspecified reasons.

NotSupported indicates the Device made a request for a feature currently not supported by the RI.

AccessDenied indicates that the Device is not authorized to contact this RI.

NotFound indicates that the requested object was not found.

MalformedRequest indicates that the RI failed to parse the Device's request.

UnknownRequest indicates that the RI did not recognize the request type.

UnknownCriticalExtension indicates that a critical ROAP extension used by the Device was not supported or recognized by the RI.

UnsupportedVersion indicates that the Device used a ROAP protocol version not supported by the RI.

UnsupportedAlgorithm indicates that the Device suggested algorithms that are not supported by the RI (this error should not occur as long as all Devices and all RIs implement the mandatory algorithms).

NoCertificateChain indicates that the RI could not verify the signature on a Device request due to not having access to the Device's certificate chain.

InvalidCertificateChain indicates that the RI could not verify the signature on a Device request due to the certificate chain being invald in some way (other than the absence of a trusted root certificate which could be used to verify the chain)

TrustedRootCertificateNotPresent indicates that the RI could not verify the signature on a Device request due to the absence of a trusted root certificate which could be used to verify the chain.

SignatureError indicates that the RI could not verify the Device's signature.

DeviceTimeError indicates that a Device request was invalid due to the Device DRM Time being inaccurate as assessed by the Rights Issuer. The Device SHOULD initiate the 4-pass Registration protocol, using the ***riURL*** as indicated in the riURL attribute of the ROAP-Response message in which this error was sent. If this attribute is not

present then the Device MAY use the ***riURL*** as stored in the RI Context. The Device MUST have user consent to contact the RI, in the same way as for processing ROAP triggers as specified in section 5.2.1.

NotRegistered indicates that the Device tried to contact an RI with which it has not completed a valid registration. The RI SHOULD include the ***riURL*** attribute in the ROAP-Response message in which this error code is sent. The Device SHOULD initiate the 4-pass Registration protocol, using the ***riURL*** attribute of the ROAP-Response message in which this error was sent. The Device MUST have user consent to contact the RI, in the same way as for processing ROAP triggers as specified in section 5.2.1.

InvalidDCFHash is sent when the RI detects an incorrect DCF hash value in a ROAP-RORequest message.

InvalidDomain indicates that the request was invalid due to an unrecognized Domain Identifier.

DomainFull indicates that no more Devices are allowed to join the Domain.

Upon transmission or receipt of a message for which Status is not "Success", both the sending and the receiving parties shall immediately close the connection and terminate the protocol. RI systems and Devices are required to forget any session-identifiers, nonces, keys, and/or secrets associated with a failed run of the ROAP protocol.

5.3.6 The Extensions type

The **Extensions** type is a list of type-value pairs that define optional ROAP features supported by a Device or an RI. Extensions may be sent with any ROAP message. Please see Section 5.4in this document for applicable extensions. Unless an extension is marked as critical, a receiving party need not be able to interpret it, and a receiving party is always free to disregard any (non-critical) extensions.

```
<complexType name="Extensions">
  <sequence maxOccurs="unbounded">
    <element name="extension" type="roap:Extension"/>
  </sequence>
</complexType>

<complexType name="Extension" abstract="true">
  <attribute name="critical" type="boolean"/>
</complexType>
```

5.3.7 The Protected Rights Object type

The **ProtectedRO** type is a sequence of an **<ro>** element of type **roap:ROPayload** and a **<mac>** element carrying a MAC value over the **<ro>** element. The ProtectedRO type is used to carry protected Rights Objects in: 1) ROAP-ROResponse messages and 2) Domain ROs when sent in DCFs or separately.

```
<!-- May be sent standalone (domain ROs) -->
<element name="protectedRO" type="roap:ProtectedRO"/>

<complexType name="ProtectedRO">
  <sequence>
    <element name="ro" type="roap:ROPayload"/>
    <element name="mac" type="ds:SignatureType"/>
  </sequence>
</complexType>
```

The **<ro>** element is described in the next section.

The **<mac>** element provides integrity of the **<ro>** element and key confirmation. The MAC is calculated over the complete **<ro>** element. Before the MAC calculation, the **<ro>** element SHALL be canonicalized using the [XC14N] canonicalization method. The ***URI*** attribute of the **<ds:Reference>** element of the **<ds:SignedInfo>** child element of the **<mac>** SHALL reference the **<ro>** element by having the same value as the ***id*** attribute of the **<ro>** element. The ***URI*** attribute of the **<ds:RetrievalMethod>** element of the **<ds:KeyInfo>** child element of

the **<mac>** SHALL reference a wrapped MAC key in the **<ro>** element's **<encKey>** child element by having the same value as the ***Id*** attribute of the **<encKey>** element.

In the case of a Domain RO, the **<ProtectedRO>** element can be shared between Devices either sent as a standalone message or inserted into a DCF. When sent standalone, its MIME type SHALL be `application/vnd.oma.drm.pro+xml`.

5.3.8 The Rights Object Payload type

Values of the **ROPayload** type carries (protected) REL elements and wrapped keys that can be used to decrypt encrypted portions of the REL elements.

```
<!-- Rights Object Definitions -->
<complexType name="ROPayload">
  <sequence>
    <element name="riID" type="roap:Identifier"/>
    <element name="rights" type="o-ex:rightsType"/>
    <element name="signature" type="ds:SignatureType" minOccurs="0"/>
    <element name="timeStamp" type="dateTime" minOccurs="0"/>
    <element name="encKey" type="xenc:EncryptedKeyType"/>
  </sequence>
  <attribute name="version" type="roap:Version" use="required" />
  <attribute name="id" type="ID" use="required" />
  <attribute name="stateful" type="boolean"/>
  <attribute name="domainRO" type="boolean"/>
  <attribute name="riURL" type="anyURI"/>
</complexType>
```

The **<riID>** element is of type **roap:Identifier** and SHALL identify the issuing RI.

The **<rights>** element is of type **o-ex:rightsType** and MUST be conformant with [DRMREL-v2]. The ***o-ex:id*** attribute of this type SHALL be present.

The **<signature>** element is of type **ds:SignatureType** from [XMLDsig] and MUST be present when the RO is a Domain RO. The ***URI*** attribute of a **<ds:Reference>** element of the **<ds:SignedInfo>** child element of the **<signature>** SHALL reference the **<rights>** element by having the same value as the ***o-ex:id*** attribute of the **<rights>** element (i.e., when present, the signature SHALL be made at least over the **<rights>** element). All signed elements SHALL be canonicalized using the exclusive canonicalization method defined in [XC14N] before carrying out the signature operation. The **<ds:KeyInfo>** child element of the **<signature>** element SHALL identify the signing key. The Device MUST verify that the signing key is associated with the RI identified in the **<riID>** element.

The **<timeStamp>** value MUST be given in Universal Coordinated Time (UTC). The time-stamp provides replay protection, see further in section 9.4.

The **<encKey>** element is of type **xenc:EncryptedKeyType** from [XMLEnc]. It consists of a wrapped concatenation of a MAC key, K_{MAC} and an RO encryption key, K_{REK}. The ***Id*** attribute of this element SHALL be present and SHALL have the same value as the value of the ***URI*** attribute of the **<ds:RetrievalMethod>** element in any **<ds:KeyInfo>** elements inside the **<rights>** element. The **<ds:KeyInfo>** child element of the **<encKey>** element SHALL identify the wrapping key. In the case of a Rights Object intended for a Device, the child of the **<ds:KeyInfo>** element SHALL be of type **roap:X509SPKIHash**, identifying a particular DRM Agent's public key through the (SHA-1) hash of the DER-encoded subjectPublicKeyInfo value in its certificate. In the case of a Rights Object intended for a Domain, it will be of the type **roap:DomainIdentifier**, identifying the correct Domain key. Note that the encrypted key material consists of ***two*** keys - a MAC key and a Rights Object Encryption key. For further information, see the Key Management discussion in section 7.

The ***version*** attribute indicates the version of the ROPayload type. For this version of the OMA DRM specification, the value SHALL be "1.0". Minor version upgrades must always be backwards compatible. The ROPayload version must not be confused with the OMA DRM version, which is independently set. The reason for

having different versions is to enable Domain ROs to be shared between Devices with different OMA DRM protocol versions.

The ***id*** attribute of the **ROPayload** type identifies the RO and will, when applicable, correspond to an **<roID>** value in a previous ROAP-RORequest. The ***id*** attribute is also used as a reference point for the MAC as described in the previous section.

The ***stateful*** attribute, when present and set to "**true**", indicates that the RO contains stateful rights (i.e. needs replay protection). The ***id*** attribute MUST be globally unique when this attribute is present and set to true, in order to enable a Device to correctly enforce replay protection (Note: one way for an RI to generate globally unique identifiers is to combine an RI-unique and freshly generated nonce with the hash of the RI's public key). If the ***stateful*** attribute is not present, or is set to "**false**", then the RI does not regard the RO as stateful.

The ***domainRO*** attribute, when present and set to "**true**", indicates that the RO is for a Domain. If the ***domainRO*** attribute is not present, or is set to "**false**", then the RO is for a particular Device.

The ***riURL*** attribute, if present, SHALL contain a URL that the Device can use to contact the RI, for example, to register with the RI or to join a Domain (as specified in section 8.6.2.1) indicated in a **roap:DomainIndentifier** element. The value of the ***riURL*** MUST be a URL according to [RFC2396], and MUST be an absolute identifier. If the Device utilizes the ***riURL*** for registration purposes, the Device MUST have user consent to contact the RI, in the same way as the requirement for processing ROAP triggers as specified in section 5.2.1.

5.3.9 The Nonce type

The Nonce type is used to carry arbitrary values in the ROAP protocol messages. Nonce, as the name implies, must be used only once. For each ROAP message that requires a nonce element to be sent, a fresh nonce SHALL be generated randomly each time. Nonce values MUST be at least 14 Base64-encoded characters long (approx. 80 bits).

```
<simpleType name="Nonce">
  <restriction base="base64Binary">
    <minLength value="14"/>
  </restriction>
</simpleType>
```

5.4 ROAP Messages

In this section, ROAP protocol suite messages, including their parameters, encodings and semantics are defined. The ROAP protocol messages are divided into three categories: Registration, RO Acquisition, and Domain management.

5.4.1 Notation

In the message parameter tables below, "M" stands for "mandatory presence" and "O" stands for "optional presence".

5.4.2 Registration Protocol

5.4.2.1 Device Hello

The ROAP-DeviceHello message is sent from the Device to the Rights Issuer to initiate the 4-pass Registration protocol. This message expresses Device information and preferences.

5.4.2.1.1 Message description

Parameter	ROAP-DeviceHello
Version	M
Device ID	M
Supported Algorithms	O
Extensions	O

Table 1: Device Hello Message Parameters

Version is a <major.minor> representation of the highest ROAP version number supported by the Device. For this version of the protocol, *Version* SHALL be set to "**1.0**". Minor version upgrades must always be backwards compatible.

Device ID identifies the Device to the RI. The only identifier currently defined is the hash of the Device's public key info, as it appears in the certificate (i.e. the hash of the complete DER-encoded `subjectPublicKeyInfo` component in the Device's certificate). The default hash algorithm is SHA-1. Other identifiers are allowed but interoperability when using them is not guaranteed.

Supported Algorithms identifies the cryptographic algorithms (hash algorithms, MAC algorithms, signature algorithms, key transport algorithms and key wrap algorithms) that are supported by the Device. Algorithms are identified using common URIs. The following algorithms and associated URIs MUST be supported by all Devices and RIs:

Hash algorithms:

SHA-1: http://www.w3.org/2000/09/xmldsig#sha1

MAC algorithms:

HMAC-SHA-1: http://www.w3.org/2000/09/xmldsig#hmac-sha1

Signature algorithms:

RSA-PSS-Default: http://www.rsasecurity.com/rsalabs/pkcs/schemas/pkcs-1#rsa-pss-default

Key transport algorithms:

RSAES-KEM-KDF2-KW-AES128:

http://www.rsasecurity.com/rsalabs/pkcs/schemas/pkcs-1#rsaes-kem-kdf2-kw-aes128

Key wrapping algorithms:

AES-WRAP: http://www.w3.org/2001/04/xmlenc#kw-aes128

Use of other algorithm URIs is optional. Since all Devices and all RIs must support the algorithms above, they need not be sent. Only URIs for algorithms not in this list needs to be sent in a ROAP-DeviceHello message.

Extensions: The following extensions are defined for the ROAP-DeviceHello message:

Certificate Caching: The presence of this extension indicates to the RI that the Device has a capability to store information in the RI context whether an RI has stored Device certificate information or not. (Note: This is not about whether the Device has stored RI certificate information or not. For this, the *Peer Key Identifier* extension is used - see the ROAP-RegistrationRequest, ROAP-RORequest, and ROAP-JoinDomainRequest messages.)If the Device has this capability, then the Device MUST include the *Certificate Caching* extension. If this extension is used, the RI can use the *Peer Key Identifier* or the *Certificate Caching* extension in its ROAP-RIHello message to indicate that it has stored the Device public key or that it is capable of storing Device certificate information, respectively.

5.4.2.1.2 Message syntax

The **<deviceHello>** element specifies the ROAP-DeviceHello message, which is the first message sent in the 4-pass ROAP Registration protocol. It has complex type **roap:DeviceHello**, which extends the basic **roap:Request** type.

```
<element name="deviceHello" type="roap:DeviceHello"/>

<complexType name="DeviceHello">
  <annotation>
    <documentation xml:lang="en">
      Message sent from Device to RI to establish an RI Context.
    </documentation>
  </annotation>
  <complexContent>
    <extension base="roap:Request">
      <sequence>
        <element name="version" type="roap:Version"/>
        <element name="deviceID" type="roap:Identifier"
                 maxOccurs="unbounded"/>
        <element name="supportedAlgorithm" type="anyURI"
                 minOccurs="0" maxOccurs="unbounded"/>
        <element name="extensions" type="roap:Extensions"
                 minOccurs="0"/>
      </sequence>
    </extension>
  </complexContent>
</complexType>
```

The following schema fragment defines the **Version** type. As noted above, for this version of ROAP, its value shall be "**1.0**".

```
<simpleType name="Version">
  <restriction base="string">
    <pattern value="\d{1,2}\.\d{1,3}"/>
  </restriction>
</simpleType>
```

The following schema fragment defines the Identifier type and its alternatives. Any non-standard identifier value must be expressed in well-formed XML.

```
<complexType name="Identifier">
  <choice>
    <element name="keyIdentifier" type="roap:KeyIdentifier"/>
    <any namespace="##other" processContents="strict"/>
  </choice>
</complexType>

<complexType name="KeyIdentifier" abstract="true"/>
```

A key can be defined by use of a hash of the key. The hash shall in this case be made over the DER-encoded `subjectPublicKeyInfo` value from the applicable certificate.

```
<complexType name="X509SPKIHash">
  <complexContent>
    <extension base="roap:KeyIdentifier">
      <sequence>
        <element name="hash" type="base64Binary"/>
      </sequence>
      <attribute name="algorithm" type="anyURI" default="http://www.w3.org/2000/09/xmldsig#sha1"/>
```

```
    </extension>
  </complexContent>
</complexType>

<!-- The corresponding ds:KeyInfo element -->
<element name="X509SPKIHash" type="roap:X509SPKIHash"/>
```

The following extension is defined for the ROAP-DeviceHello message:

```
<complexType name="CertificateCaching">
  <complexContent>
    <extension base="roap:Extension"/>
  </complexContent>
</complexType>
```

5.4.2.2 RI Hello

The ROAP-RIHello message is the second message of the Registration protocol and is sent from the Rights Issuer to the Device in response to a ROAP-DeviceHello message. The message expresses RI preferences and decisions based on the values supplied by the Device.

5.4.2.2.1 Message description

Parameter	ROAP-RIHello	
	Status = "Success"	Status ≠ "Success"
Status	M	M
riURL	-	O
Session ID	M	-
Selected Version	M	-
RI ID	M	-
Selected Algorithms	O	-
RI Nonce	M	-
Trusted Device Authorities	O	-
Server Info	O	-
Extensions	O	-

Table 2: RI Hello Message Parameters

Status indicates if the ROAP-DeviceHello request was successfully (Status = *Success*) handled or not. In the latter case an error code as specified in Section 5.3.5 is sent.

riURL indicates the URL that the Device SHOULD use in a subsequent ROAP session that is triggered as a result of receiving a specific error message as specified in section 5.3.5. For the *DeviceTimeError* and *NotRegistered* error message the RI MUST include the ***riURL*** attribute in the ROAP-RIHello message.

Session ID is a protocol session identifier set by the RI. This allows for several, concurrent, RI-Device sessions. *Selected Version* is the selected ROAP version. The selected version will be *min*(Device suggested version, highest version supported by RI). This information is part of the RI Context.

RI ID identifies the RI to the Device. The only identifier currently defined is the hash of the Rights Issuer's public key info, as it appears in the certificate (i.e. the hash of the complete DER-encoded `subjectPublicKeyInfo` component in the Rights Issuer's certificate). The default hash algorithm is SHA-1. Other identifiers are allowed but interoperability when using them is not guaranteed. This information is part of the RI Context.

Selected Algorithms specifies the cryptographic algorithms (hash algorithm, signature algorithm, MAC algorithm and key transport algorithm) to use in subsequent ROAP interactions. If the Device indicated support of only

mandatory algorithms (i.e. left out the **<supportedAlgorithms>** element), then the RI need not send this field. Otherwise, the RI MUST provide this parameter and MUST identify one algorithm of each type. This information is part of the RI context.

RI Nonce is a random nonce sent by the RI. Nonces are generated and used in this message as specified in section 5.3.9.

Trusted Device Authorities is a list of Device trust anchors recognized by the RI. This parameter is optional. The parameter is not sent if the RI already has the Device's certificate or otherwise is able to verify a signature made by the Device. If the parameter is present but empty, it indicates that the Device is free to choose any Device certificate to authenticate itself. Otherwise the Device MUST choose a certificate chaining back to one of the recognized trust anchors. Trust anchors are identified in the same manner as Devices and RIs.

Server Info contains server-specific information that the Device must return unmodified, in the ROAP-RegistrationRequest. The Device must not attempt to interpret the value of this parameter. Devices MUST support the Server Info element being of length 512 bytes and MAY support Server Info elements of length greater than 512 bytes. RIs SHOULD keep Server Info length to 512 bytes or less.

Extensions: The following extensions are defined for the ROAP-RIHello message:

- *Peer Key Identifier*: An identifier for a Device public key stored by the RI. If the extension is empty or if the identifier matches the Device's current public key, it means the RI has already stored the Device ID and the corresponding Device certificate chain, and the Device need not send its certificate chain in a later request message. Keys are identified in the same way as Devices are (a hash of the DER-encoded `subjectPublicKeyInfo` component of the Device's certificate). If the RI has stored the Device public key the RI MUST use this extension in the ROAP-RIHello. This extension also informs the Device that the RI has the capability to store information about Device certificates.
- *Certificate Caching:* When present, this extension indicates to the Device that the RI has the capability to store information about the Device certificate and that Device certificate chain sending is not necessary in subsequent protocol instances once the RI has received the Device certificate chain. This extension is not needed if the *Peer Key Identifier* is used, since the latter contains even more specific information.
- *Device Details:* By including this extension, the RI requests the Device to return Device-specific information such as manufacturer and model in a subsequent ROAP-RegistrationRequest message. When present, the DeviceDetails extension SHALL be empty (i.e. <extension xsi:type="roap:DeviceDetails"/>)".

If the *Certificate Caching* extension was present in the ROAP-DeviceHello message and the RI has capabilities to store Device certificates, then the RI MUST send either the *Peer Key Identifier* or the *Certificate Caching* extension in its ROAP-RIHello message. If the *Certificate Caching* extension was not present in the ROAP-DeviceHello message, then the RI need not send the *Certificate Caching* extension in its ROAP-RIHello. If the ROAP-RIHello contains a *Peer Key Identifier* extension, it SHOULD NOT contain a *Certificate Caching* extension.

Information about the RI's capabilities to store Device certificate information is part of the RI Context. If either the *Peer Key Identifier* or the *Certificate Caching* extension is sent, the RI must store necessary information about the Device certificate and the Device will note the RI's *Certificate Caching* capability in the RI Context.

5.4.2.2.2 Message syntax

The **<riHello>** element specifies the ROAP-RIHello message, which is sent in response to the ROAP-DeviceHello message. It has complex type **roap:RIHello.**

```
<element name="riHello" type="roap:RIHello"/>

<complexType name="RIHello">
  <annotation>
    <documentation xml:lang="en">
      Message sent from RI to Device in response to a DeviceHello.
    </documentation>
  </annotation>
```

```
 <complexContent>
  <extension base="roap:Response">
   <sequence minOccurs="0">
    <element name="selectedVersion" type="roap:Version"/>
    <element name="riID" type="roap:Identifier"/>
    <element name="selectedAlgorithm" type="anyURI" maxOccurs="unbounded"
        minOccurs="0"/>
    <element name="riNonce" type="roap:Nonce"/>
    <element name="trustedAuthorities" type="roap:KeyIdentifiers" minOccurs="0"/>
    <element name="serverInfo" type="base64Binary" minOccurs="0"/>
    <element name="extensions" type="roap:Extensions" minOccurs="0"/>
   </sequence>
   <attribute name="sessionId" type="hexBinary" use="required"/>
  </extension>
 </complexContent>
</complexType>

<complexType name="KeyIdentifiers">
 <sequence minOccurs=”0” maxOccurs="unbounded">
  <element name="keyIdentifier" type="roap:KeyIdentifier"/>
 </sequence>
</complexType>
```

The following schema fragment defines the *Peer Key Identifier* extension:

```
<complexType name="PeerKeyIdentifier">
 <complexContent>
  <extension base="roap:Extension"/>
    <sequence minOccurs=”0”>
     <element name="identifier" type="roap:KeyIdentifier"/>
    </sequence>
  </extension>
 </complexContent>
</complexType>
```

The following schema fragment defines the Device Details extension:

```
<complexType name="DeviceDetails">
 <complexContent>
  <extension base="roap:Extension">
   <sequence minOccurs=”0”>
    <element name="manufacturer" type="string"/>
    <element name="model" type="string"/>
    <element name="version" type="string"/>
   </sequence>
  </extension>
 </complexContent>
</complexType>
```

5.4.2.3 Registration Request

A Device sends the ROAP-RegistrationRequest message to an RI to request registration with the RI. The message is sent as the third message in the 4-pass Registration protocol.

5.4.2.3.1 Message description

Parameter	ROAP-RegistrationRequest
Session ID	M
Device Nonce	M
Request Time	M
Certificate Chain	O
Trusted RI Authorities	O
Server Info	O
Extensions	O
Signature	M

Table 3: Registration Request Message Parameters

Session ID SHALL be identical to the *Session ID* parameter of the preceding ROAP-RIHello message, otherwise the RI shall terminate the Registration protocol.

Device Nonce is a nonce chosen by the Device. Nonces are generated and used in this message as specified in section 5.3.95.3.9.

Request Time is the current DRM Time as measured by the Device. Connected Devices and Unconnected Devices that support DRM Time MUST insert their current DRM Time.Unconnected Devices that do not support DRM Time MUST use the value “Undefined”.

Certificate Chain: This parameter MUST be present unless the preceding ROAP-RIHello message contained the *Peer Key Identifier* extension and its value identified the key in the Device's current certificate. When present, the value of a *Certificate Chain* parameter shall be a certificate chain including the Device's certificate. The chain SHALL not include the root certificate. The Device certificate must come first in the list. Each following certificate must directly certify the one preceding it. If the RI indicated trust anchor preferences in the previous ROAP-RIHello message, the Device MUST select a Device certificate and chain which chains back to one of the trust anchors indicated by the RI. This mimics the features of [RFC3546]. If the ROAP-RIHello message contained the *Peer Key Identifier* or the *Certificate Caching* extension, then the RI MUST store necessary information about the Device certificate. The RI may need to update this information based on the received Certificate Chain.

Trusted RI Authorities is a list of RI trust anchors recognized by the Device. If the parameter is empty, it indicates that the RI is free to choose any certificate. Trust anchors are identified in the same way as Devices and RIs.

Server Info: As discussed above, this parameter will only be present if a *Server Info* parameter was present in the preceding ROAP-RIHello message. In that case, the *Server Info* parameter MUST be present and MUST be identical to the *Server Info* parameter received in the preceding ROAP-RIHello message.

Extensions: The following extensions are defined for the ROAP-RegistrationRequest message:

- *Peer Key Identifier:* An identifier for an RI public key stored in the Device. If the identifier matches the RI's current public key, or if the extension is empty, it means the RI need not send down its certificate chain in its response message. Keys are identified in the same way as Devices and RIs.
- *No OCSP Response*: Presence of this extension indicates to the RI that there is no need to send an OCSP Response since the Device has cached a valid OCSP Response for this RI.
- *OCSP Responder Key Identifier*: This extension identifies an OCSP responder key stored in the Device and is used to save bandwidth. If the identifier matches the key in the certificate used by the RI's OCSP responder, the RI MAY remove the OCSP Responder certificate chain from the OCSP response before providing the OCSP response to the Device.
- *Device Details*: This extension defines three fields: manufacturer, model and version. The manufacturer field identifies the Device’ manufacturer, the model field identifies the Device's model and the version field

identifies the Device's version as defined by its manufacturer. This extension MUST be supported and MUST be sent by a Device that receives an empty *Device Details* extension in a ROAP-RIHello message.

If the Device has stored the RI public key, the Device MUST send the *Peer Key Identifier* extension. If the Device has a valid OCSP Response, the Device MUST send the *No OCSP Response* extension. If the Device has stored an OCSP responder key for this RI, the Device MUST send the *OCSP Responder Key Identifier* extension; otherwise, the Device MUST NOT use this extension.

Signature is a signature on data sent so far in the protocol. The signature is made using the Device's private key on a hash of the two previous messages (ROAP-DeviceHello, ROAP-RIHello) and all elements of this message (besides the *Signature* element itself). The signature method is as follows:

The previous messages and the current one except the *Signature* element is canonicalized using the exclusive canonicalization method defined in [XC14N].

The three messages are concatenated in their chronological order, starting with the ROAP-DeviceHello message. The resulting data *d* is considered as input to the signature operation.

The signature is calculated on *d* in accordance with the rules of the negotiated signature scheme.

The RI MUST verify the signature on the ROAP-RegistrationRequest message.

5.4.2.3.2 Message syntax

The **<registrationRequest>** element specifies the ROAP-RegistrationRequest message, which is the third message in the ROAP Registration protocol. It has complex type **roap:RegistrationRequest**, which extends the basic **roap:Request** type.

```
<element name="registrationRequest" type="roap:RegistrationRequest"/>

<complexType name="RegistrationRequest">
 <annotation>
  <documentation xml:lang="en">
   Message sent from Device to RI to request registration.
  </documentation>
 </annotation>
 <complexContent>
  <extension base="roap:Request">
   <sequence>
    <element name="nonce" type="roap:Nonce"/>
    <element name="time" type="roap:dateTimeOrUndefined"/>
    <element name="certificateChain" type="roap:CertificateChain"
          minOccurs="0"/>
    <element name="trustedAuthorities" type="roap:KeyIdentifiers"
          minOccurs="0"/>
    <element name="serverInfo" type="base64Binary" minOccurs="0"/>
    <element name="extensions" type="roap:Extensions" minOccurs="0"/>
    <element name="signature" type="base64Binary"/>
   </sequence>
   <attribute name="sessionId" type="hexBinary" use="required"/>
  </extension>
 </complexContent>
</complexType>

<simpleType name="dateTimeOrUndefined">
 <union memberTypes="dateTime roap:UndefinedString"/>
</simpleType>

<simpleType name="UndefinedString">
 <restriction base="string">
```

```
  <enumeration value="Undefined"/>
  </restriction>
</simpleType>
```

The **<time>** element expresses, in UTC, the current DRM Time as measured by the Device.The value "Undefined" is used by Unconnected Devices that do not support DRM Time.

The following schema fragment defines the **CertificateChain** type:

```
<complexType name="CertificateChain">
  <sequence maxOccurs="unbounded">
    <element name="certificate" type="base64Binary"/>
  </sequence>
</complexType>
```

The following schema fragment defines the extensions defined for the ROAP-RegistrationRequest message (besides the *Peer Key Identifier* and *Device Details* extensions already defined earlier in this document):

```
<complexType name="NoOCSPResponse">
  <complexContent>
    <extension base="roap:Extension"/>
  </complexContent>
</complexType>

<complexType name="OCSPResponderKeyIdentifier">
  <complexContent>
    <extension base="roap:Extension">
      <sequence>
        <element name="identifier" type="roap:KeyIdentifier"/>
      </sequence>
    </extension>
  </complexContent>
</complexType>
```

5.4.2.4 Registration Response

The ROAP-RegistrationResponse message is sent from the Rights Issuer to the Device in response to a ROAP-RegistrationRequest message. This message completes the Registration protocol, and if successful, enables the Device to establish an RI Context for this RI.

5.4.2.4.1 Message description

Parameter	ROAP-RegistrationResponse	
	Status = "Success"	*Status ≠ "Success"*
Status	M	M
riURL	M	O
Session ID	M	M
Certificate Chain	O	-
OCSP Response	O	-
Extensions	O	-
Signature	M	-

Table 4: Registration Response Message Parameters

Status indicates if the ROAP-RegistrationRequest message was successfully (Status = *Success*) handled or not. In the latter case an error code as specified in Section 5.3.5 is sent.

riURL: if the ROAP-RegistrationRequest message was successful (Status=Success) then the riURL parameter indicates the URL that SHOULD be stored in the RIContext. If the ROAP-RegistrationRequest message was not successful (Status≠Success) the riURL parameter indictates the URL that the Device SHOULD use in a subsequent ROAP session that is triggered as a result of receiving a specific error message as specified in section 5.3.5. For the *DeviceTimeError* and *NotRegistered* error message the RI MUST include the ***riURL*** attribute in the ROAP-RegistrationResponse message.

Session ID SHALL be identical to the *Session ID* of the preceding ROAP-RegistrationRequest (and ROAP-RIHello) message. If the Session ID of the ROAP-RegistrationResponse does not equal the Session ID of the corresponding ROAP-RIHello, the Device MUST terminate the protocol.

Certificate chain: This parameter MUST be present unless the preceding ROAP-RegistrationRequest message contained the *Peer Key Identifier* extension, the extension was not ignored by the RI, and its value identified the RI's current key. When present, the value of a *Certificate Chain* parameter shall be a certificate chain including the RI's certificate. The chain MUST NOT include the root certificate. The RI certificate must come first in the list. Each following certificate must directly certify the one preceding it. If the Device indicated trust anchor preferences in its ROAP-RegistrationRequest message, the RI SHOULD select a certificate and chain which chains back to one of the trust anchors in the Device's list. This mimics the features of [RFC3546].

The Device MAY store RI certificate verification data indicating that an RI certificate chain has been verified. The purpose of this is to avoid repeated verification of the same certificate chain. The RI certificate verification data stored in this way MUST uniquely identify the RI certificate and MUST be integrity protected. The Device SHOULD check if the RI certificate chain received in this parameter corresponds to the stored certificate verification data for this RI. If so, the Device need not verify the RI certificate chain again, otherwise the Device MUST verify the RI certificate chain. If an RI certificate is received that is not in the stored certificate verification data for this RI, and if the Device can determine (in the case of Connected Devices and Unconnected Devices that support DRM Time) that the expiry time of the received RI certificate is later than the RI Context for this RI, and the certificate status of the RI certificate as indicated in the OCSP response is `good` (see [OCSP-MP]) then the Device MUST verify the complete chain and SHOULD replace the stored RI certificate verification data with the received RI certificate data and set the RI context expiry time to that of the received RI certificate expiry time. However, if the Device does store RI certificate verification data in this way it MUST store the expiry period of the RI's certificate (as indicated by the notAfter field within the certificate) and MUST compare the Device's current DRM Time with the stored RI certificate expiry time whenever verifying the signature on signed messages from the RI. If the Device's current DRM Time is after the stored RI certificate expiry time then the Device MUST abandon processing the RI message and MUST initiate the registration protocol.

OCSP Response SHALL be a valid OCSP response for the RI's certificate and MAY also include a valid OCSPResponse for other certificates in the RI's certificate chain. The Device MUST NOT fail due to the presence of more than 1 OCSP Response element. This parameter will not be sent if the Device sent the Extension *No OCSP Response* in the preceding ROAP-RegistrationRequest (and the RI did not ignore that extension). An exception to this is when the RI deems that the Device's DRM Time is inaccurate. When the *OCSP Response* parameter is received, the Device MUST verify that the RI certificate status is `good`.

The RI SHOULD always provide the most recent OCSP response to the Device (regardless of whether it contains a Device-supplied nonce or not), but MAY use a regularly updated time-based OCSP response. RI's MAY also include valid OCSPResponses for other certificates in their certificate chain.

Extensions: The following extensions are defined for the ROAP-RegistrationResponse message.

- *Domain Name Whitelist*: This extension allows an RI to specify a list of fully qualified domain names (as defined in [RFC 2396]) that are to be regarded as trusted for the purposes of Silent and Preview headers. The Device MUST store the domain names along in the RI Context for this RI. The Device MUST be able to use these domain names for processing DCFs containing the Silent header or a Preview header with method “preview-rights” and a specified preview URL, as defined in section 5.2.2 of this document. The Device MUST treat each domain name received in the Domain Name Whitelist as if it were a fully qualified domain name that had been extracted from a RI URL according to the conditions defined in section 5.2.2 of this document. The Device MUST be capable of storing a minimum of 5 fully qualified domain names for each RI Context supported on the Device.

Signature is a signature on data sent in the protocol. The signature is made using the RI's private key on a hash of the previous message (ROAP-RegistrationRequest) and all elements of this message (besides the *Signature* element itself). The signature method is as follows:

- The previous message and the current one except the *Signature* element is canonicalized using the exclusive canonicalization method defined in [XC14N].
- The two messages are concatenated in their chronological order, starting with the ROAP-RegistrationRequest message. The resulting data *d* is considered as input to the signature operation.
- The signature is calculated on *d* in accordance with the rules of the negotiated signature scheme

The Device MUST verify this signature. A Device MUST NOT accept the Registration protocol as successful unless the signature verifies, the RI certificate chain has been successfully verified, and the OCSP response indicates that the RI cerificate status is `good`. If the registration failed the Device MUST NOT store the RI Context for this RI, otherwise the Device SHOULD store the RI Context for this RI.

The stored RI Context SHALL at a minimum contain: riURL, RI ID, Selected Version, Selected Algorithms, and a Certificate Caching indication if the RI has stored the Device certificate or not (all this information is carried in the ROAP-RIHello message). The RI Context MAY also contain RI certificate validation data, OCSP responder key and the current OCSP response. The RI Context SHALL also contain an RI Context Expiry Time, which is defined to be the RI certificate expiry time. For Unconnected Devices that do not support DRM Time, the RI Context is infinite i.e., it does not have an expiry time.If the RI Context has expired, the Device MUST NOT execute any other protocol than the 4-pass Registration protocol with this RI, and upon detection of RI Context expiry the Device SHOULD initiate the Registration protocol using the riURL stored in the RI Context. The Device SHALL have at most one RI Context with each RI. An existing RI Context SHALL be replaced with a newly established RI Context after successful re-registration with the same RI.

Note that any cached OCSP response has its own validity period, which normally will be much shorter than the validity period of the RI Context.

5.4.2.4.2 Message syntax

The **<registrationResponse>** element specifies the ROAP-RegistrationResponse message, and constitutes the last message in the Registration protocol. It has complex type **roap:RegistrationResponse**, which extends the basic **roap:Response** type.

```
<element name="registrationResponse" type="roap:RegistrationResponse"/>

<complexType name="RegistrationResponse">
 <annotation>
  <documentation xml:lang="en">
   Message sent from RI to Device in response to a
   registrationRequest message.
  </documentation>
 </annotation>
 <complexContent>
  <extension base="roap:Response">
   <sequence minOccurs="0">
    <element name="certificateChain" type="roap:CertificateChain"
          minOccurs="0"/>
    <element name="ocspResponse" type="base64Binary" minOccurs="0"
          maxOccurs="unbounded"/>
    <element name="extensions" type="roap:Extensions" minOccurs="0"/>
    <element name="signature" type="base64Binary"/>
   </sequence>
   <attribute name="sessionId" type="hexBinary" use="required"/>
  </extension>
 </complexContent>
</complexType>
```

5.4.3 RO Acquisition

5.4.3.1 RO Request

The ROAP-RORequest message is sent from a Device to an RI to request Rights Objects. This message is the first message of the 2-pass RO Acquisition protocol.

5.4.3.1.1 Message description

ROAP-RORequest	
Parameter	**Mandatory/Optional**
Device ID	M
Domain ID	O
RI ID	M
Device Nonce	M
Request Time	M
RO Info	M
Certificate Chain	O
Extensions	O
Signature	M

Table 5: RO Request Message Parameters

Device ID identifies the requesting Device as specified in section 5.4.2.1.1.

Domain ID, when present, identifies the Domain for which the requested ROs shall be issued.

RI ID identifies the authorizing RI as specified in section 5.4.2.2.1.

Device Nonce is a nonce chosen by the Device. Nonces are generated and used in this message as specified in section 5.3.9.

Request Time is the current DRM Time, as seen by the Device.

RO Info identifies the requested Rights Object(s). The parameter consists of a (non-empty) set of Rights Object identifiers identifying the requested Rights Objects, and for each RO identifier an optional hash of the DCF associated with the requested RO. The DCF hash SHOULD be included when the Device is in possession of the associated DCF, unless its inclusion, as determined by some vendor-specific algorithm, would be impractical (e.g. due to the size of the DCF). The DCF hash, if computed, MUST be computed as specified in section 5.3 of [DRMCF-v2].

Certificate Chain: This parameter is sent unless it is indicated in the RI Context that this RI has stored necessary Device certificate information. When present, the parameter value SHALL be as described for the *Certificate Chain* parameter in the ROAP-RegistrationRequest message.

Extensions: The following extensions are defined for the ROAP-RORequest message:

– *Peer Key Identifier:* An identifier for an RI public key stored in the Device. If the identifier matches the RI's current public key, or if the extension is empty, it means the Device has already stored the RI ID and the corresponding RI certificate chain, and the RI need not send down its certificate chain in its response message.

- *No OCSP Response*: This extension allows the Device to indicate to the RI that there is no need to send an OCSP Response since the Device has cached a valid OCSP Response for this RI.
- *OCSP Responder Key Identifier*: This extension identifies an OCSP responder key stored in the Device. If the identifier matches the key in the certificate used by the RI's OCSP responder, the RI MAY remove the OCSP Responder certificate chain from the OCSP response before providing the OCSP response to the Device.
- *Transaction Identifier*: Allows a Device to provide the RI with information for tracking of transactions, for example relating to loyalty programs (an example of this could be reward scheme information from the DCF scheme).

If the Device has stored the RI public key, the Device MUST send the *Peer Key Identifier* extension. If the Device has a valid OCSP Response, the Device MUST send the *No OCSP Response* extension. If the Device has stored the OCSP responder key for this RI, the Device MUST send the *OCSP Responder Key Identifier* extension; otherwise, the Device MUST NOT use this extension.

Signature is a signature on this message (besides the *Signature* element itself). The signature method is as follows:

- The message except the *Signature* element is canonicalized using the exclusive canonicalization method defined in [XC14N].
- The result of the canonicalization, *d*, is considered as input to the signature operation.
- The signature is calculated on *d* in accordance with the rules of the negotiated signature scheme

The RI MUST verify the signature on the ROAP-RORequest message.

5.4.3.1.2 Message syntax

The **<roRequest>** element specifies the ROAP-RORequest message. It has complex type **roap:RORequest**, which extends the basic **roap:Request** type.

```
<element name="roRequest" type="roap:RORequest"/>

<complexType name="RORequest">
 <annotation>
  <documentation xml:lang="en">
   Message sent from Device to RI to request an RO.
  </documentation>
 </annotation>
 <complexContent>
  <extension base="roap:Request">
   <sequence>
    <element name="deviceID" type="roap:Identifier"/>
    <element name="domainID" type="roap:DomainIdentifier"
          minOccurs="0"/>
    <element name="riID" type="roap:Identifier"/>
    <element name="nonce" type="roap:Nonce"/>
    <element name="time" type="dateTime"/>
    <element name="roInfo">
     <complexType>
      <sequence maxOccurs="unbounded">
       <element name ="roID" type="ID"/>
       <element name="dcfHash" minOccurs="0">
        <complexType>
         <sequence>
          <element name="hash" type="base64Binary"/>
         </sequence>
         <attribute name="algorithm" type="anyURI"
                  default="http://www.w3.org/2000/09/xmldsig#sha1"/>
        </complexType>
```

```
          </element>
        </sequence>
      </complexType>
    </element>
    <element name="certificateChain" type="roap:CertificateChain" minOccurs="0"/>
    <element name="extensions" type="roap:Extensions" minOccurs="0"/>
    <element name="signature" type="base64Binary"/>
   </sequence>
  </extension>
 </complexContent>
</complexType>
```

The following schema fragment defines the *Transaction Identifier* extension:

```
<complexType name="TransactionIdentifier">
 <complexContent>
  <extension base="roap:Extension">
   <sequence>
    <element name="id">
     <simpleType>
      <restriction base="string">
       <length value="16"/>
      </restriction>
     </simpleType>
    </element>
   </sequence>
  </extension>
 </complexContent>
</complexType>
```

5.4.3.2 RO Response

The ROAP-ROResponse message is sent from the RI to the Device either in response to a ROAP-RORequest message (two-pass variant) or by RI initiative (one-pass variant). It carries the protected ROs.

5.4.3.2.1 Message description

Parameter	ROAP-ROResponse

	2-pass Status = Success	*2-pass Status ≠ Success*	*1-pass*
Status	M	M	M
riURL	-	O	O
Device ID	M	-	M
RI ID	M	-	M
Device Nonce	M	-	-
Protected ROs	M	-	M
Certificate Chain	O	-	O
OCSP Response	O	-	M
Extensions	O	-	O
Signature	M	-	M

Table 6: RO Response Message Parameters

Status indicates if the request was successfully handled or not. In the latter case an error code specified in Section 5.3.5 is sent.

riURL indictates the URL that the Device SHOULD use in a subsequent ROAP session that is triggered as a result of receiving a specific error message as specified in section 5.3.5. For the *DeviceTimeError* and *NotRegistered* error message the RI MUST include the ***riURL*** attribute in the ROAP-ROResponse message.

Device ID identifies the requesting Device, in the same manner as in the ROAP-DeviceHello message as specified in section 5.4.2.1.1. The value returned here MUST equal the Device ID sent by the Device in the ROAP-RORequest message that triggered this response in the 2-pass ROAP. In the 1-pass ROAP, the RI selects the Device ID of the recipient Device. If the Device ID is incorrect, the ROAP-ROResponse processing will fail and the Device MUST discard the received ROResponse PDU.

RI ID identifies the RI. The value returned here MUST equal the RI ID sent by the Device in the ROAP-RORequest message that triggered this response in the 2-pass ROAP. Otherwise, it should be an RI identifier as specified in section 5.4.2.2.1.

Device Nonce: This parameter, if present (2-pass), MUST have the same value as the corresponding parameter value in the preceding ROAP-RORequest.

Protected RO(s) are the Rights Objects (in the form of **<ProtectedRO>** elements), in which sensitive information (such as content encryption keys, CEKs) is encrypted.

Certificate Chain: This parameter MUST be present unless a preceding ROAP-RORequest message contained the *Peer Key Identifier* extension, the extension was not ignored by the RI, and its value identified the RI's current key. When present, the value of a *Certificate Chain* parameter shall be as described for the *Certificate Chain* parameter of the ROAP-RegistrationResponse message

The Device SHOULD check if the RI certificate chain received in this parameter corresponds to stored certificate verification data for this RI. If so, the Device need not verify the RI certificate chain again, otherwise the Device MUST verify the RI certificate chain. If an RI certificate is received that is not in the stored certificate verification data for this RI, and if the expiry time of the received RI certificate is later than the RI Context for this RI, and the certificate status of the RI certificate as indicated in the OCSP response is `good`, then the Device MUST verify the complete chain and SHOULD replace the stored RI certificate verification data with the received RI certificate data and set the RI context expiry time to that of the received RI certificate expiry time.

OCSP Response SHALL be a valid OCSP response for the RI's certificate and MAY also include a valid OCSPResponse for other certificates in the RI's certificate chain. The Device MUST NOT fail due to the presence of more than 1 OCSP Response element. This parameter will not be sent if the Device sent the Extension *No OCSP Response* in a preceding ROAP-RegistrationRequest (and the RI did not ignore that extension). If the

OCSP Response parameter is received, the Device MUST verify that the RI certificate status is `good`; otherwise the RO acquisition was not successful.

Extensions: The following extensions are defined for the ROAP-ROResponse message:

– *Transaction Identifier*: Allows an RI to provide a Device with information for tracking of transactions, for example relating to loyalty programs (an example of this could be reward scheme information from the DCF).

Signature is a signature on data sent in the protocol. The signature is computed using the RI's private key and all elements of this message (besides the *Signature* element itself). The signature method is as follows:

– All elements except the *Signature* element are canonicalized using the exclusive canonicalization method defined in [XC14N].

– The resulting data *d* is considered as input to the signature operation.

– The signature is calculated on *d* in accordance with the rules of the negotiated signature scheme

The Device MUST verify this signature. A Device MUST NOT accept the RO acquisition as successful unless the signature verifies, the RI certificate chain has been successfully verified, and the OCSP response indicates that the RI cerificate status is `good`. If the acquisition protocol failed, the Device MUST NOT install the received ROs.

Before installing any received ROs that are stateful (indicated by the ***stateful*** attribute of the **<ro>** element), the Device MUST apply the RO Replay protection described in the Replay Protection Section.

5.4.3.2.2 Message syntax

The **<roResponse>** element specifies the ROAP-ROResponse message. It has complex type **roap:ROResponse**, which extends the basic **roap:Response** type.

```
<element name="roResponse" type="roap:ROResponse"/>

<complexType name="ROResponse">
 <annotation>
  <documentation xml:lang="en">
   Message sent from RI to Device in response to an RORequest.
  </documentation>
 </annotation>
 <complexContent>
  <extension base="roap:Response">
   <sequence minOccurs="0">
    <element name="deviceID" type="roap:Identifier"/>
    <element name="riID" type="roap:Identifier"/>
    <element name="nonce" type="roap:Nonce" minOccurs="0"/>
    <element name="protectedRO" type="roap:ProtectedRO" maxOccurs="unbounded"/>
    <element name="certificateChain" type="roap:CertificateChain" minOccurs="0"/>
    <element name="ocspResponse" type="base64Binary" minOccurs="0" maxOccurs="unbounded"/>
    <element name="extensions" type="roap:Extensions" minOccurs="0"/>
    <element name="signature" type="base64Binary"/>
   </sequence>
  </extension>
 </complexContent>
</complexType>
```

The **roap:ProtectedRO** type is defined in The Protected Rights Object payload type section.

5.4.4 Domain Management

5.4.4.1 Join Domain Request

The ROAP-JoinDomainRequest message is sent from the Device to the RI. This message is the first message in the 2-pass Join Domain protocol. The ROAP-JoinDomainRequest message only supports a request to join a single domain.

5.4.4.1.1 Message description

ROAP-JoinDomainRequest	
Parameter	**Mandatory/Optional**
DeviceID	M
RI ID	M
Device Nonce	M
Request Time	M
Domain Identifier	M
Certificate Chain	O
Extensions	O
Signature	M

Table 7: Join Domain Request Message Parameters

Device ID identifies the requesting Device as specified in section 5.4.2.1.1.

RI ID identifies the authorizing RI as specified in section 5.4.2.2.1.

Device Nonce is a nonce chosen by the Device. Nonces are generated and used in this message as specified in section 5.3.95.3.9.

Request Time is the current DRM Time, as seen by the Device. Connected Devices and Unconnected Devices that support DRM Time MUST insert their current DRM Time. Unconnected Devices that do not support DRM Time MUST use the value “Undefined”.

Domain Identifier shall identify the Domain the Device wishes to join.

Certificate Chain: This parameter is sent unless *Certificate Caching* is indicated in the RI Context with this RI. When present, the parameter value shall be as described for the *Certificate Chain* parameter in the ROAP-RegistrationRequest message.

Extensions: The following extensions are defined for the ROAP-JoinDomainRequest message:

- *Peer Key Identifier:* An identifier for an RI public key stored in the Device. If the identifier matches the RI's current public key, or if it is empty, it means the Device has already stored the RI ID and the corresponding RI certificate chain, and the RI need not send down its certificate chain in its response message.
- *No OCSP Response*: This extension allows the Device to indicate to the RI that there is no need to send an OCSP response since the Device has cached a valid OCSP response for this RI.
- *OCSP Responder Key Identifier*: This extension identifies an OCSP responder key stored in the Device. If the identifier matches the key in the certificate used by the RI's OCSP responder, the RI MAY remove the OCSP Responder certificate chain from the OCSP response before providing the OCSP response to the Device.
- *Hash Chain Support*: When this extension is present, it signals that the client supports a technique of generating Domain Keys through hash chains, see section 8.7.1.

If the Device has stored the RI public key, the Device MUST send the *Peer Key Identifier* extension. If the Device has a valid OCSP Response, the Device MUST send the *No OCSP Response* extension. If the Device has stored the OCSP responder key for this RI, the Device MUST send the *OCSP Responder Key Identifier* extension. If the Device supports hash-chained Domain keys the Device MUST send the *Hash Chain Support* extension; otherwise, the Device MUST NOT use this extension.

Signature is a signature on this message (excluding the *Signature* element itself). The signature method is as follows:

- The message except the *Signature* element is canonicalized using the exclusive canonicalization method defined in [XC14N].
- The result of the canonicalization, *d*, is considered as input to the signature operation.
- The signature is calculated on *d* in accordance with the rules of the negotiated signature algorithm.

The RI MUST verify the signature on the ROAP-JoinDomainRequest message.

5.4.4.1.2 Message syntax

The **<joinDomainRequest>** element specifies the ROAP-JoinDomainRequest message. It has complex type **roap: DomainRequest**, which extends the basic **roap:Request** type. Note that this type is used both for join and leave Domain request messages (the **notMember** attribute is only used in ROAP-LeaveDomainRequest messages).

```
<element name="joinDomainRequest" type="roap:DomainRequest"/>

<complexType name="DomainRequest">
  <annotation>
    <documentation xml:lang="en">
      General PDU for sending domain-related requests from a Device to an RI.
    </documentation>
  </annotation>
  <complexContent>
    <extension base="roap:Request">
      <sequence>
        <element name="deviceID" type="roap:Identifier"/>
        <element name="riID" type="roap:Identifier"/>
        <element name="nonce" type="roap:Nonce"/>
        <element name="time" type="roap:dateTimeOrUndefined"/>
        <element name="domainID" type="roap:DomainIdentifier"/>
        <element name="certificateChain" type="roap:CertificateChain" minOccurs="0"/>
        <element name="extensions" type="roap:Extensions" minOccurs="0"/>
        <element name="signature" type="base64Binary"/>
      </sequence>
      <attribute name="notMember" type="boolean"/>
    </extension>
  </complexContent>
</complexType>
```

The following schema fragment defines the **roap:DomainIdentifier** type. The last two characters (digits) represent the Domain Generation (see section 8.7 for further information). RIs will always respond with the Domain Key corresponding to the most recent Domain Generation and, if hash chains are not supported, all earlier Domain Keys for this Domain too.

```
<simpleType name="DomainIdentifier">
  <restriction base="string">
    <pattern value=".{1,18}\d{2}"/>
  </restriction>
</simpleType>
```

The following schema fragment defines the *Hash Chain Support* extension:

```
<complexType name="HashChainSupport">
  <complexContent>
    <extension base="roap:Extension"/>
  </complexContent>
</complexType>
```

5.4.4.2 Join Domain Response

The ROAP-JoinDomainResponse message is sent by an RI to a Device in response to a ROAP-JoinDomainRequest message. This message is the second message in the 2-pass protocol to join a Device to a Domain.

5.4.4.2.1 Message description

Parameter	ROAP-JoinDomainResponse	
	Status = "Success"	*Status ≠ "Success"*
Status	M	M
riURL	-	O
Device ID	M	-
RI ID	M	-
Device Nonce	M	-
Domain Info	M	-
Certificate chain	O	-
OCSP Response	O	-
Extensions	O	-
Signature	M	-

Table 8: Join Domain Response Message Parameters

Status indicates if the request was successfully handled or not. In the latter case an error code as specified in Section 5.3.5 is sent.

riURL indictates the URL that the Device SHOULD use in a subsequent ROAP session that is triggered as a result of receiving a specific error message as specified in section 5.3.5. For the *DeviceTimeError* and *NotRegistered* error message the RI MUST include the ***riURL*** attribute in the ROAP-JoinDomainResponse message.

Device ID identifies the requesting Device. The value returned here MUST equal the Device ID sent by the Device in the ROAP-JoinDomainRequest message that triggered this response.

RI ID identifies the RI. The value returned here MUST equal the RI ID sent by the Device in the ROAP-JoinDomainRequest message that triggered this response.

Device Nonce: This parameter, if present (2-pass), MUST have the same value as the corresponding parameter value in the preceding ROAP-JoinDomainRequest.

Domain Info: This parameter carries Domain keys (encrypted using Device's public key) as well as information about the maximum lifetime of the Domain. Devices MAY use a shorter lifetime than suggested by the RI.

Certificate Chain: This parameter MUST be present unless a preceding ROAP-JoinDomainRequest message contained the *Peer Key Identifier* extension, the extension was not ignored by the RI, and its value identified the RI's current key. When present, the value of a *Certificate Chain* parameter shall be as described for the *Certificate Chain* parameter of the ROAP-RegistrationResponse message.

The Device SHOULD check if the RI certificate chain received in this parameter corresponds to stored certificate verification data for this RI. If so, the Device need not verify the RI certificate chain again, otherwise the Device MUST verify the RI certificate chain. If an RI certificate is received that is not in the stored certificate verification data for this RI, and if the expiry time of the received RI certificate is later than the RI Context for this RI, and the certificate status of the RI certificate as indicated in the OCSP response is "good," then the Device MUST verify the complete chain and SHOULD replace the stored RI cerficate verification data with the received RI certificate data and set the RI context expiry time to that of the received RI certificate expiry time.

OCSP Response SHALL be a valid OCSP response for the RI's certificate and MAY also include a valid OCSPResponse for other certificates in the RI's certificate chain. The Device MUST NOT fail due to the presence of more than 1 OCSP Response element. This parameter will not be sent if the Device sent the Extension *No OCSP Response* in the preceding ROAP-RegistrationRequest (and the RI did not ignore that extension). If the *OCSP Response* is received, the Device MUST verify that the status of the RI certificate is `good`, otherwise the Join Domain protocol was not successful.

For Connected Devices and Unconnected Devices that support DRM Time the RI SHOULD always provide the most recent OCSP Response to the Device (regardless of whether it contains a Device-supplied nonce or not, but MAY use a regularly updated time-based OCSP Response. RI's MAY also include valid OCSPResponses for other certificates in their certificate chain.

Unconnected Devices that do not support DRM Time will not be able to use a time based OCSP Response. Because of this, RIs SHOULD NOT include such OCSP Response messages in responses to Unconnected Devices that do not support DRM Time.

If the RI detects (using its own criteria) that a Device's DRM Time is inaccurate then the RI MAY return an invalidDeviceTime error in the status parameter of the JoinDomainResponse. Receipt of this error code SHOULD trigger the DRM agent to initiate the Registration protocol with the RI.

Extensions: The following extension is currently defined for the ROAP-JoinDomainResponse message:

- *Hash Chain Support:* When this extension is present it indicates that the RI is using the technique of generating Domain Keys through hash chains described in the Domains Section. The RI MUST NOT include this extension in the ROAP-JoinDomainResponse unless the same extension was received in the preceeding ROAP-JoinDomainRequest. If the Device receives the *Hash Chains Support* extension then it needs only store the latest Domain Key for a given Domain.

Signature is a signature on this message (besides the *Signature* element itself). The signature method is as follows:

- The message except the *Signature* element is canonicalized using the exclusive canonicalization method defined in [XC14N].
- The result of the canonicalization, *d*, is considered as input to the signature operation
- The signature is calculated on *d* in accordance with the rules of the negotiated signature algorithm.

The Device MUST verify this signature. A Device MUST NOT accept the Join Domain protocol as successful unless the signature verifies, the RI certificate chain has been successfully verified, and the OCSP response indicates that the RI cerificate status is `good`. If the Join Domain protocol failed the Device MUST NOT store a Domain Context, otherwise the Device MUST store the resulting Domain Context.

The stored Domain Context SHALL at a minimum contain: The Domain ID (which includes the Domain Generation), the Domain Context Expiry Time, and, if applicable, an indication that the RI supports hash-chained Domain Keys. If the Device and RI both support hash chains, the Domain Context SHALL contain the Domain Key corresponding to the highest known generation, otherwise the Domain Context SHALL contain all Domain Keys of all Domain Generations. The Domain Context SHALL also contain the RI Public Key for the case when the Domain Context Expiry Time extends beyond the RI Context Expiry Time.

A Device MUST NOT install any Domain ROs for a Domain whose Domain Context has expired. In the case of Unconnected Devices that do not support DRM Time, the Domain Context does not expire and hence has a value that is infinite, as indicated in the **DomainInfo:NotAfter** element.

NOTE: Rights Issuers should carefully consider the security implications of using the value “Infinite” for Devices that support DRM Time.

A Device MAY have several Domain Contexts with an RI.

5.4.4.2.2 Message syntax

The **<joinDomainResponse>** element specifies the ROAP-JoinDomainResponse message. It has complex type **roap:JoinDomainResponse**, which extends the basic **roap:Response** type.

```
<element name="joinDomainResponse" type="roap:JoinDomainResponse"/>

<complexType name="JoinDomainResponse">
  <annotation>
    <documentation xml:lang="en">
      Message sent from RI to Device in response to a
      JoinDomainRequest.
    </documentation>
  </annotation>
  <complexContent>
    <extension base="roap:Response">
      <sequence minOccurs="0">
        <element name="deviceID" type="roap:Identifier"/>
        <element name="riID" type="roap:Identifier"/>
        <element name="nonce" type="roap:Nonce"/>
        <element name="domainInfo" type="roap:DomainInfo"/>
        <element name="certificateChain" type="roap:CertificateChain" minOccurs="0"/>
        <element name="ocspResponse" type="base64Binary" minOccurs="0" maxOccurs="unbounded"/>
        <element name="extensions" type="roap:Extensions" minOccurs="0"/>
        <element name="signature" type="base64Binary"/>
      </sequence>
    </extension>
  </complexContent>
</complexType>
```

The following schema fragment defines the **DomainInfo** type:

```
<complexType name="DomainInfo">
  <sequence>
    <element name="notAfter" type="dateTimeOrInfinite"/>
    <element name="domainKey" type="roap:ProtectedDomainKey" maxOccurs="unbounded"/>
  </sequence>
</complexType>

<simpleType name="dateTimeOrInfinite">
  <union memberTypes="dateTime InfiniteString"/>
</simpleType>

<simpleType name="InfiniteString">
  <restriction base="string">
  <enumeration value="Infinite"/>
  </restriction>
</simpleType>
```

The **<notAfter>** element expresses, in UTC, the expiry time of the Domain Context. The value **”Infinite”** indicates infinite lifetime of the Domain Context.

The **<domainKey>** element contains the wrapped Domain key and a key-confirming MAC key, see below.

```
<complexType name="ProtectedDomainKey">
  <sequence>
```

```
    <element name="encKey" type="xenc:EncryptedKeyType"/>
    <element name="riID" type="roap:Identifier"/>
    <element name="mac" type="base64Binary"/>
  </sequence>
</complexType>
```

The **<encKey>** element contains a MAC key, K_{MAC}, and a Domain Key, K_D, wrapped as specified in the Key Management section 7. The value of the **<encKey>** element's ***Id*** attribute must equal the value of the **<domainId>** element in the preceding ROAP-JoinDomainRequest message, save for the Domain Generation part. If Hash Chains are supported by both the Device and the RI, only the Domain Key corresponding to the most recent Domain Generation SHOULD be included, otherwise all Domain Keys for all Domain Generations MUST be included (including their domain identifiers as ***Id*** attributes). The child of the **<ds:KeyInfo>** element inside the **<encKey>** element SHALL be of type **roap:X509SPKIHash**, identifying a particular DRM Agent's public key through the hash of the `subjectPublicKeyInfo` value in its certificate.

The **<riID>** element is necessary for key confirmation purposes. A Device MUST verify that it has the same value as the **<riID>** element of the ROAP-JoinDomainResponse message itself.

The **<mac>** element provides key-confirmation through a MAC on the canonical [XC14N] version of the **<domainKey>** element (excluding the **<mac>** element itself) using the MAC key K_{MAC} wrapped in the **<encKey>** element. The MAC algorithm to use is defined by the RI Context. Devices MUST NOT install domain keys where the MAC is invalid.

5.4.4.3 Leave Domain Request

The ROAP-LeaveDomainRequest message is sent from the Device to the RI. This message is the first message in the 2-pass protocol for removing a Device from a Domain.

5.4.4.3.1 Message description

ROAP-LeaveDomainRequest	
Parameter	**Mandatory/Optional**
DeviceID	M
RI ID	M
Device Nonce	M
Request Time	M
Domain Identifier	M
Certificate Chain	O
Extensions	O
Signature	M

Table 9: Leave Domain Request Message Parameters

Device ID identifies the requesting Device as defined in section 5.4.2.1.1.

RI ID identifies the authorizing RI as defined in section 5.4.2.2.1.

Device Nonce is a nonce chosen by the Device. Nonces are generated and used in this message as specified in section 5.3.95.3.9.

Request Time is the current DRM Time, as seen by the Device. Connected Devices and Unconnected Devices that support DRM Time MUST insert their current DRM Time. Unconnected Devices that do not support DRM Time MUST use the value “Undefined”.

Domain Identifier identifies the Domain.

Certificate Chain: This parameter is sent unless *Certificate Caching* is indicated in the RI Context with this RI. When present, the parameter value shall be as described for the *Certificate Chain* parameter in the ROAP-RegistrationRequest message.

Extensions: The following extension is currently defined for the ROAP-LeaveDomainRequest message:

- *Not a Domain Member*: Presence of this extension indicates to the RI that the Device does not consider itself a member of this Domain (even though it is sending a request for the RI to remove it from the Domain). This could happen, for example, if the Device already has left the Domain, but receives a new trigger to leave it (perhaps because the RI never received the previous ROAP-LeaveDomainRequest). This extension MUST be included in the request if the Device is not a member of the identified Domain.

Signature is a signature on this message (excluding the *Signature* element itself). The signature method is as follows:

- The message except the *Signature* element is canonicalized using the exclusive canonicalization method defined in [XC14N].
- The result of the canonicalization, *d*, is considered as input to the signature operation.
- The signature is calculated on *d* in accordance with the rules of the negotiated signature algorithm.

The RI MUST verify the signature on the ROAP-LeaveDomain message.

The Device MUST ensure that the Domain Context of the corresponding Domain is deleted **before** sending the ROAP-LeaveDomainRequest to the RI.

5.4.4.3.2 Message syntax

The **<leaveDomainRequest>** element specifies the ROAP-LeaveDomainRequest message. It has complex type **roap:DomainRequest**, which extends the basic **roap:Request** type.

```
<element name="leaveDomainRequest" type="roap:DomainRequest"/>
```

The following schema fragement defines the *Not a Domain Member* extension:

```
<complexType name="NotDomainMember">
  <complexContent>
    <extension base="roap:Extension"/>
  </complexContent>
</complexType>
```

5.4.4.4 Leave Domain Response

The ROAP-LeaveDomainResponse message is sent by an RI to a Device in response to a ROAP-LeaveDomainRequest message. This message is the second message in the 2-pass protocol for removing a Device from a Domain.

5.4.4.4.1 Message description

ROAP-LeaveDomainResponse		
Parameter	Mandatory/Optional	
	Status = "Success"	**Status ≠ "Success"**

Status	M	M
riURL	-	O
Device Nonce	M	-
Domain Identifier	M	-
Extensions	O	-

Table 10: Leave Domain Response Message Parameters

Status indicates if the request was successfully handled or not. In the latter case an error code defined in section 5.3.5 is sent.

riURL indictates the URL that the Device SHOULD use in a subsequent ROAP session that is triggered as a result of receiving a specific error message as specified 5.3.5. For the *DeviceTimeError* and *NotRegistered* error message the RI MUST include the ***riURL*** attribute in the ROAP-LeaveDomainResponse message.

Device Nonce is the nonce sent by the Device. This parameter MUST have the same value as the corresponding parameter value in the preceding ROAP-LeaveDomainRequest.

Domain Identifier identifies the Domain from which the RI removed the Device. The Domain Generation part of the Domain Identifier SHALL be ignored.

Extensions: No extensions are currently defined for the ROAP-LeaveDomainResponse message.

The RI sends the ROAP-LeaveDomainResponse after having deleted the association of this Device to the Domain (i.e. updated the Domain membership status).

5.4.4.4.2 Message Syntax

The **<leaveDomainResponse>** element specifies the ROAP-LeaveDomainResponse message. It has complex type **roap:LeaveDomainResponse**, which extends the basic **roap:Response** type.

```
<element name="leaveDomainResponse" type="roap:LeaveDomainResponse"/>

<complexType name="LeaveDomainResponse">
  <annotation>
    <documentation xml:lang="en">
      Message sent from RI to Device in response to a leaveDomainRequest
    </documentation>
  </annotation>
  <complexContent>
    <extension base="roap:Response">
      <sequence minOccurs="0">
        <element name="nonce" type="roap:Nonce"/>
        <element name="domainID" type="roap:DomainIdentifier"/>
        <element name="extensions" type="roap:Extensions" minOccurs="0"/>
      </sequence>
    </extension>
  </complexContent>
</complexType>
```

6. Certificate Status Checking & Device Time Synchronization

6.1 Certificate status checking by RI

For each request signed by the Device that requires the RI to perform substantial processing, the RI MUST check the signature, expiry date (validity), and the revocation status of the Device certificate.

6.2 Certificate status checking by DRM Agents

For each message signed by the RI, the Device MUST check the signature and if possible MUST check the certificate status of Rights Issuer certificates. The means to do this are specified in the ROAP description above.

In particular whenever an OCSP response is received by the Device, it MUST be verified that the RI certificate status is `good`. DRM Agents MUST support all client requirements in [OMA-OCSP-MP] with the following exceptions:

- DRM Agents need not be able to generate OCSPRequests
- Clients need only be able to handle OCSPResponses with one SingleResponse value
- Clients need not support the authorityInfoAccess certificate extension (as they will not contact OCSP responders directly)
- DRM Agents need not support OCSP over HTTP/1.1 (as they will not contact OCSP responders directly)

Clients MUST be able to match a nonce sent for OCSP purposes in the ROAP protocol with a nonce in the received OCSPResponse.

6.3 Device DRM Time Synchronization

An RI, which receives an RORequest or a JoinDomainRequest, and detects that the Device's DRM Time as specified in the request is inaccurate, SHALL respond with the status code DeviceTimeError. A Device receiving this status code SHOULD attempt to re-register with the RI by initiating the Registration protocol.

An RI, which receives a RegistrationRequest, and detects that the Device's time as specified in the request is inaccurate, MUST send an OCSP request to its responder, and include the nonce sent by the Device in the OCSP request. The nonce-based OCSP response returned from the OCSP responder MUST be included in the RegistrationResponse message sent back to the Device.

A Device, which receives a RegistrationResponse message containing a nonce-based OCSP response where the nonce in the OCSP response matches the nonce sent in the Device's RegistrationRequest, MUST adjust its time to match the time in the `producedAt` component of the OCSP response, assuming the Registration protocol exchange otherwise was successful. Barring network latency and response times, the procedure described here will synchronize the Device DRM Time with the OCSP responder's.

To avoid excessive re-registrations and a high load on OCSP responders,

1. Rights Issuers MUST use the time obtained from the OCSP responders as its reference time in order to judge the inaccuracies in the Device’s DRM Time.
2. Rights Issuers SHOULD allow for a reasonable drift in the Device’s DRM Time.
3. Connected Devices and Unconnected Devices that support DRM Time should maintain DRM Time to an accuracy of 120ppm (this equates to approximately 60 minutes per year).

7. Key Management

7.1 Cryptographic Components

7.1.1 RSAES-KEM-KWS

RSA-KEM-KWS is an asymmetric encryption scheme defined in [X9.44] and [IETF-KEM] and based on the "generic hybrid cipher" in [ISO/IEC 18033]. In this scheme, the sender uses the recipient's public key to securely transfer symmetric-key material to the recipient. Specifically, given the recipient's public RSA key *P,* consisting of a modulus *m* and a public exponent *e*, the sender generates a value Z as a statistically uniform random integer in the interval [0,…,*m*-1]. The value *Z* is then converted to a key-encryption key *KEK* as follows:

$$KEK = \text{KDF}(Z, \textbf{\textit{NULL}}, kekLen)$$

where KDF is defined below, ***NULL*** is the empty string, and *kekLen* shall be set to the desired length of *KEK* (in octets).

Given *KEK*, a key-wrapping scheme WRAP and the symmetric key material *K* to be transported, the sender wraps *K* to get ciphertext C_2:

$$C_2 = \text{WRAP}(KEK, K)$$

After this, the sender encrypts Z using the recipient's public RSA key *P* to yield C_1:

$$C_1 = \text{RSA.ENCRYPT}(P,Z) = Z^e \bmod m$$

The scheme output is $C = C_1 \mid C_2$ which is transmitted to the recipient. The decryption operation follows straightforwardly: the recipient recovers *Z* from C_1 using the recipient's private key, converts *Z* to *KEK*, and then unwraps C_2 to recover *K*.

7.1.2 KDF

KDF is equivalent to the key derivation function KDF2 defined in [X9.44] (and KDF in [X9.42], [X9.63]). It is defined as a simple key derivation function based on a hash function. For the purposes of this specification, the hash function shall be SHA-1.

KDF takes three parameters: the shared secret value *Z*: an octet string of (essentially) arbitrary length, *otherInfo*: other information for key derivation, an octet string of (essentially) arbitrary length (may be the empty string), and *kLen*: intended length in octets of the keying material. *kLen* shall be an integer, at most $(2^{32} - 1)hLen$ where *hLen* is the length of the hash function output. The output from KDF is the key material *K*, an octet string of length *kLen.* The operation of KDF is as follows:

1) Let *T* be the empty string.

2) For *counter* from 1 to $\lceil kLen / hLen \rceil$, do the following:

   Let *D* = 4-byte, unsigned big-endian representation of *counter*[1]

   Let $T = T \,||\, \text{Hash}(Z \,||\, D \,||\, otherInfo)$.

3) Output the first *kLen* octets of *T* as the derived key *K*.

[1] Example: If *counter* = 946, *D* will be 00 00 03 b2

7.1.3 AES-WRAP

AES-WRAP is the symmetric-key wrapping scheme based on AES and defined in [AES-WRAP]. It takes as input a key-encryption key *KEK* and key material *K* to be wrapped. The scheme outputs the result *C* of the wrapping operation:

$$C = \text{AES-WRAP}(KEK, K)$$

7.2 Key Transport Mechanisms

7.2.1 Distributing K_{REK} and K_{MAC} under a Device Public Key

This section applies when protecting a Rights Object for a Device.

K_{REK} and K_{MAC} are each 128-bit long keys generated randomly by the sender. K_{REK} ("Rights Object Encryption Key") is the wrapping key for the content-encryption key K_{CEK} in Rights Objects. K_{MAC} is used for key confirmation of the message carrying K_{REK}.

The asymmetric encryption scheme RSAES-KEM-KWS shall be used with the AES-WRAP symmetric-key wrapping scheme to securely transmit K_{REK} and K_{MAC} to a recipient Device using the Device's RSA public key. An independent random value *Z* shall be chosen for each encryption operation. For the AES-WRAP scheme, K_{MAC} and K_{REK} are concatenated to form *K*, i.e.:

$$C_1 = \text{RSA.ENCRYPT}(PubKey_{\text{Device}}, Z)$$

$$KEK = \text{KDF}(Z, \textbf{\textit{NULL}}, kekLen)$$

$$C_2 = \text{AES-WRAP}(KEK, K_{MAC} \mid K_{REK})$$

$$C = C_1 \mid C_2$$

where *kekLen* shall be set to 16 (128 bits). In this way, AES-WRAP is used to wrap 256 bits of key data (K_{MAC} | K_{REK}) with a 128-bit key-encryption key (*KEK*).

After receiving *C*, the DRM Device splits it into C_1 and C_2 and decrypts C_1 using its private key, yielding *Z*:

$$C_1 \mid C_2 = C$$

$$Z = \text{RSA.DECRYPT}(PrivKey_{\text{Device}}, C_1)$$

Using *Z*, the Device can derive *KEK*, and from *KEK* unwrap C_2 to yield K_{MAC} and K_{REK}.:

$$K_{MAC} \mid K_{REK} = \text{AES-UNWRAP}(KEK, C_2)$$

The following URI shall be used to identify this key transport scheme in **<xenc:EncryptionMethod>** elements:

http://www.rsasecurity.com/rsalabs/pkcs/schemas/pkcs-1#rsaes-kem-kdf2-kw-aes128

7.2.2 Distributing K_D and K_{MAC} under a Device Public Key

This section applies when provisioning a Device with a Domain key, K_D.

K_D is the symmetric key-wrapping key used when protecting K_{REK} and K_{MAC} in a Rights Object issued to a Domain *D*. K_D is a 128-bit long AES key generated randomly by the sender and shall be unique for each Domain *D*. K_{MAC} is used for key confirmation of the message carrying K_D.

In this case, exactly the same procedure as in the previous section shall be used, the only difference being the replacement of K_{REK} with K_D.

7.2.3 Distributing K_{REK} and K_{MAC} under a Domain Key K_D

This section applies when protecting a Rights Object for a Domain.

The key-wrapping scheme AES-WRAP SHALL be used. *KEK* in AES-WRAP SHALL be set to K_D and *K* to the concatenation of K_{MAC} and K_{REK}, i.e.:

$$C = \text{AES-WRAP}(K_D, K_{MAC} \mid K_{REK})$$

After receiving *C*, the DRM Device decrypts *C* using K_D:

$$K_{MAC} \mid K_{REK} = \text{AES-UNWRAP}(K_D, C)$$

The following URI shall be used to identify this key transport scheme in **<xenc:EncryptionMethod>** elements:

http://www.w3.org/2001/04/xmlenc#kw-aes128

7.3 Use of Hash Chains for Domain Key Generation

To simplify Domain Key management when several generations of a Domain are expected (see section 8 for information on Domains), an RI may elect to make use of hash chains, and derive later Domain Keys from earlier ones. The procedure to do this is as follows: When creating the Domain, the RI generates a master Domain key, K_M. The RI then hashes (using SHA-1) K_M at least as many times *n* as the RI believes there will be generations of the Domain. The result, $K_{D1} = hash^n(K_M) = sha1(sha1(\ldots(sha1(K_M)))$ is then distributed as described in section 6.3.4.2 as the first key for Domain D. When a Device in a Domain has been revoked, or the RI otherwise decides to create a new Domain generation (shift Domain key), the RI computes and distributes $K_{D2} = hash^{n-1}(K_M)$. Devices supporting this mechanism therefore only need to store K_{Di}, for the latest received Domain generation *i*, since for any earlier generation *j* ($j < i$), $K_{Dj} = hash^{i-j}(K_{Di})$. RIs supporting this mechanism only need to store the current generation number *i*, the maximum number of generations *n,* and the Domain master key K_M.

Support for this mechanism is optional, both for RIs and Devices. As described in sections 5.4.4.1.1 and 5.4.4.2.1, the Device and RI negotiate the use of this mechanism during the 2-pass Domain join protocol.

8. Domains

8.1 Overview

A Domain is a set of Devices that possess a common Domain Key provisioned by a Rights Issuer. Devices in a Domain may share Domain Rights Objects and are able to consume and share any DCFs controlled by Domain Rights Objects.

The OMA DRM Domain concept is network centric. An RI defines the Domains, manages the Domain Keys, and controls which and how many Devices are included and excluded from the Domain. A user may request to add Devices to a Domain before acquiring Domain-bound content, or make these requests incrementally after receiving Domain-bound content.

A Domain is associated with a unique Domain Identifier, which includes a Domain Generation counter, and one or more Domain Keys. Multiple Domain Keys are a result of Domain upgrades performed by the Rights Issuer that manages the Domain. Each Domain Key corresponds to a specific Domain Generation. The value of the Domain Generation counter indicates the number of upgrades performed on the Domain.

Devices may join multiple Domains managed by one or more RIs.

8.2 Device Joins Domain

To join a Domain, a Device must have established, or will establish as part of a successful Join Domain protocol, an RI Context with the RI.

A Device joining a Domain is the process of an RI authorizing a particular Device to be able to use all ROs for this Domain. When a Device joins a Domain it receives the necessary Domain information to be able to install Domain ROs.

A Device executes the Join Domain protocol (see 5.4.4) to join a Domain. The result of a successful Join Domain in the Device is the establishment of a Domain Context for a given Domain. The Domain Context includes Domain Key(s), Domain Identifier(s) and an Expiry Time.

A Device MAY join multiple Domains managed by one or more RIs.

The Join Domain protocol is triggered by the ROAP trigger.

If a Device joins a Domain with multiple Domain Generations (i.e. a Domain where more than one Domain Keys have been issued), the RI SHOULD issue to the Device the Domain Keys of all previous generations of the Domain, to allow use of all ROs bound to this Domain. But, if both the Device and RI are using the hash chain mechanism, the RI only needs to supply the most recent generation Domain key.

8.3 Domain RO Acquisition

To be able to use a Domain RO, a Device must have joined the corresponding Domain.

Domain ROs can be acquired by the same mechanism as Device ROs, using the 2-pass RO Request/Response protocol or the 1-pass RO Response protocol. The Device specifies the Domain Identifier in the RO Request. Domain ROs can also be acquired without being wrapped in a ROAP PDU, e.g. delivered to Devices as a result of a browsing session.

8.4 Device Leaves a Domain

In order for a Device to leave a Domain, it must assure the RI that it has deleted all information about the Domain that enables it to use any ROs for the Domain. When leaving a Domain a Device MAY, but is not required to, remove the corresponding Domain ROs and associated Content. The Device SHOULD obtain user confirmation before deleting Domain ROs and associated Content.

A Device MUST execute the Leave Domain protocol (see 5.4.4) to leave a Domain.

Prior to sending a Leave Domain Request, the Device MUST ensure that the corresponding Domain Context is deleted.

8.5 Support for Multiple Domains per Rights Issuer

To provide flexibility in Domain management, the system supports multiple Domains per Rights Issuer. The Device SHALL support the ability to join multiple Domains for each RI Context it establishes.

To ensure that each DRM Agent is able to provide a minimum level of functionality, a Device SHALL support at least 6 Domains, distributed among the established RI Contexts in any proportion.

The Device MAY optionally support more than 6 Domains. These additional Domains may also be distributed among the established RI Contexts in any proportion.

8.6 Domain RO Processing Rules

8.6.1 Overview

As a general principle, the processing rules for inbound Domain ROs are agnostic to the origin of the Domain RO i.e. it does not matter whether the Domain RO was delivered OTA from a RI or copied from another Device. There is no binding to a specific transport mechanism or protocol.

Domain ROs MAY be delivered to the Device either on the course of the RO acquisition protocol, inside a DCF file, as a separate standalone MIME object, or as part of a MIME multipart/related message [RFC2387]. As part of the installation of an RO, the Device must make a number of checks for all Domain ROs that are to be used by the Device, including integrity and authenticity checks and replay attack related checks as described below.

8.6.2 Inbound Domain RO

The Device MUST support receiving a Domain RO in a ROAP-ROResponse message.

The Device MUST support receiving a Domain RO as a separate object.

The Device MUST support receiving a Domain RO inside a DCF.

Before installing and using a Domain RO to render the media objects inside the associated DCF the Device MUST process the Domain RO as defined in chapter 8.6.2.1.

8.6.2.1 Installing a Domain RO

When a Device receives a Domain RO, it SHOULD compare the **<domainId>** field within the domain-RO with the domainId for any Domains already established with the RI that sent the ROAP trigger, with the sending RI as identified by the **<riID>** field. There are three possible outcomes of this comparison:

1. The **<domainId>** field matches a stored domainId. The Device MAY install the Domain RO.

2. The **<domainId>** field matches the first 18 digits of a stored domainId, but the Domain Generation of the RO is greater than the Generation of the stored domainId. The device MAY attempt to upgrade the Domain by sending an HTTP request to the URL specified in the ***riURL*** attribute of the roap:ROPayload (see section 5.3.8). The Device SHOULD perform this action silently, if the user has given permission for silent communication with this RI. If the user has not given permission for silent communication, the Device MUST acquire the user's consent prior to sending the HTTP request, but SHOULD present messages to the user indicating that the request is for Domain upgrade and not for joining an entirely new Domain.

3. The **<domainId>** field does not match a stored domainId. The Device MAY attempt to join the Domain by sending an HTTP request to the URL specified in the ***riURL*** attribute of the roap:ROPayload. The Device MUST acquire the user's consent prior to sending the HTTP request.

Prior to sending an HTTP request to the URL specified in the riURL attribute of the roap:ROPayload, the Device MUST check the value of the **<riID>** element of the roap:ROPayload. If the value of the **<riID>** element matches that of an riID in a valid RI Context then, the Device MUST verify the signature of the Domain RO using the RI's Public Key. If this verification fails then the Device MUST NOT send an HTTP request to the URL specified in the ***riURL*** attribute of the roap:ROPayload and the Device SHOULD delete the Domain RO.

When the Device sends an HTTP request to the URL specified in the ***riURL*** attribute of the roap:ROPayload, the RI can at this point choose (using its own criteria) whether to allow the Device to join the Domain or not. If the RI chooses to allow the Device to join the Domain then the RI MUST return a *joinDomain* ROAP Trigger to the Device to indicate that the Device should send a roap:JoinDomainRequest message in order to join the Domain. In the event that the RI chooses not to allow the Device to join the Domain the RI MAY offer the user the opportunity to acquire a Device RO.

The Device MUST successfully verify the signature of the Domain RO using the RI's Public Key before installing the Domain RO.

If the Domain RO is stateful**,** then the Device MUST perform the replay protection related checks defined in Section 9.4 .

If the Domain Context has expired (indicated by the Domain Context Expiry Time) the Device MUST NOT install ROs for this Domain and the Device SHOULD delete the Domain Context.

8.6.2.2 Postprocessing after installing the Domain RO

These processing rules apply for Domain ROs that were not received inside a DCF i.e. the Domain RO was received separately from the DCF.

The Device SHOULD only skip further post-processing if it concludes, using an algorithm not defined in this specification, that sending the installed Domain RO to other Devices does not add value for the end user. One such case could be that the Domain Context has expired.

The Device MUST attempt to find the DCF associated with the installed Domain RO. If that fails the Device MUST discontinue post-processing for the time being but SHOULD continue the post-processing if it finds the associated DCF later on e.g. when rendering the DCF or when sending it out from the Device.

If the Device finds multiple DCF instances associated to the installed Domain RO, it SHOULD apply the processing rules defined below for each one of them.

8.6.3 Outbound DCF

For outbound DCFs the Device SHOULD continue a possibly discontinued postprocessing as defined in chapter 8.6.2.2 before sending the DCF from the Device.

If the DCF already contains Domain RO(s), the Device MUST remove the Domain ROs corresponding to Domains which the Device is not member of.

The Device SHOULD insert a copy of the installed Domain RO into the DCF [DRMDCF-v2].

However, the Device SHOULD only choose not to insert a Domain RO if it concludes, using an algorithm not defined in this specification, that replacing does not add value for the end user (for example, if the installed Domain RO is more restrictive, the Domain RO has already been consumed, etc).

8.7 Domain Upgrade

A Rights Issuer may *upgrade* a Domain if, for example, a Domain Key has been compromised or if a Device in the Domain has been revoked. This will probably be a rare event, but may be necessary as a last resort to stop DRM Content from leaking out of the system in the clear.

In order to upgrade a Domain, a RI MUST change the Domain Key and MUST increment the Domain Generation by one. If the Domain Generation value reaches 99 the Domain becomes obsolete. A RI MUST NOT issue ROs for an obsolete Domain and MUST NOT allow new Devices to join an obsolete Domain.

A Domain upgrade does not result in any Domain Context being deleted in any Device. After an upgrade, Domain ROs issued before the upgrade may still be used and shared. This applies to all Devices (revoked and unrevoked) previously in the Domain, and to any new Devices added to the Domain after the upgrade.

A Rights Issuer performs a Domain upgrade using the Join Domain protocol (see sections 8.2 and 5.4.4). An RI MAY initiate this protocol for the purposes of Domain upgrade by sending a ROAP trigger to a Device whose Domain membership it wishes to upgrade. If a Device receives a Join Domain ROAP trigger, it SHOULD compare the **<domainID>** field with the domainId for any domains already established with the RI that sent the ROAP trigger, with the sending RI as identified by the **<riID>** field. There are two possible outcomes of this comparison:

1. The **<domainID>** field matches the first 18 digits of a stored domainId, but the value of the Domain Generation in the trigger is greater than the value stored by the Device. The incoming trigger represents a Domain upgrade, as described in this section. The Device SHOULD in this case silently upgrade the Domain using the Join Domain protocol, if the user has given permission for silent communication with this RI and if the trigger was authenticated. If the user has not given permission for silent communication, or if the trigger was not authenticated, the Device MUST request user permission to upgrade the Domain, but SHOULD present appropriate messages to the user indicating that the request is for Domain upgrade and not for joining an entirely new Domain.
2. If the **<domainID>** field does not match a stored domainId, then the Device is not a member of the Domain. The Device MUST behave as if it had received a domain-RO for a Domain it was not a member of, as specified in section 8.6.2.1.

8.7.1 Use of hash chains for Domain key management

To avoid storage of multiple keys per Domain in the Device and in the RI (for the purpose of using old and new Domain ROs after Domain upgrade) it is possible to have a relation between the Domain Keys using Hash Chains (see section 7.3), as illustrated in the example below. The Device MAY support Hash Chains and the RI MAY support Hash Chains.

Example1. Without hash chains

When generating a new Domain, the RI generates:

- a unique Domain Identifier DI, the Domain Generation is set to 00.
- a random secret Domain Key DK_0

At Domain upgrade the Domain Generation *g* is increased by 1, which is reflected in the Domain Identifier, and a new Domain Key DK_g is generated. The old Domain Key(s) must be stored in RI and Device to allow use of ROs issued before the upgrade. When Devices join a Domain, all Domain Keys of this Domain are sent in the Protected Domain Info of ROAP-JoinDomainResponse (see ROAP protocol suite).

Example 2. With Hash Chains (optional)

When generating a new Domain, the RI

- generates a unique Domain Identifier DI, the Domain Generation is set to 00.
- generates a secret random number R
- selects the maximum number of generations n for this Domain (not larger than 99)
- defines a sequence of Domain Keys using R and applying the efficient hash function SHA1 iteratively
    - $DK_n = R$ corresponding to DI with Domain Generation n
    - $DK_{n-1} = SHA1(DK_n)$ corresponding to DI with Domain Generation n-1 etc. until
    - $DK_0 = SHA1(DK_1)$ corresponding to DI with Domain Generation 0

Since old Domain Keys (with low generation value) are possible to efficiently derive from new Domain Keys (with higher generation value), it is only necessary to store the newest Domain Key in the Device (and corresponding Domain Identifier so the Domain Generation is known). For the RI it is sufficient to store DK_n (=R).

9. Protection of Content and Rights

9.1 Protection of Content Objects

The Content Objects are protected by symmetric key encryption. The details of the content format are specified in [DRMCF-v2] document. Protecting content confidentiality is a key part of the DRM system. Only the intended Devices must be able to decrypt the content. To accomplish this content protection, the Rights Issuer MUST encapsulate the Content Encryption Key (CEK) in a Rights Object. This Rights Object, in turn, is protected as described in Section 7.2 to ensure that only the intended Devices may access the CEK and therefore the Protected Content.

For integrity protection of the DCF, a cryptographic hash value of the DCF is generated and inserted into the Rights Object. This hash value MUST be generated over the entire DCF, including all the elements and the headers except for the FreeSpace box, if present. This box is subject to change by the Device as defined in section 12.2. DRM Agents in client Devices MUST verify that the hash value in the Rights Object is identical to the hash value calculated by the DRM Agent over the DCF. If the hash values are not identical, the DRM Agent MUST prohibit the DCF from being decrypted and used.

9.2 Composite Content Objects and Associated Rights Objects

9.2.1 Multiple Rights for Composite Objects

A Rights Object can contain one or more Permissions and Constraints (i.e. multiple rights). Each set of Permissions and Constraints is identified by a unique identifier, and uniquely associated with a Media Object by the identifier. One Rights Object may contain Permissions that are associated with Media Objects contained in separate DRM Containers (DCFs). Some example use cases include:

- Multiple DCFs delivered at different times (e.g. subscription-based MMS where several MMS messages are sent to a user)
- Multiple DCFs delivered at the same time but not encapsulated in a single package (e.g. streaming media (audio stream and video stream)).
- Multiple DCFs delivered at the same time and in a single package that is not a DCF (e.g. an MMS message containing several pictures, each encapsulated in its own DCF)

The Rights Objects can also specify permissions and constraints for each of the individual Media Objects within a Multipart DCF. In this case, the individual Media Objects can be referenced separately by the Rights Object associated with the Multipart DCF.

9.2.1.1 Multiple Rights for Multipart DCFs

A Multipart DCF contains multiple separate Media Objects, e.g., a theme consisting of a ringing tone and a logo. When Permissions are associated with a Multipart DCF, there are two types of relation between the Permissions and the Media Objects inside the Multipart DCF. One is that the same Permissions and Constraints are associated with all individual Media Objects in the Multipart DCF. For example, when a Multipart DCF contains three images as separate Media Objects, a Content Provider can grant a user a single Permission to display all three images in the Multipart DCF. Another case is where individual Permissions are associated with individual Media Objects inside a Multipart DCF. For example, when a Multipart DCF contains an audio file and two images, a Content Provider can grant a user the Permissions to play the audio data, display the two images, and print the second image three times.

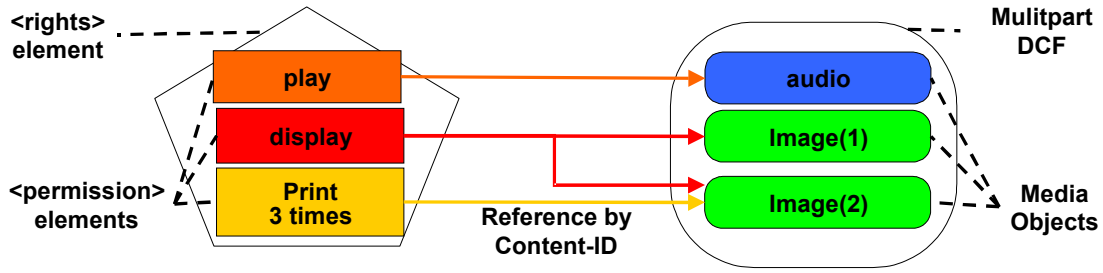

Figure 7: Multiple Rights for Multipart DCFs

When multiple Media Objects in a Multipart DCF are associated with individual Permissions, each individual Media Object MUST have an individual Content-ID assigned within the Multipart DCF for reference by the Rights Object. Also, common Permissions and Constraints can be associated with all Media Objects in a Multipart DCF.

Another case is where a Media Object is a Composite Object, i.e. it contains other Media Objects by means of inclusion. Such a Composite Object can have assigned only a single Content-ID which can be referenced by a Rights Object. Permission and Constraints expressed referring to the Composite Object Must be applied to all individual Media Objects contained in the Composite Object (e.g. the images and audio files contained in a zip archive).

9.3 Protection of Rights Objects

In the OMA DRM Architecture, a given Content Object is associated with one or more Rights Objects. The Rights Object is made up of the required header information, security elements, and the rights information for the associated Content Object. The Rights Objects are acquired by the Device as a result of a successful completion of the Rights Object Acquisition Protocol or through sharing in a Domain.

Integrity protection prevents un-authorized modification of the rights information within the Rights Object. The syntax and semantics of the Rights Object is specified in the [DRMREL-v2] document. The [DRMREL-v2] specification calls for the use of XML-DSIG to create a digital signature over the set of elements that need integrity protection. The DRM Agent MUST verify the digital signature, when available, within the Rights Object, before the associated content is made available to the user. Use of the digital signature provides the client the ability to verify the authenticity & integrity of the information. The Rights Issuer MUST provide the certificate chain necessary to validate the signature either during the ROAP session or by use of “out-of-band” methods.

If a Rights Object is associated with a composite Content Object, all the rights expressions for the component elements MUST be included within a single <ds:Signature> element. If a Rights Object is associated with a composite Content Object, it may contain a number of CEKs to enable the encryption/decryption of component elements with different keys.

The Rights Object MUST be assigned a unique identifier by the Rights Issuer.

9.4 Replay Protection of Stateful Rights Objects

9.4.1 Introduction

Rights Objects containing permissions with constraint elements such as <count>, <interval>, or <accumulated> requires the current state of the usage permissions to be maintained in the DRM Agent. In contrast with stateless rights, there has to be a mechanism to protect against an attacker replaying the reception of such *stateful* ROs to the Device, which could cause an unauthorized extension of the permissions.

In certain variants of RO acquisition described in this specification such a replay protection mechanism is inherent in the protocol. In particular, the 2-pass RO Acquisition protocol contains a Device nonce, sent in the RO request and sent back and signed in the RO response. The DRM Agent compares an incoming correctly signed RO

Response with the nonce in a sent RO Request and unless there is a match, the RO is rejected and replay of the RO Response is not possible. RI authentication provided by the 2-pass protocol can thus be used to control replay.

In contrast, the 1-pass RO Acquisition protocol or the sharing of ROs in a Domain does not offer a challenge/response mechanism. 1-pass ROAP offers a limited replay protection through the time-based RI authentication, but it is not optimal in that the synchronization between RI and Device cannot be guaranteed.

To accommodate for this, a local *replay cache* will be kept in the Device. Logically, the replay cache is a table where each entry contains a Globally Unique RO Identity (GUID) for a received, stateful RO, and the RI Time Stamp for the RO. The GUID must be unique for each instance of the RO (or else a user who legitimately twice in a row buys the same stateful RO could be seen as mounting a replay attack).

When stateful ROs with GUIDs and time stamps are received, they will be compared with previously received stateful ROs in the replay cache. If there is a match with an existing entry, the newly received RO will not be installed. When the replay cache is full, ROs with newer (later) time stamps replace entries with older time stamps and ROs with time stamps older than the oldest time stamp in the cache are rejected. This mechanism provides a secure replay protection. Appropriate sizing of the replay cache minimizes the risk that a long delivery time of one stateful RO in combination with mass distribution of other stateful ROs with later time stamps causes the delayed RO to be rejected (in situations of mass distribution of stateful ROs, the RI could use the 2-pass ROAP protocol since that has an inherent replay protection mechanism that does not interfere with the mechanism described here.).

A limitation of the method described above is that sharing of Domain ROs with very old time stamps may be affected by the finiteness of the replay cache. A second mechanism is therefore included to eliminate this limitation. This second mechanism defines a *separate* replay cache for ROs with a GUID, but without a timestamp. GUIDs of new ROs without timestamps will then be compared to GUIDs in the GUID-only replay cache. If there is a match, the RO is rejected; otherwise it is accepted and the replay cache is updated. If the GUID-only replay cache is full, a previous entry is removed to give room for the GUID of the new RO. This mechanism does not limit sharing of ROs but is possible to circumvent, since it is possible to replay stateful ROs with GUIDs that has been deleted from the cache.

The reason for having separate replay caches is that the secure mechanism based on timestamps and GUIDs should not be affected by the latter, more limited, replay protection mechanism. A separate replay cache for GUID-only entries still provides a certain degree of protection for corresponding ROs, allowing RIs to balance security interests against the risk of unintentional rejection of "old" Domain ROs.

9.4.2 Replay Protection Mechanisms

This section defines two mechanisms enabling protection against Device RO as well as Domain RO replay attacks.

The OMA DRM Release 2 replay protection mechanisms are intended to support the use case of stateful Device ROs or Domain ROs that are delivered without a prior RO Request, i.e. in the 1-pass ROAP, or Domain ROs delivered outside of ROAP. In the case of Domain ROs, the statefulness is **per Device** in the Domain. E.g. if a Domain RO with a count 3 constraint is successfully shared between Devices, each Device is allowed 3 uses.

The **roap:ROPayload** type contains two components for stateful RO replay protection management: the Globally Unique ID attribute ***id*** and the RI Time Stamp element **<timeStamp>**. In addition, the RI indicates that an RO is stateful by setting the ***stateful*** attribute to **True**. The **<timeStamp>** element is optional and provides the RI with two different methods for replay protection: Replay protection with and without RI-assigned timestamps (RITS). These methods are described in the following.

A Device MUST have two (logical) replay caches: one with <GUID, RITS> entries for ROs with GUIDs and RITS, and one with <GUID> entries for ROs with GUIDs only. The Device MUST protect the integrity of its replay caches. A Device MUST have a documented size of the replay caches. It is recommended that each replay cache is able to store at least 100 entries.

9.4.2.1 Stateful ROs with RI Time Stamps

This replay protection mechanism is applicable to both Device ROs and Domain ROs and is secure, i.e. it can guarantee protection against replay attacks. However, in the Domain case, subsequent sharing may be restricted by the replay protection mechanism and cannot be guaranteed. In particular, a receiving Device may reject Domain ROs that are shared long after they have been received from the RI.

When receiving a stateful RO with a **<timestamp>** element (RITS), the Device MUST perform the following procedure:

a) If the RITS is more than 24 hours in the future when compared to the Device DRM Time then the Device MUST reject the RO. The user MUST be informed of the event and of the present Device DRM Time, and SHOULD be asked if the Device DRM Time is correct. If the DRM Time is not correct the Device SHOULD initiate Device DRM Time synchronization by re-registering with the RI using the Registration protocol.

b) Failing a), if the GUID for the RO is already in the <GUID, RITS> replay cache then the Device MUST reject the RO.

c) Failing b), if the <GUID, RITS> replay cache is not full, the Device MUST accept the RO and insert the ROs GUID and RITS values as an entry in the replay cache. Note: The GUID value is the id attribute of the roap:ROPayload.

d) If the replay cache is full, and the RITS is before the earliest RI Time Stamp in the replay cache the Device MUST reject the RO.

e) Otherwise – if the replay cache is full, and the RITS is after the earliest RI Time Stamp in the replay cache the Device MUST accept the RO and insert the corresponding <GUID, RITS> values as an entry in the replay cache, by deleting the cache entry with the earliest RITS value.

9.4.2.2 Stateful ROs without RI Time Stamps

This replay protection mechanism is mainly intended for Domain ROs. It does not restrict subsequent sharing, installation or usage of Domain ROs but it is less secure than the mechanism in Section 9.4.2.1 and it does not guarantee replay protection. Hence, if protection from replay of a stateful RO is important, the RI should include an RI Time Stamp in the RO payload. If indefinite sharing of stateful Domain ROs in a Domain is important and it is acceptable that, with some effort from an attacker, this stateful RO may be replayed, then the RI should not include an RI Time Stamp in the RO payload.

When receiving a stateful RO without a **<timestamp>** element, the Device MUST perform the following procedure:

a) If the RO's GUID is in the GUID-only replay cache then the Device MUST reject the RO.

b) Failing a), if the GUID-only replay cache is not full, the Device MUST accept the RO and insert the RO's GUID value as an entry in the cache.

c) Otherwise – if the GUID-only replay cache is full, the Device MUST accept the RO and insert the RO's GUID value as an entry in the GUID-only replay cache by deleting an existing entry in the cache. The Device MAY use FIFO in the GUID-only replay cache or MAY select a random entry for deletion.

9.5 Subscription Rights Object

A Rights Object may specify Rights for content acquired as part of a subscription. In this case, the Rights Expression will inherit Permissions for the digital asset from another Subscription Rights Object, using the <inherit> syntax as specified in [DRMREL-v2].

In this section, the Rights Object that inherits permissions is referred to as a Content Rights Object (C-RO). The Rights Object that contains the Permissions that are inherited is referred to as a Subscription Rights Object (S-RO).

Client Devices MUST verify that the Content Rights Object and its related Subscription Rights Object were issued by the same Rights Issuer before the associated content is made available to the user.

9.5.1 Subscription Rights Objects and Domains

A Rights Issuer MAY bind Content Rights Objects and Subscription Rights Objects to a Device or to a Domain. The permission inheritance mechanism described in this section is independent of the cryptographic binding of the Rights Objects.

9.5.2 Semantics of stateful constraints

The DRM Agent MUST maintain the state of any stateful constraint relative to the Rights Object in which the constraint appears, and not relative to any single Media Object. If only one Media Object references a Rights Object, the DRM Agent will interpret the stateful constraints in the Rights Object as applying to that one Media Object. If more than one Media Object references a Rights Object, directly or by inheritance (see section 9.5 above), the DRM Agent MUST interpret the stateful constraints as applying collectively to all Media Objects that reference that Rights Object.

The figure below illustrates these semantics in the context of a Subscription Rights Object. Two Content Rights Objects inherit permissions from a single Subscription Rights Object. On the left side, each C-RO specifies a <play> permission with a count constraint. The constraint applies individually to the content item linked to the C-RO. The user may use DCF-1 up to 5 times, and DCF-2 twice. On the right side, the S-RO specifies the constrained <play> permissions. In this case, the user may use either DCF up to a total of 7 times. This may be 4 uses of DCF-1 and 3 uses of DCF-2, or even no uses of DCF-2 and 7 uses of DCF-1.

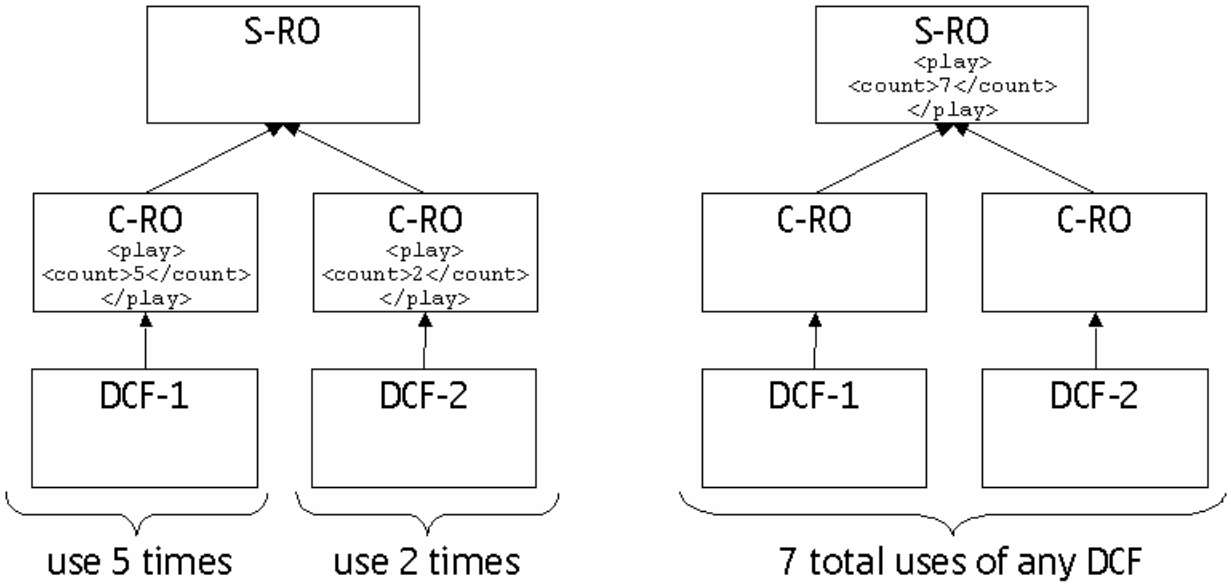

Figure 8: Subscription ROs and Associated Semantics

9.6 Off-Device Storage of Content and Rights Objects

Because Devices have a limited amount of storage space in which to store Protected Content and Rights Objects, users may desire to move Protected Content and Rights Objects off the Device, e.g. to removable memory, a personal computer, or a network store to make room for new Protected Content and Rights Objects. A given Rights Object can be insterted into the corresponding DCF for purposes of storage and simplicity in managing the

objects. At some later point in time, they may want to retrieve said Protected Content and Rights Objects from the remote storage back onto the Device store.

As explained in earlier sections of this specification, both the Protected Content and Rights Objects are protected and bound to a specific Device or a Domain. For this reason, Protected Content and Rights Objects MAY be allowed to leave the Device provided the following conditions are met:

- The Rights Object MUST not contain any stateful constraints. Stateful constraints include <interval>, <count>, <export> and <accumulated> as defined in [DRMREL-v2].
- The Protected Content and the Rights Objects MUST be in a protected form, meaning they cannot be accessed by any other Device/Domain than the original intended Device/Domain to which the rights were issued.

10.Capability Signalling

When Devices contact Content Issuers and Rights Issuers, the Devices need to advertise their capabilities. This allows Content Issuers and Rights Issuers to customize content, purchase options, and so forth based upon the features and functionalities of the Device, thereby improving the overall user experience. OMA DRM relies upon two mechanisms for advertising Device capabilities: HTTP headers [HTTP] and User Agent Profile [UAProf].

10.1 HTTP Headers

When a Device uses HTTP to communicate with Content Issuers and Rights Issuers, the Device MUST advertise support for the following media types using the HTTP Accept header:

- application/vnd.oma.drm.ro+xml (DRM Rights Object)
- application/vnd.oma.drm.dcf (DRM Content Format)
- application/vnd.oma.drm.roap-pdu+xml (DRM ROAP PDUs)
- application/vnd.oma.drm.roap-trigger+xml (DRM ROAP Trigger)

In addition to the supported media types, Devices MUST advertise the DRM version using the "<major>.<minor>" format defined below. The version number advertised by OMA DRM v2 Devices MUST match the DRM Enabler Release version that the Device supports.

```
DRM Version = "DRM-Version" ":" *DIGIT "." *DIGIT
```

10.2 User Agent Profile

OMA DRM v2 Devices SHOULD advertise supported DRM methods, permissions, constraints, media types,, version and if supported, its external DRM capabilities using UAProf. "External DRM" refers to a DRM system to which the Device is able to export OMA DRM protected content, for example, a DRM system used on a memory card. See Appendix D for an example.

If the Device supports UAProf, then the Device MUST advertise the attributes in the table below as indicated in the "MUST Advertise" column.

The attributes pertaining to an external DRM system MUST be included if the Device is capable of exporting OMA DRM protected content to such a system. The attributes MUST NOT be included if the Device is incapable thereof.

UAProf Attribute	Description	Example Values	MUST Advertise
DrmClass	DRM v1 Conformance Classes as defined in [DRM]	"ForwardLock", "CombinedDelivery", "SeparateDelivery"	"ForwardLock" plus other supported DRM v1 methods
DrmPermissions	Optional DRM permissions that are supported as defined in [DRMREL] or [DRMREL-v2]	"play", "display", "execute", "print"	Supported permissions using the same syntax as defined in the REL specification.
DrmConstraint	Optional DRM permission constraints as defined in [DRMREL] or [DRMREL-v2]	"datetime", "interval", "accumulated"	Supported constraints using the same syntax as defined in the REL specification.

DrmMediaTypes	Media types the Device supports inside a DCF	"image/gif", "audio/midi", "video/3gpp"	Media types supported inside a DCF, expressed as MIME media types [RFC2045].
DrmVersion	DRM Enabler Release version supported by the client	“2.0”	Supported DRM Enabler Release version in “<major>.<minor>” format.
ExtDrmName	Name of the external DRM	"Very Secure Card"	A textual name of the external DRM system. Well-defined names for external DRM systems are managed by OMNA.

Table 11: User Agent Profile Attributes

10.3 Issuer Responsibilities

When a Content Issuer or Rights Issuer receives a request from a Device indicating that the Device supports OMA DRM version 2.x (any minor version of the DRM v2 specs), the:

- Content Issuer MAY issue Forward Locked Content.
- Content Issuer MAY issue Combined Delivery Content and the Rights Object within the DRM Message is DRM v1.0 Rights Object, only if the Device advertises support for Combined Delivery.
- Content Issuer MAY issue Separate Delivery Content only if the Device advertises support for Separate Delivery.
- Content Issuer MAY issue Separate Delivery Content encapsulated in a DRM Message, only if the Device advertises support for Separate Delivery.
- Rights Issuer MAY issue a DRM v1 Rights Object for Separate Delivery Content, only if the client advertises support for Separate Delivery.
- Content Issuer SHOULD issue DRM v2 content.
- Content Issuer MAY issue DRM v2.0 Content encapsulated in a DRM Message.
- Rights Issuer SHOULD issue a DRM v2.0 Rights Object for DRM v2.0 Content.
- Rights Issuer SHOULD send the ROAP Trigger to initiate the ROAP protocol (see section 5.2.1).
- Rights Issuer MUST NOT issue any DRM v2.0 Rights Object for Combined Delivery Content, even if the Device advertises support for Combined Delivery.
- Rights Issuer MUST NOT issue any DRM v2.0 Rights Object for Separate Delivery Content, even if the Device advertises support for Separate Delivery.
- Rights Issuer MUST NOT issue any DRM v1.0 Rights Object for DRM v2.0 Content.

11.Transport Mappings

The following sections describe how ROAP PDUs are delivered using typical delivery protocols, the most common being HTTP. Examples are illustrated in Appendix I.1.

11.1 HTTP Transport Mapping

11.1.1 HTTP Features

The Rights Issuer MAY use standard HTTP features such as HTTP redirections, etc.

The DRM Agent MUST support all mandatory HTTP features according to [HTTP].

11.1.2 RI Hello

If HTTP is used as the transport, an RI Hello message MUST be sent as an HTTP response with the ROAP PDU as the body of the request. The ROAP PDU MUST comprise only a single valid RI Hello message.

11.1.3 RO Response

If HTTP is used as the transport, an RO Response message MUST be sent as an HTTP response with the ROAP PDU either as the body of the response or as an entity in a multipart/related response [RFC2387]. The ROAP PDU MUST comprise only a single valid RO Response message.

11.2 OMA Download OTA

A Rights Issuer MAY use OMA Download OTA [DLOTA] when delivering Content and Rights Objects in order to take advantage of managed download features such as terminal capability negotiation and installation notification. For example, a Rights Issuer may use the OMA Download OTA installation notification as a billing trigger.

Depending on specific deployment and business scenarios, OMA Download OTA can be used in different ways in the context of delivering protected content and Rights Objects. Appendix I.2 illustrates this with the help of a few examples, but is not meant to be an exhaustive collection of deployment scenarios.

11.2.1 Download Agent and DRM Agent Interaction

The Download Agent must collaborate with the DRM Agent when OMA Download OTA is used to deliver content and/or Rights Objects. In general, the DRM Agent will participate in the “Installation” phase of the Download OTA protocol.

The Download OTA protocol utilizes a Download Descriptor (DD) to provide information to the user and the Device prior to initiating the content object download. The following sections describe how the Download Agent and DRM Agent should behave when the Download Descriptor is used for DRM purposes.

11.2.1.1 Downloading DRM Content

When using Download OTA to download a DRM protected content object (that is, an encrypted content object packaged in the DRM content format), the Download Descriptor:

- MUST include *type* attribute indicating the MIME type for each of the object(s) to be downloaded.
- MUST include a *size* attribute indicating the size of the entire DRM Content Format object (which includes the encrypted content object)

- MUST include an *objectURI* attribute pointing to the protected content object.
- MAY include other optional attributes.

The Download Agent will process the Download Descriptor and perform the content object download as defined in [DLOTA].

The Download Agent SHOULD support the *nextURL* attribute of the Download Descriptor since two ore more download transactions may be concatenated by the *nextURL*. For instance, the *nextURL* attribute of the Download Descriptor of a first download transaction for a DCF may point to the Download Descriptor of a second download transaction for the download of a ROAP Trigger.

11.2.1.2 Downloading ROAP Trigger or Rights Objects

A Device supporting OMA Download OTA for the download of a ROAP Trigger or a Rights Object MUST support the co-delivery method.For the co-delivery method, as defined in the [DLOTA] the Download Descriptor MUST be the first entity in the multipart, and the ROAP Trigger, or the Rights Object MUST be the second entity of the multipart.

If Download OTA separate delivery method is used, the *objectURI* in the Download Descriptor will provide the URL for retrieving the ROAP Trigger. The Download Agent, upon receiving the Download Descriptor, will retrieve the ROAP Trigger and deliver it to the DRM Agent for installation as defined in the Download OTA specification.

When using OMA Download OTA for delivery of the ROAP Trigger or the Rights Object, the Download Descriptor:

- MUST include *type* attribute(s) indicating the MIME type(s) of the object(s) being downloaded.
- MUST include an *objectURI* attribute containing the Content-ID of the ROAP Trigger in the multipart if the ROAP Trigger is co-delivered with the Download Descriptor. Otherwise, this attribute MUST contain the URL with which the Device may retrieve the ROAP Trigger
- MUST include a *size* attribute indicating the size of the object(s) being downloaded.
- MAY include other optional attributes.

When the Download Agent receives the ROAP Trigger (either via co-delivery or separate delivery), the Download Agent MUST send the ROAP Trigger to the DRM Agent after processing the Download Descriptor as defined in [DLOTA]. [DLOTA] requires that the Download Agent should use the information in the Download Descriptor to give the user a chance to confirm that they want to install the media object. In order to provide the desired end user experience, there is one exception:

- Where the value of a *type* attribute in the Download Descriptor indicates the MIME type of the ROAP Trigger or of the Rights Object then the Download Agent SHOULD NOT present the user with a user confirmation.

Upon receiving the ROAP Trigger, the DRM Agent MUST initiate the ROAP as defined in section 5.1.6 . The DRM Agent MUST notify the Download Agent of installation success or failure (including an appropriate error code as defined in [DLOTA]).

As defined in OMA Download OTA, the Download Agent MUST make a best effort attempt to send an installation status report to the Rights Issuer provided the *installNotifyURI* is present in the DD.

In case the download OTA is used for downloading the Rights Object using 1-pass delivery without the ROAP Trigger itself then the Rights Object (instead of the ROAP Trigger) is co-delivered with the Download Descriptor.

11.2.1.3 Downloading DRM Content and Rights Object Together

When using OMA Download OTA to download a Rights Object, the Download Descriptor MUST be co-delivered with the ROAP Trigger to download DRM Content and Rights Object together. If OMA Download OTA is used to download the Rights Object and DRM Content in a single multipart message, the Download Descriptor:

- MUST include type attribute(s) indicating the MIME type(s) of the object(s) being downloaded.
- MUST include an *objectURI* attribute containing the Content-ID of the ROAP Trigger in the multipart.
- MUST include a *size* attribute indicating the size of the Rights Object plus the size of the DRM Content.
- MUST include one or more type attributes with the content type of the protected content objects
- MAY include other optional attributes.

When the Download Agent receives a Download Descriptor and the ROAP Trigger, the Download Agent MUST send the ROAP Trigger to the DRM Agent after processing the Download Descriptor as defined in [DLOTA]. Upon receiving the ROAP Trigger, the DRM Agent MUST initiate the ROAP as defined in section 5.1.6. The Rights Issuer MUST provide the RO Response PDU and DRM Content in a multipart/related media type [RFC2387]. The RO Response PDU MUST be the first entry in the multipart and the DRM Content MUST be the second entry in the multipart. The DRM Agent MUST extract the RO Response PDU and DRM Content from the multipart and process both entities. The DRM Agent MUST notify the Download Agent of installation success or failure. As defined in [DLOTA], the Download Agent MUST make a best effort attempt to send this installation status to the Rights Issuer provided the *installNotifyURI* is present in the DD.

11.3 WAP Push

11.3.1 Push Application ID

The well-known value for the Push Application ID of the DRM User Agent Push remains unchanged from OMA DRM 1.0:

- URN: x-wap-application:drm.ua

- Number: 0x08

Rights Issuers and Content Issuers MUST use this Push Application ID when using WAP Push to deliver DRM Content or Rights Objects to the DRM Agent.

11.3.2 Content Push

A ROAP-ROResponse PDU MAY be delivered using WAP Push [PUSHOTA].

The DRM Agent MUST be able to receive and process a ROAP PDU that is pushed using the Push Application ID defined above.

A ROAP Trigger MAY be delivered using WAP Push [PUSHOTA].

The DRM Agent MUST be able to receive and process ROAP Triggers that are pushed to the DRM Agent using the Push Application ID defined above.

11.4 MMS

The Multimedia Messaging Service (MMS) may be used to transfer Protected Content in MMS Protocol Data Units (PDUs) as defined in [MMSENC]. In regard to DRM two use cases need to be distinguished:

a) The Protected Content is referenced from within the SMIL presentation description of the multimedia message (ie it can be rendered as part of a multimedia presentation).

b) The Protected Content is not referenced from within the SMIL presentation description of the multimedia message. This content can be handled by the Device independently from MMS.

If a multipart DCF is referenced from within the SMIL presentation description the first object is assumed to be the referenced Content Object. The reference for the Content Object is the header field “Content-Location” or “Content-ID” which is associated with the body part of the MMS message. This must not be confused with the Content-ID inside the DCF, which is used as a reference for the Rights Object.

An Example is illustrated in Appendix I.3.

11.5 ROAP over OBEX

11.5.1 Overview

OBEX is a protocol for exchanging objects. It can be used with Bluetooth, infrared, USB and RS232 and other bearers. The requirements of this document refer to [OBEX] version 1.3.

OBEX is a session-oriented protocol, which allows multiple request/response exchanges in one session. An OBEX session is initiated by an OBEX CONNECT request, and is established when the other Device returns a success response. The connection is terminated by sending a OBEX DISCONNECT request.

In this specification a Connected Device that supports the functionality to provide connectivity for Unconnected Devices (as specified in section 14) MUST contain an OBEX client and an Unconnected Device MUST contain an OBEX server.

When a session has been established, ROAP messages originating from the RI MUST be transferred from the Connected Device to the Unconnected Device using the OBEX PUT method. The Unconnected Device acknowledges the data, by sending a response with a status code, and possibly also containing some ROAP data.

ROAP requires that an OBEX connection is established. Connectionless OBEX cannot be used with ROAP.

Example messages are illustrated in Appendix I.4.

11.5.2 OBEX Server Identification

The ROAP-OBEX server is identified by the following UUID (to be used as a value for the "Target" header in OBEX CONNECT operations):

```
1d29f667-3236-374a-bf63-3c7a023bb17d
```

11.5.3 OBEX Profile

11.5.3.1 OBEX operations

The table below shows the OBEX operations that are used by the ROAP OBEX profile. Connected Devices that support the functionality to provide connectivity for Unconnected Devices (as specified in section 14) and Unconnected Devices MUST support these OBEX operations.

OBEX Operation	Opcode
Connect	0x80
Disconnect	0x81
Put	0x02 (0x82)
Get	0x83
Abort	0xFF

11.5.3.2 OBEX headers

The table below shows the OBEX headers that are used in the ROAP OBEX profile. Connected Devices that support the functionality to provide connectivity for Unconnected Devices (as specified in section 14) and Unconnected Devices MUST support these OBEX operations.

OBEX Header	Header Identifier	Comment
Type	0x42	application/vnd.oma.roap-pdu+xml
Length	0xC3	
Target	0x46	Required in CONNECT requests.
Who	0x4A	Identifies responding server in responses to CONNECT requests
Connection Id	0xCB	Value is set by the Connected Device in response to the CONNECT operation
Body	0x48	Carries ROAP PDUs; present if there is a need to send the PDU in several chunks.
End of Body	0x49	Carries ROAP PDUs.

11.5.3.3 OBEX Connect

The OBEX CONNECT operation SHALL contain the following OBEX fields and headers:

Field/Header	Name	Explanation/Value
Field	Opcode for CONNECT	0x80
Field	Packet length	Varies
Field	OBEX version	0x10 (for version 1.0 of the OBEX *protocol*)
Field	Flags	Varies; normally all zero
Field	Maximum packet length	Varies
Header	Target	`1d29f667-3236-374a-bf63-3c7a023bb17d`

The response code to a successful OBEX CONNECT operation SHALL be 0xA0. The following fields and headers SHALL be present in the response:

Field/Header	Name	Explanation/Value
Field	Response code	0xA0 for success
Field	Packet length	Varies
Field	OBEX version	0x10 (for version 1.0 of the OBEX *protocol*)
Field	Flags	Varies; normally all zero
Field	Maximum packet length	Varies
Header	Who	Shall have same value as the preceding "Target" header
Header	Connection ID	Identifies the connection

11.5.3.4 OBEX Disconnect

An OBEX DISCONNECT request SHALL contain the following fields and headers:

Field/Header	Name	Explanation/Value
Field	Opcode for DISCONNECT	0x81
Field	Packet length	Varies
Header	Connection ID	As established in the response to the CONNECT operation

The response code to a successful OBEX DISCONNECT operation SHALL be 0xA0. The following fields and headers SHALL be present in the response:

Field/Header	Name	Explanation/Value
Field	Response code	0xA0 for success
Field	Packet length	Varies

11.5.3.5 OBEX Abort

Note: The OBEX ABORT operation MAY be used to abort a multi-packet operation before it would normally end.

The OBEX ABORT operation SHALL, when requested, contain the following fields and headers:

Field/Header	Name	Explanation/Value
Field	Opcode for ABORT	0xFF
Field	Packet length	Varies
Header	Connection ID	As established in the response to the CONNECT operation

The response code to a successful OBEX ABORT operation SHALL be 0xA0 (or else the client will simply disconnect the OBEX connection). The following fields and headers SHALL be present in the response:

Field/Header	Name	Explanation/Value
Field	Response code	0xA0 for success; otherwise the client will disconnect with a failure indication
Field	Packet length	Varies

11.5.3.6 OBEX PUT

The OBEX PUT operation SHALL contain the following OBEX fields and headers:

Field/Header	Name	Explanation/Value
Field	Opcode for PUT	0x02 or 0x82 (0x02 is used for non-terminal chunked messages, 0x82 is used for the terminal packet in a chunked message)
Field	Packet length	Varies
Header	Connection ID	Varies
Header	Type	Application/vnd.oma.roap-pdu+xml
Header	Body, End of Body	End of Body identifies the last chunk of an object; for other chunks the Body header shall be used.

In addition to these headers, the Length header MAY be used to indicate the complete length of an object

The response code to a successful OBEX PUT operation SHALL be 0xA0 or 0x90, depending on whether the PUT operation was non-final (0x02) or final (0x82). The following fields and headers SHALL be present in the response:

Field/Header	Name	Explanation/Value
Field	Response code	0x90 (Continue) or 0xA0 (Success) for success
Field	Packet length	Varies

In addition, the following headers SHALL be present when the result of the OBEX PUT operation triggers the transmission of a ROAP message from the unconnected Device to the ROAP server (through the Connected Device):

Field/Header	Name	Explanation/Value
Header	Type	application/vnd.oma.roap-pdu+xml
Header	Body, End of Body	End of Body is used for last chunk of an object, for other chunks the Body header shall be used.

The response code shall be 0x90 when the size of the ROAP message in the response requires "chunking" (see [OBEX]). In this case, and in order to retrieve remaining parts, the Connected Device shall issue OBEX GET requests until it receives a response with response code 0xA0 (see below).

11.5.3.7 OBEX GET

The OBEX GET operation SHALL contain the following OBEX fields and headers:

Field/Header	Name	Explanation/Value
Field	Opcode for GET	0x83
Field	Packet length	Varies
Header	Connection ID	Varies
Header	Type	application/vnd.oma.roap-pdu+xml

The response code to a successful OBEX GET operation SHALL be 0xA0 or 0x90, depending on whether the message contains the complete (final part) of the object or not. The following fields and headers SHALL be present in the response:

Field/Header	Name	Explanation/Value
Field	Response code	0x90 (Continue) or 0xA0 (Success) for success
Field	Packet length	Varies
Header	Body, End of Body	End of Body is used for last chunk of an object, for other chunks the Body header shall be used.

The response code shall be 0x90 when the size of the object requires "chunking." In this case, and in order to retrieve remaining data, the Connected Device SHALL continue to issue OBEX GET requests until it receives a response with response code 0xA0.

11.5.4 Exchanging ROAP messages over OBEX

ROAP messages originating from the RI are sent from the Connected Device to the Unconnected Device using the OBEX PUT operation. When receiving a ROAP Trigger that contains the *proxy* attribute and which is therefore

not intended for the Connected Device the Connected Device SHALL maintain the connection to the RI and attempt to establish an OBEX connection to the Unconnected Device's OBEX server and sends the ROAP Trigger in an OBEX PUT operation. The Connected Device MUST extract the *roapURL* from the ROAP Trigger and store for later use. The Connected Device searches for available OBEX servers through service discovery, see Section 11.5.5. In the case where the Connected Device detects multiple OBEX servers (i.e Unconnected Devices) the Connected Device SHOULD at this time prompt the user to determine which Unconnected Device to connect to.

When receiving a ROAP message in the body of an OBEX response message from the Unconnected Device, the Connected Device SHALL forward the message to the *roapURL* as specified in the ROAP Trigger, re-using the maintained connection. The Connected Device SHALL close the connection to the RI when the OBEX session ends. The Connected Device MAY close the connection to the RI when receiving a response to a PUT request with response code 0xA0 and no Body (or End of Body) header.

Sending a ROAP message can take one or more OBEX packets. The OBEX server on Unconnected Devices MUST be able to receive multiple sequential PUT requests.

ROAP messages originating from the Unconnected Device are received by the Connected Device in response to PUT operations or by use of the OBEX GET operation (when the response is larger than the maximum OBEX packet length). A Connected Device that has sent a PUT request and receives a response with response code 0x90 MUST issue GET requests until the complete ROAP message has been received (response code 0xA0).

Each ROAP message MUST be transferred as a ROAP MIME media type within the body of the OBEX request or response. However in order to transfer the message it may split the message into several PUT requests (or GET responses), followed by a PUT Final request (or a final GET response).

11.5.5 Service Discovery

11.5.5.1 IrDA

To enable an OBEX connection over IrDA, the OBEX protocol stack needs to provide IAS setting information to the IAS protocol stack. The Unconnected Device SHOULD use the following IAS entry settings for ROAP communication via OBEX over IrDA:

Class OBEX:ROAP-client

Attribute Name: IrDA:TinyTP:LsapSel

Attribute Type: Integer

Attribute Description: IrLMP LSAP selector for ROAP over IrOBEX, legal values from 0x01 to 0x6F

11.5.5.2 Bluetooth

Service discovery can enhance the user experience by automating selection procedures. This section contains a definition of the corresponding service records and SDP PDUs, needed to enable a Connected Device to automatically find suitable Unconnected Devices to connect to when using the Bluetooth protocol stack.

To enable ROAP over the Bluetooth protocol stack, the Unconnected Device SHOULD advertise service records, which can be retrieved by a Connected Device using the Bluetooth Service Discovery Protocol (SDP).

In the case of the Unconnected Device, the following information, i.e., service records, SHOULD be put into the SDDB (Service Discovery Database):

Item	Definition	Type/ Size	Value	AttrID	Status	Default Value
Service Class ID List			N/A	0x0001**	MUST	
Service Class #0	ROAP unconnected Device	UUID	1d29f667-3236-374a-bf63-3c7a023bb17d	N/A	MUST	
Protocol Descriptor list			N/A	0x0004**	MUST	
Protocol ID #0	L2CAP	UUID	0x0100**	N/A	MUST	
Protocol ID #1	RFCOMM	UUID	0x0003**	N/A	MUST	
Param #0	CHANNEL	Uint8	Varies	N/A	MUST	
Protocol ID #2	OBEX	UUID	0x0008**	N/A	MUST	
Service name	Displayable Text name	String	Varies	0x0000+b***	MAY	"ROAP client"

Table 12 ROAP Client Service Records

** The value or the attribute ID is specified in the Bluetooth Assigned Numbers specification.

*** 'b' in this table represents a base offset as given by the LanguageBaseAttributeIDList attribute. For the principal language b must be equal to 0x0100 as described in the [Bluetooth SDP] specification.

Table 13 shows the specified SDP PDUs (Protocol Data Units), which are required.

PDU no.	SDP PDU	Ability to Send		Ability to Retrieve	
		ROAP Connected Device	ROAP unconnected Device	ROAP Connected Device	ROAP unconnected Device
1	SdpErrorResponse	N/A	MUST	MUST	N/A
2	SdpServiceSearchAttribute-Request	MUST	N/A	N/A	MUST
3	SdpServiceSearchAttribute-Response	N/A	MUST	MUST	N/A

Table 13 SDP PDUs

11.5.6 Bluetooth Considerations

11.5.6.1 Use of Bluetooth security

Bluetooth authentication and link encryption may be used when running ROAP over OBEX (over Bluetooth). Before these services are available the Connected Device and the Unconnected Device must have gone through an initialization procedure, i.e. be paired. The initialization procedure could be a part of the first ROAP session or it could be done in advance if the Connected Device and the Unconnected Device are already paired for other services.

It is expected that Devices in the user's environment are paired once to enable several services.

12.Super Distribution

OMA DRM v2 provides two mechanisms for superdistribution:

- Protected content, in the form of a DCF, can be distributed from one Device to another over any physical removable media, wired or wireless network connection without any restrictions.
- If the ContentURL header is present within a given DCF (as defined in OMA DCF Specification [DCF-v2]), this URL MAY be distributed from one Device to another without any restrictions.

12.1 Preview

If a super-distributed DCF has headers indicating that it supports previews, then the receiving Device MAY use the information provided to generate a preview for the user. This preview may be provided in the form of “instant preview”, where the DCF itself has a preview element that can be used without a Rights Object. In addition, the DCF headers may also indicate a preview method where the Device would need to acquire a preview Rights Object before providing any preview capabilities. See the [DRMDCF-v2] for further details on the appropriate DCF headers.

12.2 Transaction Tracking

A DCF may contain a TransactionID as an information element inside a OMADRMTransactionTracking box according to [DRMCF-v2]. The TransactionID may be used to track the content flow from one user to another via super distribution from an RI perspective.

The Device MUST ensure the consent of the user for related operations performed by the Device to ensure the privacy issues of the user. This can be done by general settings in the Device, by individual settings per Rights Issuer or on a case by case basis and is implementation specific.

To enable transaction tracking a DCF or PDCF must contain an OMADRMTransactionTracking box when it is received by the Device.

If a DRM Agent receives an RO Response containing an RO and a TransactionID it MUST ask the user for consent to replace the TransactionID in the DCF/PDCF. This can be done in general or on a case by case basis. If consent is given, the DRM Agent MUST replace the TransactionID contained in the OMADRMTransactionTracking box of the corresponding DCF or PDCF with the TransactionID received else the DRM Agent doesn't change the DCF/PDCF. Note: a Device neither needs to generate an OMADRMTransactionTracking box nor needs to change the size of the DCF/PDCF.

If a Device submits an RO Request based on a DCF or PDCF that contains an OMADRMTransactionTracking box it MUST insert the TransactionID of the corresponding DCF or PDCF into the RO Request as the *TransactionID.*

Transaction tracking might not work if

- the first user decides to super distribute only the ContentURL instead of the DCF or PDCF or
- the Rights Object is received prior to the DCF or PDCF.

Informative Note: The transaction tracking feature may be used by a Rights Issuer to implement a reward mechanism by which a first user may obtain a benefit from super distributing Protected Content to another user which purchases an RO to obtain access to the super distributed content. Transaction tracking comprises the following steps:

a) The RI provides a TransactionID in an RO Response message to the Device of the first user.

b) *The Device of the first user replaces the TransactionID in the DCF or PDCF already on the Device with the received TransactionID.*

c) *The first user super distributes the DCF or PDCF to a second user.*

d) *The second user sends an RO Request message including the TransactionID of the received DCF or PDCF to the RI.*

e) *The RI maps the received TransactionID to the same TransactionID related to the initial transaction with the first user.*

The kind of benefit the first and/or second user may get from the RI is out of scope of this specification.

12.3 DCF Integrity

A DCF, once downloaded from a content portal, is deemed to be immutable with a single exception. Devices MAY replace the *TransactionID* contained in an OMADRMTransactionTracking box in a DCF or PDCF but MUST NOT modify rest of the DCF or PDCF before super-distributing the content to other Devices. The integrity check on the DCF/PDCF is always carried out excluding the FreeSpace box, if present. Therefore, the integrity validation will fail if the DCF/PDCF has been modified except for the authorized exchange of the TransactionID. This applies to all DCFs whether it is a Multipart DCF composite object with multiple DRM elements Containers included or a simple DCF object with only one DRM Container element within it.

13.Export

After downloading OMA DRM protected content, the User may wish to render that content on another Device that has a different DRM protection format. Export is an operation in which the DRM content and corresponding Right Object are transferred to a DRM system or content protection scheme other than the OMA DRM system. The Rights Issuer controls whether or not to allow the export.

The Rights Issuer must explicitly grant permission (with the <export> element in [DRMREL-v2]) before the content and Rights Object can be exported. The Rights Issuer also specifies to which DRM system or content protection scheme the DRM content is allowed to be exported. The Rights Issuer MAY permit export to more than one system.

The basic concept of export from OMA DRM to another DRM system or content protection scheme is specified in this document. OMA does not specify the exact rules for transcribing Rights Objects to the other protection mechanisms. It is the responsibility of appropriate bodies governing the use of those protection systems to define the necessary mechanisms for transcribing OMA DRM Rights Objects. Figure 9 below explains the principle.

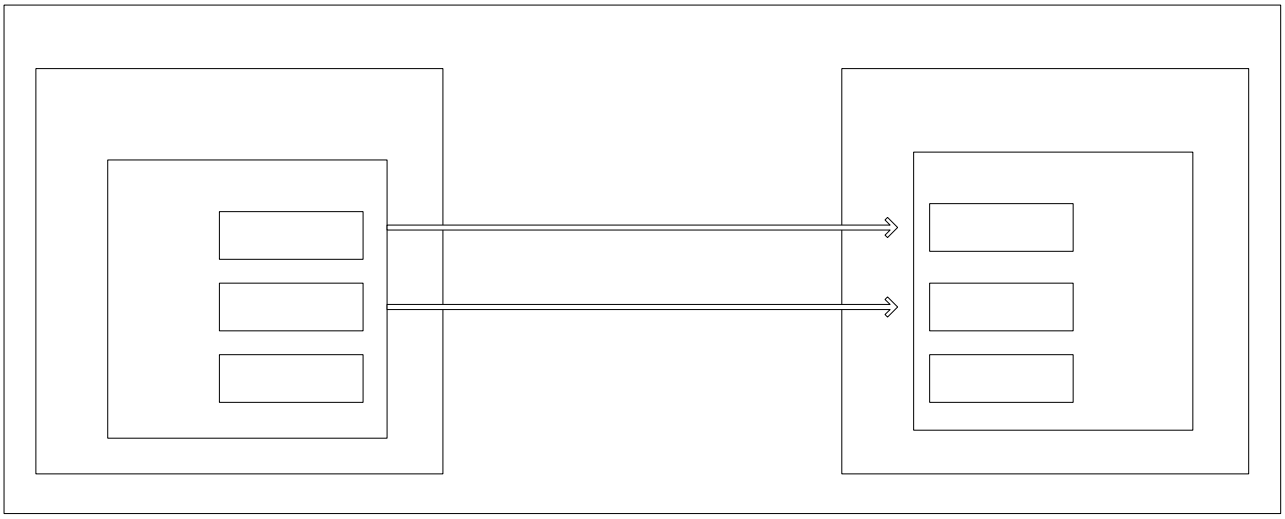

Figure 9: Exporting from OMA DRM

13.1 Export Modes

The Rights Issuer can specify if the DRM content and Rights Object are available on the original Device after the export (“copy”) or are permanently removed following the export (“move”).

In the case of “copy”, the DRM content and Rights Object remain on the original Device and available for rendering following the export. The Rights Issuer MAY specify the number of times the “copy” export is permitted. The original Rights Object is exported without state information if it is a stateful Rights Object and MUST remain unchanged on the original Device after the export.

In the case of “move”, the original Rights Object MUST become permanently unusable on the original Device, after exporting is conducted. The Rights Object MUST be exported with the current state information at the time of the export if it is a stateful Rights Object. That is, if a stateful right has been partially consumed, only the remaining portion is exported. The Content Object MAY remain on the original Device.

In either mode, the <export> permission MUST NOT be transcribed into the other DRM system or content protection scheme. This restriction prevents further export once the content is protected by the other DRM system.

13.2 Compatibility with Other DRM Systems

The targeted DRM system may not support all of the capabilities of OMA DRM. Some potential areas of incompatibility include:

- Content Types
- OMA REL usage permissions and constraints
- Multiple Rights Objects for a single content
- Rights for multiple content objects in a single Rights Object

This section defines some general rules to minimize incompatibilities when exporting to non-OMA DRM systems. The detailed rules for the transcription of OMA Rights Objects to those of another DRM system are specific to the target system and, therefore, are not part this document.

During discovery and download of content for future export, the best possible content and rights should be provided to the Device according to device capability, the capability of the other DRM system, and user preferences. This information MAY be indicated to the Content Issuer using UAProf as specified in section 5.2.

When creating a Rights Object for Export (i.e. <export> permission is included), the Rights Issuer SHOULD construct the Rights Object so that all the permissions and constraints within it are supported by the other DRM system. All permissions and constraints in the original Rights Object MUST be transcribed provided they are supported in the target DRM system.

As described in section 9.2, a single Rights Object can contain rights for multiple content objects either within a multipart DCF or separate DCFs. The <export> permission is applied to the entire Rights Object so that when such a Rights Object is exported, each associated content object MUST also be exported.

A single content object may have more than one corresponding Rights Object. If the user wishes to export this content object, all Rights Objects with permission to export to the targeted DRM system MUST also be exported. If the target DRM system supports multiple rights for a single content object, multiple rights in the original Rights Object MUST be transcribed. If the target DRM system does not support multiple rights for a single content object, the multiple rights MAY be merged into one Rights Object and then transcribed.

13.3 Streaming to Other Devices

Another form of export allows the user to stream DRM content from the original Device to a rendering Device (i.e. headphones) for immediate playback. The content MUST be streamed over a copy protected medium where the transmission protocol between the Devices ensures that the DRM content cannot be copied in an unauthorized manner.

The general rules above in terms of transcribing the content and rights SHOULD be followed when streaming over protected links for rendering purposes.

When <export> permissions are granted and the target system is a link protection scheme, it is understood that a transient copy is made to facilitate rendering on the target Device. The appropriate signalling MUST be used to indicate to the target DRM/protection system, that the streamed content is used only for rendering purposes.

14.Unconnected Device Support

The following section identifies how a Connected Device can act as an intermediary to assist an Unconnected Device to purchase and download content and Rights Objects. This Functionality enables, for example, a portable mobile Device that does not have inherent network connectivity to acquire content and associated rights. This functionality builds on the Domain concept as described in section 7.

An Unconnected Device SHALL be capable of connecting to a Rights Issuer via a Connected Device using an appropriate protocol over a local connectivity technology. E.g. OBEX over IrDA, Bluetooth or USB as specified in section 8.

Unconnected Devices MUST support the 4-pass Registration protocol as specified in section 5.4.2.

Unconnected Device MUST support Domain Join and Domain Leave protocols as specified in section 5.4.4.

Unconnected Devices MAY support DRM Time.

Connected Devices MUST support DRM Time.

A Connected Device MAY also implement Unconnected Device functionality.

Connected Devices SHALL be capable of directly connecting to a Rights Issuer using an appropriate protocol over an appropriate wide area transport/network layer interface (e,g, HTTP over TCP-IP).

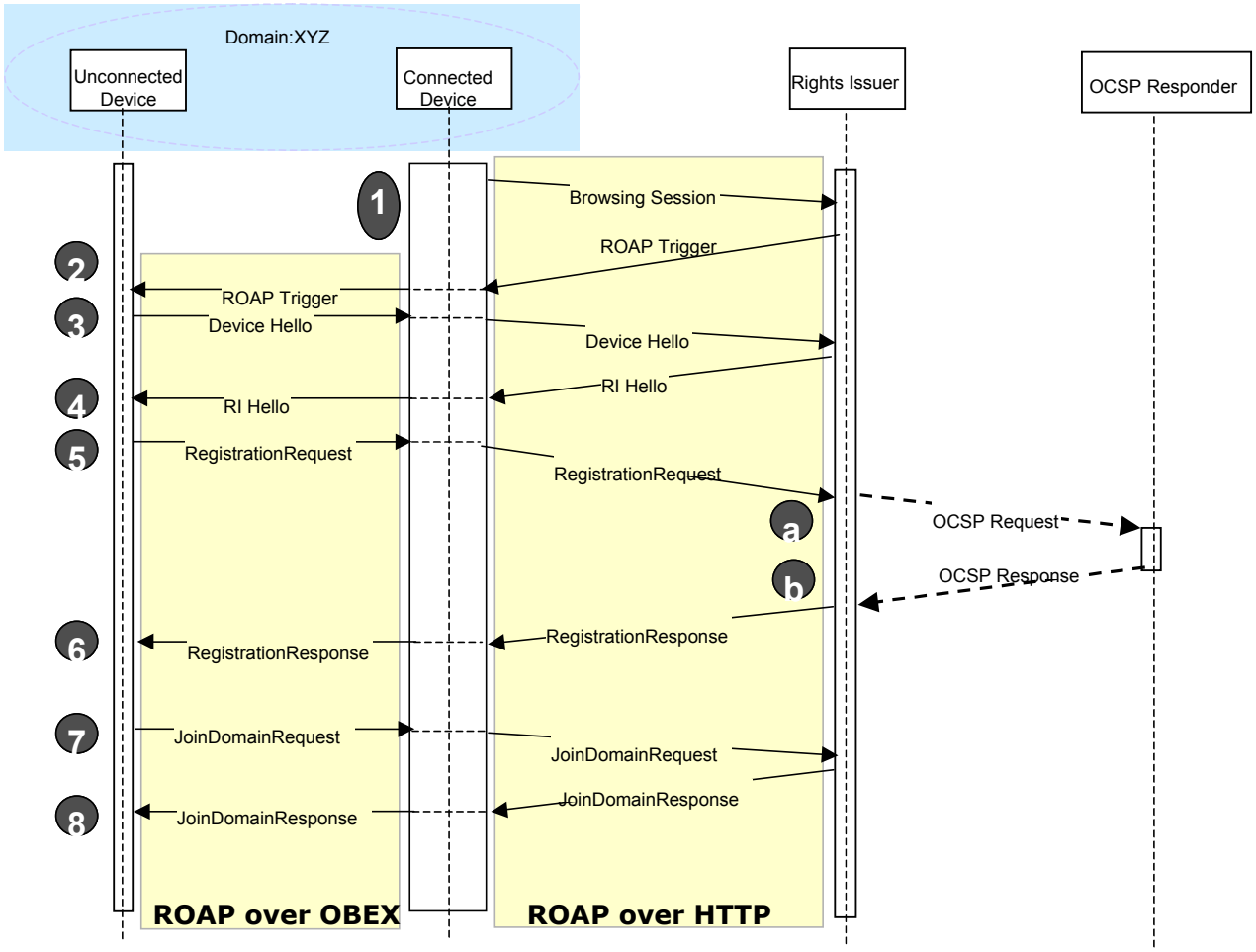

Figure 10: Unconnected Device Registration and Domain Establishment

The above diagram shows how an Unconnected Device establishes an RI Context (Registration) and is added to the Domain: XYZ. In the above diagram it is assumed that the Connected Device has already performed the required steps in order to join the Domain: XYZ.

1. The user initiates a browsing session from the Connected Device to an RI. The user indicates to the RI that they would like to add an Unconnected Device to the Domain: XYZ (how this is achieved is outside of the scope of this specification).
2. The RI returns a ROAP Trigger of type *joinDomain* to the Connected Device and includes the *proxy* attribute with the value set to "True".
3. Upon receipt of the ROAP Trigger, the Connected Device determines that the ROAP Trigger is intended for an Unconnected Device (through examination of the *proxy* attribute). At this point the Connected Device SHALL maintain the connection to the RI and attempt to establish an OBEX connection to the Unconnected Device's OBEX server. Once the OBEX connection is established the Connected Device MUST send the ROAP Trigger in an OBEX PUT operation. The Connected Device MUST extract the *roapURL* from the ROAP Trigger and store for later use.

   If it is not clear to the Connected Device which Unconnected Device should receive the ROAP trigger (e.g. because the Connected Device is already in communication with more than one Unconnected Device) then the Connected Device SHOULD display a list of the Unconnected Devices to the user (using user friendly identifiers for the Unconnected Devices) and request the user to select the Unconnected Device that the user wishes to be joined to the Domain). The Connected Device MUST attempt to establish an OBEX connection to the OBEX server of the user-selected Unconnected Device.
4. Upon reception of the *joinDomain* ROAP Trigger the Unconnected Device MUST determine whether it has an RI context with the RI or not. If the Unconnected Device does not have an RI context with the RI indicated in the ROAP trigger the Unconnected Device MUST send a ROAP-DeviceHello message in the OBEX response to the Connected Device. The Connected Device SHALL forward the message to the *roapURL* as specified in the ROAP Trigger, re-using the maintained connection. If the Unconnected Device has an RI Context then steps 4 – 6 do not apply.
5. The RI MUST respond with a ROAP-RIHello message which the Connected Device MUST send to the Unconnected Devices's OBEX server in an OBEX PUT operation
6. The Unconnected Device MUST respond with a ROAP-RegistrationRequest message in the OBEX response to the Connected Device. The Connected Device SHALL forward the message to the *roapURL* as specified in the ROAP Trigger re-using the maintained connection.
7. The RI MUST respond with a ROAP-RegistrationRespond message which the Connected Device will send to the Unconnected Devices's OBEX server in an OBEX PUT operation
8. Upon successfully establishing an RI context, the Unconnected Device MUST send a ROAP-JoinDomainRequest message in the OBEX response to the Connected Device. The Connected Device SHALL forward the message to the *roapURL* as specified in the ROAP Trigger, re-using the maintained connection.
9. The RI MUST respond with a ROAP-JoinDomainResponse message which the Connected Device MUST send to the Unconnected Devices's OBEX server in an OBEX PUT operation.
10. The Unconnected Device MAY respond with an OBEX Disconnect or MAY respond with an OBEX message containing the code 0xA0 and no Body (or End of Body) header. Upon reception of the OBEX Disconnect operation, the Connected Device SHALL close the connection to the RI. The Connected Device MAY close the connection to the RI when receiving a response to a PUT request with response code 0xA0 and no Body (or End of Body) header.

In the above diagram and text it is assumed that no ROAP specific errors occur during the ROAP session. If ROAP specific errors occur during the ROAP session then the Unconnected Device SHOULD use the value of status parameter as defined in section 5.3.5 and to act accordingly.

Once an Unconnected Device has successfully registered and joined the same Domain as the Connected Device then the Connected Device can acquire content and rights on behalf of the Unconnected Device. RO acquisition is shown below.

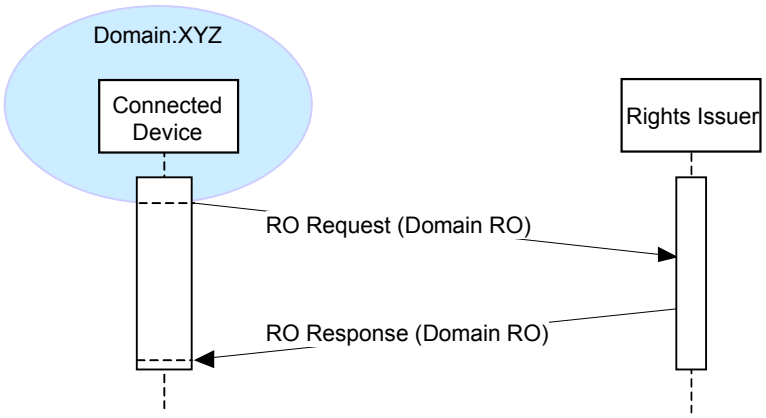

Figure 11: Content Acquistion

Once the Connected Device has received the Domain RO, it SHOULD insert the Domain RO in the associated DCF as specified in section 8.6.3. This enables the DCF and embedded RO to be transferred to the Unconnected Device using a simple file transfer operation over OBEX as shown in the following diagram.

Note: As an Unconnected Device may not support the acquisition of rights, a Connected Device should present a suitable warning to the user, if the user attempts to transfer a DCF without an embedded Domain ROs to an Unconnected Device.

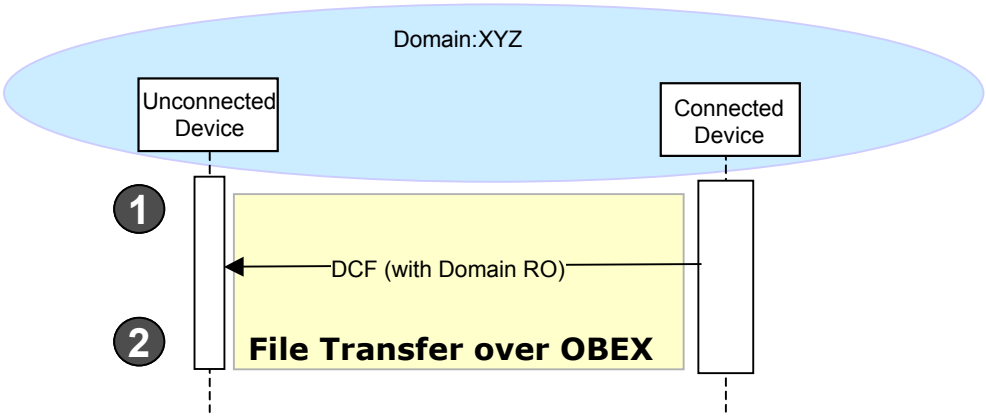

Figure 12: Content Acquistion

In the case where a user wishes to remove an Unconnected Device from a Domain, this is achieved as follows:

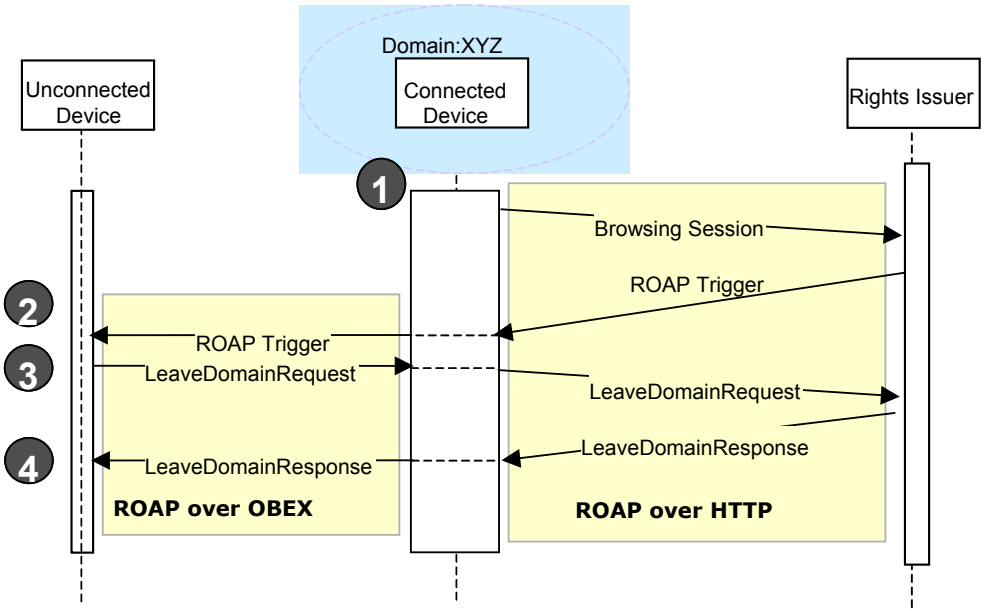

Figure 13: Unconnected Device leaving a Domain

1. The user initiates a browsing session from the Connected Device to an RI. The user indicates to the RI that they would like to remove an Unconnected Device from the Domain: XYZ (how this is achieved is outside of the scope of this specification). The RI returns a ROAP Trigger of type *leaveDomain* to the Connected Device and includes the *proxy* attribute with the value set to "True".
2. Upon receipt of the ROAP Trigger the Connected Device determines that the ROAP Trigger is intended for an Unconnected Device (through examination of the *proxy* attribute). At this point the Connected Device SHALL maintain the connection to the RI and attempt to establish an OBEX connection to the Unconnected Device's OBEX server and sends the ROAP Trigger in an OBEX PUT operation. The Connected Device MUST extract the *roapURL* from the ROAP Trigger and store for later use.
3. Upon reception of the *leaveDomain* ROAP Trigger and after performing the steps specified in section 8.4 the Unconnected Device MUST send a ROAP-LeaveDomainRequest message in the OBEX response to the Connected Device. The Connected Device SHALL forward the message to the *roapURL* as specified in the ROAP Trigger re-using the maintained connection.
4. The RI will respond with a ROAP-LeaveDomainResponse message, which the Connected Device will send to the Unconnected Devices's OBEX server in an OBEX PUT operation.

   The Unconnected Device MAY respond with an OBEX Disconnect or MAY responsed with an OBEX message containing the code 0xA0 and no Body (or End of Body) header. Upon receptioin of the OBEX Disconnect operation the Connected Device SHALL close the connection to the RI. The Connected Device MAY close the connection to the RI when receiving a response to a PUT request with response code 0xA0 and no Body (or End of Body) header.

15.Binding Rights to User Identities

15.1 IMSI uid

If the Device supports a SIM/USIM/R-UIM and the <uid> element of a child <context> element of an <individual> element within a Rights Object specifies an IMSI, the DRM Agent MUST observe the following behaviour.

When the associated content is selected for rendering the DRM Agent MUST check that the IMSI on the currently installed SIM/USIM/R-UIM (as stored within EFIMSI elementary file, which is defined in [3GPP TS 51.011],[3GPP TS 31.102] and 3GPP2 C.S0023-A) matches the IMSI specified within the <uid> element or in the case where the the RO is bound to multiple IMSIs one of the IMSI's specified within the <uid> element.

If the IMSI of the currently installed SIM/USIM/R-UIM matches the value (or in the case when the RO is bound to multiple IMSIs one of the values) specified in the <uid> element, as specified in [DRMRELv2], then the <permission> SHOULD be exercised if all other constraints are fulfilled.

If the IMSI of the currently installed SIM/USIM/R-UIM does not match the value (or in the case where the the RO is bound to multiple IMSI's any of the values) specified in the <uid> element then the <permission> MUST NOT be exercised.

15.2 WIM uid

If the Device or SIM, UICC in the Device supports a WIM and if the Device supports binding to WIM and, if the <uid> element of a child <context> element of an <individual> element within a Rights Object specifies a PKC_ID, the DRM Agent MUST observe the following behaviour.

1. The Device attempts to retrieve the user certificate from the WIM [WIM], identified by PKC_ID i.e. the value of PKC_ID matches with the value of CommonCertificateAttributes.certHash field from the user certificate CDF entry,
2. Compute a hash (e.g. thumbprint) over the user certificate. The hash is calculated over the DER encoding of the complete certificate and SHA1 hashing algorithm MUST be used,
3. Check that this hash (e.g. thumbprint) matches with the value of PKC_ID,

Go to step 4 if the result of the check is successful. If unsuccessful, the permission MUST NOT be exercised.

4. Generate a 20 bytes challenge value,
5. Ensure that the rights to access signature key are granted,
6. Request the WIM to sign the challenge using the private key associated with the identified user certificate,
7. Verify the signature using the user certificate.

If the verification of the signature is successful then the <permission> MUST be exercised.

15.2.1 Support for WIM uid

If the Device supports a WIM and if the Device supports binding to WIM then the DRM Agent SHOULD support User certificate for authentication as defined in Appendix F.

The said user certificate MUST be stored locally in the WIM. The logical record of the WIM CDF that provides information for that certificate thus makes use of the path identifier reference choice and MUST in addition contain the optional field CommonCertificateAttributes.certHash. The use of the private key associated to the said user certificate MUST be protected by the PIN-G i.e., the logical record of the WIM PrKDF that corresponds to that key provides a commonObjectAttributes.authId field that identifies the PIN-G authentication object.

To optimise (i.e. save certificate hashing operation) the next procedures that make use of the said user certificate, it is RECOMMENDED that once the DRM Agent successfully passed the step 3 it stores the trusted couple (user certificate, user certificate hash (e.g. thumbprint)) in its local storage area. Thus, the DRM Agent MAY resume the

sequence, starting from step 4 and making use of the user certificate from its local storage area to perform step 7 i.e., selected by PKC_iD == user certificate hash (e.g. thumbprint).

Interactions between the DRM Agent and the WIM are described in Appendix G.

16.Security Considerations (Informative)

16.1 Background

DRM solutions usually have to follow a number of important security requirements. Three properties any DRM solution must fulfil are as follows:

- Methods enforcing that DRM Content can be used only by authenticated, authorised DRM Agent implementations.
- Rights and constraints on licensed content must be honoured, i.e. application programs rendering DRM Content must behave in exactly the way that guarantees that the RO associated to the content is respected.
- DRM Content does not leave the Device in an unprotected format.

OMA DRM defines the architecture (ARCH), requirements (REQ), content formats (DCF), rights expression language (REL), and the ROAP protocols, which are subject to this specification. They guarantee authentication, authorisation, and the secure download of ROs in order to use the protected media object. The trust model assumes that the DRM Agent's behaviour conforms to the specification, i.e. it embodies a trusted entity in the Device enforcing permissions and constraints associated with DRM Content as well as controlling access to DRM Content.

16.2 Trust Model

The OMA DRM trust model states that the DRM Agent has to be trusted by the Rights Issuer, i.e. the DRM Agent behaves correctly and the implementations of the DRM Agent are secure. Each DRM Agent has a unique key pair and an associated certificate. The certificate identifies the DRM Agent and certifies the binding between the agent and its keys. It is assumed that an appropriate trust management infrastructure (e.g. PKI for OMA DRM), is available and allows the refusal or revocation of devices with an untrusted DRM Agent.

16.3 Security Mechanisms of OMA DRM

16.3.1 Confidentiality

Confidentiality ensures that data is not accessible by an unauthorised party. In OMA DRM, the media object must be accessible only by the intended recipient. The DRM content is protected by the CEK. To access the DRM content, the CEK must be extracted from the RO using the REK. Thus, CEK is protected by the REK. The data is then passed to the DRM Agent using a hybrid cipher scheme based on RSA and AES.

16.3.2 Mutual Unilateral and Implicit Authentication between DRM Agent and RI

Mutual authentication involves both the RI and the Device sending and checking each other's hashed public key info as seen in their respective certificates. The Device uses as Device identity the SHA-1 hash of the DRM Agent certificate's public key information in the authentication process. Mutual authentication is achieved by the ROAP 4-pass registration protocol, the ROAP 2-pass acquisition of the RO, and the 2-pass Domain joining protocol.

ROAP 1-pass achieves mutual implicit authentication because the RI has signed the data, which is then encrypted with the DRM Agent's public key. Hence, in this way the DRM Agent is authenticated, since only it has access to the private key for decrypting the RO.

The ROAP Domain leaving protocol only achieves unilateral authentication.

The usage of nonces guarantees freshness. After the RI has sent the ROAP-RIHello including a fresh nonce, the Device includes another fresh nonce in the ROAP-RegistrationRequest message and creates a signature of the hash of all the data sent and received in the protocol so far. When responding with a ROAP-

RegistrationResponse, the RI also generates a signature of the hash over this message and the one received. This accomplishes the mutual authentication.

16.3.3 Data Integrity

Data integrity means that if data is modified (either intentionally or unintentionally), this modification is detected. In the ROAP protocol the usage of the signature guarantees integrity, i.e., when the recipient verifies the signature, he will detect a change of data.

Note, that mutual authentication between the DRM Agent and the RI implies data integrity since the signature is made over the data sent in the ROAP.

16.3.4 Key Confirmation

A MAC calculated over the RO provides key confirmation.

16.3.5 Public Key Infrastructure (PKI)

OMA DRM assumes a trust model that is based on a Public Key Infrastructure (PKI).

A PKI provides, manages, and revokes keys, and therefore enables mutual authentication as performed by the ROAP protocol. The PKI is needed to complement the DRM system, such that communication over an open, unsecured network can take place with the assurance that it is exactly the two parties exchanging messages.

16.3.6 Prevention of Replay Attacks

A replay attack would allow an attacker to send a message again, such that the user could process DRM content more than once using the same RO. The ROAP protocol prevents replay attacks by introducing fresh nonces with every message and, therefore, guarantees that the same message cannot be processed more than once.

To give the same amount of protection to protocols that do not offer a challenge/response mechanism, i.e. the 1-pass RO Acquisition protocol or the sharing of ROs in a Domain, a local replay cache is kept in the Device, where each entry contains a Globally Unique RO Identity (GUID) for a received, stateful RO, and the RI Time Stamp for the RO. To overcome the problem that sharing of Domain ROs with very old time stamps may be affected by the finiteness of the replay cache, a separate replay cache for ROs with a GUID, but without a timestamp, is included (see Section 9.4).

16.3.7 Secure Time

OMA DRM assumes that the DRM agent time is accurate and not changeable by users.

Since users are not able to change the DRM agent time, the OMA DRM specifications provide mechanisms for the DRM time to be synchronised when necessary, e.g. if time is lost after prolonged power failure.

16.3.8 Domain Content Protection

For Domain content protection a group key is used. The group key H(n) is a generated from a list of hash values H1 = H(H0), H2 = H(H1),and so on. If one member leaves the Domain, the RI will issue H(n-1) to the rest of the group. If a new member joins, he can easily calculate all hashes from the currently available and can therefore use all content that has been supplied for the Domain so far. The member who left the Domain knows only H(n) and as one property of hash values is, that they can easily be calculated but the backward function is nearly impossible, the DRM Agent will not be able to decrypt any new data received.

16.3.9 The Transport Protocols

Security is implemented at the application layer by using confidentiality and integrity protection mechanisms, more specifically a secret shared key for data protection and an asymmetric encryption scheme to protect the secret data while transmitting it to the DRM Agent.

Hence, the transport protocols HTTP, Download OTA, WAP Push, and MMS are not required to apply security mechanisms.

16.4 Threat Model

If the trust model holds, an attacker has

- no control of the entities involved, i.e., no ability to compromise DRM Agent, RI, CI, CA, and OCSP Responder
- no knowledge of the private key information of the DRM Agent,
- but can
- listen to the communication channel over which RI and DRM Agents communicate,
- can read, remove, change, or inject ROAP messages, DCF, and RO, and
- is able to generate data that appears to be sent from a trusted entity.

Further, it is assumed that an attacker has limited computational power. This means that we assume that it is very difficult, if not impossible, to break the cryptographic mechanisms by brute force (in particular plain-text attacks).

16.5 Threat Analysis

The main threat of DRM in general is that the end user himself tries to get the content for free. Since he has all it needs to try to do that in his hands, i.e. the Device, the DRM Agent inside the Device must be protected in particular. Other threats involve unauthorized behaviour, if RI, CI, OCSP Responder, etc are compromised. In the following sections, possibilities of misuse of the proposed OMA DRM solution in general and the ROAP protocol in particular are discussed. The considerations cover two cases:

i. the trust model holds and
ii. the assumptions of the trust model do not hold.

However, case (ii) is discussed to emphasise the importance of protecting the RI/CI and the DRM Agent against both internal and external threats. Attackers will always have access to DRM agents due to the reversed threat model since a compromised Device will render the trust chain invalid.

16.5.1 No Acknowledged Result Indication

ROAP does not provide an acknowledgement of the ROAP-LeaveDomainResponse message. The RI sends this message to the DRM Agent after the association of Device and Domain has been deleted at the RI's registry. However, the Device must ensure that the Domain Context of the corresponding Domain is deleted before even the ROAP-LeaveDomainRequest was sent.

In case (i) and (ii) the following threat seams possible: If an attacker deletes the ROAP-LeaveDomainRequest message but there is no must for an acknowledged result indication, the user leaves the Domain while the RI will still assume that the Device is part of the Domain.

16.5.2 Attack against Confidentiality

The confidentiality of data on the communication channel is guaranteed as long as nobody can break the asymmetric RSA-KEM-KWS encryption scheme used. If the shared secret value is publicly known, REK and CEK could easily be derived. An attacker with very high computational power could try a brute force attack. In this case, it would be preferable that the key information gathered can only be used for one media object or even only for one part of the DCF, e.g., if streaming data is sent.

The shared secret key, when decrypted by the DRM Agent, must not be accessible to anybody (except the DRM Agent) by any means.

From the security point of view, no new attack seems possible by the distribution of the Domain key. It seems to be a correct solution for joining and leaving a Domain (compare with Section 16.3.8).

16.5.3 Attack against Data Integrity

ROAP ensures data integrity by signing messages. However, in the ROAP 2-pass Domain Management protocol the ROAP-LeaveDomainResponse message is not signed. Thus, the DRM Agent cannot verify the integrity of this message. A similar attack as described in Section 16.5.1 is possible though the ROAP-LeaveDomainResponse was delivered.

Even assuming case (i) the following attack might occur:

An attacker *A* pretends to be the RI and receives the ROAP-LeaveDomainRequest. The message is not encrypted but signed by the DRM Agent. Thus *A* reads the content, takes the *nonce*-information and the *DomainIdentifier*, generates a ROAP-LeaveDomainResponse, and sends the answer to the Device. The DRM Agent assumes that leaving the Domain was successful since it got a reply. However, since the RI never got the request it must assume that the Device is still part of the Domain. If the ROAP-LeaveDomainResponse would be signed, this attack could not occur. DRM is just one enabler of multiple that are needed to complete a full DRM solution. If data integrity is given through other enablers such as download, billing, discovery, and so on, the attack becomes impossible.

Later on the DRM Agent is charged for being able to use Domain content though not part of the group anymore.

Thus, deleting the context before sending the request might still create a misunderstanding between the participants in case of an attack. However, the attack seems to be unlikely, especially since it is foreseen to use a trigger for delivering the ROAP-LeaveDomainRequest message, that is signed and must chain back to the RI responsible for this Domain.

16.5.4 Attack against Non-Repudiation

Non-repudiation means that neither the RI (and/or CI) nor the DRM Agent can deny having performed a certain action. All messages can be uniquely traced to the entity, which is responsible for its action. In particular, a proof of origin and a proof of delivery of any data unit can be given. This gives one party the assurance that only the other party can be responsible for certain behaviour. A signature over the data sent is the appropriate security mechanism.

In case (i), the trust model defines that RI, CI, and DRM Agent are reliable parties. However, there is the following security problem of non-repudiation.

The ROAP 4-pass protocol identifies and authorizes a DRM Agent by proving that the credentials, i.e. certificates, submitted are valid. The DRM Agent does the same for the RI during the mutual authentication, which establishes a security association. All data delivered during the session must be from the other party. For the proof of entity and data integrity and as a receipt of correctly having received the data of the RI, the DRM Agent sends the signature as explained in Section 16.3.1.

However, when the actual RO is transmitted using 2-pass or 1-pass, there is no legal assurance by the DRM enabler that the RO has arrived, since there is no receipt message by the user or another mechanism for this purpose. However, DRM is only one enabler for a DRM solution, the Download notification might be used instead.

The billing trigger is a mechanism that will force the billing procedure, however even with a signed acknowledgement the user could stop the acknowledgement process and could claim that he did not receive any RO and therefore not pay for it.

Nevertheless the DRM Agent can use the RO. Though claimed that he did not receive any RO, he has got all the information to unwrap the REK and CEK and therefore is able to use the DCF. However, in reality a user can behave like this two or three times, subsequently the content provider would put the user's identity and/or the identity of the user's Device on a black list and would not give the user the possibility to join again.

In case (ii) another threat is possible. If the REK or any other part in the key chain (CEK, Domain key) is extracted and somebody distributes the content to the market, the ROAP protocol supplies no means to serve justice. It can be anybody who made identical copies of the content. Even if a security mechanism such as watermarking, fingerprint or steganography would be applied, it is still unclear, who is the attacker.

That is because it is legally impossible to prove who the attacker is. It could be the recipient who has tampered with the content but also it could be the party who generated the keys. However, also protocols that do involve

both parties for the key generation have the same problem. A solution to this issue is not trivial, but could involve the same methods providing non-repudiation and fairness in e-commerce.

16.5.5 Replay Attacks

Since it is not stated in the specification whether the replay cache is part of the DRM Agent, an attacker could access this cache, which is applicable to case (i). In case (ii) the threat pointed out in Section 9.4.1 might occur if there is a cache overflow and parts of the data must be removed to give room for new GUIDs and RO.

16.5.6 Denial of Service Attacks

Denial of service attacks are attacks against the availability of a system and include attacks that consume resources (bandwidth, storage) and/or destruction of resources (e.g. software or hardware components, data destruction and physical destruction). Such attacks can result in significant loss of time and money.

An attacker could send multiple RO requests to the RI, whether authentic or not. This would occupy the processing capabilities of the RI while it serves the attacker, verifies the signatures and sends rejections back to the attacker. If this is done constantly by multiple attackers, the RI will be kept busy and might not be able to serve the genuine users.

The remedy would be for the RI to block the IP source address of the attackers.

Another issue seen is that DRM Agent and Device are bound to each other by the inclusion of the Device identity for the authentication procedure. The RI maintains a database with certificate information of the devices, such that the Device does not need to send the certificate again if the RI can associate the DeviceID with any public key information stored in the database.

In case (i) this could be subject to the following attack assuming an entry in the database: Anybody can pretend to be the Device and send a ROAP-DeviceHello and the RI would answer with the ROAP-RIHello and therefore spam the RI and/or the Device. The former, i.e. the attacker spams the RI, is possible but unlikely since not very effective, since the work done by the RI is low; no expensive operations are made until after the client has authenticated. The latter, i.e. the attacker spams the Device indirectly via sending the ROAP-DeviceHello to the RI, would keep the DRM Agent of the Device busy since it must process all ROAP-RIHello messages that have been initiated by an attacker pretending to be the Device.

No further attack is possible in this case, because the subsequently sent ROAP-RegistrationRequest> message must be signed with the private key of the Device. This is assured because of the assumption that the DRM Agent behaves in the correct way.

In case (ii), if somebody gains the private key, the system would be compromised completely. The implementers of OMA DRM must be aware that the complete chain of trust relies on the protection of the private key. Once the private key is compromised, the attacker can get the REK and therefore the CEK, too.

16.5.7 Private Key Protection

It is assumed that all devices that are part of OMA DRM must be DRM compliant devices. To elaborate this in more detail, these devices must have keys and certificates bound to the DRM Agent.

This is an obligation to the manufacturer which should not be underestimated. It is a critical factor in maintaining the security. Assuming case (ii), failure of client implementations and RIs to protect their private keys will seriously compromise the security of OMA DRM solutions. Existence of unauthorized or cloned client devices or providers will break the basic assumptions around the DRM security model prescribed in the OMA DRM specification.

16.5.8 Trust in the DRM Agent

The DRM Agent on the Device contributes in the ROAP protocol and implements the necessary security and trust elements so that the ROs are utilized in a conforming manner. The primary function of the DRM Agent is to enforce the permissions specified in the RO during content usage. The secrets and keys that are part of the system security must be protected and handled such that unauthorized usage is prevented.

Thus, the key material must be protected in a secure way to implement trust in the DRM Agent. If this cannot be guaranteed as assumed in case (ii), the DRM Agent private key could be extracted or duplicated to another Device.

Furthermore, parts of OMA DRM that could be subject to an attack are, for example:

- the protected media objects (DCF) that are stored at the Device
- the corresponding RO
- application programs, that play or display the DCF
- the module that decrypts the RO
- the module that decrypts the DCF
- the program that proves the integrity of the programs in use
- devices that are used for display, play-back, storage, and so on.

In addition, typically a Device is not only used for processing DRM content but has also other application functions/programs that are not protected by the DRM Agent. Even if the DRM Agent can be trusted it is still possible to manipulate the Device.

Thus, not only keys but also the operation of the DRM Agent and the applications or drivers that it interacts with must be protected as to prevent extracting content. For instance, the data are sent to the video cache, from which an attacker could read them. If there is no secure operating system for the DMR agent, it is possible to install programs that read the memory, change usage rights, and so on. The manipulation of the operating system might enable an attacker to read the memory. For instance, it may be possible to dump a handset's memory.

16.5.9 PKI problems

The implementation of an appropriate PKI is out of the scope of the specification. However a PKI is an essential element to the trust model in the OMA DRM specification. Since a DRM system should give access to various devices such as mobile phone, PDA, mp3-player, digital camera, the fulfilment of this requirement will be difficult and needs a great deal of organisational effort. Once this is solved, another concern lays in the re-keying. Certificates are valid for a distinct period of time. It must be organized to renew the certificates or to supply new keys to a Device in time. Very long-lived certificates could be an alternative here.

16.5.10 Secure time

The possibility of time synchronization in case of time loss could open another security hole if not carefully implemented.

ROs that contain permissions with constraint elements <count>, <interval> or <accumulated> require state information to be kept in the DRM Agent in order to determine whether the permissions are not used up yet. Therefore, the DRM Agent must keep the state information at a distinct memory for processing stateful rights.

Under the assumption of case (i), this specification suggests the usage of the <GUID> and time stamps to prevent replay attacks in the 1-pass and the Domain protocol. A local cache at the Device is used for storing the <GUID>. Because no RI authentication is foreseen, as done in the 2-pass, these measures must be applied to control replays.

However, a compromised operating system could still find a way around. For instance, since the table storing those values is updated in intervals, a system crash by purpose would recover the old system state of the machine though the content was already processed and the user can process the data once again.

In case (ii), if this information is not controlled by the DRM Agent, it might be easily modified or deleted.

Thus, the DRM Agent must rely on a secure time source. If the system time can be compromised, for example the interval of playing a movie could be extended indefinitely.

Note that it might be difficult to guarantee the availability of secure time. However, the probability of such an attack is not very high, since time can be synchronised with the OCSP responder with which the RI communicates when the Device connects.

Note that it is essential that devices must have correct and synchronized secure time to be able to accurately verify a Rights Issuer's revocation status. If a Device's clock drifts such that the Device's current notion of DRM Time goes back to a point in time where a Rights Issuer that has been revoked was still valid, then this Rights Issuer would be able to illegally continue issuing ROs to such a Device by re-using an old OCSP response that it cached from when it was still valid even though the RI has been revoked since.

Furthermore the availability and correct functioning of OCSP responder and secure time server must be guaranteed to avoid denial of service attacks to the DRM system. Without valid OCSP responses available to a RI, DRM Agents will not be able to accept ROs even from a legitimate, unrevoked RI.

16.5.11 Generating Random Numbers

Random numbers are used in various parts of the ROAP. All nonces generated by either DRM Agent or RI are randomly generated. Furthermore, for the hybrid cipher scheme to protect REK and CEK a statistically uniform random integer in the interval of 0 till m-1, where m is the modulus of the RSA public key, must be created.

DRM Agent and RI should have a good source of randomness to generate the random numbers required in the ROAP protocol.

Note that there are many random generators available that are not cryptographically strong.

16.5.12 Manipulation of the Counter in Stateful Rights

Counters must be protected from unauthorized modification.

16.5.13 Man in the Middle Attack

Man in the middle attack and session hijacking are avoided by the ROAP protocol, as all data are integrity protected and the freshness of data is guaranteed, with a small exception of the unsigned ROAP-LeaveDomainResponse.

16.6 Privacy

Privacy is the right of an individual to control or influence the amount of information about itself collected by others. The data that should be protected can be divided into personal data and interest data. A content issuer evaluating such data, for instance, if one person or Device downloads content, can adapt its offers accordingly to all kinds of demands. On one side this will achieve user convenience. On the other side it limits the right of self-determination of the individual. Furthermore, keeping log files that store information, such as who has done what at which time, reveals user behaviour and might not be wished by a single individual.

The ROAP protocol has no measures to anonymize the connection between DRM Agent, downloaded DRM content and associated RO, since the RI and CI are either administered by one organization or might exchange information freely. Also, the messages that are sent do not protect the identities of the communicating parties.

Also transaction id mechanisms to track super distribution behavior, e.g. for reward purposes, might perceived as privacy intruding. For instance, a CI inserting values in the Transaction Tracking box of a DCF with the purpose of, e.g., rewarding customers for super distributing content, potentially learns a great deal of information about users forwarding behavior.

OMA DRM providers might need to consider that privacy will be a demand that needs to be satisfied by implementing anonymity or pseudonym methods (such as identity protection schemes) in future.

Appendix A. ROAP Schema

```
<?xml version="1.0" encoding="UTF-8"?>

<schema
  targetNamespace="urn:oma:bac:dldrm:roap-1.0"
  xmlns="http://www.w3.org/2001/XMLSchema"
  xmlns:roap="urn:oma:bac:dldrm:roap-1.0"
  xmlns:o-ex="http://odrl.net/1.1/ODRL-EX"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
  elementFormDefault="unqualified"
  attributeFormDefault="unqualified">

<!-- Should probably import the OMA profile of ODRL instead -->
<import namespace="http://odrl.net/1.1/ODRL-EX"
      schemaLocation="../odrl/odrl-ex.xsd"/>

<import namespace="http://www.w3.org/2000/09/xmldsig#"
      schemaLocation="http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/xmldsig-core-
schema.xsd"/>

<import namespace="http://www.w3.org/2001/04/xmlenc#"
      schemaLocation="http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/xenc-schema.xsd"/>

<!-- Basic Types -->
<complexType name="Request" abstract="true"/>

<complexType name="Response" abstract="true">
  <attribute name="status" type="roap:Status" use="required"/>
  <attribute name=”riURL” type=”anyURI”/>
</complexType>

<simpleType name="Version">
  <restriction base="string">
    <pattern value="\d{1,2}\.\d{1,3}"/>
  </restriction>
</simpleType>

<simpleType name="Status">
  <restriction base="string">
    <enumeration value="Success"/>
    <enumeration value="UnknownError"/>
    <enumeration value="Abort"/>
    <enumeration value="NotSupported"/>
    <enumeration value="AccessDenied"/>
    <enumeration value="NotFound"/>
    <enumeration value="MalformedRequest"/>
    <enumeration value="UnknownRequest"/>
    <enumeration value="UnknownCriticalExtension"/>
    <enumeration value="UnsupportedVersion"/>
    <enumeration value="UnsupportedAlgorithm"/>
    <enumeration value="NoCertificateChain"/>
    <enumeration value=”InvalidCertificateChain”/>
    <enumeration value=”TrustedRootCertificateNotPresent”/>
    <enumeration value="SignatureError"/>
    <enumeration value="DeviceTimeError"/>
```

```
    <enumeration value="NotRegistered"/>
    <enumeration value="InvalidDCFHash"/>
    <enumeration value="InvalidDomain"/>
    <enumeration value="DomainFull"/>
  </restriction>
</simpleType>

<complexType name="Extensions">
  <sequence maxOccurs="unbounded">
    <element name="extension" type="roap:Extension"/>
  </sequence>
</complexType>

<complexType name="Extension" abstract="true">
  <attribute name="critical" type="boolean"/>
</complexType>

<!-- ROAP extensions -->

<!-- No need for OCSPResponse to be sent -->
<!-- Mainly for use in the 2-pass RO Request protocol -->
<complexType name="NoOCSPResponse">
  <complexContent>
    <extension base="roap:Extension"/>
  </complexContent>
</complexType>

<!-- No need for receiving party's certificate chain to be sent -->
<!-- Mainly for use in the 2-pass RO Request protocol -->
<complexType name="PeerKeyIdentifier">
  <complexContent>
    <extension base="roap:Extension">
      <sequence minOccurs="0">
        <element name="identifier" type="roap:KeyIdentifier"/>
      </sequence>
    </extension>
  </complexContent>
</complexType>

<!-- No need for inclusion of OCSP responder certificates -->
<!-- Mainly for use in the 2-pass RO Request protocol -->
<complexType name="OCSPResponderKeyIdentifier">
  <complexContent>
    <extension base="roap:Extension">
      <sequence>
        <element name="identifier" type="roap:KeyIdentifier"/>
      </sequence>
    </extension>
  </complexContent>
</complexType>

<!-- Device Details -->
<!-- Used in ROAP-RIHello and ROAP-RegistrationRequest messages -->
<complexType name="DeviceDetails">
  <complexContent>
    <extension base="roap:Extension">
      <sequence minOccurs="0">
```

```
      <element name="manufacturer" type="string"/>
      <element name="model" type="string"/>
      <element name="version" type="string"/>
     </sequence>
    </extension>
  </complexContent>
</complexType>

<!-- Loyalty program information -->
<!-- Mainly for use in two-pass RO Request protocol-->
<complexType name="TransactionIdentifier">
  <complexContent>
    <extension base="roap:Extension">
      <sequence>
        <element name="id">
          <simpleType>
            <restriction base="string">
              <length value="16"/>
            </restriction>
          </simpleType>
        </element>
      </sequence>
    </extension>
  </complexContent>
</complexType>

<!-- Certificate chain caching capabilities extension -->
<!-- (Device signals support of the extension, RI signals if it will -->
<!-- store the device's certificates) -->
<complexType name="CertificateCaching">
  <complexContent>
    <extension base="roap:Extension"/>
  </complexContent>
</complexType>

<!-- Support for hash chains in Domains -->
<complexType name="HashChainSupport">
  <complexContent>
    <extension base="roap:Extension"/>
  </complexContent>
</complexType>

<!-- Device does not consider itself a member of the domain it is -->
<!-- leaving -->
<complexType name="NotDomainMember">
  <complexContent>
    <extension base="roap:Extension"/>
  </complexContent>
</complexType>

<!-- Basic types to identify entities -->

<complexType name="Identifier">
  <choice>
    <element name="keyIdentifier" type="roap:KeyIdentifier"/>
    <any namespace="##other" processContents="strict"/>
  </choice>
```

```
</complexType>

<complexType name="KeyIdentifiers">
  <sequence minOccurs="0" maxOccurs="unbounded">
    <element name="keyIdentifier" type="roap:KeyIdentifier"/>
  </sequence>
</complexType>

<complexType name="KeyIdentifier" abstract="true"/>

<!-- Hash of complete DER-encoded subjectPublicKeyInfo from -->
<!-- key holder's certificate -->
<complexType name="X509SPKIHash">
  <complexContent>
    <extension base="roap:KeyIdentifier">
      <sequence>
        <element name="hash" type="base64Binary"/>
      </sequence>
      <attribute name="algorithm" type="anyURI"
              default="http://www.w3.org/2000/09/xmldsig#sha1"/>
    </extension>
  </complexContent>
</complexType>

<!-- The corresponding ds:KeyInfo type -->
<element name="X509SPKIHash" type="roap:X509SPKIHash"/>

<!-- Domain Identifier -->
<!-- Last two characters (decimal digits) shall be interpreted as -->
<!-- domain generation -->
<simpleType name="DomainIdentifier">
  <restriction base="string">
    <pattern value=".{1,18}\d{2}"/>
  </restriction>
</simpleType>

<!-- Rights Object Definitions -->

<complexType name="ROPayload">
  <sequence>
    <element name="riID" type="roap:Identifier"/>
    <element name="rights" type="o-ex:rightsType"/>
    <element name="signature" type="ds:SignatureType" minOccurs="0"/>
    <element name="timeStamp" type="dateTime" minOccurs="0"/>
    <element name="encKey" type="xenc:EncryptedKeyType"/>
  </sequence>
  <attribute name="version" type="roap:Version" use="required"/>
  <attribute name="id" type="ID" use="required"/>
  <attribute name="stateful" type="boolean"/>
  <attribute name="domainRO" type="boolean"/>
  <attribute name="riURL" type="anyURI"/>
</complexType>

<!-- May be sent standalone (domain ROs) -->
<element name="protectedRO" type="roap:ProtectedRO"/>

<complexType name="ProtectedRO">
```

```
  <sequence>
    <element name="ro" type="roap:ROPayload"/>
    <element name="mac" type="ds:SignatureType"/>
  </sequence>
</complexType>

<!-- Registration protocol -->

<!-- ROAP-DeviceHello -->
<element name="deviceHello" type="roap:DeviceHello"/>

<complexType name="DeviceHello">
  <annotation>
    <documentation xml:lang="en">
      Message sent from Device to RI to establish a security
      association.
    </documentation>
  </annotation>
  <complexContent>
    <extension base="roap:Request">
      <sequence>
        <element name="version" type="roap:Version"/>
        <element name="deviceID" type="roap:Identifier"
                maxOccurs="unbounded"/>
        <element name="supportedAlgorithm" type="anyURI"
                minOccurs="0" maxOccurs="unbounded"/>
        <element name="extensions" type="roap:Extensions"
                minOccurs="0"/>
      </sequence>
    </extension>
  </complexContent>
</complexType>

<!-- ROAP-RIHello -->
<element name="riHello" type="roap:RIHello"/>

<complexType name="RIHello">
  <annotation>
    <documentation xml:lang="en">
      Message sent from RI to Device in response to a DeviceHello.
    </documentation>
  </annotation>
  <complexContent>
    <extension base="roap:Response">
      <sequence minOccurs="0">
        <element name="selectedVersion" type="roap:Version"/>
        <element name="riID" type="roap:Identifier"/>
        <element name="selectedAlgorithm" type="anyURI" minOccurs="0"
                maxOccurs="unbounded"/>
        <element name="riNonce" type="roap:Nonce"/>
        <element name="trustedAuthorities" type="roap:KeyIdentifiers"
                minOccurs="0"/>
        <element name="serverInfo" type="base64Binary" minOccurs="0"/>
        <element name="extensions" type="roap:Extensions" minOccurs="0"/>
      </sequence>
      <attribute name="sessionId" type="hexBinary" use="required"/>
    </extension>
```

```
  </complexContent>
</complexType>

<simpleType name="Nonce">
  <restriction base="base64Binary">
    <minLength value="14"/>
  </restriction>
</simpleType>

<!-- ROAP-RegistrationRequest -->
<element name="registrationRequest" type="roap:RegistrationRequest"/>

<complexType name="RegistrationRequest">
  <annotation>
    <documentation xml:lang="en">
      Message sent from Device to RI to request registration.
    </documentation>
  </annotation>
  <complexContent>
    <extension base="roap:Request">
      <sequence>
        <element name="nonce" type="roap:Nonce"/>
        <element name="time" type="roap:dateTimeOrUndefined"/>
        <element name="certificateChain" type="roap:CertificateChain"
                 minOccurs="0"/>
        <element name="trustedAuthorities" type="roap:KeyIdentifiers"
                 minOccurs="0"/>
        <element name="serverInfo" type="base64Binary" minOccurs="0"/>
        <element name="extensions" type="roap:Extensions" minOccurs="0"/>
        <element name="signature" type="base64Binary"/>
      </sequence>
      <attribute name="sessionId" type="hexBinary" use="required"/>
    </extension>
  </complexContent>
</complexType>

<simpleType name="dateTimeOrUndefined">
  <union memberTypes="dateTime roap:UndefinedString"/>
</simpleType>

<simpleType name="UndefinedString">
  <restriction base="string">
  <enumeration value="Undefined"/>
  </restriction>
</simpleType>

<complexType name="CertificateChain">
  <sequence maxOccurs="unbounded">
    <element name="certificate" type="base64Binary"/>
  </sequence>
</complexType>

<!-- ROAP-RegistrationResponse -->
<element name="registrationResponse" type="roap:RegistrationResponse"/>

<complexType name="RegistrationResponse">
  <annotation>
```

```
    <documentation xml:lang="en">
      Message sent from RI to Device in response to a
      registrationRequest message.
    </documentation>
  </annotation>
  <complexContent>
    <extension base="roap:Response">
      <sequence minOccurs="0">
        <element name="certificateChain" type="roap:CertificateChain"
                 minOccurs="0"/>
        <element name="ocspResponse" type="base64Binary" minOccurs="0"
                 maxOccurs="unbounded"/>
        <element name="extensions" type="roap:Extensions" minOccurs="0"/>
        <element name="signature" type="base64Binary"/>
      </sequence>
      <attribute name="sessionId" type="hexBinary" use="required"/>
    </extension>
  </complexContent>
</complexType>

<!-- RO acquisition protocol -->

<!-- ROAP-RORequest -->
<element name="roRequest" type="roap:RORequest"/>

<complexType name="RORequest">
  <annotation>
    <documentation xml:lang="en">
      Message sent from Device to RI to request an RO.
    </documentation>
  </annotation>
  <complexContent>
    <extension base="roap:Request">
      <sequence>
        <element name="deviceID" type="roap:Identifier"/>
        <element name="domainID" type="roap:DomainIdentifier"
                 minOccurs="0"/>
        <element name="riID" type="roap:Identifier"/>
        <element name="nonce" type="roap:Nonce"/>
        <element name="time" type="dateTime"/>
        <element name="roInfo">
          <complexType>
            <sequence maxOccurs="unbounded">
              <element name ="roID" type="ID"/>
              <element name="dcfHash" minOccurs="0">
                <complexType>
                  <sequence>
                    <element name="hash" type="base64Binary"/>
                  </sequence>
                  <attribute name="algorithm" type="anyURI"
                   default="http://www.w3.org/2000/09/xmldsig#sha1"/>
                </complexType>
              </element>
            </sequence>
          </complexType>
        </element>
        <element name="certificateChain" type="roap:CertificateChain"
```

```
            minOccurs="0"/>
      <element name="extensions" type="roap:Extensions" minOccurs="0"/>
      <element name="signature" type="base64Binary"/>
    </sequence>
   </extension>
  </complexContent>
</complexType>

<!-- ROAP-ROResponse -->
<element name="roResponse" type="roap:ROResponse"/>

<complexType name="ROResponse">
  <annotation>
   <documentation xml:lang="en">
    Message sent from RI to Device in response to an RORequest.
   </documentation>
  </annotation>
  <complexContent>
   <extension base="roap:Response">
    <sequence minOccurs="0">
     <element name="deviceID" type="roap:Identifier"/>
     <element name="riID" type="roap:Identifier"/>
     <element name="nonce" type="roap:Nonce" minOccurs="0"/>
     <element name="protectedRO" type="roap:ProtectedRO"
            maxOccurs="unbounded" />
     <element name="certificateChain" type="roap:CertificateChain"
            minOccurs="0"/>
     <element name="ocspResponse" type="base64Binary" minOccurs="0"
        maxOccurs="unbounded"/>
     <element name="extensions" type="roap:Extensions"
            minOccurs="0"/>
     <element name="signature" type="base64Binary"/>
    </sequence>
   </extension>
  </complexContent>
</complexType>

<!-- Domain registration protocol -->

<!-- ROAP-JoinDomainRequest -->
<element name="joinDomainRequest" type="roap:DomainRequest"/>

<complexType name="DomainRequest">
  <annotation>
   <documentation xml:lang="en">
    General PDU for sending domain-related requests from a Device to
    an RI.
   </documentation>
  </annotation>
  <complexContent>
   <extension base="roap:Request">
    <sequence>
     <element name="deviceID" type="roap:Identifier"/>
     <element name="riID" type="roap:Identifier"/>
     <element name="nonce" type="roap:Nonce"/>
     <element name="time" type="dateTime"/>
     <element name="domainID" type="roap:DomainIdentifier"/>
```

```
      <element name="certificateChain" type="roap:CertificateChain"
            minOccurs="0"/>
      <element name="extensions" type="roap:Extensions"
            minOccurs="0"/>
      <element name="signature" type="base64Binary"/>
     </sequence>
     <attribute name="notMember" type="boolean"/>
   </extension>
  </complexContent>
</complexType>

<!-- ROAP-JoinDomainResponse -->
<element name="joinDomainResponse" type="roap:JoinDomainResponse"/>

<complexType name="JoinDomainResponse">
  <annotation>
    <documentation xml:lang="en">
      Message sent from RI to Device in response to a
      JoinDomainRequest.
    </documentation>
  </annotation>
  <complexContent>
    <extension base="roap:Response">
      <sequence minOccurs="0">
        <element name="deviceID" type="roap:Identifier"/>
        <element name="riID" type="roap:Identifier"/>
        <element name="nonce" type="roap:Nonce" minOccurs="0"/>
        <element name="domainInfo" type="roap:DomainInfo"/>
        <element name="certificateChain" type="roap:CertificateChain"
              minOccurs="0"/>
        <element name="ocspResponse" type="base64Binary" minOccurs="0"
              maxOccurs="unbounded"/>
        <element name="extensions" type="roap:Extensions"
              minOccurs="0"/>
        <element name="signature" type="base64Binary"/>
      </sequence>
    </extension>
  </complexContent>
</complexType>

<complexType name="DomainInfo">
  <sequence>
    <element name="notAfter" type="roap:dateTimeOrInfinite"/>
    <element name="domainKey" type="roap:ProtectedDomainKey"
          maxOccurs="unbounded"/>
  </sequence>
</complexType>

<simpleType name="dateTimeOrInfinite">
  <union memberTypes="dateTime roap:InfiniteString"/>
</simpleType>

<simpleType name="InfiniteString">
  <restriction base="string">
  <enumeration value="Infinite"/>
  </restriction>
</simpleType>
```

```
<complexType name="ProtectedDomainKey">
  <sequence maxOccurs="unbounded">
    <element name="encKey" type="xenc:EncryptedKeyType"/>
    <element name="riID" type="roap:Identifier"/>
    <element name="mac" type="base64Binary"/>
  </sequence>
</complexType>

<!-- ROAP-LeaveDomainRequest -->
<element name="leaveDomainRequest" type="roap:DomainRequest"/>

<!-- ROAP-LeaveDomainResponse -->
<element name="leaveDomainResponse" type="roap:LeaveDomainResponse"/>

<complexType name="LeaveDomainResponse">
  <annotation>
    <documentation xml:lang="en">
      Message sent from RI to Device in response to a
      leaveDomainRequest
    </documentation>
  </annotation>
  <complexContent>
    <extension base="roap:Response">
      <sequence minOccurs="0">
        <element name="nonce" type="roap:Nonce"/>
        <element name="domainID" type="roap:DomainIdentifier"/>
        <element name="extensions" type="roap:Extensions" minOccurs="0"/>
      </sequence>
    </extension>
  </complexContent>
</complexType>

</schema>
```

Appendix B. ROAP Protocol Exchange Examples

All examples are syntactically correct. Signature, MAC, cipher and digest values are fictitious however.

B.1 Registration Protocol

B.1.1 Device hello

```
<?xml version="1.0" encoding="utf-8"?>
<roap:deviceHello
 xmlns:roap="urn:oma:bac:dldrm:roap-1.0"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <version>1.0</version>
  <deviceID>
    <keyIdentifier xsi:type="roap:X509SPKIHash">
      <hash>vXENc+Um/9/NvmYKiHDLaErK0gk=</hash>
    </keyIdentifier>
  </deviceID>
  <extensions>
    <extension xsi:type="roap:CertificateCaching"/>
  </extensions>
</roap:deviceHello>
```

B.1.2 RI Hello

```
<?xml version="1.0" encoding="utf-8"?>
<roap:riHello
 xmlns:roap="urn:oma:bac:dldrm:roap-1.0"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 status="Success" sessionId="433211">
  <selectedVersion>1.0</selectedVersion>
  <riID>
    <keyIdentifier xsi:type="roap:X509SPKIHash">
      <hash>aXENc+Um/9/NvmYKiHDLaErK0fk=</hash>
    </keyIdentifier>
  </riID>
  <riNonce>dsaiuiure9sdwerfqwer</riNonce>
  <trustedAuthorities>
    <keyIdentifier xsi:type="roap:X509SPKIHash">
      <hash>bew3e332oihde9dwiHDLaErK0fk=</hash>
    </keyIdentifier>
    <keyIdentifier xsi:type="roap:X509SPKIHash">
      <hash>3lkpoi9fceoiuoift45epokifc0poiss</hash>
    </keyIdentifier>
  </trustedAuthorities>
  <extensions>
    <extension xsi:type="roap:CertificateCaching"/>
  </extensions>
</roap:riHello>
```

B.1.3 Registration Request

```
<?xml version="1.0" encoding="utf-8"?>
<roap:registrationRequest
 xmlns:roap="urn:oma:bac:dldrm:roap-1.0"
```

```
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  sessionId="433211">
    <nonce>32efd34de39sdwefqwer</nonce>
    <time>2004-03-17T14:20:00Z</time>
    <certificateChain>
      <certificate>miib123121234567</certificate>
      <certificate>miib234124312431</certificate>
    </certificateChain>
    <trustedAuthorities>
      <keyIdentifier xsi:type="roap:X509SPKIHash">
        <hash>432098mhj987fdlkj98lkj098lkjr409</hash>
      </keyIdentifier>
      <keyIdentifier xsi:type="roap:X509SPKIHash">
        <hash>432098ewew5jy6532fewfew4f43f3409</hash>
      </keyIdentifier>
    </trustedAuthorities>
    <signature>321ue3ue3ue10ue2109ue1ueoidwoijdwe309u09ueqijdwqijdwq09uwqwqi009</signature>
</roap:registrationRequest>
```

B.1.4 Registration Response

```
<?xml version="1.0" encoding="utf-8"?>
<roap:registrationResponse
  xmlns:roap="urn:oma:bac:dldrm:roap-1.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  status="Success" sessionId="433211" riURL="www.anyRI.com/register">
    <certificateChain>
      <certificate>miib123121234567</certificate>
      <certificate>miib234124312431</certificate>
    </certificateChain>
    <ocspResponse>fdow9rw0feijfdsojr3w09u3wijfdslkj4sd</ocspResponse>
    <signature>321ue3ue3ue10ue2109ue1ueoidwoijdwe309u09ueqijdwqijdwq09uwqwqi009</signature>
</roap:registrationResponse>
```

B.2 Rights Object Acquisition

B.2.1 RO Request

The request is for a Device RO.

```
<?xml version="1.0" encoding="utf-8"?>
<roap:roRequest
  xmlns:roap="urn:oma:bac:dldrm:roap-1.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <deviceID>
      <keyIdentifier xsi:type="roap:X509SPKIHash">
        <hash>vXENc+Um/9/NvmYKiHDLaErK0gk=</hash>
      </keyIdentifier>
    </deviceID>
    <riID>
      <keyIdentifier xsi:type="roap:X509SPKIHash">
        <hash>aXENc+Um/9/NvmYKiHDLaErK0fk=</hash>
      </keyIdentifier>
    </riID>
    <nonce>32efd34de39sdwefqwer</nonce>
    <time>2004-03-17T14:20:00Z</time>
    <roInfo>
```

```
      <roID>n8yu98hy0e2109eu09ewf09u</roID>
    </roInfo>
    <certificateChain>
      <certificate>miib123121234567</certificate>
      <certificate>miib234124312431</certificate>
    </certificateChain>
    <signature>321ue3ue3ue10ue2109ue1ueoidwoijdwe309u09ueqijdwqijdwq09uwqwqi009</signature>
</roap:roRequest>
```

B.2.2 RO Response

The response is a Rights Object intended for the recipient only. Note that the response indicates that the Rights Object is stateful. The REL element is only outlined (an empty **<asset>** element).

```
<?xml version="1.0" encoding="utf-8"?>
<roap:roResponse
  xmlns:roap="urn:oma:bac:dldrm:roap-1.0"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
  xmlns:o-ex="http://odrl.net/1.1/ODRL-EX"
  xmlns:o-dd="http://odrl.net/1.1/ODRL-DD"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  status="Success">
    <deviceID>
      <keyIdentifier xsi:type="roap:X509SPKIHash">
        <hash>vXENc+Um/9/NvmYKiHDLaErK0gk=</hash>
      </keyIdentifier>
    </deviceID>
    <riID>
      <keyIdentifier xsi:type="roap:X509SPKIHash">
        <hash>aXENc+Um/9/NvmYKiHDLaErK0fk=</hash>
      </keyIdentifier>
    </riID>
    <nonce>32efd34de39sdwefqwer</nonce>
    <protectedRO>
      <ro id="n8yu98hy0e2109eu09ewf09u" stateful="true" version="1.0">
        <riID>
          <keyIdentifier xsi:type="roap:X509SPKIHash">
            <hash>aXENc+Um/9/NvmYKiHDLaErK0fk=</hash>
          </keyIdentifier>
        </riID>
        <rights o-ex:id="REL1">
          <o-ex:context>
            <o-dd:version>2.0</o-dd:version>
            <o-dd:uid>RightsObjectID</o-dd:uid>
          </o-ex:context>
          <o-ex:agreement>
            <o-ex:asset>
              <o-ex:context>
                <o-dd:uid>ContentID</o-dd:uid>
              </o-ex:context>
              <o-ex:digest>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <ds:DigestValue>bLLLc+Um/5/NvmYKiHDLaErK0fk=</ds:DigestValue>
              </o-ex:digest>
              <ds:KeyInfo>
                <xenc:EncryptedKey>
                  <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#kw-aes128"/>
```

```
                        <xenc:CipherData>
                           <xenc:CipherValue>EncryptedCEK</xenc:CipherValue>
                        </xenc:CipherData>
                     </xenc:EncryptedKey>
                     <ds:RetrievalMethod URI="K_MAC_and_K_REK"/>
                  </ds:KeyInfo>
               </o-ex:asset>
               <o-ex:permission>
                  <o-dd:play/>
               </o-ex:permission>
            </o-ex:agreement>
         </rights>
         <encKey Id="K_MAC_and_K_REK">
            <xenc:EncryptionMethod
       Algorithm="http://www.rsasecurity.com/rsalabs/pkcs/schemas/pkcs-1#rsaes-kem-kdf2-kw-aes128"/>
            <ds:KeyInfo>
               <roap:X509SPKIHash>
                  <hash>vXENc+Um/9/NvmYKiHDLaErK0gk=</hash>
               </roap:X509SPKIHash>
            </ds:KeyInfo>
            <xenc:CipherData>

<xenc:CipherValue>231jks231dkdwkj3jk321kj321j321kj423j342h213j321jh321jh2134jhk3211fdslfdsopfespj
oefwopjsfdpojvct4w925342a</xenc:CipherValue>
            </xenc:CipherData>
         </encKey>
      </ro>
      <mac>
         <ds:SignedInfo>
            <ds:CanonicalizationMethod
        Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod
        Algorithm="http://www.w3.org/2000/09/xmldsig#hmac-sha1"/>
            <ds:Reference URI="#n8yu98hy0e2109eu09ewf09u">
               <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
               <ds:DigestValue>j6lwx3rvEPO0vKtMup4NbeVu8nk=</ds:DigestValue>
            </ds:Reference>
         </ds:SignedInfo>
         <ds:SignatureValue>j6lwx3rvEPO0vKtMup4NbeVu8nk=</ds:SignatureValue>
         <ds:KeyInfo>
            <ds:RetrievalMethod URI="#K_MAC_and_K_REK"/>
         </ds:KeyInfo>
      </mac>
   </protectedRO>
   <ocspResponse>miibewqoidpoidsa</ocspResponse>
   <extensions>
      <extension xsi:type="roap:TransactionIdentifier">
         <id>09321093209-2121</id>
      </extension>
   </extensions>
   <signature>d93e5fue3susdskjhkjedkjrewh53209efoihfdse10ue2109ue1</signature>
</roap:roResponse>
```

B.2.3 Domain RO

The Domain RO may be sent separately, as here, or within a ROAP-ROResponse.

```
<?xml version="1.0" encoding="utf-8"?>
```

```
<roap:roResponse
 xmlns:roap="urn:oma:bac:dldrm:roap-1.0"
 xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
 xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
 xmlns:o-ex="http://odrl.net/1.1/ODRL-EX"
 xmlns:o-dd="http://odrl.net/1.1/ODRL-DD"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 status="Success">
  <deviceID>
    <keyIdentifier xsi:type="roap:X509SPKIHash">
      <hash>vXENc+Um/9/NvmYKiHDLaErK0gk=</hash>
    </keyIdentifier>
  </deviceID>
  <riID>
    <keyIdentifier xsi:type="roap:X509SPKIHash">
      <hash>aXENc+Um/9/NvmYKiHDLaErK0fk=</hash>
    </keyIdentifier>
  </riID>
  <nonce>32efd34de39sdwefqwer</nonce>
  <protectedRO>
    <ro id="n8yu98hy0e2109eu09ewf09u" stateful="true" version="1.0">
      <riID>
        <keyIdentifier xsi:type="roap:X509SPKIHash">
          <hash>aXENc+Um/9/NvmYKiHDLaErK0fk=</hash>
        </keyIdentifier>
      </riID>
      <rights o-ex:id="REL1">
        <o-ex:context>
          <o-dd:version>2.0</o-dd:version>
          <o-dd:uid>RightsObjectID</o-dd:uid>
        </o-ex:context>
        <o-ex:agreement>
          <o-ex:asset>
            <o-ex:context>
              <o-dd:uid>ContentID</o-dd:uid>
            </o-ex:context>
            <o-ex:digest>
              <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
              <ds:DigestValue>bLLLc+Um/5/NvmYKiHDLaErK0fk=</ds:DigestValue>
            </o-ex:digest>
            <ds:KeyInfo>
              <xenc:EncryptedKey>
                <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#kw-aes128"/>
                <xenc:CipherData>
                  <xenc:CipherValue>EncryptedCEK</xenc:CipherValue>
                </xenc:CipherData>
              </xenc:EncryptedKey>
              <ds:RetrievalMethod URI="K_MAC_and_K_REK"/>
            </ds:KeyInfo>
          </o-ex:asset>
          <o-ex:permission>
            <o-dd:play/>
          </o-ex:permission>
        </o-ex:agreement>
      </rights>
      <encKey Id="K_MAC_and_K_REK">
        <xenc:EncryptionMethod
```

```
      Algorithm="http://www.rsasecurity.com/rsalabs/pkcs/schemas/pkcs-1#rsaes-kem-kdf2-kw-aes128"/>
          <ds:KeyInfo>
            <roap:X509SPKIHash>
              <hash>vXENc+Um/9/NvmYKiHDLaErK0gk=</hash>
            </roap:X509SPKIHash>
          </ds:KeyInfo>
          <xenc:CipherData>

<xenc:CipherValue>231jks231dkdwkj3jk321kj321j321kj423j342h213j321jh321jh2134jhk3211fdslfdsopfespj
oefwopjsfdpojvct4w925342a</xenc:CipherValue>
          </xenc:CipherData>
        </encKey>
      </ro>
      <mac>
        <ds:SignedInfo>
          <ds:CanonicalizationMethod
       Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
          <ds:SignatureMethod
       Algorithm="http://www.w3.org/2000/09/xmldsig#hmac-sha1"/>
          <ds:Reference URI="#n8yu98hy0e2109eu09ewf09u">
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>j6lwx3rvEPO0vKtMup4NbeVu8nk=</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>j6lwx3rvEPO0vKtMup4NbeVu8nk=</ds:SignatureValue>
        <ds:KeyInfo>
          <ds:RetrievalMethod URI="#K_MAC_and_K_REK"/>
        </ds:KeyInfo>
      </mac>
    </protectedRO>
    <ocspResponse>miibewqoidpoidsa</ocspResponse>
    <extensions>
      <extension xsi:type="roap:TransactionIdentifier">
        <id>09321093209-2121</id>
      </extension>
    </extensions>
    <signature>d93e5fue3susdskjhkjedkjrewh53209efoihfdse10ue2109ue1</signature>
</roap:roResponse>
```

B.3 Join Domain Protocol

B.3.1 Join Domain Request

```
<?xml version="1.0" encoding="utf-8"?>
<roap:joinDomainRequest
  xmlns:roap="urn:oma:bac:dldrm:roap-1.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <deviceID>
      <keyIdentifier xsi:type="roap:X509SPKIHash">
        <hash>vXENc+Um/9/NvmYKiHDLaErK0gk=</hash>
      </keyIdentifier>
    </deviceID>
    <riID>
      <keyIdentifier xsi:type="roap:X509SPKIHash">
        <hash>aXENc+Um/9/NvmYKiHDLaErK0fk=</hash>
      </keyIdentifier>
    </riID>
```

```
   <nonce>32efd34de39sdwefqwer</nonce>
   <time>2004-03-17T14:30:00Z</time>
   <domainID>Domain-XYZ-01</domainID>
   <certificateChain>
      <certificate>miib123121234567</certificate>
      <certificate>miib234124312431</certificate>
   </certificateChain>
   <signature>321ue3ue3ue10ue2109ue1ueoidwoijdwe309u09ueqijdwqijdwq09uwqwqi009</signature>
</roap:joinDomainRequest>
```

B.3.2 Join Domain Response

```
<?xml version="1.0" encoding="utf-8"?>
<roap:joinDomainResponse
 xmlns:roap="urn:oma:bac:dldrm:roap-1.0"
 xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
 xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 status="Success">
  <deviceID>
     <keyIdentifier xsi:type="roap:X509SPKIHash">
        <hash>vXENc+Um/9/NvmYKiHDLaErK0gk=</hash>
     </keyIdentifier>
  </deviceID>
  <riID>
     <keyIdentifier xsi:type="roap:X509SPKIHash">
        <hash>aXENc+Um/9/NvmYKiHDLaErK0fk=</hash>
     </keyIdentifier>
  </riID>
  <nonce>32efd34de39sdwefqwer</nonce>
  <domainInfo>
     <notAfter>2004-12-22T03:02:00Z</notAfter>
     <domainKey>
        <encKey Id="Domain-XYZ-01">
           <xenc:EncryptionMethod
     Algorithm="http://www.rsasecurity.com/rsalabs/pkcs/schemas/pkcs-1#rsaes-kem-kdf2-kw-aes128"/>
           <ds:KeyInfo>
              <roap:X509SPKIHash>
                 <hash>vXENc+Um/9/NvmYKiHDLaErK0gk=</hash>
              </roap:X509SPKIHash>
           </ds:KeyInfo>
           <xenc:CipherData>

<xenc:CipherValue>231jks231dkdwkj3jk321kj321j321kj423j342h213j321jh321jh2134jhk3211fdslfdsopfespj
oefwopjsfdpojvct4w925342a</xenc:CipherValue>
           </xenc:CipherData>
        </encKey>
        <riID>
           <keyIdentifier xsi:type="roap:X509SPKIHash">
              <hash>aXENc+Um/9/NvmYKiHDLaErK0fk=</hash>
           </keyIdentifier>
        </riID>
        <mac>ewqrewoewfewohffohr3209832r3</mac>
     </domainKey>
  </domainInfo>
  <certificateChain>
     <certificate>MIIB223121234567</certificate>
```

```
      <certificate>MIIB834124312431</certificate>
    </certificateChain>
    <ocspResponse>miibewqoidpoidsa</ocspResponse>
    <signature>d93e5fue3ue10ue2109ue1ueoidwoijdwe309u09ueqijdwqijdwq09uwqwqi009</signature>
</roap:joinDomainResponse>
```

B.4 Leave Domain Protocol

B.4.1 Leave Domain Request

```
<?xml version="1.0" encoding="utf-8"?>
<roap:leaveDomainRequest
  xmlns:roap="urn:oma:bac:dldrm:roap-1.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <deviceID>
      <keyIdentifier xsi:type="roap:X509SPKIHash">
        <hash>vXENc+Um/9/NvmYKiHDLaErK0gk=</hash>
      </keyIdentifier>
    </deviceID>
    <riID>
      <keyIdentifier xsi:type="roap:X509SPKIHash">
        <hash>aXENc+Um/9/NvmYKiHDLaErK0fk=</hash>
      </keyIdentifier>
    </riID>
    <nonce>32efd34de39sdwefqwer</nonce>
    <time>2004-03-17T19:20:00Z</time>
    <domainID>Domain-XYZ-01</domainID>
    <certificateChain>
      <certificate>miib123121234567</certificate>
      <certificate>miib234124312431</certificate>
    </certificateChain>
    <signature>321ue3ue3ue10ue2109ue1ueoidwoijdwe309u09ueqijdwqijdwq09uwqwqi009</signature>
</roap:leaveDomainRequest>
```

B.4.2 Leave Domain Response

```
<?xml version="1.0" encoding="utf-8"?>
<roap:leaveDomainResponse
  xmlns:roap="urn:oma:bac:dldrm:roap-1.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  status="Success">
    <nonce>32efd34de39sdwefqwer</nonce>
    <domainID>Domain-XYZ-01</domainID>
</roap:leaveDomainResponse>
```

B.5 Roap Trigger

This example is for a "Leave Domain" trigger.

```
<?xml version="1.0" encoding="UTF-8"?>

<roap-trigger:roapTrigger
  xmlns:roap-trigger="urn:oma:bac:dldrm:roap-trigger-20040120"
  xmlns:roap="urn:oma:bac:dldrm:roap-1.0"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
```

```
  xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="
    urn:oma:bac:dldrm:roap-trigger-20040120 ../roap-trigger.xsd
    urn:oma:bac:dldrm:roap-1.0 roap.xsd
    http://www.w3.org/2000/09/xmldsig#
    http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/xmldsig-core-schema.xsd
    http://http://www.w3.org/2001/04/xmlenc#
    http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/xenc-schema.xsd">
  <leaveDomain id="de32r23r4">
    <riID>
      <keyIdentifier xsi:type="roap:X509SPKIHash">
        <hash>aXENc+Um/9/NvmYKiHDLaErK0fk=</hash>
     </keyIdentifier>
    </riID>
    <roapURL>http://ri.example.com/ro.cgi?tid=qw683hgew7d</roapURL>
    <domainID>Domain-XYZ-01</domainID>
  </leaveDomain>
  <mac>
    <ds:SignedInfo>
      <ds:CanonicalizationMethod
        Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      <ds:SignatureMethod
        Algorithm="http://www.w3.org/2000/09/xmldsig#hmac-sha1"/>
      <ds:Reference URI="#de32r23r4">
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <ds:DigestValue>j6lwx3rvEPO0vKtMup4NbeVu8nk=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>j6lwx3rvEPO0vKtMup4NbeVu8nk=</ds:SignatureValue>
    <ds:KeyInfo>
      <ds:RetrievalMethod URI="#K_MAC"/>
    </ds:KeyInfo>
  </mac>
  <encKey Id="K_MAC">
    <xenc:EncryptionMethod
     Algorithm="http://www.w3.org/2001/04/xmlenc#kw-aes128"/>
    <ds:KeyInfo>
      <roap:DomainIdentifier>Domain-XYZ-01</roap:DomainIdentifier>
    </ds:KeyInfo>
    <xenc:CipherData>
      <xenc:CipherValue>32fdsorew9ufdsoi09ufdskrew9urew0uderty5346wq</xenc:CipherValue>
    </xenc:CipherData>
  </encKey>
</roap-trigger:roapTrigger>
```

Appendix C. Backward Compatibility with Release 1.0 (Normative)

Devices that support OMA DRM v2 MUST support the mandatory features of OMA DRM V1 [DRM]. To ensure consistent, interoperable behaviour, OMA DRM v2 Devices MUST behave in the following manner when receiving OMA DRM v1 Content.

DRM v2 Client receives the following DRM v1 content type	DRM v1 method *not* supported	DRM v1 method *is* supported
Forward Lock content	n/a (DRM v1 Forward Lock is mandatory)	Handle content as defined in [DRM]
Combined Delivery content	Handle content as defined in [DRM]	Handle content as defined in [DRM]
Separate Delivery Content	MAY notify the user	Handle content as defined in [DRM]; Upon contacting the CI/RI the Device MUST advertise DRM version and supported media types as defined in section 10.

Table 14: Backward Compatibility with Release 1.0

Appendix D. Exporting to Other DRMs (Informative)

D.1 High-level Example : Exporting to Removable Media

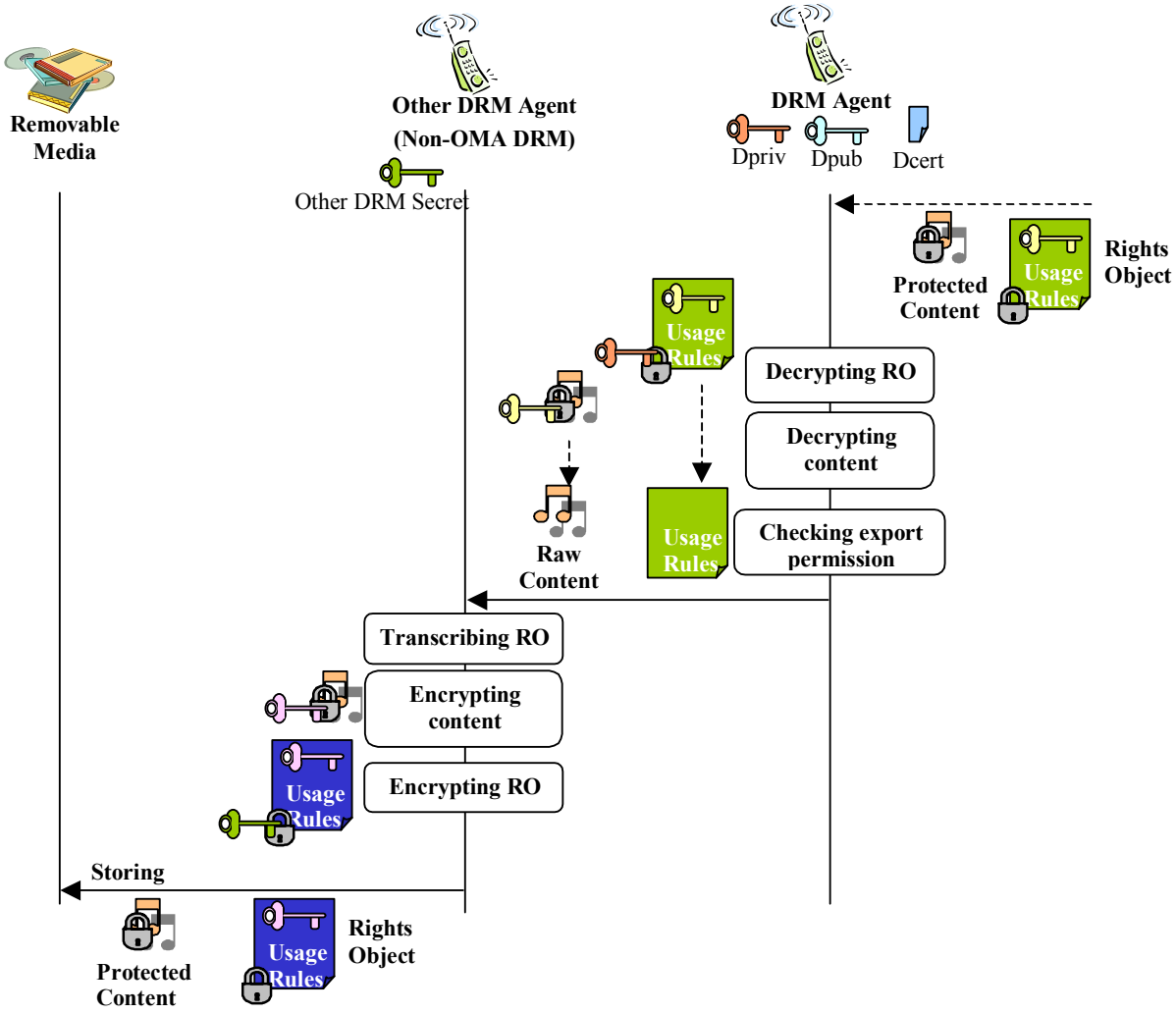

Figure 14:. Example - Exporting to Removable Media

An example of exporting DRM protected content and Rights Object to other DRM (non-OMA DRM) system, which has some authorized protection mechanism, is shown above.

1. After Protected Content and protected Rights Object are delivered to a trusted OMA DRM Agent, the Protected Content is consumed by the OMA DRM Agent according to permissions and constraints described in the protected Rights Object. When consuming the content, OMA DRM Agent decrypts the protected RO with DRM Agent private key and decrypts the protected content with CEK that is derived from decrypted Rights Object.

2. When exporting, OMA DRM Agent checks permissions described in the Rights Object whether Rights Issuer allows the content to be exported to targeted DRM system, whether its content type is appropriate and whether its usage rules are compatible with targeted DRM system.

   When user wants to download exportable content and Rights Issuer notices it in the course of content discovery interaction, it would be expected that both of the Protected Content and RO are suitable for the targeted DRM capability.

3. The raw content and usage rules are transferred from OMA DRM Agent to the other DRM Agent.

4. The other DRM Agent transcribes the compatible usage rules to the other DRM usage rules according to the general rule and the specific rule defined by the other DRM system and Rights Issuer to maintain consistency of the Rights Object.

   Sample transcription rules are:
   Any other permissions MUST NOT be granted.
   Any existing constraints MUST NOT be ignored.
   Default permissions and constraints MAY be supplied.

   Even stateful Rights Object could be transcribed and exported to other DRM system if those rules allow it.

5. The other DRM Agent creates new CEK inside, and encrypts the content with the new CEK and encrypts transcribed usage rules including the CEK with other DRM system's secret key.

6. The other DRM Agent and the removable media authenticate with each other to make sure that they are trusted, and stores the encrypted content and the usage rules onto a removable media according to the other DRM specific format.

7. Then user can pull out the removable media from the Device, insert it to other DRM compliant Device such as portable music player, to enjoy playing the content.

The two DRM Agents, OMA DRM Agent and the other DRM Agent, may reside in a single Device or different Devices, but these two agents and data channel between the two have to be implemented in a secure manner according to some compliance rules or robustness rules which may be defined related to a specific service, by Rights Issuers, Service Providers, and Device Manufacturers who participate in the service.

Appendix E. Application to Services (Informative)

E.1 Application to Streaming Services

The main scope of OMA DRM is protection of downloadable objects, which can by their nature be embedded into DCFs and be delivered under DRM control. This is not immediately possible with streaming media, since streaming media are transported using protocols and mechanisms that do not allow embedding into download DCFs, and also since streams are not per se limited in time and size. Thus, the protected transport of streams and some associated signaling has to be defined separately for streaming media. On the other hand, OMA DRM ROs can be used for streaming services for the definition and transport of rights/permissions, and of content decryption keys.

Thus, the basic concept for the application of OMA DRM to streaming services is that OMA DRM ROs, and the ROAP, are used in the same way as for downloadable objects/DCFs. This is specified in this standard. The exact way of protecting streams, storing streams at a streaming server, and transporting streams to a Device (including associated signaling) are not specified in this specification. It is the responsibility of streaming standardization bodies to define appropriate mechanisms that work seamlessly together with the concept laid out in the DRM specification, especially with the RO concept and format. **Figure 16** explains the principle.

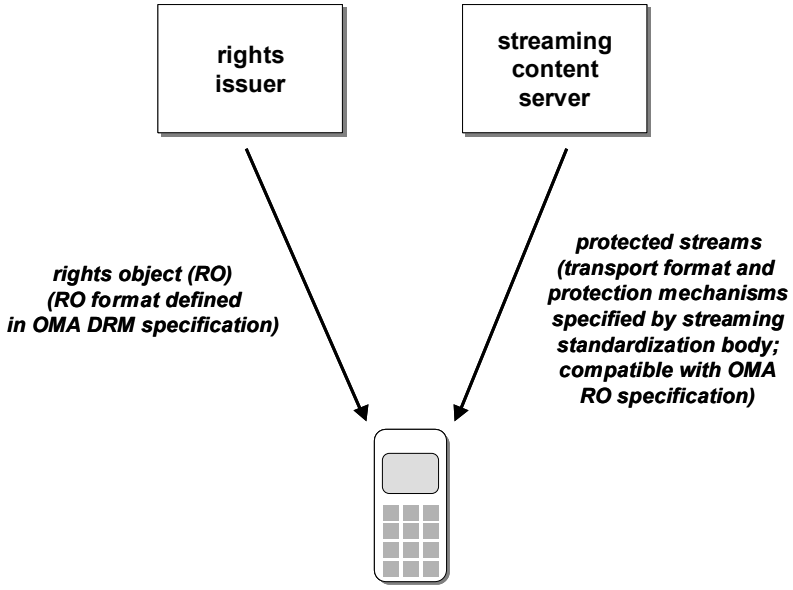

Figure 15: Generic principle of application of OMA DRM to streaming services

E.1.1 Application to the 3GPP Packet-Switched Streaming Service

For the special case of the 3GPP Packet-Switched Streaming Service (PSS) Release 6, i.e., the 3GPP streaming standard [3GPP PSS], OMA and 3GPP have been working together to define DRM protection of PSS media. The basic principle is the one shown in Figure 15, but there are some extensions that consider special features and properties of the PSS standard, namely

a) PSS sessions can consist of a mixture of discrete (e.g., JPEG images) and continuous (e.g., H.263 video) media

b) There are 3 different methods to initiate a PSS session using different streaming tokens: either a SMIL presentation description, or an SDP session description, or an RTSP URL. A streaming token can get to a Device as a download from a server, or by super-distribution from other Devices, or by other means like user input of an RTSP URL via the keyboard.

c) Time-continuous protected media like audio and video tracks that are stored on a PSS server in the 3GP file format defined by 3GPP can either be downloaded by (progressive) download of the whole 3GP file,

or streamed by extraction of protected media tracks from the 3GP file format and transport using real-time transport protocols. OMA has adopted the 3GP file format for protected packetized content as a special DCF, the Packetized DCF (PDCF) [DRMDCF-v2]. It should thus be understood that a 3GP file holding encrypted tracks as defined in [TS26.244] is automatically a valid OMA DRM PDCF [DRMDCF-v2].

Figure 16 gives an overview of the involved entities and data flows for DRM protection of 3GPP PSS sessions and media.

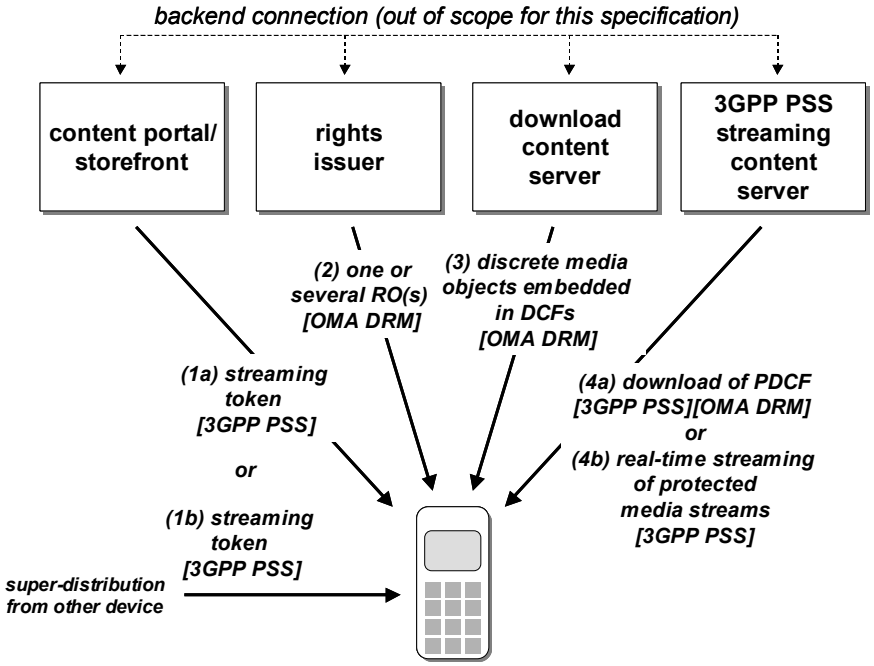

Figure 16: Application of OMA DRM to the 3GPP Packet-Switched Streaming Service (Release 6). References in brackets indicate where the respective data format or protocol is specified

For a protected PSS presentation, the content provider can confidentiality protect and integrity protect discrete media (images etc.) by embedding them into OMA DCFs. Further, he can confidentiality protect and integrity protect continuous media using the mechanisms defined by 3GPP, and storing them in a file in the 3GP file format [TS26.244], i.e., in a PDCF. The DCFs are stored on a content download server, the protected 3GP files = PDCFs on a 3GPP PSS server. Note that the PDCF can later be used for download or streaming of the included tracks/streams ((4a) or (4b) in.**Figure 16**).

All information needed to generate ROs for the DCFs and PDCFs must be conveyed to the Rights Issuer; how this is done is outside the scope of this specification. This information includes the used content encryption keys for the discrete and continuous media, and usage rights/permissions.

The required steps to initiate, set up, receive, and render a protected 3GPP PSS session are then the following:

A. A streaming session is initiated via a streaming token, i.e. a SMIL presentation, SDP file, or RTSP URL [3GPP PSS]. The streaming token can arrive to the Device by download from a server/content portal/content storefront (see (1a) in Figure 16), or by super-distribution (see (1b) in Figure 16), by messaging (MMS), or by other means (e.g. an RTSP URL can be manually entered by the user). The streaming token can optionally be embedded into a DCF.

B. If the streaming token has been acquired directly from a server or portal, the server can initiate the delivery of one or several ROs to the Device that contain the keys and rights for the media referenced by the token (see (2) in Figure 16). In all other cases, the ROs for protected streams are requested during session setup to the streaming server, and the ROs for protected discrete objects after download of the respective DCFs, see (D)

C. When the user decides to start the PSS streaming session, she or he executes/launches the streaming token which is delivered to the streaming player. The streaming player evaluates the streaming token.

D. Depending on the type of streaming token, the following applies:

- SMIL presentation: Referenced discrete objects are downloaded from the respective download servers (see (3) and (4a) in Figure 16.). If ROs are not on the Device yet they can be acquired at this point, using the RI URL in the DCFs . Referenced streams are set up and started using PSS streaming protocols [3GPP PSS] (see (4b) in Figure 16.). If ROs are not on the Device yet they can be acquired at this point, using the RI URL. Note: SMIL allows to download objects / start streams during a presentation. In this case it may be an implementation optimization to fetch all ROs before starting the presentation.
- RTSP URL: Referenced streams are set up and started using PSS streaming protocols [3GPP PSS] (see (4b) in Figure 16). If ROs are not on the Device yet they can be acquired at this point, using the RI URL.
- SDP: Referenced streams are set up and started using PSS streaming protocols [3GPP PSS] (see (4b) in Figure 16). If ROs are not on the Device yet they can be acquired at this point, using the RI URL.

E. Discrete objects (DCFs), downloaded PSS content (PDCFs), and PSS streams are decrypted and rendered subject to the terms and permissions of the respective ROs.

F. The streaming token can be super-distributed to another Device. To be able to receive and render the referenced PSS media content, the receiving Device must acquire the respective RO(s).

E.1.2 DCF Packaging of Streaming Session Descriptors

The section describes an optional variation of the basic architecture and method for protection of streams using OMA DRM. In this variation, the streaming token / streaming session description is itself packaged into a DCF. This is illustrated in **Figure 17**.

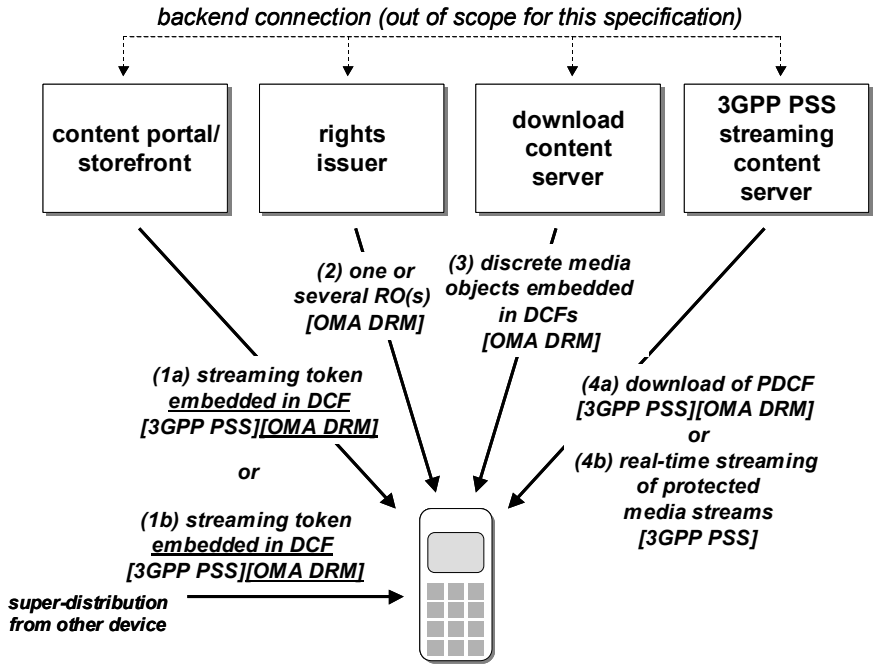

Figure 17: Application of OMA DRM to the 3GPP Packet-Switched Streaming Service (Release 6) with streaming token packaged into DCF. Underlined text denotes differences to Figure 16.

With this method, the typical steps to initiate, set up, receive, and render a protected 3GPP PSS session are similar as described in section E.1.1, with a few differences. The differences are outlined below.

(A) *Unchanged, see section E.1.1.*

(B) If the streaming token has been acquired directly from a server or portal, the server can initiate the delivery of one or several ROs to the Device that contain the keys and rights for the media referenced by the token (see (2) in **Figure 17**). Otherwise, the Device can use the RI URL in the streaming token DCF to request Rights Objects. If the RO or ROs delivered in response to this request contain the keys and rights for all media elements and streams being part of the PSS session associated with the token, no further RO requests are necessary.

(C) *Unchanged, see section E.1.1.*

(D) Depending on the type of streaming token, the following applies:

a. SMIL presentation: Referenced discrete objects are downloaded from the respective download servers (see (3) and (4a) in **Figure 17**). Referenced streams are set up and started using PSS streaming protocols [3GPP PSS] (see (4b) in **Figure 17**).

b. RTSP URL: Referenced streams are set up and started using PSS streaming protocols [3GPP PSS] (see (4b) in **Figure 17**). Please note that an RTSP URL per se cannot be packaged into a DCF, because there is no MIME type for RTSP URLs. However, a workaround is to package the RTSP URL into a helper file (e.g. a minimal SMIL file), and package the helper file into a DCF.

c. SDP: Referenced streams are set up and started using PSS streaming protocols [3GPP PSS] (see (4b) in **Figure 17**).

(E) *Unchanged, see section E.1.1.*

(F) *Unchanged, see section E.1.1.*

A difference using the optional method is the point in time when ROs are requested/acquired: it is always (including the super-distribution case) possible to request rights when the DCF containing the streaming token is available on the Device, and before streaming of content is initiated. If the RO (or ROs) delivered in response contain rights and keys for all media objects and streams used in the respective PSS presentation, no further RO requests are necessary.

Also, the RI can associate permissions or constraints with the streaming token, in addition to constraints on the referenced media objects or streams. For example, for datetime based restrictions on streams, the same restriction could be imposed on the token. If the user tries to use the streaming token after expiry, this is then recognized when the token is executed, and before any communication with the streaming server is set up.

All DCF-associated functionality is applicable to a streaming token packaged into a DCF (e.g., integrity protection of DCF, preview rights URL, etc.).

The described optional method of packaging streaming tokens into DCFs has no implications on the security or protection of the referenced media objects and streams.

Appendix F. Certificate Profiles and Requirements (Normative)

F.1 DRM Agent Certificates

The profile for DRM Agent certificates follows the profile for "User Certificates for Authentication" in [WAPCertProf] with the following modifications:

Version	3
Signature	MUST be RSA with SHA-1
Serial Number	MUST be less than, or equal to, 20 bytes in length
Issuer Name	MUST be present and MUST use a subset of the following naming attributes from [WAPCertProf] – countryName, organizationName, organizationalUnitName, commonName, and stateOrProvinceName.
Subject Name	MUST be present and MUST use a subset of the following naming attributes from [WAPCertProf] – countryName, organizationName, organizationalUnitName, commonName, and serialNumber. The structure and contents of a Device subject name shall be as follows: [countryName=<Country of manufacturer>] [organizationName=<Manufacturer company name>] [organizationalUnitName=<Manufacturing location>] [commonName=<Model name>] serialNumber=<Unique identifier for Device, as assigned by the Certificate Issuer. Does not have to be the same as the IMEI> The serialNumber attribute MUST be present. The countryName, organizationName, organizationalUnitName, and commonName may be present. Other attributes are not allowed and must not be included. For all naming attributes of type DirectoryString, the PrintableString or the UTF8String choice must be used. Note that the maximum length (in octets) for values of these attributes is as follows: countryName – 4 (country code in accordance with ISO/IEC 3166), organizationName, organizationalUnitName, commonName, and serialNumber – 64. Example: C="US";O="DRM Devices 'R Us"; CN="DRM Device Mark V"; SN="1234567890"

Extensions	The extKeyUsage extension SHALL be present, and contain (at least) the **oma-kp-drmAgent** key purpose object identifier:
	`oma-kp-drmAgent OBJECT IDENTIFIER ::= {oma-kp 2}`
	`oma-kp OBJECT IDENTIFIER ::= {??}`
	CAs are recommended to set this extension to critical.
	- If CAs include the keyUsage extension (recommended), then both the digitalSignature bit and the keyEncipherment bit must be set, if the corresponding private key is to be used both for authentication and decryption. Otherwise only the applicable bit shall be set. When present, this extension shall be set to critical.
	CAs may include the certificatePolicy extension, indicating the policy the certificate has been issued under, and possibly containing a URI identifying a source of more

	information about the policy. CAs are recommended to not include any other extensions, but may, for compliance with [RFC3280], include the authorityKeyIdentifier extension. CAs may also include the authorityInfoAccess extension from [RFC3280] for OCSP responder navigation purposes. CAs MUST NOT include any other critical extensions.

RI implementations MUST meet all requirements on entities processing user certificates defined in [WAPCertProf]. In addition, RIs:

- MUST be able to process DRM Agent certificates with serial numbers up to 20 bytes long; and
- MUST recognize and require the presence of the **oma-kp-drmAgent** object identifier defined above in the extKeyUsage extension in DRM Agent certificates.

F.2 Rights Issuer Certificates

The profile for RI certificates follows the profile for "X.509-compliant server certificate" in [WAPCertProf] with the following modifications:

Signature	MUST be RSA with SHA-1
Serial Number	MUST be less than, or equal to, 20 bytes in length
Issuer Name	MUST be present and MUST use a subset of the following naming attributes from [WAPCertProf] – countryName, organizationName, organizationalUnitName, commonName, and stateOrProvinceName.
Subject Name	MUST be present and MUST use a subset of the following naming attributes from [WAPCertProf] – countryName, stateOrProvinceName, localityName, organizationName, organizationalUnitName, and commonName. The structure and contents of a Rights Issuer subject name shall be as follows: countryName=<Country of operation> [stateOrProvinceName=<State/Province>] [localityName=<City>] organizationName=<RI company name> [organizationalUnitName=<RI subsidiary/location>] commonName=<RI company name> "OMA Rights Issuer" [<serNo>] (For the commonName attribute, the <serNo> string is specified when a given organization has several RIs.) The countryName, organizationName, and commonName naming attributes must be present. The stateOrProvinceName, localityName, and/or organizationalUnitName naming attributes may be present. Other attributes are not allowed and must not be included. For all naming attributes of type DirectoryString, the PrintableString or the UTF8String choice must be used. Note that the maximum length (in octets) for values of these attributes is as follows: countryName – 4, stateOrProvinceName and localityName – 128, organizationName, organizationalUnitName, and commonName – 64. Example: C="US";O="ROs for everyone"; CN="ROs for everyone OMA Rights Issuer"

Extensions	The extKeyUsage extension shall be present, and contain (at least) the **oma-kp-rightsIssuer** key purpose object identifier: `oma-kp-rightsIssuer OBJECT IDENTIFIER ::= {oma-kp 1}` CAs are recommended to set this extension to critical. If the keyUsage extension is present (recommended), then the digitalSignature bit shall be set. When present, this extension shall be set to critical. CAs may include the certificatePolicy extension, indicating the policy the certificate has been issued under, and possibly containing a URI identifying a source of more information about the policy. CAs are recommended to not include any other extensions, but may, for compliance with RFC3280, include the authorityKeyIdentifier extension. CAs may also include the authorityInfoAccess extension from [RFC3280] for OCSP responder navigation purposes. CAs MUST NOT include any other critical extensions.

DRM Agents processing Rights Issuer certificates MUST meet the requirements on clients processing "X.509-compliant server certificates" defined in [WAPCertProf]. In addition, DRM Agents:

- MUST be able to process RI certificates up to 1500 bytes long;
- MUST be able to process RI certificates with serial numbers 20 bytes long; and
- MUST recognize and require the presence of the **oma-kp-rightsIssuer** object identifier defined above in the extKeyUsage extension in RI certificates.

F.3 CA Certificates

The profile for OMA DRM CA certificates follows the profile for "Authority Certificates" in [WAPCertProf] with the following modifications:

Signature	MUST be RSA with SHA-1
Serial Number	MUST be less than, or equal to, 20 bytes in length

RIs and DRM Agents MUST meet the requirements on relying parties defined in [WAPCertProf]. Note that this implies, among other things, a requirement on RIs and DRM Agents to also recognize the basicConstraints and the subjectKeyIdentifier extensions. In addition, DRM Agents:

- MUST be able to process authority certificates up to 1500 bytes long; and
- MUST be able to process authority certificates with serial numbers 20 bytes long.

F.4 OCSP Responder Certificates

The profile for OCSP responder certificates in [OCSP-MP] applies. RIs and DRM Agents MUST meet the requirements on "Authority Certificate" relying parties defined in [WAPCertProf]. In addition, RIs and DRM Agents:

- MUST be able to process OCSP responder certificates up to 1500 bytes long;
- MUST be able to process OCSP responder certificates with serial numbers 20 bytes long; and
- MUST recognize the extKeyUsage extension and its **id-kp-OCSPSigning** object identifier (i.e. support OCSP responder delegation).

F.5 User Certificates for Authentication

The profile specified in [WAPCertProf] MUST be used. If a Device supports WIM and binding to the WIM, then, note that this implies a requirement on DRM Agents to also recognize the keyUsage, extKeyUsage, certificatePolicies, subjectAltName, and basicConstraints extensions.

Appendix G. Interactions between the DRM Agent and the WIM(Informative)

G.1 WIM Operations in Exercising "permission" to bind Rights Objects to the User Identity

This chapter describes messages sent between the DRM Agent and the WIM that come up to exercise permission to bind RO to the user identity procedure. The message flow between the DRM Agent and the WIM is described at a functional level, using service primitives.

The preliminary exchanges based on *device control* and *verification related* primitives c.f., [WIM] are intentionally omitted from this flowchart but MAY be required.

The DRM Agent must set the WIM_GENERIC_RSA Security Environment to perform the signature operations.

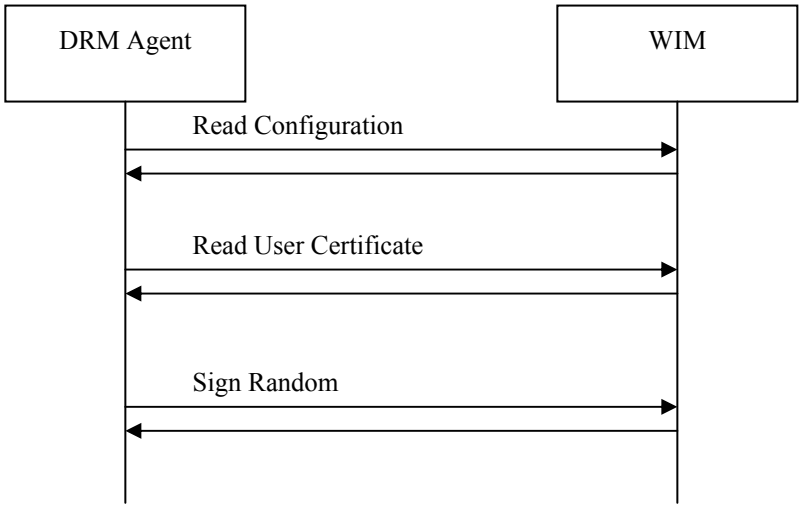

Figure 18: DRM Agent and WIM Interaction

Read configuration
Before starting the procedure, the DRM Agent needs to know which algorithms the WIM supports and information on keys and certificates stored in the WIM.
To read the configuration the DRM Agent uses data access primitives: WIM-OpenFile, WIM-ReadBinary etc.

Read user certificate
The DRM Agent may read the user certificate stored in the WIM and identified by PKCS_iD.
To read the user certificate the DRM Agent uses data access primitives: WIM-OpenFile, WIM-ReadBinary etc.

Sign random
The WIM has to sign the challenge number sent by the DRM Agent and return the signature. The DRM Agent may successfully verify the signature prior to exercise the permission.
To get the signature the DRM Agent uses the WIM-ComputeDigitalSignature primitive. The primitive returns the signature.

G.2 PIN Management

Said user private key is protected by a PIN-G (Global PIN), thus the procedure may require PIN-G verification i.e., the DRM Agent may have to send the WIM-Perform-Verification primitive one time per WIM session. Once PIN-G right is granted, the procedure does not require PIN-G verification anymore for the current WIM session.

1. Note: in case the WIM application is present on a UICC smart card platform [UICC] together with a USIM [3GPP TS 31.102] application, the WIM PIN-G can be mapped on the USIM PIN.

Appendix H. Static Conformance Requirements (Normative)

The notation used in this appendix is specified in [IOPPROC].

H.1 Client Conformance Requirements

The table below enumerates the client conformance requirements on all Devices – Connected, as well as Unconnected Devices.

Item	Function	Reference	Status	Requirements
DRM-CLI-CMN-001	ROAP Schema parsing and processing support.	5.3	M	
DRM-CLI-CMN-002	Comparison of ROAP values	5.3.2	M	
DRM-CLI-CMN-003	Nonce values in ROAP messages	5.3.9	M	
DRM-CLI-CMN-004	Processing and responding to status codes during ROAP protocol runs	5.3.5,5.4.2	M	
DRM-CLI-CMN-005	ROAP Trigger parsing and processing	5.2.1	M	
DRM-CLI-CMN-006	ProtectedRO support	5.3.7,5.3.8	M	
DRM-CLI-CMN-007	XML Canonicalization	5.3.8,5.4	M	
DRM-CLI-CMN-008	4-pass ROAP-Registration protocol	5.4.2	M	
DRM-CLI-CMN-009	ROAP Extensions	5.4.2,5.4.3, 5.4.4	O	
DRM-CLI-CMN-010	Hash Algorithms: SHA-1 and associated URI	5.4.2.1.1	M	
DRM-CLI-CMN-011	MAC Algorithms: HMAC-SHA-1 and associated URI	5.4.2.1.1	M	
DRM-CLI-CMN-012	Signature Algorithms: RSA-PSS-Default and associated URI	5.4.2.1.1	M	
DRM-CLI-CMN-013	Key Transport Algorithms: RSAES-KEM-KDF2-KW-AES128 and associated URI	5.4.2.1.1	M	
DRM-CLI-CMN-014	Key Wrap Algorithms: AES-WRAP and associated URI	5.4.2.1.1	M	
DRM-CLI-CMN-015	Hash Chains for Domain Key Management	5.4.4.1.1,7.3,8.7.1	O	
DRM-CLI-CMN-016	DRM Agent Certificates	F.1	M	
DRM-CLI-CMN-017	User Certificates for WIM Binding	F.5	O	
DRM-CLI-CMN-018	RI Certificate Processing and Certificate Chain Validation	5.4.2.4,5.4.3.2,5.4.4.2,	M	

		6.2		
DRM-CLI-CMN-019	RI Signature Validation	5.4.2.4,5.4.3.2,5.4.4.2	M	
DRM-CLI-CMN-020	OCSP Response Validation	5.4.2.4,5.4.3.2,5.4.4.2,6.3	M	
DRM-CLI-CMN-021	IMSI Binding	15.1	O	
DRM-CLI-CMN-022	WIM Binding	15.2	O	
DRM-CLI-CMN-023	Transaction Tracking	12.2	O	
DRM-CLI-CMN-024	User Consent for ROAP Triggers and associated processing	5.2.1	M	
DRM-CLI-CMN-025	User Consent for Silent and Preview Headers	5.2.2	M	
DRM-CLI-CMN-026	RI Certificate Caching	5.4.2.1.1	O	
DRM-CLI-CMN-027	RI Certificate Verification data storage in the RI Context	5.4.2.4.1	O	
DRM-CLI-CMN-028	Replay Protection for Stateful Rights Objects	9.4,5.3.8	M	
DRM-CLI-CMN-029	Maintaining state information for Stateful Rights Objects	9.4.1	M	
DRM-CLI-CMN-030	Domain Name Whitelists	5.4.2.4.1	M	
DRM-CLI-CMN-031	Multiple Domain Contexts	8.2	O	
DRM-CLI-CMN-032	Domain Context	5.4.4.2.1,8.2	O	
DRM-CLI-CMN-033	Domain Context Expiry processing	5.4.4.2.1	O	
DRM-CLI-CMN-034	Installing Domain ROs	8.6.2.1, 8.6,5.4.4.2	M	
DRM-CLI-CMN-035	Multiple RI Contexts	5.4.2.4.1	M	
DRM-CLI-CMN-036	RI Context	5.4.2.4.1	M	
DRM-CLI-CMN-037	Use of riID as identifiers for RI Contexts stored in the Device	5.4.2.4.1,5.3.7,5.2.1	M	
DRM-CLI-CMN-038	RI Context Expiry processing	5.4.2.4.1	M	
DRM-CLI-CMN-039	DCF Hash verification; usage in ROAP	5.4.3.1.1	O	
DRM-CLI-CMN-040	Domain RO Processing	8.6	O	
DRM-CLI-CMN-041	MIME Types for ROAP PDU, Trigger, ProtectedRO, and Rights Objects	5.3.7,10.1	M	

DRM-CLI-CMN-042	Exporting to other DRMs and Protected Links	13	O	
DRM-CLI-CMN-043	Super Distribution of the DCF	12	O	
DRM-CLI-CMN-044	Super Distribution of the ContentURL	12	O	
DRM-CLI-CMN-045	Subscription Rights Object	9.5	O	
DRM-CLI-CMN-046	Off-device storage of content and Rights Objects	9.6	O	
DRM-CLI-CMN-047	Capability signaling to Content Issuers and Rights Issuers	10	M	
DRM-CLI-CMN-048	Processing Content Objects, Rights Objects and ROAP Triggers received via WAP PUSH	11.3	M	
DRM-CLI-CMN-049	DCF Integrity protection after the DCFs are downloaded to the Device	12.3	M	
DRM-CLI-CMN-050	Backwards Compatibility to OMA DRM v1	Appendix C	M	
DRM-CLI-CD-051	DRM Time	6.3,5.4	O	
DRM-CLI-CD-052	DRM Time Synchronization	6.3,5.4	O	
DRM-CLI-CD-053	Connectivity for Unconnected Devices via ROAP over OBEX	11.5	O	
DRM-CLI-CD-054	Connectivity to Rights Issuers over appropriate transport connections	14	O	
DRM-CLI-CD-055	2-pass ROAP-ROAcquisition protocol	5.4.3	O	
DRM-CLI-CD-056	1-pass ROAP-ROAcquisition protocol	5.4.3.2.1	O	
DRM-CLI-CD-057	2-pass ROAP-JoinDomain protocol	5.4.4.1	O	
DRM-CLI-CD-058	2-pass ROAP-LeaveDomain protocol	5.4.4.3	O	
DRM-CLI-CD-059	HTTP Transport Mapping	11.1	O	
DRM-CLI-CD-060	Capability Signalling	10	O	
DRM-CLI-CD-061	Silent and Preview header processing in DCFs	5.2.2	O	
DRM-CLI-UD-062	DRM Time	6.3,5.4	O	
DRM-CLI-UD-063	DRM Time Synchronization	6.3,5.4	O	
DRM-CLI-UD-064	Utilize the connectivity provided by the Connected Device to conduct ROAP protocols	14	O	
DRM-CLI-UD-065	ROAP-OBEX Server	14,11.5	O	

DRM-CLI-UD-066	2-pass ROAP JoinDomain protocol	5.4.4.1	O	
DRM-CLI-UD-067	2-pass ROAP LeaveDomain protocol	5.4.4.3	O	
DRM-CLI-UD-068	HTTP transport mapping	11.1	O	
DRM-CLI-UD-069	Capability Signalling	10	O	

H.2 Server Conformance Requirements

Item	Function	Reference	Status	Requirements
DRM-SERVER-001	ROAP schema parsing and message processing	5.3	M	
DRM-SERVER-002	Comparison of ROAP values	5.3.2	M	
DRM-SERVER-003	Nonce values in ROAP messages	5.3.9	M	
DRM-SERVER-004	Indicating the status parameter in the runs of the ROAP protocols as defined	5.3.5,5.4.2	M	
DRM-SERVER-005	XML Canonicalization	5.3.8,5.4	M	
DRM-SERVER-006	RI Certificates	F.2	M	
DRM-SERVER-007	DRM Agent Certificate processing and Certificate Chain Validation	5.4.2.3.1	M	
DRM-SERVER-008	Unique riID in ROAP Protocols.	5.4	M	
DRM-SERVER-009	Support for OCSP Requests including nonce extensions.	5.4.2.4.1	M	
DRM-SERVER-010	Providing the most recept OCSP Response to Devices in ROAP protocol runs	5.4.2.4.1	O	
DRM-SERVER-011	ROAP Trigger support and initiating the ROAP protocol using ROAP Triggers	5.2.1	M	
DRM-SERVER-012	domainID element in ROAP Triggers	5.2.1	O	
DRM-SERVER-013	More than one roID elements in a roAcquisition trigger	5.2.1	O	
DRM-SERVER-014	Use of MAC in leaveDomain ROAP Trigger	5.2.1	M	
DRM-SERVER-015	4-pass ROAP-Registration Protocol	5.4.2	M	
DRM-SERVER-016	2-pass ROAP-ROAcquisition Protocol	5.4.3	M	
DRM-SERVER-017	1-pass ROAP-ROResponse Protocol	5.4.3.2.1	M	
DRM-SERVER-018	2-pass ROAP-JoinDomain Protocol	5.4.4.1	M	
DRM-SERVER-019	2-pass ROAP-LeaveDomain Protocol	5.4.4.3	M	
DRM-SERVER-020	Hash Chain support for Domain Key	8.7.1	O	

	Generation			
DRM-SERVER-021	ProtectedRO support	5.3.7	M	
DRM-SERVER-022	Signature on Domain RO	5.4.3.2.1,5.3.8	M	
DRM-SERVER-023	Signature on Device RO	5.3.8,5.4.3.2.1	O	
DRM-SERVER-024	domainRO and riURL attributes in ProtectedRO for Domain ROs	5.3.8	M	
DRM-SERVER-025	Hash Algorithms: SHA-1 and associated URI	5.4.2.1.1	M	
DRM-SERVER-026	MAC Algorithms: HMAC-SHA-1 and associated URI	5.4.2.1.1	M	
DRM-SERVER-027	Signature Algorithms: RSA-PSS-Default and associated URI	5.4.2.1.1	M	
DRM-SERVER-028	Key Transport Algorithms: RSAES-KEM-KDF2-KW-AES128 and associated URI	5.4.2.1.1	M	
DRM-SERVER-029	Key Wrap Algorithms: AES-WRAP and associated URI	5.4.2.1.1	M	
DRM-SERVER-030	Unique identifier for Rights Issuers	5.3.8	M	
DRM-SERVER-031	Subscription Rights Object	9.5	O	
DRM-SERVER-032	Issuer Responsibilities	10.3	M	
DRM-SERVER-033	Download OTA support for delivering Content , ROAP Triggers, and Rights Objects	11.2	O	
DRM-SERVER-034	Billing trigger utilizing Download OTA mechanisms	11.2	O	
DRM-SERVER-035	Use of WAP PUSH to deliver Content, ROAP Triggers, and Rights Objects	11.3	M	
DRM-SERVER-036	Transaction Tracking	12.2	M	

Appendix I. Examples (Informative)

I.1 HTTP Transport Mapping Examples

I.1.1 Separate Delivery of DCF and Rights Object

This first example is a basic use case assuming only minimal integration between RI and CI (exchange of CEK and content ID prior to content and Rights Object delivery).

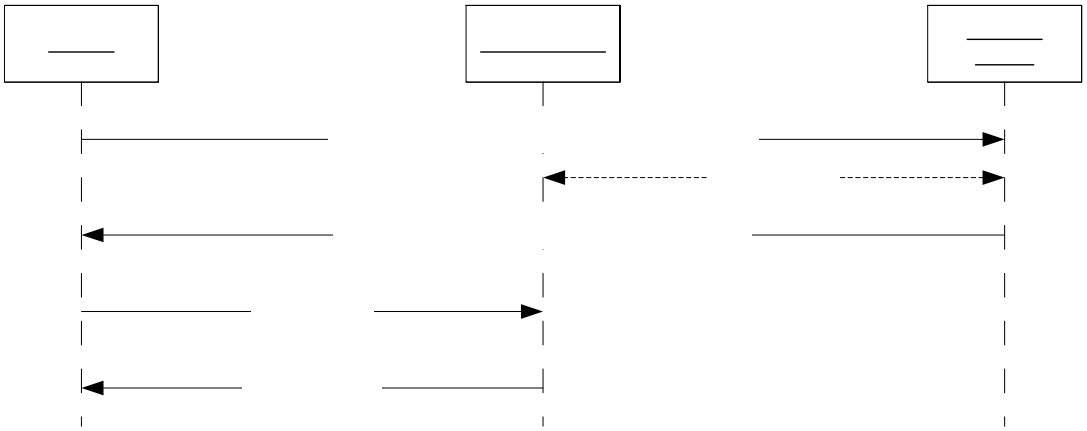

Figure 19: Separate Delivery of DCF and RO

- A user browses through a content portal, selects content and so on.
- A Rights Object is generated for the purchase transaction using some backend interaction between RI and CI.
- The CI returns an HTTP Response containing a multipart/mixed. One entity is the content DCF, the other entity is the ROAP Trigger.

```
HTTP 1.1 200 OK
 Server: CoolServer/1.3.12
 Content-Type: multipart/mixed; boundary="XX---XX"

--XX---XX
 Content-Length: 1232
 Content-Type: application/vnd.oma.drm.dcf
... [DCF] ...
--XX---XX
 Content-Length: 986
 Content-Type: application/vnd.oma.drm.roap-trigger+xml
... [ROAP Trigger XML document] ...
--XX---XX--
```

- The ROAP Trigger is used by the DRM Agent on the Device to initiate a ROAP session to download a Rights Object. The DRM Agent issues an HTTP POST to the URL specified by the ROAP Trigger. The POST includes a ROAP-RORequest PDU in the HTTP request body.

```
POST http://www.acme.com/ro.cgi?roID=qw683hgew7d
 Host: www.acme.com
 User-Agent: CoolPhone/1.4
 Accept: application/vnd.oma.drm.roap-pdu+xml
 Accept-Charset: utf-8
 Content-Length: 125
 Content-Type: application/vnd.oma.drm.roap-pdu+xml
```

```
... [ROAP PDU] ...
```

An established RI Context is assumed in the example. If this were not the case, then the ROAP-RORequest would be preceded by a ROAP Registration transaction.

- The Rights Issuer returns an HTTP response containing a ROAP-ROResponse PDU in the HTTP response body.

```
HTTP 1.1 200 OK
 Server: CoolServer/1.3.12
 Content-Length: 986
 Content-Type: application/vnd.oma.drm.roap-pdu+xml

... [ROAP PDU] ...
```

I.1.2 Combined Delivery of DCF and Rights Object

This second example is a variation on the previous example with a closer relationship with RI and CI.

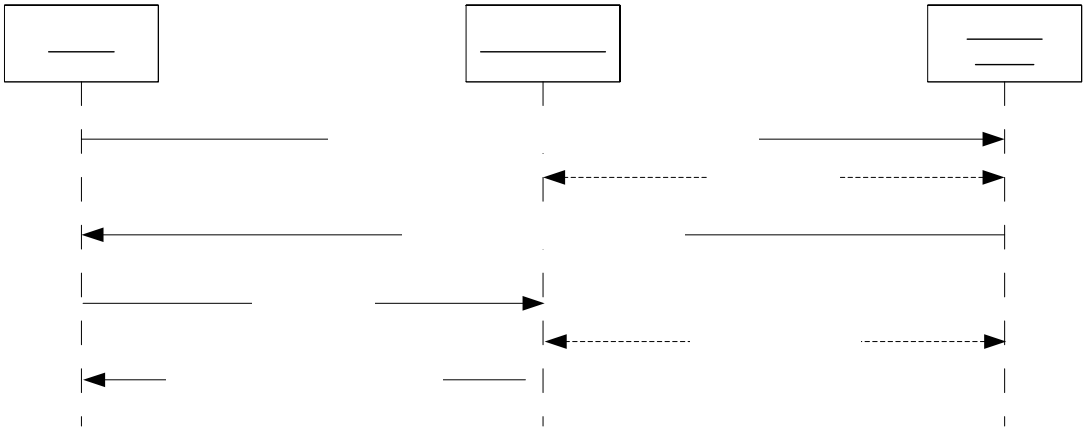

Figure 20: Combined Delivery of DCF and RO

1. A user browses through a content portal, selects content and so on.
2. A Rights Object is generated for the purchase transaction using some backend interaction between RI and CI.
3. The CI returns an HTTP Response containing a ROAP Trigger.

```
HTTP 1.1 200 OK
 Server: CoolServer/1.3.12
 Content-Length: 986
 Content-Type: application/vnd.oma.drm.roap-trigger+xml

... [ROAP Trigger] ...
```

4. The ROAP Trigger is used by the DRM Agent on the Device to initiate a ROAP session to download a Rights Object. The POST includes a ROAP-RORequest PDU in the HTTP request body.

```
POST http://www.acme.com/ro.cgi?roID=qw683hgew7d
 Host: www.acme.com
 User-Agent: CoolPhone/1.4
 Accept: application/vnd.oma.drm.roap-pdu+xml
 Accept-Charset: utf-8
 Content-Length: 125
 Content-Type: application/vnd.oma.drm.roap-pdu+xml
```

```
... [ROAP PDU] ...
```

A previously established RI Context is assumed in the example. If this were not the case, then the ROAP-RORequest would be preceded by a ROAP-Registration transaction.

5. The Rights Issuer interacts with the CI to retrieve the DCF, and returns a multipart HTTP response containing as one entity a ROAP-ROResponse PDU, and as another entity the content object (DCF).

```
HTTP 1.1 200 OK
 Server: CoolServer/1.3.12
 Content-Type: multipart/related; boundary="XX---XX"

--XX---XX
 Content-Length: 986
 Content-Type: application/vnd.oma.drm.roap-pdu+xml
... [ROAP PDU] ...
--XX---XX
 Content-Length: 1232
 Content-Type: application/vnd.oma.drm.dcf
... [DCF] ...
--XX---XX—
```

I.1.3 Silent RO Acquisition Triggered by DCF Headers

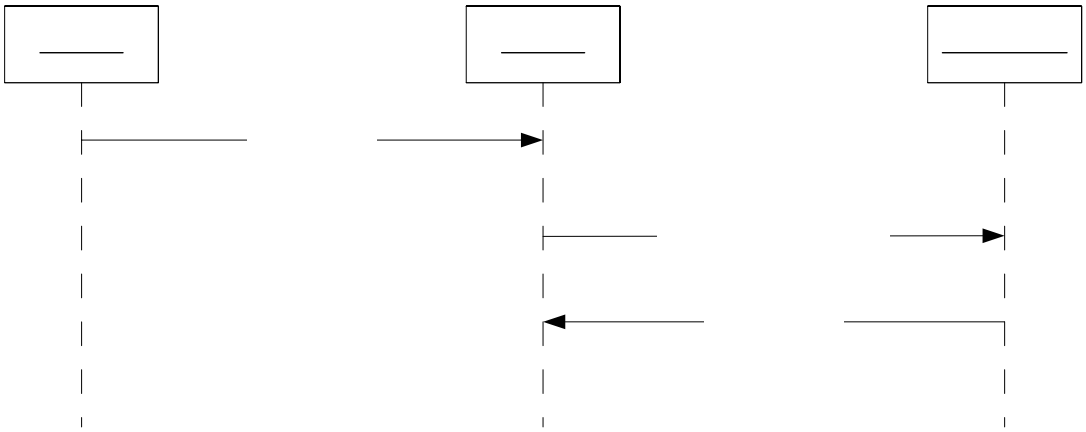

Figure 21: Silent RO Acquisition Triggered by DCF Headers

In this case a DCF is superdistributed to a Device, and the DRM Agent uses DCF headers to initiate a ROAP transaction and download a Rights Object.

– A user receives a DCF from another Device, e.g. through MMS, peer-to-peer, removable media, or some other transfer mechanism.

– If the DCF contains either a Silent header or a Preview header, then the DRM Agent attempts to request a Rights Object automatically. If the DRM Agent has an existing RI Context for the Rights Issuer, and has obtained user consent to request Rights Objects from the Rights Issuer, then the DRM Agent may proceed silently without further user interaction.

  The DRM Agent sends an HTTP Post to the URL specified by the Silent or Preview headers. The POST includes a ROAP-RORequest PDU in the HTTP request body.

```
POST http://www.acme.com/ro.cgi?roID=qw683hgew7d
 Host: www.acme.com
 User-Agent: CoolPhone/1.4
 Accept: application/vnd.oma.drm.roap-pdu+xml
 Accept-Charset: utf-8
 Content-Length: 125
 Content-Type: application/vnd.oma.drm.roap-pdu+xml

... [ROAP PDU] ...
```

– The Rights Issuer returns an HTTP response containing a ROAP-ROResponse PDU in the HTTP response body.

```
HTTP 1.1 200 OK
 Server: CoolServer/1.3.12
 Content-Length: 986
 Content-Type: application/vnd.oma.drm.roap-pdu+xml

... [ROAP PDU] ...
```

I.2 Download OTA Examples

I.2.1 Separate Delivery of DRM Content and Rights Object

A Service Provider may use OMA Download OTA to deliver both the DRM Content and the Rights Object in separate transactions. The following figure shows the interaction between the logical system components residing in the Device and logical server components hosted by the Service Provider during the separate delivery of DRM Content and Rights Objects. Note that in the download transaction for retrieving the Rights Objects, the ROAP Trigger is co-delivered with the Download Descriptor using OMA Download OTA co-delivery method.

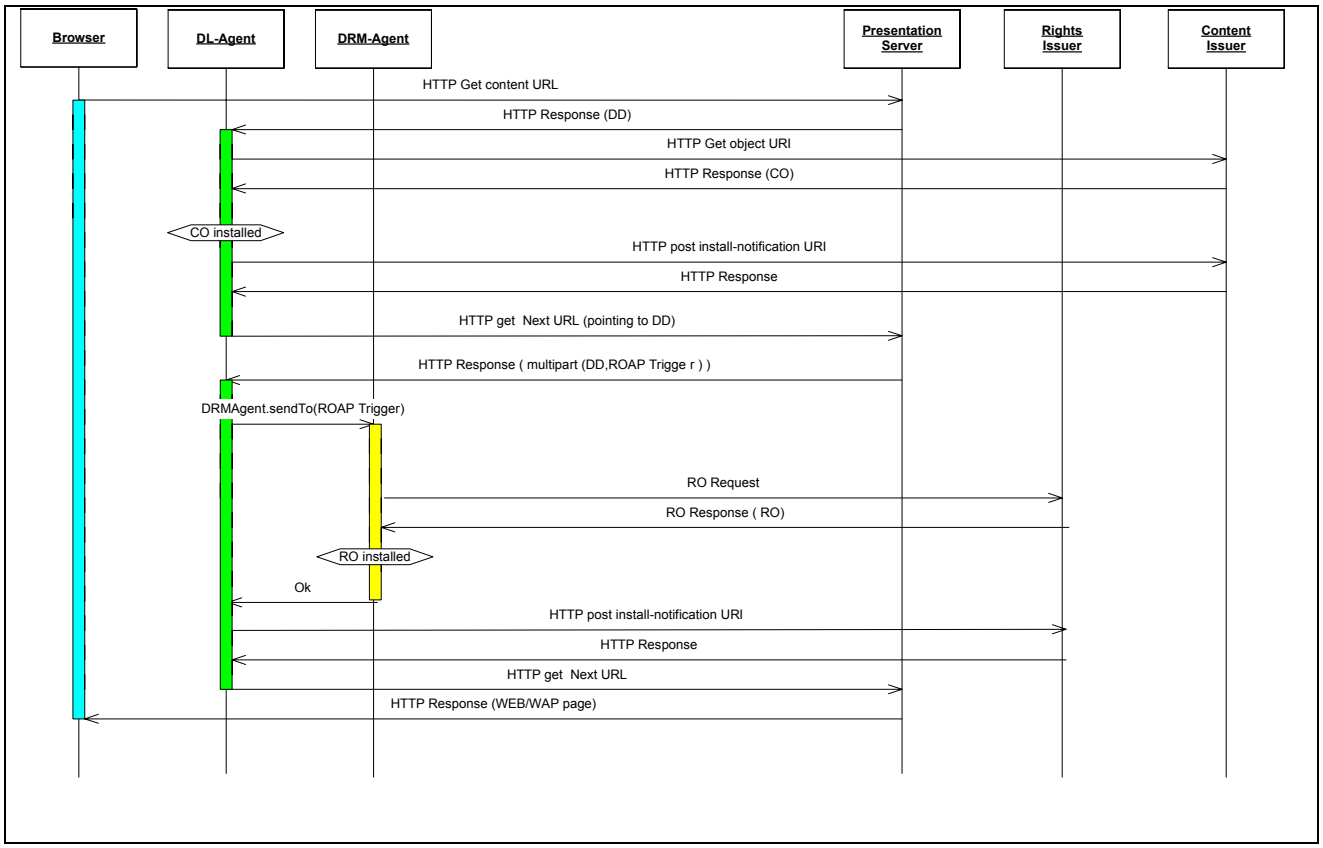

Figure 22: Using Download OTA to deliver DRM Content and Rights Object

1. A user browses through a content portal, selects content and so on. When it is time to deliver content, the server returns an HTTP Response with a Download Descriptor (DD). The DD might, for example, point to a DCF file containing a JPEG image.

```
HTTP 1.1 200 OK
 Server: CoolServer/1.3.12
 Content-Length: 1232
 Content-Type: application/vnd.oma.dd+xml; charset=utf-8

<media xmlns="http://www.openmobilealliance.org/xmlns/dd">
  <type>application/vnd.oma.drm.dcf</type>
  <type>image/jpeg</type>
  <objectURI>http:/download.example.com/image.dcf</objectURI>
  <size>100</size>
  <installNotifyURI>
    http://download.example.com/notify?tid=2h3jh3g4
  </installNotifyURI>
  <nextURL>
    http://ri.example.com/ro?tid=2h3jh3g4
  </nextURL>
</media>
```

2. The Download Agent requests the Content using the *objectURI*.

```
GET /image.dcf HTTP/1.1
Host: download.example.com
Accept: image/gif, image/jpg, application/vnd.oma.drm.dcf
```

3. The DCF is returned to the Download Agent.

```
HTTP/1.1 200 OK
Server: CoolServer/1.3.12
Content-Length: 1234
Content-Type: application/vnd.oma.drm.dcf

… DCF containing JPEG picture…
```

4. The Download Agent installs the Content and posts an installation notification.

```
POST /notify?tid=2h3jh3g4 HTTP/1.1
 Host: download.example.com
 Content-Length: 13
900 Success
```

5. In this example the DD for the DCF specifies a *nextURL*. This means that when the Download Agent is done downloading and installing the DCF, it will automatically issue an HTTP GET to the URL specified by the *nextURL* DD parameter. This can be used to seamlessly redirect the Device from the CI to the RI.

```
GET /ro?tid=2h3jh3g4 HTTP/1.1
Host: ri.example.com
```

6. The RI returns a DD and the ROAP Trigger.

```
HTTP 1.1 200 OK
 Server: CoolServer/1.3.12
 Content-Type: multipart/related; boundary="XX---XX"
 --XX---XX
 Content-Length: 1232
 Content-Type: application/vnd.oma.dd+xml; charset=utf-8

<media xmlns="http://www.openmobilealliance.org/xmlns/dd">
  <type>application/vnd.oma.drm.roap-pdu+xml</type>
  <type>application/vnd.oma.drm.ro+xml</type>
  <objectURI>cid:w087w78087sdf80@ri.example.com</objectURI>
  <size>1232</size>
  <installNotifyURI>
    http://ri.example.com/notify?tid=2h3jh3g4
  </installNotifyURI>
  <nextURL>
    http://provider.example.com/trans_complete.html
  </nextURL>
</media>
--XX---XX
Content-Length: 986
Content-ID: <w087w78087sdf80@ri.example.com>
Content-Type: application/vnd.oma.drm.roap-trigger+xml
<roapTrigger xmlns="urn:oma:bac:dldrm:roap-trigger-20040120">
  <roAcquisition>
      <riID>
       <keyIdentifier xsi:type="roap:X509SPKIHash">
         <hash>aXENc+Um/9/NvmYKiHDLaErK0fk=</hash>
       </keyIdentifier>
     </riID>
      <roapURL>http://ri.example.com/ro.cgi?tid=qw683hgew7d</roapURL>
     <roID>239087dsf78</roID>
  </roAcquisition>
</roapTrigger>
--XX---XX
```

7. The ROAP Trigger is used by the DRM Agent on the Device to initiate a ROAP session to download a Rights Object. The DRM Agent issues an HTTP POST to the ROAP Trigger URL. The POST includes a ROAP-RORequest PDU in the HTTP request body.

```
POST /ro.cgi?tid=qw683hgew7d HTTP/1.1
 Host: ri.example.com
 User-Agent: CoolPhone/1.4
 Accept: application/vnd.oma.drm.roap-pdu+xml,
application/vnd.oma.drm.ro+xml
 Content-Length: 125
 Content-Type: application/vnd.oma.drm.roap-pdu+xml

... [ROAP PDU] ...
```

8. The RI returns the ROAP-ROResponse PDU.

```
HTTP 1.1 200 OK
 Server: CoolServer/1.3.12
 Content-Length: 986
 Content-Type: application/vnd.oma.drm.roap-pdu+xml

... [ROAP PDU] ...
```

9. The DRM Agent processes the ROAP PDU and sends the installation status (success or failure) to the Download Agent. The Download Agent sends the installation status to the RI using the *installNotifyURI*.

```
POST /notify?tid=2h3jh3g4 HTTP/1.1
 Host: ri.example.com
 Content-Length: 13
900 Success
```

10. The Download Agent immediately navigates to the *nextURL*.

```
GET /trans_complete.html HTTP/1.1
Host: provider.example.com
```

I.2.2 Combined Delivery of Content DCF and Rights Object

This example is an extension to the previous example, assuming a closer relationship between the RI and CI allowing the content DCF and the RO to be delivered together in a single OMA Download OTA transaction. Also in this example, the ROAP Trigger is co-delivered with the Download Descriptor using theOMA Download OTA co-delivery method.

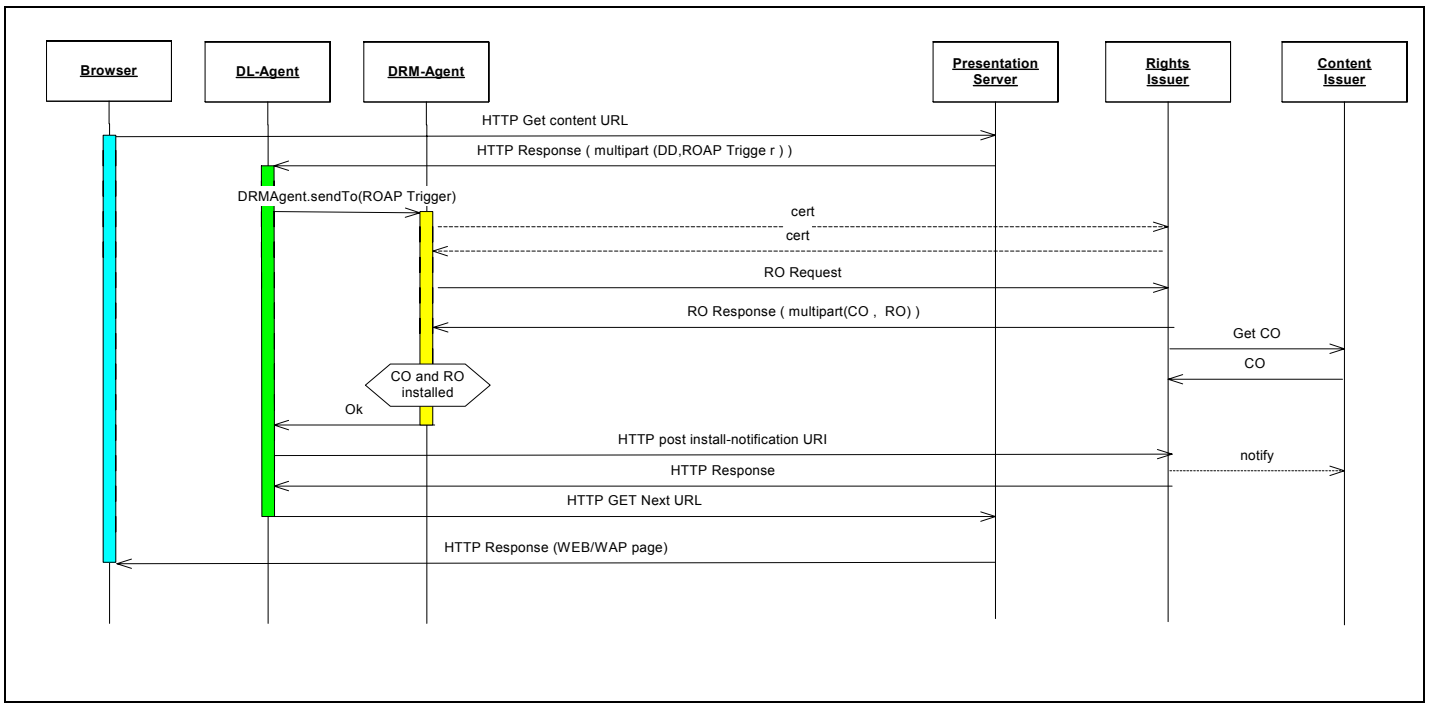

Figure 23: Combined Delivery of DRM Content and Rights Object

1. A user browses through a content portal, selects content and so on. When it is time to deliver content, the server returns a DD and the ROAP Trigger to initiate delivery of the combined Rights Object and DRM Content.

```
HTTP 1.1 200 OK
 Server: CoolServer/1.3.12
Content-Type: multipart/related; boundary="XX---XX"
 --XX---XX
 Content-Length: 1232
 Content-Type: application/vnd.oma.dd+xml; charset=utf-8

<media xmlns="http://www.openmobilealliance.org/xmlns/dd">
  <type>application/vnd.oma.drm.roap-pdu+xml</type>
  <type>application/vnd.oma.drm.ro+xml</type>
  <type>application/vnd.oma.drm.dcf</type>
  <objectURI>cid:sd8963234l@ri.example.com</objectURI>
  <size>2118</size>
  <installNotifyURI>
    http://ri.example.com/notify?tid=2h3jh3g4
  </installNotifyURI>
  <nextURL>
    http://provider.example.com/trans_complete.html
  </nextURL>
</media>
--XX---XX
Content-Length: 986
Content-ID: <sd8963234l@ri.example.com>
Content-Type: application/vnd.oma.drm.roap-trigger+xml
<roapTrigger xmlns="http://www.openmobilealliance.org/xmlns/roap-
trigger">
      <riID>
       <keyIdentifier xsi:type="roap:X509SPKIHash">
         <hash>aXENc+Um/9/NvmYKiHDLaErK0fk=</hash>
       </keyIdentifier>
     </riID>
      <roURL>2498sdfcvxs@ri.example.com</roURL>
```

```
      <roapURL>http://ri.example.com/ro.cgi?tid=g97sd976s90</roapURL>
      <protocol>Acquisition</protocol>
      <signature>...signature_data...</signature>
</roapTrigger>
--XX---XX
```

2. The ROAP Trigger is used by the DRM Agent on the Device to initiate a ROAP session to download the combined Rights Object and DRM Content..The DRM Agent issues an HTTP POST to the URL specified by the ROAP Trigger. The POST includes a ROAP-RORequest PDU in the HTTP request body.

```
POST /ro.cgi?tid=g97sd976s90 HTTP/1.1
 Host: ri.example.com
 User-Agent: CoolPhone/1.4
 Accept: application/vnd.oma.drm.roap-pdu+xml,
application/vnd.oma.drm.ro+xml, application/vnd.oma.drm.dcf
 Content-Length: 125
 Content-Type: application/vnd.oma.drm.roap-pdu+xml

... [ROAP PDU] ...
```

3. The RI returns a multipart containing a ROAP-ROResponse PDU and the DRM Content.

```
HTTP 1.1 200 OK
 Server: CoolServer/1.3.12
 Content-Type: multipart/related; boundary="XX---XX"

--XX---XX
 Content-Length: 986
 Content-Type: application/vnd.oma.drm.roap-pdu+xml
... [ROAP PDU] ...
--XX---XX
 Content-Length: 1232
 Content-Type: application/vnd.oma.drm.dcf
... [DCF] ...
--XX---XX--
```

4. The DRM Agent installs the Rights Object and DRM Content. The DRM Agent notifies the Download Agent of installation success. The Download Agent posts the installation notification.

```
POST /notify?tid=2h3jh3g4 HTTP/1.1
 Host: ri.example.com
 Content-Length: 13

900 Success
```

I.3 MMS Examples

I.3.1 MMS delivery of DCF within a SMIL presentation

The example MMS message shown below contains a presentation description in the form of a SMIL document. From within this document the second body part of the message is referenced by a Content-ID, which is associated with the referenced part in the multipart structure in the form of a header field (containing the ID "same-reference-as-in-SMIL-doc " in this example). This is explicitly different from the Content-ID included in the DCF ("same-reference-as-used-in-associated-ROs ") which serves as a reference for the Rights Object(s) associated with the Media Object. As an alternative to the Content-ID in the multipart structure a Content-Location may be used according to [MMSENC]. For a better understanding, the example below is illustrated in textual format, although the MMS PDUs are binary encoded on the interface between the MMS Proxy-Relay and the MMS Client according to [MMSENC].

```
From:customer@mmsprovider.com
To:anothercustomer@anothermmsprovider.com
Subject:MMS message with DRM content
X-MMS-Version:1.2
...[More MMS headers]
Content-Type:multipart/related;boundary=firststring;start=secondstring

--firststring
Content-ID:secondstring
Content-Type:application/smil
...[SMIL doc]
--firststring
Content-ID:same-reference-as-in-SMIL-doc
Content-Type: application/vnd.oma.drm.dcf
...[DCF containing Content-ID:same-reference-as-used-in-associated-ROs]
--firststring--
```

I.4 ROAP over OBEX Examples

Example messages between the Connected Device and the Unconnected Device are illustrated in this section utilizing ROAP over OBEX transport mapping.

I.4.1 ROAP Trigger

This message is sent from the Connected Device to the Unconnected Device after:

1. The Connected Device has received the trigger from the RI;
2. The Connected Device has determined that the ROAP Trigger is not for itself; and
3. The Connected Device has established a directed OBEX connection to the Unconnected Device's OBEX server.

Bytes	Meaning
0x82	Opcode PUT, single packet request, final bit set
0x0301	Packet length (a total of 769 bytes in this case)
0xCB	Connection Id HI
0x00000001	ConnectionId = 1
0x42	Type HI
0x0027	Total length of Type header (including HI and length fields)
"application/vnd.oma.roap-trigger+xml"	Type of object, null terminated ASCII text
0x49	End-of-Body HI
0x02D2	Length of body (trigger) is 719 bytes (= whole object)(+ 3 bytes header information)
0x….	The ROAP-JoinDomain trigger goes here…

I.4.2 ROAP-OBEX Server Response

This is the response message from the Unconnected Device, sent by that Device's OBEX server.

Bytes	Meaning
0xA0	Opcode SUCCESS, Final bit set
0x016B	Length of response packet (363 bytes)
0xCB	Connection Id HI
0x00000001	ConnectionId = 1
0x42	Type HI
0x001F	Total length of Type header (28 bytes + 3 bytes header information)
"application/vnd.oma.roap+xml"	Type of object, null terminated ASCII
0x49	End-of-Body HI
0x0144	Body header length (321 bytes + 3 bytes header information)
0x….	The triggered ROAP request goes here

Appendix J. Change History (Informative)

J.1 Approved Version History

Reference	Date	Description
n/a	n/a	No prior version –or- No previous version within OMA

J.2 Document History

This section is available in pre-approved versions – it should be removed in the actual approved versions. DELETE THIS COMMENT

Document Reference	Description
OMA-DRM-DRM-V2_0-20040420-D	Current; last set of editorial changes; changes accepted in the call on 4/20.
OMA-DRM-DRM-V2_0-20040416-D	Current; added SCR Tables; Folded in feedback from WG call of 4/15 and suggested changes since 4/10 edition of the spec.
OMA-DRM-DRM-V2_0-20040410-D	Submitted to the WG for review
OMA-DRM-DRM-V2_0-20040320-D	Submitted to the WG for review.
OMA-DRM-DRM-V2_0-20040228-D	Submitted to the WG for review.
OMA-DRM-DRM-V2_0-20040127-D	Version discussed in Beverly Hills meeting
OMA-DRM-DRM-V2_0-20040108-D	version distributed to the reflector with changes to most of the chapters and a major update to the ROAP section.
OMA-DRM-DRM-V2_0-20031121-D	post-London OMA version
OMA-DRM-DRM-V2_0-20030902-D	version submitted to Berlin TP
OMA-DRM-DRM-V2_0-20030810-D	Version submitted to both DLDRM and Security WGs for review before Berlin.
OMA-DRM-DRM-V2_0-20030715-D	Version submitted for discussion in Paris.