Open Geospatial Consortium Inc.

Date: 2006-12-29

Reference number of this OGC® document: OGC 06-004r4

Version: 1.0.0

Category: Abstract Specification

Editor: Graham Vowles

The OpenGIS® Abstract Specification
Topic 18: Geospatial Digital Rights Management Reference Model (GeoDRM RM)

Modèle de la référence pour la gestion des droits pour l'usage dans l'information géographique

Warning:
This document is an OGC Standard. However, it is subject to change without notice.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type:	**Abstract Specification**
Document subtype:	**Reference Model**
Document stage:	**Version 1.0.0**
Document language:	**English**

Please read this Clarification Note

All examples in this document are informative. Such informative examples should not be considered as endorsement of a given implementation approach. This document is defines a Reference Model for GeoDRM that is implementation neutral.

Copyright © 2006 Open Geospatial Consortium, Inc. All Rights Reserved.

Contents

Figures

Tables

i. Preface

Suggested additions, changes, and comments on this draft are welcome and encouraged. Such suggestions may be submitted by email message or by making suggested changes in an edited copy of this document.

The changes made in this document version, relative to the previous version, are tracked by Microsoft® Word, and can be viewed if desired. If you choose to submit suggested changes by editing this document, please first accept all the current changes, and then make your suggested changes with change tracking on.

ii. Document terms and definitions

This document uses the specification terms defined in Subclause 5.3 of [OGC 05-008], which is based on the **ISO/IEC Directives, Part 2: Rules for the structure and drafting of International Standards**. In particular, the word "shall" (not "must") is the verb form used to indicate a requirement to be strictly followed to conform to this specification.

iii. Document contributors contact points.

All questions regarding this document should be directed to the editor or the contributors:

Name	Organization
Graham Vowles	Ordnance Survey®
John R. Herring	Oracle® Corporation
Cecil Goodwin	Tele Atlas N.V.
Mark V. Scardina	Oracle Corporation
Andreas Matheus	University of the German Armed Forces, Munich
Cristian Opincaru	University of the German Armed Forces, Munich
Wayne Debeugny	Technical Editor, Ordnance Survey

iv. Revision history

Date	Release	Editor	Primary clauses modified	Description

Date	Release	Editor	Primary clauses modified	Description
1 September 2005	0.0.1	Graham Vowles		Initial glossary, roles and scenario definition.
17 October 2005	0.0.2	John R. Herring	Preface, Forward, 1 Scope 2 Conformance 3 References 4 Definitions (first few)	Filling in gaps in boilerplate for specifics of GeoDRM, subject to WG (working group) review. Some format changes were made in 3 and 4 (first few definitions) to get nearer ISO rules.
26 October 2005	0.0.3	Cecil Goodwin	4 Definitions	Refined definitions
28 October 2005	0.0.4	John R. Herring	3, 4, 5	Filling in gaps in boilerplate and formats for specifics of GeoDRM, subject to WG review. Some format changes were made in 3 and 4 to get nearer ISO rules. Exteriorizing external definition (changing a quote to a reference).
22 November 2005	0.0.5	Mark V. Scardina	4. Definitions, comments	
29 November 2005	0.0.6	John R. Herring	Reorganize and clean-up	
12 December 2005	0.0.7	John R. Herring	Reorganize and new rights section	Rights model based on 6 Dec. 05 telecom, and up for discussion for 13 Dec. 05
20 December 2005	0.0.8	John R. Herring	Clause 1, 3, 4 Clause 6 Clause 9	Answered Mark's comment and added more information model detail. More work on definitions.
22 December 2005	0.0.9	John R. Herring	Clause 6.4, 9.4.2	Trust and Process-derived rights proposal
27 December 2005	0.0.10	John R. Herring	9.1	Deleted old comments, clean up of some formatting issues, Expanded 9.1
5 January 2006	0.0.11	John R. Herring	4, Annex B	Fixed some definitions sources, fixed use of principal. Added Model annex.
11 January 2006	0.0.12	Andreas Matheus, Cristian Opincaru	Introduction, 3, 9	Comments, Minor changes
20 January 2006	0.0.13	Graham Vowles	Enterprise Viewpoint	Add edits from Munich workshop
25 January 2006	0.0.14	John R. Herring	Various	Add edits from Munich workshop
26 January 2006	0.0.15	Andreas Matheus	Motivation, 6.1	Add Motivation and GeoDRM Roadmap
26 January 2006	0.0.16	John R. Herring	9, Annex B and some other minor edits	Information viewpoint text added and general editorial clean-up. Annex B still and the Information Model Clause 9 have been harmonized. Annex B is not informative.
31 January 2006	0.0.17	Graham Vowles	1-6 Editorial, 7 and 8 Updated	Added a description of how the GeoDRM RM relates to other documents. Editorial changes and update of Enterprise Viewpoint. Added Joe Cardinale edits to Section 8 Computational Viewpoint.
3 February 2006	0.0.18	Graham Vowles	Annex C	Added scenarios from GeoDRM Game
27 February. 06	06-004r2	Wayne Debeugny	All over	Grammar and style corrections.

Copyright © 2006 Open Geospatial Consortium, Inc. All Rights Reserved.

v. Changes to the OGC Abstract Specification

The OGC Abstract Specification requires changes to accommodate the technical contents of this document. This document becomes a new volume in the Abstract Specification.

No changes to existing abstract specification volumes are foreseen.

vi. Future work

Improvements in this document and to extensions of this document are desirable to:

1. Establish rights expression language (REL) extensions for geospatial resource.
2. Establish a resource identification and description metadata language to extend ISO 19115, and provide control information for GeoDRM-enabled systems.
3. Establish a process identification and compliance language to provide control information for GeoDRM-enabled systems.
4. Establish a variety of implementation models that balance Trust, Protection, and Remediation as required for different community-specific scenarios.

Foreword

This document is a reference model for digital rights management (DRM) functionality for geospatial resources (GeoDRM). As such, it is connected to the general DRM market in that geospatial resources must be treated as nearly as possible like other digital resources, such as music, text, or services. It is not the intention here to reinvent a market that already exists and is thriving, but to make sure that a larger market has access to geospatial resources through a mechanism that it understands and that is similar to the ones already in use.

This document does not replace any previous OGC specification, but it is dependent upon them. Each resource and service OGC specification that exists or will exist becomes a resource description in this document, and hopefully shall be subject to the same sorts of protection that is afforded to other digital resources.

This document includes four annexes; Annexe A is normative, and Annexes B, C and D are informative.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. The OGC shall not be held responsible for identifying any or all such patent rights.

Copyright © 2006 Open Geospatial Consortium, Inc. All Rights Reserved.

Introduction

To create a marketplace, individuals who own something of value (here a resource) must have some level of assurance that they will be able to obtain fair value for its use or purchase. In a digital world, due to the nature of digital resources and commerce, most digital entities are not sold in the usual sense. When a user acquires an application, he actually acquires the right to use a copy of the application. Possession does not equate with ownership, and a system of software and resource licensing has grown up in the digital world that ensures the following types of things:

- The user may legitimately act upon a resource if he has a corresponding licence for that act.

- The owner should maintain the resource, fixing error ("bug-fix") and assuring a guaranteed level of functionality.

- Optionally, the user may be asked to pay the owner of the resource based upon agreed criteria, whether that is a one-time fee, a per-machine fee, a usage fee or some other mechanism stated in the legal contract or licence between user and owner.

- The user agrees to protect the owner's rights based on the agreement. This usually means he cannot backward engineer code or resource, nor redistribute the resource without proper permission.

- The owner agrees to maintain the resource and allow a reasonable access to the users for any fixes that may be required. Again, the extent or degree of maintenance is stated in the user agreement.

- To create and support a large-scale, open market in geospatial resources, this type of protection is needed to assure that a "fair value for work (investment)" ethic can be guaranteed so that suppliers can be sure of fair return on individual sales, and users can be sure of fair value for purchases of uses of resources.

This document describes how this is to be done.

Motivation

For the licensing of digital content, different standards already exist. However, the existing standards (e.g. MPEG-REL or ISO-REL, ISO 21000) describe the licensing of digital media content and cannot be used for licensing of geographic information unless they are extended. Therefore, this DRM Rights Model for geographic information is necessary and its relevance can be explained by examining its various aspects.

First, the Rights Model for digital geographic content must accommodate licensing for different types of business relationships and participants with different roles, as it is described in chapter 8.1, Overview: Roles and Responsibilities. Here, direct licensing as well as sub-licensing can take place for business-to-business (B2B) or business-to-consumer (B2C) relationships. In particular for sub-licensing, it must be possible to grant licences for issuing licences, which is not covered by existing ISO-REL Rights Models.

Second, licensing in the GeoDRM domain must support the licensing of digital content, based on different infrastructures: licensing can take place for a static product as it can be delivered on CD-ROM. However, even more important is the aspect that licensing can also take place on geographic information as it can be dynamically "created" by using OpenGIS Web Services. Here, the digital geographic content (called resource in this specification) that is to be licensed is the result of a service invocation using particular parameters. For example, maps can be created by using a Web Map Service and feature collections can be created by executing a Web Feature Service. The GeoDRM Rights Model therefore supports the capability to describe rights for executing a service using certain constraints on parameters (parameter values must be in a certain range). This capability, as described in 9.5.3.3.9, Parameter Range conditions, is also not covered by other Rights Models such as in the ISO-21000 [11] or ODRL [17] and OMA DRM [18].

Third, licensing of geographic information requires support to declare and enforce rights, as they are based on the geometry of the digital content. This capability is described in this standard by defining geo-specific conditions on a right, as defined in section 9.5.3.3.6, Spatial Temporal Conditions.

Geospatial Digital Rights Management Reference Model (GeoDRM RM)

Modèle de la référence pour la gestion des droits pour l'usage dans l'information géographique

1 Scope

This standard defines:

- A conceptual model for digital rights management of geospatial resources, providing a framework and reference for more detailed specification in this area.
- A metadata model for the expression of rights that associate users to the acts that they can perform against a particular geospatial resource, and associated information used in the enforcement and granting of those rights, such as owner metadata, available rights and issuer of those rights.
- Requirements that are placed on rights management systems for the enforcement of those rights. A rights management system must be necessary and sufficient: it must implement only those restrictions necessary to enforce the rights defined therein, and it must be sufficient to enforce those rights.
- How this is to work conceptually in the larger DRM context to assure the ubiquity of geospatial resources in the general services market.

A resource in this context is a data file, or service for geographic information or process.

This abstract specification builds on and complements the existing OGC specifications, and defines at an abstract level a Rights Model to enable the digital rights management of standards-based geospatial resources. Future GeoDRM Implementation Specifications will be written to implement the concepts defined in this document.

Copyright © 2006 Open Geospatial Consortium, Inc. All Rights Reserved.

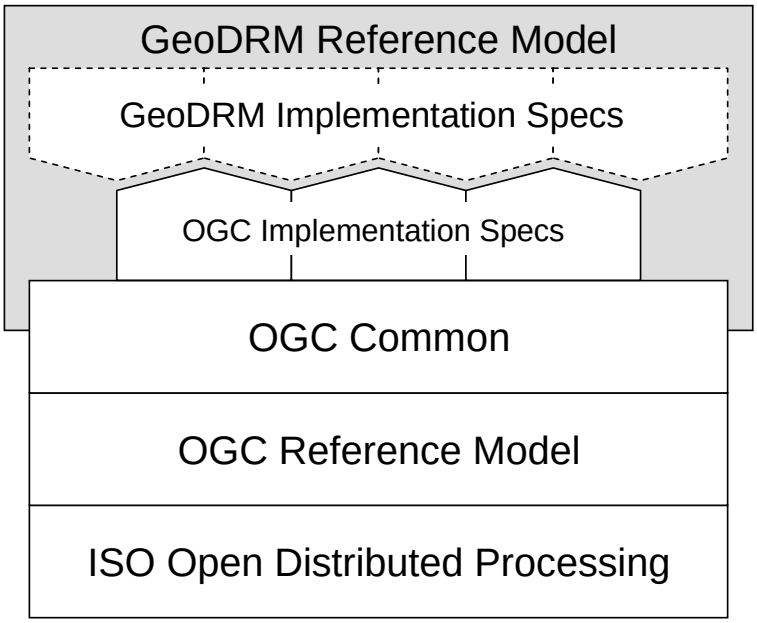

Figure 1: GeoDRM Reference Model Context

Figure 1 shows a simplified view of how this document, the Geospatial Digital Rights Management Reference Model (indicated in grey) relates to the ISO Open Distributed Processing standard, OGC Reference Model and OWS Common initiative. The purpose of this document is to define the conceptual framework and rights model for the future GeoDRM Implementation Standards, which will enable the digital rights management of geospatial resources.

This specification is not intended to delve into questions of morals, ethics, market model, or implementations any further than is necessary to express requirements against rights management functionalities and systems.

2 Conformance

Conformance with this specification shall be checked using tests specified in Annex A (normative). Conformance classes for this standard are:

- Alignment of rights expression to the abstract rights model,
- The expression for applicability of rights for geospatial resources, and
- The enforcement of rights for geospatial resources.

Resources that are augmented by GeoDRM licence metadata will be referred to as GeoDRM extended resources. Processing resources that have met the requirements to maintain GeoDRM resource and enforce the licensing procedures shall be referred to as GeoDRM enabled.

3 Normative references

The following normative documents contain provisions that, through reference in this text, constitute provisions of this document. For dated references, subsequent

amendments to, or revisions of, any of these publications do not apply. For undated references the latest edition of the normative document referred to applies.

[1] ISO 2382-6: Information processing systems – Vocabulary – Part06: Preparation and handling of resource

[2] ISO/IEC 15408: Information technology – Security techniques – Evaluation for IT security.

[3] ISO/IEC TR 15446 Information technology – Security techniques – Guide for the Production of Protection Profiles and Security Targets

[4] ISO/IEC 17799 Information technology – Code of practice for information security management

[5] ISO/IEC 27001 Information Security Management Systems – Requirements

[6] ISO 19105:2000, Geographic information – Conformance and Testing

[7] OGC 05-008, OGC Web Services Common Specification

[8] OGC Glossary at http://www.opengeospatial.org/resources/?page=glossary

[9] W3C, Web Services Glossary, W3C Working Group Note, 11 February 2004, http://www.w3.org/TR/ws-gloss/

[10] ISO/IEC 10746: Information technology – Open Distributed Processing – Reference model (RM-ODP); freely available at (in its parts) http://isotc.iso.org/livelink/livelink/fetch/2000/2489/Ittf_Home/PubliclyAvailableStandards.htm

[11] ISO/IEC 21000, Information Technology –Multimedia Framework – Information technology –Multimedia framework (MPEG-21) [1]

[12] ISO/IEC TR 21000-1, Information Technology – Multimedia Framework – Information technology – Multimedia framework (MPEG-21) – Part 1: Vision, Technologies and Strategy; freely available at http://standards.iso.org/ittf/PubliclyAvailableStandards/c040611_ISO_IEC_TR_21000-1_2004(E).zip

[13] ISO/IEC 21000-5, Information Technology – Multimedia Framework – Rights Expression Language

[14] XML Schema, Part 1: Structures, W3C Recommendation, 2 May 2001, available at http://www.w3.org/TR/xmlschema-1/

[15] **XML Schema, Part 2: Datatypes, W3C Recommendation, 2 May 2001, available at** http://www.w3.org/TR/xmlschema-2/

[16] **XML-Signature Syntax and Processing**, W3C Recommendation, 12 February 2002, available at http://www.w3.org/TR/xmldsig-core/

[1] The MPEG21 (ISO/IEC 21000) standard is a work in progress. It will eventually have at least 14 parts, only the first few are available at the moment. The intent is to eventually incorporate as much of ISO/IEC 21000 as appropriate in this GeoDRM standard in order to assure interoperability of geospatial resource DRM with that used for other multimedia information.

[17] **Open Digital Rights Language (ODRL), Version 1.1. ODRL Initiative, available at http://odrl.net**

[18] **OMA DRM Specification – Rights Expression Language, Version 2.0. Open Mobile Alliance, available at http://www.openmobilealliance.org/release_program/drm_v2_0.html**

This OWS Common Specification contains a list of normative references that are also applicable to this Implementation Specification.

4 Terms and definitions

If a term is not defined in this document, it will take the definition supplied in their original context in the last reference in the following list in which it occurs, or, if still undefined, its usual English (Oxford English Dictionary (OED) or Webster) definition.

- ISO 2382-6 [1]: for common processing terms such as read, write, copy, duplicate, input, output, collection, acquisition, transform, convert, encode, decode, search, index, edit, and extract.
- ISO/IEC 15408 [2]: for common information technology (IT) security terms such as authentication resource, authorised user, identity, security attribute, security policy, and trusted channel.
- OWS Common Implementation Specification [OGC 05-008].
- OGC Glossary [8] for terms and examples specifically related to OGC standardized web services.
- RM-ODP [10] for system modelling terms such as the enterprise, computational and information viewpoints.
- ODRL [17], OMA DRM REL [18] and ISO/IEC 21000 [11], for terms specific to rights expressions languages, such as principal, licence, right, grant, condition, and resource.

Terms that are multiply defined in these resources shall assume the definition supplied here in the context of GeoDRM.

The following terms and definitions apply.

4.1
access control
combination of authentication and authorisation

4.2
agency
legal relationship of a person (called the **agent**) who acts on behalf of another person, company or government (called the **principal**)

4.3
agent
one who acts on behalf of another

4.4
annotate
adding notations or commentaries to a resource (or parts of it) creating a new resource

4.5
authentication
verification that a potential partner in a conversation is capable of representing a person or organization

[W3C; http://www.w3.org/TR/2004/NOTE-ws-gloss-20040211/#defs]

4.6
authorisation
determination whether a subject is allowed to have the specified types of access to a particular resource

Note: Usually, authorisation is in the context of authentication. Once a subject is authenticated, it may be authorized to perform different types of access.

[Security Taxonomy and Glossary; HYPERLINK "http://www.garlic.com/~lynn/secure.htm" http://www.garlic.com/~lynn/secure.htm]

4.7
bypass
mechanism to defeat the purpose of a subsystem by avoiding its invocation

Note: Security systems are bypassed usually by using security faults in the operating system. Such infringements are more an aspect of the operating system than of the security system. To correct this, the relationship between the security system and the operating system must be modified to prevent bypass mechanisms.

4.8
chain of agency
sequence of **agency** where the agent in each relationship is the principal of the next in the chain

Note: A chain of agency, with the proper agreements at each step creates a transitive agency between the agent of the first link and the principal of the last. This chain can be spoken of in either direction, either as “principal → agent = principal → agent” (normal or granting order) or “agent → principal = agent → principal” (reverse, acceptance, verification or tracing order).

4.9

chain of licence

sequence of **licences** that traces a **chain of agency**, where a **licence** is granted at each link of the chain, allowing the **agent** at that link to act as the **principal** in the next

Note: As with the chain of agency, this chain can be spoken of in either direction.

4.10

contract

agreement between two or more principals that creates in each principal a duty to do or not do something and a right to performance of the other's duty or a remedy for the breach of the other's duty

(after http://dictionary.lp.findlaw.com/)

4.11

copyleft (GPL)

licence that accompanies some open source software that details how the software and its accompanying source code can be freely copied, distributed and modified

Note: The most widespread use of **GPL** (General Public Licence) is in reference to the GNU GPL, which is commonly abbreviated simply as GPL when it is understood that the term refers to the GNU GPL. One of the basic tenets of the GPL is that anyone who acquires the material must make it available to anyone else under the same licensing agreement. The GPL does not cover activities other than the copying, distributing and modifying of the source code. A GPL is also referred to as a copyleft, in contrast to a copyright, which identifies the proprietary rights of material. (DRMWatch.com)

4.12

digital licence

document or its representation that specifies the rights granted to a particular user or organization with respect to a specific content or group of content

Note: The core concept in DRM is the use of digital licences. Instead of buying the digital content, the consumer purchases a licence granting certain rights with respect to the content. A licence is the mechanism by which a rights holder conveys rights to another party, such as a consumer or distributor.

4.13

Digital Rights Management (DRM)

packaging, distributing, controlling and tracking content based on rights and licensing information

Note: DRM covers a much broader spectrum of capabilities and underlying technologies supporting description, identification, trading, protecting monitoring and tracking of all forms of rights usages for both tangible and intangible (electronic) assets, including the management of rights-holders relationships. See for example Iannella [21]

“Digital” refers to the material over which the rights exist. “Rights” applies to the intellectual property rights linked to the material. “Management” covers both defining a policy and enforcing that policy in such a way that rights are respected.

The ultimate goal of a distributed DRM system is for content authors to be able to project policies governing their content into remote environments with confidence that those policies will be respected by the remote nodes – LaMacchia (2002).

For the purposes of this document, DRM is taken to mean technology that enable the secure distribution (and where appropriate, sale) of digital media content on the Internet. (JISC, Shared Service and Middleware Studies, Scoping Study into DRM ITT)

4.14

expected risk

expected value (statistics) of loss

Note: Expected risk is calculated by multiplying the probability of the types of infringement by the cost of that infringement, summed up over all types of infringement.

4.15

fair use

uses of content that are considered valid defences to copyright infringement, such as for criticism or educational purposes

[U.S. legal term]

Note: Fair use is based on case-law precedents derived from general principles. The term is often misapplied to refer to the reasonable expectations of consumers to be able to use purchased content on all owned devices. (DRMWatch.com)

4.16

general public licence

licence containing rights accorded to the general public without an existing agreement

Note: GPLs can be granted by the owner of a resource or may be applied to a resource by law, usually as part of the copyright law. The most obvious GPL concept is “fair use” in the United States for copyrighted material. Other GPL rights may be demanded by the source of the resource or other “public good” considerations.

4.17

GeoDRM enabled (applied to processing resources)

capable of maintaining **GeoDRM extended** resources and enforcing GeoDRM defined rights and protections

4.18

GeoDRM extended (applied to resources)

associated to GeoDRM metadata indicating types of licences that apply

4.19

geoLicence

licence related to geo-information

4.20

geoLicence resolution

settling or resolving the status of a geoLicence

4.21

geoLicence infringement

act or an instance of the unauthorized access or use of protected, copyrighted or patented material or of a trademark, trade name, or trade dress

(after http://dictionary.lp.findlaw.com/)

4.22

infringement (of a licence)

act of a principal contrary to rights granted to that principal on a resource

Note: Infringement of a licence should require the DRM system to be bypassed in some manner. If licences can be infringed without bypassing the DRM system, then the system is not sufficient.

4.23

infringement (of a right)

prevention of an act of a principal consistent with rights granted to that principal on a resource

Note: Infringement of a right is a fault in the DRM system. If rights can be infringed without bypassing the DRM system, then the system is not properly restricted to that which is necessary.

4.24

joint ownership

ownership by two or more persons each having undivided shares in the property as a whole

(http://dictionary.lp.findlaw.com/)

Note: In this case the principal as owner is a principal group, i.e. a group of other principals.

4.25

lease

allowing the resource to be made available for a fixed period of time then returned

Note: During this period, the resource is only available to the lessee. Temporal constraints are required for downstream use.

4.26

lend

lease without exchange of value

4.27

licence

representation of grants that convey to principals the rights to use specified resources subject to specified conditions

(derived from XrML 2.0 specification, part 5)

Note: A licence represents, but is not, a contract that grants a party explicit rights to use intellectual property.

4.28

licence extents

scope or applicability of a licence

Note: The extent can be described in spatial, temporal or any other parameter range appropriate to the rights described in the licence.

4.29
licence manager
application that tracks licences available within an organization and coordinates the issuing of these licences to requesting clients

(after http://www.basis.com/advantage/mag-v3n2/flexconcepts.html)

4.30
licensee
one to whom a licence is given

(http://dictionary.lp.findlaw.com/).

4.31
licensing agent
principal authorized to act on behalf of and under the control of another in dealing with third parties in the context of issuing licences for specified resources

(after http://dictionary.lp.findlaw.com/ for 'agent')

4.32
licensor
issuer of a licence

(after http://dictionary.lp.findlaw.com/)

Note: May be a content owner or a licensing agent.

4.33
lineage
chain of legal ownership of content; history of ownership

4.34
map
visual representation of geoinformation; a map is not the resource itself

Note: A Web Map Service (WMS) produces maps of georeferenced resource. Therefore a WMS can provide many different representations of the same underlying geoinformation.

4.35
necessary
capable of recognizing and properly acting upon all legitimate requests, as defined by the requirements of the system

Note: All aspects of a DRM system are necessary if they do not prevent legitimate requests from execution.

4.36
owner
one with an interest in and dominion over content: as

a) "legal owner" in this entry
b) one with the right to exclusive use, control, or possession of content
c) a purchaser under a contract for the sale of real content

(after http://dictionary.lp.findlaw.com/)

4.37
party
principle
a person or organisation that plays a role in a rights transaction

Note These two terms are used as near synonym from ORDL and ISO 21000. There shall be no distinction between these two terms made here, but there may be distinctions in legal documents depending on local laws.

For example, in some legal traditions, “party” refers to person in a legal dispute, while “principal” may be the entity initiating a contract, such as an agency.

4.38
payment provider
party that has an established billing relation with a consumer

(http://www.newgenpay.com/faq.html)

Note: Payment providers may be telephone and cellular companies, banks, credit card corporations, ISPs, network operators and utility companies. The payment provider bills the consumer, deducts a fee, and forwards the payment to the content provider. The payment provider is thus responsible for the balancing of accounts.

4.39
persistent protection mechanisms
protection mechanism that remains in force regardless of where the content of the original resource is located or reproduced

Note: Persistent protection mechanisms involve authentication, authorization and encryption technologies for effectively locking digital contents and limiting distribution to those who pay.

4.40
protection
aspect of the system that lowers the capability of **party** to commit **infringement**

4.41
provenance
information on the place and time of origin or derivation or a resource or a record or proof of authenticity or of past ownership

4.42
resource
entity that is protected by a licence

Note: In general, a resource is data, metadata (a type of data describing other resources) or some service or process that can be invoked on other resources. Licences describe rights on resources and, as such, are resources in themselves.

4.43

remediation

act or process of correcting a fault or deficiency

Note: Remediation allows more **trust** because it lowers **expected risk**. The first act in a remediation sequence is detection of the fault.

4.44

right

permission to act that makes a party entitled to act with respect to all or part of a specified resource under the terms of the license

(after ISO 21000 - 5)

Note: A right specifies an action (or activity) or a class of actions that a principal may perform on or using the associated resource. A right is for all intents and purposes a legally recognized entitlement to do something to or with the content of a resource. (DRMWatch.com).

4.45

rights holder

principal that owns the right to license rights to a resource

(After http://www.europe4drm.com/l_menue/glossary/glossary.htm)

Note: Rights may be by law (copyright), by agreement or by contract (the “licence” agreement). In the case of digital commerce, DRM ensures that licences are adhered to, and that rights holders are compensated as appropriate for each transaction. Agents of the original rights holder may also issue licences, but their ability is only under the agency contract to the original principal.

4.46

rights management

tracking and controlling the use of content, rights, licences and associated information

Note: (based on Rosenblatt [25])

4.47

risk

value of what may be lost if infringement occurs

4.48

sublicence

licence granted by the original licensee to a third party under the grants and condition of the original licence granted to the original licensee by his licensor

after Palmer & Dodge, LLP; (http://dictionary.lp.findlaw.com/)

Note: This is essentially the right to loan one's licence to another principal.

4.49
sublicensee
principal granted a **sublicence**

4.50
sufficient
capable of enforcing the requirements of a system

Note: A sufficient DRM system would have to be bypassed if an infringement would be possible. Proof of sufficiency may be difficult since it may be dependent on an "attack model", which describes the sorts of attacks to which the system is immune.

4.51
transaction
set of actions joined into the same unit of work, such that the actions either succeed or fail as a unit

[after W3C, http://www.w3.org/TR/2004/NOTE-ws-gloss-20040211/#transaction]

4.52
trust
sum total of all mitigating factors with respect to a particular licensee that reduces **expected risk**

Note: Trust allows the owner (or his agent) to act with a higher potential risk because the expected risk has been lowered. Be careful, this is slightly different from the plain language of trust. Normally, trust requires something, but if the principal at risk decides that no risk exists, then trust exists (in the sense here) since risk has been reduced, whatever the reason.

5 Conventions

5.1 Abbreviated terms

Abbreviated terms found in the references use in the terminology clause 4 apply to this document, plus the following abbreviated terms.

API	Application Program Interface
DCE	Distributed Computing Environment
DRM	Digital Rights Management
IDL	Interface Definition Language
IT	Information Technology
GI	Geographic Information (and Services) as an extension of IT
REL	Rights Expression Language[2]
UML	Unified Modeling Language

[2] Not all RELs use this acronym. The most common usage is ISO REL, but unless the full name is used, REL will mean any compliant licence expression language.

5.2 UML notation

Diagrams that appear in this specification as conceptual models of software and information systems are presented using the Unified Modeling Language, Version 2.0 (UML 2.0) as described in ISO/IEC 15901 and the follow-up OMG specifications.

6 GeoDRM Design Principles

6.1 GeoDRM Roadmap

In order to support GeoDRM-enabled licensing of geographic information, as it can be available offline or online in a Spatial Data Infrastructure (SDI), different functionalities can be identified as necessary. Bundling a certain set of functionalities into a function package allows defining (i) interfaces between the packages to ensure interoperability and (ii) responsibilities for each package to return the expected result upon a given request. The following is a list of possible packages:

- **Rights Model**: The definition of an abstract Rights Model is the topic of this specification. It defines the basis for developing a geo-specific Rights Expression Language as well as other specifications necessary to establish a GeoDRM-enabled SDI.

- **Rights Expression Language**: This package provides the capabilities to express usage rights in the form of a machine-readable and machine-processible representation. The definition of a geo-specific Rights Expression Language is not part of this document, but is to be defined upon the Rights Model declared in this specification.

- **Encryption**: This package includes required functionality to protect a GeoDRM-enabled SDI against fraud. First, encryption enables the protection of a licence so that it cannot be modified by an adversary in order to obtain additional rights. Second, encryption is also useful to protect the digital geographic content against unlicensed use. An example from the music industry exists, where the encrypted music file can only be decrypted (and played) by a certified software or hardware device. Because security and trust are not geo-specific, no standardization is planned from this WG.

- **Trust**: Every type of business relationship that has been represented in an electronic way needs a mechanism to differentiate between reliable and unreliable partners. In that sense, trust tells a relying partner that the other behaves in a certain predictable (loyal) way. One mechanism to establish trust between entities in an SOA [spell out] can be done by adding authenticity information on the digital content that is been exchanged between the partners. This mechanism, typically called a Digital Signature, is not geo-specific and therefore is not a relevant topic for standardization by this WG.

- **Licence Verification**: This package defines the functionality that is required to validate a licence. The licence verification has to occur before the rights of the licence can be enforced. Because document authentication is not geo-specific, it is not a topic for standardization by this WG.

- **Enforcement and Authorization**: The rights expressed in a GeoLicence need to be enforced. In this specification, this package functionality is represented by the "Gate Keeper" metaphor (see Figure 2). The acceptance or denial decision for a particular request (with its associated licences) is based on the authorization decision, as it is derived by the authorization engine. Because enforcement and authorization is geo-specific, the appropriate standardization is upcoming work to be based on this specification.

- **Authentication**: The basic requirement for trust, licence verification and enforcement/authorization is proof of identity, as it is provided by the functionality of this package. Different international standards, which define how to enable this functionality, exist. Because authentication is not geo-specific, it is not a topic for standardization by this WG.

6.2 Basics

DRM is first a metadata-tracking problem. Both resources and principals are associated to descriptions (metadata) and those descriptions must be tracked and matched for the controlled actions to proceed. The resource metadata is the resource identity and description, and the principal metadata is the set of licences he has or has access to.

Second, DRM is an enforcement problem. Once identity and licences have been checked, the results enter into the stage where the principal wishes to take action with respect to that resource. The DRM system controls the scope of those actions to a degree determined by design of the system. This “degree of control” is a measure of trust. The more the principals can be trusted, the less control is needed. In a zero or negative trust (distrust) environment the control may be great and will be critical for protection against malicious or licence-inconsistent acts of users.

6.3 Flow model of GeoDRM

In describing acts on resources, we will consider directed graphs where each arrow in the graph is a triple consisting of:

- a set of 1 or more input resources, (the start point of the arrow),

- an act (the arrow), and

- a set of 0 or more of output resources (the end point of the arrow).

For example, the act of applying a WMS.GetMap to a Feature Collections to derive a (raster) Map would be represented as:

$$FeatureCollection \xrightarrow{WMS.GetMap} ImageMap$$

If the act is to apply a licensable process resource to a licensable data resource, then the input resources are the process resource and data resource, the act is to execute the process against the data, and the output is the results of the act. If the result is not licensable, then the last part of the triple may be NULL or empty. For the example above, the user would have to have an execute right for the feature collection resource where the process satisfied the WMS specification, an execute right for the resource that executed the WMS.GetMap process, and a derived right to view (display, print) the image map produced.

This is a logical function that allows the descriptions here to be consistent, and helps the semantics of licences, which cannot be analysed against a data and process flow diagram represented by a directed graph as described above.

6.4 GeoDRM Gatekeeper Metaphor

The GeoDRM processing at its minimum is a mechanism to test if an action (an orchestrated set of processing arrows in the graph representation described above) is permissible given:

- the party requesting the action,
- the resources (data and processing being used),
- the licences belonging to the party in a), including descriptions of rights, resources and conditions,[3]
- the owner of the resources, and a mechanism to trace his agency chains from the resources in b), and
- the local context of the resources, including local general rights (held by all), applicable laws/policies and the local security system ratings.

The GeoDRM system acts as a gatekeeper, making the decision to allow or disallow request for processing based on the information verified and passed to it by the local secure process controller. Figure 2 shows a simple local topology for such a system. In general, the components are location independent as long as secure communication can be assured between the three basic components:

1) A security system capable of validating the documents and resource data supplied to in external request for processing.
2) A GeoDRM logic module (here called Gatekeeper) that would decide on the consistency of:
    - the request,
    - the licences available to the principal making the request, and
    - the processes available to the system, either directly or through other gateway/gatekeeper pairs.
3) A processing node supplies a secured environment where licensed resources can be used without leakage.

The only data in or out of the system is under the control of the security system and the consent of the gatekeeper GeoDRM.

In the simplest case, where a single request does not cascade, then the communication topology of Figure 2 is sufficient. The sequence is as follows:

[3] In a license, several rights may be assigned to parties on different resources. Each subunit of the licence (called a "grant" in this model) will consist of either explicit or implicit descriptions of the party concerned, the rights (acts) to be done by this party, one or more resource that is involved in the act, and any conditions or constraints on this grant.

1. A request containing the functional information concerning the request and whatever licence information the user believes is needed arrives from a user. This information may be by reference, and may only be the user's verifiable identity so that the security system can fetch validated copies of his licences from a local store.

2. The Security component of the systems verifies identities and the various signatures associated to the documents, which gives all documents a traceable provenance. This information is passed to the GeoDRM Gatekeeper, who has access to all pertinent context information on the resources being invoked.

3. The Gatekeeper verifies that the licences give the users the rights to the resources (both data and processing) that would allow him to execute his request. If the licence does not cover the request or an important document was found to be invalid, the security system returns an error message to the user on causes of the error.

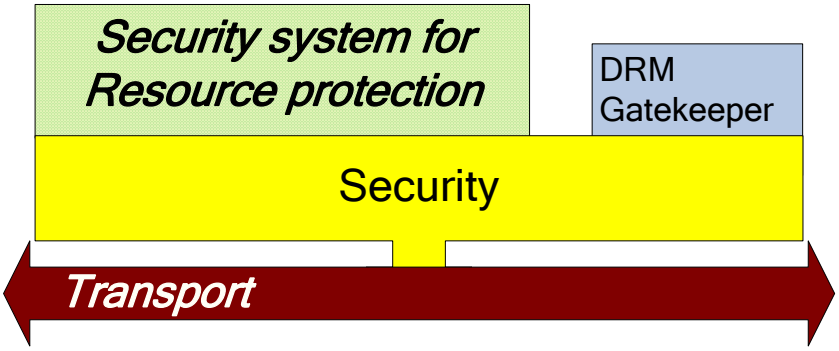

Figure 2: Gate Keeper metaphor for GeoDRM

4. If the licence does cover the request, then the security system passes the request to the geoserver for processing.

5. When the geoserver is done, the results are passed back to Security. Any new resource will be marked with metadata as to use and sublicensing restrictions.

6. The Security system passes the results to the user.

In a more complex scenario, where more that one geoserver is used, transport topologies like the one in Figure 3 may come into play.

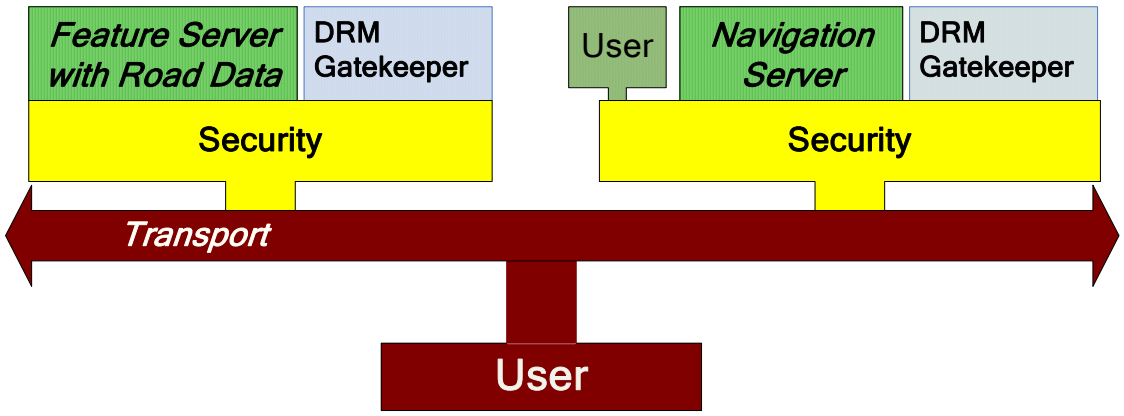

Figure 3: Topology for complex gatekeeper example

In this example a user makes a navigation request to one server, who cascades a feature data (WFS) request to another server for roads data. In many such cases in the real world, the relationship between the two geoservers will likely be optimised, and simpler more direct sequences will be used. For the purposes of this example, we will assume here that no such prearrangement has been put in place. The sequence of request and responses is given in the sequence diagram in Figure 4

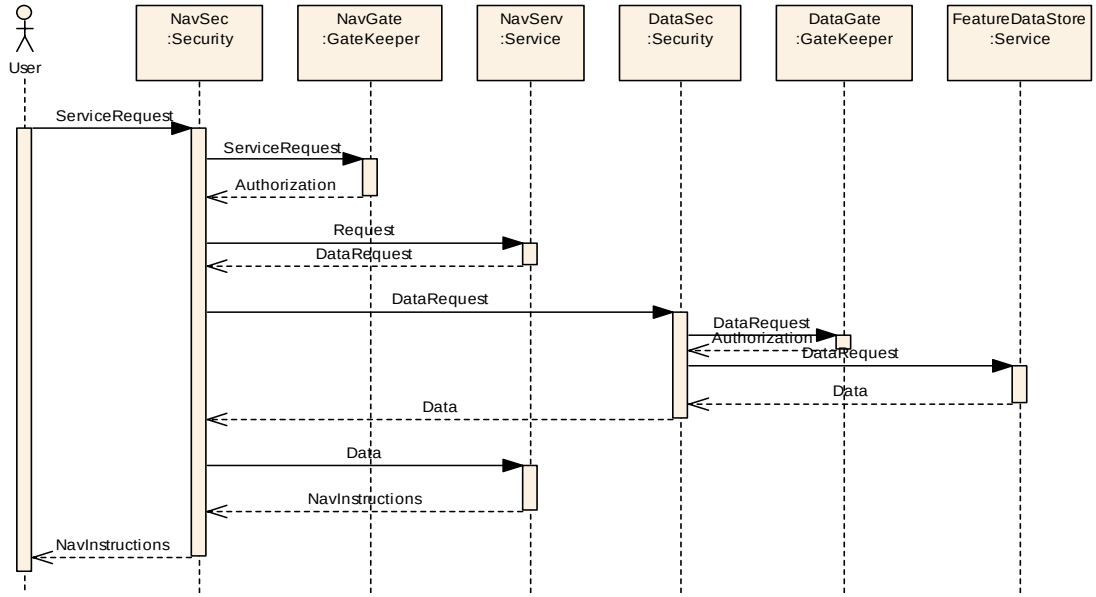

Figure 4: Sequence diagram for a two-stage geoserver interaction

The sequence of response pairs is very similar to that in the previous example.

1. A request containing the functional information concerning the request and whatever licence information the user believes is needed arrives from a user.

2. The Security component of the systems verifies identities and the various signatures associated to the documents, which gives all documents a traceable provenance. This information is passed to the local GeoDRM Gatekeeper, who has access to all pertinent context information on the resources being invoked.

3. The Gatekeeper verifies that the licences give the user the rights to the resources (both data and processing) that would allow him to execute his request. If the licence does not cover the request or an important document was found to be invalid, the Security system returns an error message to the user on causes of the error. If the licence does cover the request, then a “request is valid” message is sent to the Security system.

4. The Security system passes the request to the local navigation geoserver for processing.

5. The navigation geoserver finds a point in the process where data from an external roads database is needed. It formats a request giving its local identity as sender, and including a “temporary transactional” licence showing that it is acting as a computing agent for the original requestor, and that it has been certified to handle licensed data locally.

6. This request is passed through Security to the Security of the feature server.

7. The feature server Security passes the transaction licence data to its local Gatekeeper.

8. The local Gatekeeper validates the transaction, and returns the decision to the requesting Security gateway.

9. Security passes the request to the local geoserver.

10. The local geoserver performs the task and send the results back to Security

11. The feature service Security passes the results to the Navigation server Security.

12. Navigation Security passes the data to the Navigation server

13. When the Navigation server is done, the results (a set of navigation instructions) are passed back to Security. Any new resource will be marked with metadata as to use and sublicensing restrictions.

14. Security sends the final results to the user.

Notice that the sequence diagram, which ignores transport details, does not differ between the two user types in Figure 3. Several variations on the transport topology would yield the same sequence diagram. Most of the GeoDRM processing is location transparent.

6.5 DRM metadata – licence model

The general model of a licence is depicted in the following diagram:

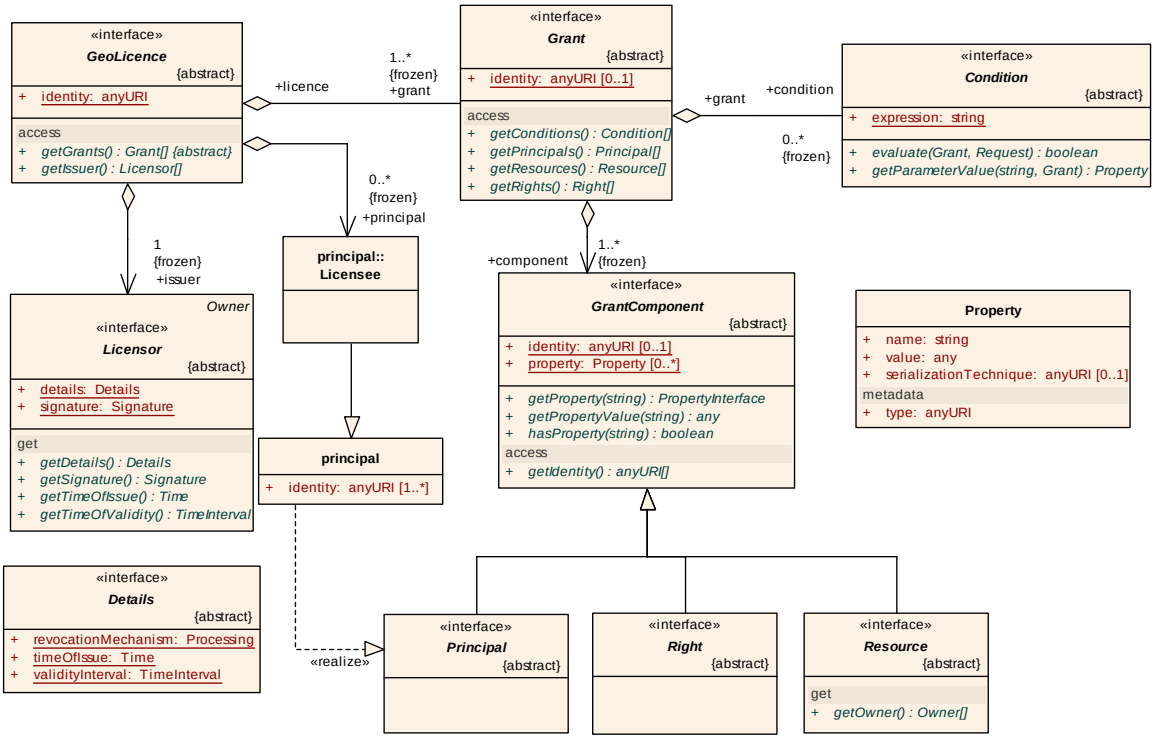

Figure 5: General Licence Model (UML)

The basic semantics of a licence document representation is given in [13].

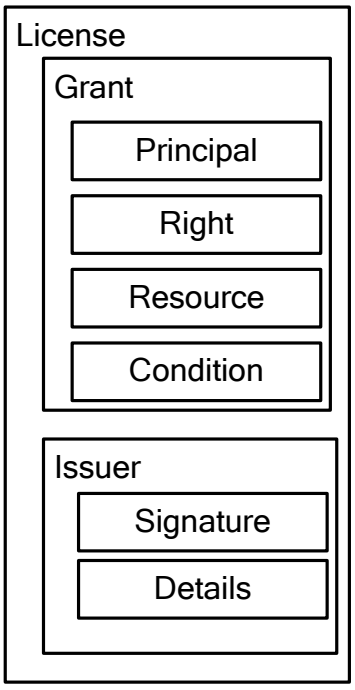

Figure 6: Structure of a Licence

From this we see that the needed information for DRM to work includes:

1. A mechanism for identifying principals, for both the identification of the licensee and licensor of each licence,

2. A mechanism for identifying resources so that licences and resources can be matched to validate the licence,

3. A set of rights that may be granted in a geoLicence,

4. An association of each of those rights to particular “software-based” actions,

5. A definition of the types and meanings of conditions that may apply to each right, principal or resource and

6. A signature mechanism for authentication of identity and to verify that the licence has not been modified in any significant manner.

The parts of the licence have the following conceptual meanings:

Table 1: Semantics of licence structure

Licence	Digital representation of the agreement between the Principal and the Issuer
Grant	Description of the right being conveyed (one to many instances)
Principal	Entity to whom the right has been granted
Right	Act associated to the right that has been granted
Resource	Resource associated to the act above
Condition	Conditions that modify the right
Issuer	The other party to the licence, the source of the rights.
Signature	Digital signature of the issuer of this licence
Details	Other information needed to assure validity of this licence

6.6 Developmental Guidelines

In developing this specification several design guidelines have been followed. These include, but are not limited to, the following “best practices”:

- The GeoDRM Model must support ubiquitous geographic information.
- Keep the DRM policy really simple, but no simpler.
- Keep DRM as coarse-grained as possible while maintaining basic requirements.
- Apply as little DRM as possible, but no less.
- Delegate licence creation maintenance, enforcement and security.
- Licence management should be transparent to the end-user; licence flows should be identical to unlicensed ones where feasible.
- Adapt to fit common business, trading, pricing and licensing models.

- Accept manageable risks then manage them.

The ultimate goal of geographic standards is to make geographic information and services available and readily usable to the entire information services community. Therefore the use of geographic information and other information should be minimally different.

6.7 The components of managing risk

Managing risk is about balancing trust with protection and remediation. The optimal balance among these components depends on the specific business context. For example, where high levels of trust exist, lower levels of protection and remediation may be acceptable.

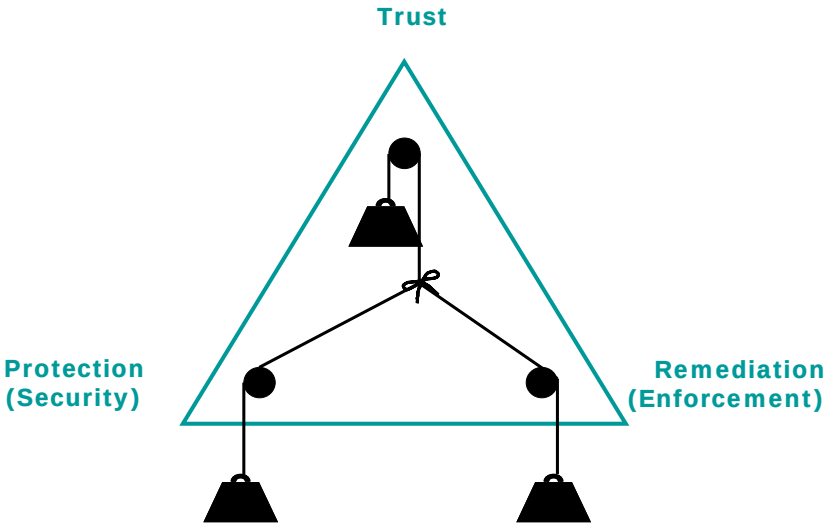

Figure 7: Balancing trust with protection and remediation

The following sections examine these components in more detail.

6.7.1 Trust

Digital rights management is about trust. Internet commerce cannot occur without some level of mutual trust, even more so when the parties are not in personal contact and resources are ethereal like digital data. These criteria often make business models based on classical business practices inappropriate – see [19].

The contract that exists between buyer and seller is a description of that trust, and the DRM system aids both parties by aiding in the enforcement of the contract through the software that accesses and processes the resource.

Since the DRM system should enforce that which is not in the contract and only the contract, it aids in maintaining a position of fair enforcement that enhances the relationship and prevents misunderstanding while preserving the rights of both parties.

The business environment for a DRM system can vary widely. In one extreme, everyone is trusted and the DRM is simply an aid for tracking process and data flows for the

purposes of the system (possibly including remediation if the trust is broken). In the other extreme, no one is truly trusted and the DRM controls all resource flows that involve licences. In this case, the licensed resources are “locked” from general use and all software handling licensed transactions is “trusted” in the sense that it is integrated sufficiently with the DRM system to prevent the gatekeeper from being bypassed, and a licensed resource “leaking” into a freely available world.

The most likely scenario is a trust model that is “gated,” capable of controlling the level of freedom in each transaction based on the rights and conditions stated in the various licences involved. While complex, such a system allows maximum flexibility based on the DRM business model in use. Most of the examples in this document are from this middle ground, where the control over how a resource is to be handled is embodied in the licences that are issued against it and not in the system design. This makes the licence content independent of implementation.

6.7.2 Protection - security

A DRM system enhances the altruistic trust by providing before the fact (*ex ante facto*) protections. The user, through trusted software, knows that he can legally do that which he is allowed to do and the owner of the resource knows that abuse of the contract is at least difficult. The degree of difficulty should be proportional to the risk to the resource, where valuable resources are generally protected more than ones of lesser value.

Examples of protection can be anything that restricts access to resources to those able to present and prove licensed rights to those resources. An authorization "log-in" system could be used in those cases where the structured contact between system and user gives some guarantee of identity. Other systems may depend on the proving of identity and reference to a valid licence with each interaction of user and resource.

Protection systems (i.e. security systems) are a realm unto themselves, and DRM systems will be heavily dependent on the choice of security implementation – see [2] and [3]. The most likely candidates for web-based DRM security involve the ability to distribute keyed files that are unreadable without the key, and then to control the key distribution (cryptography).

6.7.3 Remediation - enforcement

Remediation is an act or process of correcting a fault or deficiency. Since no protection system is perfect, there is an additional need to track licensable acts. This tracking allows the software to act as the first step in any remediation steps taken after the fact (*ex post facto*). The actual remedial actions may be stated in the contract, or in the written or common law.

For example, if a buyer wishes to minimize the cost of his licence by restricting it to those things he actually uses, he can agree to be subject to a flexible licensing agreement that grows the licence on an “as-needed” basis. In this case, the remedial event of the first use of a licensable act would be the granting (and billing) of a new licence update to cover that act.

6.7.4 Metadata in support of trust

Support of trust through protection and remediation is predicated on the unambiguous identification of users, resources, rights and processes. The mechanism for this is the association of metadata to each that enables the tracking of resources, users, licences, rights and the actions that they reference.

User metadata consists of user identification and various licences and access rights that describe their geo-processing environment.

Resource metadata consists of resource identification and authority control information that describes what rights and licences are associated to this resource.

Licence metadata consists of the identification of the various resources, licensees, licensors, rights and restrictions that will act as software control mechanism under the DRM system.

Rights metadata consists of the definition of the act that right allows. Such metadata can be references to standard IT processing mechanisms or other specific geo-processing standards, such as those from ISO TC 211 or the OGC. It can also be implementation specific, identifying what software or software resource that may be used in the action allowed by the right.

Process metadata consists of the identification of the underlying software and the various standards and rights' acts that can be executed with this software. Since the use of software is essential in the execution of the rights-specified acts, the identification and certification of processes may be the purview of the standards-creating organization responsible for its standardization.

The procedures involved in a DRM system at its core is the control of actions taken on resources under the control of the DRM system as determined by the comparison of the various types of metadata described above.

For example, if a *user* requests a *process* on a *resource*, the DRM system would be responsible for identification of the *user*, the assessment of the *rights* associated to the *user*, and the comparison of those *rights* with the *process* and *resource* requested. If everything matches, then the action of executing the *process* on the *resource* is allowed.

7 GeoDRM Enterprise Viewpoint and Abstract Rights Model

In this section, we will define those key concepts needed for geospatial rights definition. The purpose of the GeoDRM Abstract Rights Model is to define the base conceptual model, which may then be used for the definition of GeoDRM Implementation Specifications.

Managing Intellectual Property is essentially an abstract problem. In the physical world we can see the boundaries between physical properties, and we intuitively understand the rights to access that property based on social, legal and political conventions. Before you enter your friend’s home you need his permission. When you travel to a foreign country you need to present your passport before you are allowed access to that territory.

However, managing Intellectual Property presents us with the key challenge that the "territory" we want to manage only exists in the abstract and not the physical world. Before we can manage and protect this Intellectual Property "landscape" effectively, we need to define a shared concept of what is being managed, which is universally understood by all involved.

The key purpose of the GeoDRM Abstract Rights Model is to create a simplified model of geospatial Intellectual Property so that it may be practically licensed, and most importantly, rights to that Intellectual Property may be managed and protected. It is about establishing shared notions, conventions and practices that express the boundaries within the Intellectual Property "landscape". With defined Intellectual Property boundaries, we are then able to share exchange and trade rights to geospatial resources in a clearly defined and managed way.

7.1 Geospatial Resource

A geospatial resource is a well-defined set of geographic resources or functionality that can be either a resource set, a subset of a resource as specified by a filter encoding, etc.

Note: We are trying to create a rights management mechanism that is independent of the geospatial resource being managed.

7.2 GeoLicence Extents

A GeoLicence is the mechanism to manage and protect a geospatial resource.

A GeoLicence is the expression of the rights and constraints on those rights to be performed against a geospatial resource.

GeoLicence rights and constraints may be expressed using, but not limited to, the following dimensions:

- Right: A privilege that is granted by the Owner. For example, the right to View, Print, Copy, and Update, etc. a geospatial resource.
- Space: A geospatial area. For example, a specific country such as the United Kingdom.
- Time: A period of time. For example, the year 2005.

A GeoLicence is the container expressing the rights to use a specified geospatial resource, for a given geographical space, over a specific period of time – subject to other conditions.

Figure 8 shows these three dimensions with the extents of the GeoLicence drawn as the dotted block.

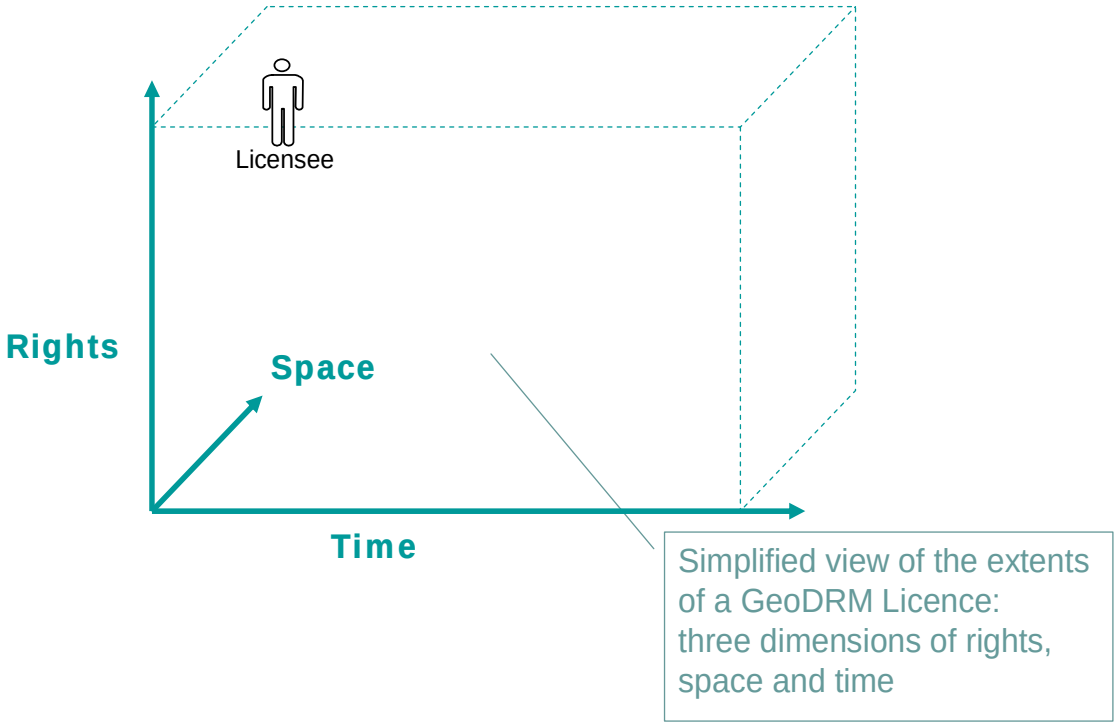

Figure 8: GeoLicence Extents

An example GeoLicence may express the rights to View, Print, Copy and Update, all United Kingdom road resource for 2005.

NOTE:

1. Potentially, we have more than one time dimension, resource time or licence time. For example, time may relate to the time when specific features were last updated (resource time), or the period of time to which the licence applies (licence time).

   For simplicity, the time dimension of a GeoLicence shall mean the period for which the licence applies (licence time).

2. Potentially, the spatial dimension could mean either the geospatial extents of the GeoLicence, or the legal jurisdiction where the licence applies, or even the location of the licensee.

   For simplicity, the space dimension of a GeoLicence shall mean the geospatial extents of the GeoLicence, namely that geospatial area of a given resource to which the licensee is granted rights.

7.3 GeoLicence Expression

GeoLicences may be expressed in different forms – which all essentially mean the same thing, but are different forms according to the intended audience. Potentially, we can envisage three corresponding expressions of GeoLicence:

- Legal Expression: A legally binding expression of the terms and conditions of the licence, which may then be legally enforced.

- Simplified Expression: A simplified, more “human” readable version of the licence, expressing key terms and conditions, which may be easily read and understood by a more general audience.

- Formal Expression: A formal, computer encoding of the key terms and conditions, particularly the GeoLicence Extents. This encoded form of the GeoLicence may then be automatically enforced by the system, when the End-User requests access to the geospatial resource.

Three aspects of GeoLicences are important: first, the expressions of the same licence should be compatible, in other words the legal, simplified and encoded expressions should capture the same essential meaning; second, GeoLicences may either be created as a result of human negotiation, or potentially automatically as the result of applying specific business rules; third, independently of how a GeoLicence is created, the same management and enforcement mechanism shall be used.

7.4 GeoLicence Creation and Enforcement

GeoLicences are the container to express the terms and conditions of a licensing agreement. GeoLicences may be granted subject to conditions of acknowledgement, or GeoLicences may be allocated based on a specific security and intelligence policy.

GeoLicences are required, whether you charge for access to resource or not.

GeoLicence creation and enforcement are separate workflows:

- **GeoLicence Creation**: requires some form of negotiation to define terms and conditions.

- **GeoLicence Enforcement**: Once GeoLicences have been created, the System can enforce the formal expression of the licence. In the event that the terms and conditions of the legal expression are breached, then legal measures may be applied.

Note: Given the limitations of the formal expression of the GeoLicence, it will not be feasible to implement a totally watertight system that prevents rights infringement or abuse. Rather, enforcement of the formal expression should be seen as complementing enforcement of the legal expression.

7.5 GeoLicence Delegation and Management

Geospatial DRM is essentially the process of creating, delegating, managing, tracking, validating and enforcing GeoLicences.

The intention is that a GeoDRM-enabled network of services will automate some or all of these functions. Various actors within the GeoDRM-enabled system will perform these key functions.

A key aspect of a scalable network is the ability to delegate responsibility to these actors in a controlled and managed way. The system would be unscalable if the administrative burden was placed on the content owner alone.

Therefore a key capability for the success of a GeoDRM-enabled system is the ability to delegate these key functions. By necessity, intermediary actors may be needed to perform these administrative functions.

Figure 9 illustrates the concept of GeoLicence delegation and management. Owner (Licensor) of the Intellectual Property can delegate the creation and management of GeoLicences to a Licensing Agent. Licensing Agents are granted the right (i.e. the authority) to issue GeoLicences subject to defined extents and conditions as defined in the agreement.

In this example, the Owner of the Intellectual Property delegates the extents to be managed to a Licensing Agent, who then has authority to issue GeoLicences to a Licensee, who may then delegate work to be done by the End-User. The End-User may then request resource within the extents of the GeoLicence. Requests that fall within the GeoLicence extents are valid, where as those requests that fall outside the extents are invalid – a GeoLicensing violation.

By encoding GeoLicences in a machine-readable way, GeoLicence enforcement becomes the mechanical process of checking that the extents of a request fall within the extents of the licence.

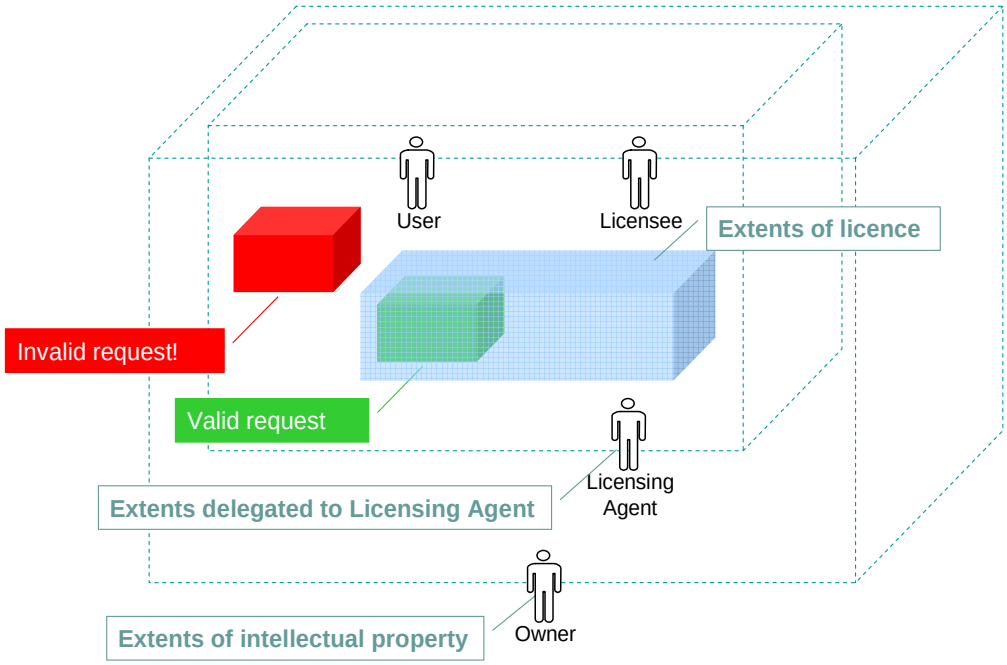

Figure 9: GeoLicence Delegation and Management

In many ways we can consider the concept of GeoLicence delegation and management as being analogous to the way a real-estate owner may rent property in the real world. Often an intermediary letting agent will create and manage rental agreements on behalf of the real-estate owner.

7.6 GeoLicence Chaining

GeoLicences need to be traceable back to the Owner of the geospatial resource. GeoLicences may be “chained” where the Owner defines the top-level constraints and terms and conditions flow down the licence chain. GeoLicences are managed by the Licence Manager, and licences are validated back up the licence chain.

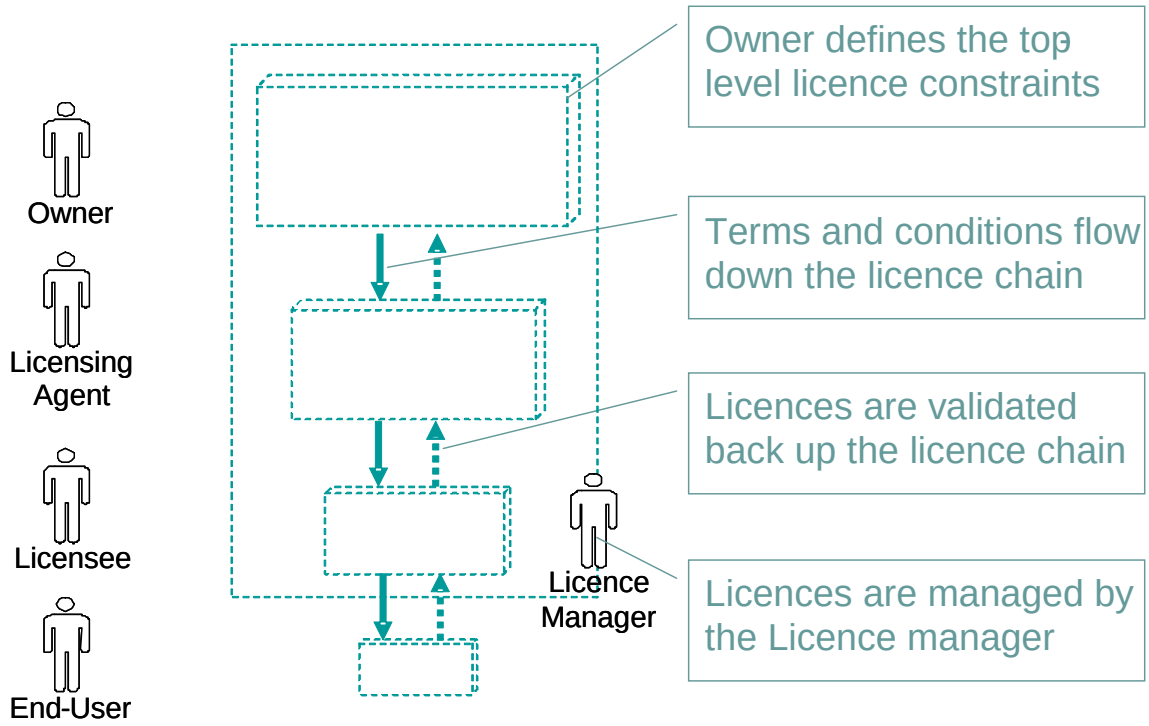

Figure 10: GeoLicence Chaining – supporting distributed licensing

Figure 10 illustrates the concept of chaining geoLicences. This is a key concept that is needed to allow the delegation of licensing responsibility and supporting the need for the distributed licensing of geospatial resources.

7.7 GeoLicensing Communities

Data sharing between human beings requires the sharing of a common understanding of information structures and their meaning. This problem is known as the Triangle of Meaning, as it was first described by Ogden & Richards in 1923. Richards pointed out that words mean different things to different people in different situations. A more recent approach is to define communities in which the same meaning is shared for the purpose of communication.

Thus, data sharing and trading tends to take place within communities of trading partners. Over time standard ways of exchanging information will evolve, for example, standard vocabularies to describe geographic features and processes, standard licence agreements or perhaps standardised pricing models.

For the geospatial problem domain, the OGC has introduced the concept of an information community in their OpenGIS® Reference Model:

*"An **information community** is a collection of people* [and organizations] *(a government agency or group of agencies, a profession, a group of researchers in the same discipline, corporate partners cooperating on a project, etc.) who…share a common digital geographic information language and common spatial feature definitions. This implies a common world view as well as common abstractions, feature representations and metadata." [OGC 03-040, p. 26]*

One example to achieve a common understanding for the exchange of geographic information is based in GML. It defines the structure (XML encoding) of geographic

phenomena and their meaning and uses the GML namespace to make them distinguishable from other definitions. In order to actually exchange GML structured data, the declaration of an application schema is required, but is not permitted to change either the structure or the definition of GML's predefined elements.

Adopting this to the GeoDRM domain, a GeoLicence community can be characterized as a domain of participants (licensor, licensee, licence broker, service provider, etc.) that communicate to each other for the purpose of exchanging licensed geospatial data. In order to do so it is important that all members of the community obey the same structure of a licence (independent by which member it has been created or used) and to the meaning of rights, as they are expressed in the licence. This specification describes the means of a "default" GeoLicensing community by defining a Rights Model and the meaning for a set of predefined rights. In order to refer to these right definitions, a unique identification mechanism based on the URI notation shall be used.

Because it cannot be sufficient to have one community only, it is possible to form other communities and structure relationships among them. Different GeoLicensing communities can exist for various reasons:

(i) different business models,

(ii) different legal rights systems,

(iii) different organisational policies or

(iv) broader / stricter definitions of particular rights.

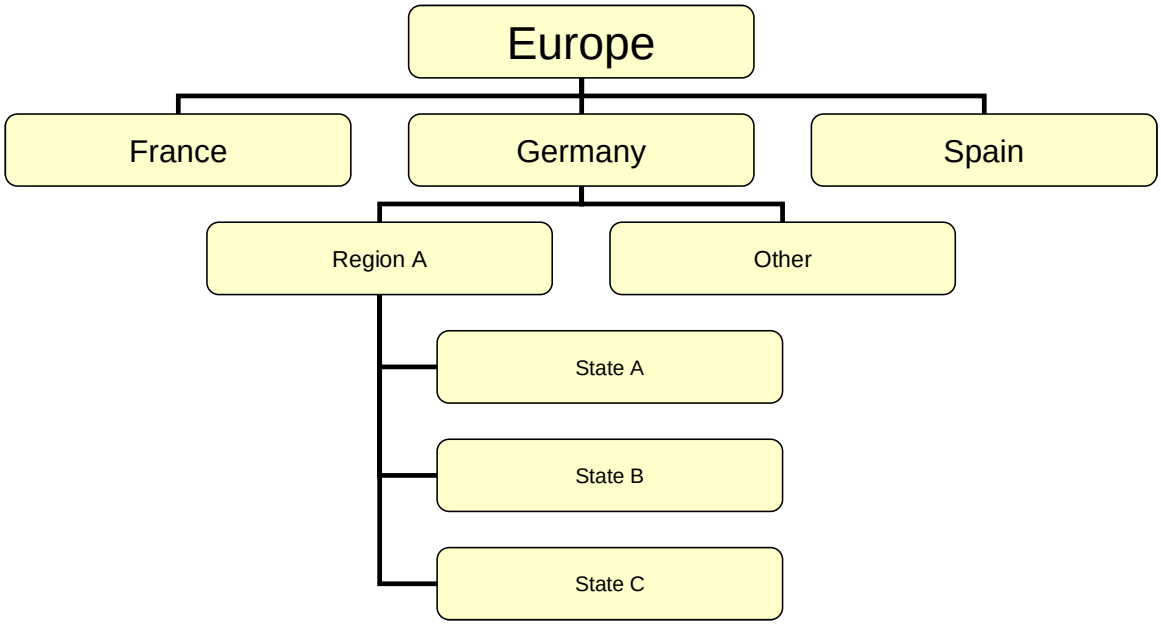

Figure 11: An Example GeoCommunity – based on geography

An example for different GeoLicensing communities, their hierarchy and relationships for Europe is illustrated in Figure 11: Europe is divided into a number of member states, with each member state divided into a number of regions. Allowing the concept of inheritance, the definitions and their meaning for Europe would also hold in France, Germany and Spain. In contrast to that, the GeoLicensing communities of France, Germany and Spain do not necessarily share the same meaning on defined rights.

7.8 GeoLicensing and resource lineage

Lineage or provenance of a geospatial resource is an important factor for both producer and consumer of geospatial information. Consumers need the assurance that the data is fit for purpose and can be used to support critical decisions, whereas providers require recognition for their contribution to a final information product.

A GeoDRM-enabled set of processing resources will allow the lineage or provenance of the derived information product to be traced. As data is processed through a chain of processing resources, a "Process History" could be generated listing those resources that have been used to generate a derived product.

7.9 Handling GeoLicence Violation – and the break-the-glass principle

GeoLicence validation will be performed by the DRM Gatekeeper. Enforcement will be the combined responsibility of the associated Security system and the Gatekeeper. The Security system will verify the information passed to the Gatekeeper for the validation of the licence use. During the verification and validation of a GeoLicence, potential licence violations may be identified.

The procedure of validation is based on the MPEG-21 Authorization model described in ISO 21000 (see [11]). This considers seven items of information associated to the request and the resources involved, as follows:

1. Principals: the identity of the requestor, or other principals associated to him.
2. Rights: the acts to be performed.
3. Resources: the resources involved in the actions requested.
4. Time: the time interval of the acts.
5. Context: known-to-be-true facts and properties, independent of the request.
6. Licence: licence elements applicable to the principal, act or resource.
7. Trust Root: grants not requiring authorization.

Given these seven data parts, the Gatekeeper has to answer one question:

> Is it permitted for a given Principal to perform a given Right upon a given Resource during a given time interval based on a given authorization context, a given set of Licences, and a given trust root?

In addition, if a condition that requires a "side effect" (an outside action initiated by the use of a licence grant, put in place the licensor at the time the grant was issued) is activated, then the Gatekeeper will trigger those side effects with the timing specified in the original grant.

If the Security system performs strictly, no actual violation will occur and the user will be informed of the "error" in his request (the lack of sufficient licence information). The user may also be passed information as a side effect of the attempted resource access.

If the Security system is less strict, and allows the access requested despite the lack of Gatekeeper validation, then a licence violation would have occurred. In creating the

context applicable to the resource in question, the Owner (or his agent) may place side affects to attempted use of invalid licences, which would include either the actions that the Owner feels appropriate to such attempts, or triggers that activate remediation efforts through the licence chair of agency, possibly all the way back to the Owner.

Two general principles should be applied when a GeoLicence violation is identified:

- First, the Owner is responsible for defining what action is performed in response to a licence violation.
- Second, for those resources that may be needed in an emergency situation, the user should be able to override the licence conditions, that is to "break the glass", and have unconstrained access to the resource.

"Break-the-glass" options can be given in grants (given in the licence or in the trust root, parts 6 and 7 of the items above) having side effects, to allow identification of the principals who may use this option (part 1 of the seven items above) and the effects of the use of the option may be embedded as a side effect in those grants.

7.10 Automated licence revocation/expiration – need to revoke privilege

GeoLicences are revocable and can expire. Once a licence has been issued, a mechanism is needed to allow the licence to be revoked. This capability is needed for the scenario where the content owner needs to revoke rights to a resource, or where the licence has a limited lifetime and expires.

The mechanism for revocation is usually associated to the Licensor metadata in the licence (see ISO 21000-5, [13]). The licensor informs the Gatekeeper or Security systems how to verify a licence document is still valid by including it with the information in the licensor "signature" included in or associated with the licence.

8 GeoDRM Computational Viewpoint

8.1 Overview: Roles and Responsibilities

This clause sets out the basic operational concepts and entities in a GeoDRM system. Figure 12 shows the **roles** within a GeoDRM-enabled network of services. Within this model an individual person or organization may perform one or more of these roles in the network. In fact, because many of us currently perform a number of these roles at the same time, it is difficult to imagine other ways of doing business where the roles and responsibilities are allocated in a different way.

In the following figure various roles have divided responsibilities, so they may be combined according to the needs of a specific business model. In many ways these roles can be thought of as the "primitives" that can be selected and assembled according to the specific needs of a business model.

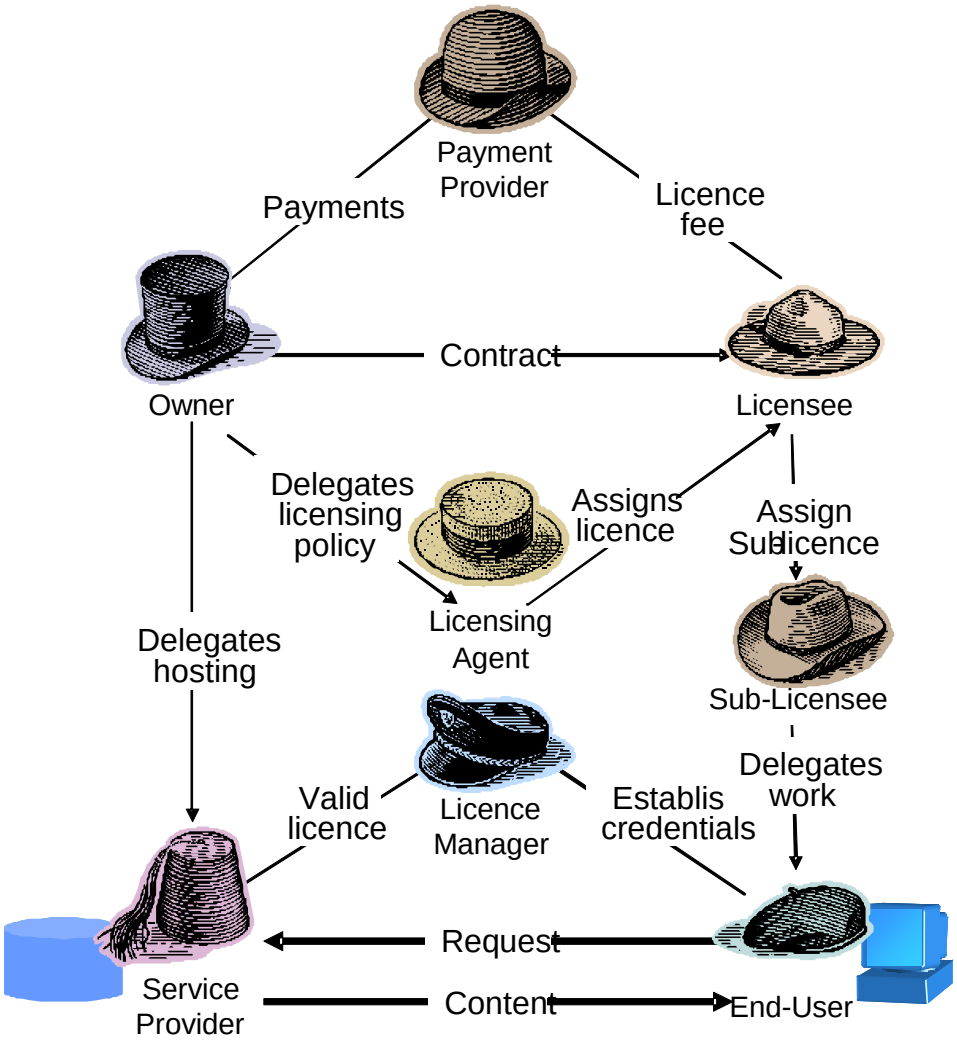

Figure 12: GeoDRM Roles and Responsibilities

Depending on the specific business model, roles may be combined in different ways. Figure 13 shows an example business model: Business A plays the roles of Owner, Licensing Agent and Service Provider; Business B plays the roles of Payment Provider and Licence Manager; and Business C plays the roles of Licensee and End-User. Other business models may make use of the same roles but configured in different ways.

The End-User should not necessarily have full knowledge of the GeoLicence terms and conditions or how the GeoLicence was created. Instead, the End-User should be able to present a valid GeoLicence and be provided access to the Geospatial Resource based on those terms and conditions.

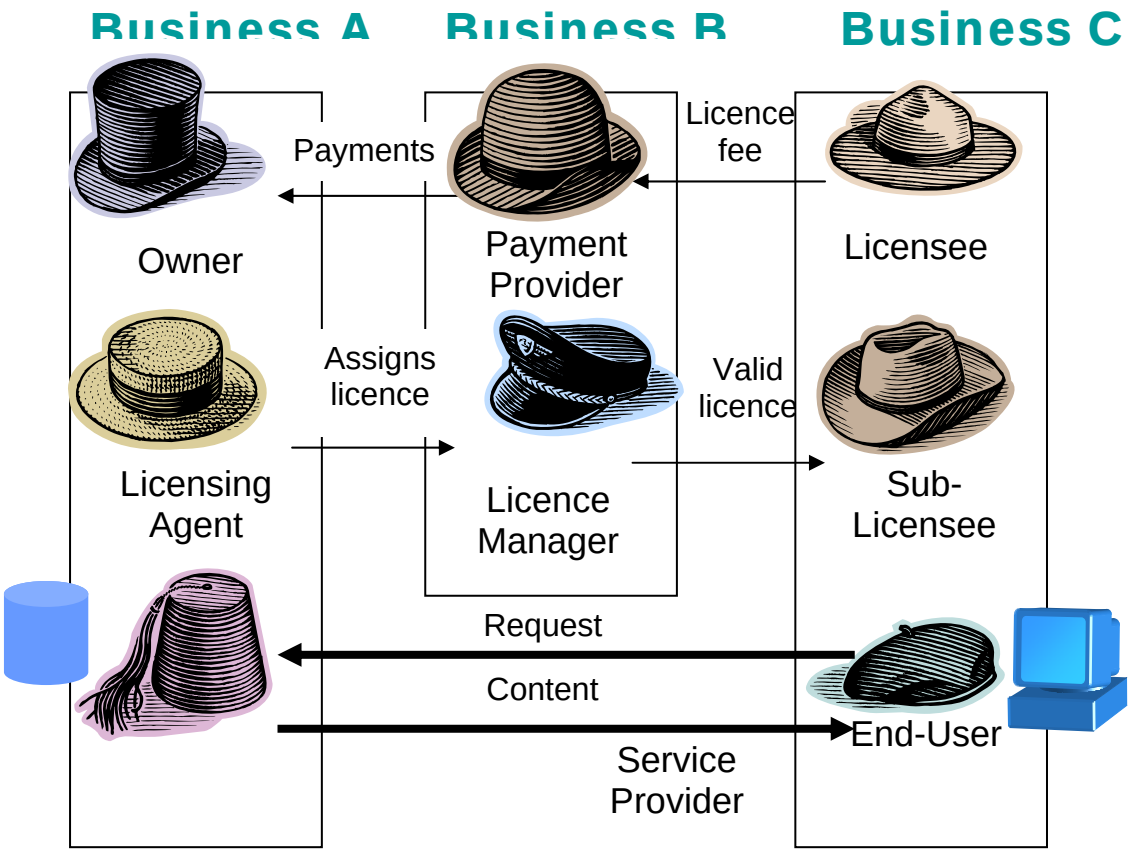

Figure 13: Example Business Model

Table 2: GeoDRM Roles and Responsibilities

Role	Description	Responsibility
Owner	Owner of the Intellectual Property. Often the individual or organization that created the content and has legal rights over how that Intellectual Property is used. Synonyms: Rights Holder, Content Provider, Licensor.	Original creator of content, holds the Intellectual Property Rights and is the licensor of that Intellectual Property. Defines the geospatial extents of the Geospatial Resource, and delegates part or whole of those extents to a Licensing Agent. Defines the Terms and Conditions to be applied within the GeoLicence. Conditions may include a Pricing Model for access to the Geospatial Resource. Defines the policy to be applied specifically when resource flows across the boundaries defined in the GeoLicensing Realm.
Licensing Agent	Manages the GeoLicence creation according to the constraints specified by the Owner – including the delegated GeoLicence Extents, Terms and Conditions, and Policy to be applied.	Creates GeoLicences based on Owner-defined constraints. Ensures that any conditions for the creation of a GeoLicence (like payment) are fulfilled before issuing. Ensures that a copy of the GeoLicence is registered with the Licence Manager for the purposes of enforcement of GeoLicence.
Service Provider	Host the Geospatial Resource on behalf of the Owner.	Ensures that access to the Geospatial Resource is only allowed when a valid GeoLicence is presented, and the request falls within the extents specified. May request GeoLicences from the Licence Manager based on the End-User's credentials.

Role	Description	Responsibility
Payment Provider	Manages payment transactions on behalf of Owner. NOTE: Payment Provider is only required if the terms and conditions of the GeoLicence include a financial compensation for the rights to access the specified Geospatial Resource.	Receives Licence fee payment details from Licensing Agent. May maintain outstanding balances between Owner and Licensees to be settled at a specified account period.
Licence Manager	Manages Licences on behalf of the Rights Managed network and acts as a trusted third party between the Owner and the Licensee.	Registers new and updated GeoLicences. Provides GeoLicence validation functions to Service Provider.
Licensee	Acquires rights to access a Geospatial Resource. Terms and Conditions of those rights are defined in the GeoLicence.	Organisation or Individual with an assigned set of rights as defined by the GeoLicence. Rights granted by the GeoLicence may include the rights to sub-license resource.
Sub-Licensee	Acquires or is assigned a subset of rights by the Licensee.	Sub-licensee is assigned a subset of the rights as defined by the GeoLicence.
End-User	The individual person who accesses the Geospatial Resource.	Accesses Geospatial resource based on the terms and conditions of the GeoLicence. GeoDRM design goal is to make the process of licence creation and enforcement as transparent as possible to the End-User.

A key challenge for the GeoDRM Reference Model is to create an abstract rights model with defined roles and responsibilities, which may then be combined in different configurations according to the specific needs of the business model.

8.2 Principals

Principals are the active entities of the systems: those that can initiate actions, such as requests. Most entities are associated to people and, by extension, to their presence on the net or in the system, i.e., their computers, software or, at least, their identity.

One of the most common authorization tasks is the verification of identity of a principal.

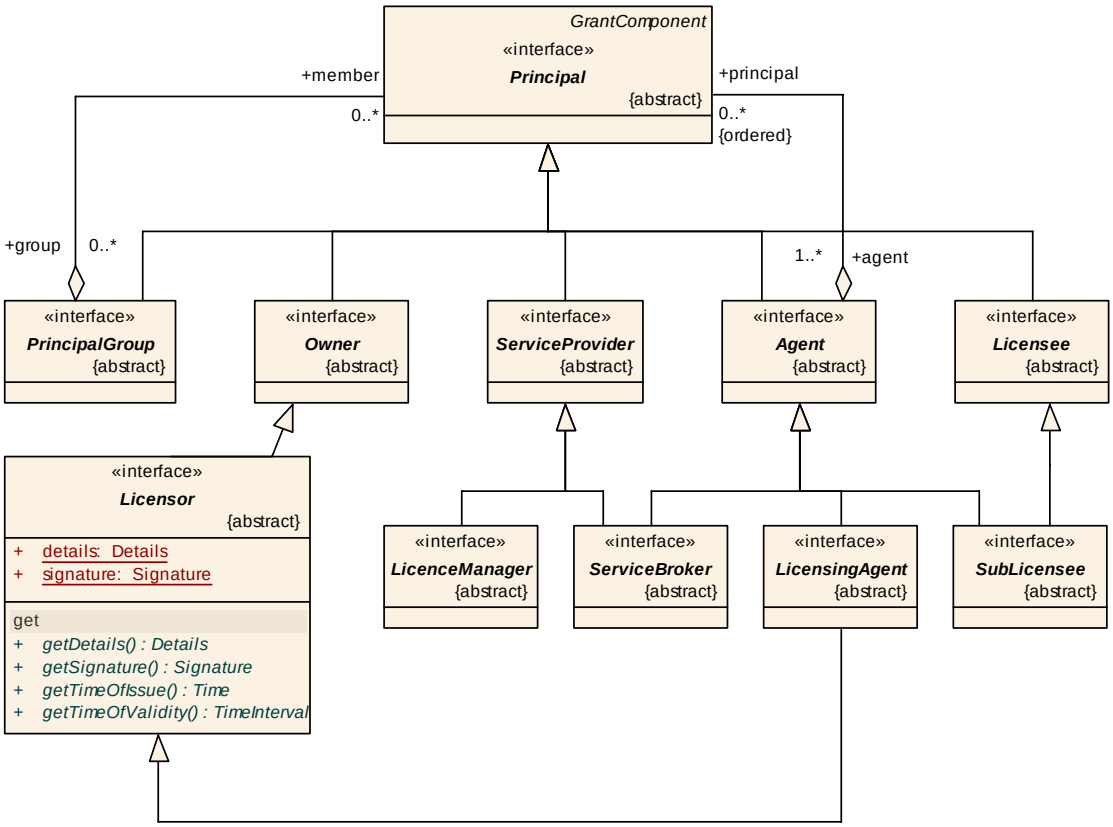

Figure 14: Various Principals in a GeoDRM system

8.3 Resource owner

Owner principals are the controllers of the resources. The relationship between the Owner and the legal owner of a resource may be defined completely outside the system, such as by legal contracts, etc., but the root or all rights resides in the legal owner, and the Owner principal is the legal owners presence or agent within the system.

8.4 Agent

Agent principals are principals allowed to act in the stead of another principal, usually supported by a licence to do so. This sort of licence is akin to the limited power of an attorney in law, as it is seldom universal and will most likely restrict the acts of the agent to specific rights as contracted with the owner.

Most Agent principal subtypes will multiply inherit (as interfaces) from Agent and as appropriate for the rights allocated to him by the other principal. There may be no manner for a user to distinguish whether he is working with and Agent or with the Licensor supporting the Agent's licence to act. The Agent may have to present credentials to other principals to prove their right to act as agent for a Principal with a separate identity.

8.5 Licence broker or licensing agent

The Licensor principal in the system is the source of all licences. It is most often an agent of the owner acting in his stead, supported by legal contracts. If the Licensor principal is not the Owner, then there should be a contract reified as a licence available for

verification to assure other principals that the Licensor is acting within his rights in issuing licences.

The implementation of Licensor validation and authorization is essentially a metalevel in the rights management system, i.e. it is a system for licensing the act of creating licences.

A Licensing Agent is an entity acting as a Licensor but not the Owner. By definition, a Licensing Agent is a type of Agent, since he is conducting the business of another principal.

8.6 Service broker

A Service Broker is an agent for one or more Service Providers that may combine multiple datasets and build licences based on existing agreed relationships.

8.7 Service provider

A Service Provider is a Principal who provides a Service.

8.8 End-User

An End-User is any object acting as a Licensee or any Agent of a Licensee (as a Sub-Licensee. A Sub-Licensee is an Agent of a Licensee qualified to use all or some of the licences belonging to these Licensees.

8.9 Licence Manager

A Licence Manager is an application that tracks licences available within an organization and coordinates the issuing of these licences to requesting clients.

9 Information Viewpoint

9.1 Overview

This clause sets out the basic information entities used to express rights in a GeoLicence in a GeoDRM system. These resource types are abstract, and implementations will differ based on the representation strategy. The information concepts here will be used to build the metadata described in Clause 9.3 and 9.5, including metadata for *users, resources, licences, rights*, and *processes.*

The form of identity used for users, resources, licences, rights and processes is an implementation decision, but the obvious associations to the Internet will often suggest the use of elements of the forms URL, URI, URN and digital signatures.

For copies of digital resources held by other than the issuing authorities, such as licences issued and copied to users, will be protected from modification by any acceptable means as may be specified in the design or standard definitions.

Once striped of its protection and verified, most DRM processing consists of comparisons of fragments of metadata.

For each process flow a set of comparisons can be formulated to assure that the DRM conditions for the act are satisfied. These comparisons must identify the following:

1. The Users and Licensees
    i. The user making the request
    ii. The principal (user or group of users) identified in the licences
2. The Act and the Rights
    i. The underlying process being done
    ii. The act covering that process
    iii. The acts covered by the licence
3. The resource
    i. The resource being address by the request
    ii. The resource or set of resources covered by the licences
4. The Licensor and Issuer
    i. The licensors authorized to issue licences for that resource
    ii. The part who issued the licence being presented by the User
5. The conditions and constraints associated to that act in the licence
    i. Parameters used for the act
        1. The constraints in the licences
        2. The parameters associated to or in the request
    ii. Other variables
        1. Variables in conditions and constraints
        2. The value of those variables for the request.

Table 3: Metadata verification and process authorization

Item	Reference in	Reference in	Comparison
User	User	Licence. Principal	User.ID must be equal to or a member of the group to whom the licence was issued.
Act	Process	Licence. Right	The act must be explicitly covered by the licence, or be a conformant implementation of a standards-based process referenced in a right.

Item	Reference in	Reference in	Comparison
Resource	Licence. Resource	Resource. Identity	Equal or consistent with a larger group.
Parameter Values	Process. Request	Licence. Constraints. Parameters	Consistency, usually as a containment test.
Issuer	Licence. Issuer	Resource. Owner	The licence must have been issued by the owner of the resource or by his agent. The owner → agent relation must be available to the Licence validation process.

Each right can be associated to conditions based on the semantics of the right. Once a right is established its definition cannot change without affecting existing licences. Therefore, once defined and accepted as a standard, a right shall not change in its meaning or structure. Each right defined in the schema shall maintain its fundamental definition in the documents associated to the schema. Each right defined in an external registry will carry a dated definition in that registry.

Further, once a licence is issued, it must not be changed (only the issuer prior to delivery may change a licence). A licence that needs to be modified shall be replaced by the issuer. This "frozen" nature of a licence is a fundamental part of the security and trust model within DRM, and once changed a licence is invalid.

A licence shall specify an Issuer. The Issuer of a licence must have the right to grant rights specified in the licence

9.2 User Metadata

The basic user metadata is identity. Participants in a DRM system (principals in terms of ISO 21000) shall be identified uniquely, so that associations by reference can be traced to them.

9.3 Properties and patterns

In this reference model for the informational viewpoint, property formalisms were chosen to support the evaluation of conditions. In such formalisms, descriptors are associated to base objects, as opposed to embedded within them in attribute formalisms. In implementations, either formalism may be used since carry the same information. The property formalisms are more appropriate here since the actual structure of abstract classes, types and interfaces are not known.

Property formalisms in implementations can be very flexible in handling ad hoc situations without the need to extend or modify classes. They have the disadvantage of requiring a more flexible and adjustable code, as structure is often being discovered at the same time that instance values are found. Implementations for document metadata using property formalism are quite common (for example, Microsoft® Office).

Attribute formalisms have the advantage of predetermined data structures, which can make a non-object-oriented code much simpler. The disadvantage is the lack of flexibility in ad hoc situations.

Patterns are collections of conditions that define collections of entities. As such, it is easy to match a pattern to a particular instance, but difficult to enumerate the set that the pattern defines. For example, it is easy to ask, “Is this principal a US resident?”, meaning that there must be a verifiable property attached to the principal declaring his citizenship or resident status, but it is difficult to ask, “Who are the US residents?”, so much so that the US government tries for an accurate list only once every 10 years, during the census, after which there is a constant debate as to its accuracy until the next one is taken.

All entities in this information model shall be “matchable” to patterns based on their attributes, properties and relations. All match requests return true if and only if verifiable information is available to assure a logical match. A failure to find such information shall always result in a “no match” or false result within or from the GeoDRM Gatekeeper.

9.4 Resource Metadata

9.4.1 General metadata

The geoinformation or geoprocessing resources that are the target of the licence shall be identified unambiguously. This identification can be used to target local copies properly labelled or by accessing or retrieving a global networked copy of the resource. As defined in **ISO 19109: Services**, this identification should be location transparent, so that local or cached copies of the resource are treated as if they were the global copy of the resource.

Some rights may be resource independent, in which case the resource part of a grant component may be unspecified.

9.4.2 GeoInformation resource metadata

When a resource is derived from the combination and/or modification of other resources, the new resource shall have appropriate metadata information associated to it that describes the processes and the parameter values used for those processes, which created the new resource

9.4.3 GeoProcessing resource metadata

In the paradigm discussed in Clause 6.3, processing resources are treated as resources not as acts. The application of a processing resource to another resource requires an execute right on the processing resource, and the appropriate right on the geoinformation as required by that processing resource’s metadata.

Geoprocessing resources shall be identified by a registered processing step or steps. The steps are “registered” if they are defined in a recognized standard or other publicly available specification (at any level of development), identified by both the name and the version of the specification; and recognized as such is a trusted public registry, either supported by OGC or some other recognized body. The processing must be executed by viable software that is conformant to the defining standard.

For a specification for which no conformance test exists, or for other reasons, the Licensors may grant access to non-proven implementations under a licence by a fully specified name or by specifying "ANY" that would allow any implementation to be used.

The default shall be to allow the licensed process to be carried out by any provably conformant implementation. Provably conformant means that the implementation is registered in a licensor-trusted registry, either globally, or locally.

The usual process identification will be by URL, URI, or URN that identify the processing address or the registry entry in a licensor-trusted registry

A service supplier may establish a special registry for any functionality that can manipulate GeoDRM extended resources. Such implementations shall be GeoDRM-enabled so that the licence metadata can be maintained.

9.5 Licence Metadata

9.5.1 Licence

A licence is defined in ISO 21000-5 as an "expression that is created by Principals to conditionally or unconditionally permit the same or other Principals to perform Rights upon Resources." A Right is an act identified by the licence subject to any conditions associated with it in the licence.

A licence is a sequence of grants. Each grant specifies a principal, which receives a right to act, and optionally, a resource upon which that right may be applied.

9.5.2 Principal or Licensee

Within a licence, most principal references within the rights grants may be patterns that are statements of the properties that would include a particular principal in the implied set of principals. This is not the case for the licensee, who is the principal actually contracted with the licensor (licensing agent) for the acquisition of the licence in question.

9.5.3 Grants

9.5.3.1 Semantics

The grants within a licence are the actual listing of rights “granted” by the licence. As such they shall include at least the following information:

- the person or persons to whom the rights is given,
- the resource upon which the right may be exercised,
- the rights which are granted, and
- any conditions that modify any of the above.

The GeoDRM Gatekeeper will be responsible for matching such grants with processing requests. Multiple resources may be involved in one request. Each grant in a licence may specify a separate resource. Consequently a request will only be authorized if, and only if, for each licensed resource in the request there is at least one grant, which match the particulars of the request, associated to the requestor in the licences.

9.5.3.2 Rights

9.5.3.2.1 Rights semantics

A Right is defined in ISO 21000-5 as "an act identified by an r:Right" which is an element of a licence. Rights may generally be classified into (but are not necessarily limited to) the following categories:

- Copyrights (©) that are legally defined rights granted to the original producer of certain types of works. They vary in nature between legal system, and not all entities of value are subject to copyright in a particular legal system.

- Ownership rights that are legally defined rights inherent in the act of producing the resource, possibly in conjunction with copyrights. The Owner is the root of most other right grants.

- Usage rights that are granted either by the owner or through legal mechanism (such as fair use in the United States) that allow principals to use a resource (entity) for some purpose. Each purpose is in effect a separate right.

- Meta-rights that are rights to grant rights.

- Management rights are those that perform acts on the entity as a whole without an interpretation of its meanings. Such rights might include copying, indexing, moving, change in formats or coordinate system. In such cases the actual resource is not used, but is only changed in format, location or inclusion in various aspects of a resource management systems.

9.5.3.2.2 Note on Multiple copies of resource and Rights names

When a resource exists in multiple identical copies, it may carry the same resource identity and be manipulated by licensees holding the appropriate rights on the resource. Any modification of the resource must result in a change of identity, and the addition of appropriate process metadata to aid in the tracking of rights back to the original resource owners (or their agents).

The requirements for name formats vary from implementation to implementation, and the names for rights used here are not meant to be normative. In proving conformance, an implementation specification should map its specified right names to the ones here.

9.5.3.2.3 Standards-defined operations

Processes defined by standards can be identified by associations with their "proof of compliance." Since integration with the GeoDRM system will require compliance with DRM standards, they will carry both base functionality proof and GeoDRM proof of compliance.

9.5.3.2.4 Usage Rights

9.5.3.2.4.1 Use right

The ***"Use"*** right allows a client to obtain a resource and have access to the information contained therein. It therefore subsumes all usage rights except Modify. Thus, many of

the rights in the sections to follow may be collectively given by a single "***Use***" right. This right may be defined as a collection of the rights, or may be defined in a stand-alone manner, even in the absence of the finer detailed usage rights.

9.5.3.2.4.2 View, Display, Print right

The "***View"*** right shall allow a licensee to view the resource as a map (properly scaled graphic representation, either vector or raster). This is the default minimal right, in that it is included almost universally in any licence that is of value. When the creation of derived or combined resource is allowed, the view right shall be licensable by the user holding the "derive" rights under which the resource was created. The limits of those licences may be restricted by that user's rights condition.

Since the usefulness of separating print, or display (such as from within an embedding document) from view is highly questionable; this specification does not distinguish between these. Implementation specifications may do so if the environments in which they work have a reason to do so. There is a technical issue that most browsers or other display software components are probably not DRM enabled and so separation of these rights may require acquisition of special display software to enforce them.

9.5.3.2.4.3 Combine, merge right

The "***Combine"*** right shall allow a licensee to integrate the resource with other resources in a map in the same coordinate reference system. All input resources must carry this same combine right and be of the same information type (e.g. all images, all maps, all feature collections).

9.5.3.2.4.4 Extract Resource or Copy right

The "***Extract Resource***" right shall allow a licensee to create a fully software-accessible local copy of all or part of the resource subject to further GeoDRM controls on the local systems in support of a specified simultaneous number of identified licensed users.

The "***Copy***" right shall allow a licensee to create one exact duplicate of the resource that can be stored locally subject to an equivalent right management system or for archival purposes. In this sense, the copy act is an extract resource act where the entire resource is extracted.

Conformant geoservers may automatically get an extract right to maintain levels of performance. In which case, the local GeoDRM Gatekeeper shall be required to make judgements on these local resources based on the licences available to specific users. The logic in this is conformant servers are qualified to maintain the integrity of the licence-to-resource relationship, and as such may act as a resource-provider agent of the owner without specific licence. This means that the required agent's licence would be included in the local grant context of the GeoDRM Gatekeeper.

9.5.3.2.4.5 Spatial Transform or Adjust right

The "***Spatial Transform***" right shall allow a licensee to create a fully software-accessible local copy of the resource in a new coordinate system subject to further GeoDRM controls on the local systems in support of a specified simultaneous number of identified licensed users. The type of coordinate system can be restricted by conditions placed on this right.

A slightly stronger "***Spatial Fit"*** or "***Adjust"*** allows a licensee to make minor adjustment in coordinates to fit an external source, such as a triangulated net or image. This is a

common process when overlaying vector data upon image or scanned raster. Depending on the requirements of the process and potentially dependent on the accuracy of the data, the fitting may be done to the vector, to the raster or to both.

9.5.3.2.4.6 Derive Resource or Further Develop right

The "***Derive Resource***" right shall allow a licensee to create (derive) resources which use the licensed resource as an identifiable part, subject to GeoDRM controls consistent with the original licence. Associated conditions on this right may modify the rights allowed to be licensed on the derived resource. Other rights that create new resources from existing ones may be included in the derive resource right.

9.5.3.2.4.7 Edit or Adapt right

The "***Edit"*** right shall allow a licensee to copy the resource into another resource in the original physical format and in the same coordinate reference system as the original, and to modify that new resource through edits. The "***Adapt"*** right shall allow a licensee to use the resource in the creation of a new resource that may incorporate the original resource in whole or in part.

This right extends to other coordinate reference systems if and only if a Spatial Transform or Adjust right is also granted in the same or a compatible licence.

Since the new resource set is not the same as the original resource set, new source metadata should be associated to the edit portions of the copy of the resource.

9.5.3.2.4.8 Modify Right

The "***Modify"*** right shall allow a licensee to edit the original resource set. In essence, this is the Edit or Adapt right with the additional capability to replace the original.

Since the new resource set is not the same as the original resource set, new source metadata should be associated to the edit portions of the copy of the resource.

If the resource identity includes a changeable date, then the original identity of the resource can be kept. The DRM system should allow interactions with distributed resource systems that allow all permanent "licensed" copies of the resource to be updated. The precise semantics of this temporal interaction is an implementation specification option.

Ownership rights of the modified resource would follow the codicils of the licence, but the default logic would be that the ownership remains unchanged.

9.5.3.2.4.9 Derive Graphic right

The "***Derive Graphic"*** right shall allow a licensee to create separate resources that correspond the transient views in View and Combine, subject to maintenance of a metadata trail back to the origin of the underlying resource.

9.5.3.2.4.10 Encode right

The "***Encode***" right shall allow a licensee to copy the original resource into a different type of encoding or representation. Conditions on format associated to this right shall specify which formats are allowable and which are explicitly excluded.

9.5.3.2.4.11 Execute right

The "***Execute***" right shall allow a licensee to use a processing resource to act on one or more other resources. For a request to be validated, execute rights must be found for the processing resource being used and for each parameter. If a parameter resource licence needs, it may reference the parameter by name.

9.5.3.2.5 Meta-rights

9.5.3.2.5.1 Semantics

Meta-rights are rights associated to the granting or lending of licences to others based on grants through a valid licence chain of agency from the owner of the resource.

9.5.3.2.5.2 License right

The "***License***" right allows the principal holding the licence grant to grant others licences against the resource. The type of licences so granted shall be subject to conditions on the right grant.

Note that the license right to grant a more basic right is not the same as the basic right. This means that a Licensing Agent of the Owner may be able to sell "view" licences to others, but unable to view the resource himself. Of course there would be little in the way of the agent from granting such a licence to himself, but that licence would be subject to the same conditions of any other licence so granted. So, in that case, the hypothetical agent would be subject to the same fees, constraints and conditions as his clients.

9.5.3.2.5.3 Sublicense

The "***Sublicense***" right allows the principal holding the licence grant to loan that right to others. The loaned licence will have no more rights than the original one, and shall be subject to conditions on the grant.

9.5.3.3 Conditions

9.5.3.3.1 Semantics

Conditions specify limitations on rights. The following can be specified for any of the rights specified above.

9.5.3.3.2 Property conditions and Grant Component patterns

Any grant component can carry a set of named properties and operations (see the UML model). Any of these may be used in a licence to restrict the grant component in any way. For example, if we wish to grant everyone in the UK a right for a fixed period of time then the following grant structure may be used:

- Grant
    - Principal
        - →location “Is Contained In” UK
        - Local NOW “Is Before” 1 January 2010
    - Resource = …
    - Right = view …

This would grant any principal holding a location property that is spatially inside the UK to view the resource up until the first day of the year 2010 CE. Note the “→” notation used above is meant to parallel “dot” notation used in Object Basic programming languages, which is a context-sensitive object navigation, i.e. tracing a “[blank].” form to the context of the block. So in the 3rd line above, the “→location” means the “Principal→location” property.

For the purpose of this “property checking” some global variables shall be made available to the GeoDRM Gatekeeper. These include but are not limited to:

- the time and date (local and GMT),
- the identity of the requestor,
- the location of the GeoDRM Gatekeeper, and
- any others as defined by the implementation specification.

9.5.3.3.3 Standards-defined operations

Processes defined by standards can be identified by associations with their "proof of compliance". Since integration with the GeoDRM system will require compliance with DRM standards, they will carry both base functionality proof and GeoDRM proof of compliance.

9.5.3.3.4 Output conditions

The licence may place conditions on the state of any “new” resource for each act (associated to a right) and for each named output of that act. The format of those conditions will usually be the assignment of meta-rights and properties for this new resource.

So, if a grant defines a right “view” that produces an output map and for “extract” that produces an output resource, then the grant may use the following structure:

- Grant
    - Principal = …
    - Resource = …
    - Right = view
        - Output→map
            - →Meta-rights = {view}
            - →Meta-data
                - →Disclaimer contains “This map contains privately own data of the UK Ordnance Survey.”
                - →Creation Date = NOW
    - Right = Extract
        - Output→resource
            - →Meta-rights = {view, extract}
            - →Meta-data
                - →Disclaimer contains “This information contains privately own data of the UK Ordnance Survey.”
                - →Creation Date = NOW

9.5.3.3.5 Transfer Right and Sublicense conditions on meta-rights

Meta-rights that allow one principal to enable another principal with grants, either as a licence or sublicence, may be restricted by the type of right so conveyed, or the persons or type of persons to whom the right may be conveyed. So a grant may contain the following type of structure:

Copyright © 2006 Open Geospatial Consortium, Inc. All Rights Reserved.

- Grant
    - Principal = …
    - Resource = …
    - Right = view …
    - Right = extract …
    - Right = sublicense
        - Transfer = view
        - Sublicensee→organization = Principal→organization
    - Right = extract
        - Output→Resource
            - →Licence→"contains right"= {view}

In this case the original licensee would have view and extract rights but could only sublicense view to anyone, and sublicense extract to members of his own organization.

Other restrictions could be placed on these rights through property conditions.

9.5.3.3.6 Spatial Temporal Conditions

A spatial condition may limit the spatial or temporal extent of the resource that the actions allowed by the right may address. The expression of a spatial or temporal or spatiotemporal extent may be in any coordinate reference system or may cover multiple reference systems for subsets of the coordinates. The default CRS is WGS 84 Latitude-Longitude (the CRS used by GPS), and the default temporal reference system is Universal Time (Zulu) (the TRS used by GPS).

The semantics of the condition shall be specified. The parameter that is restricted should be explicitly given. For example, a pure temporal condition might indicate but is not restricted to one of the following:

- Restrict access to resource originally collected within the time limits.
- Restrict access to resource entered into the resource within the time limits.
- Restrict access to the resource to the time limits.

For example, a pure spatial condition might indicate but is not restricted to one of the following:

- Restrict access to resource collected from within these limits.
- Restrict access to users currently located within these limits.

9.5.3.3.7 Layer conditions

Layer conditions shall be used to limit what resource layers that can be used or modified in conjunction with a right. For resources, this shall subset the resource based on internal layer structures. For processing rights, this shall determine what types of layers shall be processible by the software, possibly regardless of the underlying resource.

For example, the right to use an image processing service might be restricted to “visible light” layers. The right to use a navigation service might be restricted to road layers appropriately augmented with network connectivity associations. Some examples are given below.

The Massachusetts Roads Maintenance Agency is given the right to modify the roads layer of a combined New England database, as long as the records modified are part of Massachusetts road system, by the following grant form:

- Grant
    - Principal = Massachusetts Roads Maintenance Agency
    - Resource = Combined New England SDI
        - →Layer = Roads…
    - Right = modify
        - Input→location “is contained in” Massachusetts

The Massachusetts Emergency Dispatch is given the right to use navigation services against the roads layer of a combined New England database, as long as the records used are part sufficient for use by navigation systems, by the following grant form:

- Grant
    - Principal = Massachusetts Emergency Dispatch
    - Resource = Combined New England SDI
        - →layer = Roads
        - →“accepted use” = navigation
    - Right = execute
        - Process
            - → Compliance = URN:OGC:NAVIGATE

9.5.3.3.8 Implementation conditions

Implementation rights shall be used to specify which implementations of functionality may be used in using a right. If unspecified, any provably conformant implementation of the functionality is allowed. If specific implementations are identified they may be allowed or disallowed specifically.

This may be part of the trust model of the resource owner. For example, a company may wish to assure itself of the safety of the DRM by individually testing applications for what they consider a level of security. In this case, the company may put up an online directory of software implementations that have passed this rigid test, and the licences it issues of its resource might explicitly reference this online resource as the authority for what is to be considered “conformant” applications. More popular should be the restriction of a processing right to those implementations that are registered as

conformant by the standards associated testing authority. Thus, one licensor may require that his resource only be served with an OGC-compliant implementation listed in the OGC registry supported by the Open Geospatial Consortium.

The default assumption is "open world" that is, all conformant implementations are allowed unless specifically disallowed. If this is not the intent, the licence should specify a "NULL" specification-based right, and then specifically allow other implementations. An unmodified "NULL" specification effectively nullifies the right.

9.5.3.3.9 Parameter Range conditions

In functional rights that pass parameters, the allowable range of any parameter may be limited. The format of the range is type specific. For parameters that do not have any ordering or dimensional structure, the usual representation is a "white space separated" list of values. Values with internal white space should be quoted or the white space escaped appropriately for the licensing encoding mechanism being used. For ordered or dimensionally structured parameters, a set of ranges or extents should be specified in accordance to the semantics of the parameter type.

For example, to change an earlier example to only allow viewing of Boston roads, assuming the view parameters are layer, extent and style, then the following grant could be used:

- Grant
    - Principal = …
    - Resource = …
    - Right = view
        - →extent “is contained within” Boston

9.5.3.3.10 Derived Right conditions

If the right to derive resources is granted then the condition DerivedRight may be used to restrict or expand the rights that may be licensed by the creator of the derived resource in conjunction with the derived resource.

For example, if a feature resource supplier wishes to assure the manner in which his resource is used “second hand” through another process, then he may require the derived right to be “view only with citation”. This might use a licence pattern such as follows:

- Grant
    - Principal = …
    - Resource = …
    - Right = view
        - →metadata “contains citation” Licensor→citation

Another user wishing to use the same resource would then be forced to go to the original source since the first user could not convey rights other than view to his derived resource.

For this reason, any derived right shall implicitly include the right to view a graphics rendition of the resource.

- Grant
    - Principal = …
    - Resource = …
    - Right = extract
        - →metadata “contains citation” Licensor→citation

9.5.3.3.11 Encoding condition

If a right to duplicate or derive resources is given, the Encoding condition may restrict the form in which the particular resource may be presented. If absent, the default logic of the condition is that all lossless encodings are allowed.

Encoding conditions may apply to any aspect of the encoding or presentation processes. For example, if an image is originally spectrally encoded (such as an RGB for visible light), then the licensor may choose to reject transformation of that into HSI (hue, saturation, intensity) encodings.

- Grant
    - Principal = …
    - Resource = …
    - Right = encode
        - →format is not HSI

9.5.3.3.12 Side effect conditions

The use of a right may have side effects listed in the contract. To support this, each right may be associated to the conditions that cause the GeoDRM Gatekeeper to add processes to the process flows. The return value of these extra processes may affect the completion of the action.

Precondition side effects may execute extra checks on the licence, may cause extra validation on the resource or be linked into the billing system of the Licensor.

Postcondition side effects may cause extra validation on the output resources or be linked into the billing system of the Licensor. Such conditions may use the following grant structure

- Grant…
    - Right
        - Condition Side Effect
            - →Time = before use
            - →Service Request (… Text of request …)

- Condition Side Effect
  - →Type = test
  - →Time = before use
  - →Service Request (… Text of request …)
    - Return = True
- Condition Side Effect
  - →Time = after completion
  - →Service Request (… Text of request …)

9.5.4 Issuer

The issuer of the licence identifies the entity that created and built this licence. The Issuer is the last entity allowed to modify a licence. Once issued, the licence shall not be modified by anyone. Changes to a licence shall be accomplished by a new licence being issued.

The issuer must have the rights to issue licences for his licences to be valid. This means that an Issuer is the owner of the resource or a representative of the owner of the resource and is either acting in his name or as his agent.

The following of this rights chain back to the "owner" is the responsibility of some entity playing the Licence manager role.

To perform these functions, the issuer shall be associated to metadata on his identity and his relations as agents of others, in particular, his agency or chain of agency for the owners of the resources for which he grants licences.

9.6 Process metadata

Process metadata describes processes, such as services and software. It is used to identify each process implementation for licensing, either as licensing for the process itself or for the use of that process on a particular resource. It is also used as resource metadata to track the processing history of that resource.

In general, a processing resource can become part of a DRM system in one of two basic manners (albeit, variations are possible and acceptable). First, the process can be an implementation of a DRM standard, which makes it DRM aware. Such processing resources are called “trusted” in the sense that they do not break any DRM rules that would allow DRM aspects to be bypassed. Second, the process may be isolated within a DRM system that controls all of its communication with outside entities, acting as a “rights firewall” preventing resource leakage into uncontrolled environments. This second type is DRM embedded.

Annex A
Abstract Test Suite

A.1 Items covered

This standard creates conceptual requirements for the following:

1. Rights expression languages.
2. Metadata for identification of principals, processes, rights and resources.
3. GeoDRM Gatekeeper components for use in protection and enforcement systems, including GeoDRM as a requirement.

A.2 Rights expression languages

Rights expression languages are used to create GeoLicences with unambiguous meanings, as specified in this standard.

A rights expression language (REL) conformant to the standard must support the rights model defined in Clause 9.5.3.2 Rights. It must further integrate with at least one other rights expression language that covers non-geographic entities that are encountered in GI systems.

A.3 GeoDRM Metadata systems for GeoDRM

A GeoDRM metadata system, as a subsystem of a GI system shall assure that metadata associated to the maintenance of rights associated to GI are preserved. For a GeoDRM metadata system to be fully conformant, it shall be difficult to a stated degree to violate a GeoLicence within its control.

A.4 GeoDRM Gatekeeper

A GeoDRM protection and enforcement system is a security system that prevents any act unless supported by a licence; either a general public licence for those acts open to all users, or a more specific licence whose principal range is limited. It must be, or contain, a compliant GeoDRM metadata system and a GeoDRM Gatekeeper. It must include specification for:

- a rights expression language,
- a condition expression language (possibly based on SQL or OQL),
- a GeoDRM Gatekeeper specification, and
- a GeoDRM Metadata specification.

Annex B (informative)
GeoDRM UML Model

B.1 Semantics

The following UML model represents a valid interpretation of the information model presented in Clause 9, Information Viewpoint.

UML 2.0 definitions of interface were used. If a translation to UML 1.5 or earlier is desired, all stereotyped <<interface>> classifiers should be changed to stereotype <<type>>. The two models under the two versions of UML will be logically equivalent.

The rest of this annex is a documentation format provided by a UML tool (Enterprise Architect, from SparxSystems, Ltd. Australia (http://www.sparxsystems.com.au/). It has been edited for format, but the content reflects the GeoDRM model posted on the Open Geospatial Consortium portal.

Alternative UML models consistent with Clause 9, Information Viewpoint are possible, but they should be information equivalent to the one contained here.

Copyright © 2006 Open Geospatial Consortium, Inc. All Rights Reserved.

B.2 Class Diagrams

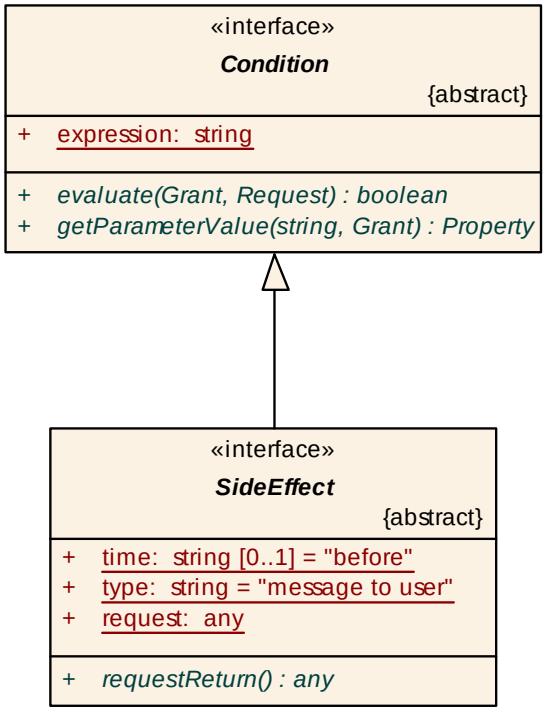

Figure B – 1: Condition

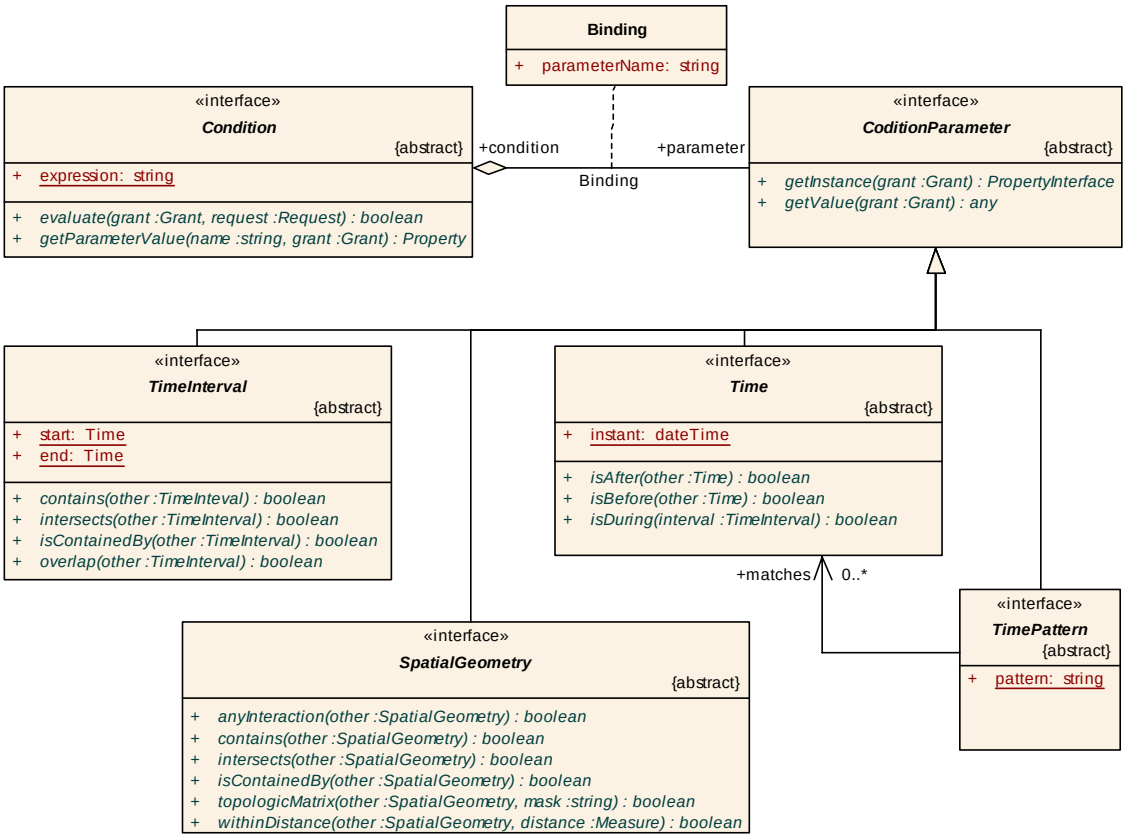

Figure B – 2: Condition Binding

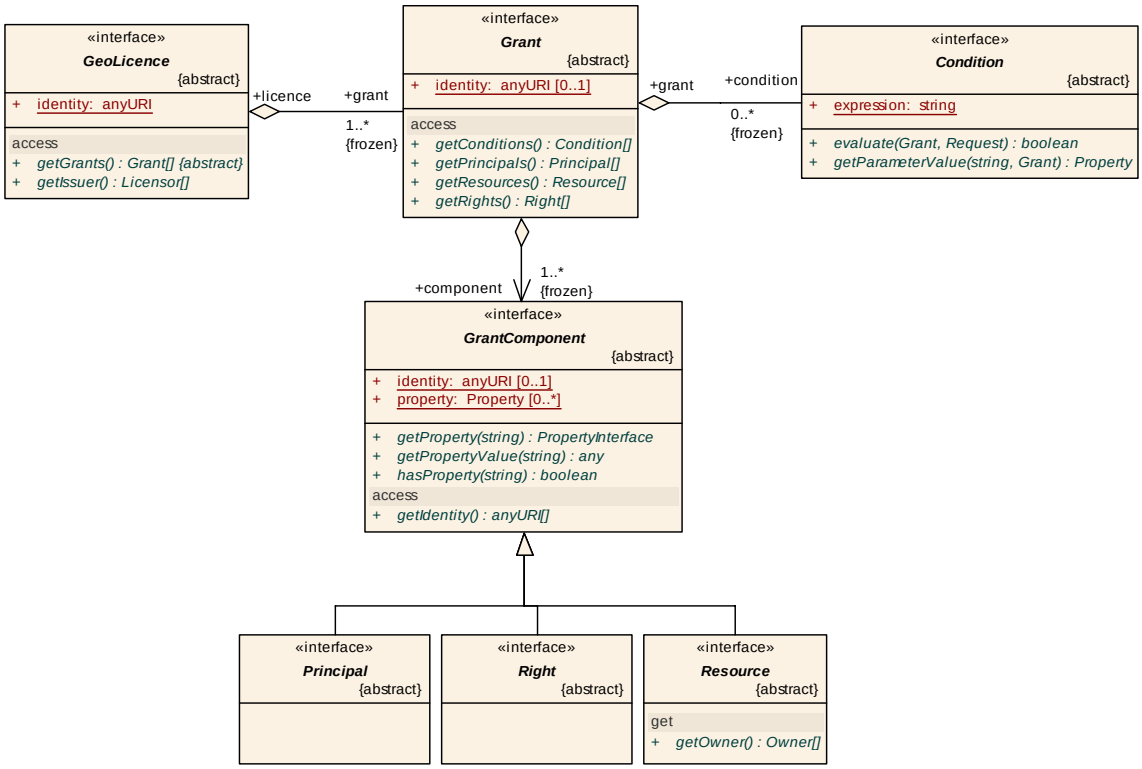

Figure B – 3: Grant

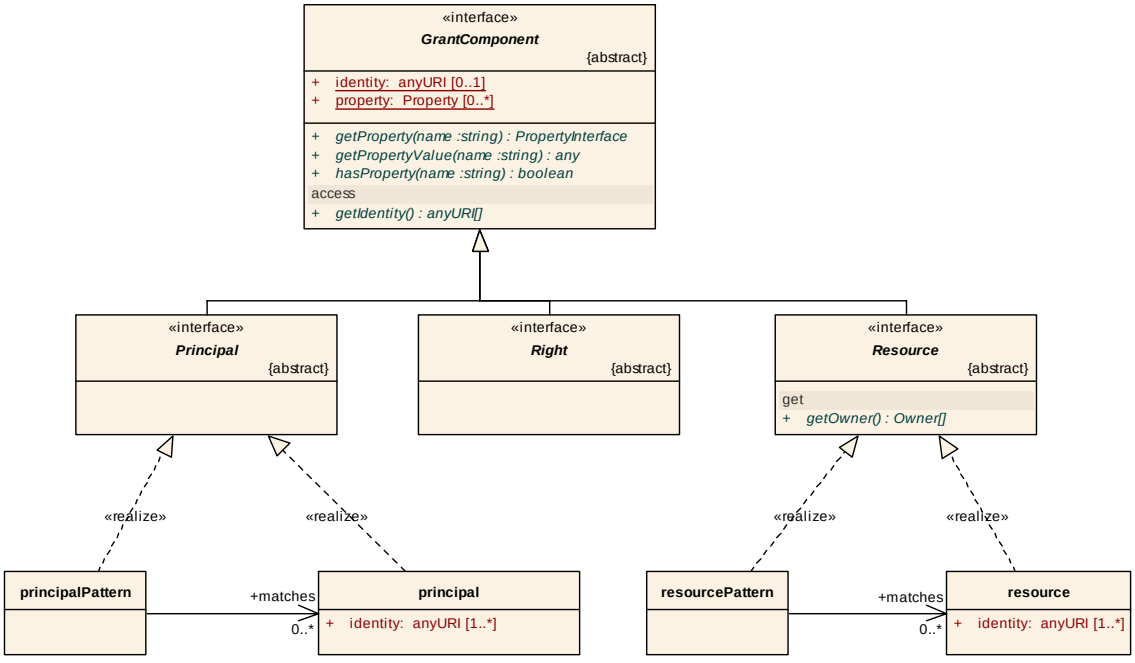

Figure B – 4: Grant Components: Principal, Right, and Resource

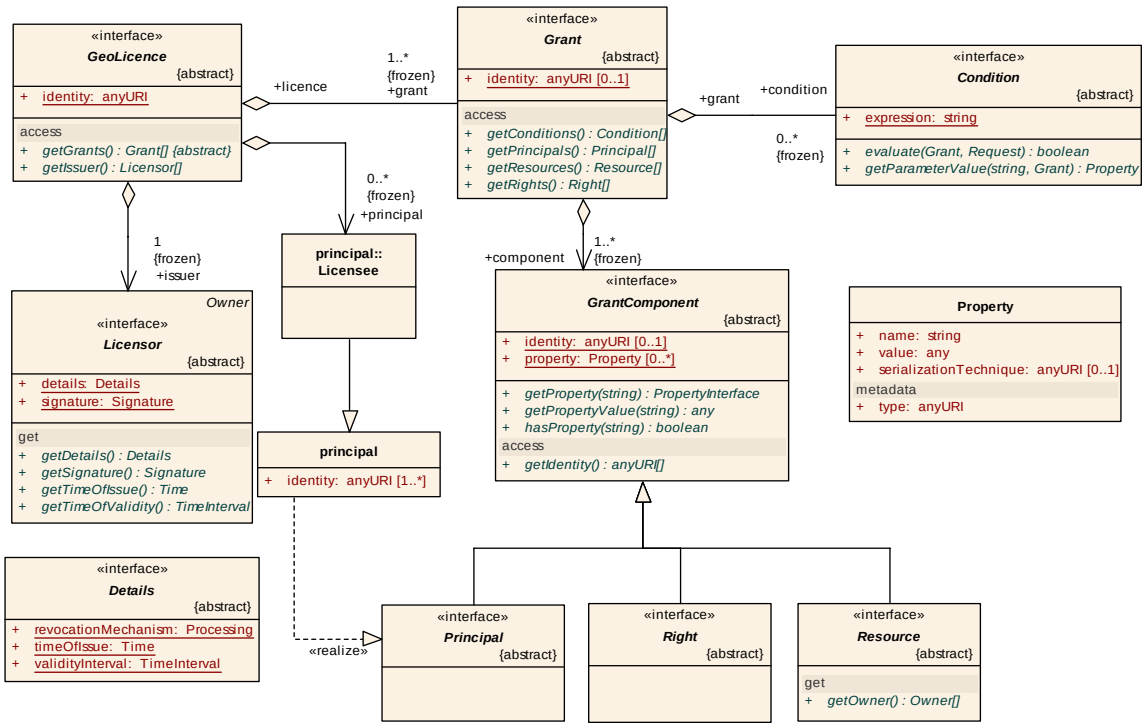

Figure B – 5: Licence

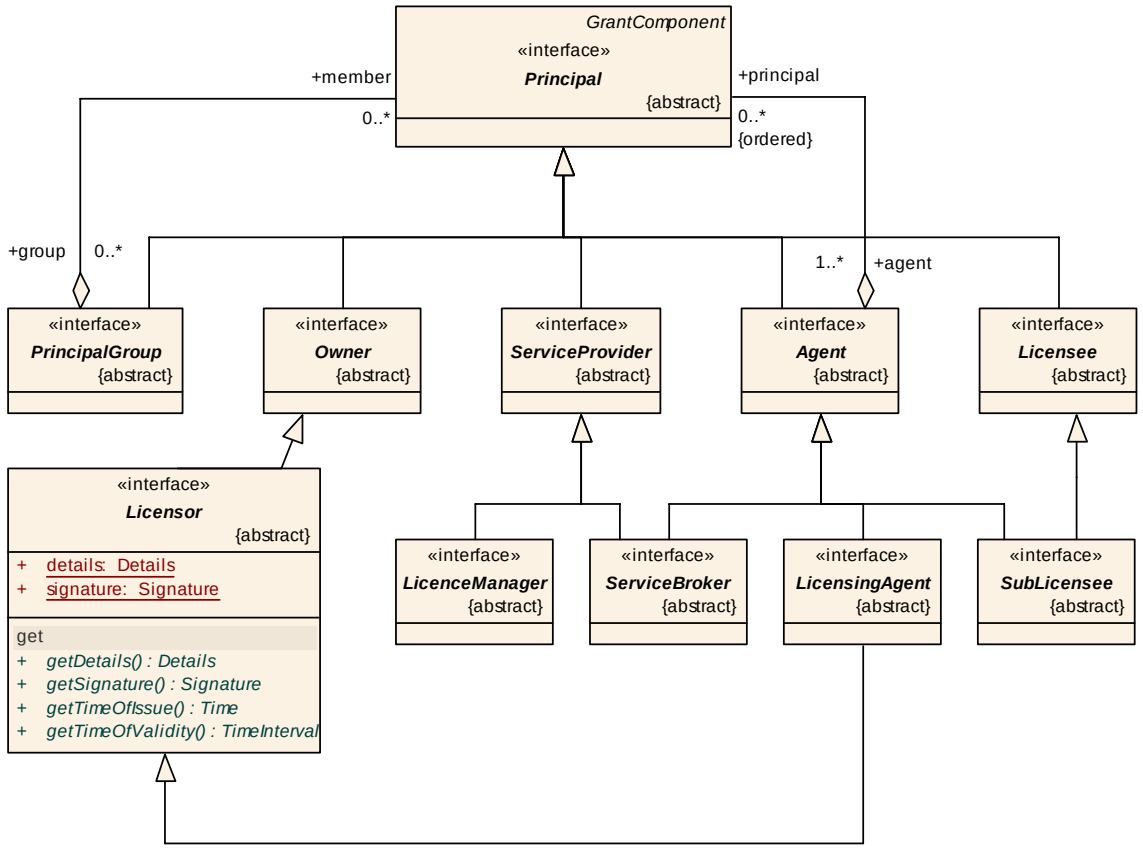

Figure B – 6: Principal

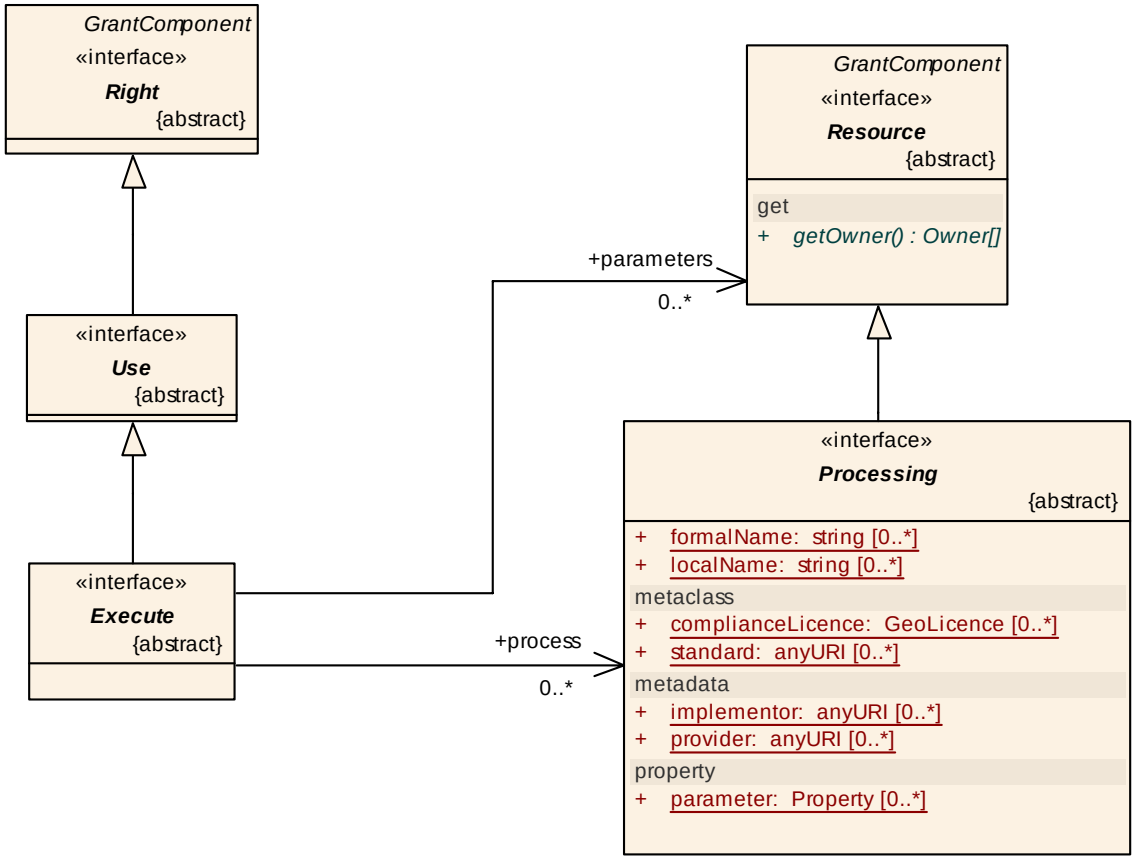

Figure B – 7: Processing Right

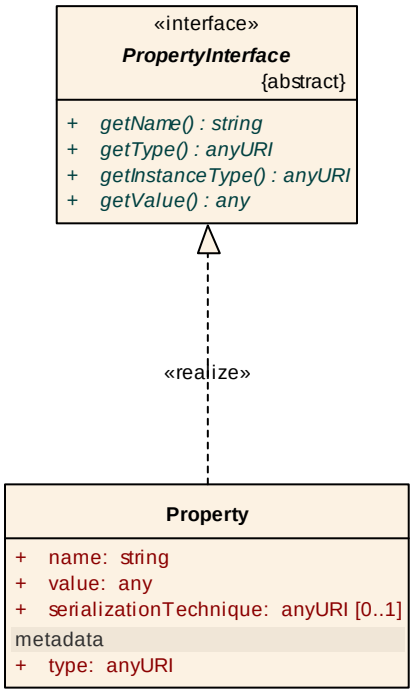

Figure B – 8: Properties

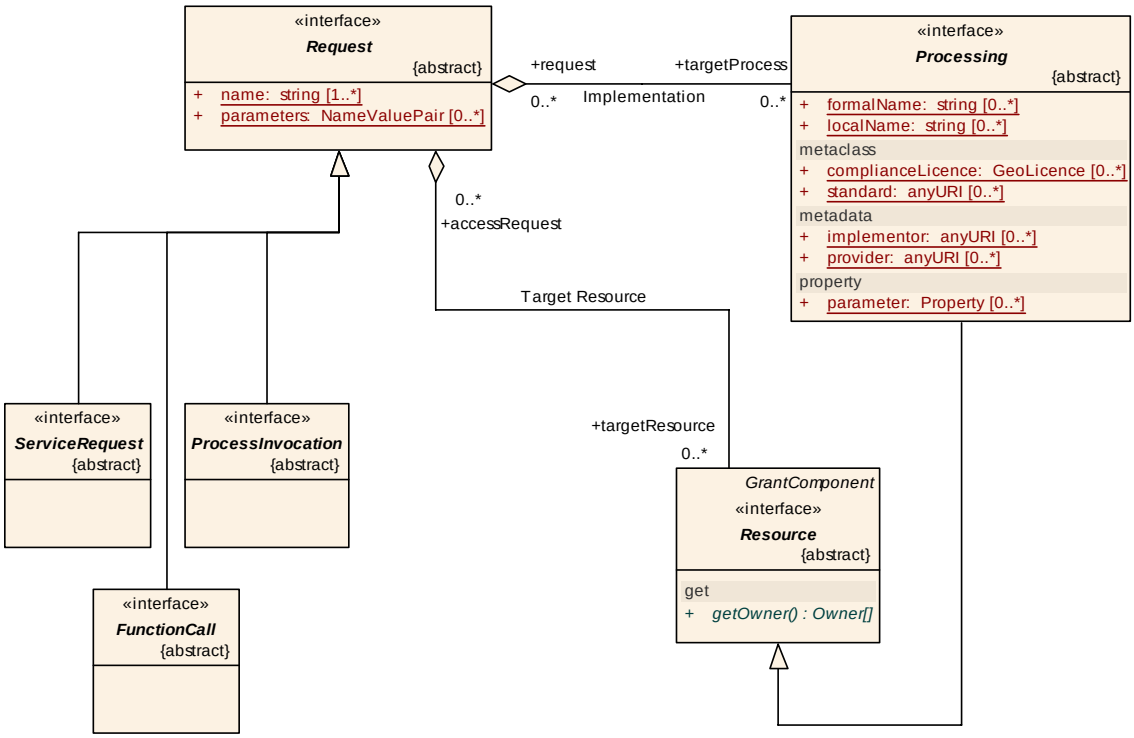

Figure B – 9: Request

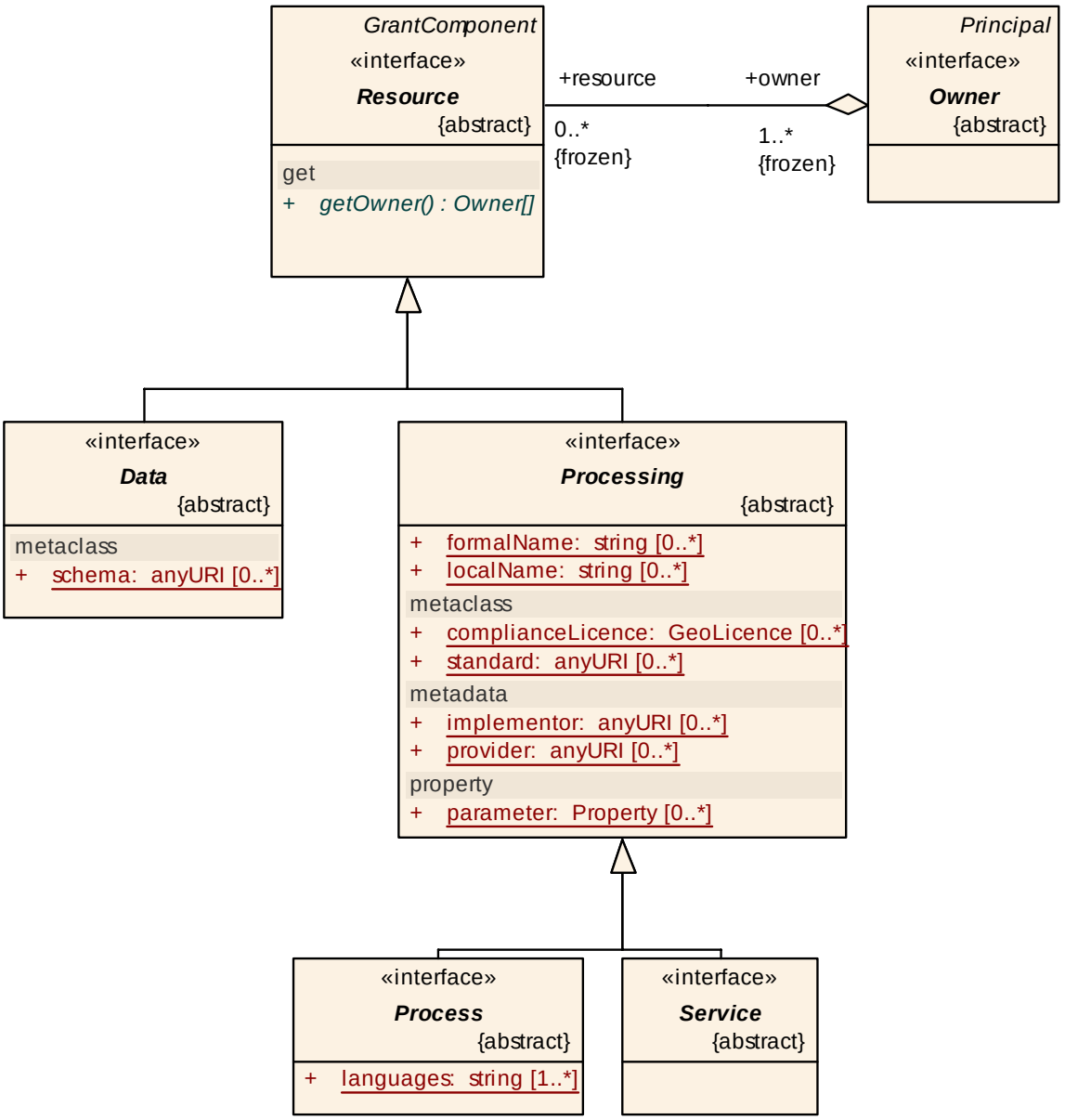

Figure B – 10: Resources

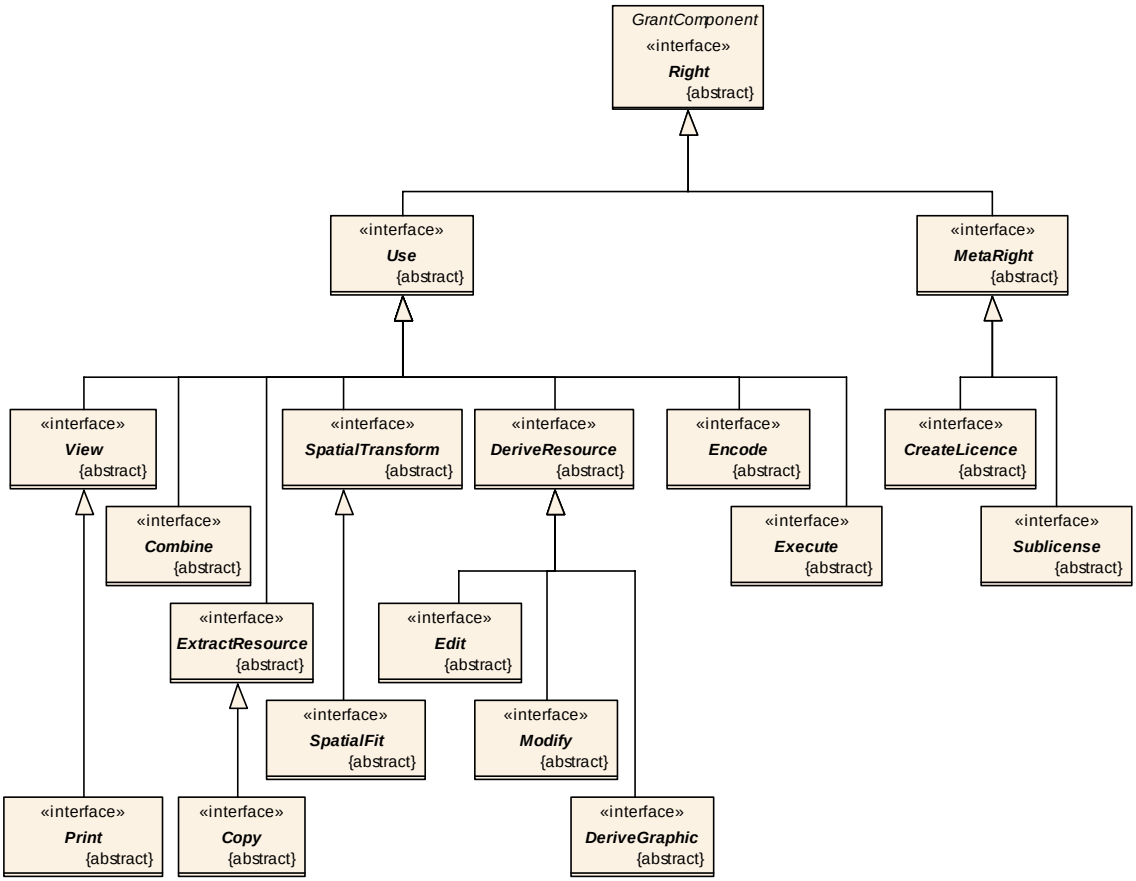

Figure B – 11: Rights

B.3 Bind

Type: *public* **Class**

Package: GeoLicence

B.4 Binding

Type: *public* **Association Class**

Package: GeoLicence

Each association between a condition and a parameter value (entity instance) must be indexed by the name of the parameter in the condition expression before the condition can be evaluated.

Table B – 1: Binding Attributes

Attribute	Type	Notes

parameterName	public : *string*	

B.5 principal

Type: *public* **Class**
Implements: *Principal.*

Package: GeoLicence

The principal abstract class is a concrete single principal, as opposed to a pattern defining a set of principals. It is used wherever a pattern is inappropriate.

Table B – 2: principal Connections

Connector	Source	Target	Notes
Association source > target	principalPattern unordered	principal +matches 0..*, unordered	
Generalization source > target	Licensee Child	principal Parent	
Realization «realize» source > target	principal Child	Principal Parent	

Table B – 3: principal Attributes

Attribute	Type	Notes
identity	public : *anyURI [1..*]*	

B.6 principal::Licensee

Type: *public* **Class**
Extends: *principal.*

Package: GeoLicence

A licensee is used in a licence to indicate the actual purchaser of the licence. The grants in the licence will use this principal as the default recipient of each grant. If a grant contains a principal, it overrides the licensee as recipient of the grant.

Table B – 4: principal::Licensee Connections

Connector	Source	Target	Notes
Aggregation source < target	Licensee +principal 0..*, unordered, frozen *Notes* Principal to whom the licence was given.	GeoLicence unordered	
Generalization source > target	Licensee Child	principal Parent	

B.7 principalPattern

Type: *public* **Class**
Implements: *Principal.*

Package: GeoLicence

Table B – 5: principalPattern Connections

Connector	Source	Target	Notes

Association source > target	principalPattern unordered	principal +matches 0..*, unordered	
Realization «realize» source > target	principalPattern Child	Principal Parent	

B.8 Property

Type: *public* **Class**
Implements: *PropertyInterface.*

Package: GeoLicence

A property descriptor entity describes the value of a property. They can be associated to or contained in any item.

Table B – 6: Property Connections

Connector	Source	Target	Notes
Realization «realize» source > target	Property Child	PropertyInterface Parent	

Table B – 7: Property Attributes

Attribute	Type	Notes
name	public : *string*	
type «metadata»	public : *anyURI*	

value	public : *any*	
serializationTechnique	public Range:0 to 1: *anyURI*	

B.9 PropertyType

Type: *public «metaclass»* **Class**

Package: GeoLicence

B.10 resource

Type: *public* **Class**
Implements: *Resource.*

Package: GeoLicence

Table B – 8: resource Connections

Connector	Source	Target	Notes
Association source > target	resourcePattern unordered	resource +matches 0..*, unordered	
Realization «realize» source > target	resource Child	Resource Parent	

Table B – 9: resource Attributes

Attribute	Type	Notes

identity	public Range:1 to *: *anyURI*	

B.11 resourcePattern

Type: *public* **Class**
Implements: *Resource.*

Package: GeoLicence

Table B – 10: resourcePattern Connections

Connector	Source	Target	Notes
Association source > target	resourcePattern unordered	resource +matches 0..*, unordered	
Realization «realize» source > target	resourcePattern Child	Resource Parent	

B.12 Agent

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *Principal.*

Package: GeoLicence

An Agent is a principal acting in another's name. As such an agent must also support the interfaces of his "client", the principal for whom he acts.

Table B – 11: Agent Connections

Connector	Source	Target	Notes

Aggregation source > target	Principal +principal 0..*, ordered, none	Agent +agent 1..*, unordered	
Generalization source > target	SubLicensee Child	Agent Parent	
Generalization source > target	Agent Child	Principal Parent	
Generalization source > target	ServiceBroker Child	Agent Parent	
Generalization source > target	LicensingAgent Child	Agent Parent	

B.13 ConditionParameter

Type: *public abstract «interface»* **Interface** {abstract}

Package: GeoLicence

Condition parameters objects are the bindings of the fully qualified names found in the condition expression. Once the names have been identified and the appropriate values found, they are typecast as parameter classes and evaluated by the operations of the parameter classes.

Table B – 12: ConditionParameter Connections

Connector	Source	Target	Notes
Association Binding	Condition +condition unordered	ConditionParameter +parameter unordered	

Generalization source > target	Time Child	ConditionParameter Parent	
Generalization source > target	SpatialGeometry Child	ConditionParameter Parent	
Generalization source > target	TimePattern Child	ConditionParameter Parent	
Generalization source > target	TimeInterval Child	ConditionParameter Parent	

Table B – 13: ConditionParameter Interfaces

Method	Type	Notes
getInstance (*Grant*)	public: *PropertyInterface*	param: grant [Grant - in]
getValue (*Grant*)	public: *any*	param: grant [Grant - in]

B.14 Combine

Alias: Merge

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *Use.*

Package: GeoLicence

The combine right allows the combination of the resource with other resources as long as coordinate systems and type are compatible.

Table B – 14: Combine Connections

Connector	Source	Target	Notes
Generalization source > target	Combine Child	Use Parent	

B.15 Condition

Type: *public abstract «interface»* **Interface** {abstract}

Package: GeoLicence

The Condition puts further restrictions on the right being granted. For an act to be valid, the Boolean function represented by the condition expression must evaluate to TRUE. This Boolean can test any values in the grant and their associated metadata, any parameters passed with the requests, metadata on the requestor, and on the process being used.

Table B – 15: Condition Connections

Connector	Source	Target	Notes
Aggregation	Condition +condition 0..*, unordered, frozen	Grant +grant unordered	
Association Binding	Condition +condition unordered	ConditionParameter +parameter unordered	
Generalization source > target	SideEffect Child	Condition Parent	

Table B – 16: Condition Attributes

Attribute	Type	Notes
expression	public static : *string*	The expression is a logical statement that evaluates to a TRUE, FALSE or INDETERMINATE (should be an error). Each variable in the statement should map to elements or attributes of grants to which this condition is applied, to the resource, to the user making the request, or to the request being made. Evaluation of any of the conditions associated to a right to false or indeterminate will invalidate the use of that licence grant in the given circumstances.

Table B – 17: Condition Interfaces

Method	Type	Notes
evaluate (*Grant*, *Request*)	public: *boolean*	param: grant [Grant - in] param: request [Request - in] The operation "evaluates" the condition based on the current circumstances presented to the GeoDRM Gatekeeper. The evaluation of any condition associated to a grant would invalidate the use of that grant to authorize an act. The failure of all grants to validate a right to act, would normally cause the GeoDRM Gatekeeper to invalidate the request presented to it.
getParameterValue (*string*, *Grant*)	public: *Property*	param: name [string - in] param: grant [Grant - in]

B.16 Copy

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *ExtractResource.*

Package: GeoLicence

Table B – 18: Copy Connections

Connector	Source	Target	Notes
Generalization source > target	Copy Child	ExtractResource Parent	

B.17 CreateLicence

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *MetaRight.*

Package: GeoLicence

Table B – 19: CreateLicence Connections

Connector	Source	Target	Notes
Generalization source > target	CreateLicence Child	MetaRight Parent	

B.18 Data

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *Resource.*

Package: GeoLicence

A Data resource is, as the name implies, data. Metadata associated to the Data resources include the owner of the data (for licensing purposes) and any schema information. Other Metadata may also be available. The schema can be used to select parts of a Data resource based on query. These parts can be specified in a licence by using conditions equivalent to the selection query.

Table B – 20: Data Connections

Connector	Source	Target	Notes
Generalization source > target	Data Child	Resource Parent	

Table B – 21: Data Attributes

Attribute	Type	Notes
schema «metaclass»	public static Range:0 to *: *anyURI*	The "schema" attribute allows the Data resource to specify its structural metadata. All data entities in the resource must have their structure defined in one of the schemas in this list.

B.19 DeriveGraphic

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *DeriveResource.*

Package: GeoLicence

The “derive graphic” right allows a user to create a graphic image (usually raster, although vector data is possible) that is a view-only representation of some subset of the original resources.

Table B – 22: DeriveGraphic Connections

Connector	Source	Target	Notes
Generalization source > target	DeriveGraphic Child	DeriveResource Parent	

B.20 DeriveResource

Alias: FurtherDevelop

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *Use.*

Package: GeoLicence

The derive right allows the user to apply analysis or other processes to the data, and create new resources. There may be restrictions as to which processes are allowed during the creation of these new resources.

Table B – 23: DeriveResource Connections

Connector	Source	Target	Notes
Generalization source > target	Edit Child	DeriveResource Parent	
Generalization source > target	Modify Child	DeriveResource Parent	
Generalization source > target	DeriveResource Child	Use Parent	
Generalization source > target	DeriveGraphic Child	DeriveResource Parent	

B.21 Details

Type: *public abstract «interface»* **Interface** {abstract}

Package: GeoLicence

Table B – 24: Details Attributes

Attribute	Type	Notes
revocationMechanism	public static : *Processing*	Process for revocation of the licence.
timeOfIssue	public static : *Time*	Time the licence was issued.
validityInterval	public static : *TimeInterval*	The "validityInterval" attribute describes the time period for which the licence is valid.

B.22 Edit

Alias: Adapt

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *DeriveResource.*

Package: GeoLicence

The edit right allows the user to copy the original resource and make changes to the data. This is a new resource with a new identity, and is subject to conditions on how rights are granted on it.

Table B – 25: Edit Connections

Connector	Source	Target	Notes
Generalization source > target	Edit Child	DeriveResource Parent	

B.23 Encode

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *Use.*

Package: GeoLicence

Table B – 26: Encode Connections

Connector	Source	Target	Notes
Generalization source > target	Encode Child	Use Parent	

B.24 Execute

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *Use.*

Package: GeoLicence

The execute right allows the user to execute a specified process on a specified set of resources. To execute a process on an information resource, the user must have an "execute" licence for both the process (which specifies which resources it may process) and the information resource (which will specify which processes may be executed on it).

Table B – 27: Execute Connections

Connector	Source	Target	Notes
Association source > target	Execute unordered	Processing +process 0..*, unordered	
Association source > target	Execute unordered	Resource +parameters 0..*, unordered	
Generalization source > target	Execute Child	Use Parent	

B.25 ExtractResource

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *Use.*

Package: GeoLicence

The extract right allows the user to subset a resource to create a new resource, usually a local copy, and always with a new identity. Metadata on the new resource should always trace the ancestry of the data back to the original resource.

Table B – 28: ExtractResource Connections

Connector	Source	Target	Notes
Generalization source > target	Copy Child	ExtractResource Parent	
Generalization source > target	ExtractResource Child	Use Parent	

B.26 FunctionCall

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *Request.*

Package: GeoLicence

Request implemented by a function call in an API.

Table B – 29: FunctionCall Connections

Connector	Source	Target	Notes
Generalization source > target	FunctionCall Child	Request Parent	

B.27 GeoLicence

Type: *public abstract «interface»* **Interface** {abstract}

Package: GeoLicence

The GeoLicence grants rights against digital resources, and has facilities to describe the geographic aspects of these grants.

Table B – 30: GeoLicence Connections

Connector	Source	Target	Notes
Aggregation	Grant +grant 1..*, unordered, frozen	GeoLicence +licence unordered	

Aggregation source < target	Licensor +issuer 1, unordered, frozen *Notes* Principal who composed the licence. The issuer of a licence must have the right to create and grant the licence in question. All such rights flow from the owner or from one of his agents.	GeoLicence unordered	
Aggregation source < target	Licensee +principal 0..*, unordered, frozen *Notes* Principal to whom the licence was given.	GeoLicence unordered	

Table B – 31: GeoLicence Attributes

Attribute	Type	Notes
identity	public const static : *anyURI*	

Table B – 32: GeoLicence Interfaces

Method	Type	Notes
getGrants ()	«access» public abstract: *Grant*	
getIssuer ()	«access» public: *Licensor*	

B.28 Grant

Type: *public abstract «interface»* **Interface** {abstract}

Package: GeoLicence

Table B – 33: Grant Connections

Connector	Source	Target	Notes
Aggregation	Condition +condition 0..*, unordered, frozen	Grant +grant unordered	
Aggregation	Grant +grant 1..*, unordered, frozen	GeoLicence +licence unordered	
Aggregation source < target	GrantComponent +component 1..*, unordered, frozen	Grant unordered	

Table B – 34: Grant Attributes

Attribute	Type	Notes
identity	public static Range:0 to 1: *anyURI*	

Table B – 35: Grant Interfaces

Method	Type	Notes
getConditions ()	«access» public: *Condition*	
getPrincipals ()	«access» public: *Principal*	
getResources ()	«access» public: *Resource*	
getRights ()	«access» public: *Right*	

B.29 GrantComponent

Type: *public abstract «interface»* **Interface** {abstract}

Package: GeoLicence

Table B – 36: GrantComponent Connections

Connector	Source	Target	Notes
Aggregation source < target	GrantComponent +component 1..*, unordered, frozen	Grant unordered	
Generalization source > target	Right Child	GrantComponent Parent	
Generalization source > target	Resource Child	GrantComponent Parent	

Generalization source > target	Principal Child	GrantComponent Parent	

Table B – 37: GrantComponent Attributes

Attribute	Type	Notes
identity	public const static Range:0 to 1: *anyURI*	
property	public static Range:0 to *: *Property*	The property attribute lists named properties of this entity.

Table B – 38: GrantComponent Interfaces

Method	Type	Notes
getIdentity ()	«access» public: *anyURI*	
getProperty (*string*)	public: *Property*	param: name [string - in] The getProperty operation returns the property descriptor of a particularly named property.
getPropertyValue (*string*)	public: *any*	param: name [string - in] The getPropertyValue operation returns the value of a particularly named property.
hasProperty (*string*)	public: *boolean*	param: name [string - in] The "hasProperty" operation determines if the entity process a particularly named property.

B.30 Licensee

Alias: User

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *Principal.*

Package: GeoLicence

A licensee is a principal in the role of a licence owner. Normally, the licensee is the default principal to which rights have been granted by this licence.

Table B – 39: Licensee Connections

Connector	Source	Target	Notes
Generalization source > target	SubLicensee Child	Licensee Parent	
Generalization source > target	Licensee Child	Principal Parent	

B.31 LicenceManager

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *ServiceProvider.*

Package: GeoLicence

A licence manager is an agent of another able to maintain licences and to verify those licences.

Table B – 40: LicenceManager Connections

Connector	Source	Target	Notes
Generalization source > target	LicenceManager Child	ServiceProvider Parent	

B.32 LicensingAgent

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *Agent, Licensor.*

Package: GeoLicence

A licensing agent is an agent of the owner (or transitively, an agent of another agent) allowed to grant and verify licences in lieu of the owner.

Table B – 41: LicensingAgent Connections

Connector	Source	Target	Notes
Generalization source > target	LicensingAgent Child	Licensor Parent	
Generalization source > target	LicensingAgent Child	Agent Parent	

B.33 Licensor

Alias: Issuer

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *Owner.*

Package: GeoLicence

A licensor is an owner or agent of an owner who has the right to grant licences of a defined type.

Table B – 42: Licensor Connections

Connector	Source	Target	Notes

Aggregation source < target	Licensor +issuer 1, unordered, frozen *Notes* Principal who composed the licence. The issuer of a licence must have the right to create and grant the licence in question. All such rights flow from the owner or from one of his agents.	GeoLicence unordered	
Generalization source > target	Licensor Child	Owner Parent	
Generalization source > target	LicensingAgent Child	Licensor Parent	

Table B – 43: Licensor Attributes

Attribute	Type	Notes
details	public static : *Details*	
signature	public static : *Signature*	

Table B – 44: Licensor Interfaces

Method	Type	Notes
getDetails ()	«get» public: *Details*	attribute_name = 'details'

getSignature ()	«get» public: *Signature*	attribute_name = 'signature'
getTimeOfIssue ()	«get» public: *Time*	
getTimeOfValidity ()	«get» public: *TimeInterval*	

B.34 MetaRight

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *Right.*

Package: GeoLicence

Table B – 45: MetaRight Connections

Connector	Source	Target	Notes
Generalization source > target	CreateLicence Child	MetaRight Parent	
Generalization source > target	Sublicense Child	MetaRight Parent	
Generalization source > target	MetaRight Child	Right Parent	

B.35 Modify

Alias: ReadWrite

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *DeriveResource.*

Package: GeoLicence

Edit or modify rights allow the user to modify the resource, and as such are usually granted on "non-identical" copies of a resource. They can modify the resource and retain identity.

Table B – 46: Modify Connections

Connector	Source	Target	Notes
Generalization source > target	Modify Child	DeriveResource Parent	

B.36 Owner

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *Principal.*

Package: GeoLicence

Owner interfaces allow principals to create and maintain resources and to grant various licences associated to the resource.

Table B – 47: Owner Connections

Connector	Source	Target	Notes
Aggregation	Resource +resource 0..*, unordered, frozen	Owner +owner 1..*, unordered, frozen	Each Resource is "owned" or under the complete control of a principal, or some number of principals. Each owner has the right to grant licences on the resource. This includes a general licence to grant other licences. In a GeoDRM system, all licences are eventually traceable back through a series of licences to the owner of the resource.
Generalization source > target	Licensor Child	Owner Parent	
Generalization source > target	Owner Child	Principal Parent	

B.37 Principal

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *GrantComponent.*

Package: GeoLicence

Principal is the root class of all participants in the systems. Subclasses of Principal can add further information needed to support the role that principal will play in the processes of the GeoDRM system. A group of principals is also a principal, and the group may take actions (such as obtaining a licence) which would normally be considered the act of a single entity. In other words, an individual has a right if he is a member of a group that has been granted that right. The basic metadata for any principal is identity, allowing that principal to be, without significant doubt, identified. A principal can have multiple identities, but each identity can only apply to one principal or one principal group.

Table B – 48: Principal Connections

Connector	Source	Target	Notes
Aggregation source > target	Principal +principal 0..*, ordered, none	Agent +agent 1..*, unordered	
Aggregation source > target	Principal +member 0..*, unordered *Notes* The members of a group are also principals, and may be groups in their own right.	PrincipalGroup +group 0..*, unordered *Notes* A principal group is a set of principals acting together in a single role in the system.	
Generalization source > target	Agent Child	Principal Parent	
Generalization source > target	Licensee Child	Principal Parent	

Connector	Source	Target	Notes
Generalization source > target	PrincipalGroup Child	Principal Parent	
Generalization source > target	Owner Child	Principal Parent	
Generalization source > target	ServiceProvider Child	Principal Parent	
Generalization source > target	Principal Child	GrantComponent Parent	
Realization «realize» source > target	principal Child	Principal Parent	
Realization «realize» source > target	principalPattern Child	Principal Parent	

B.38 PrincipalGroup

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *Principal.*

Package: GeoLicence

Table B – 49: PrincipalGroup Connections

Connector	Source	Target	Notes

Aggregation source > target	Principal +member 0..*, unordered *Notes* The members of a group are also principals, and may be groups in their own right.	PrincipalGroup +group 0..*, unordered *Notes* A principal group is a set of principals acting together in a single role in the system.	
Generalization source > target	PrincipalGroup Child	Principal Parent	

B.39 Print

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *View.*

Package: GeoLicence

Table B – 50: Print Connections

Connector	Source	Target	Notes
Generalization source > target	Print Child	View Parent	

B.40 Process

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *Processing.*

Package: GeoLicence

A "Process" is a processing resource providing functionality through an application programming interface.

Table B – 51: Process Connections

Connector	Source	Target	Notes
Generalization source > target	Process Child	Processing Parent	

Table B - 52: Process Attributes

Attribute	Type	Notes
languages	public static Range:1 to *: *string*	The "language" interface lists all programming languages in which the API for the Process may be used.

B.41 Processing

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *Resource.*

Package: GeoLicence

Processing resources are capable of acting on other resources. To use a Processing resource, a principal must have licences both for the Processing resources and for any Data resources that may be involved. Metadata about the Processing resource may include the implementer of the processing code, and the provider. The metaclass "standard" can further indicate to which standards the resource adheres. Any of this information may be used by conditions in licence grants.

Table B – 53: Processing Connections

Connector	Source	Target	Notes

Aggregation Implementation source > target	Processing +targetProcess 0..*, unordered	Request +request 0..*, unordered	The "Implementation" association lists all processes that would be invoked in any manner by the request if it were to be executed. The issuer of the request would have to have rights to the processing targets for the request to be valid. These rights may be granted as part of a public licence (i.e. anyone has the right to access the processing resource) or as a more specific licence.
Association source > target	Execute unordered	Processing +process 0..*, unordered	
Generalization source > target	Processing Child	Resource Parent	
Generalization source > target	Service Child	Processing Parent	
Generalization source > target	Process Child	Processing Parent	

Table B – 54: Processing Attributes

Attribute	Type	Notes
complianceLicence «metaclass»	public static Range:0 to *: *GeoLicence*	The "compliance licence" attribute lists proof of compliance to the various standards listed in the "standard" attribute.
formalName	public static Range:0 to *: *string*	The "formal name" is a list of names used in the "standard" attribute list to identify the functionality supplied here.
implementor «metadata»	public static Range:0 to *: *anyURI*	The "implementor" attribute identifies the implementor of the process represented.
localName	public static Range:0 to *: *string*	The "local name" attribute specifies which name or alias is actually used by this implementation.
provider «metadata»	public static Range:0 to *: *anyURI*	The "provider" attribute identifies the provider of the access to this functionality.
standard «metaclass»	public const static Range:0 to *: *anyURI*	The "standard" attribute lists the various standards that this process adheres to.
parameter «property»	public static Range:0 to *: *Property*	

B.42 ProcessInvocation

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *Request.*

Package: GeoLicence

Request implemented by a process invocation.

Table B – 55: ProcessInvocation Connections

Connector	Source	Target	Notes

Generalization source > target	ProcessInvocation Child	Request Parent	

B.43 PropertyInterface

Type: *public abstract «interface»* **Interface** {abstract}

Package: GeoLicence

Table B – 56: PropertyInterface Connections

Connector	Source	Target	Notes
Realisation «realize» source > target	Property Child	PropertyInterface Parent	

Table B – 57: PropertyInterface Interfaces

Method	Type	Notes
getName ()	public: *string*	
getType ()	public: *anyURI*	
getInstanceType ()	public: *anyURI*	
getValue ()	public: *any*	

B.44 Request

Alias: Service, Call

Type: *public abstract «interface»* **Interface** {abstract}

Package: GeoLicence

Table B – 58: Request Connections

Connector	Source	Target	Notes
Aggregation Target Resource source > target	Resource +targetResource 0..*, unordered *Notes* The "resource" role lists all resources addressed by the request.	Request +accessRequest 0..*, unordered	The "Target Resource" association lists all resources that would be accessed in any manner by the request if it were to be executed.
Aggregation Implementation source > target	Processing +targetProcess 0..*, unordered	Request +request 0..*, unordered	The "Implementation" association lists all processes that would be invoked in any manner by the request if it were to be executed. The issuer of the request would have to have rights to the processing targets for the request to be valid. These rights may be granted as part of a public licence (i.e. anyone has the right to access the processing resource) or as a more specific licence.
Generalization source > target	ServiceRequest Child	Request Parent	
Generalization source > target	ProcessInvocation Child	Request Parent	
Generalization source > target	FunctionCall Child	Request Parent	

Table B – 59: Request Attributes

Attribute	Type	Notes
name	public const static Range:1 to *: *string*	The invocation name of functions used by the service.
parameters	public static Range:0 to *: *NameValuePair*	The parameters used in the processes being invoked. If confusion is possible, the full name of the parameter is used, including process-name and parameter-name.

B.45 Resource

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *GrantComponent.*

Package: GeoLicence

A resource is any data, functionality, or any other entity subject to licensing. A resource metadata must, at a minimum, identify the resource and be traceable to its owner or an agent of its owner.

Table B – 60: Resource Connections

Connector	Source	Target	Notes
Aggregation	Resource +resource 0..*, unordered, frozen	Owner +owner 1..*, unordered, frozen	Each Resource is "owned" or under the complete control of a principal, or some number of principals. Each owner has the right to grant licences on the resource. This includes a general licence to grant other licences. In a GeoDRM system, all licences are eventually traceable back through a series of licences to the owner of the resource.

Aggregation Target Resource source > target	Resource +targetResource 0..*, unordered *Notes* The "resource" role lists all resources addressed by the request.	Request +accessRequest 0..*, unordered	The "Target Resource" association lists all resources that would be accessed in any manner by the request if it were to be executed.
Association source > target	Execute unordered	Resource +parameters 0..*, unordered	
Generalization source > target	Resource Child	GrantComponent Parent	
Generalization source > target	Processing Child	Resource Parent	
Generalization source > target	Data Child	Resource Parent	
Realization «realize» source > target	resource Child	Resource Parent	
Realization «realize» source > target	resourcePattern Child	Resource Parent	

Table B – 61: Resource Interfaces

Method	Type	Notes
getOwner ()	«get» public: *Owner*	The getOwner operation is a convenience function that tracks from this resource to its owner or one of the owner's agents (another principal of the system). This is used to validate licences since the licensor must be an agent (or transitive agent) of the owner.

B.46 Right

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *GrantComponent.*

Package: GeoLicence

A right is any act that can access the resource in any manner. Rights are often associated to the process standard that implements them. Right metadata includes any information needed to identify the action that a request may make using this right.

Table B – 62: Right Connections

Connector	Source	Target	Notes
Generalization source > target	Right Child	GrantComponent Parent	
Generalization source > target	MetaRight Child	Right Parent	
Generalization source > target	Use Child	Right Parent	

B.47 Service

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *Processing.*

Package: GeoLicence

A "Service" is a processing resource providing access through a message-oriented interface, such as a web service.

Table B – 63: Service Connections

Connector	Source	Target	Notes
Aggregation source < target	Service +service 1..*, unordered	Security +security unordered	
Generalization source > target	Service Child	Processing Parent	

B.48 ServiceBroker

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *Agent*, *ServiceProvider*.

Package: GeoLicence

Table B – 64: ServiceBroker Connections

Connector	Source	Target	Notes
Generalization source > target	ServiceBroker Child	Agent Parent	
Generalization source > target	ServiceBroker Child	ServiceProvider Parent	

B.49 ServiceProvider

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *Principal.*

Package: GeoLicence

A service provider is a principal who supports a service or functionality involved in the GeoDRM system.

Table B – 65: ServiceProvider Connections

Connector	Source	Target	Notes
Generalization source > target	ServiceBroker Child	ServiceProvider Parent	
Generalization source > target	ServiceProvider Child	Principal Parent	
Generalization source > target	LicenceManager Child	ServiceProvider Parent	

B.50 ServiceRequest

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *Request.*

Package: GeoLicence

Process invoked through a message-oriented protocol.

Table B – 66: ServiceRequest Connections

Connector	Source	Target	Notes
Generalization source > target	ServiceRequest Child	Request Parent	

B.51 SideEffect

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *Condition.*

Package: GeoLicence

Side effects are conditions that cause a logically unrelated action to occur. Such actions are usually required by the contract that the licence represents. The evaluate function,

inherited from Condition, will return true if the side effect does not uncover any reason to interrupt the flow. If a side effect has a time set beyond the end of the act, i.e. if the effect is to occur later than the successful completion of the licensed act, the return value of the Condition::evaluate function should always be true. Among other things, this would allow an emergency-inspired "break the glass" action to be reviewed after the crisis that spawned the emergency was handled.

Table B – 67: SideEffect Connections

Connector	Source	Target	Notes
Generalization source > target	SideEffect Child	Condition Parent	

Table B – 68: SideEffect Attributes

Attribute	Type	Notes
time	public static Range:0 to 1: *string*	The attribute "time" is a temporal relation string, relating the side effect action to the licensed act. Common values are "before" or "after." Initial Value: "before";
type	public static: *string*	The attribute "type" is a string describing the side effect action. It acts as instructions to the GeoDRM Gatekeeper to execute the side effect. Normal values include, message to licensor, user message, service call, function call or similar remote invocation technique. Initial Value: "message to user";
request	public static: *any*	The attribute "request" is a representation of the invocation of the side effect action. If the type is a message, then the request, possibly with parameterized content, could be the content of the message.

Table B – 69: SideEffect Interfaces

Method	Type	Notes
requestReturn ()	public: *any*	

B.52 SpatialFit

Alias: SpatialAdjust

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *SpatialTransform.*

Package: GeoLicence

Table B – 70: SpatialFit Connections

Connector	Source	Target	Notes
Generalization source > target	SpatialFit Child	SpatialTransform Parent	

B.53 SpatialGeometry

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *ConditionParameter.*

Package: GeoLicence

This condition parameter class consists of objects or entities that represent geographic geometry values. They are of one of the types defined in ISO 19107 (the OGC feature geometry abstract topic volume), some subtype of either GM_Object or TP_Object in those standards.

Table B – 71: SpatialGeometry Connections

Connector	Source	Target	Notes
Generalization source > target	SpatialGeometry Child	ConditionParameter Parent	

Table B – 72: SpatialGeometry Interfaces

Method	Type	Notes
anyInteraction (*SpatialGeometry*)	public: *boolean*	param: other [SpatialGeometry - in]
contains (*SpatialGeometry*)	public: *boolean*	param: other [SpatialGeometry - in]
intersects (*SpatialGeometry*)	public: *boolean*	param: other [SpatialGeometry - in]
isContainedBy (*SpatialGeometry*)	public: *boolean*	param: other [SpatialGeometry - in]
topologicMatrix (*SpatialGeometry, string*)	public: *boolean*	param: other [SpatialGeometry - in] param: mask [string - in]
withinDistance (*SpatialGeometry, Measure*)	public: *boolean*	param: other [SpatialGeometry - in] param: distance [Measure - in]

B.54 SpatialOperations

Type: *public abstract «interface»* **Interface** {abstract}

Package: GeoLicence

B.55 SpatialTransform

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *Use.*

Package: GeoLicence

The spatial transform data right allows the user to take data from a resource and change its coordinate reference system, and thereby create a new resource.

Table B – 73: SpatialTransform Connections

Connector	Source	Target	Notes
Generalization source > target	SpatialTransform Child	Use Parent	
Generalization source > target	SpatialFit Child	SpatialTransform Parent	

B.56 Sublicense

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *MetaRight.*

Package: GeoLicence

Table B – 74: Sublicense Connections

Connector	Source	Target	Notes
Generalization source > target	Sublicense Child	MetaRight Parent	

B.57 SubLicensee

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *Agent, Licensee.*

Package: GeoLicence

A sublicensee is a principal to whom a licensee "lends" his rights for some purpose. The licence in question must allow this for the "lending" to be acceptable, and may put conditions on such "loans".

Table B – 75: SubLicensee Connections

Connector	Source	Target	Notes

Generalization source > target	SubLicensee Child	Agent Parent	
Generalization source > target	SubLicensee Child	Licensee Parent	

B.58 TemporalOperations

Type: *public abstract «interface»* **Interface** {abstract}

Package: GeoLicence

B.59 Time

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *ConditionParameter.*

Package: GeoLicence

Table B – 76: Time Connections

Connector	Source	Target	Notes
Association source > target	TimePattern unordered	Time +matches 0..*, unordered	
Generalization source > target	Time Child	ConditionParameter Parent	

Table B – 77: Time Attributes

Attribute	Type	Notes
instant	public static : *dateTime*	

Table B – 78: Time Interfaces

Method	Type	Notes
isAfter (*Time*)	public: *boolean*	param: other [Time - in]
isBefore (*Time*)	public: *boolean*	param: other [Time - in]
isDuring (*TimeInterval*)	public: *boolean*	param: interval [TimeInterval - in]

B.60 TimeInterval

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *ConditionParameter.*

Package: GeoLicence

Table B – 79: TimeInterval Connections

Connector	Source	Target	Notes
Generalization source > target	TimeInterval Child	ConditionParameter Parent	

Table B – 80: TimeInterval Attributes

Attribute	Type	Notes
start	public static: *Time*	
end	public static: *Time*	

Table B – 81: TimeInterval Interfaces

Method	Type	Notes
contains (*TimeInteval*)	public: *boolean*	param: other [TimeInteval - in]
intersects (*TimeInterval*)	public: *boolean*	param: other [TimeInterval - in]
isContainedBy (*TimeInterval*)	public: *boolean*	param: other [TimeInterval - in]
overlap (*TimeInterval*)	public: *boolean*	param: other [TimeInterval - in]

B.61 TimePattern

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *ConditionParameter.*

Package: GeoLicence

Table B – 82: TimePattern Connections

Connector	Source	Target	Notes
Association source > target	TimePattern unordered	Time +matches 0..*, unordered	
Generalization source > target	TimePattern Child	ConditionParameter Parent	

Table B – 83: TimePattern Attributes

Attribute	Type	Notes
pattern	public static: *string*	

B.62 Use

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *Right.*

Package: GeoLicence

Usage rights allow the licensee to use the resources in order to create new resources.

Table B – 84: Use Connections

Connector	Source	Target	Notes
Generalization source > target	DeriveResource Child	Use Parent	
Generalization source > target	Encode Child	Use Parent	
Generalization source > target	SpatialTransform Child	Use Parent	
Generalization source > target	Execute Child	Use Parent	
Generalization source > target	View Child	Use Parent	
Generalization source > target	Combine Child	Use Parent	
Generalization source > target	Use Child	Right Parent	

Generalization source > target	ExtractResource Child	Use Parent	

B.63 View

Alias: Display

Type: *public abstract «interface»* **Interface** {abstract}
Extends: *Use.*

Package: GeoLicence

The view right allows the user to have access to graphic depictions of the data (not normally the resource itself) that allows for visual inspection of the data content.

Table B – 85: View Connections

Connector	Source	Target	Notes
Generalization source > target	Print Child	View Parent	
Generalization source > target	View Child	Use Parent	

Annex C
Scenarios

C.1 Introduction

This annex describes some example scenarios to illustrate how a GeoDRM-enabled system may handle the creation, distribution and enforcement of GeoLicences. The example scenarios are based on a GeoDRM Game, which we have used within the GeoDRM Working Group to understand the logic of distributed licence management.

The purpose of the GeoDRM game was to:

- To understand the roles and responsibilities within a GeoDRM network.
- To separate the *logic* of managing intellectual property from the content.
- To use a simplified game to simulate the real-world problem.
- To make the abstract problem of digital rights management more understandable in concrete terms.

Players were assigned to each of the identified roles and a given licensing scenario, played out using a pack of standard playing cards to represent the content and cardboard templates to represent licences.

The implementation of a GeoDRM-enabled solution will be based on this metaphor, and a similar sequence of electronic transactions will be needed in the digital world.

Copyright © 2006 Open Geospatial Consortium, Inc. All Rights Reserved.

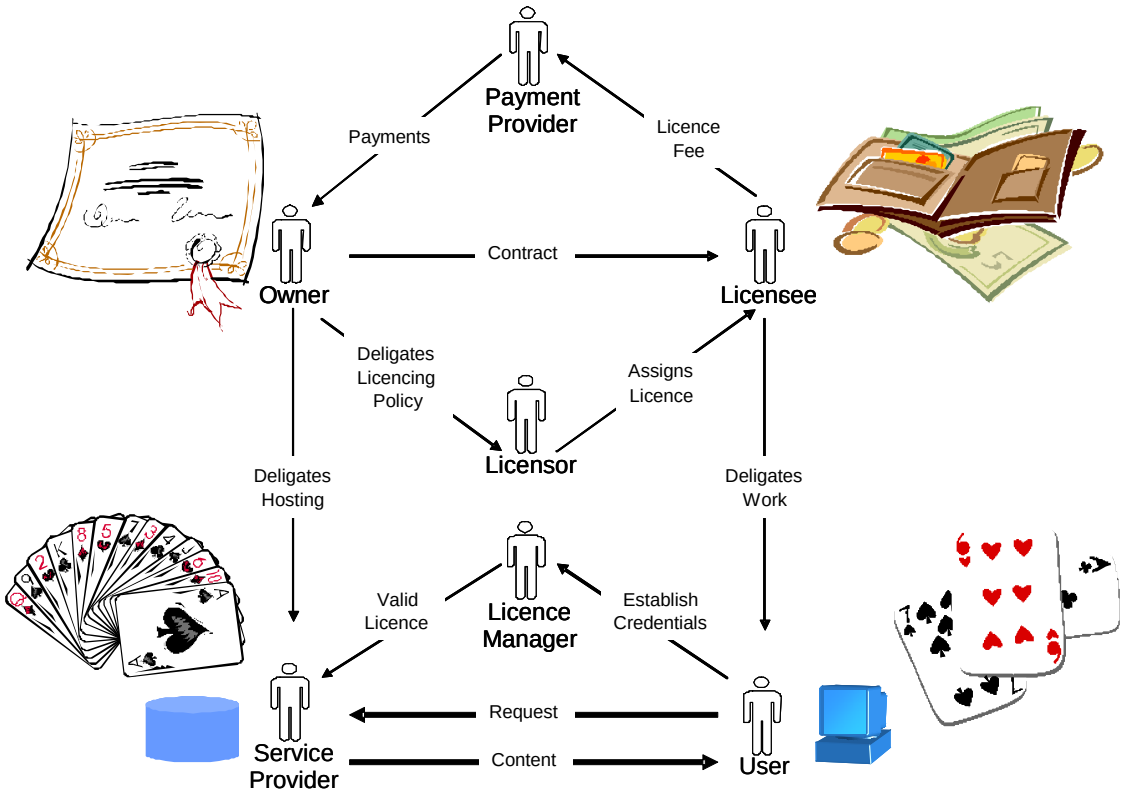

Figure C – 1: GeoDRM Game – Interactive Role Playing

Each round of the game was used to play out the scenarios as below and was used as a way to understand the dynamic and distributed nature of GeoLicence management.

C.2 Scenario 1: User accesses content from single provider

In this scenario there is a single service provider serving the suit of hearts. The scenario that was played out was to create a licence to access the 7, 8 and 9 of hearts, represented by the blue block, and enforce that licence to access the content.

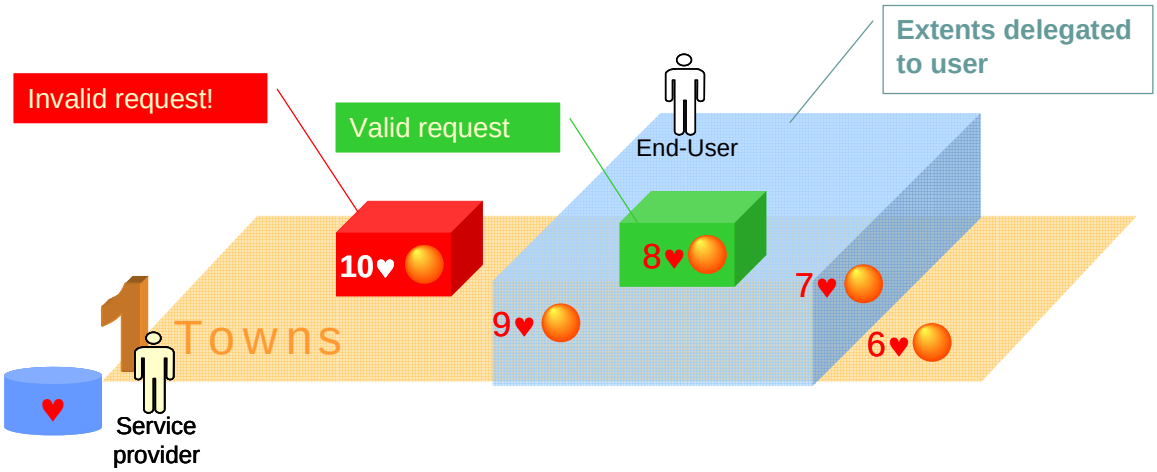

Figure C – 2: User accesses content from single provider

From playing out the scenario the following workflow for the creation and enforcement of the licence was defined.

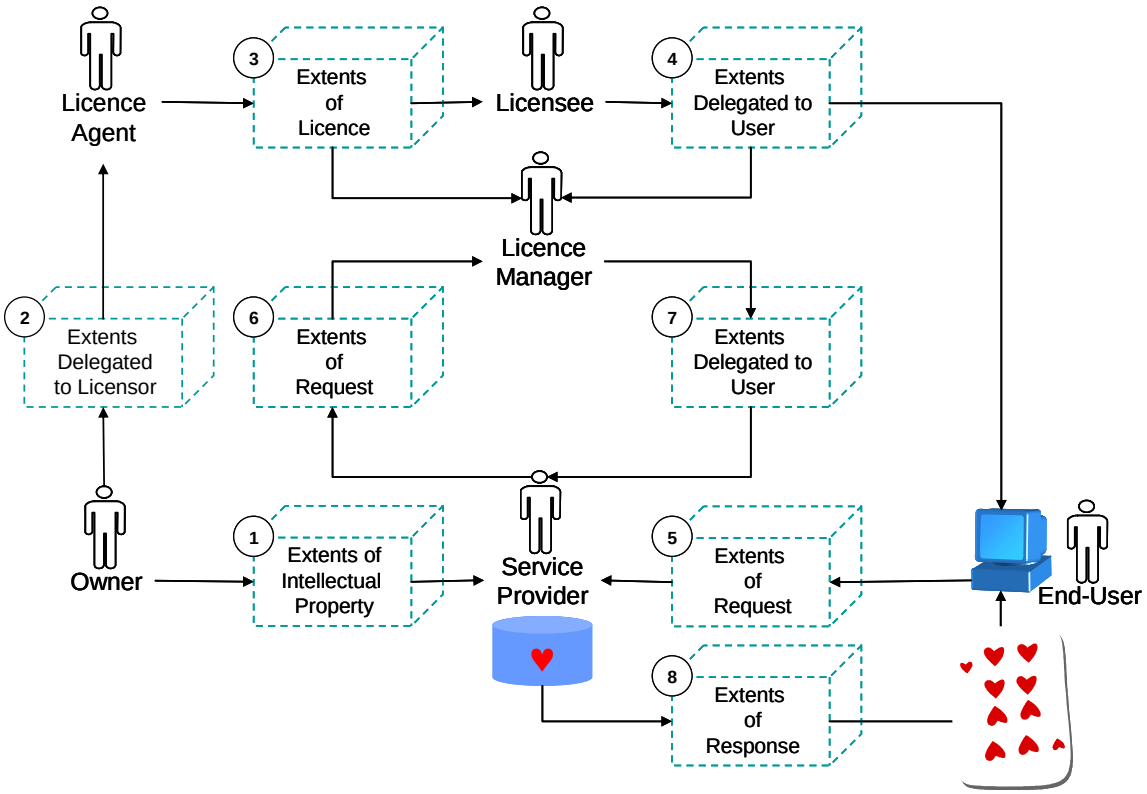

Figure C – 3: Workflow for creating and enforcing a licence

The workflow starts with the owner who (1) defines the extents of the intellectual property delegated to the service provider. Service provider is responsible for serving the suit of hearts and enforces the constraints defined in the licence. The owner then delegates (2) the extents to be licensed to the licensing agent.

Licensing agent is responsible for creating and granting licences (3) to a licensee. A copy of the licence is then registered with licence manager, and licensee then delegates the

licence extents (4) to the end-user. End-user may then request data (5) from the service provider, who then uses the extents of the request (6) to retrieve the licence and extents delegated to the end-user (7) and returns them to the service provider. Service provider is responsible for enforcing the licence and returning the requested content (8) back to the end-user.

As identified in 8.1 Overview: Roles and Responsibilities, these roles may be performed by the same entity, depending on the specific business model. Second, once a licence has been created it may be used as many times as required by the end-user to access the content.

C.3 Scenario 2: Overlaying content from multiple providers

This scenario introduces the more realistic situation where an end-user needs to access content from multiple providers, each serving data for different owners. A single licensing agent and licence manager is used to create a licence to manage and protect access to the content.

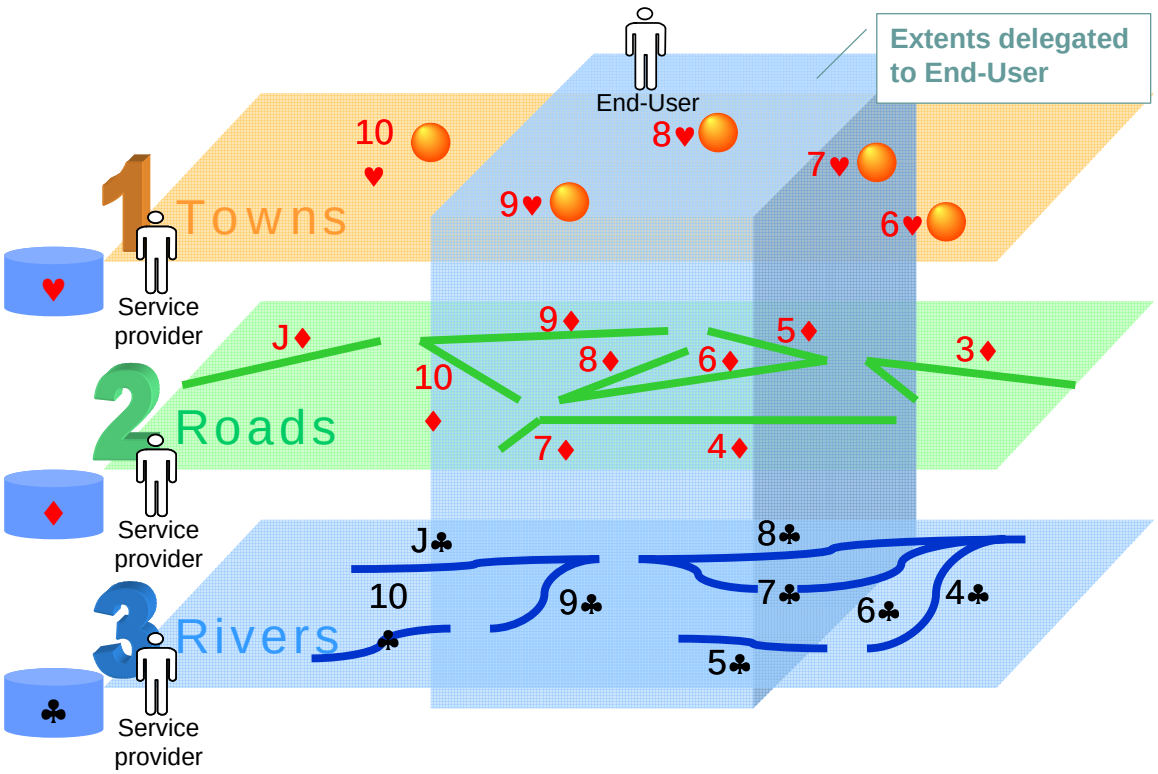

Figure C – 4: Overlaying content from multiple providers

We can imagine that content represented by the various suits of cards represents towns, roads and rivers data. The end-user accesses each of these resources to create a combined resource overlaying the town, roads and rivers data for a given geographical extent.

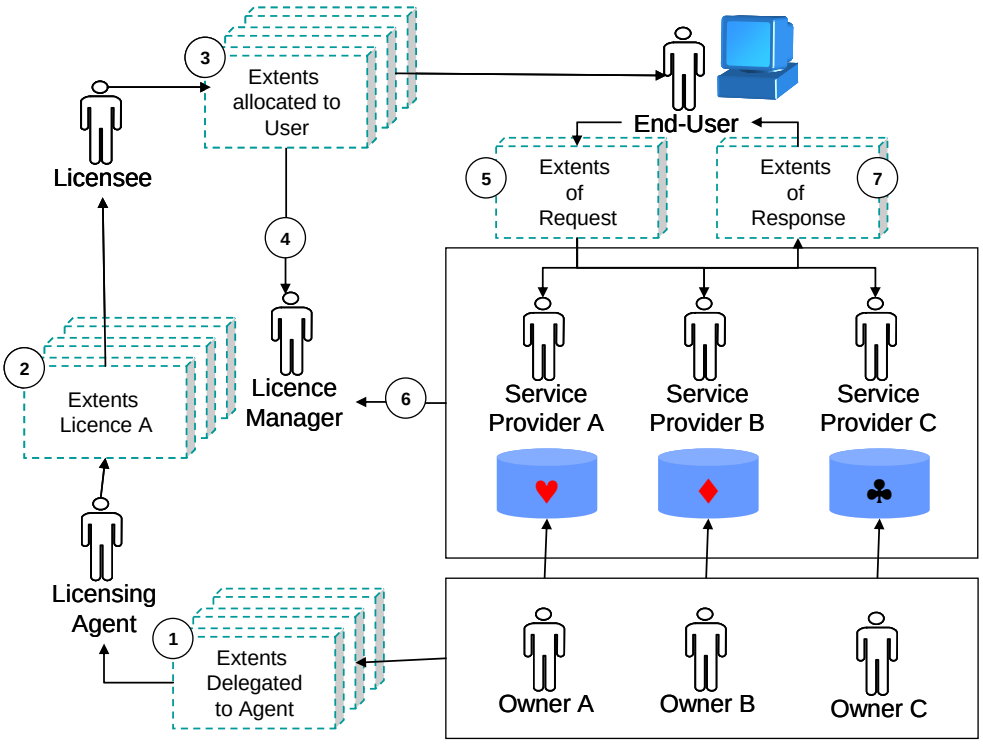

Figure C – 5: Workflow licensed access to content from multiple providers

In this workflow each of the owners delegate the content to service providers who are responsible for serving the towns, roads and rivers data respectively. Then each owner delegates the extent to be licensed (1) to the licensing agent.

Licensing agent then creates a licence (or licences) to be granted to the licensee. A copy of that licence is registered with the licence manager (4), and a sublicence granted to the end-user.

End-user can request access to the content (5), with each service provider retrieving a valid licence (6) from the licence manager, enforcing the constraints of the licence, and finally returning the response (7) back to the end-user.

C.4 Scenario 3: Joining content from multiple providers

This scenario is similar to Scenario 2, but instead of combining content of different types it represents the scenario of accessing the same content type from multiple providers. In this scenario we imagine each of the suits of cards to represent content of the roads data type, but being served by multiple providers.

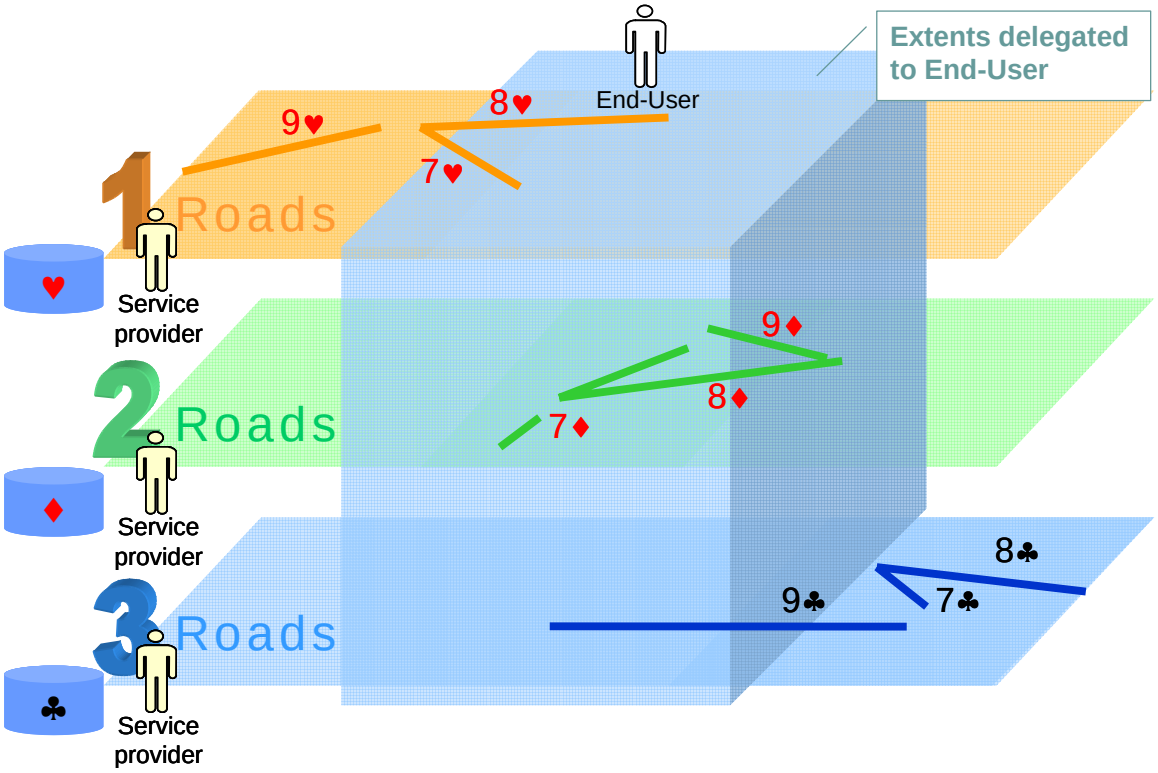

Figure C – 6: Joining resources from multiple providers

The conclusion from playing out this scenario was that the workflow logic from a licensing perspective was the same as that for Scenario 2.

C.5 Scenario 4: Derived resource adding content

This scenario represents the joining of multiple datasets and adding additional content. It is based on the idea that the output generated by Scenario being combined with additional content. In other words, the combined roads data is overlaid with pubs data to create a new derived product. Recall from Clause 1, that a GeoDRM system must be necessary and sufficient. In this case this means that the tracking of derived products must match the contractual agreement between licensee and licensor.

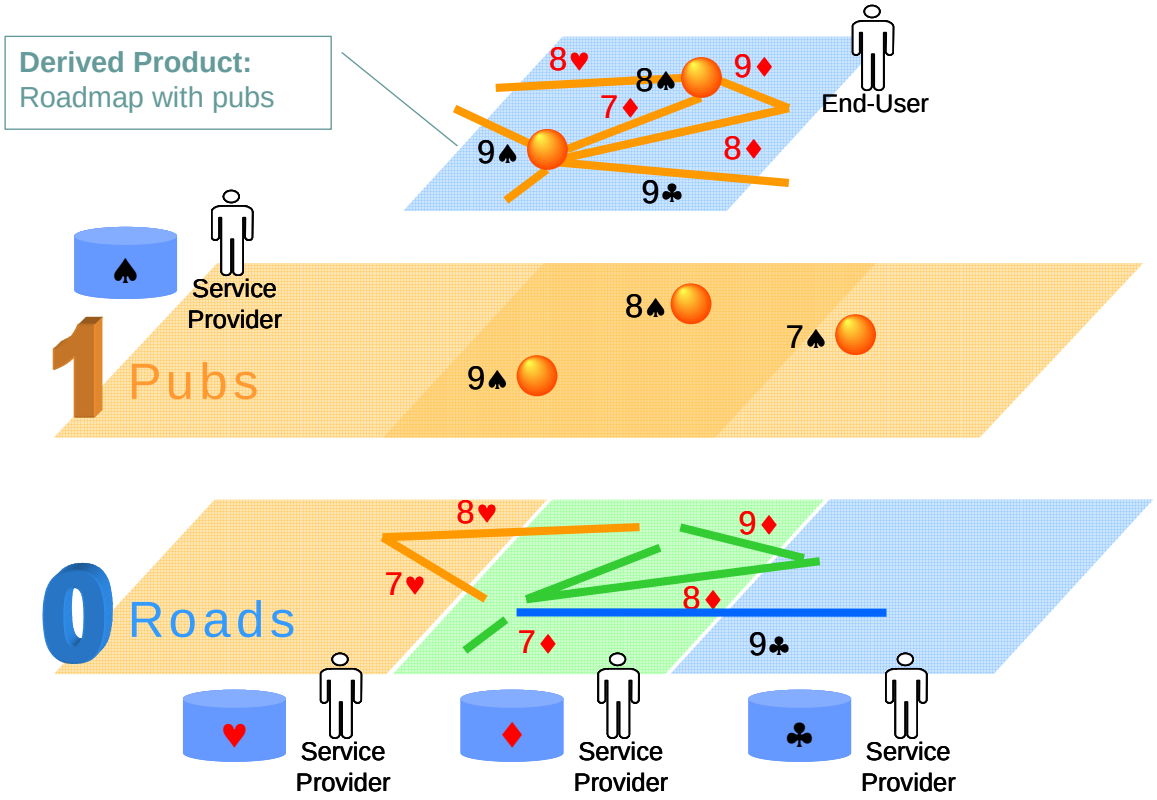

Figure C – 7: Derived resource adding content

The derived product now contains information content from multiple owners. This information may have been manipulated in a manner consistent with the licences involved. The GeoDRM system should allow the contribution of each owner to be recognised and tracked as required by the licence.

Annex D
Editor's notes

D.1 The spelling of licence in its various forms

This document follows the Oxford English Dictionary spelling of "licence" (as opposed to "license") when used as a noun. When used as a verb, or a verb form, the term is "license." Hence, the phrase "a licence is licensed to a licensee by a licensor during the licensing process" is in fact spelled correctly, albeit a bit confusing.

Copyright © 2006 Open Geospatial Consortium, Inc. All Rights Reserved.

Bibliography

[19] Camp, L. Jean; **Trust and Risk in Internet Commerce**; The MIT Press, Cambridge, Massachusetts, 2000.

[20] Herring, John (editor), Hari Reddy, Mark Scardina, Thomas DeMartini; **Geographic Digital Rights Management: Licence Encodings in XML**, Working Draft, OGC Project Document 2005-044, 23 May 2005

[21] Iannella, R. Digital Rights Management (DRM) Architectures, D-Lib Magazine, June 2001, Volume 7 Number 6.
Available from http://www.dlib.org/dlib/june01/iannella/06iannella.html

[22] ISO/IEC 21000-5, Information Technology — Multimedia Framework — Rights Expression Language

[23] ISO/IEC TR 21000-1, Information Technology — Multimedia Framework — Information technology — Multimedia framework (MPEG-21) — Part 1: Vision, Technologies and Strategy; available at
http://standards.iso.org/ittf/PubliclyAvailableStandards/c040611_ISO_IEC_TR_21000-1_2004(E).zip

[24] Ferguson, Niels, Bruce Schneier, **Practical Cryptography**, Wiley Publishing Incorporated, 2003

[25] Rosenblatt, Bill, Bill Trippe, Stephen Mooney, **Digital Rights Management: Business and Technology**, M&T Books, 2002

[26] Schneier, Bruce, **Applied Cryptography, Second Edition**, John Wiley and Sons, Inc, 1996.

[27] **ISO/IEC 21000-5 ISO-REL XML schemas,** available at
http://standards.iso.org/ittf/PubliclyAvailableStandards/MPEG-21_schema_files/rel-r/

[28] **ISO/IEC TR 10000: Information technology — Framework and taxonomy of International Standardized Profiles.** Parts 1, 2, and 3 available at:
http://standards.iso.org/ittf/PubliclyAvailableStandards/c030726_ISO_IEC_TR_10000-1_1998(E).zip
http://standards.iso.org/ittf/PubliclyAvailableStandards/c030728_ISO_IEC_TR_10000-2_1998(E).zip
http://standards.iso.org/ittf/PubliclyAvailableStandards/c030727_ISO_IEC_TR_10000-3_1998(E).zip

[29] **XML-Signature Syntax and Processing**, W3C Recommendation, 12 February 2002, available at http://www.w3.org/TR/xmldsig-core/