INTERNATIONAL STANDARD

**ISO 19153**

First edition
2014-02-15

# Geospatial Digital Rights Management Reference Model (GeoDRM RM)

*Modèle de référence pour la gestion numérique des droits d'utilisation de l'information géographique*



Reference number
ISO 19153:2014(E)



ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

# Contents

Page

 

# Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC 211, *Geographic information/Geomatics*, jointly with the Open Geospatial Consortium, Inc. (OGC).

# Introduction

To create a marketplace, individuals who own something of value (here a resource) shall 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 can legitimately act upon a resource if he has a corresponding licence for that act.

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

— Optionally, the user can 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 can 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 ensure 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 International Standard describes how this is to be done.

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



 

# Geospatial Digital Rights Management Reference Model (GeoDRM RM)

## 1 Scope

This International Standard 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 resources, such as music, text, or services.

This International 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.

NOTE 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 ensure 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 descriptive International Standard builds on and complements the existing standards, and defines at an abstract level a rights model to enable the digital rights management of standards-based geospatial resources. Future GeoDRM standards will be written to implement the concepts defined in this International Standard.



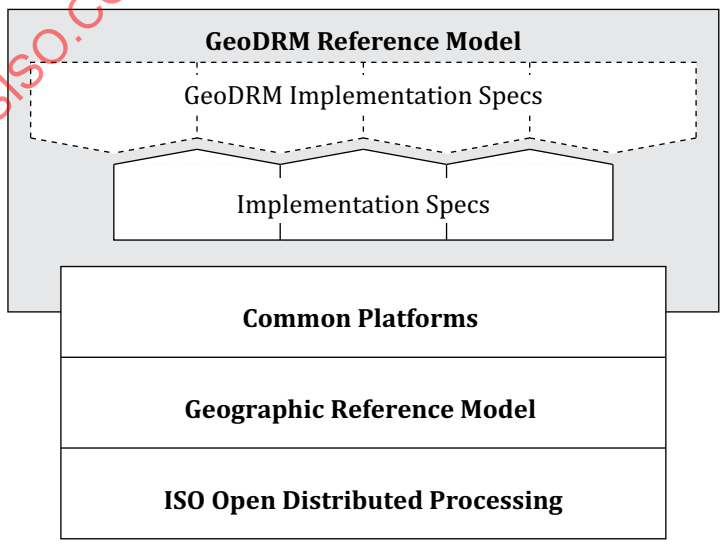


**Figure 1 — GeoDRM reference model context**

Figure 1 shows a simplified view of how this International Standard, 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 International Standard 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 International Standard 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

Because the normative nature of a reference model is embedded in its "reference" description of the semantics of the environment which it describes, the central requirement of this International Standard is:

> Any standard or implementation conformant to this International Standard shall be consistent with the semantics described within this International Standard or within the normative references of this International Standard.

Conformance with this specification shall be checked using tests specified in Annex A. Conformance classes for this International Standard are

— alignment of rights expression to the abstract rights model,

— expression for applicability of rights for geospatial resources, and

— enforcement of rights for geospatial resources.

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

This is a complex subject, and Annexes B to D are informative annexes that aid in understanding the normative specification of the rights expression language.

## 3 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 2382-6, *Information processing systems — Vocabulary — Part 6: Preparation and handling of data*

ISO/IEC 15408, *Information technology — Security techniques — Evaluation for IT security*

ISO/IEC 21000 (all parts), *Information technology — Multimedia framework (MPEG-21)*[1)]

ISO/IEC 21000-5, *Information technology — Multimedia framework (MPEG-21) — Part 5: Rights Expression Language*

1) The MPEG 21 (ISO/IEC 21000) standard is a work in progress. It will eventually have at least 14 parts. Only the first few are available now. The intent is to eventually incorporate as much of ISO/IEC 21000 as appropriate in this International Standard in order to assure interoperability of geospatial resource DRM with that used for other multimedia information.



 

# 4 Terms and definitions

For the purposes of this document, the terms and definitions in ISO 2382-6 and ISO/IEC 15408 and the following apply.

NOTE 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 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 for common information technology (IT) security terms such as authentication resource, authorized user, identity, security attribute, security policy, and trusted channel.

— OWS Common Implementation Specification [OGC 05-008[13]].

— OGC Glossary[14] for terms and examples specifically related to OGC standardized web services.

— RM-ODP[8] for system modelling terms such as the enterprise, computational, and information viewpoints.

— ODRL,[19] OMA DRM REL,[15] and ISO/IEC 21000 for terms specific to rights expressions languages, such as principal, licence, right, grant, condition, and resource.

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

**4.1**
**access control**
combination of *authentication* (4.4) and *authorization* (4.5)

**4.2**
**agency**
legal relationship of a person (called the *agent* [4.3]) who acts on behalf of another person, company, or government (called the *principal* [4.35])

**4.3**
**agent**
one who acts on behalf of another

**4.4**
**authentication**
verification that a potential partner in a conversation is capable of representing a person or organization

[SOURCE: W3C, Web Services Glossary]

**4.5**
**authorization**
determination whether a subject is allowed to have the specified types of access to a particular *resource* (4.40)

Note 1 to entry: Usually, authorization is in the context of *authentication* (4.4). Once a subject is authenticated, it can be authorized to perform different types of access.

**4.6**
**bypass**
mechanism to defeat the purpose of a subsystem by avoiding its invocation

[SOURCE: W3C, Web Services Glossary]

Note 1 to entry: Security systems are bypassed usually by using security faults in the operating system. Such *infringements* (4.21 and 4.22) 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 shall be modified to prevent bypass mechanisms.

**4.7**
**chain of agency**
sequence of *agency* (4.2) where the *agent* (4.3) in each relationship is the *principal* (4.35) of the next in the chain

Note 1 to entry: 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).

**4.8**
**chain of licence**
sequence of *licences* (4.26) that traces a *chain of agency* (4.7), where a licence is granted at each link of the chain, allowing the *agent* (4.3) at that link to act as the *principal* (4.35) in the next

Note 1 to entry: As with the chain of agency, this chain can be spoken of in either direction.

**4.9**
**contract**
agreement between two or more *principals* (4.35) 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

[SOURCE: FindLaw, modified]

**4.10**
**copyleft**
*licence* (4.26) that accompanies some open source software that details how the software and its accompanying source code can be freely copied, distributed, and modified

Note 1 to entry: A copyleft is a form of *general public licence* (4.15).

**4.11**
**digital licence**
document or its representation that specifies the *rights* (4.42) granted to a particular user or organization with respect to a specific content or group of content

Note 1 to entry: The core concept in *DRM* (4.12) is the use of digital licences. Instead of buying the digital content, the consumer purchases a *licence* (4.26) granting certain rights with respect to the content. A licence is the mechanism by which a *rights holder* (4.43) conveys rights to another *party* (4.35), such as a consumer or distributor.

**4.12**
**digital rights management**
**DRM**
packaging, distributing, controlling, and tracking content based on *rights* (4.42) and licensing information

Note 1 to entry: 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, Reference [5]. "Digital" refers to the material over which the rights exist. "Rights" applies to the Intellectual Property rights linked to the material. "Management" covers both the defining of 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.[12] For the purposes of this International Standard, DRM is taken to mean technology that enables the secure distribution (and where appropriate, sale) of digital media content on the Internet.[26]

**4.13**
**expected risk**
expected value (statistics) of loss

Note 1 to entry: Expected *risk* (4.45) is calculated by multiplying the probability of the types of *infringement* (4.21 and 4.22) by the cost of that infringement, summed up over all types of infringement.

**4.14**
**fair use**
uses of content that are considered valid defences to copyright *infringement* (4.21 and 4.22), such as for criticism or educational purposes

[SOURCE: U.S. legal term derived from Title 17 of the United States Code, Section 107]

Note 1 to entry: 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.[29]

**4.15**
**general public licence**
**GPL**
*licence* (4.26) containing *rights* (4.42) accorded to the general public without an existing agreement

Note 1 to entry: GPLs can be granted by the *owner* (4.34) of a *resource* (4.40) or can be applied to a resource by law, usually as part of the copyright law. The most obvious GPL concept is *fair use* (4.14) in the United States for copyrighted material. Other GPL rights can be demanded by the source of the resource or other "public good" considerations.

Note 2 to entry: The most widespread use of GPL 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 shall 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* (4.10), in contrast to a copyright, which identifies the proprietary rights of material.[29]

**4.16**
**GeoDRM enabled**
capable of maintaining *GeoDRM extended* (4.17)*resources* (4.40) and enforcing GeoDRM defined *rights* (4.42) and *protections* (4.38)

Note 1 to entry: Applied to processing resources.

**4.17**
**GeoDRM extended (applied to resources)**
associated to GeoDRM metadata indicating types of *licences* (4.26) that apply

**4.18**
**GeoLicence**
*licence* (4.26) related to geoinformation

**4.19**
**GeoLicence resolution**
settling or resolving the status of a *GeoLicence* (4.18)

**4.20**
**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

[SOURCE: FindLaw, modified]

**4.21**
**infringement (of a licence)**
act of a *principal* (4.35) contrary to *rights* (4.42) granted to that principal on a *resource* (4.40)

Note 1 to entry: Infringement of a *licence* (4.26) will require the *DRM* (4.12) system to be bypassed in some manner. If licences can be infringed without bypassing the DRM system, then the system is not *sufficient* (4.48).

**4.22**
**infringement (of a right)**
prevention of an act of a *principal* (4.35) consistent with *rights* (4.42) granted to that principal on a *resource* (4.40)

Note 1 to entry: Infringement of a right is a fault in the *DRM* (4.12) system. If rights can be infringed without bypassing the DRM system, then the system is not properly restricted to that which is *necessary* (4.33).

**4.23**
**joint ownership**
ownership by two or more persons each having undivided shares in the property as a whole

[SOURCE: FindLaw, modified]

Note 1 to entry: In this case, the *principal* (4.35) as *owner* (4.34) is a principal group, i.e. a group of other principals.

**4.24**
**lease**
allowing the *resource* (4.40) to be made available for a fixed period of time then returned

Note 1 to entry: During this period, the resource is only available to the lessee. Temporal constraints are required for downstream use.

**4.25**
**lend**
*lease* (4.24) without exchange of value

**4.26**
**licence**
representation of grants that convey to *principals* (4.35) the *rights* (4.42) to use specified *resources* (4.40) subject to specified conditions

[SOURCE: XrML 2.0 specification, part 5, modified]

Note 1 to entry: A licence represents, but is not, a *contract* (4.9) that grants a *party* (4.35) explicit rights to use Intellectual Property.

**4.27**
**licence extents**
scope or applicability of a *licence* (4.26)

Note 1 to entry: The extent can be described in spatial, temporal, or any other parameter range appropriate to the *rights* (4.42) described in the licence.

**4.28**
**licence manager**
application that tracks *licences* (4.26) available within an organization and coordinates the issuing of these licences to requesting clients

[SOURCE: New Concepts In BASIS Licensing, modified]

**4.29**
**licensee**
one to whom a *licence* (4.26) is given

[SOURCE: FindLaw]

**4.30**
**licensing agent**
*principal* (4.35) authorized to act on behalf of and under the control of another in dealing with third parties in the context of issuing *licences* (4.26) for specified *resources* (4.40)

[SOURCE: Derived from FindLaw for “agent”]



 

**4.31**
**licensor**
issuer of a *licence* (4.26)

[SOURCE: FindLaw, modified]

Note 1 to entry: The licensor is a content *owner* (4.34) or a *licensing agent* (4.30).

**4.32**
**map**
portrayal of geographic information as a digital image file suitable for display on a computer screen

[SOURCE: ISO 19128:2005, 4.7]

Note 1 to entry: A map is not the *resource* (4.40) itself. A Web Map Service (WMS) produces maps of georeferenced resource. Therefore, a WMS can provide many different representations of the same underlying geoinformation.

**4.33**
**necessary**
capable of recognizing and properly acting upon all legitimate requests, as defined by the requirements of the system

Note 1 to entry: All aspects of a *DRM* (4.12) system are necessary if they do not prevent legitimate requests from execution.

**4.34**
**owner**
one with an interest in and dominion over content as a) "legal owner" in this entry, b) one with the *right* (4.42) to exclusive use, control, or possession of content, c) a purchaser under a *contract* (4.9) for the sale of real content

[SOURCE: FindLaw, modified]

**4.35**
**party**
**principal**
person or organization that plays a role in a *rights* (4.42)*transaction* (4.49)

Note 1 to entry: These two terms are used as near synonyms from ORDL and ISO 21000. There will be no distinction between these two terms made here, but there can be distinctions in legal documents depending on local laws.

EXAMPLE In some legal traditions, "party" refers to person in a legal dispute, while "principal" can be the entity initiating a *contract* (4.9), such as an *agency* (4.2).

**4.36**
**payment provider**
*party* (4.35) that has an established billing relation with a consumer

Note 1 to entry: Payment providers can 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.

**4.37**
**persistent protection mechanism**
*protection* (4.38) mechanism that remains in force regardless of where the content of the original *resource* (4.40) is located or reproduced

Note 1 to entry: Persistent protection mechanisms involve *authentication* (4.4), *authorization* (4.5), and encryption technologies for effectively locking digital contents and limiting distribution to those who pay.

**4.38**
**protection**
aspect of the system that lowers the capability of a *party* (4.35) to commit *infringement* (4.21 and 4.22)

**4.39**
**provenance**
information on the place and time of origin or derivation or a *resource* (4.40) or a record or proof of authenticity or of past ownership

**4.40**
**resource**
<GeoDRM> entity that is protected by a *licence* (4.26)

Note 1 to entry: 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* (4.42) on resources and, as such, are resources in themselves.

**4.41**
**remediation**
act or process of correcting a fault or deficiency

Note 1 to entry: Remediation allows more *trust* (4.50) because it lowers *expected risk* (4.13). The first act in a remediation sequence is detection of the fault.

**4.42**
**right**
<GeoDRM> permission to act that makes a *party* (4.35) entitled to act with respect to all or part of a specified *resource* (4.40) under the terms of the license

[SOURCE: ISO/IEC 21000-5, modified]

Note 1 to entry: A right specifies an action (or activity) or a class of actions that a *principal* (4.35) can perform on or using the associated resource. A right is essentially a legally recognized entitlement to do something to or with the content of a resource.

**4.43**
**rights holder**
*principal* (4.35) that owns the *right* (4.42) to license rights to a *resource* (4.40)

Note 1 to entry: Rights can be by law (copyright), by agreement, or by *contract* (4.9) [the *licence* (4.26) agreement]. In the case of digital commerce, *DRM* (4.12) ensures that licences are adhered to, and that rights holders are compensated as appropriate for each *transaction* (4.49). *Agents* (4.3) of the original rights holder can also issue licences, but their ability is only under the *agency* (4.2) contract to the original principal.

**4.44**
**rights management**
<GeoDRM> tracking and controlling the use of content, *rights* (4.42), *licences* (4.26), and associated information

[SOURCE: See Bibliography reference 18, modified]

**4.45**
**risk**
value of what can be lost if *infringement* (4.21 and 4.22) occurs

**4.46**
**sublicence**
*licence* (4.26) granted by the original *licensee* (4.29) to a third *party* (4.35) under the grants and condition of the original licence granted to the original licensee by his *licensor* (4.31)

[SOURCE: Derived from Palmer & Dodge, LLP; (FindLaw)]

Note 1 to entry: This is essentially the *right* (4.42) to loan one's licence to another *principal* (4.35).

**4.47**
**sublicensee**
*principal* (4.35) granted a *sublicence* (4.46)

**4.48**
**sufficient**
capable of enforcing the requirements of a system

Note 1 to entry: A sufficient *DRM* (4.12) system would have to be bypassed if an *infringement* (4.21 and 4.22) would be possible. Proof of sufficiency can be difficult because it can be dependent on an "attack model", which describes the sorts of attacks to which the system is immune.

**4.49**
**transaction**
set of actions joined into the same unit of work, such that the actions either succeed or fail as a unit

[SOURCE: Web Services Glossary, modified]

**4.50**
**trust**
sum total of all mitigating factors with respect to a particular *licensee* (4.29) that reduces *expected risk* (4.13)

Note 1 to entry: Trust allows the *owner* (4.34) [or his *agent* (4.3)] to act with a higher potential *risk* (4.45) because the expected risk has been lowered. This is slightly different from the plain language of trust. Normally, trust requires something, but if the *principal* (4.35) at risk decides that no risk exists, then trust exists (in the sense here) because risk has been reduced, whatever the reason.

# 5 Conventions

## 5.1 Abbreviated terms

Abbreviated terms found in the references used in Clause 4 apply to this International Standard, plus the following abbreviated terms.

| | |
|---|---|
| API | Application Program Interface |
| DCE | Distributed Computing Environment |
| DRM | Digital Rights Management |
| GeoDRM | Geospatial Digital Rights Management |
| GI | Geographic Information (services/systems) as an extension of IT |
| GPL | General Public License |
| IDL | Interface Definition Language |
| IT | Information Technology |
| ODRL | Open Digital Rights Language |
| REL | Rights Expression Language |
| SDI | Spatial Data Infrastructure (a distributed information system for geographic data) |
| UML | Unified Modeling Language |

## 5.2 UML notation

Diagrams that appear in this International Standard 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) the interfaces between the packages to ensure interoperability and (ii) the 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 International Standard. It defines the basis for developing a geo-specific Rights Expression Language (REL) as well as other specifications necessary to establish a GeoDRM-enabled SDI. Basic definitions and concepts are defined in the ISO 21000 series of standards, especially in ISO/IEC/TR 21000-1.

— **Rights Expression Language (REL)**: This package provides the capabilities to express usage rights in the form of a machine-readable and machine-processable representation. The definition of a geo-specific Rights Expression Language is not part of this International Standard, but is to be defined upon the rights model declared in this International Standard. The basic requirements and operational semantics of a REL are defined in ISO/IEC 21000-5.

— **Encryption**: This package includes the 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 required specific to this type of data. Standard encryption methods suffice and is not dependent (in modern mechanisms) on data type.

— **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 a service-oriented architecture (SOA) can be done by adding authenticity information on the digital content that is being 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 ISO/TC 211.

— **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 ISO/TC 211.

— **Enforcement and authorization**: The rights expressed in a GeoLicence need to be enforced. In this International Standard, this package functionality is represented by the “Gatekeeper” 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 an upcoming work to be based on this International Standard.

— **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 ISO/TC 211.

## 6.2 Basics

First, DRM is a metadata-tracking problem. Both resources and principals are associated with descriptions (metadata) and those descriptions shall 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 the user 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 the 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 can be great and become critical for protection against malicious or licence-inconsistent acts of users.

## 6.3 Flow model of GeoDRM

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

— a set of one or more input resources (the start point of the arrow),

— an act (the arrow), and

— a set of zero or more of output resources (the end point of the arrow).

For example, the act of applying a WMS.GetMap to a feature collection to derive a (raster) map would be represented as follows:

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

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 can be NULL or empty. For the example above, the user would need 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

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

a) the party requesting the action,

b) the resources (data and processing being used),

c) the licences belonging to the party in a), including the descriptions of rights, resources, and conditions,

d) the owner of the resources, and a mechanism to trace his agency chains from the resources in b), and

e) the local context of the resources, including the local general rights (held by all), the applicable laws/policies, and the local security system ratings.

The Gatekeeper, using the general context available to it and the specifics of a licence presented to it, shall perform authorizations and validation of the request made to ensure that all rights needed to complete the tasks requested are available to the user making the request.

This extends to the process described in ISO/IEC 21000-5:2004, Clause 5, by including the restrictions types allowed by extension in this International Standard.

The fully compliant system shall be or contain a compliant GeoDRM metadata system and a GeoDRM Gatekeeper. It shall 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.

The GeoDRM system acts as a gatekeeper, deciding whether to allow or disallow a 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 ensured among the three basic components:

a) a security system capable of validating the documents and resource data supplied to an external request for processing;

b) a GeoDRM logic module (here called Gatekeeper) that would decide on the consistency of:

   1) the request;

   2) the licences available to the principal making the request;

   3) the processes available to the system, either directly or through other gateway/gatekeeper pairs;

c) a processing node that supplies a secured environment where licensed resources can be used without leakage.

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

In the simplest case, where a single request does not cascade, then the communication topology of Figure 3 is sufficient. The sequence is as follows.

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

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

c) The Gatekeeper verifies that the licences give the users the rights to the resources (both data and processing) that would allow the user to execute the 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.

d) If the licence does cover the request, then the security system passes the request to the geoServer for processing.

e) 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.

f) The security system passes the results to the user.

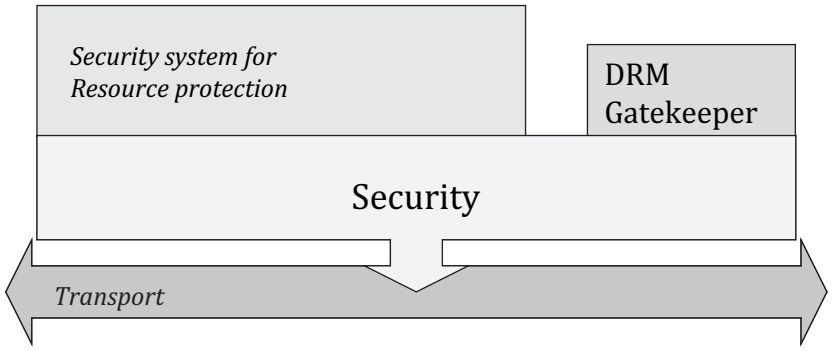


**Figure 2 — Gatekeeper metaphor for GeoDRM**

In a more complex scenario, where more than one geoServer is used, transport topologies like the one in Figure 3 can come into play.

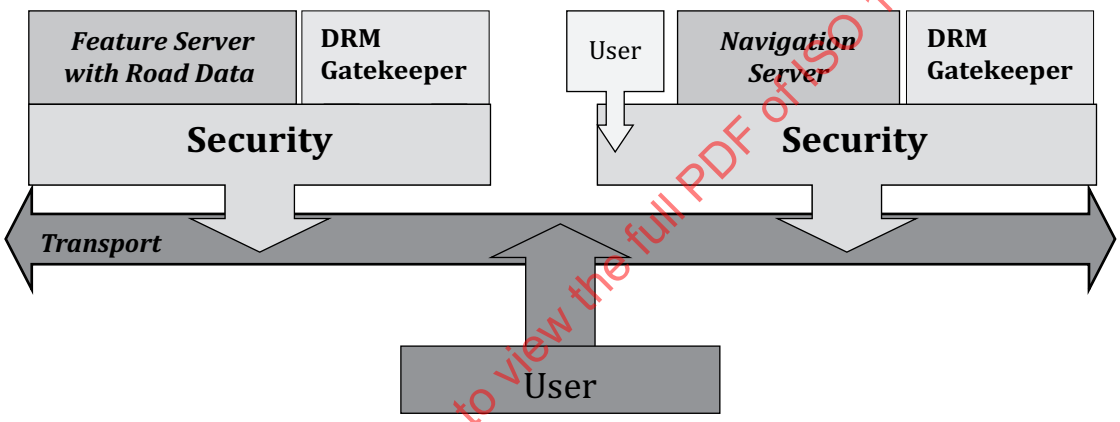


**Figure 3 — Topology for complex gatekeeper example**

In this example, a user makes a navigation request to one server, which 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 likely becomes optimized, and simpler, more direct sequences are used. For the purposes of this example, it is assumed in this International Standard that no such pre-arrangement has been put in place. The sequence of requests and responses is given in the sequence diagram in Figure 4.

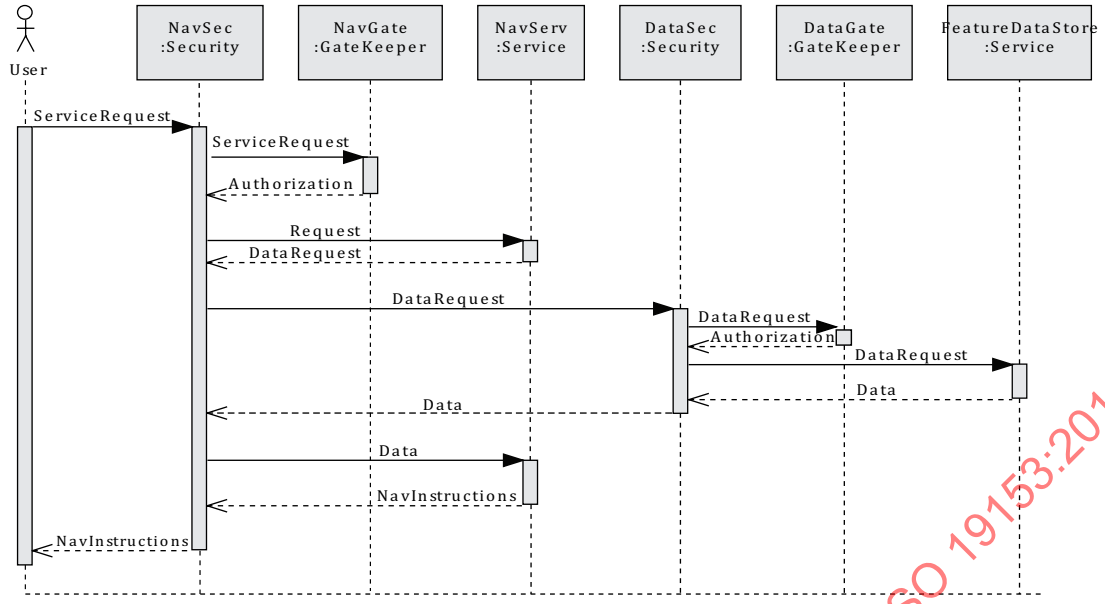


**Figure 4 — Sequence diagram for a two-stage geoServer interaction**

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

a) A request that contains the functional information, concerning the request and whatever licence information the user believes is needed, arrives from a user.

b) The security component of the system verifies the identities and the various signatures associated with the documents, which gives all documents a traceable provenance. This information is passed to the local GeoDRM Gatekeeper, which has access to all pertinent context information on the resources being invoked.

c) The Gatekeeper verifies that the licences give the user the rights to the resources (both data and processing) that would allow the user to execute the 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.

d) The security system passes the request to the local navigation geoServer for processing.

e) The navigation geoServer finds a point in the process where data from an external roads database are 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.

f) This request is passed through security to the security of the feature server.

g) The feature server security passes the transaction licence data to its local Gatekeeper.

h) The local Gatekeeper validates the transaction and returns the decision to the requesting security gateway.

i) The security passes the request to the local geoServer.

j) The local geoServer performs the task and sends the results back to the security.

k) The feature service security passes the results to the navigation server security.

l) The navigation security passes the data to the navigation server.

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

n) The security sends the final results to the user.

NOTE 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 Figure 5.

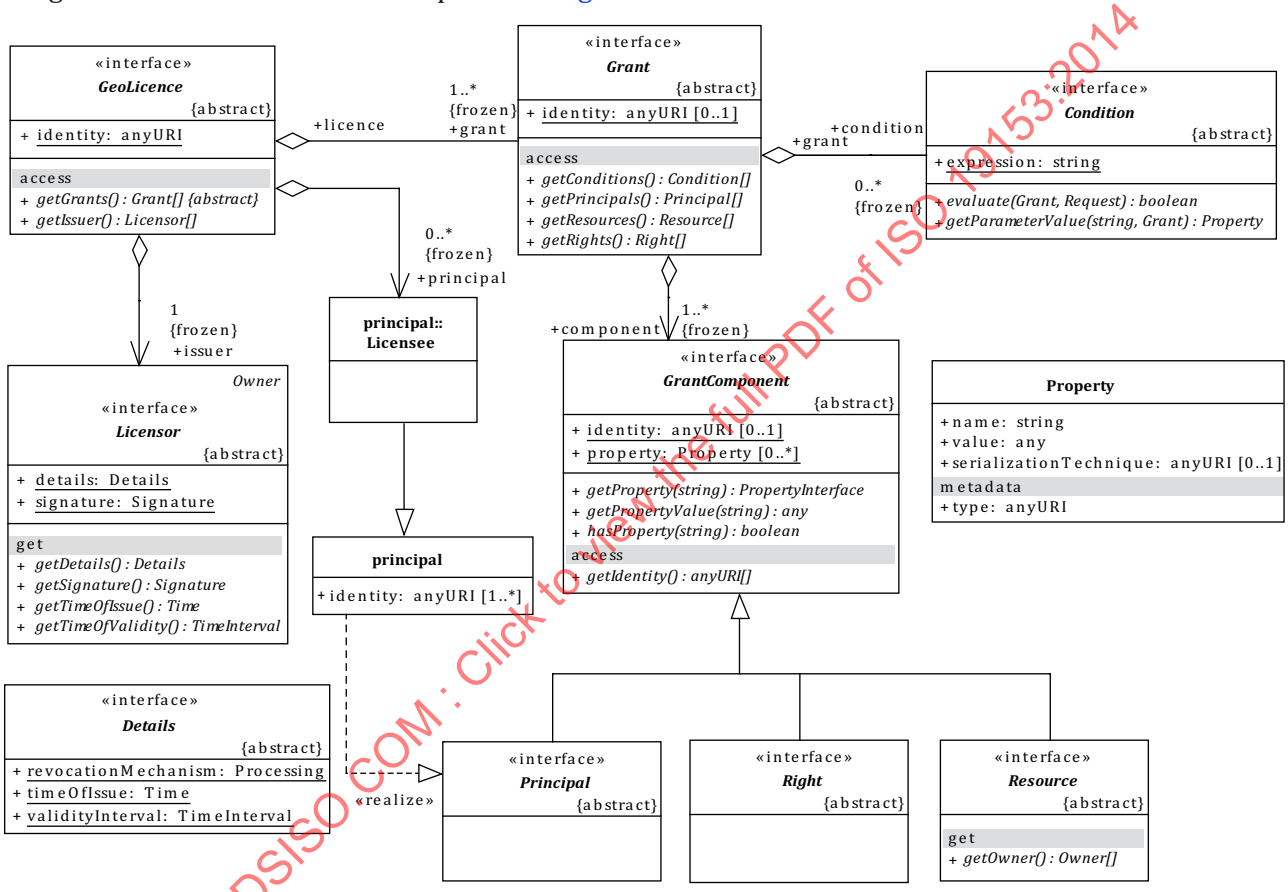


**Figure 5 — General licence model (UML)**



The basic semantics of a licence document representation is given in ISO/IEC 21000-5. A further description is given in Annex B. The parts of the licence have the conceptual meanings shown in Table 1.

**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 | Condition that modify the right |
| Issuers | 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 |

From Figure 5 and Table 1, it is shown that the needed information for DRM to work includes:

a) a mechanism for identifying the principals, for both the identification of the licensee and licensor of each licence;

b) a mechanism for identifying the resources so that licences and resources can be matched to validate the licence;

c) a set of rights that can be granted in a GeoLicence;

d) an association of each of those rights to particular "software-based" actions;

e) a definition of the types and meanings of conditions that can apply to each right, principal, or resource;

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

## 6.6 Developmental guidelines

In developing this International Standard, several design guidelines have been followed. These include, but are not limited to, the following "best practices".

— The GeoDRM model shall 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

### 6.7.1 General

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 can be acceptable.

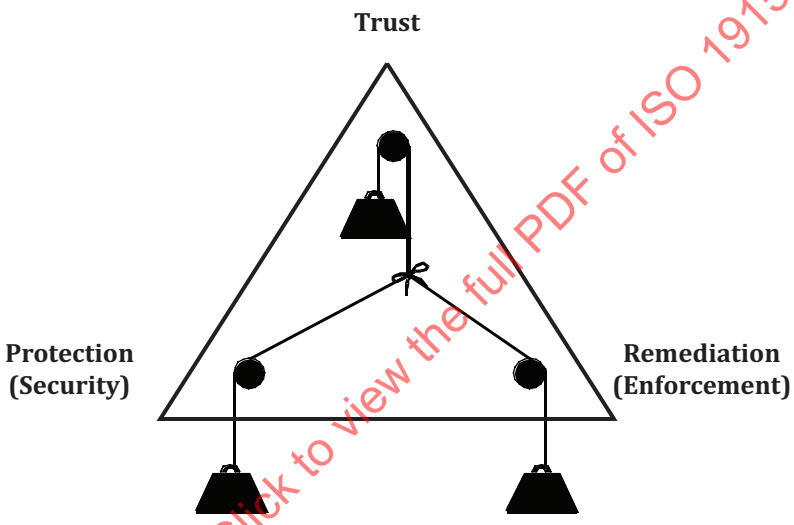


**Figure 6 — Balancing trust with protection and remediation**

These components are examined in more detail in 6.7.2 to 6.7.5.

### 6.7.2 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 Reference [1]).

The contract that exists between the buyer and the 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.

Because the DRM system should enforce that which is in the contract, and only that which is in 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 the 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 the 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 International Standard 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.

### 6.7.3 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 more protected 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 the system and the user gives some guarantee of identity. Other systems can depend on the proving of identity and reference to a valid licence with each interaction of the user and the resource.

Protection systems (i.e. security systems) are a realm unto themselves, and DRM systems become heavily dependent on the choice of security implementation (see ISO/IEC/TR 21000-1 and ISO/IEC 21000-5). 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).

### 6.7.4 Remediation — enforcement

Remediation is an act or process of correcting a fault or deficiency. Because 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 can 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 subjected 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.

### 6.7.5 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 the resources, the users, the licences, the 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 various resources, licensees, licensors, rights, and restrictions that act as a 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 can 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. Because the use of software is essential in the execution of the rights-specified acts, the identification and certification of processes can be the purview of the standards-creating organization responsible for its standardization.

The procedures involved in a DRM system at its core are 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 the 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 executing the process on the resource is allowed.

# 7 GeoDRM enterprise viewpoint and Abstract Rights Model

## 7.1 General

The key concepts needed for geospatial rights definition are defined in 7.2 to 7.11. The purpose of the GeoDRM Abstract Rights Model is to define the base conceptual model, which can 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 one enters a friend's home, permission is required. When one travels to a foreign country, presentation of passport is needed to allow 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 in the physical world. Before one can manage and protect this Intellectual Property "landscape" effectively, it is needed 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 can be practically licensed, and most importantly, rights to that Intellectual Property can be managed and protected. It is about establishing shared notions, conventions, and practices that express the boundaries within the Intellectual Property "landscape". With the defined Intellectual Property boundaries, users and owners are then able to share, exchange, and trade rights to geospatial resources in a clearly defined and managed way.

## 7.2 Geospatial resource

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

NOTE Creation of a rights management mechanism that is independent of the geospatial resource being managed is under development.

## 7.3 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 can 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, 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);

— representation parameters (such as scale, resolution, layer, or symbology);

— source of data;

— other metadata.

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 as listed above).

Figure 7 shows these three dimensions with the extents of the GeoLicence drawn as the dotted block.

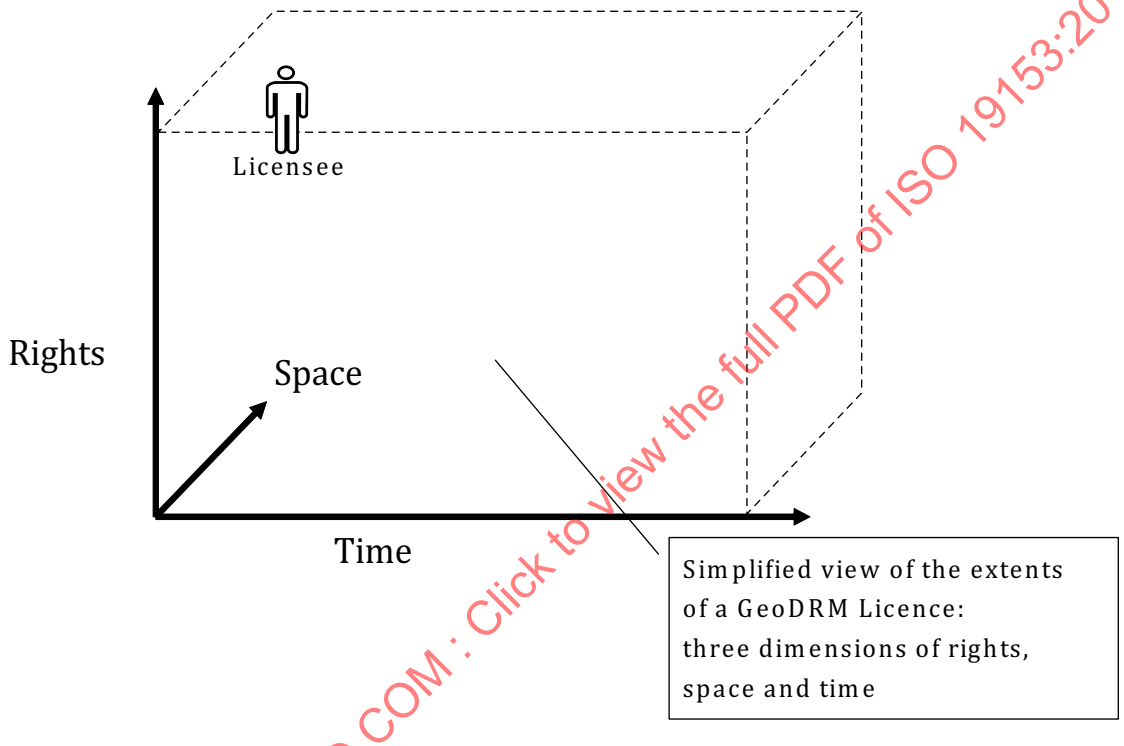


**Figure 7 — GeoLicence extents**

A GeoLicence can express the rights to view, print, copy, and update all United Kingdom road resource for 2005.

NOTE 1 Potentially, there is more than one time dimension, resource time or licence time. For example, time can 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 means the period for which the licence applies (licence time).

NOTE 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 means the geospatial extents of the GeoLicence, namely, that geospatial area of a given resource to which the licensee is granted with rights.

## 7.4 GeoLicence expression

GeoLicences can be expressed in different forms, which all essentially mean the same thing, but differ according to the intended audience. Potentially, the three corresponding expressions of GeoLicence that can be envisaged are the following:

— Legal expression: A legally binding expression of the terms and conditions of the licence, which can then be legally enforced.

— Simplified expression: A simplified, more "human"-readable version of the licence, expressing key terms and conditions, which can 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 can 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 can either be created as a result of human negotiation, or potentially, an automatic result of applying specific business rules. Third, independently of how a GeoLicence is created, the same management and enforcement mechanism should be used.

## 7.5 GeoLicence creation and enforcement

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

GeoLicences are required, whether charged 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 can be applied.

NOTE Given the limitations of the formal expression of the GeoLicence, it is not 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.

## 7.6 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 automates some or all of these functions. Various actors within the GeoDRM-enabled system 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 have to perform these administrative functions.

Figure 8 illustrates the concept of GeoLicence delegation and management. The 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 the authority to issue GeoLicences to a licensee, who can then delegate work to be done by the end-user. The end-user can then request resource within the extents of the GeoLicence. Requests that fall within the GeoLicence extents are valid, whereas 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.

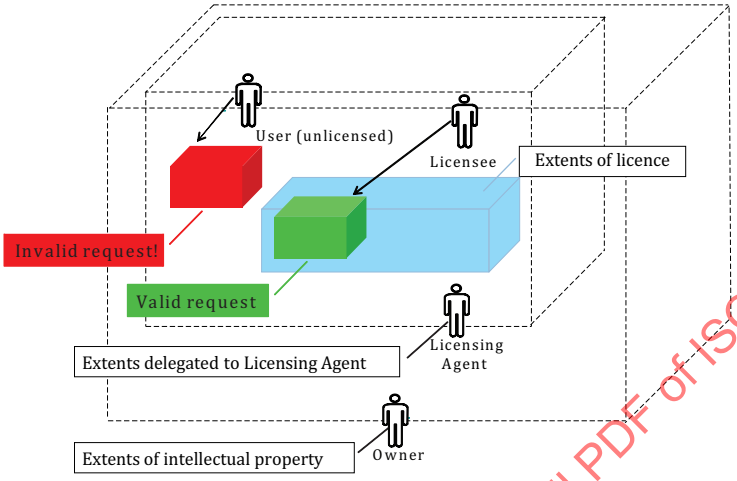


**Figure 8 — GeoLicence delegation and management**

In many ways, the concept of GeoLicence delegation and management can be considered as being analogous to the way a real-estate owner can rent a property in the real world. Often, an intermediary letting agent creates and manages rental agreements on behalf of the real-estate owner.

## 7.7 GeoLicence chaining

GeoLicences need to be traceable back to the owner of the geospatial resource. GeoLicences can 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.

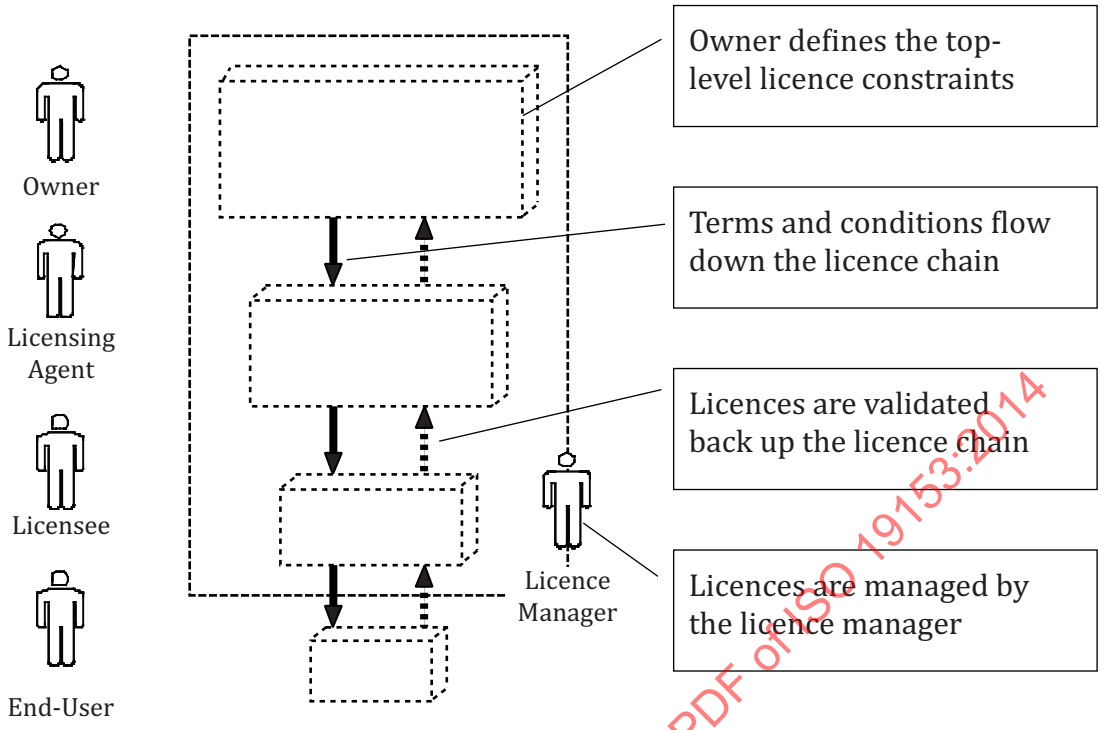


**Figure 9 — GeoLicence chaining (supporting distributed licensing)**

Figure 9 illustrates the concept of chaining the GeoLicences. This is a key concept that is needed to allow the delegation of licensing responsibility and to support the need for the distributed licensing of geospatial resources.

## 7.8 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 in Reference [27]. 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 tend to take place within communities of trading partners. Over time, standard ways of exchanging information evolve, for example, standard vocabularies to describe geographic features and processes, standard licence agreements, or perhaps standardized pricing models.

For the geospatial problem domain, the OGC has introduced the concept of an information community in their OpenGIS® Reference Model[2]:

*"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."*[28]

2) This information is given for the convenience of users of this International Standard and does not constitute an endorsement by ISO TC 211 of the product named. Equivalent products may be used if they can be shown to lead to the same results.

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 of the member who created or who will use it) and to the meaning of rights, as they are expressed in the licence. This International Standard 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 is 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:

— different business models;

— different legal rights systems;

— different organizational policies;

— broader/stricter definitions of particular rights.

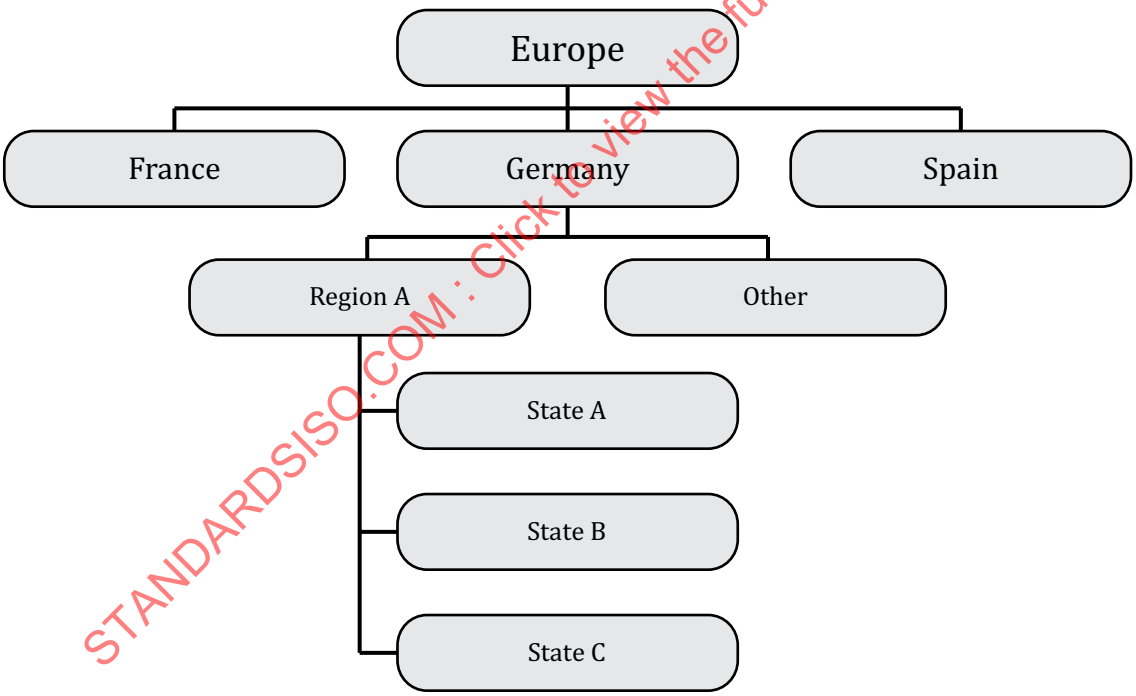




**Figure 10 — An example of GeoCommunity (based on geography)**

An example for different GeoLicensing communities, their hierarchy, and relationships for Europe is illustrated in Figure 10. 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.

## 7.9 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 are 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 allows the lineage or provenance of the derived information product to be traced. As data are 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.

## 7.10 Handling GeoLicence violation — and the break-the-glass principle

GeoLicence validation is performed by the DRM Gatekeeper. Enforcement is the combined responsibility of the associated security system and the gatekeeper. The security system verifies the information passed to the gatekeeper for the validation of the licence use. During the verification and validation of a GeoLicence, potential licence violations can be identified.

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

— Principals: the identity of the requestor, or other principals associated to him.

— Rights: the acts to be performed.

— Resources: the resources involved in the actions requested.

— Time: the time interval of the acts.

— Context: known-to-be-true facts and properties, independent of the request.

— Licence: licence elements applicable to the principal, act, or resource.

— 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 by the licensor at the time the grant was issued) is activated, then the gatekeeper triggers those side effects with the timing specified in the original grant.

If the security system performs strictly, no actual violation occurs and the user is informed of the "error" in the request (the lack of sufficient licence information). The user can also pass the 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) can place side effects 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 chain of agency, possibly all the way back to the owner.

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

1) The owner is responsible for defining what action is performed in response to a licence violation.

2) For those resources that could 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 seven items above) having side effects to allow identification of the principals who can use this option (part 1 of the seven items above), and the effects of the use of the option can be embedded as a side effect in those grants.

### 7.11 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/IEC 21000-5). The licensor informs the gatekeeper or security systems how to verify whether 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

Clause 8 sets out the basic operational concepts and entities in a GeoDRM system. Figure 11 shows the roles within a GeoDRM-enabled network of services. Within this model, an individual person or organization can 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 Figure 11, various roles have divided responsibilities, so they can 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.

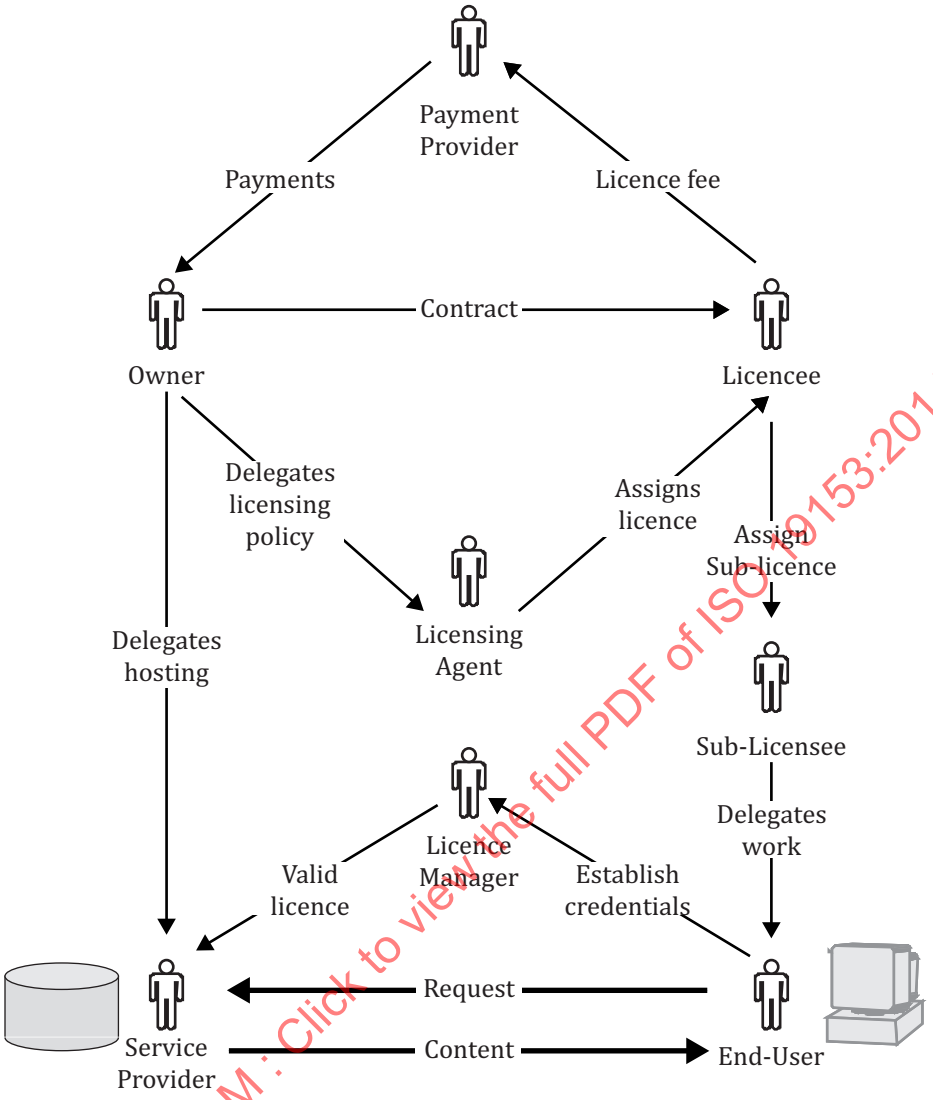


**Figure 11 — GeoDRM roles and responsibilities**

Depending on the specific business model, roles can be combined in different ways. Figure 12 shows an example business model. Business A plays the roles of the 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 can 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.

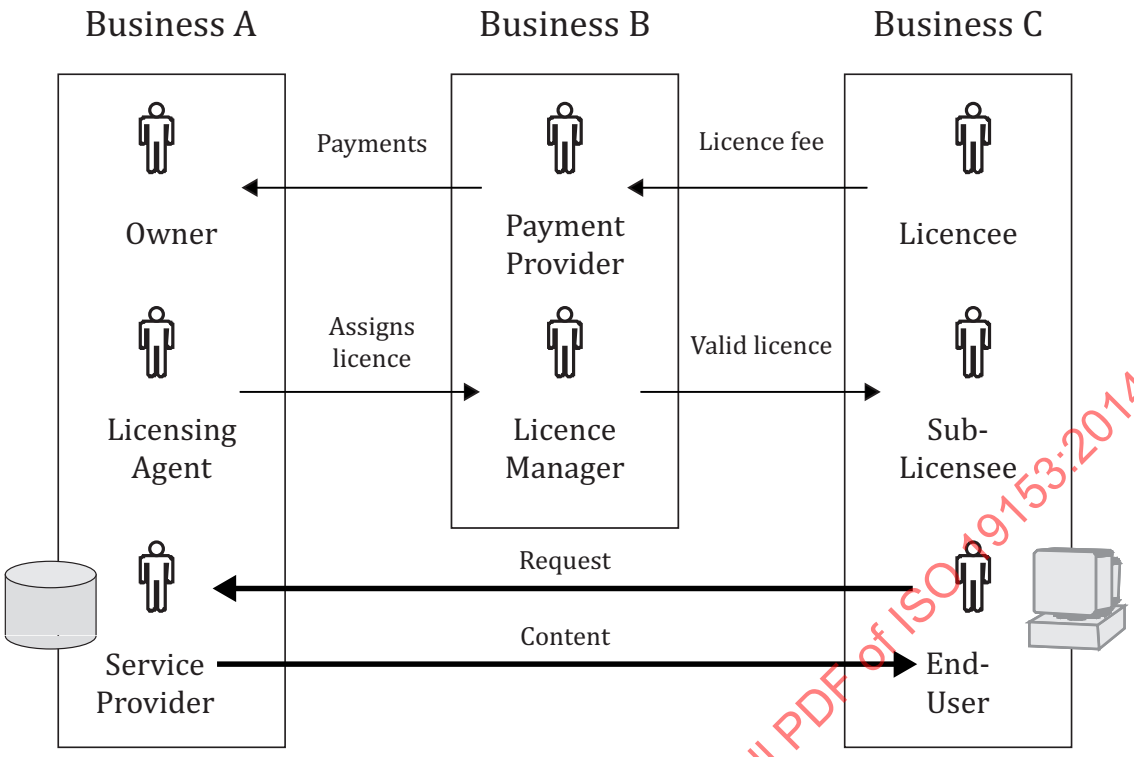


**Figure 12 — Example business model**

**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.<br>Synonyms: rights holder, content provider, licensor | Original creator of content, holds the Intellectual Property rights, and is the licensor of the Intellectual Property.<br>Defines the geospatial extents of the geospatial resource, and delegates the part or whole of those extents to a licensing agent.<br>Defines the terms and conditions to be applied within the GeoLicence (conditions can include a pricing model for access to the geospatial resource.)<br>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.<br>Ensures that any conditions for the creation of a GeoLicence (like payment) are fulfilled before issuing.<br>Ensures that a copy of the GeoLicence is registered with the licence manager for the purposes of enforcement of GeoLicence. |
| Service provider | Hosts 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.<br>Can request GeoLicences from the licence manager based on the end-user's credentials. |
| Payment provider | Manages payment transactions on behalf of the owner.<br>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 the licensing agent.<br>Can maintain outstanding balances between the owner and the 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.<br>Provides GeoLicence validation functions to service provider. |
| Licensee | Acquires the rights to access a geospatial resource. Terms and conditions of those rights are defined in the GeoLicence. | Organization or individual with an assigned set of rights as defined by the GeoLicence.<br>Rights granted by the GeoLicence can 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.<br>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 can 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 who 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.

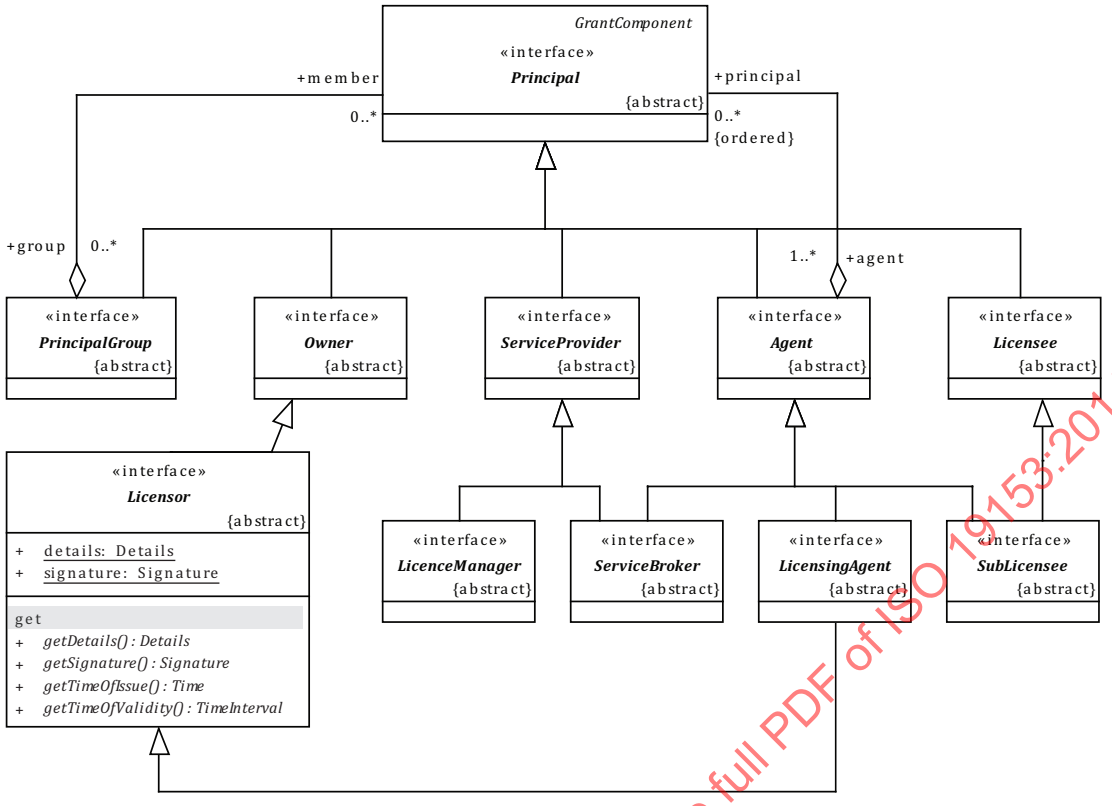


**Figure 13 — Various principals in a GeoDRM system**

## 8.3 Resource owner

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

## 8.4 Agent

Agents 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 most likely restricts the acts of the agent to specific rights as contracted with the owner.

Most agent subtypes multiply inherit (as interfaces) from the agent and, as appropriate, to other principals for the rights allocated to him by others. There could be no manner for a user to distinguish whether he is working with an agent or with the licensor supporting the agent's licence to act. The agent could 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 ensure 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 because 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 can combine multiple data sets 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 the requesting clients.

## 9 Information viewpoint

### 9.1 Overview

Clause 9 sets out the basic information entities used to express rights in a GeoLicence in a GeoDRM system. These resource types are abstract, and implementations differ based on the representation strategy. The information concepts here is used to build the metadata described in 9.2 to 9.6, 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.

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

Once stripped 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 ensure that the DRM conditions for the act are satisfied. These comparisons shall identify the following:

a) the users and licensees:

   1) the user making the request;

   2) the principal (user or group of users) identified in the licences;

b) the act and the rights:

   1) the underlying process being done;

   2) the act covering that process;

3) the acts covered by the licence;

c) the resource:

1) the resource being address by the request;

2) the resource or set of resources covered by the licences;

d) the licensor and issuer:

1) the licensors authorized to issue licences for that resource;

2) the party who issued the licence being presented by the user;

e) the conditions and constraints associated to that act in the licence:

1) the parameters used for the act:

— the constraints in the licences;

— the parameters associated to or in the request;

2) other variables:

— variables in conditions and constraints;

— the value of those variables for the request.

**Table 3 — Metadata verification and process authorization**

| Item | Reference in | Reference in | Comparison |
|---|---|---|---|
| User | User | Licence<br>Principal | User ID shall be equal to or a member of the group to whom the licence was issued. |
| Act | Process | Licence<br>Right | The act shall be explicitly covered by the licence or be a conformant implementation of a standards-based process referenced in a right. |
| Resource | Licence<br>Resource | Resource<br>Identity | Equal or consistent with a larger group |
| Parameter values | Process<br>Request | Licence<br>Constraints<br>Parameters | Consistency, usually as a containment test |
| Issuer | Licence<br>Issuer | Resource<br>Owner | The licence shall be issued by the owner of the resource or by his agent. The owner-agent relation shall 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 be changed without affecting the existing licences. Therefore, once defined and accepted as a standard, a right shall not have any 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 carries a dated definition in that registry.

Further, once a licence is issued, it shall not be changed (only the issuer prior to delivery can 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 shall have the right to grant rights specified in the licence.

For a licensing system to be conformant to this International Standard, the types of metadata described in this information model shall be available to the gatekeeper and shall be properly interpreted in the assessment of rights.

## 9.2 User metadata

The basic user metadata is identity. Participants in a DRM system (principals in terms of ISO/IEC 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 can be used because they carry the same information. The property formalisms are more appropriate here because 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[3]).

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 is 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 shall be a verifiable property attached to the principal declaring his citizenship or resident status. However, it is so difficult to ask, “Who are the US residents?”, so much so that the US government tries for an accurate list only once every 10 y, 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 ensure 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 19119, 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 can be resource independent, in which case the resource part of a grant component can be unspecified.

3) This information is given for the convenience of users of this document and does not constitute an endorsement by ISO TC 211 of the product named. Equivalent products may be used if they can be shown to lead to the same results.

### 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 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 both by the name and the version of the specification, and recognized as such in a trusted public registry, either supported by ISO, OGC, or some other recognized body. The processing shall 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 can 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 is by URL, URI, or URN that identifies the processing address or the registry entry in a licensor-trusted registry.

A service supplier can 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/IEC 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 license conformant to this International Standard shall conform to the model in this International Standard. This clause contains that model.

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 can be applied.

### 9.5.2 Principal or licensee

Within a licence, principal references within the rights grants can 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 are given;

— the resource upon which the right can be exercised;

— the rights which are granted;

— any conditions that modify any of the above.

The GeoDRM Gatekeeper is responsible for matching such grants with processing requests. Multiple resources can be involved in one request. Each grant in a licence can specify a separate resource. Consequently, a request is authorized if, and only if, for each licensed resource in the request there is at least one grant, which matches 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/IEC 21000-5 as "an act identified by an r:Right" which is an element of a licence. Rights can 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 systems, 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 that perform acts on the entity as a whole without an interpretation of its meanings (Such rights might include copying, indexing, moving, and 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 system.).

##### 9.5.3.2.2 Note on multiple copies of resource and rights names

When a resource exists in multiple identical copies, it can carry the same resource identity and be manipulated by licensees holding the appropriate rights on the resource. Any modification of the resource shall 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". Because integration with the GeoDRM system requires compliance with DRM standards, they 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 right. Thus, many of the rights in the sections to follow can be collectively given by a single Use right. This right can be defined as a collection of the rights, or can 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 can be restricted by that user's rights condition.

Because 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 can 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 can 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 shall carry this same *"**Combine**"* right and be of the same information type (e.g. all images, all maps, and 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 can 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 can 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***" right 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 the 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 can 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 can modify the rights allowed to be licensed on the derived resource. Other rights that create new resources from existing ones can 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 can 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.

Because 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 to 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 shall be found for the processing resource being

used and for each parameter. If a parameter resource licence is needed, it can 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 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 could 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 right

The "***Sublicense***" right allows the principal holding the licence grant to loan that right to others. The loaned licence has 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 Annex B for the UML model). Any of these can 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 can 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 that 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 third 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;

— 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". Because integration with the GeoDRM system requires compliance with DRM standards, they carry both the base functionality proof and the GeoDRM proof of compliance.

#### 9.5.3.3.4 Output conditions

The licence can 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 usually becomes the assignment of meta-rights and properties for this new resource.

So, if a grant defines a View right that produces an output map and an Extract right that produces an output resource, then the grant can use the following structure:

— Grant
  — Principal = …
  — Resource = …
  — Right = view
    — Output→map
      — →Meta-rights = {view}
      — →Meta-data
        • →Disclaimer contains "This map contains privately owned 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 owned 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, can be restricted by the type of right so conveyed, or the persons or type of persons to whom the right can be conveyed. So a grant can contain the following type of structure:

- 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 can limit the spatial or temporal extent of the resource that the actions allowed by the right can address. The expression of a spatial, temporal, or spatiotemporal extent can be in any coordinate reference system or can cover multiple reference systems for subsets of the coordinates. The default coordinate reference system (CRS) is WGS 84 Latitude–Longitude (the CRS used by GPS), and the default temporal reference system is Universal Time (Zulu) [the trimble reference station (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 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 processed 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 the 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 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 can be used in using a right. If unspecified, any provably conformant implementation of the functionality is allowed. If specific implementations are identified, they can be allowed or disallowed specifically.

This can be part of the trust model of the resource owner. For example, a company can wish to ensure itself of the safety of the DRM by individually testing the applications for what they consider a level of security. In this case, the company can 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 can require that his resource be served only 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 can 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 with 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 can be used to restrict or expand the rights that can be licensed by the creator of the derived resource in conjunction with the derived resource.

For example, if a feature resource supplier wishes to ensure the manner in which his resource is used "second hand" through another process, then he can 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 because the first user could not convey rights other than View right 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 can restrict the form in which the particular resource can be presented. If absent, the default logic of the condition is that all lossless encodings are allowed.

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

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

Postcondition side effects can cause extra validation on the output resources or be linked into the billing system of the licensor. Such conditions can 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 shall 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 can 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
(normative)

# Abstract test suite

## A.1 Items covered

This International Standard creates conceptual requirements for the following:

a) rights expression languages;

b) metadata for identification of principals, processes, rights, and resources;

c) GeoDRM Gatekeeper components for use in protection and enforcement systems, including GeoDRM as a requirement.

## A.2 Rights expression languages conformance class

Rights expression languages are used to create GeoLicences with unambiguous meanings, as specified in this International Standard. A licence conformant to this International Standard shall conform to the model in this International Standard (see 9.5).

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

The test case is as follows:

a) test purpose: check the conformance of a license to the definition of the model;

b) test method: automated parser dependent on licence language;

c) reference: 9.5;

d) test type: capability.

## A.3 Metadata system conformance class

A GeoDRM metadata system, as a subsystem of a geographic system, shall ensure 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. See 9.2, 9.3, and 9.4.

For a licensing system to be conformant to this International Standard, the types of metadata described in this information model shall be available to the Gatekeeper and shall be properly interpreted in the assessments of rights.

The test case is as follows:

a) test purpose: check whether the Gatekeeper is capable of using use global metadata properly;

b) test method: vary global metadata available to the Gatekeeper and test for proper decisions;

c) reference: 9.2, 9.3, 9.4, and ISO/IEC 21000-5:2004, Clause 5;

d) test type: capability.

## A.4 Gatekeeper conformance class

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. See Clause 9 and 6.4.

The Gatekeeper, using the general context available to it and the specifics of a licence presented to it, shall perform the authorizations and validations of the request made to ensure that all rights needed to complete the tasks requested are available to the user making the request.

The test case is as follows:

a) test purpose: check whether the Gatekeeper is capable of using use licence data properly;

b) test method: keeping global metadata constant, supply the Gatekeeper with requests and licence sets and test for proper decisions;

c) reference: Clause 9, 6.4, and ISO/IEC 21000-5:2004, Clause 5;

d) test type: capability.

# Annex B
(informative)

# GeoDRM UML model

## B.1 Semantics

The UML model in Annex B represents a valid interpretation of the information model presented in Clause 9.

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 are logically equivalent.

The rest of Annex B is a documentation format provided by a UML tool [Enterprise Architect, from SparxSystems, Ltd. Australia (http://www.sparxsystems.com.au/)][4]. 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 are possible, but they should be information equivalent to the one contained here.

## B.2 Class diagrams

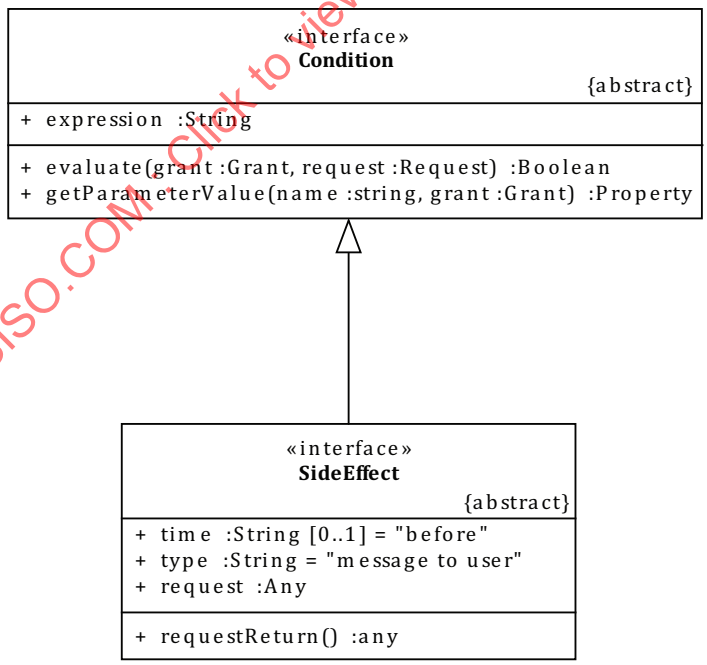


**Figure B.1 — Condition**



4) This information is given for the convenience of users of this document and does not constitute an endorsement by ISO TC 211 of the product named. Equivalent products may be used if they can be shown to lead to the same results.

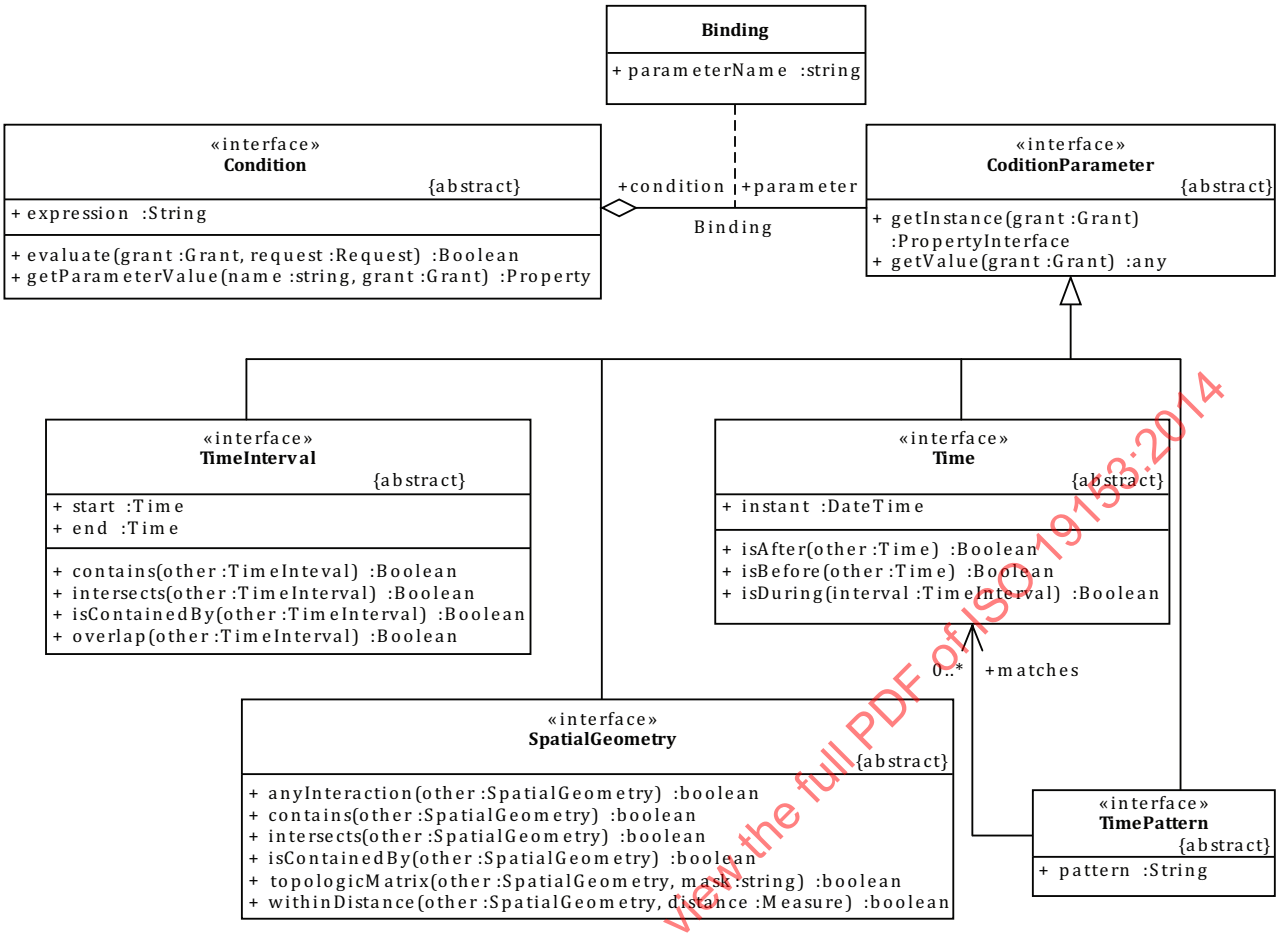


**Figure B.2 — Condition binding**

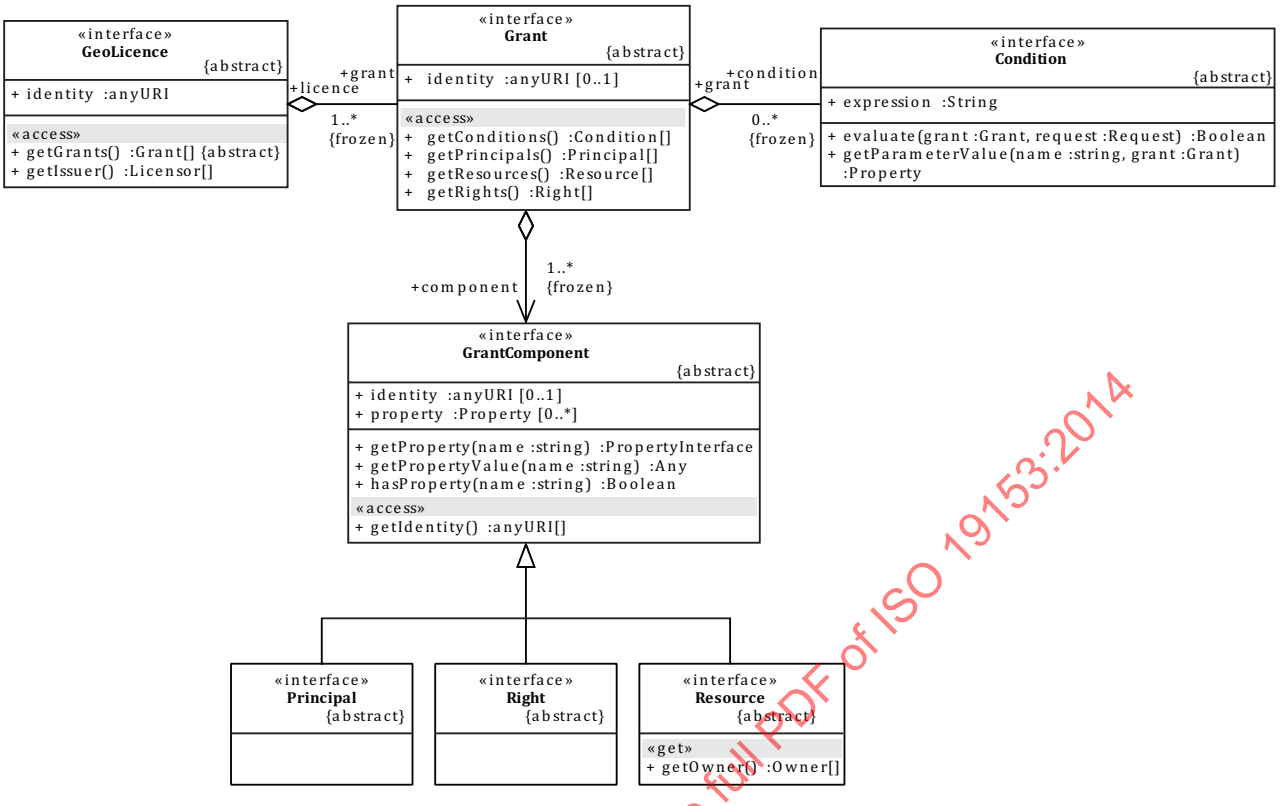


**Figure B.3 — Grant**

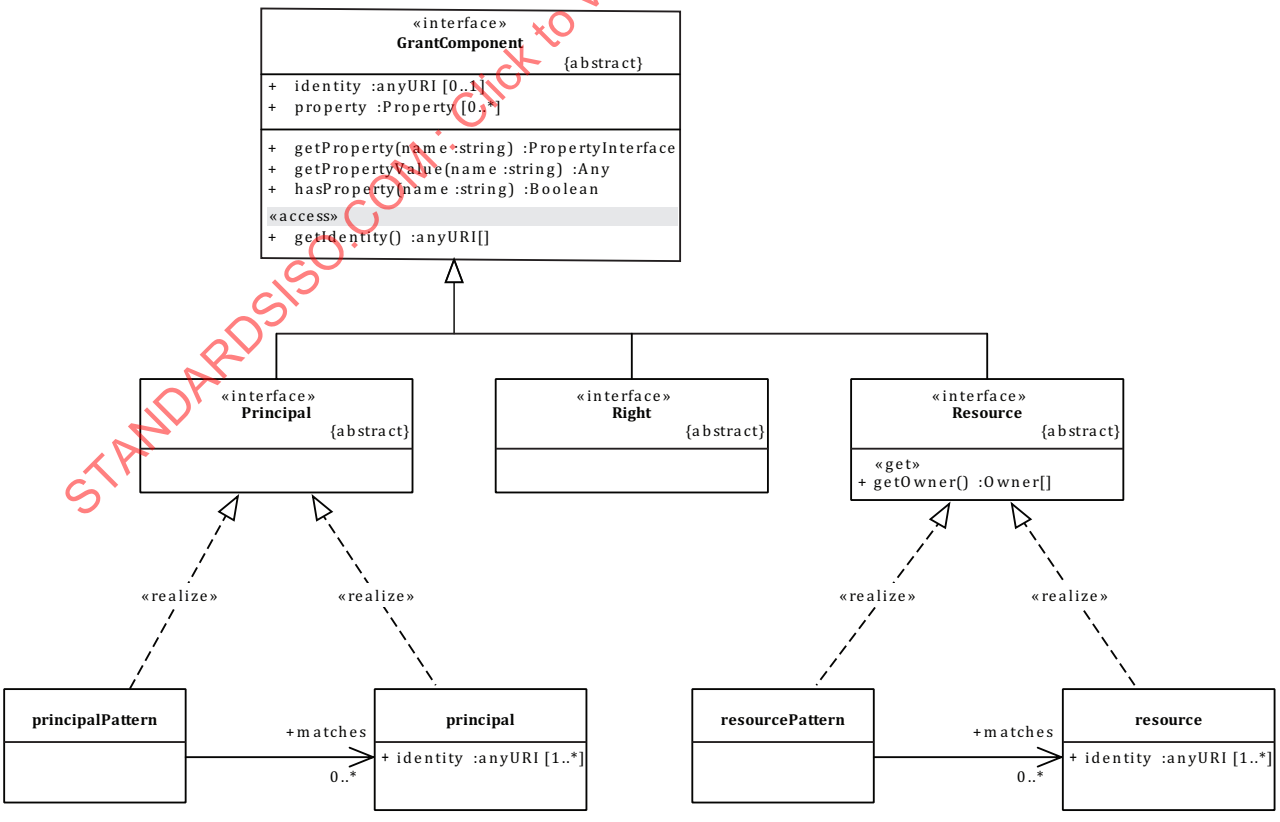


**Figure B.4 — Grant components: principal, right, and resource**

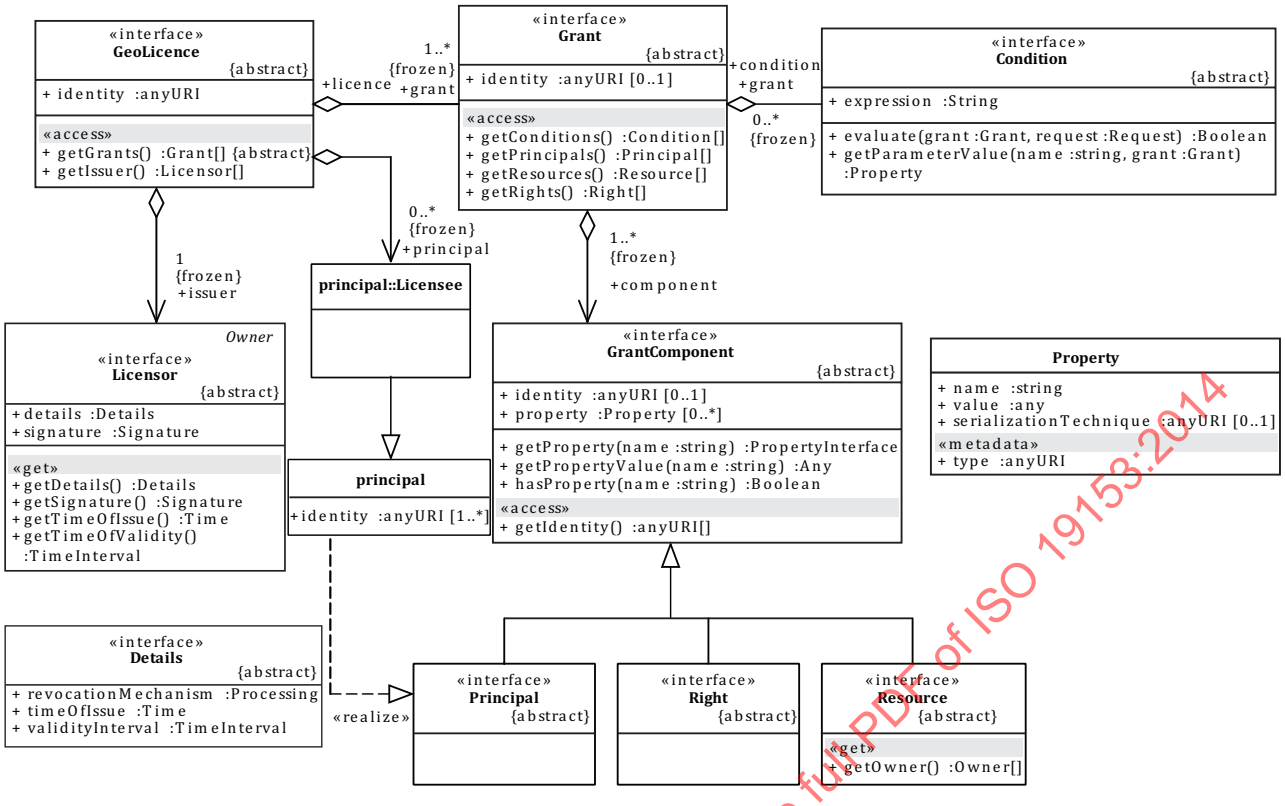


**Figure B.5 — Licence**

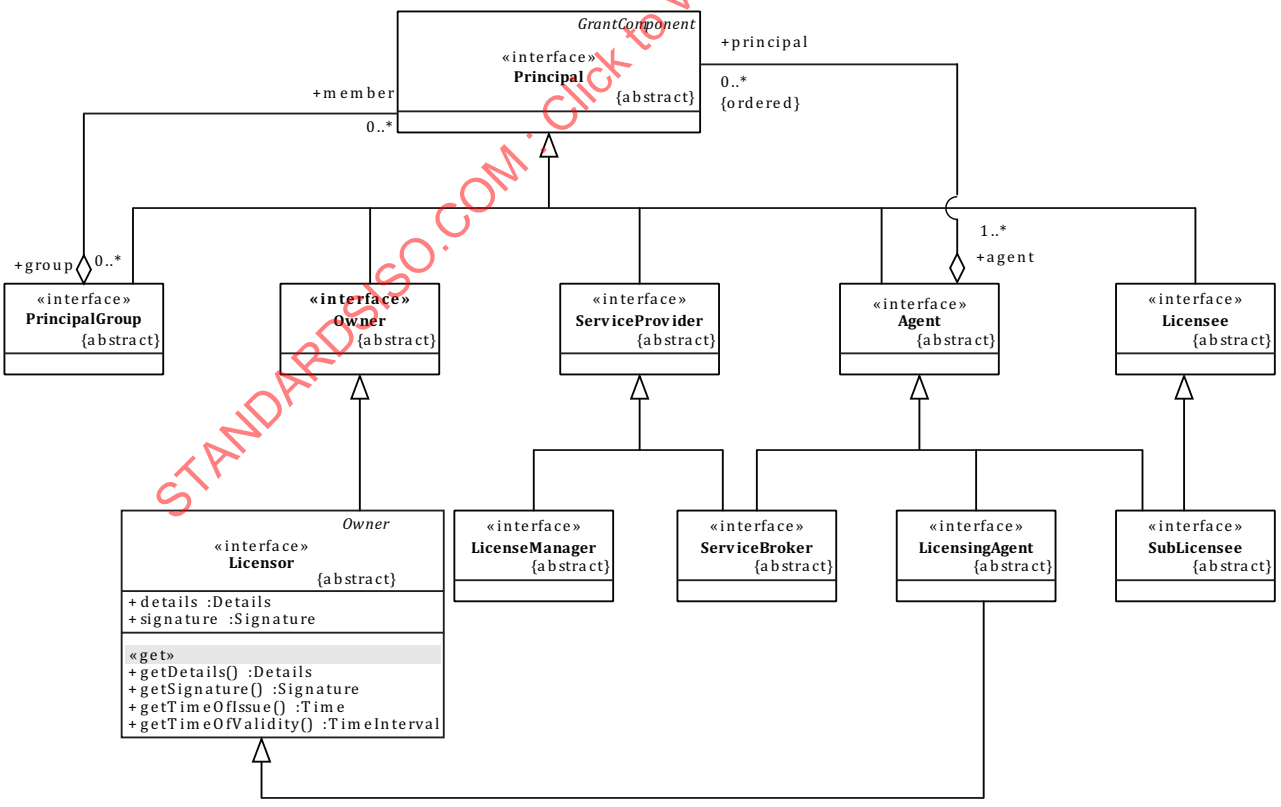


**Figure B.6 — Principal**

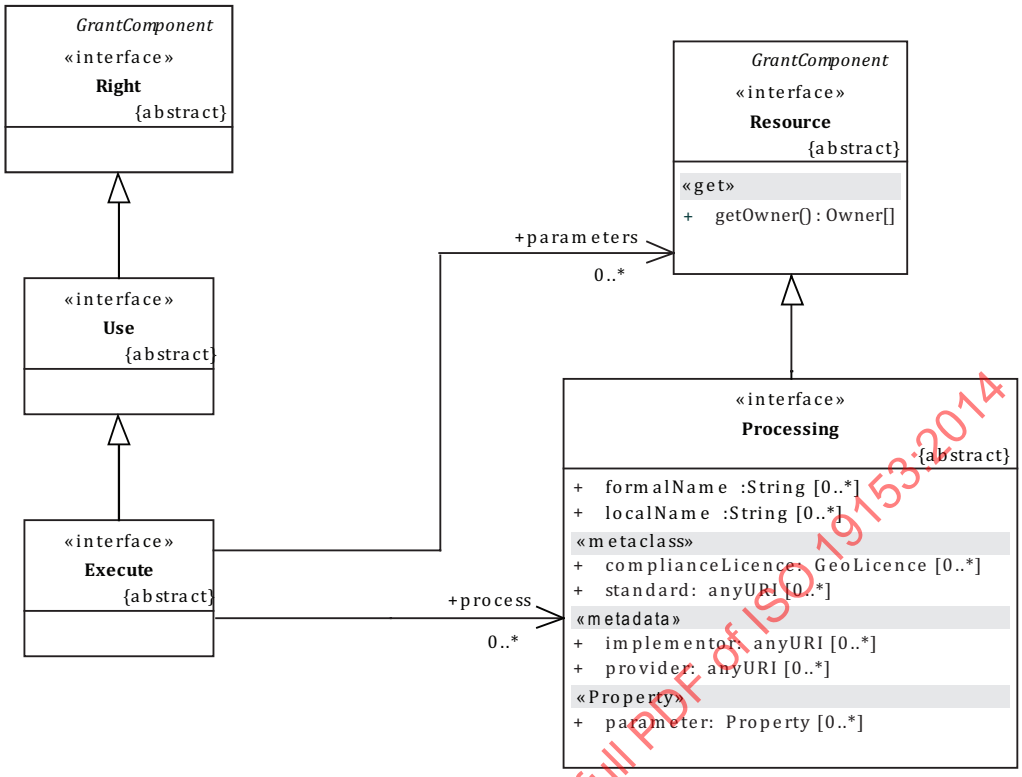


**Figure B.7 — Processing right**

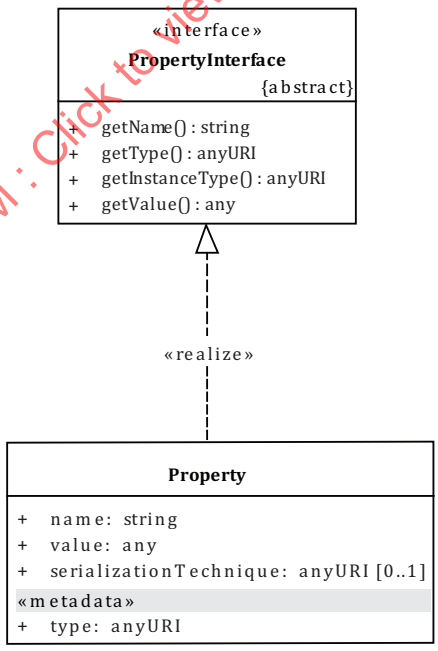


**Figure B.8 — Properties**

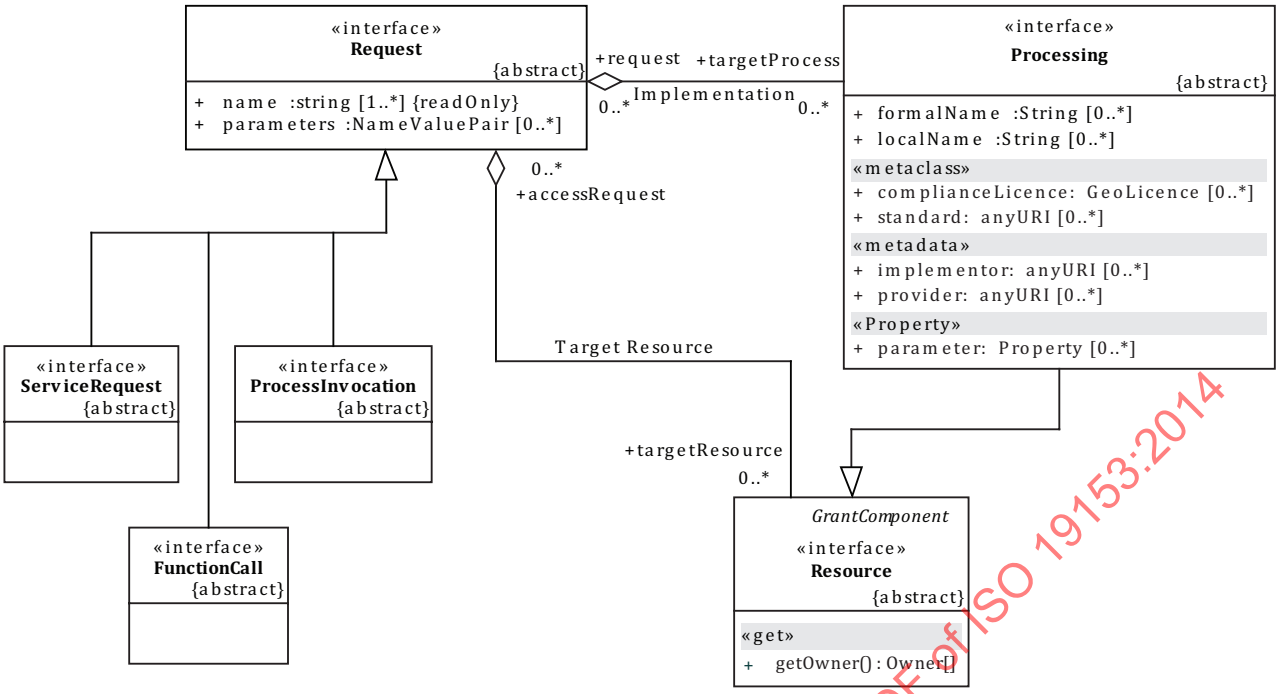


**Figure B.9 — Request**

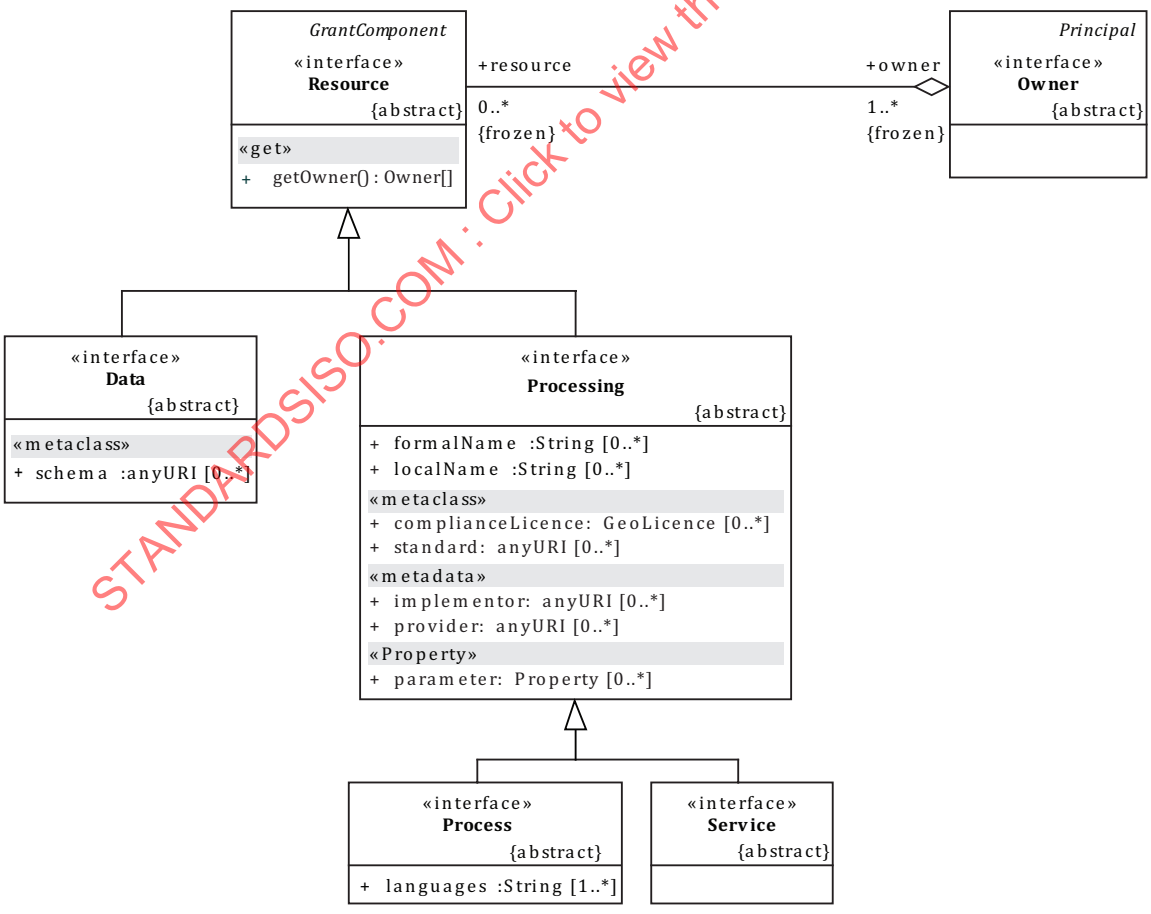


**Figure B.10 — Resources**

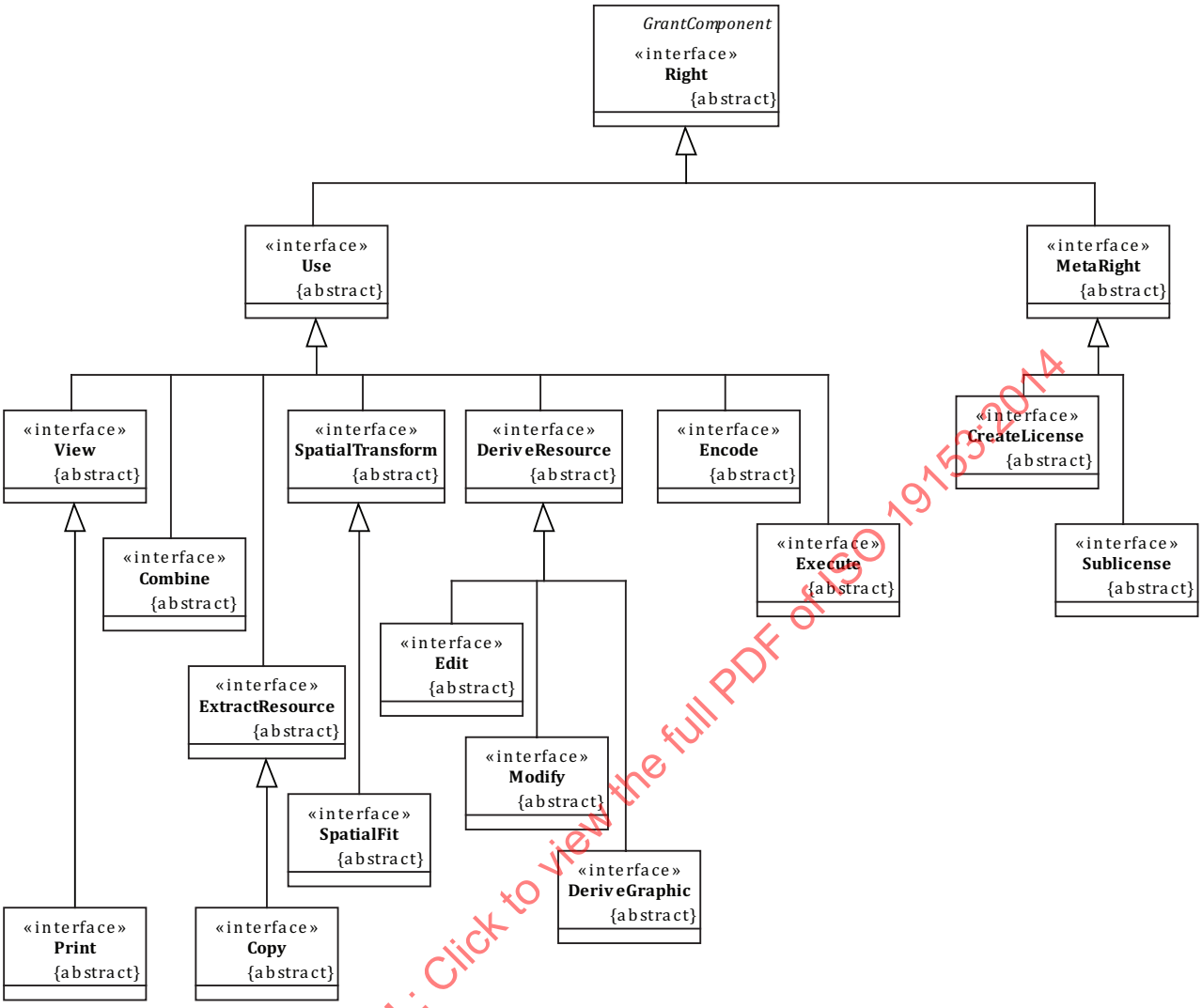


**Figure B.11 — Rights**



## 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) shall 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:<br>*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**<br>source > target | **principalPattern**<br>unordered | **principal**<br>+matches<br>0..*, unordered | |
| **Generalization**<br>source > target | **Licensee**<br>Child | **principal**<br>Parent | |
| **Realization**<br>«realize»<br>source > target | **principal**<br>Child | **Principal**<br>Parent | |

**Table B.3 — Principal attributes**

| Attribute | Type | Notes |
|---|---|---|
| identity | public:<br>*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 use this principal as the default recipient of each grant. If a grant contains a principal, it overrides the licensee as the recipient of the grant.

**Table B.4 — principal::Licensee connections**

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

## B.7 principalPattern

*Type:* *public* **Class**

Implements: *Principal.*

*Package*: GeoLicence

**Table B.5 — principalPattern connections**

| Connector | Source | Target | Notes |
|---|---|---|---|
| **Association**<br>source > target | **principalPattern**<br>unordered | **principal**<br>+matches<br>0..*, unordered | |
| **Realization**<br>«realize»<br>source > target | **principalPattern**<br>Child | **Principal**<br>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**<br>«realize»<br>source > target | **Property**<br>Child | **PropertyInterface**<br>Parent | |

**Table B.7 — Property attributes**

| Attribute | Type | Notes |
|---|---|---|
| name | public:<br>*String* | |
| type<br>«metadata» | public:<br>*anyURI* | |
| value | public:<br>*Any* | |
| serializationTechnique | public<br>Range:0 to 1:<br>*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**<br>source > target | **resourcePattern**<br>unordered | **resource**<br>+matches<br>0..*, unordered | |
| **Realization**<br>«realize»<br>source > target | **resource**<br>Child | **Resource**<br>Parent | |

**Table B.9 — resource attributes**

| Attribute | Type | Notes |
|---|---|---|
| identity | public<br>Range:1 to *:<br>*anyURI* | |

## B.11 resourcePattern

*Type:* *public* **Class**

Implements: *Resource*.

*Package:* GeoLicence

**Table B.10 — resourcePattern connections**

| Connector | Source | Target | Notes |
|---|---|---|---|
| **Association**<br>source > target | **resourcePattern**<br>unordered | **resource**<br>+matches<br>0..*, unordered | |
| **Realization**<br>«realize»<br>source > target | **resourcePattern**<br>Child | **Resource**<br>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 shall also support the interfaces of his "client", the principal for whom he acts.

**Table B.11 — Agent connections**

| Connector | Source | Target | Notes |
|---|---|---|---|
| **Aggregation**<br>source > target | **Principal**<br>+principal<br>0..*, ordered, none | **Agent**<br>+agent<br>1..*, unordered | |
| **Generalization**<br>source > target | **SubLicensee**<br>Child | **Agent**<br>Parent | |
| **Generalization**<br>source > target | **Agent**<br>Child | **Principal**<br>Parent | |
| **Generalization**<br>source > target | **ServiceBroker**<br>Child | **Agent**<br>Parent | |
| **Generalization**<br>source > target | **LicensingAgent**<br>Child | **Agent**<br>Parent | |

## B.13 ConditionParameter

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

*Package:* GeoLicence

Condition parameter 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**<br>Binding | **Condition**<br>+condition<br>unordered | **ConditionParameter**<br>+parameter<br>unordered | |
| **Generalization**<br>source > target | **Time**<br>Child | **ConditionParameter**<br>Parent | |
| **Generalization**<br>source > target | **SpatialGeometry**<br>Child | **ConditionParameter**<br>Parent | |
| **Generalization**<br>source > target | **TimePattern**<br>Child | **ConditionParameter**<br>Parent | |
| **Generalization**<br>source > target | **TimeInterval**<br>Child | **ConditionParameter**<br>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**<br>source > target | **Combine**<br>Child | **Use**<br>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 shall evaluate to TRUE. This Boolean function 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**<br>+condition<br>0..*, unordered, frozen | **Grant**<br>+grant<br>unordered | |
| **Association**<br>Binding | **Condition**<br>+condition<br>unordered | **ConditionParameter**<br>+parameter<br>unordered | |
| **Generalization**<br>source > target | **SideEffect**<br>Child | **Condition**<br>Parent | |

**Table B.16 — Condition attributes**

| Attribute | Type | Notes |
|---|---|---|
| expression | public:<br>*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 invalidates the use of that licence grant in the given circumstances. |

**Table B.17 — Condition interfaces**

| Method | Type | Notes |
|---|---|---|
| evaluate (*Grant, Request*) | public: *Boolean* | public: param: grant [ Grant - in ]<br>param: request [ Request - in ]<br>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 ]<br>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**<br>source > target | **Copy**<br>Child | **ExtractResource**<br>Parent | |

## B.17 CreateLicence

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

Extends: *MetaRight*.

*Package:* GeoLicence

**Table B.19 — CreateLicence connections**

| Connector | Source | Target | Notes |
|---|---|---|---|
| **Generalization**<br>source > target | **CreateLicence**<br>Child | **MetaRight**<br>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 can 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**<br>source > target | **Data**<br>Child | **Resource**<br>Parent | |

**Table B.21 — Data attributes**

| Attribute | Type | Notes |
|---|---|---|
| schema<br>«metaclass» | public<br>Range:0 to *:<br>*anyURI* | The “schema” attribute allows the Data resource to specify its structural metadata. All data entities in the resource shall 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 are possible) that is a view-only representation of some subset of the original resources.

**Table B.22 — DeriveGraphic connections**

| Connector | Source | Target | Notes |
|---|---|---|---|
| **Generalization**<br>source > target | **DeriveGraphic**<br>Child | **DeriveResource**<br>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 can 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**<br>source > target | **Edit**<br>Child | **DeriveResource**<br>Parent | |
| **Generalization**<br>source > target | **Modify**<br>Child | **DeriveResource**<br>Parent | |
| **Generalization**<br>source > target | **DeriveResource**<br>Child | **Use**<br>Parent | |
| **Generalization**<br>source > target | **DeriveGraphic**<br>Child | **DeriveResource**<br>Parent | |

## B.21 Details

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

*Package:* GeoLicence

**Table B.24 — Details attributes**

| Attribute | Type | Notes |
|---|---|---|
| revocationMechanism | public:<br>*Processing* | Process for revocation of the licence |
| timeOfIssue | public:<br>*Time* | Time the licence was issued |
| validityInterval | public:<br>*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**<br>source > target | **Edit**<br>Child | **DeriveResource**<br>Parent | |

## B.23 Encode

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

Extends: *Use.*

*Package:* GeoLicence

**Table B.26 — Encode connections**

| Connector | Source | Target | Notes |
|---|---|---|---|
| **Generalization**<br>source > target | **Encode**<br>Child | **Use**<br>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 shall have an "execute" licence for both the process (which specifies which resources it can process) and the information resource (which specifies which processes can be executed on it).

**Table B.27 — Execute connections**

| Connector | Source | Target | Notes |
|---|---|---|---|
| **Association**<br>source > target | **Execute**<br>unordered | **Processing**<br>+process<br>0..*, unordered | |
| **Association**<br>source > target | **Execute**<br>unordered | **Resource**<br>+parameters<br>0..*, unordered | |
| **Generalization**<br>source > target | **Execute**<br>Child | **Use**<br>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**<br>source > target | **Copy**<br>Child | **ExtractResource**<br>Parent | |
| **Generalization**<br>source > target | **ExtractResource**<br>Child | **Use**<br>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**<br>source > target | **FunctionCall**<br>Child | **Request**<br>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**<br>+grant<br>1..*, unordered, frozen | **GeoLicence**<br>+licence<br>unordered | |
| **Aggregation**<br>source < target | **Licensor**<br>+issuer<br>1, unordered, frozen | **GeoLicence**<br>unordered | Principal who composed the licence. The issuer of a licence shall have the right to create and grant the licence in question. All such rights flow from the owner or from one of his agents. |
| **Aggregation**<br>source < target | **Licensee**<br>+principal<br>0..*, unordered, frozen | **GeoLicence**<br>unordered | Principal to whom the licence was given. |

**Table B.31 — GeoLicence attributes**

| Attribute | Type | Notes |
|---|---|---|
| identity | public:<br>*anyURI* | |

**Table B.32 — GeoLicence interfaces**

| Method | Type | Notes |
|---|---|---|
| getGrants () | «access»<br>public abstract: *Grant* | |
| getIssuer () | «access»<br>public: *Licensor* | |

## B.28 Grant

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

*Package:* GeoLicence

**Table B.33 — Grant connections**

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

**Table B.34 — Grant attributes**

| Attribute | Type | Notes |
|---|---|---|
| identity | public<br>Range:0 to 1:<br>*anyURI* | |

**Table B.35 — Grant interfaces**

| Method | Type | Notes |
|---|---|---|
| getConditions () | «access»<br>public: *Condition* | |
| getPrincipals () | «access»<br>public: *Principal* | |
| getResources () | «access»<br>public: *Resource* | |
| getRights () | «access»<br>public: *Right* | |

## B.29 GrantComponent

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

*Package:* GeoLicence

**Table B.36 — GrantComponent connections**

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

**Table B.37 — GrantComponent attributes**

| Attribute | Type | Notes |
|---|---|---|
| identity | public<br>Range:0 to 1:<br>*anyURI* | |
| property | public<br>Range:0 to *:<br>*Property* | The property attribute lists named properties of this entity. |

**Table B.38 — GrantComponent interfaces**

| Method | Type | Notes |
|---|---|---|
| getIdentity () | «access»<br>public: *anyURI* | |
| getProperty (*String*) | public: *Property* | param: name [ String - in ]<br>The getProperty operation returns the property descriptor of a particularly named property. |
| getPropertyValue (*String*) | public: *Any* | param: name [ String - in ]<br>The getPropertyValue operation returns the value of a particularly named property. |
| hasProperty (*String*) | public: *Boolean* | param: name [ String - in ]<br>The hasProperty operation determines the entity process of 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**<br>source > target | **SubLicensee**<br>Child | **Licensee**<br>Parent | |
| **Generalization**<br>source > target | **Licensee**<br>Child | **Principal**<br>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**<br>source > target | **LicenceManager**<br>Child | **ServiceProvider**<br>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**<br>source > target | **LicensingAgent**<br>Child | **Licensor**<br>Parent | |
| **Generalization**<br>source > target | **LicensingAgent**<br>Child | **Agent**<br>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**<br>source < target | **Licensor**<br>+issuer<br>1, unordered, frozen | **GeoLicence**<br>unordered | Principal who composed the licence. The issuer of a licence shall have the right to create and grant the licence in question. All such rights flow from the owner or from one of his agents. |
| **Generalization**<br>source > target | **Licensor**<br>Child | **Owner**<br>Parent | |
| **Generalization**<br>source > target | **LicensingAgent**<br>Child | **Licensor**<br>Parent | |

**Table B.43 — Licensor attributes**

| Attribute | Type | Notes |
|---|---|---|
| details | public:<br>*Details* | |
| signature | public:<br>*Signature* | |

**Table B.44 — Licensor interfaces**

| Method | Type | Notes |
|---|---|---|
| getDetails () | «get»<br>public: *Details* | attribute_name = 'details' |
| getSignature () | «get»<br>public: *Signature* | attribute_name = 'signature' |
| getTimeOfIssue () | «get»<br>public: *Time* | |
| getTimeOfValidity () | «get»<br>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**<br>source > target | **CreateLicence**<br>Child | **MetaRight**<br>Parent | |
| **Generalization**<br>source > target | **Sublicence**<br>Child | **MetaRight**<br>Parent | |
| **Generalization**<br>source > target | **MetaRight**<br>Child | **Right**<br>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**<br>source > target | **Modify**<br>Child | **DeriveResource**<br>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**<br>+resource<br>0..*, unordered, frozen | **Owner**<br>+owner<br>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**<br>source > target | **Licensor**<br>Child | **Owner**<br>Parent | |
| **Generalization**<br>source > target | **Owner**<br>Child | **Principal**<br>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 plays in the processes of the GeoDRM system.

A group of principals is also a principal, and the group can 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**<br>source > target | **Principal**<br>+principal<br>0..*, ordered, none | **Agent**<br>+agent<br>1..*, unordered | |
| **Aggregation**<br>source > target | **Principal**<br>+member<br>0..*, unordered | **PrincipalGroup**<br>+group<br>0..*, unordered | The members of a group are also principals and can be groups in their own right.<br>A principal group is a set of principals acting together in a single role in the system. |
| **Generalization**<br>source > target | **Agent**<br>Child | **Principal**<br>Parent | |
| **Generalization**<br>source > target | **Licensee**<br>Child | **Principal**<br>Parent | |
| **Generalization**<br>source > target | **PrincipalGroup**<br>Child | **Principal**<br>Parent | |
| **Generalization**<br>source > target | **Owner**<br>Child | **Principal**<br>Parent | |
| **Generalization**<br>source > target | **ServiceProvider**<br>Child | **Principal**<br>Parent | |
| **Generalization**<br>source > target | **Principal**<br>Child | **GrantComponent**<br>Parent | |
| **Realization**<br>«realize»<br>source > target | **Principal**<br>Child | **Principal**<br>Parent | |
| **Realization**<br>«realize»<br>source > target | **principalPattern**<br>Child | **Principal**<br>Parent | |



## B.38 PrincipalGroup

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

Extends: *Principal*.

*Package:* GeoLicence

**Table B.49 — PrincipalGroup connections**

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

## B.39 Print

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

Extends: *View*.

*Package:* GeoLicence

**Table B.50 — Print connections**

| Connector | Source | Target | Notes |
|---|---|---|---|
| **Generalization**<br>source > target | **Print**<br>Child | **View**<br>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**<br>source > target | **Process**<br>Child | **Processing**<br>Parent | |

**Table B.52 — Process attributes**

| Attribute | Type | Notes |
|---|---|---|
| languages | public<br>Range:1 to *:<br>*String* | The "language" interface lists all programming languages in which the API for the Process can 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 shall have licences both for the Processing resources and for any Data resources that can be involved. Metadata about the Processing resource can 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 can be used by conditions in licence grants.

**Table B.53 — Processing connections**

| Connector | Source | Target | Notes |
|---|---|---|---|
| **Aggregation**<br>Implementation<br>source > target | **Processing**<br>+targetProcess<br>0..*, unordered | **Request**<br>+request<br>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 can 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**<br>source > target | **Execute**<br>unordered | **Processing**<br>+process<br>0..*, unordered | |
| **Generalization**<br>source > target | **Processing**<br>Child | **Resource**<br>Parent | |
| **Generalization**<br>source > target | **Service**<br>Child | **Processing**<br>Parent | |
| **Generalization**<br>source > target | **Process**<br>Child | **Processing**<br>Parent | |

**Table B.54 — Processing attributes**

| Attribute | Type | Notes |
|---|---|---|
| complianceLicence<br>«metaclass» | public<br>Range:0 to *:<br>*GeoLicence* | The "compliance licence" attribute lists proof of compliance to the various standards listed in the "standard" attribute. |
| formalName | public<br>Range:0 to *:<br>*String* | The "formal name" is a list of names used in the "standard" attribute list to identify the functionality supplied here. |
| implementor<br>«metadata» | public<br>Range:0 to *:<br>*anyURI* | The "implementor" attribute identifies the implementor of the process represented. |
| localName | public<br>Range:0 to *:<br>*String* | The "local name" attribute specifies which name or alias is actually used by this implementation. |
| provider<br>«metadata» | public<br>Range:0 to *:<br>*anyURI* | The "provider" attribute identifies the provider of the access to this functionality. |
| standard<br>«metaclass» | public<br>Range:0 to *:<br>*anyURI* | The "standard" attribute lists the various standards that this process adheres to. |
| parameter<br>«property» | public<br>Range:0 to *:<br>*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**<br>source > target | **ProcessInvocation**<br>Child | **Request**<br>Parent | |

## B.43 PropertyInterface

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

*Package:* GeoLicence

**Table B.56 — PropertyInterface connections**

| Connector | Source | Target | Notes |
|---|---|---|---|
| **Realization**<br>«realize»<br>source > target | **Property**<br>Child | **PropertyInterface**<br>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