BS ISO 19153:2014

BSI Standards Publication

Geospatial Digital Rights Management Reference Model (GeoDRM RM)

bsi.

...making excellence a habit.™

Document Sharing Hub

Full document details: BS ISO 19153:2014

National foreword

This British Standard is the UK implementation of ISO 19153:2014.

The UK participation in its preparation was entrusted to Technical Committee IST/36, Geographic information.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2014. Published by BSI Standards Limited 2014

ISBN 978 0 580 64455 9

ICS 35.240.70

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 28 February 2014.

Amendments issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO 19153:2014

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)

Documents
Document Sharing Hub

© ISO 2014

Full document details: BS ISO 19153:2014

COPYRIGHT PROTECTED DOCUMENT

© ISO 2014

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO 19153:2014

Contents

Page

Foreword ... **v**

Introduction ... **vi**

1 Scope ... **1**

2 Conformance ... **2**

3 Normative references ... **2**

4 Terms and definitions ... **3**

5 Conventions ... **9**
5.1 Abbreviated terms ... 9
5.2 UML notation ... 9

6 GeoDRM design principles ... **10**
6.1 GeoDRM roadmap ... 10
6.2 Basics ... 10
6.3 Flow model of GeoDRM ... 11
6.4 GeoDRM Gatekeeper ... 11
6.5 DRM metadata — licence model ... 15
6.6 Developmental guidelines ... 16
6.7 The components of managing risk ... 17

7 GeoDRM enterprise viewpoint and Abstract Rights Model ... **19**
7.1 General ... 19
7.2 Geospatial resource ... 19
7.3 GeoLicence extents ... 19
7.4 GeoLicence expression ... 21
7.5 GeoLicence creation and enforcement ... 21
7.6 GeoLicence delegation and management ... 21
7.7 GeoLicence chaining ... 22
7.8 GeoLicensing communities ... 23
7.9 GeoLicensing and resource lineage ... 25
7.10 Handling GeoLicence violation — and the break-the-glass principle ... 25
7.11 Automated licence revocation/expiration — need to revoke privilege ... 26

8 GeoDRM computational viewpoint ... **26**
8.1 Overview — roles and responsibilities ... 26
8.2 Principals ... 29
8.3 Resource owner ... 30
8.4 Agent ... 30
8.5 Licence broker or licensing agent ... 30
8.6 Service broker ... 31
8.7 Service provider ... 31
8.8 End-user ... 31
8.9 Licence manager ... 31

9 Information viewpoint ... **31**
9.1 Overview ... 31
9.2 User metadata ... 33
9.3 Properties and patterns ... 33
9.4 Resource metadata ... 33
9.5 Licence metadata ... 34
9.6 Process metadata ... 44

Annex A (normative) **Abstract test suite** ... **45**

Annex B (informative) **GeoDRM UML model** ... **47**

Annex C (informative) **Scenarios** ... **82**

AVA Documents
Document Sharing Hub

© ISO 2014 – All rights reserved

Full document details: BS ISO 19153:2014

Annex D (informative) **Editor's notes** **88**
Bibliography **89**

© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 19153:2014

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).

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 19153:2014

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.

© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 19153:2014

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.

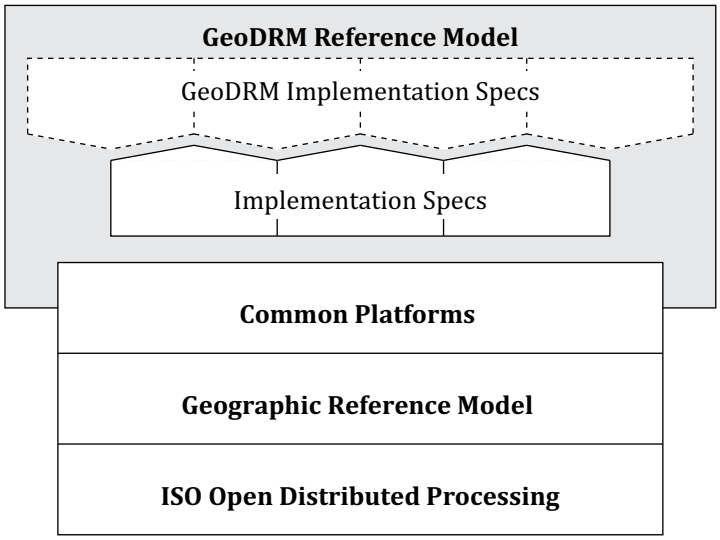

Figure 1 — GeoDRM reference model context

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

© ISO 2014 – All rights reserved

AVA Documents Document Sharing Hub

Full document details: BS ISO 19153:2014

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.

© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 19153:2014

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.

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 19153:2014

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.

© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 19153:2014

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).

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 19153:2014

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”]

© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 19153:2014

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).

© ISO 2014 – All rights reserved

AVA Documents
Document Sharing Hub
Full document details: BS ISO 19153:2014

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)

© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 19153:2014

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.

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 19153:2014

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

© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 19153:2014

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.

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 19153:2014

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.

© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 19153:2014

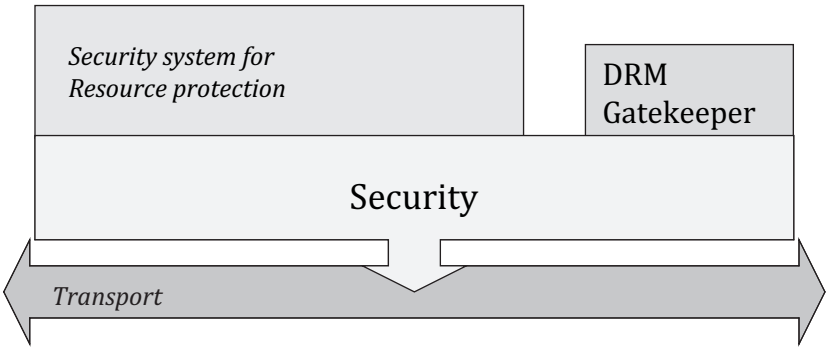

Figure 2 — Gatekeeper metaphor for GeoDRM

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

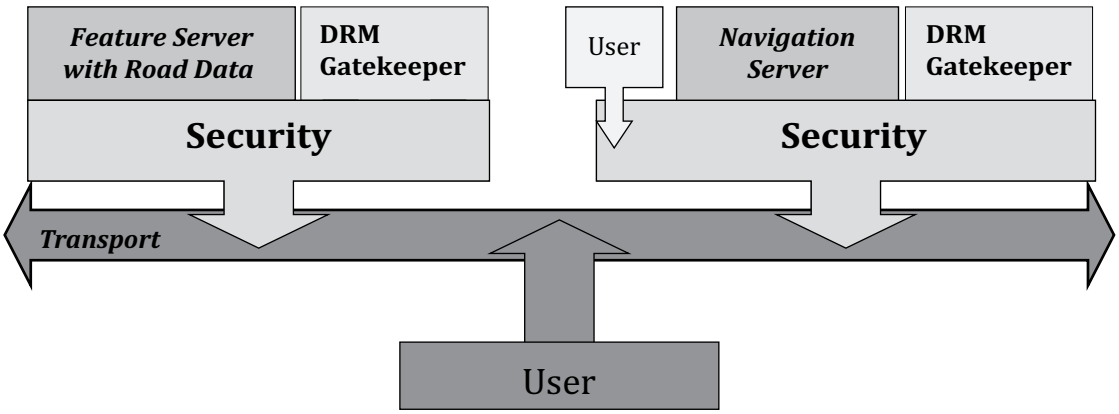

Figure 3 — Topology for complex gatekeeper example

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.

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 19153:2014

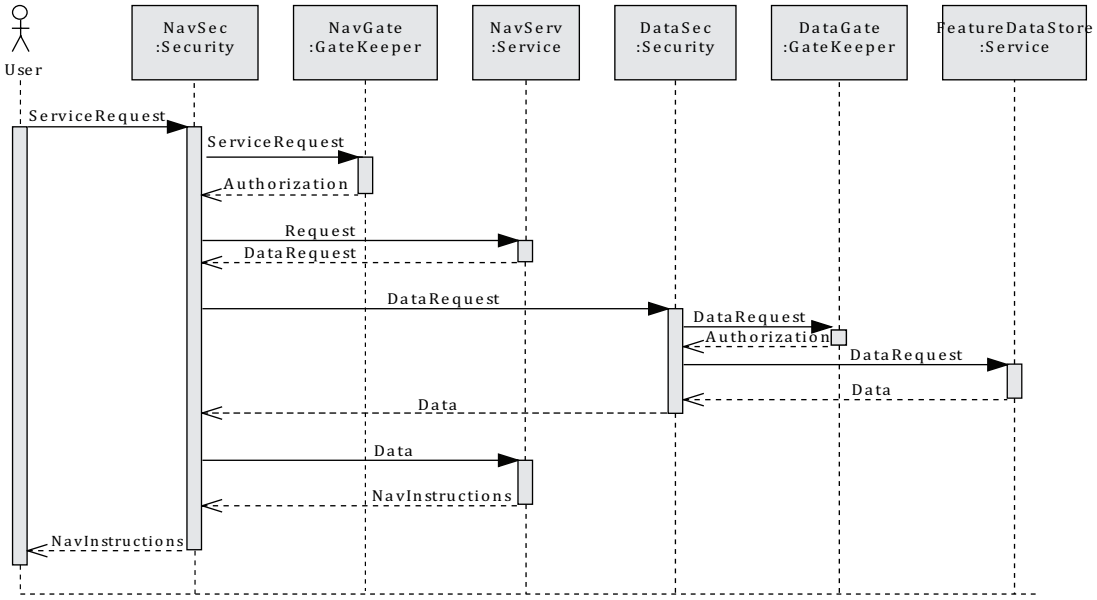

Figure 4 — Sequence diagram for a two-stage geoServer interaction

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.

© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 19153:2014

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.

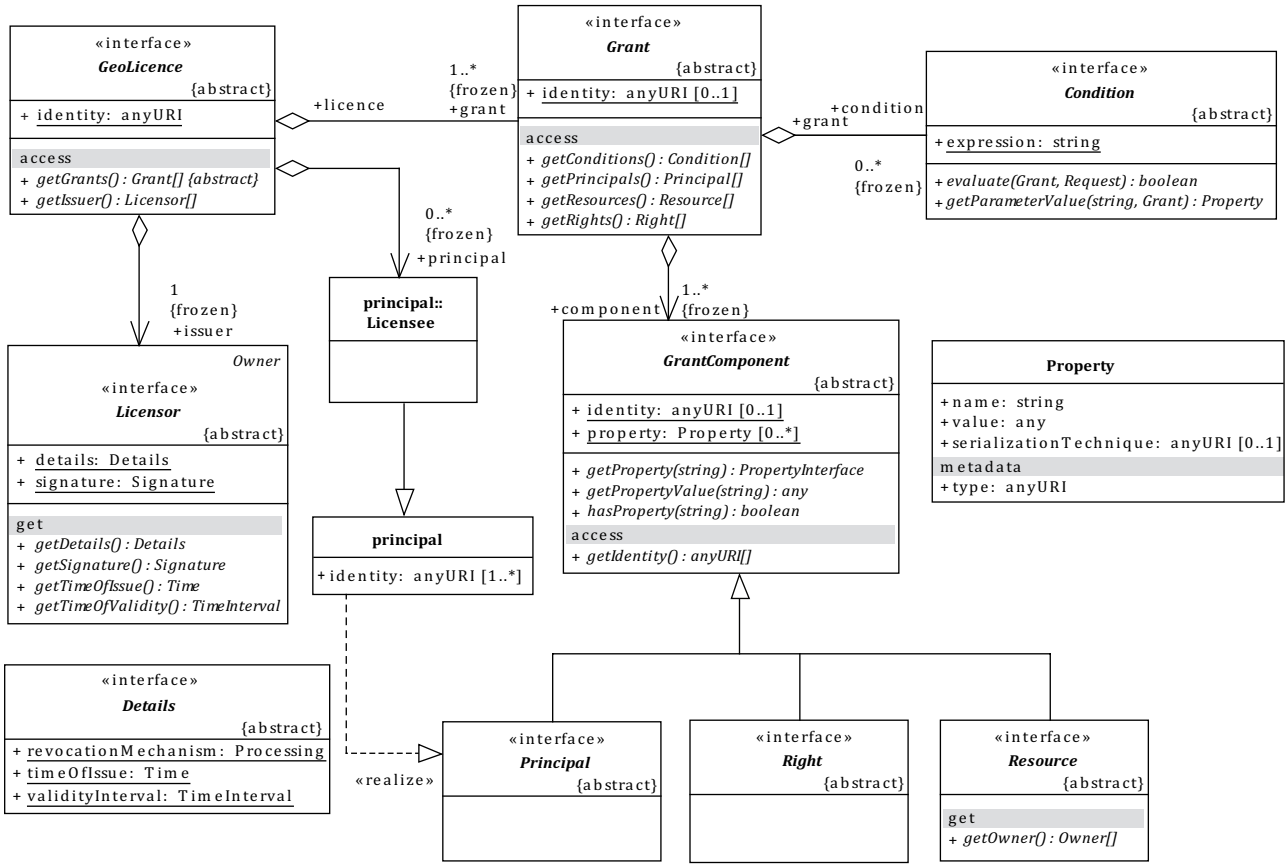

Figure 5 — General licence model (UML)

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.

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 19153:2014

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.

© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 19153:2014

— 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.

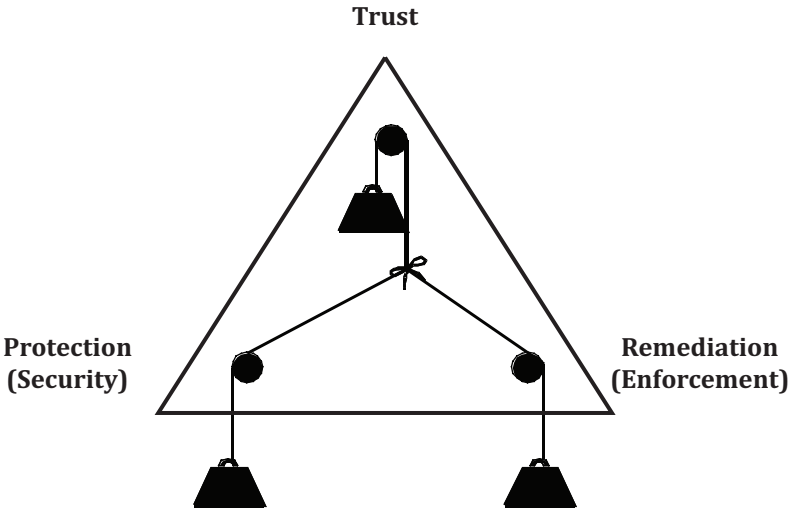

Figure 6 — Balancing trust with protection and remediation

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.

© ISO 2014 – All rights reserved

AVA Documents
Document Sharing Hub
Full document details: BS ISO 19153:2014

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.

© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 19153:2014

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);

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 19153:2014

— 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.

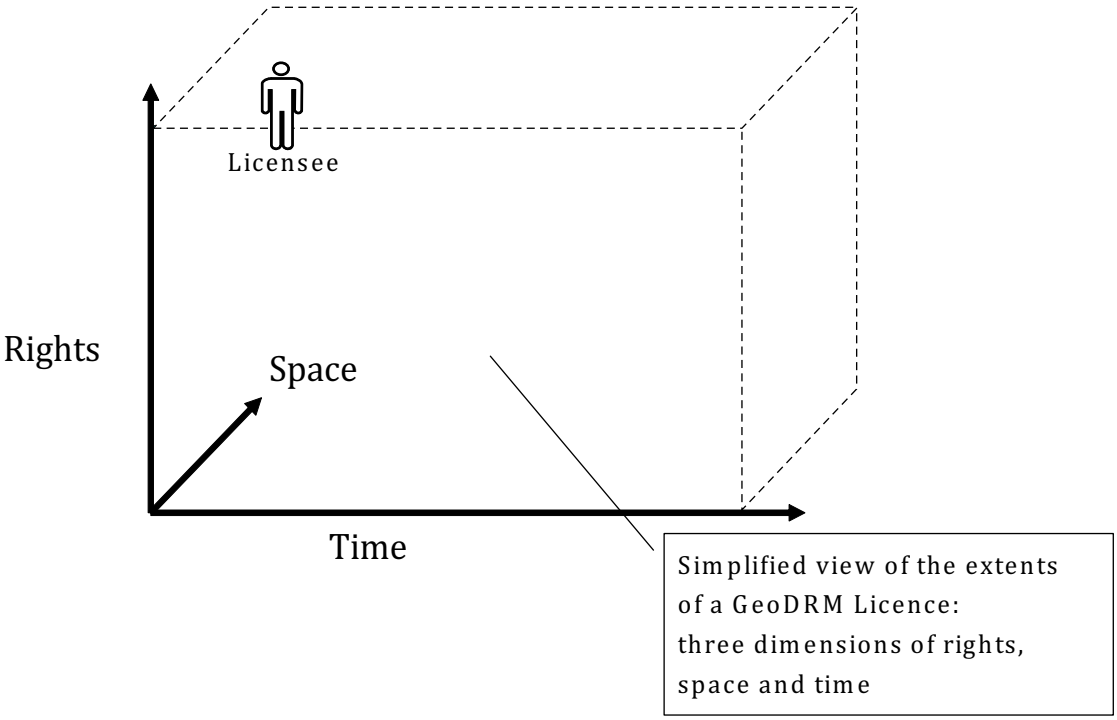

Figure 7 — GeoLicence extents

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.

© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 19153:2014

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.

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 19153:2014

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.

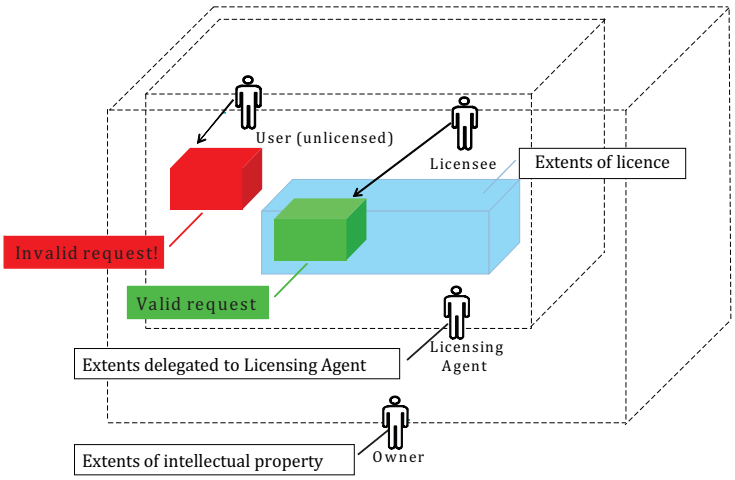

Figure 8 — GeoLicence delegation and management

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.

© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 19153:2014

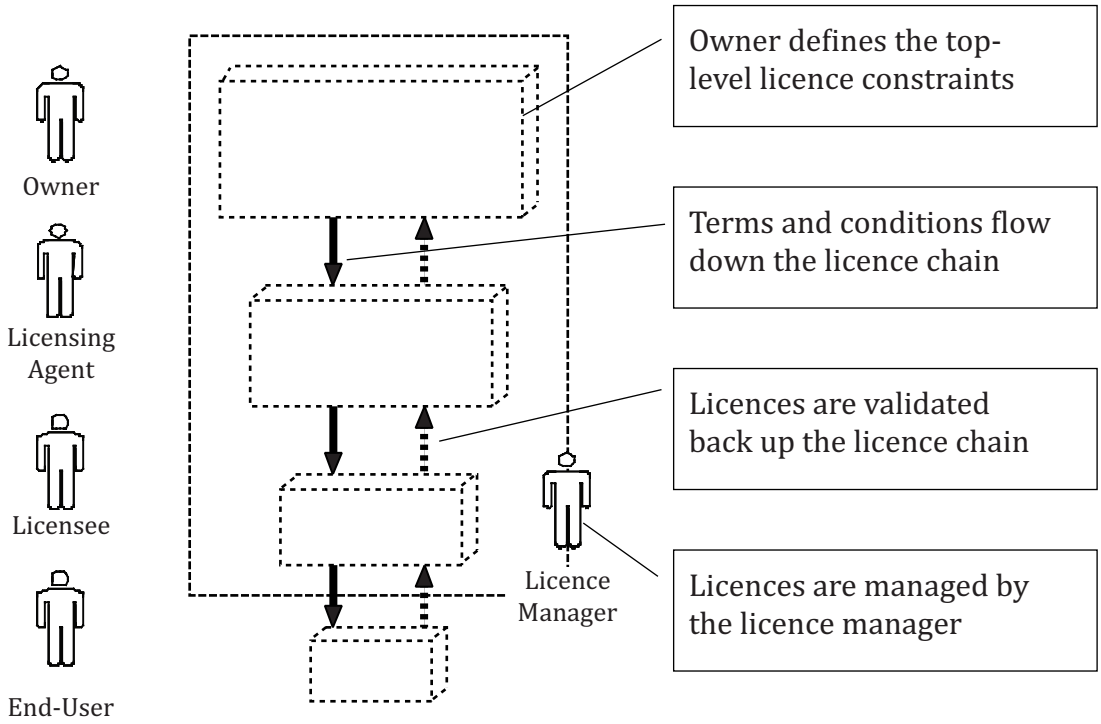

Figure 9 — GeoLicence chaining (supporting distributed licensing)

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.

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 19153:2014