Alban Gabillon

Patrick Capolsini

November 2008

DRM policies for Web Map Service

Alban Gabillon, Patrick Capolsini

University of French Polynesia - Tahiti

Université de la Polynésie Française (UPF)
BP 6570 Faa'a aéroport
TAHITI – Polynésie Français

The authors

Alban Gabillon
Professor

Patrick Capolsini
Assistant Professor

Presentation overview

I. **Introduction**
II. Geospatial data & Web Map Service (WMS)
III. Open Digital Rights Language (ODRL)
IV. WMS Security
V. DRM Architecture
VI. Conclusion & Perspectives

Introduction

- Open Geospatial Consortium (OGC) : an international industry consortium
- The OGC GeoRM (Geo Rights Management) Working Group deals with the protection/licensing of geographic data/services
- The GeoRM WG has issued the DRM Reference Model (RM) which highlights the fact that existing REL (Rights Expression Languages) cannot be used for licensing of geographic information unless they are extended.

Introduction

- The RM states that the rights model must accommodate licensing for geographic data which are dynamically created by using OpenGIS web services (e.g. WMS)
- Our aim = extend ODRL to accommodate licensing for geographic data created by OpenGIS Web Map Services (WMS)

➔ **Definition of an ODRL WMS Profile**

Presentation overview : where are we ?

I. Introduction

II. **Geospatial data & Web Map Service (WMS)**

III. Open Digital Rights Language (ODRL)

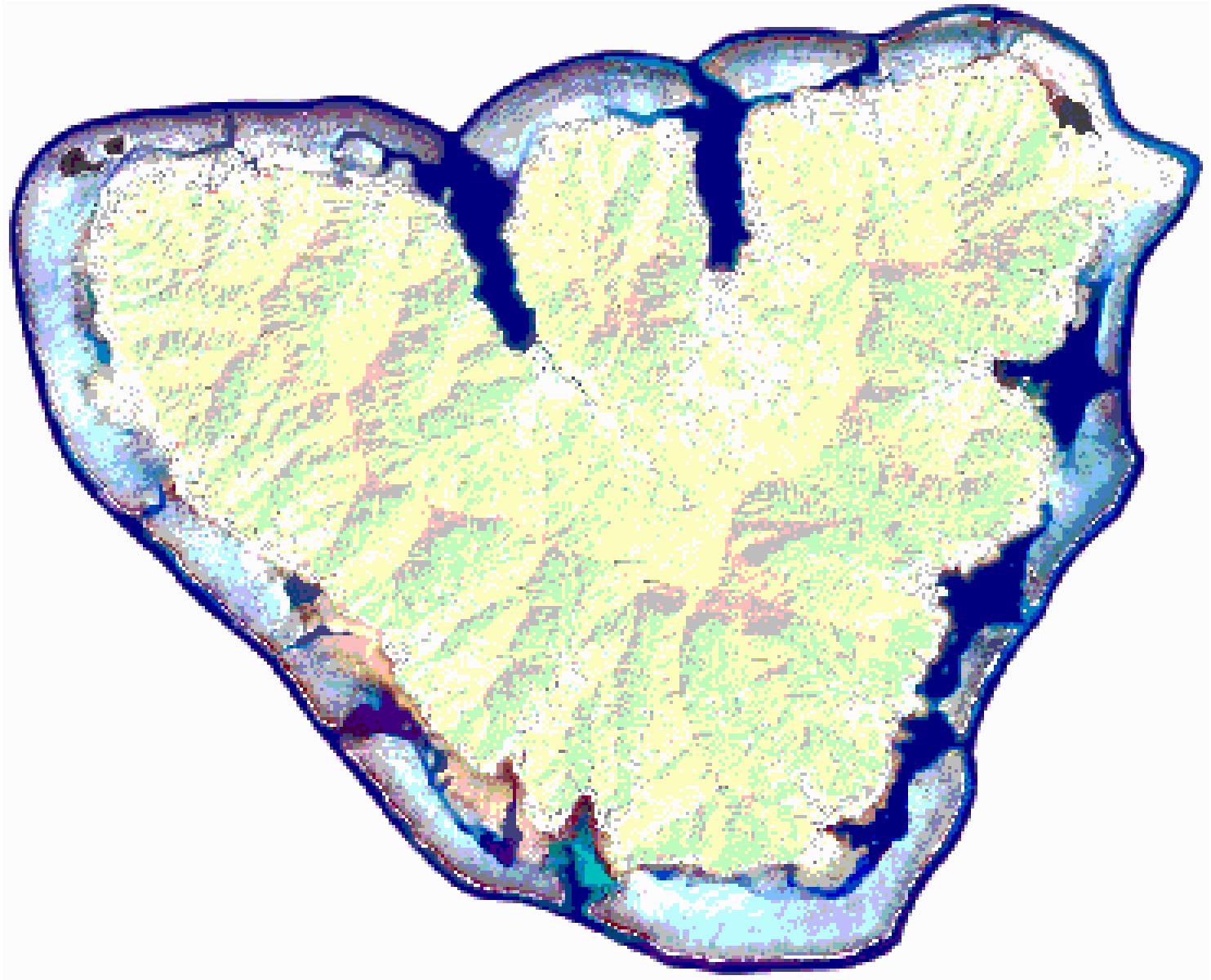
IV. WMS Security

V. DRM Architecture

VI. Conclusion & Perspectives

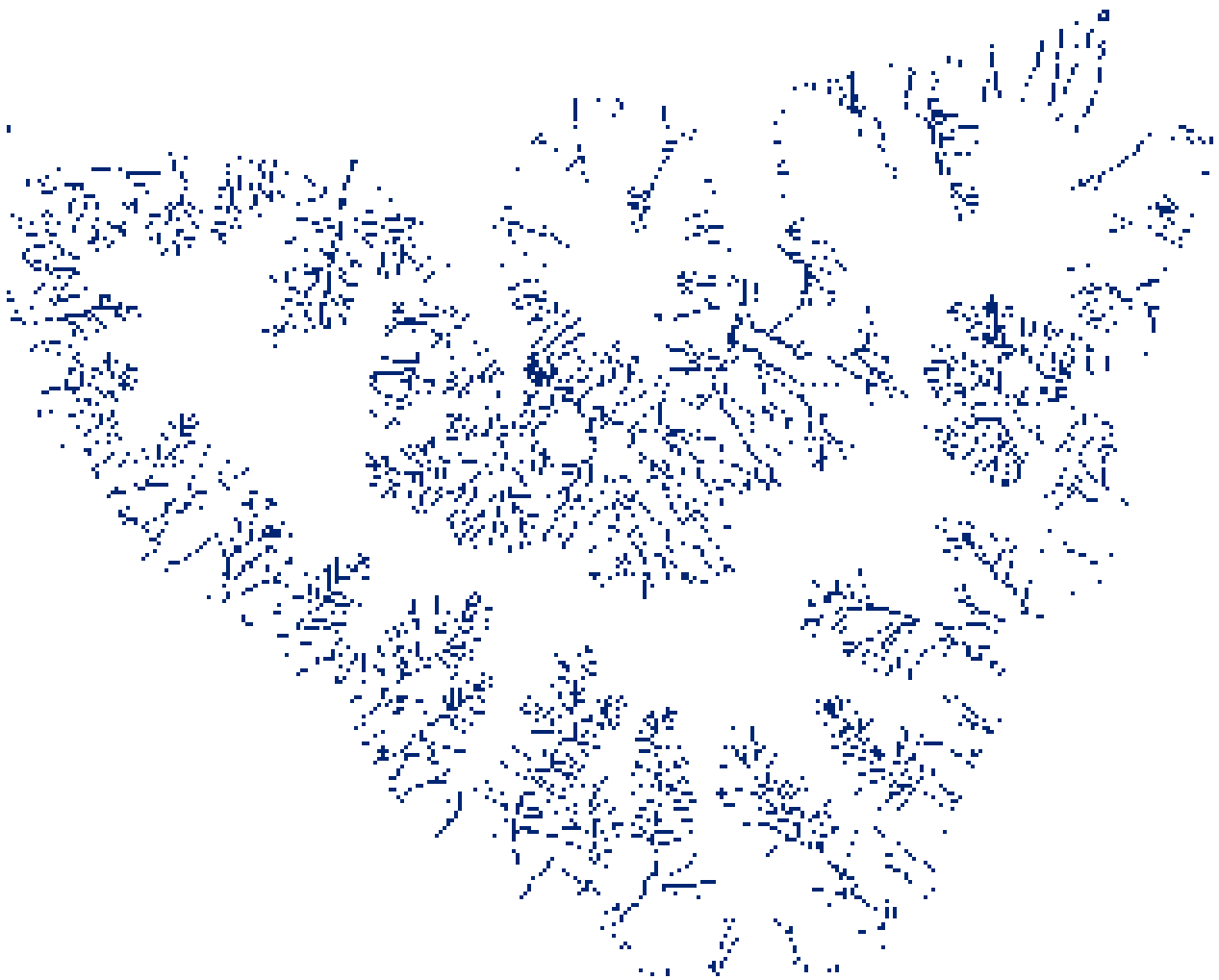
Geospatial Data & WMS

- Geographic Information Systems (GIS) are widely used
- Geodata = geo-referenced data handled as layers
- Two types of Geodata layers
  - Raster layers (images)
  - Vector layers (points, lines, polygons, …)
- Geodata (layers) storage : files or records in a spatially enabled databases
- Layers are overlaid ➔ final visualization of the dataset

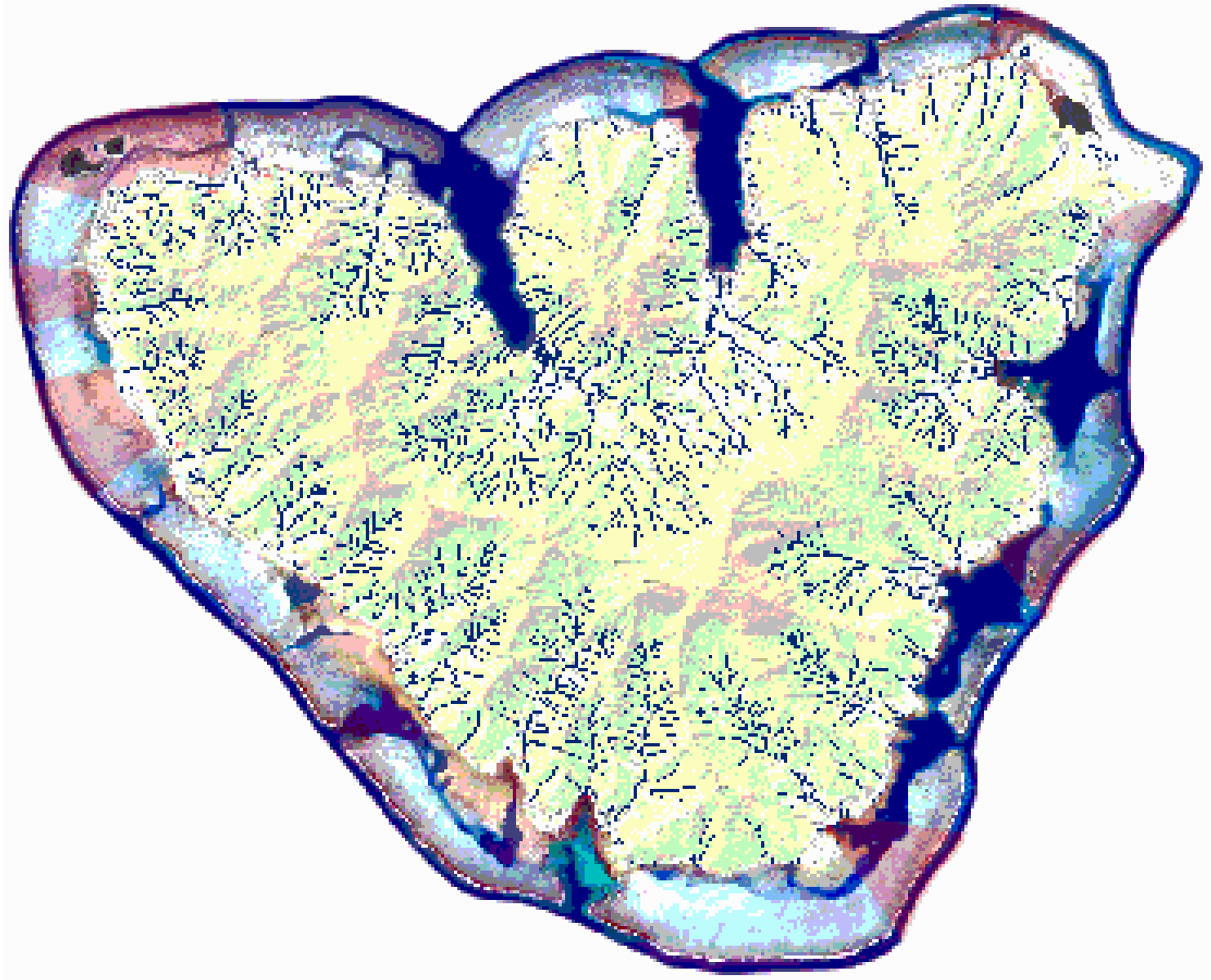


Raster layer : topographic map + aerial photography of Moorea island

Vector layer (polygons) : Protected Marine Areas of Moorea island



Vector layer (poly-lines) : hydrology of Moorea island



Final dataset : layers overlaid

Geospatial Data & WMS

Two main OGC openGIS® specifications :

- Web Feature Service (WFS) allows online retrieval/update of Geodata using GML (Geographic Markup Language)
- Web Map Service (WMS) allows retrieval of Geodata in a *pictoral format (gif, jpeg or png)*

Geospatial Data & WMS

- Three WMS requests :
  - **GetCapabilities** returns service-level metadata,
  - **GetMap** returns a map according to well-defined geographic and dimensional parameters
  - **GetFeatureInfo** (optional for a basic WMS server) returns information about particular features shown on a map

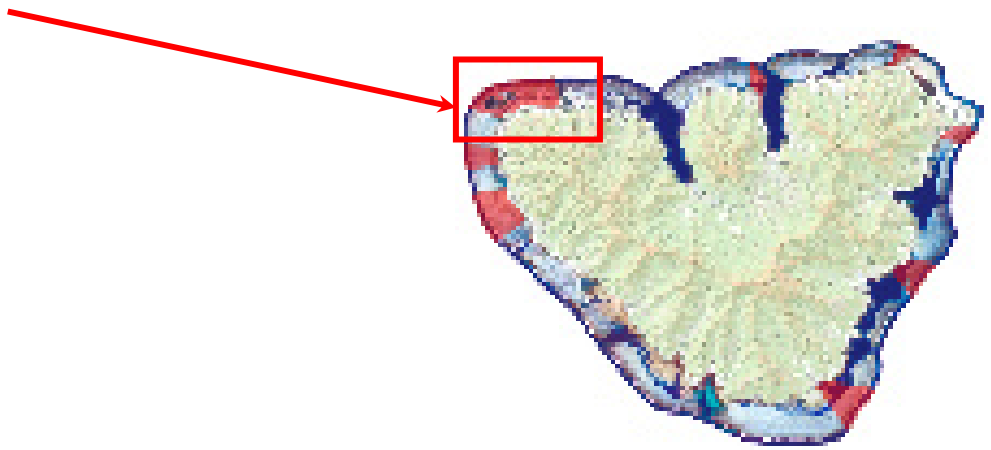
Geospatial Data & WMS

- Each layer has a size (a geographic extent)
- Size of final map = size of largest layer
- A WMS *GetMap* query specifies :
  - a set of layers
  - a bounding box

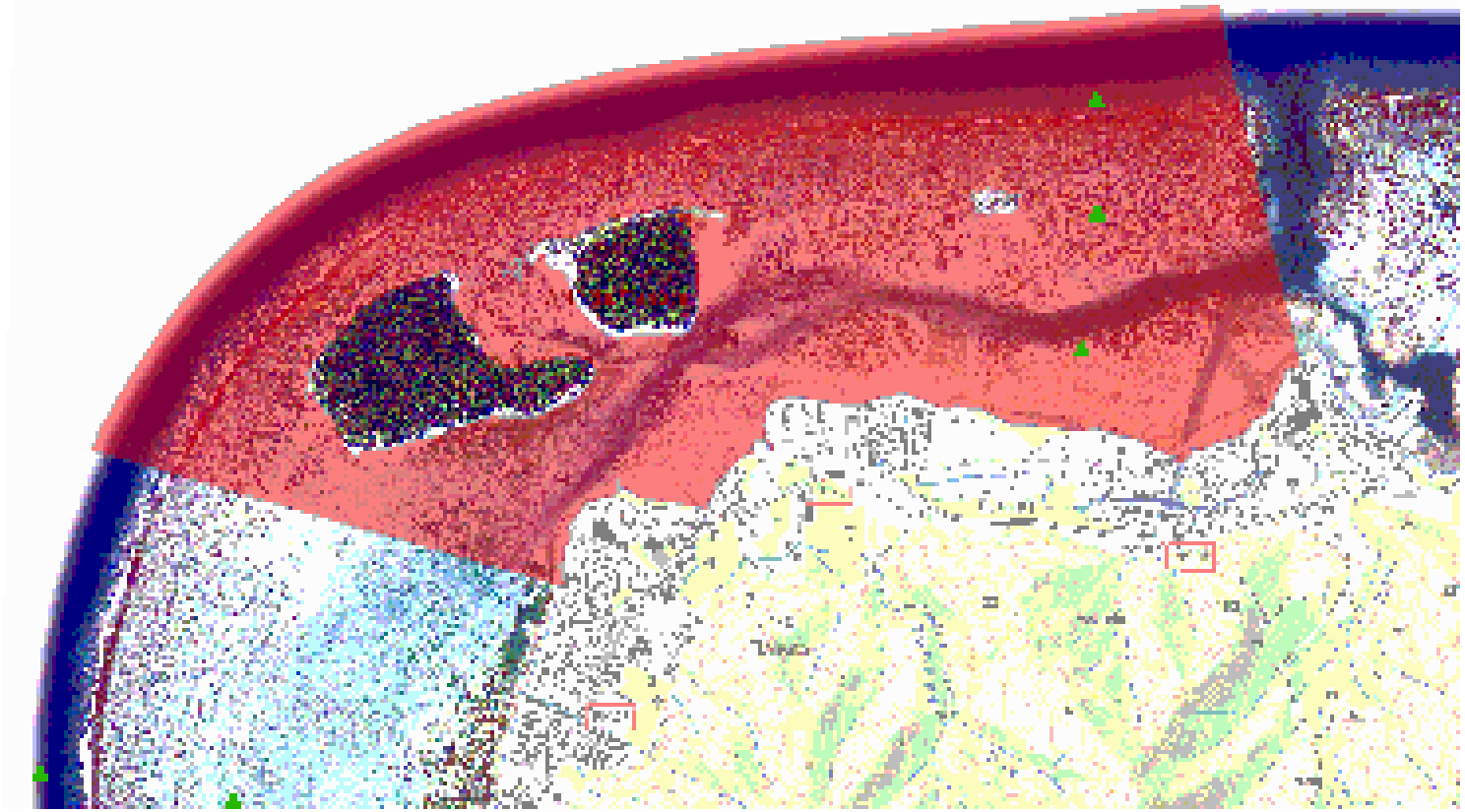
➔A bounding box smaller than the map size leads to a zoom-in operation

Geospatial data and WMS : an example

http://webgis.upf.pf/cgi-bin/mapserv?
map=/home/webgis/cartoweb3/projects/Moorea/server_conf/Moorea/Moorea_limited.map&
SERVICE=WMS&
VERSION=1.1.1&
REQUEST=GetMap&
LAYERS=composite,amp,criobe&
SRS=epsg:4326&
BBOX=-149.928742,-17.500643,-149.890238,-17.471618



Geospatial Data & WMS : GetMap query result



Presentation overview : where are we ?

I. Introduction
II. Geospatial data & Web Map Service (WMS)
III. **Open Digital Rights Language (ODRL)**
IV. WMS Security
V. DRM Architecture
VI. Conclusion & Perspectives

ODRL : Definition

- The Open Digital Rights Language (ODRL) v1.1 is an open, XML-based, extensible language for specifying usage control policies
- ODRL utilizes two XML schemas
  - First schema : Expression Language elements + relationships between these elements
  - Second schema : Data Dictionary elements used to instantiate the Expression Language elements when writing a rights policy. This schema may be user-extended.

ODRL : Basic expression language elements

- ODRL can express offers and agreements involving the three following basic Expression Language elements :
  - **Asset** : used to declare objects to which the rights policy applies
  - **Permission** : used to define the rights policy. Permissions are rules regulating access and use of assets
  - **Party** : used to declare subjects involved in the offer and/or agreement

ODRL: Example

```
<o-ex:rights
        xmlns:o-ex="http://odrl.net/1.1/ODRL-EX"
        xmlns:o-dd="http://odrl.net/1.1/ODRL-DD">
    <o-ex:agreement>
        <o-ex:asset>                                    asset
            <o-ex:context>
                <o-dd:uid>dvd:Winnie the Pooh</o-dd:uid>
            </o-ex:context>
        </o-ex:asset>
        <o-ex:permission>
            <o-dd:play />                               permission
        </o-ex:permission>
        <o-ex:party>                                    party
            <o-ex:context>
                <o-dd:uid>Cyrus</o-dd:uid>
            </o-ex:context>
        </o-ex:party>
    </o-ex:agreement>
</o-ex:rights>
```

ODRL : Custom Dictionary

```
<xsd:schema
        targetNamespace=http://www.upf.pf/~gabillon/dvd-DD
        xmlns:xsd="http://www.w3.org/2001/XMLSchema"
        xmlns:o-ex=" http://odrl.net/1.1/ODRL-EX"
        xmlns:dvd="http://www.upf.pf/~gabillon/dvd-DD"
        elementFormDefault="qualified" attributeFormDefault="qualified">
<xsd:import
        namespace="http://odrl.net/1.1/ODRL-EX"
        schemaLocation="http://odrl.net/1.1.ODRL-EX-11.xsd"/>
<xsd:element                                                    element
        name="audio-track"
        type="o-ex:constraintType"
        substitutionGroup="o-ex:constraintElement"/>
</xsd:schema>
```

ODRL: Extended policy

```
<o-ex:rights
        xmlns:o-ex="http://odrl.net/1.1/ODRL-EX"
        xmlns:o-dd="http://odrl.net/1.1/ODRL-DD"
        xmlns:dvd="http://www.upf.pf/~gabillon/dvd-DD">
    ...
<o-dd:play>
    <o-ex:constraint>
        <dvd:audio-track>
            <o-ex:context>
                <o-dd:uid>English</o-dd:uid>
            </o-ex:context>
        </dvd:audio-track>
    </o-ex:constraint>
</o-dd:play>
...
</o-ex:rights>
```

new constraint

Presentation overview : where are we ?

I. Introduction
II. Geospatial data & Web Map Service (WMS)
III. Open Digital Rights Language (ODRL)
IV. **WMS Security**
V. DRM Architecture
VI. Conclusion & Perspectives

WMS Security

"the online browsing of map information available from a Web Map Service creates an infinite number of different contents" [1]

➔ Dealing with access and use of WMS-created data poses the problem of identifying the asset.

[1] A. Matheus, *Authorization for digital rights Management in the geospatial domain*, in 5th ACM workshop on Digital rights management, Alexandria, VA, USA, pp. 55-64, 2005

WMS Security

- Two solutions :
  - Use of core ODRL by identifying each content with its corresponding WMS query (an URL)
    - ➔ unrealistic to enumerate in a license each and every permitted WMS query

OR

  - Extend ODRL to identify as an asset **a set** of contents

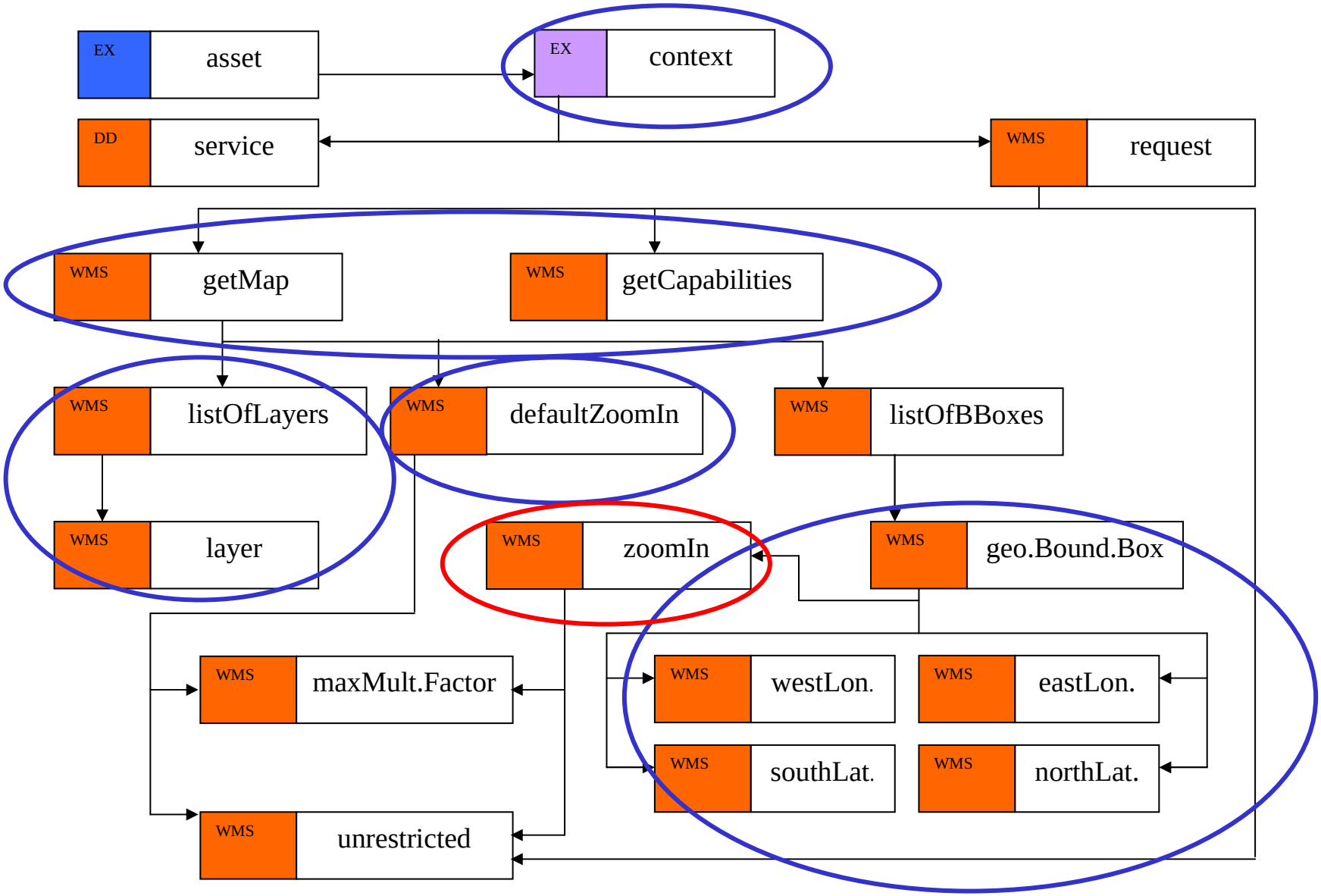
WMS Security : WMS profile

- Extend ODRL with one *context element*
  - ➔identify a **set of contents** created by a **range of WMS queries**
- This *context element* is of complex type
  - ➔allows us to specify **ranges of values** for the main WMS parameters

WMS Security : WMS profile

- Express rights policies regulating **access** and **zoom-in** operations to the main parameters of a WMS GetMap request : coordinates and layers
- **Not** a formal model for geographic data, since formal models exist, see for example [1] or [2] :
  - V. Atluri, and S. A. Chun, *A geotemporal role-based authorisation system*, *International Journal of Information and Computer Security*, vol. 1, no. 1/2, pp. 143-168, January, 2007.
  - Damiani, M.L., et al., *GEO-RBAC : A spatially Aware RBAC*. ACM Transactions on Information Systems and Security, 2006. 00(00): p. 1-34.
- Only extend ODRL in order to write rights policies protecting contents created by WMS

ODRL WMS Context Model



Security policy

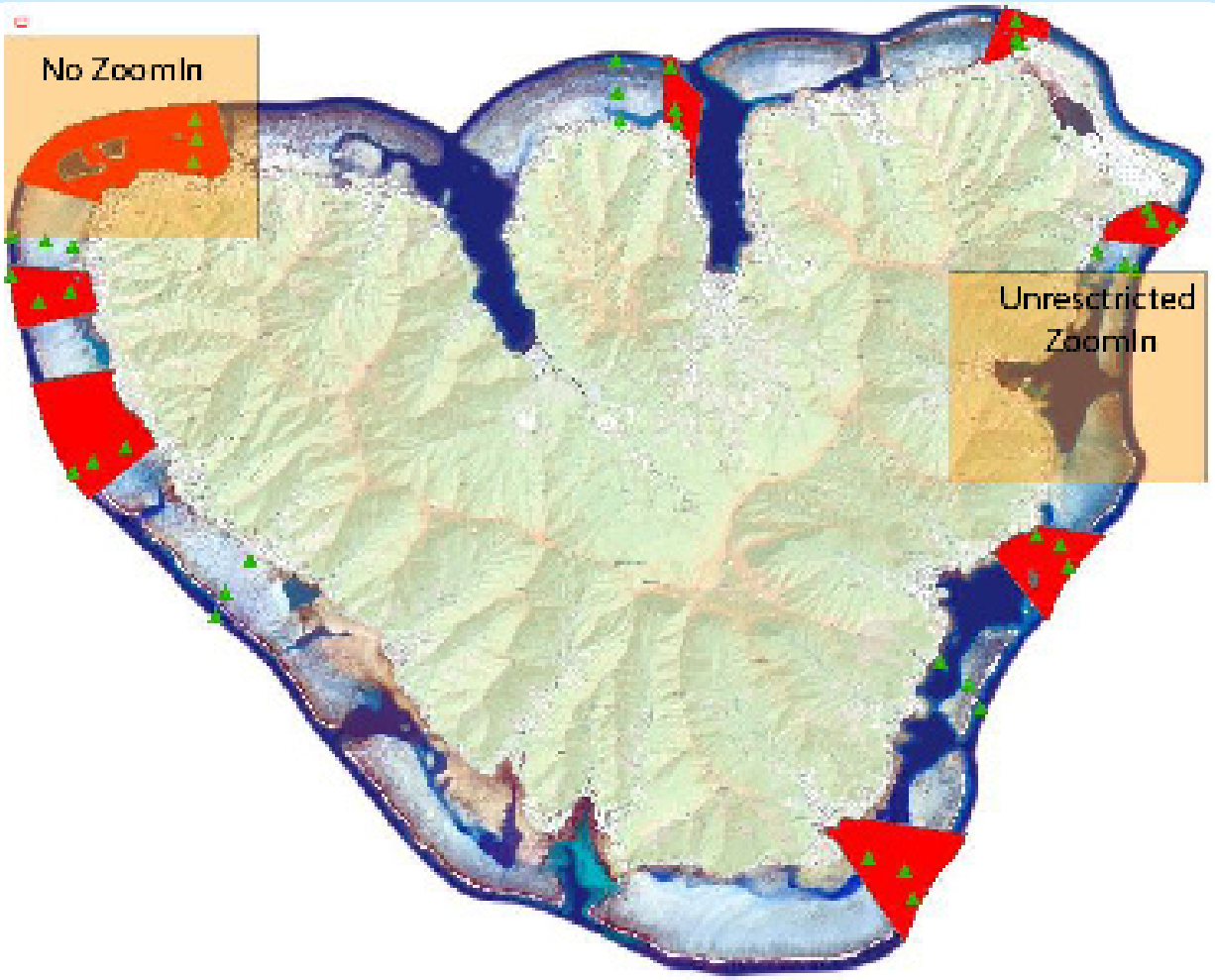
Two points to define :

- The permitted queries
  - Our policy defines **a range** of permitted queries
  - Result of one of these permitted queries must belong to the asset
- The usage policy

➔A license then contains **both** the :

- Permitted queries (access control) **and**
- Usage policy (usage control)

Moorea island example



Three layers: background raster image + Marine Protected Areas (amp) + Criobe (sampling zones)

Moorea island : Security Policy (rule 1)

Definition of rule 1 :

- Permitted queries : any *GetMap* query whose layers parameter is equal to any subset of {composite,amp}. Zoom-in should be everywhere unrestricted
- Usage of permitted contents : display and print

Security Policy : rule 1

```
<o-ex:offer>
    <o-ex:asset o-ex:id="ASSET1">
        <o-ex:context>
            <o-dd:uid>WMS_ASSET1</o-dd:uid>
            <wms:request>
                <wms:getMap>
                    <wms:listOfLayers wms:setFunction="subsetOf">
                        <wms:layer>composite</wms:layer>
                        <wms:layer>amp</wms:layer
                    </wms:listOfLayers>
                    <wms:defaultZoomIn>
                        <wms:unrestricted/>
                    </wms:defaultZoomIn>
                </wms:getMap>
            </wms:request>
            <o-dd:service>
http://webgis.upf.pf/cgi-bin/mapserv?map=/home/webgis/cartoweb3/projects/Moorea/server_conf/Moorea/Moorea_limited.map
            </o-dd:service>
...
```

Security policy : rule 1 usage

```
</o-ex:permission>
    <o-ex:asset o-ex:idref="ASSET1"/>
    <o-ex:asset o-ex:idref="ASSET3"/>
    <o-dd:display />
    <o-dd:print />
</o-ex:permission>
<o-ex:permission>
    <o-ex:asset o-ex:idref="ASSET2"/>
    <o-dd:display />
    <o-dd:print>
        <o-ex:constraint>
            <o-dd:count>10</o-dd:count>
        </o-ex:constraint>
    </o-dd:print>
</o-ex:permission>
...
```

Moorea island : Security Policy (rule 2)

Definition of rule 2 :

- Permitted queries : any *GetMap* query whose layers parameter includes the layer *criobe*
  - For such queries, the default MZF should be equal to 5
  - There is one area more sensitive than the others, with a specific MZF equal to 1 (i.e. zoom-in is forbidden)
  - There is one area with an unrestricted MZF
- Usage of permitted contents :
  - display
  - print no more then 10 times

Security Policy : rule 2 (1/2)

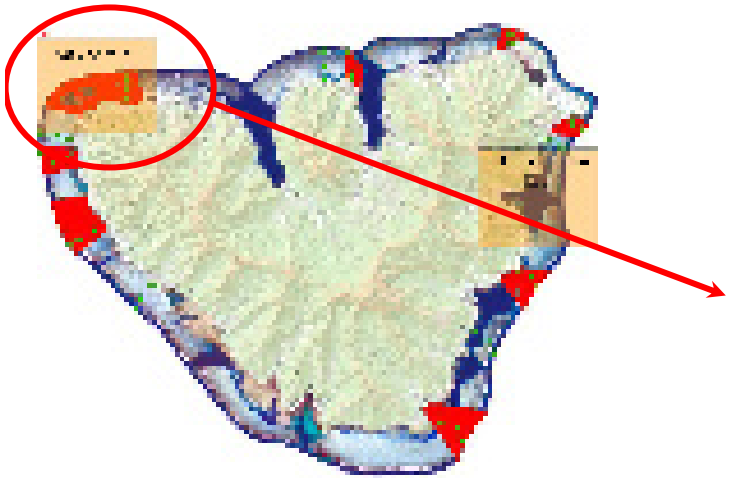
```
<o-ex:asset o-ex:id="ASSET2">
    <o-ex:context>
        <o-dd:uid>WMS_ASSET2</o-dd:uid>
          <wms:request>
            <wms:getMap>
```

Layer criobe

```
<wms:listOfLayers wms:setFunction="include">
        <wms:layer>criobe</wms:layer>
</wms:listOfLayers>
```

Default zoom-in

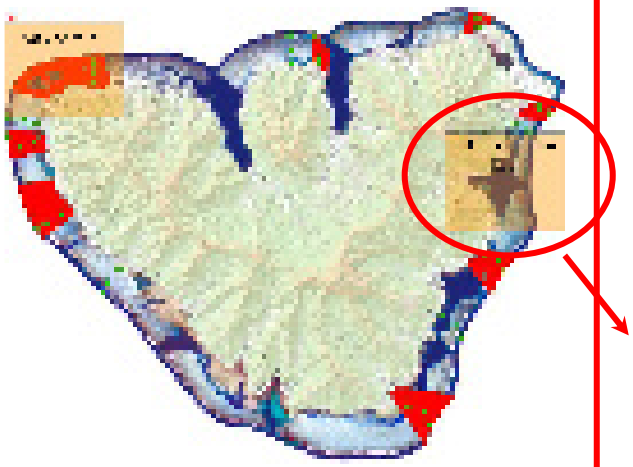
```
<wms:defaultZoomIn>
  <wms:maxMultiplicativeFactor>5</wms:maxMultiplicativeFactor>
</wms:defaultZoomIn>
```



```
<wms:listOfBBoxes>
  <wms:geographicBoundingBox>
    <wms:westLongitude>-149.928742</wms:westLongitude>
    <wms:southLatitude>-17.500643</wms:southLatitude>
    <wms:eastLongitude>-149.890238</wms:eastLongitude>
    <wms:northLatitude>-17.471618</wms:northLatitude>
    <wms:zoomIn>
        <wms:maxMultiplicativeFactor> 1
        </wms:maxMultiplicativeFactor>
    </wms:zoomIn>
  </wms:geographicBoundingBox>
```

….

Security Policy : rule 2 (2/2)



```
<wms:geographicBoundingBox >
        <wms:westLongitude> -149.788651 </wms:westLongitude>
        <wms:southLatitude> -17.537058 </wms:southLatitude >
        <wms:eastLongitude> -149.749546 </wms:eastLongitude>
        <wms:northLatitude> -17.507470 </wms:northLatitude>
                <wms:zoomIn>
                        <wms:unrestricted/>
                </wms:zoomIn>
</wms:geographicBoundingBox>
        </wms:listOfBBoxes>
    </wms:getMap>
</wms:request>
<o-dd:service>
http://webgis.upf.pf/cgi-bin/mapserv?map=/home/webgis/cartoweb3/projects/Moorea/server_conf/Moorea/Moorea_limited.map
</o-dd:service>
</o-ex:context>
</o-ex:asset>
```

Security policy : rule 2 usage

```
</o-ex:permission>
    <o-ex:asset o-ex:idref="ASSET1"/>
    <o-ex:asset o-ex:idref="ASSET3"/>
    <o-dd:display />
    <o-dd:print />
</o-ex:permission>
<o-ex:permission>
    <o-ex:asset o-ex:idref="ASSET2"/>
    <o-dd:display />
    <o-dd:print>
        <o-ex:constraint>
            <o-dd:count>10</o-dd:count>
        </o-ex:constraint>
    </o-dd:print>
</o-ex:permission>
...
```

ODRL WMS profile : online resources

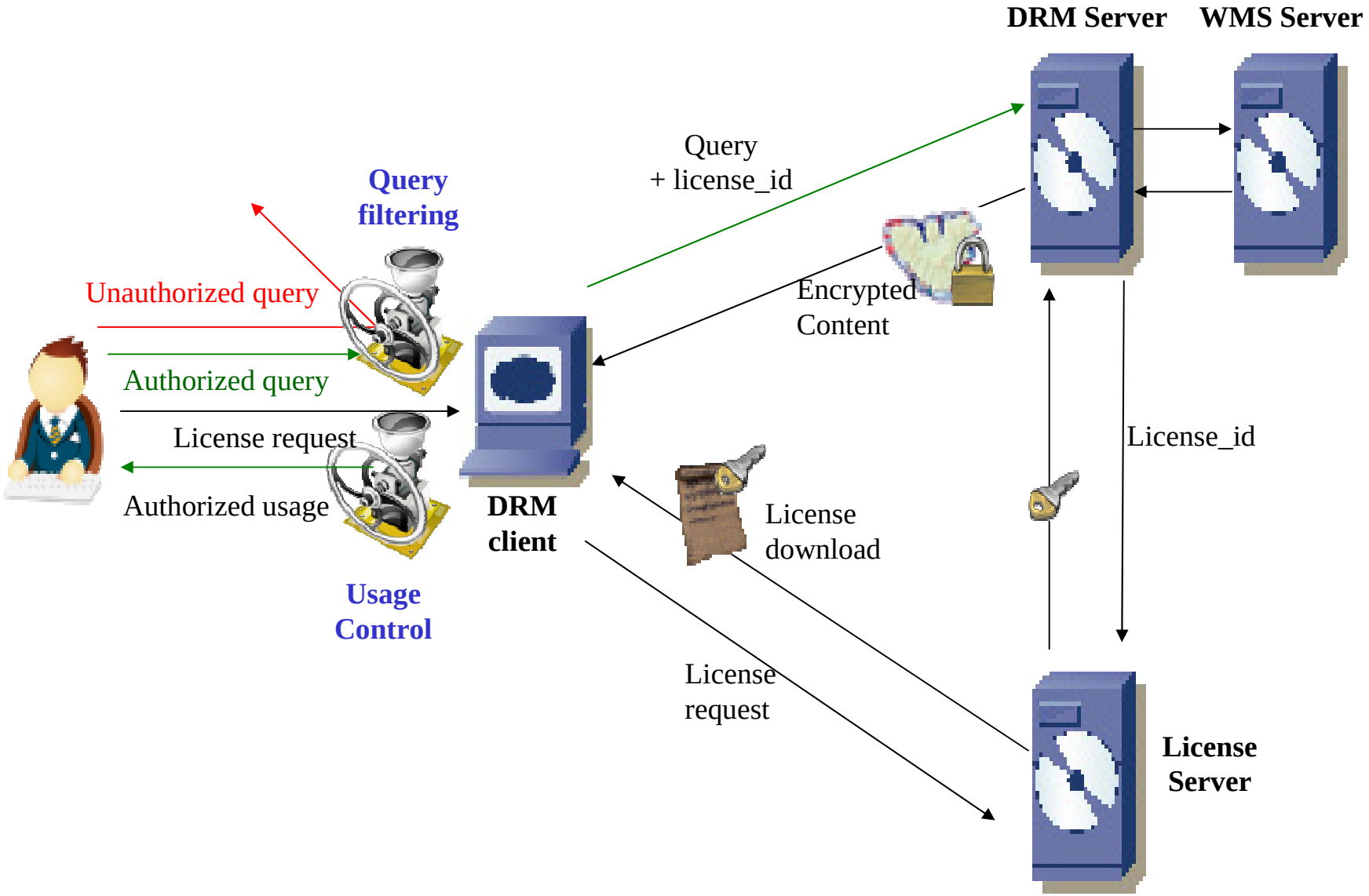
- WMS Profile: see http://pages.upf.pf/Alban.Gabillon/odrl/wms.xsd
- Security Policy: see http://pages.upf.pf/Alban.Gabillon/odrl/policy.xml
- WMS requests examples : see

http://pages.upf.pf/Patrick.Capolsini/rech/WMS_maps.htm

Presentation overview : where are we ?

I. Introduction
II. Geospatial data & Web Map Service (WMS)
III. Open Digital Rights Language (ODRL)
IV. WMS Security
V. **DRM Architecture**
VI. Conclusion & Perspectives

DRM Architecture



Presentation overview : where are we ?

I. Introduction
II. Geospatial data & Web Map Service (WMS)
III. Open Digital Rights Language (ODRL)
IV. WMS Security
V. DRM Architecture
VI. **Conclusion & Perspectives**

Conclusion

- The paper builds foundations for an ODRL WMS-profile
- Other RELs or Access Control languages (geoXACML for example) may be used to achieve paper's ideas

Perspectives

- Write new ORDL profiles for WMS **contents**
  - Raster images : rotation, reduction, edition, …
  - SVG images : permissions on individual vector belonging to the SVG image
  - XML (*GetCapabilities*) : permissions for filtering out some XML nodes
- Extend to WFS & GML
- Build a prototype of a WMS/WFS DRM-enabled platform

Alban Gabillon

Patrick Capolsini

November 2008

Achieving the security of geodata is becoming a critical issue

This work was conducted as part of the ANR funded project under reference ANR-SESUR-2007-FLUOR

Thank you for your attention

Université de la Polynésie Française (UPF)
BP 6570 Faa'a aéroport
TAHITI – Polynésie Français

Moorea island : Security Policy (rule 3)

Definition of rule 3 :

- Permitted queries : any *GetCapabilities* query
- Usage of permitted contents : display and print

Security Policy : rule 3

```
<o-ex:asset o-ex:id="ASSET3">
    <o-ex:context>
            <o-dd:uid>WMS_ASSET3</o-dd:uid>
            <wms:request>
                <wms:getCapabilities/>
            </wms:request>
        <o-dd:service>
    http://webgis.upf.pf/cgi-bin/mapserv?map=/home/webgis/cartoweb3/projects/Moorea/server_conf/Moorea/Moorea_limited.map
        </o-dd:service>
    </o-ex:context>
</o-ex:asset>
```

Security policy : rule 3 usage

```
</o-ex:permission>
    <o-ex:asset o-ex:idref="ASSET1"/>
    <o-ex:asset o-ex:idref="ASSET3"/>
    <o-dd:display />
    <o-dd:print />
</o-ex:permission>
<o-ex:permission>
    <o-ex:asset o-ex:idref="ASSET2"/>
    <o-dd:display />
    <o-dd:print>
        <o-ex:constraint>
            <o-dd:count>10</o-dd:count>
        </o-ex:constraint>
    </o-dd:print>
</o-ex:permission>
...
```

Difference between ODRL and XACML

ODRL

- Usage control
- More on the client side

XACML

- Access control
- Rather on the server side
- Becomes more and more general

➔ is there still a big difference with Usage control RELs ?