



# GeoShield



a server side  
user permissions management  
to OGC services

# Presentation outline

 **Introduction**

 **services architecture**



 **GeoShield**

 **WMS example**

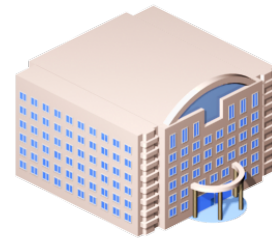
 **Demonstration**

 **Future Work**

 **Conclusione**

# Introduction

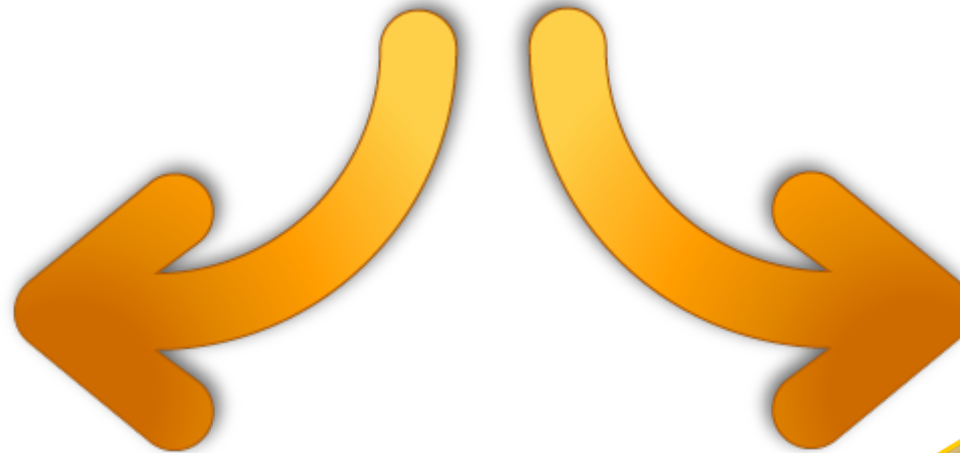
The Institute of Earth Sciences



Public data



Open Architecture



Protected data



Secured Architecture

**SUPSI**

Scuola Universitaria Professionale  
della Svizzera Italiana

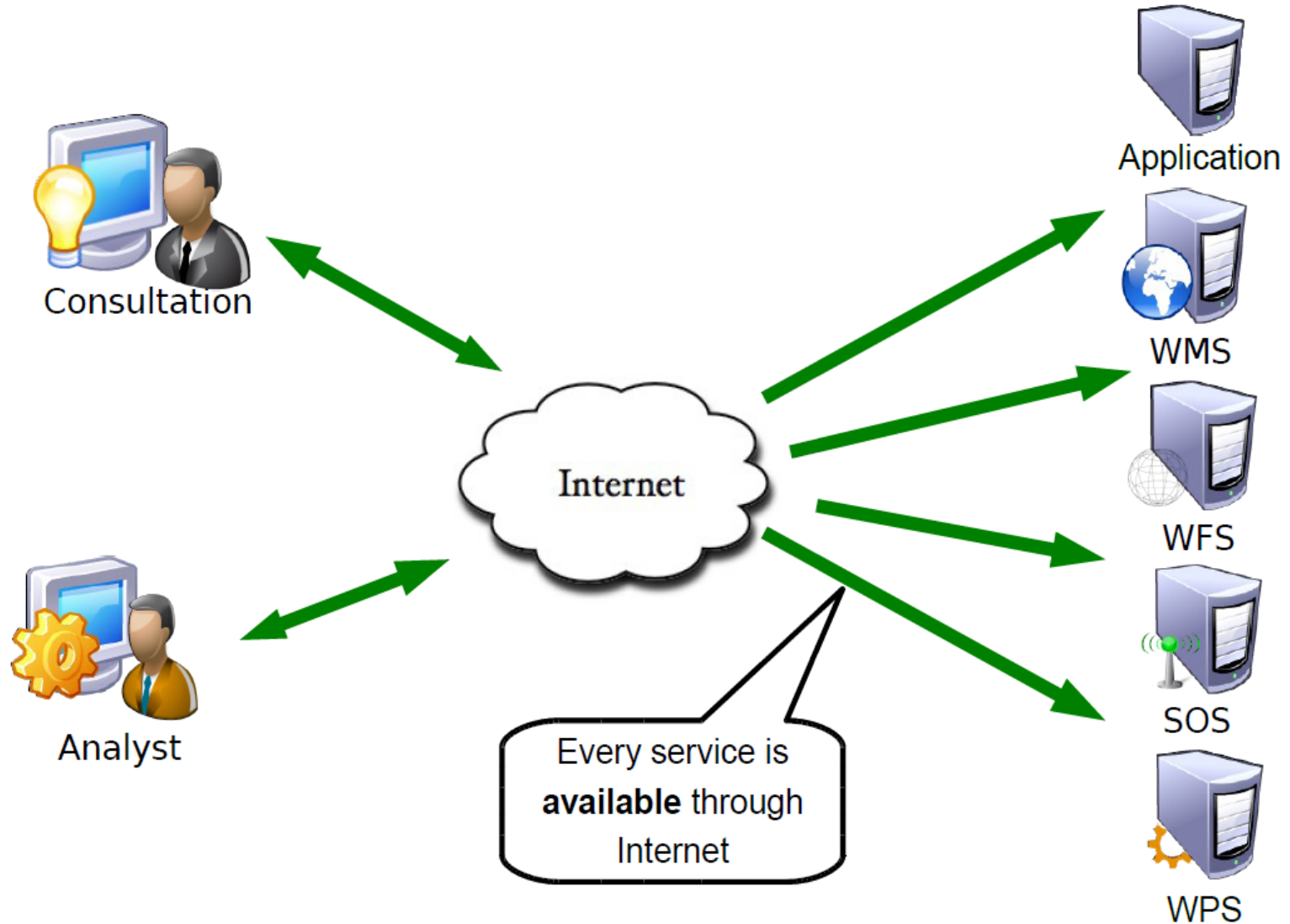


# The OGC stack at the IST

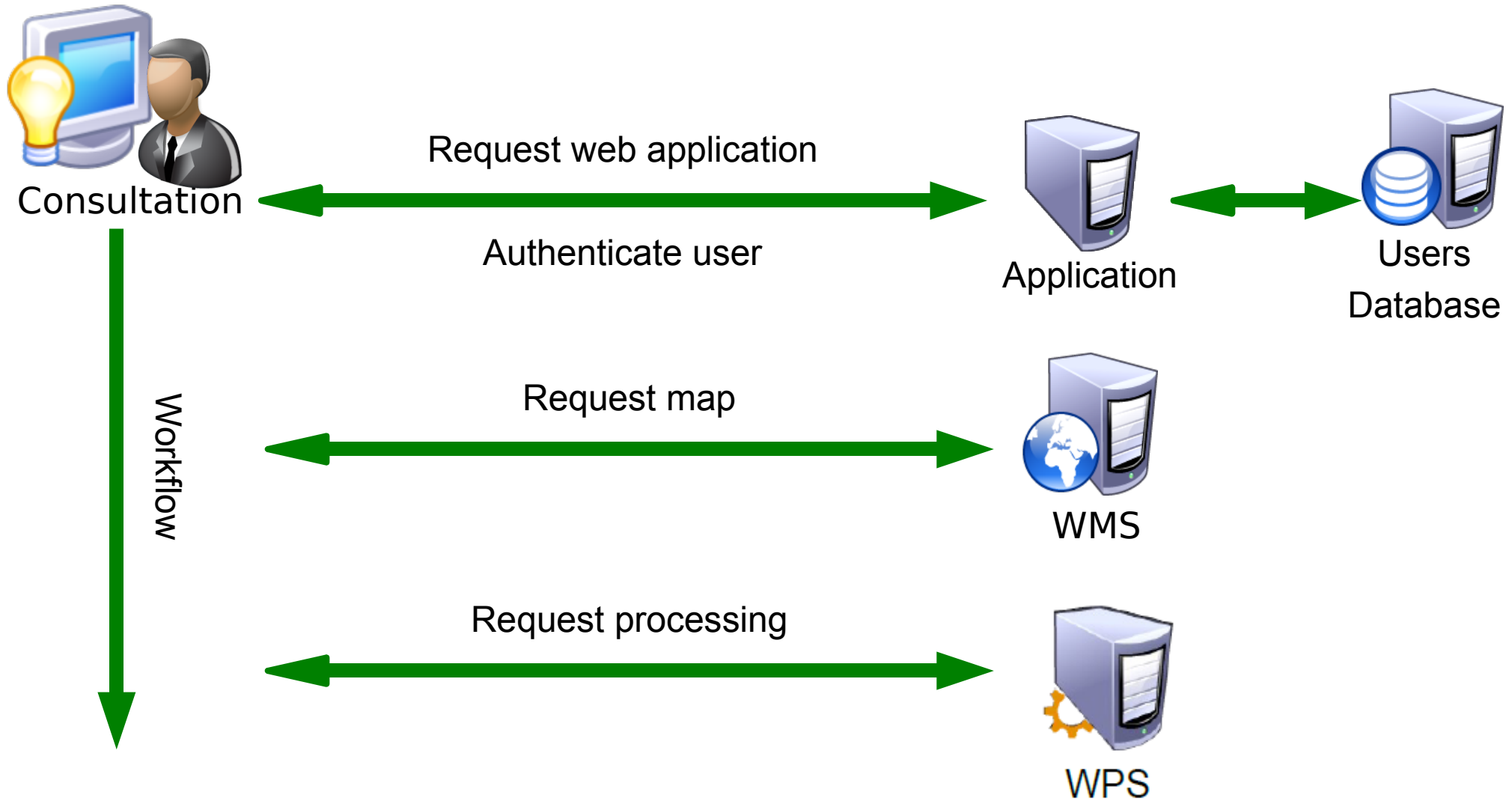
services implementation at the  
Institute of Earth Science



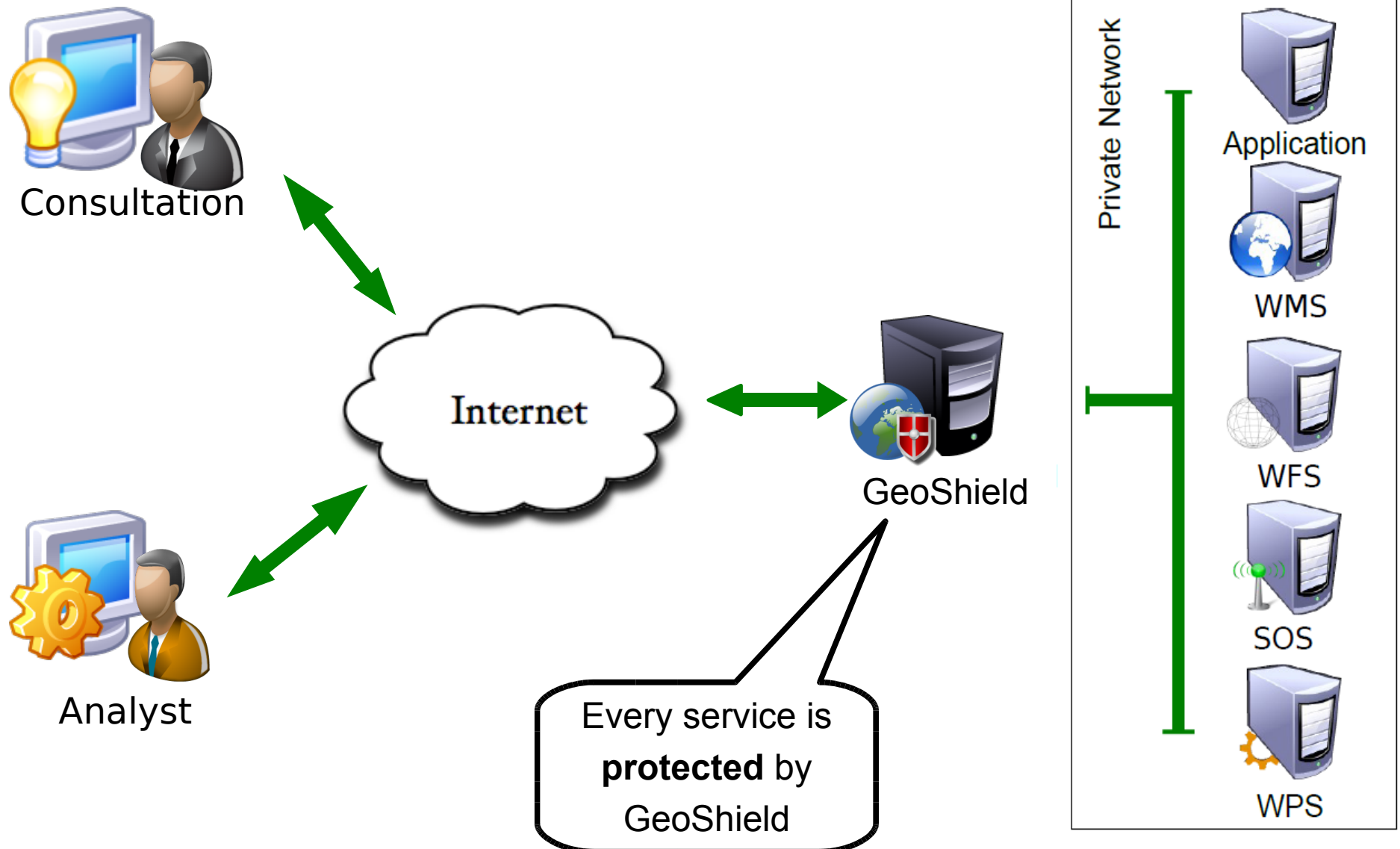
# Open architecture – system distribution



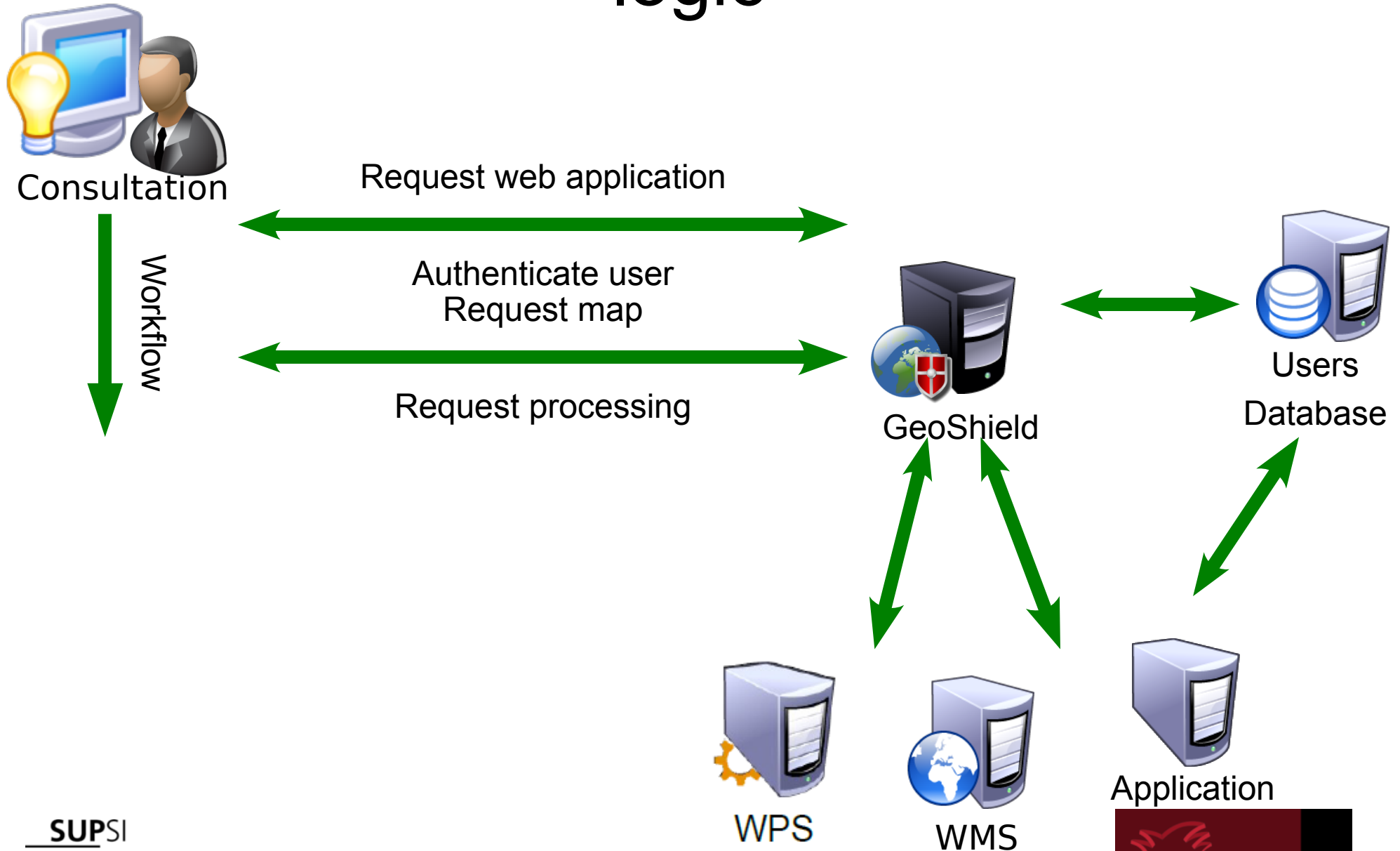
# Open architecture - application logic



# GeoShield architecture - system distribution



# GeoShield architecture - application logic





# GeoShield - technologies

Server side:



## **Java Servlet:**

- *Handling http request*



## **GeoTools, GeoApi:**

- *CQL to OGC:FILTER conversion*
- *Merge FILTERS*



## **Peristence Api (TopLink lib):**

- *Database interfacing framework*



## **PostgreSQL database**

- *Storing User-Group data and Services policies*

Web administration:



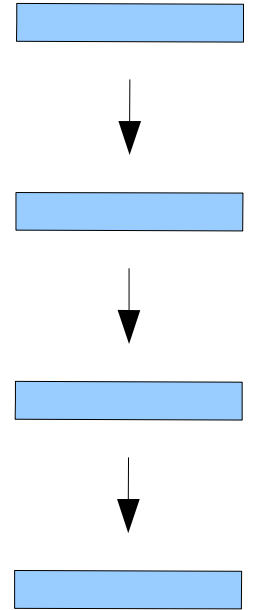
## **ExtJS interface**

- *Administering users and groups policies*

# GeoShield - Intercepting filter pattern

## Benefits:

- 📌 Modular architecture
- 📌 Easily add new filters for different services
- 📌 Redirect application requests
  - 📌 For example to unique login page
- 📌 Preprocessing and post-processing
  - 📌 Actively modification of client's requests and service's responses



# GeoShield administration interface

📌 Developed using  Ext JS framework

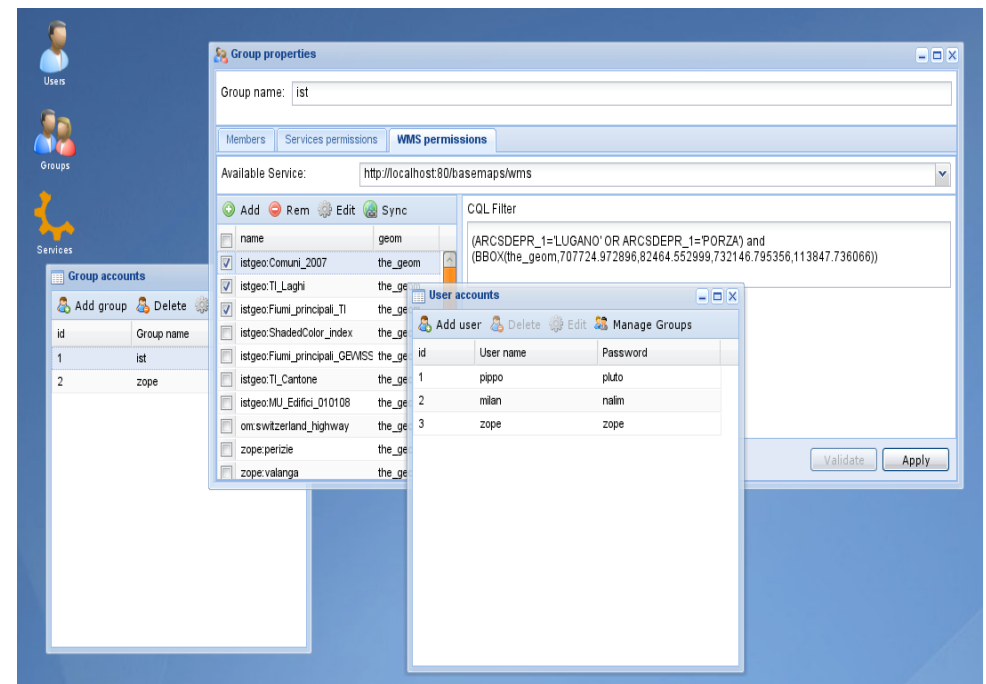
📌 Password protected

📌 Desktop-like interface

📌 User / Group management

📌 Service initialization

📌 Policy definition



# WMS example

- 📌 Access to service from different client applications
- 📌 Define access privilege for each layer provided by the service
- 📌 Specify if a layer can be viewed or not
- 📌 Define permissions on single features
- 📌 Define geometrical extent of view permission.
- 📌 Privileges definition with Common Query Language (CQL) a compact and human readable language, that allows interesting combination of permissions.

# WMS example: life cycle



Consultation



```
http://www.myurl.ch/geoshield/map/srv1?  
REQUEST=GetMap&  
BBOX=-97.105,24.913,-78.794,36.358&  
WIDTH=560&HEIGHT=350&  
LAYERS=DEMO&  
FORMAT=image/png&  
SERVICE=WMS
```



GeoShield

(...)



GetMap Request



**Authentication Filter**

*User not authenticated*



**Return HTTP code 401 Unauthorized**



*User authenticated*

**Service Filter**

*Service forbidden*



**Return HTTP code 403 Forbidden**



*Service allowed*

**WMS Filter**

*Layer "DEMO" forbidden*



**Return HTTP code 403 Forbidden**



(...)

(...)



**WMS  
Filter**

- **Load user CQL filters for layer DEMO:**

`"BBOX(the_geom, 147.15,-43, 147.5,-42.75)"`

- **Convert CQL to OpenGIS Filter Encoding**

`"<ogc:Filter>`

`<ogc:BBOX>`

`<ogc:PropertyName>the_geom</ogc:PropertyName>`

`<gml:Box>`

`<gml:coordinates>147.15,-43, 147.5,-42.75</gml:coordinates>`

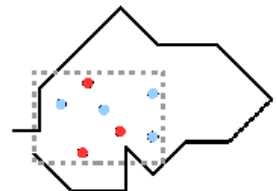
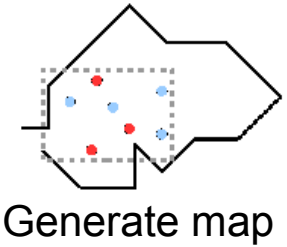
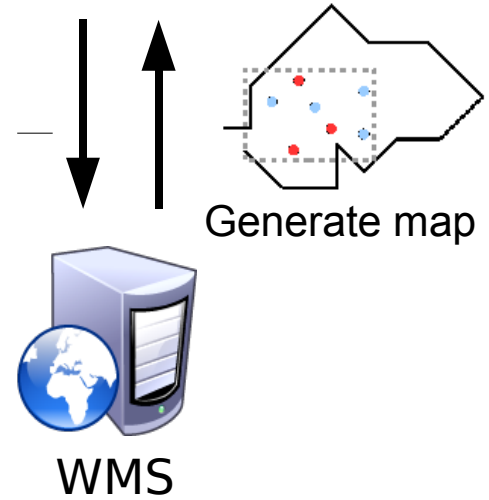
`</gml:Box>`

`</ogc:BBOX>`

`</ogc:Filter>"`

# Request map to WMS with Filter parameter

```
http://www.otherurl.ch/map/wms?  
REQUEST=GetMap& [...]  
Filter=  
<ogc:Filter>  
<ogc:BBOX>  
<ogc:PropertyName>  
the_geom  
</ogc:PropertyName>  
<gml:Box>  
<gml:coordinates>  
147.15,-43, 147.5,-42.75  
</gml:coordinates>  
</gml:Box>  
</ogc:BBOX>  
</ogc:Filter>
```



Consultation



# WMS example: main features

- 📌 Centralization for user/group management
- 📌 Managing many layers request in a single request
- 📌 Merge user filter with geoshield user permissions
- 📌 Creation of filters with Common Query Language (CQL)
  - Use of spatial operator for establish access policies
- 📌 Manage user / group permission
- 📌 Managing group permission on multiple services that can be on different servers

# DEMO

**SUPSI**

Scuola Universitaria Professionale  
della Svizzera Italiana



# Work in progress

📌 Other services protection:

📌 WPS

📌 SOS

📌 Interface enhancement with OpenLayers for WMS and WFS  
policy definition and testing

📌 Older application protection

📌 For user authentication

# For technical details contact: milan.antonovic@supsi.ch



*Institute of Earth Science:*  
<http://www.ist.supsi.ch>

*Division of Geomatics:*  
<http://istgeo.ist.supsi.ch>

**SUPSI**

Scuola Universitaria Professionale  
della Svizzera Italiana

Cannata Massimiliano - Antonovic Milan

