GeoShield

a server side user permissions management to OGC services

Cannata Massimiliano - Antonovic Milan
Institute of Earth Science - Switzerland
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
The OGC stack at the IST

services implementation at the
Institute of Earth Science

GeoServer
WMS, WFS, WCS

PyWPS
Web Processing Service

IST
Sensor Observation Service

SUPSI
Scuola Universitaria Professionale
della Svizzera Italiana
Open architecture – system distribution

Every service is available through Internet
Open architecture - application logic

- Consultation
  - Request web application
  - Authenticate user
  - Request map
  - Request processing
  - Workflow

- Application
- Users
- Database
- WMS
- WPS

SUPSI
Scuola Universitaria Professionale
della Svizzera Italiana
GeoShield architecture - system distribution

Every service is protected by GeoShield
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

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
- 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>
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
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.supssi.ch

Division of Geomatics:  
http://istgeo.ist.supssi.ch

Cannata Massimiliano - Antonovic Milan