License and Permission-based access to OGC Web Services with 52°North

Jan Drewnak/Bastian Schäffer
52North.org
52N Security Community
http://www.52north.org/security

• Topics
  – Access Control for Services in SDI
  Alice is allowed to access all layers except <points of interest>
  – License Management
  Alice must agree to the terms of use before she can access the WMS
  – Client Software
  Alice wants to access the protected service with her favorite map client software as usual
Basic Architecture

Identity Provider

(52north WAS)

Service Provider

Policy Enforcement Service

(52north WSS)

Policy Decision Service

(52north PDP)

¬ Credentials ← Identity

→ Request + Identity ← Response

¬ Identity + Resources ← Policy Decision

→ WPS1

→ WMS1

→ WFS1

→ SOS1
How to get access

• ...by policies established by some admin user
• Policy describes permissions and denials
• Policy refers to dedicated
  – Subject: users, roles, IP addresses, ...
  – Resources: layers, areas, ...
  – Actions: GetMap, GetFeature, GetCapabilities,…
How to get access

• …by licenses as a result of accepting certain terms of use (online!)
• A particular license includes
  – policy
  – licensor (issuer)
  – Signature
  – licensee
  – terms of use: academic, private, …
  – duration
  – price model: once, per-use
• Advantages of online-licensing
  – speed
  – cost
  – transparency
  – expand business
License vs. License Model

• License
  – concrete instance
  – licensee, policy, price, period of validity

• License Model
  – no concrete licensee
  – defines parameters and value ranges
  – defines price models that may depend on the parameters
Pre-Licensing Architecture

Identity Provider
(52north WAS)

Service Provider

Policy Enforcement Service
(52north WSS)

Policy Decision Service
(52north PDP)

WPS1
WMS1
WFS1
SOS1

(52north WSS)
Licensing Architecture

License was concluded

Go on with WPS Execution

(52north LB) .scenes  Encryption  (52north LM Service)

(52north PDP)

Lic(Ref)

Lic(Policy)

Service Request + ID + License Ref

Service Response

(ID + Result + License Ref)

Policy Decision Service

License Broker

License Manager

License Provider

License Ref

Store Lic

Need: ID + License!

GetCapabilities

C re de ntial

ID

N e goti e &Or de r

http://localhost:8080/LicenseBrokerClient/confirmPaymentDataPaypal.jsf
Licensing Architecture

Identity Provider

Use 52n WSC.Web application to enable any client to deal with licensing workflow!

License Broker
(52north LB)

License Manager
(52north LM Service)

Policy Enforcement Service

Policy Decision Service
(52north PDP)

Service Provider

This may require connection to accounting service (in case of commercial licenses)

Trust required! Service Provider ↔ Identity Provider
Service Provider ↔ License Provider

Identity Provider

Negotiate & Order
License Reference

Store
License Reference

Response
I D + R e s p o n s e + L i c R e f

Use 52n WSC.Web application to enable any client to deal with licensing workflow!

This is a web application that is usually part of a portal or shop.

Trust required! Service Provider ↔ Identity Provider
Service Provider ↔ License Provider

Licensing Architecture

www.52north.org/security
Summary

• Dynamic Access Control
• Advantages of online-licensing
  – speed
  – cost
  – transparency
  – expand business
Current State

- 52N completely implements the licensing workflow
- License Broker currently limited to static license models (no parameterization)
- In accordance with OGC GeoRM Reference Model

52N allows to implement policy & license-based access to
- WMS (layers, area, operations)
- WFS (feature types, features, attributes, area, operations)
- WPS (processes and operations)
- SOS (observations, POI, ... plus operations)
Enjoy FOSS4G!

Dipl.-Geoinf.
Jan Drewnak

52°North GmbH
Muenster
Germany

drewnak@52north.org
www.52north.org

Dipl.-Geoinf.
Bastian Schäffer

52°North GmbH
Muenster
Germany

schaeffer@52north.org
www.52north.org