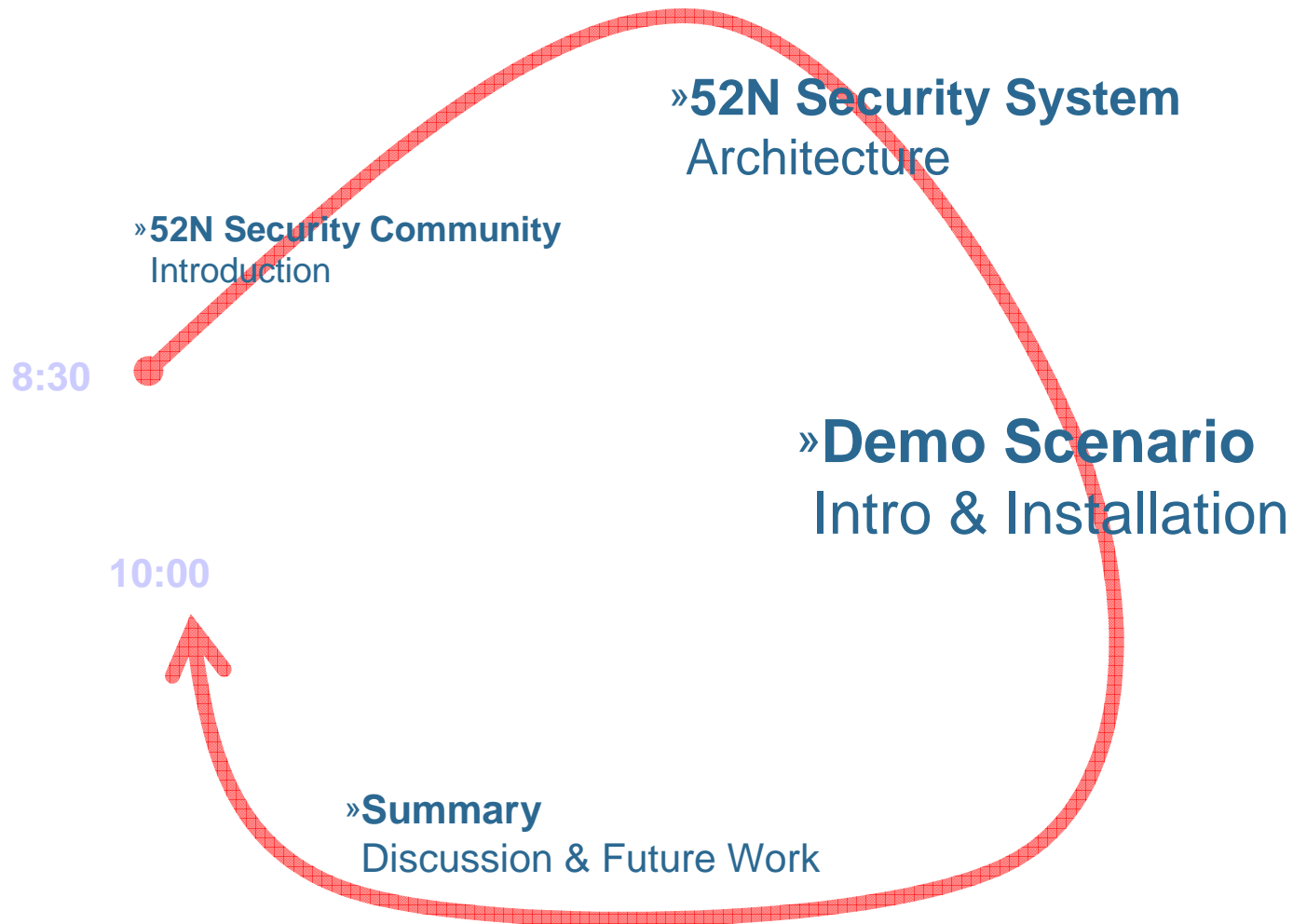


# Protecting OGC Web Services with the 52North Security System

Jan Drewnak/Bastian Schäffer  
52North.org

# Tutorial Roadmap



# 52North

or „52-N“ or „5-2-N“ or „52-North“ or „5-2-North“

- Founded in 2004
  - Institute for Geoinformatics, Münster, Germany
  - ITC Enschede, The Netherlands
  - con terra GmbH, Münster, Germany
  - since 2006: ESRI Inc., Redlands, US
- Mission: Development of innovative components for spatial data infrastructures

Sensor Web Enablement		Security (Access Control)
Processing Services		Raster Processing
- License Model: Dual Licensing (GPL 2.0 & Commercial)
  - Example: con terra securityManager, based on 52n Security Services

# 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

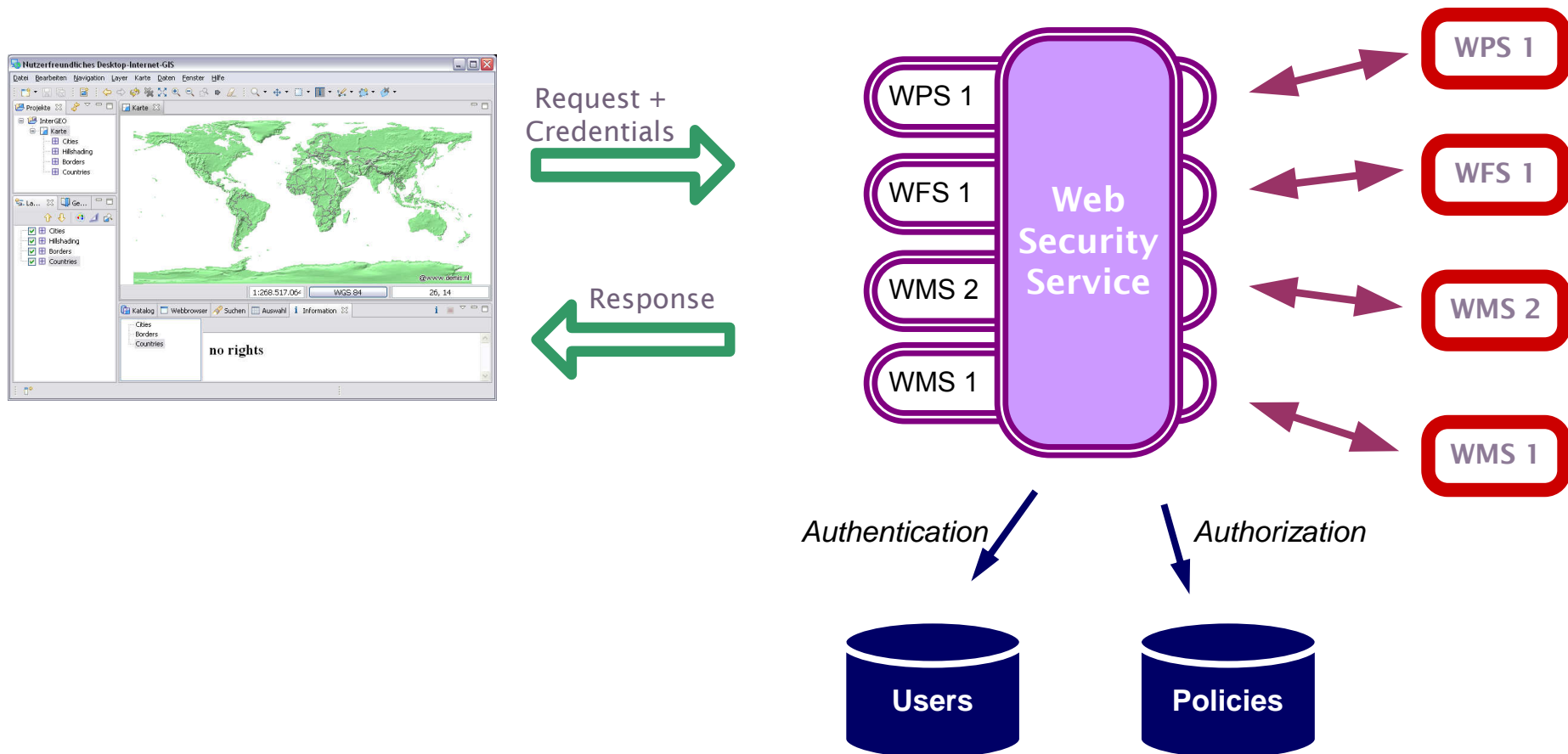
- Client Software



Alice wants to access the protected service with her favorite map client software as usual

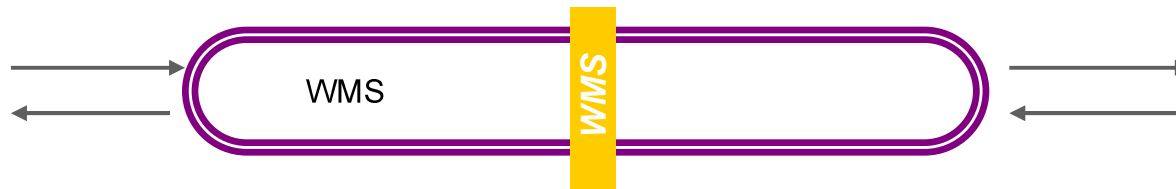
# Security Architecture

# Basic Architecture



# Interceptors

- Operation allowed? → Block/Forward request
- Layer allowed? → remove Layer from request or capabilities
- Area allowed? → block or clip response



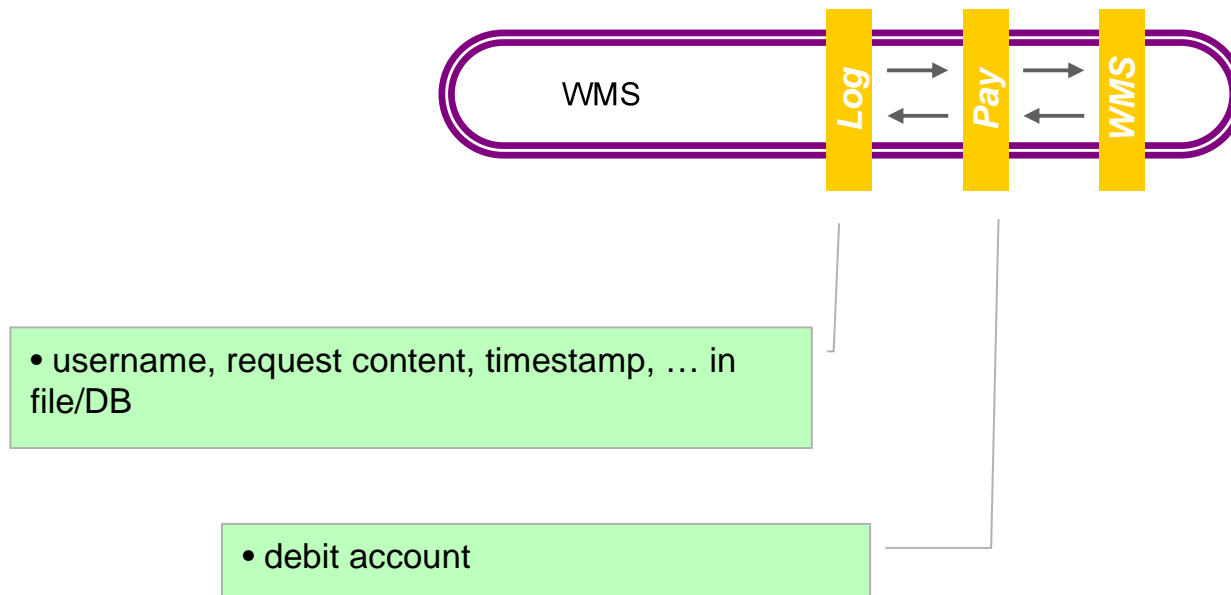
## 52N Interceptors

- WMS: operations/layers/spatial extent
- SOS: operations/FOI,offerings,.../ spatial and temporal extent
- *Logging Interceptor*

## Further known

- WFS(-T)
- WCS
- ArcIMS
- ArcGIS Server

# Interceptors – Chaining



# Authentication Processors



- \* Extract credentials
- \* Protocol specific

## 52N Authentication Schemes

- *HTTP Basic Auth*: username/password in HTTP header
- *"No Auth"*: default user
- *WSS-native*: SAML

## Wish list

- *WS-S Token Profiles*
- *HTTP Digest Authentication*
- *OpenID*

# LoginModules

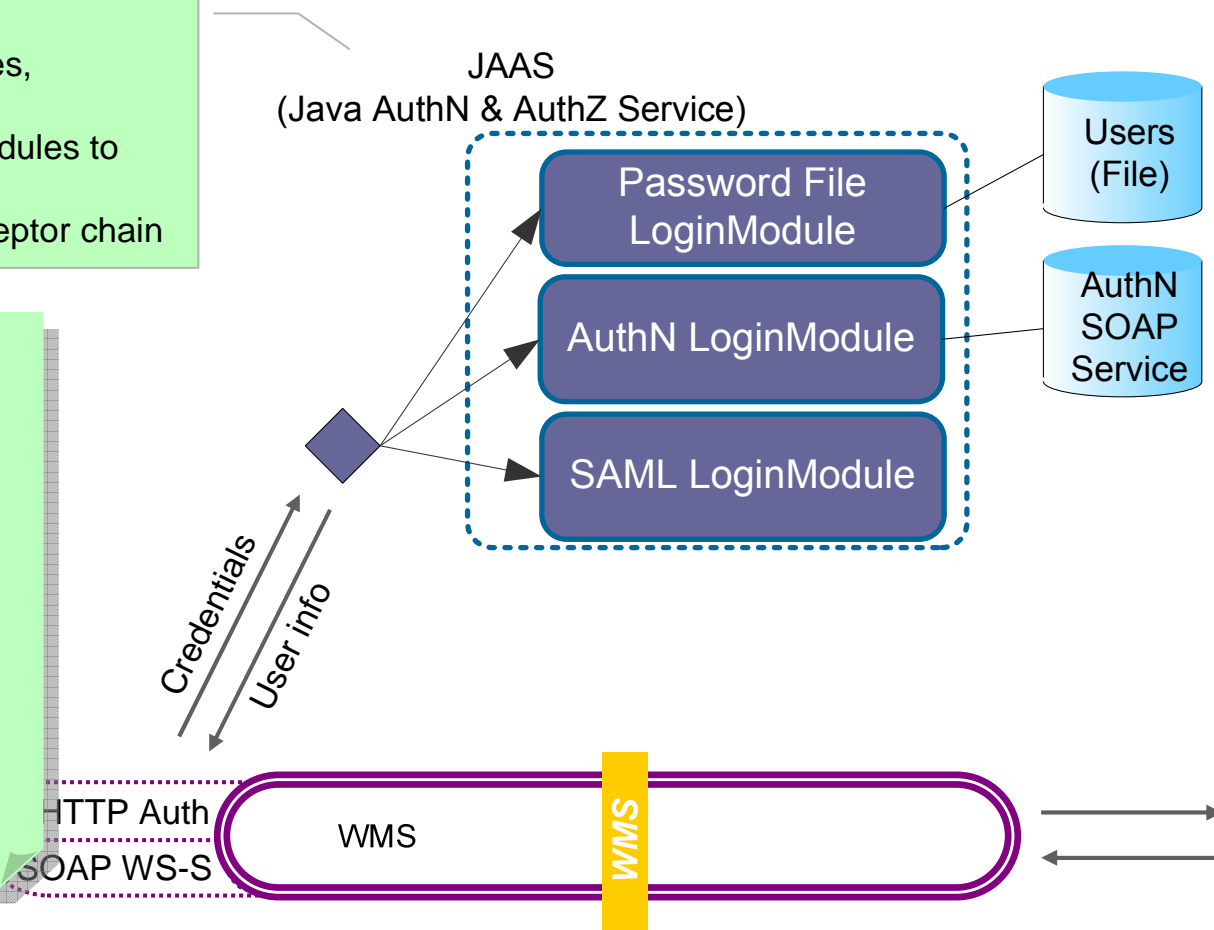
- verify credentials
- retrieve user information: name, roles, address,...
- sequentially walks through LoginModules to collect information
- User information is passed to interceptor chain

## 52N LoginModules

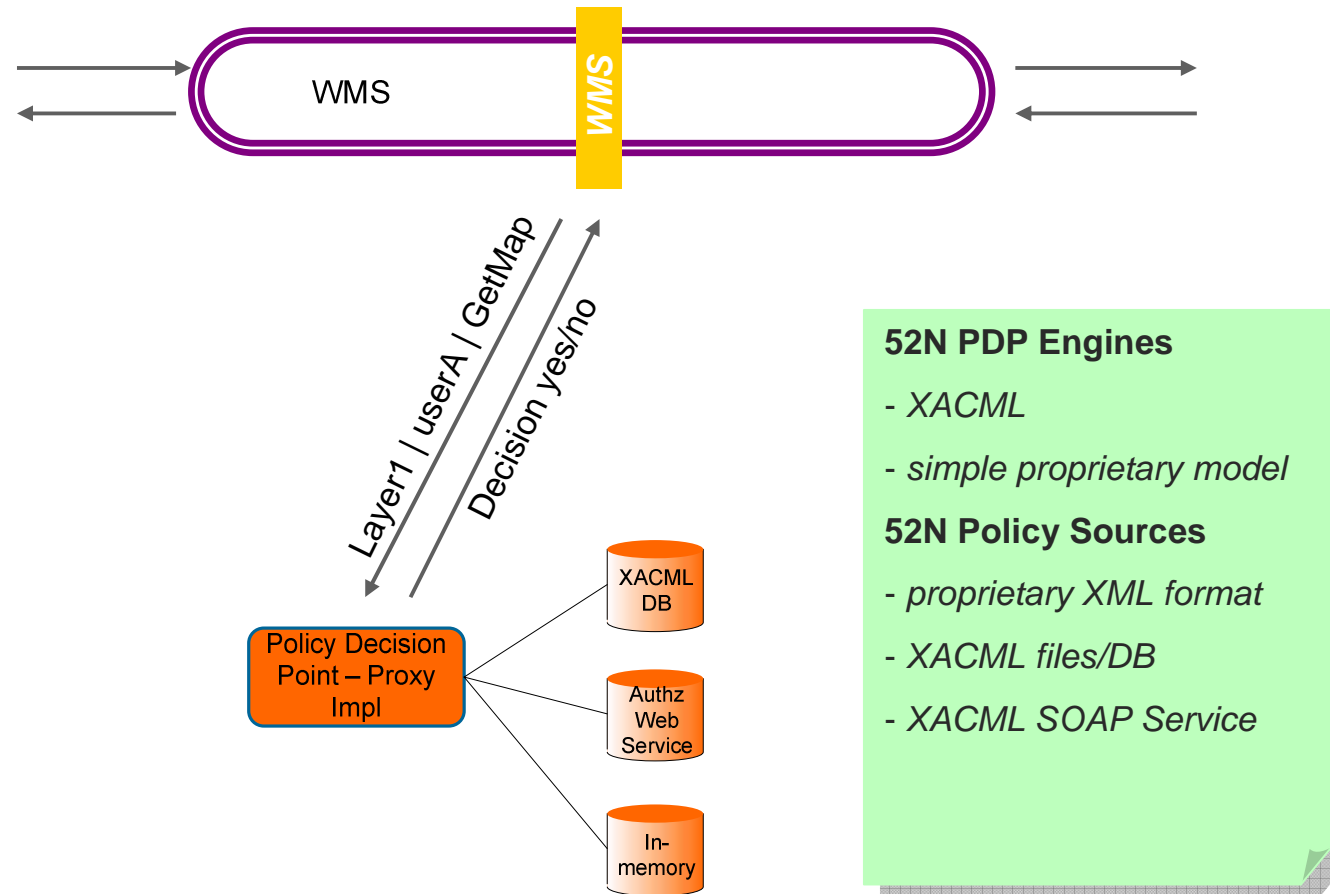
- SAML LM: verify SAML Assertion
- Password File LM: verify username/password
- WAS LM: Dedicated AuthN Service

## Further known

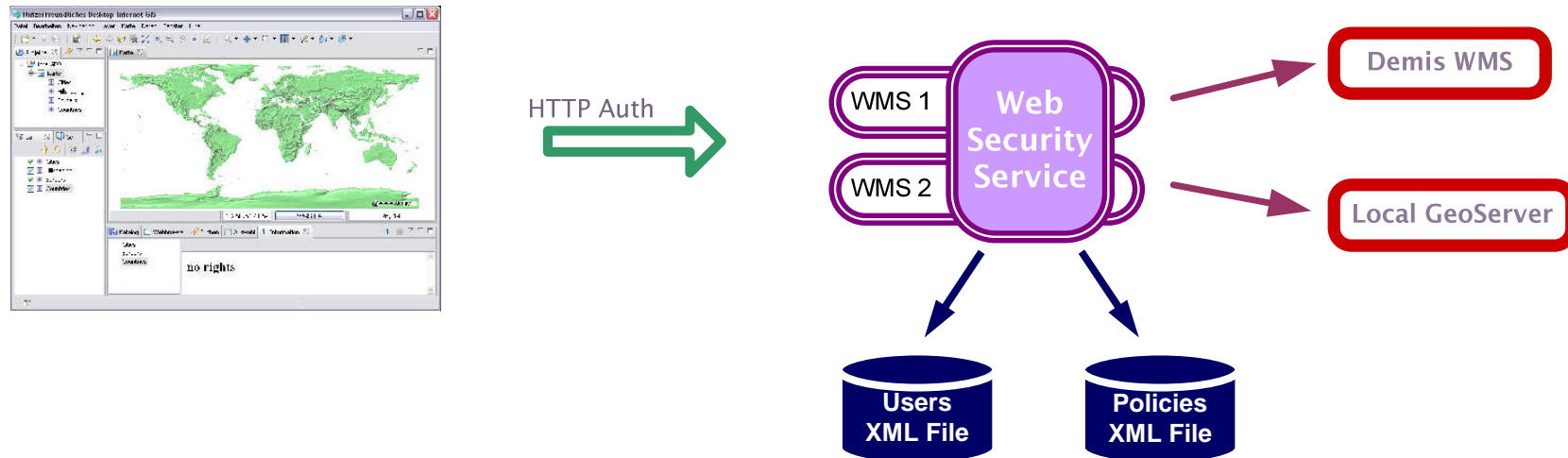
- LDAP LM
- Password DB LM
- X.509 LM



# Policy Decision Points



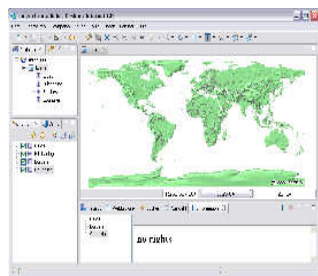
# Demo Szenario



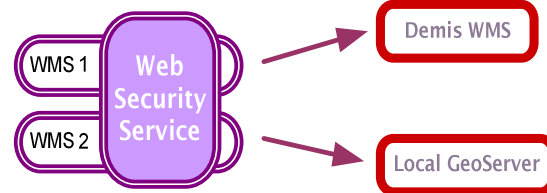
## Requirements & suggested setup

Software	Source
Windows OS	Your laptop ;-)
uDig	Arramagong Live DVD or 52n Security CD
Java	52N Security CD
Jetty Web Server bundle: WSS + local GeoServer	52N Security CD
Text Editor, Browser, ...	Your laptop

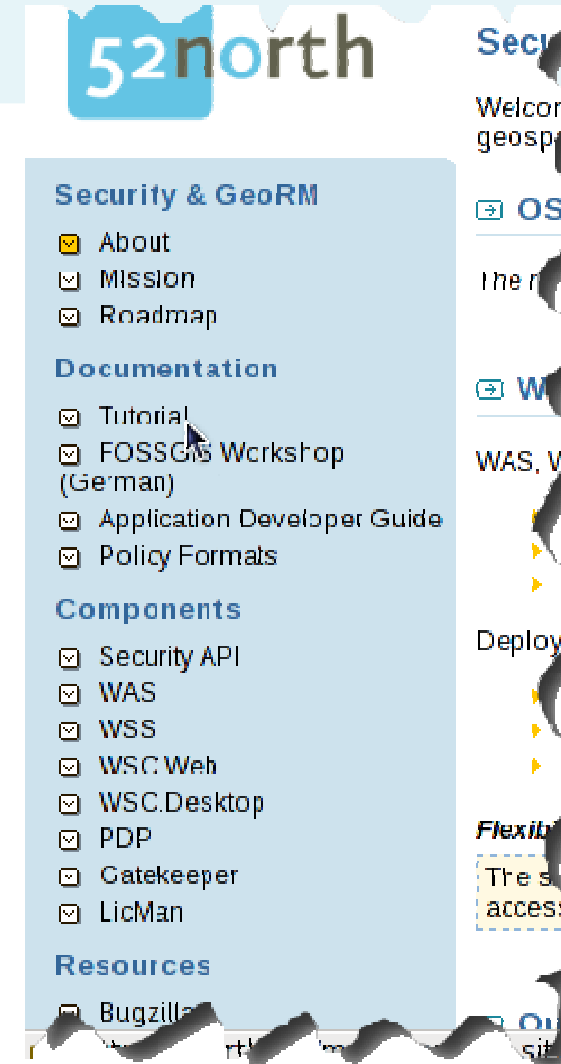
# Demo Scenario



HTTP Auth →



[www.52north.org/security](http://www.52north.org/security)



# Future Work

Beyond the daily maintenance work...

- Implement additional authentication schemes
  - esp. SOAP WS-S as proposed by OGC
- Stabilize and release WPS and WFS interceptors
- Support Spring-based configuration
- ? Integrate with OGC service implementations
- Implement license workflow
  - User gets access only after they accepted a click-through license

# Enjoy FOSS4G!

Dipl.-Geoinf.  
**Jan Drewnak**

52North GmbH  
Muenster  
Germany

[drewnak@52north.org](mailto:drewnak@52north.org)  
[www.52north.org](http://www.52north.org)

Dipl.-Geoinf.  
**Bastian Schäffer**

52North GmbH  
Muenster  
Germany

[schaeffer@52north.org](mailto:schaeffer@52north.org)  
[www.52north.org](http://www.52north.org)