Protecting OGC Web Services with the 52°North Security System

Jan Drewnak
52North.org
52°North
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

• Mission: Development of innovative components for spatial data infrastructures
  Sensor Web Enablement | Security (Access Control)

• New working areas
  (Geo) Processing Services | Raster Processing

• License Model: Dual Licensing (GPL 2.0 & Commercial)
• **Topics**

  – Access Control for Services in SDI

  – License Management

  – Client Software

Alice is allowed to access all layers except <points of interest>.

Alice must agree to the terms of use before she can access the WMS.

Alice wants to access the protected service with her favorite map client software as usual.
Security Architecture
52N’s current approach

• Based on specifications of the Regional SDI in North Rhine-Westphalia (since 1999)
• First developments in the security area 2001
• Goals of the development
  – Access control for OGC Web Services (authentication and authorization)
  – Security solution that integrates seamlessly into existing infrastructure, that means:
    – Existing service specifications, and thus implementations, need not to be changed
    – Consider current security specifications of general IT
52N’s current approach

- Result: 2 service specifications
  - Web Authentication Service (WAS)
    - Authenticates users by means of arbitrary authentication methods
    - Issues SAML tickets
  - Web Security Service (WSS)
    - Gateway to protected OGC Web Services
    - Processes SAML tickets
    - Forwards service requests according to the user’s permissions
- Introduced to the OGC
Variant (not implemented):
- exchange facade id as cookie

52N Implementations:
- WSC.Web
- WSC.Desktop

https://my.org/34bd-45baf-423d-2342
- WSS: https://your.org/WSS
- Ticket: <SAMLAssertion>for Jan...
- Expiration: in 15 min.

https://my.org/guest
- WSS: https://your.org/WSS
- Ticket: <SAMLAssertion>for guest...
- Expiration: never

http://localhost:1099/yourorg
- WSS: https://your.org/WSS
- Ticket: <SAMLAssertion>for Jan...
- Expiration: never

- secret
- remote
- temporary
- user initiated

- public
- remote
- permanent
- admin initiated

- local
- permanent
- user initiated
52N Interceptors:
- GetCapabilities / GetMap / GetFeatureInfo Interceptor
- Logging Interceptor
Further known
- WFS(-T)
- WCS
- ArcIMS
- ArcGIS Server

52N PDP Proxies:
- XML File (proprietary)
- XACML Files
Further known
- XACML DB
- proprietary, product-specific
52N LoginModules:
- XML File (proprietary), Password
- Database (proprietary), Password
Further known (used with WAS)
- LDAP, Password
Demo Scenario

- uDig
  - GetMap
  - Map
  - local

- WSC.Web
  - GetMap & SAML Ticket
  - Map
  - http://localhost:9090/wscweb

- WSS
  - GetMap
  - Map
  - http://localhost:9090/wss/WSS

- Demis World WMS
  - http://www2.demis.nl/wms/wms.asp?wms=WorldMap

- WAS
  - Credentials
  - SAML Ticket
  - http://localhost:9090/was/WAS

- User XML File
  - Policies XML File
Demo Scenario

Security Community
- About
- Mission
- Roadmap
- News

Sub-Projects
- Security Applications
  - WAS
  - WSS
  - WSC/Web
  - LiCMan
- Security API
  - 1.2 (stable)
  - 2.0 (development)

Resources
- Bugzilla
- Mailing Lists
- Sources
- Wiki
- Schemas

Extras
- Tutorials
- FOSS4G 200/ Tutorial

52n Projects
- Security

www.52north.org/security
Future Work

Beyond the daily maintenance work…

• Switch to SOAP based interfaces
  – based on OGC OWS testbed results)
  => OASIS Web Services-Security compliant

• Release dedicated PDP XACML service

• Redesign WSC.Desktop
Enjoy FOSS4G!

Dipl.-Geoinf.
Jan Drewnak

52°North GmbH
Muenster
Germany

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