How to protect OGC web services

03.09.2012
Jari Reini

OGC
Nordic Interoperability Day
3 September • Stockholm
Agenda

- Geospatial web services
  - WMS, WFS, W*S
- Authentication and authorization
  - SAML (Shibboleth)
  - XACML, GeoXACML
- Products
NLS Open Data – May 1 2012

Topographic maps 1:25,000 ... (raster)

Topographic Database (vector)

Elevation model 2m, 10m ... (grid)

Background maps 1:10,000 ... 1:8 M (raster)

Ortophotos (0,5 m)

Laser scanning data (LAS)

http://www.maanmittauslaitos.fi/en/opendata
Interface standards

- **WMS** Web Map Service
  - *Serves georeferenced images*
  
  [http://www.opengeospatial.org/standards/wms](http://www.opengeospatial.org/standards/wms)

- **WMTS** Web Map Tiling Service
  - *provides map tiles (small images that are part of a map)*

  [http://www.opengeospatial.org/standards/wmts](http://www.opengeospatial.org/standards/wmts)
Interface standards

- **WFS Web Feature Service**
  - *an interface allowing requests for geographical features across the web*
  - **GML**

http://www.opengeospatial.org/standards/wfs
http://www.opengeospatial.org/standards/filter
Authentication and authorization

- **Authentication**
  - "you are who you say you are"
  - *Methods: http basic, SAML etc.*

- **Authorization**
  - "you are permitted to do what you are trying to do"
  - *Authorization comes after authentication*
Authorization

- **XACML 2.0 (OASIS)**
  - *Policy Language supporting the declaration of access rights in XML*
  - *Definition of message formats to request authorization decisions*
  - *Not supporting spatial rights*

- **GeoXACML 1.0**
  - *Extension to XACML 2.0*
  - *Geospatial functions*
  - *GeoXACML is an OGC standard*
Authentication & Authorization architecture

Application -> Federation -> Authentication -> SAML -> Authorization -> XACML / GeoXACML -> Unchanged Web Services -> Data storage

Application -> Users -> SAML

Application -> SAML -> XACML / GeoXACML

Policies -> WMS -> WFS -> W*S
Potential use cases

- **Web Map Service (WMS)**
  - *User Jari has full access to all layers and operations on the WMS*
  - *User guest has GetMap access to the backgroundmap and buildupareas layers*
  - *User Jari can query (GetFeatureInfo) on all layers*

- **Web Feature Service (WFS)**
  - *User Jari can retrieve parcel information as vector content (GML) only from his planning area*

- **Web Processing Service (WPS)**
Products

- 52north

- Conterra

- Secure Dimensions
  - http://secure-dimensions.de/index.html.en
Demo

- WMS service (unchanged)
- Authorisation service in front of WMS
- Two users
  - guest – limited access
  - NLS – full access
Any questions?

jari.reini@nls.fi