der Bundeswehr Universität München

Geospatial eXtensible Access Control Markup Language (GeoXACML)

W3C PLING Meeting

Andreas Matheus
Universität der Bundeswehr München

Motivation

- Interoperable exchange of access rights across jurisdictions
  - Horizontal rights management
  - Vertical rights management
- Standard Policy Language to declare and enforce access rights in a flexible way for geospatial data
  - Independent from architecture
  - Independent from data structure and storage

GeoXACML Overview

- OGC Standard since February 2008
  - Core document: 07-026r2
  - Extension A: 07-098r1
  - Extension B: 07-099r1
- Support for the declaration and enforcement of (not only) geo-specific access rights
- Geo-specific extension to the eXtensible Access Control Markup Language (XACML)
  - Using XACML extension points

XACML Introduction

- eXtensible Access Control Markup Language (XACML) is a standard by OASIS
  - OASIS = Organization for the Advancement of Structured Information Standards
- Policy Language in XML
  - Structure of Policy: XML elements
  - data types and functions (non geo-specific)
  - Structure of authorization decision request / response
- Defines how to derive the authorization decision based on an authorization decision request and a policy instance

GeoXACML Introduction

- Definition of geometry data type and possible geometry encoding
  - Extension A: GML2 based geometry encoding
  - Extension B: GML3 based geometry encoding
- Definition of geo-specific functions based on OGC Simple Features Specification
  - Topological, Geometric, Set / Bag Functions
- Definition of Conversion Functions
- Use of XACML schemata for
  - authorization decision request / response
  - Policy

GeoXACML Policy Example (Snippet)

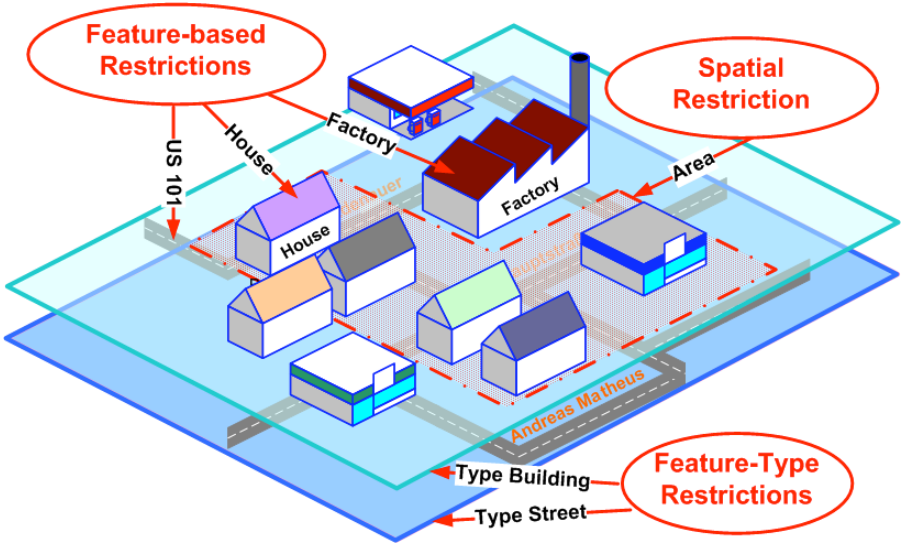
```
<Condition FunctionId="urn:oasis:names:tc:xacml:1.0:function:all-of">
  <Function FunctionId="urn:ogc:def:function:geoxacml:1.0:within"/>
  <AttributeValue DataType="http://www.opengis.net/gml#polygon">
    <gml:Polygon … gid="P2" srsName="EPSG:4326">
      <gml:outerBoundaryIs><gml:LinearRing>
        <gml:coordinates cs="," ts=" ">
              -74.28798767828596,40.72400955310945
              -74.12552621736093,40.722605998371435
              -74.12552621736093,40.614883172228936
              -74.28939123302396,40.61558494959794
              -74.28798767828596,40.72400955310945
              -74.28798767828596,40.72400955310945
              -74.28798767828596,40.72400955310
        </gml:coordinates>
      </gml:LinearRing></gml:outerBoundaryIs>
    </gml:Polygon>
  </AttributeValue>
  <AttributeSelector DataType="http://www.opengis.net/gml#box"
   MustBePresent="false" RequestContextPath="//ogc:BBOX/gml:Box"/>
</Condition>
```

Spatial <Function>

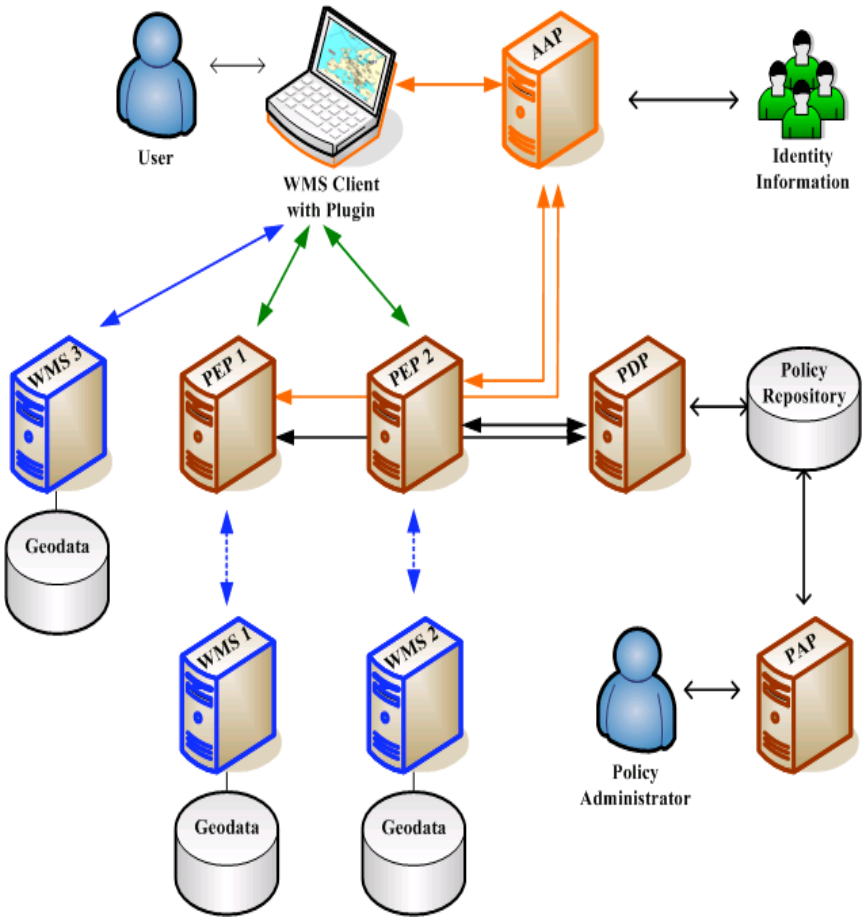
Spatial <AttributeValue>

GeoXACML – What else can you do with it?

- Control access to services, data, sensors, etc. in a Service Oriented Architecture
- Exchange / harmonize rights across jurisdiction based on the GeoXACML Policy Language
- Declare flexible access rights based on the characteristics of the data

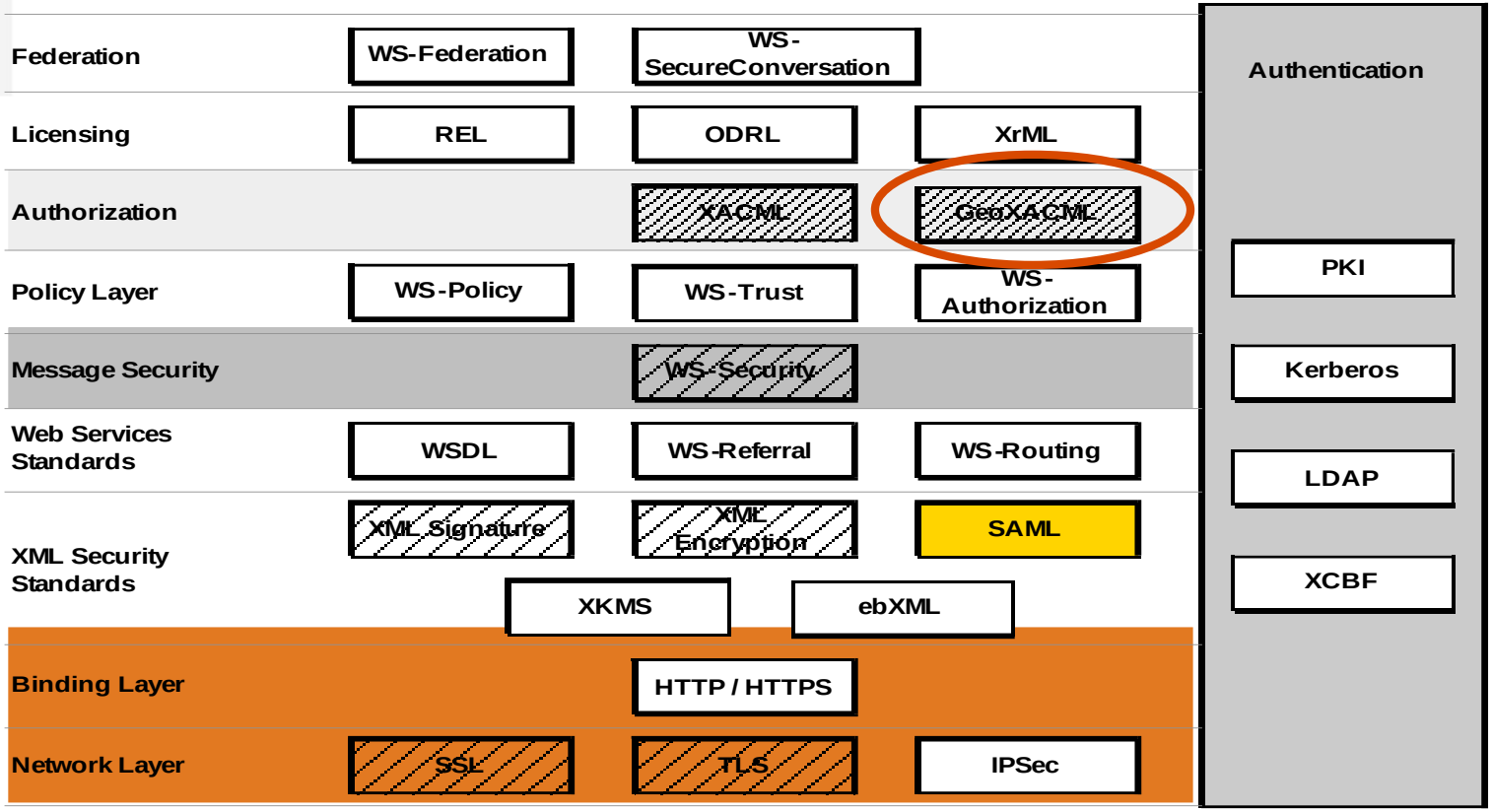


GeoXACML – How to use it with OGC Services



- AAP
  - Authentication Administration Point supports login with WMS client and request of SAML assertions from PEPs
- PAP
  - Policy Administration Point supports the Policy administrator in creating and maintaining GeoXACML policies
- PEP
  - Policy Enforcement Point intercepts communication from client to service and controls access based on authorization decisions received from PDP
- PDP
  - Policy Decision Point derives authorization decision for PEPs based on information received from authorization decision request and GeoXACML Policy
- WMS
  - Web Map Service to be protected

Standards Overview

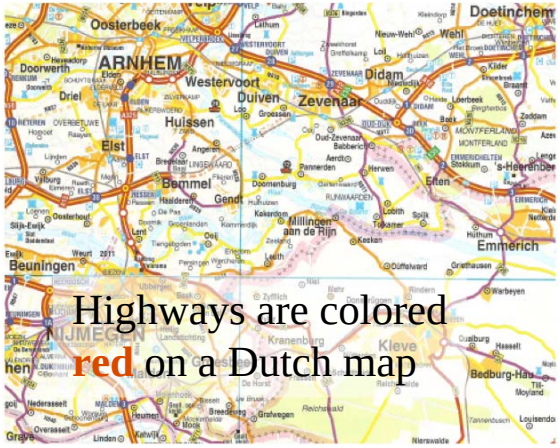


Cross Border Use Case (1/4)

- Origin
  - Use Case from the University of the Bundeswehr
  - Submitted for the *Persistent Testbed on Geo-spatial Services for Research and Teaching (PTB)*
  - *AGILE/EuroSDR/OGC* initiative

Cross Border Use Case (2/4)

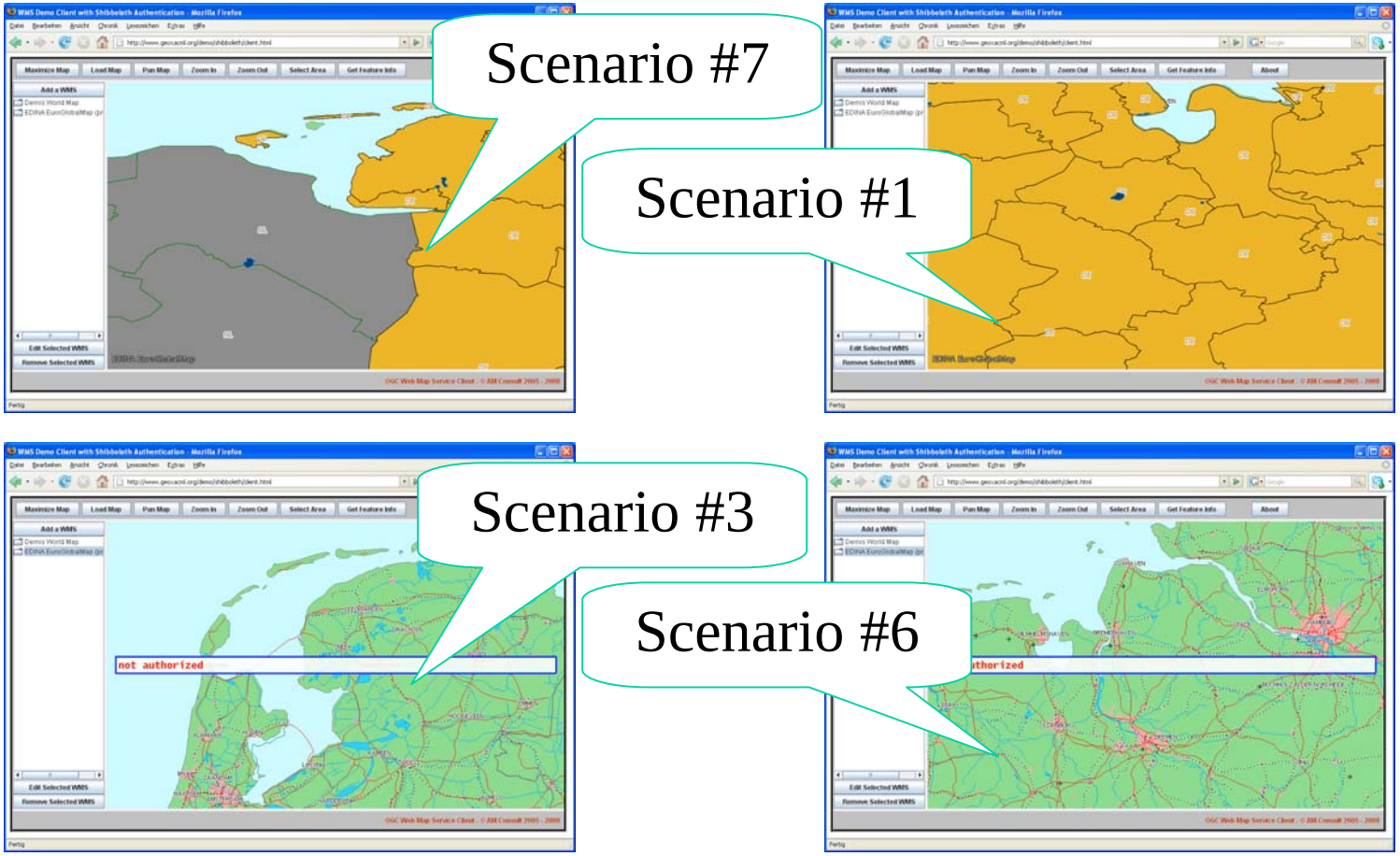
- Two national rescue centers manage cross border events together
- Problem
  - Operators of the centers are used to national styling of maps
- Solution
  - Allow operator of other nation to render maps using their national styling but only for maps of their terrain or cross border



Cross Border Use Case (3/4)

Scenario	Description of Access Restrictions
#1	A German user can apply German styling to German features
#2	A Dutch user can apply Dutch styling to Dutch features
#3	A German user cannot access Dutch features only (no cross-border operation!)
#4	A Dutch user cannot access German features only (no cross-border operation!)
#5	A Dutch User can never apply German styling
#6	A German User can never apply Dutch styling
#7	A German user can apply German styling to German AND Dutch features (cross-border operation)
#8	A Dutch user can apply Dutch styling to German AND Dutch features (cross-border operation)

Cross Border Use Case (4/4)



thank you very much for your attention!

questions please …

Andreas.Matheus@unibw.de
http://www.unibw.de/Andreas.Matheus