

GeoXACML, a spatial profile of XACML (OGC 05-036)

54th OGC Meeting, St. John's, Newfoundland

Andreas Matheus

University of the Federal Armed Forces Munich

Andreas.Matheus@UniBW.de

Clarification first

◆ What is 05-036 all about?

- Access Control for a Spatial Data Infrastructure

◆ What possible impacts does it have?

- Has impact to the Architecture Discussion
- Describes one possible technology to protect geodata

◆ What is the intension of 05-036?

- Feedback to create a consolidated Discussion Paper for the November meeting in Bonn.
- Describing a possible solution as a GeoDRM technology for Authorization

Content of this presentation / 05-036

- ◆ Introduction and Motivation
- ◆ Advanced SDI Architecture
- ◆ eXtensible Access Control Markup Language (XACML) from OASIS
- ◆ GeoXACML, a spatial profile of XACML
- ◆ Conclusion

Introduction and Motivation

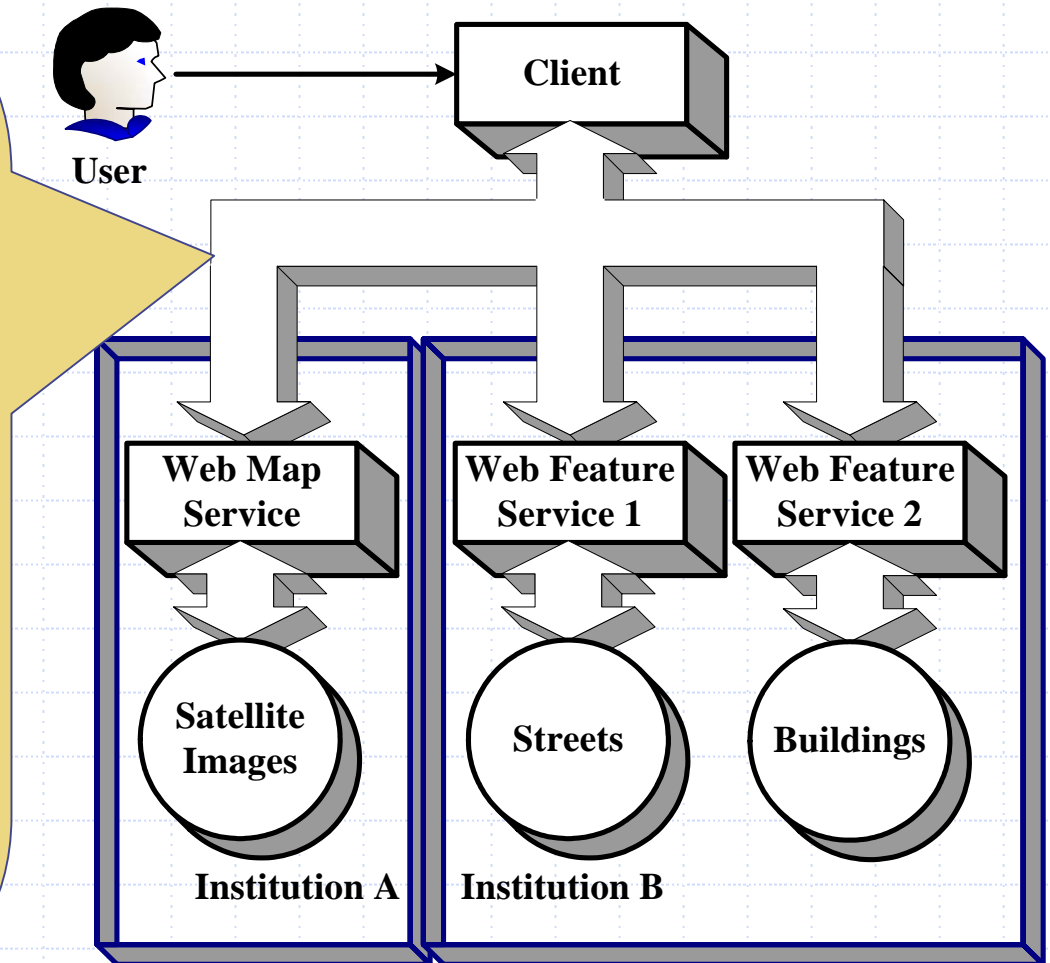
- ◆ Existing SDI with free access to geodata
 - Typically low quality data, not up-to-date
 - An adversary can possibly “download” all data from the service ⇒ **restrict access**
- ◆ Combined use of distributed and restricted geodata through a SDI requires
 - **Service-interface** interoperability
 - **Data-model** interoperability
 - **Access Control** interoperability
- ◆ What is the impact on the architecture of a SDI?

Basic SDI Architecture

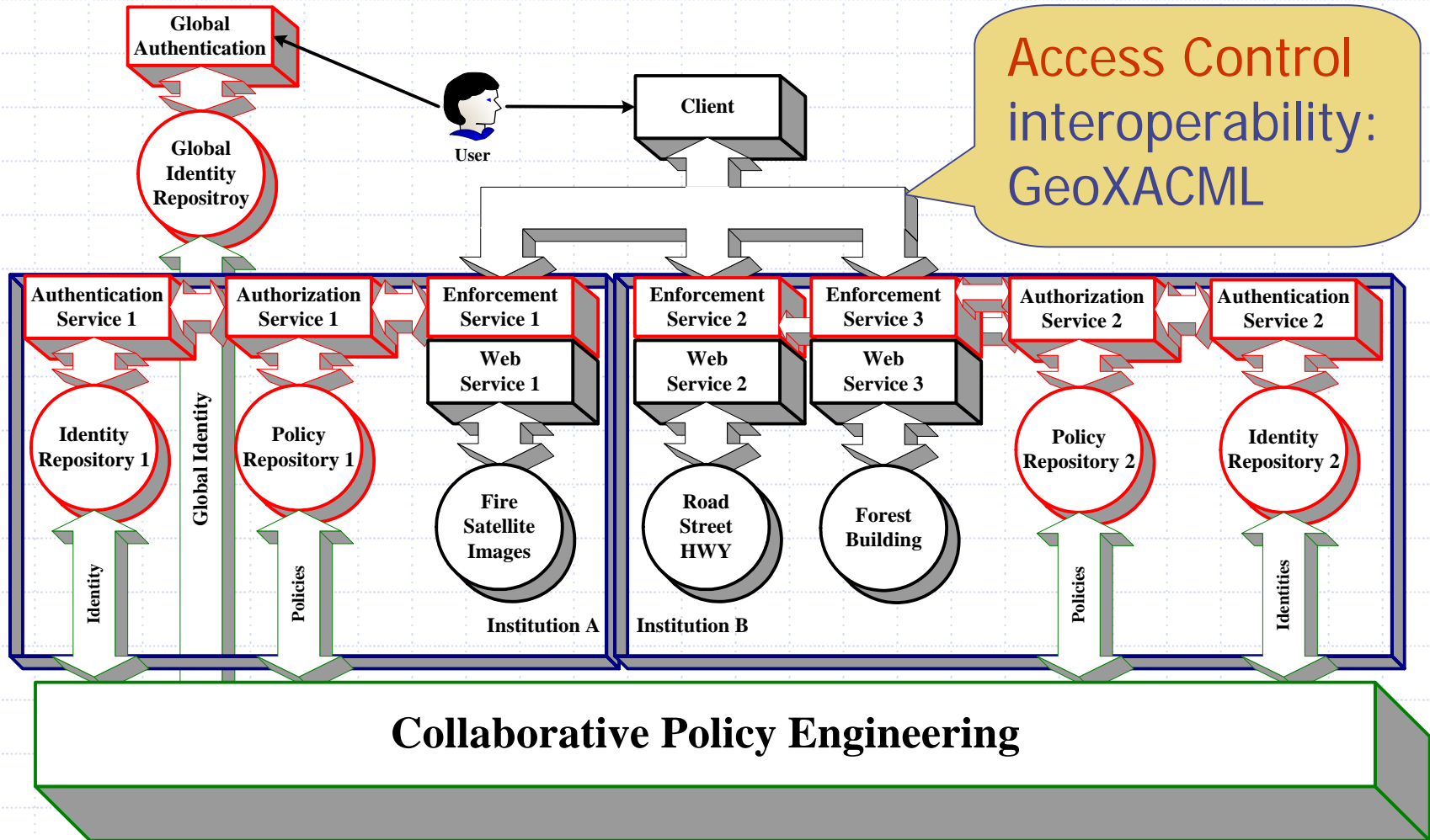
Service-interface interoperability:
WMS, WFS

Data-model interoperability:
GML, map in binary or vector format

Access Control interoperability:
N/A



Advanced SDI Architecture



Impact on Service Architecture

- ◆ Communication based on **SOAP** (literal encoding)
 - **<Header>** element keeps the access control required metadata, e.g. identity or role information of identities
 - **<Body>** element keeps the native OGC HTTP-Post request
- ◆ Authentication for Single-Sign-On required
 - **Liberty Alliance** describes mechanisms
 - **SAML** standard from OASIS describes data flow and message structure for communicating authentication and authorization information
- ◆ Authentication and possibly required security is based on PKI ⇒ **PKI must be in place**
- ◆ **How to incorporate these pre-requirements?**

Possibly a technology in GeoDRM?

- ◆ Licensing = Delegation of Rights
- ◆ Describe and evaluate proper delegation
 - Prove change of trust: Issuer, Distributer, User
- ◆ Describe and enforce the Rights of a License
- ◆ Access Control is based on Access Rights, so specialized Rights
 - No delegation!
 - The issuer is always in control of the declared rights
 - The issuer enforces the declared access rights

eXtensible Access Control Markup Language (XACML)

- ◆ Standard from OASIS <http://www.oasis-open.org/specs/index.php#xacmlv2.0>
- ◆ Rule-based access control
 - Define **conditions** to **permit** or **deny** access
 - RBAC profile of XACML defines Role Based Access Control
- ◆ Defines the means for restricting access to XML (hence GML) encoded information
 - **Policy language**: <Rule>, <Policy>, <PolicySet>, ...
 - **Data flow**: Deriving an authorization decision
 - **Message structure**: Authorization decision request / response
- ◆ **But, no support for spatial restrictions!**

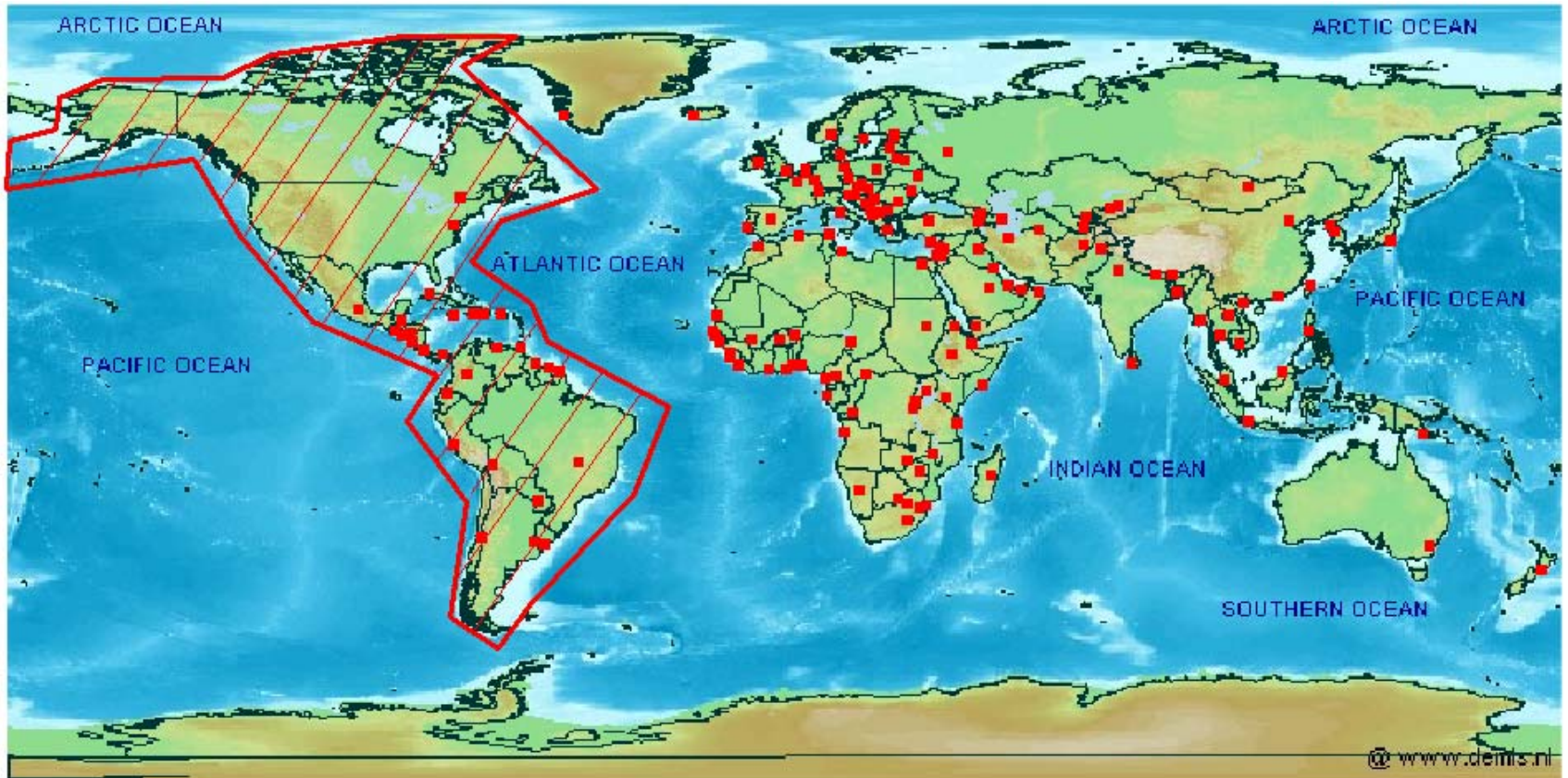
GeoXACML, a spatial profile of XACML

- ◆ **Obeys** to XACML policy language and data flow
- ◆ Definition of structured `<AttributeValue>` types for **expressing geometry**
 - GML 2.1 simple geometry
`<gml:Point>`, `<gml:LineString>`, `<gml:LinearRing>`,
`<gml:Box>`, `<gml:Polygon>`
 - Use of GML 3.0 simple geometry is possible but effects implementation
- ◆ Definition of functions for **testing topological relations between geometries**
 - Disjoint, Touches, Crosses, Within, Overlaps, Intersects, Equals, Contains

Capable to Declare and Enforce Feature-based Restrictions

- ◆ **Class-based** restrictions: GML feature type(s)
 - Associated to all features of a given feature type
 - E.g.: All features of the type Building
- ◆ **Object-based** restrictions: feature(s)
 - Associated to all features, selected by non-spatial characteristics – attribute(s) of the feature
 - E.g.: All features of type Building, painted black
- ◆ **Spatial** restrictions: geometry of feature(s)
 - Associated to all features, selected by spatial characteristics – geometry attribute(s) of the feature
 - E.g.: All features of type Building, within the administrative boundary of St. John's

Example Restrictions I/II (from January presentation)



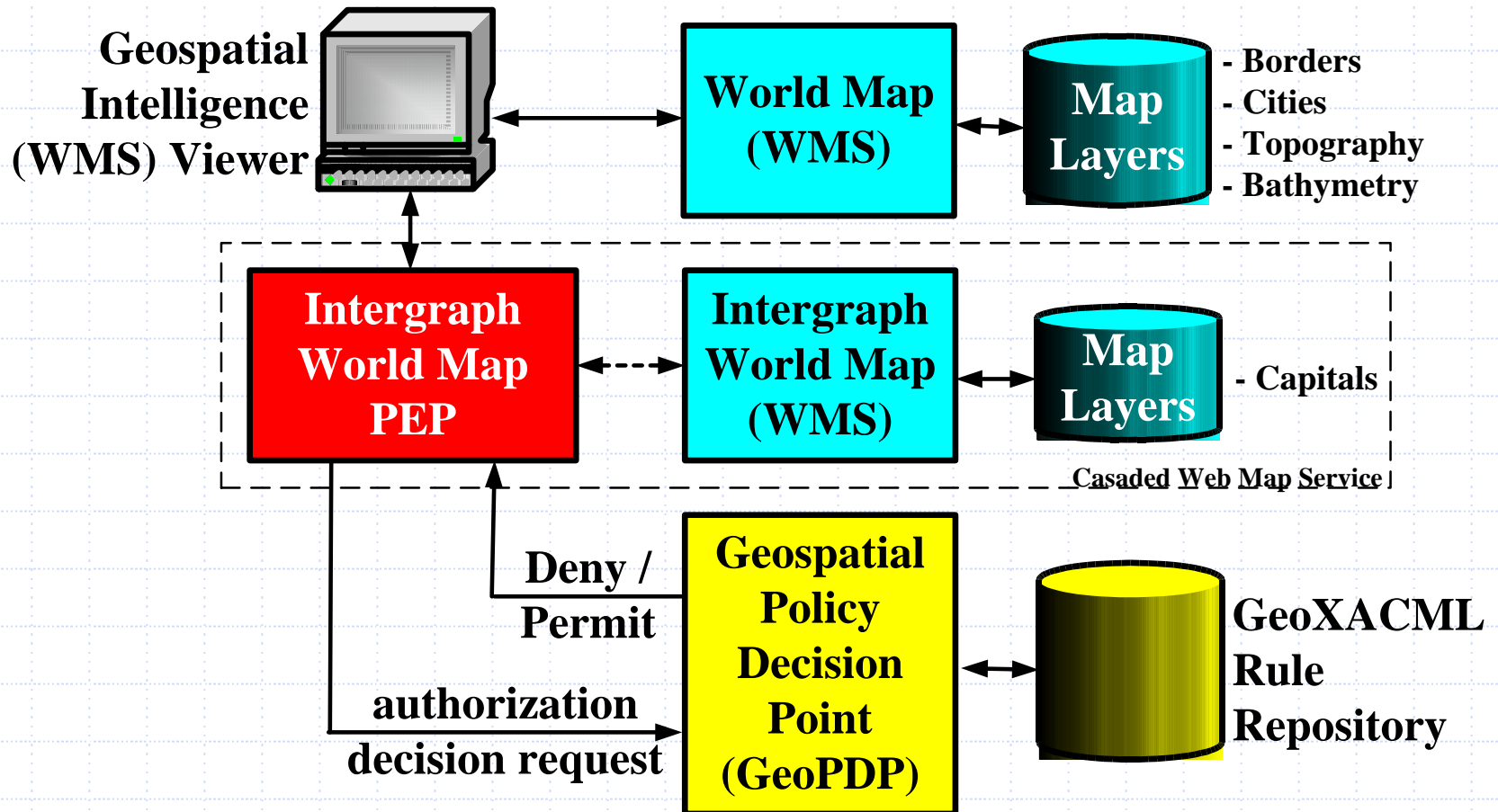
Mapping is denied to Capitals within red marked area

Example Restrictions II/II (from January presentation)



Read is permitted to Capitals within red marked area

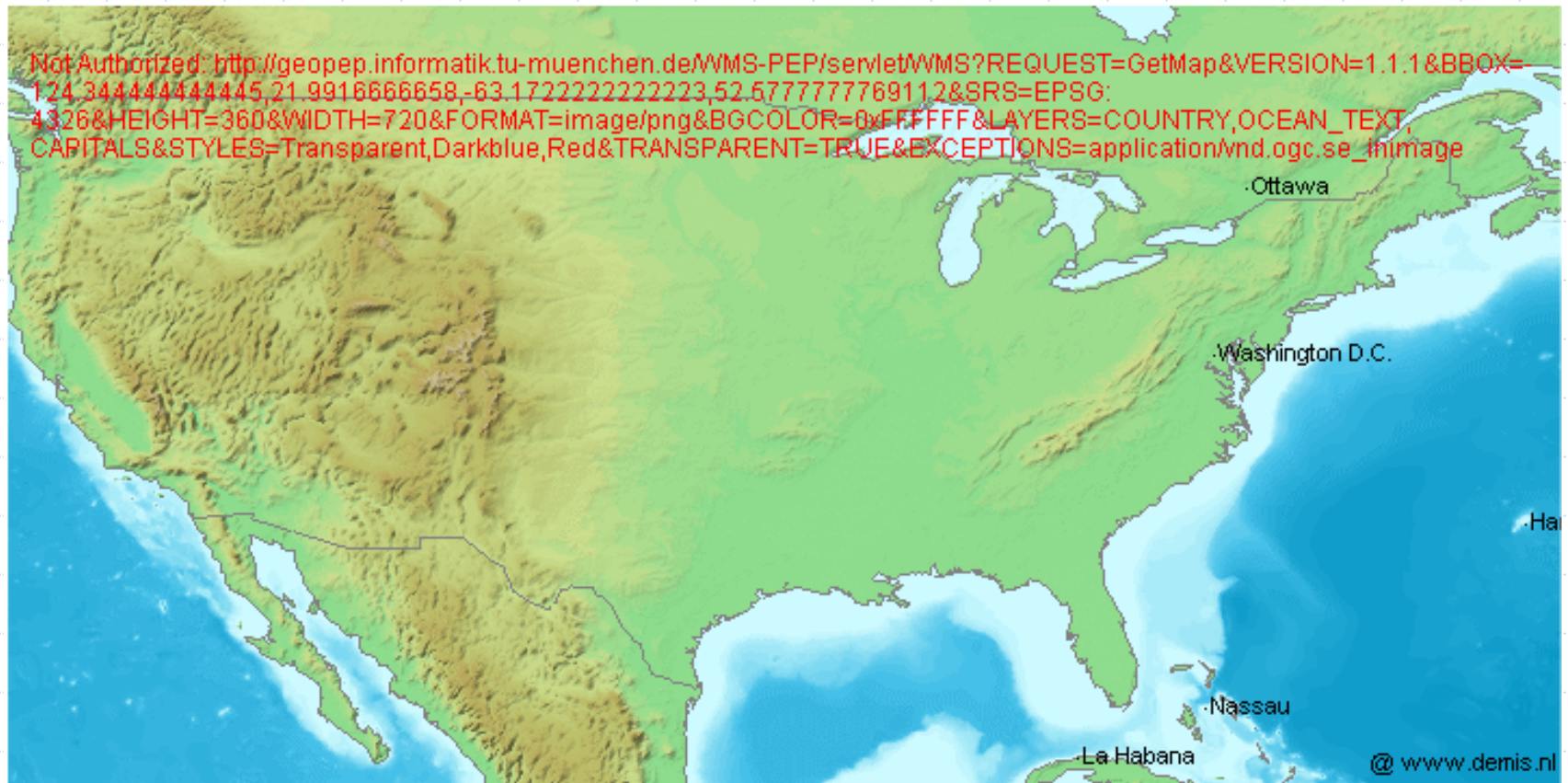
Demonstration Infrastructure according to XACML



URLs for the Demonstration

- ◆ Geospatial Intelligence Viewer - WMS Client
 - <http://ogc.intergraph.com/webmapviewer> (netscape 7.x)
- ◆ World Map – WMS Capabilities URL
 - <http://www2.demis.nl/mapservers/request.asp?WMTVER=1.0.0&REQUEST=capabilities>
- ◆ Intergraph World Map – WMS Capabilities URL
 - <http://maps1.intergraph.com/wms/world/request.asp?SERVICE=WMS&VERSION=1.1.0&REQUEST=GetCapabilities>
- ◆ Intergraph World Map PEP – Capabilities URL
 - <http://geo pep.informatik.tu-muenchen.de/WMS-PEP/servlet/WMS?SERVICE=WMS&VERSION=1.1.0&REQUEST=GetCapabilities>
- ◆ GeoXACML Example Policy
 - <http://geo pep.informatik.tu-muenchen.de/PDP/World.xml>

Mapping Request for Capitals in North America is denied



Ottawa and Washington D.C.: Capital symbols are missing

Mapping Request for Capitals in Europe is Permitted



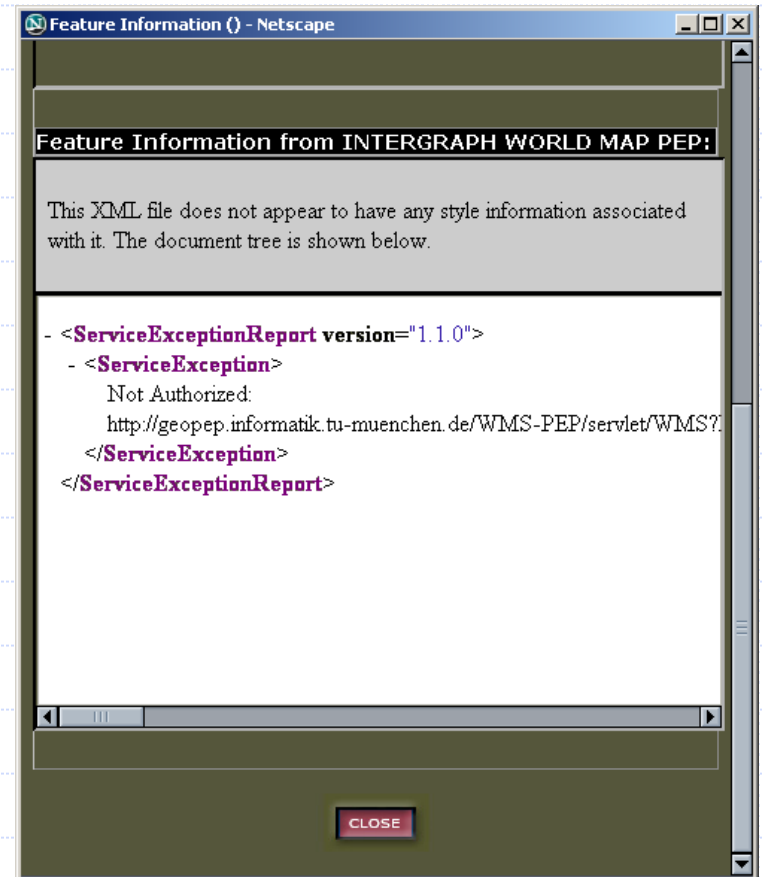
Capitals (red symbols) are present

Read Request for Capitals in Europe

Berlin is permitted



Moscow is denied



Conclusion

- ◆ **Assumption:** Spatial Data Infrastructure exists
- ◆ **Issue 1:** Restrict access to geodata
- ◆ **Issue 2:** Combined use of restricted geodata is to be achieved

- ◆ **A possible solution is introduced in 05-036**
 - Extend SDI by **SSO-Authentication, Enforcement and Authorization** has impact on architecture!
 - GeoXACML = XACML + spatial functions + geometry attributes

The Final Slide

Thank you very much for the attention

Questions, please...

Dr. Andreas Matheus

University of the Federal Armed Forces Munich

andreas.matheus@unibw.de