

# Location Based Access Control on Geospatial Data with GeoXACML policies

Topic: Workshop proposal for COM.Geo 2013

Authors: Andreas Matheus

---

## Introduction

Many different types of high quality and up-to-date geospatial information are available from different providers. Often, Intranet solutions exist where trusted users can access information with very few access constraints. In contrast, making information available to users outside of a trusted environment requires the implementation of many security requirements of which Access Control is paramount.

## Challenge

When implementing access control systems, a challenge exists in enabling access rights that are highly dependent on many different things. Therefore, it is usually a good idea to separate the implementation and the configuration of the access control system. This allows the use of mature software that can be configured to enforce specific access rights.

## About the workshop

This workshop is divided in two parts:

1. The theoretical base of the GeoXACML Policy Language:  
GeoXACML is the OGC standard language aimed specifically at declaring and enforcing geo-specific access rights, which protect access to geospatial data or services. This workshop will introduce GeoXACML and will illustrate how to write GeoXACML Policies for OGC WMS and WFS services.
2. The practical portion of the workshop will provide attendees an environment for hands-on exercises to experiment writing GeoXACML policies and testing them in a demo environment.

## Workshop Agenda

09:00 – 09:15	Speaker and audience intro
09:15 – 10:00	Brief introduction to security requirements and standards including GeoXACML
10:00 – 10:15	“Cross Border” Use – Full system integration demo focusing on Access Control
10:15 – 11:15	Hands-On session
11:15 – 11:45	Use Case “Fire at the airport” walk-through
11:45 – 12:00	Wrap-up

## Brief introduction to security requirements and standards

Requirements are

- Authentication
- Access Control
- Integrity
- Confidentiality
- Availability
- Authenticity
- (Non-Repudiation)

Available standards for implementing the requirements:

Federation	WS-Federation	WS-SecureConversation		Authentication
Licensing	REL	ODRL	XrML	
Authorization		XACML	GeoXACML	
Policy Layer	WS-Policy	WS-Trust	WS-Authorization	
Message Security		WS-Security		
Web Services Standards	WSDL	WS-Referral	WS-Routing	
XML Security Standards	XML Signature	XML Encryption	SAML	
		XKMS	ebXML	
Binding Layer		HTTP / HTTPS		PKI
Network Layer	SSL	TLS	IPSec	
				Kerberos
				LDAP
				XCBF

## GeoXACML introduction

## Cross Border Use Case

## Hands-On session

Class has to be given a set of ADRs and what the response is going to be (PERMIT or DENY). We also need to have a Policy

(1) The simple WMS lesson (example from GeoXACML standard)

