

Open Geospatial Consortium Inc.

Date: 2007-03-22

Reference number of this OGC® project document: **OGC 07-026**

Version: 0.3.0

Category: OGC® Implementation Specification

Editor: Andreas Matheus

Geospatial eXtensible Access Control Markup Language (GeoXACML)

Document type: OGC® Publicly Available Standard
Document subtype: if applicable
Document stage: Draft
Document language: English

Copyright notice

Copyright © 2007 Open Geospatial Consortium, Inc. All Rights Reserved.
To obtain additional rights of use, visit <http://www.opengeospatial.org/legal/>.

Warning

This document is not an OGC Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an OGC Standard.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Contents

1	Scope.....	1
2	Conformance	1
3	Normative references.....	2
4	Terms and definitions	3
4.1	XACML terms and definitions	3
4.2	GML terms and definitions (from GML 3.1.1)	5
4.2	Topological relations terms and definitions	5
5	Conventions	7
5.1	Symbols (and abbreviated terms).....	7
5.2	UML Notation	7
6	Brief Introduction to XACML (informative).....	9
6.1	Policy Language Model and Authorization.....	9
6.2	Information Flow Model	11
6.3	Extension capabilities of XACML.....	12
6.3.1	Defining new <AttributeValue> Types using the extension based on DataType.....	12
6.3.2	Defining new <Function> Types using the extension based on FunctionId	13
6.3.3	Defining new <AttributeDesignatorTypes> using the extension based on AttributeId.....	13
7	GeoXACML (normative)	14
7.2	Geometry type <AttributeValue>.....	14
7.2	Test functions for topological relations.....	14
7.3	OpenGIS Web Services specific ResourceAttributeDesignator	15
7.4	CRS-specific ResourceAttributeDesignator	16
A.1	Service-Id <ResourceAttributeDesignator >	17
A.2	Service-Id <ResourceAttributeDesignator >	17
A.3	CRS <ResourceAttributeDesignator >.....	17
B.1	Point Geometry Attribute Value	18
B.2	Function	18
B.3	Condition	18
B.4	GeoXACML Policy Example.....	19

i. Preface

The Policy Language introduced in this document defines a geo-specific extension to the XACML Policy Language, as defined by the OASIS standard “eXtensible Access Control Markup Language (XACML), Version 2.0” [1].

Attention is drawn to the point that this document defines a Policy Language in the context of access control and not a Rights Expression Language, typically used to enforce usage rights in the context of Digital Rights Management.

In that sense, this specification is not meant to be an implementation specification in regard to the GeoDRM RM, as released by the OGC as “The OpenGIS® Abstract Specification Topic 18: Geospatial Digital Rights Management Reference Model (GeoDRM RM)” [9]. However, this geo-specific extension to the existing OASIS standard can be seen as the baseline for the development of an implementation specification in the context of [9].

ii. Submitting organizations

The following organizations submitted this Implementation Specification to the Open Geospatial Consortium Inc. as a Request For Comment (RFC):

Universität der Bundeswehr München

Andreas Matheus
Werner-Heisenberg-Weg 39
D-85579 Neubiberg
Germany
andreas.matheus@unibw.de

Galdos Systems Inc.

Ron Lake
1300-409 Granville St
Vancouver V6C 1T2
Canada
rlake@galdosinc.com

iii. Submission contact points

All questions regarding this submission should be directed to the editor or the submitters:

CONTACT	COMPANY	EMAIL
Andreas Matheus	Universität der Bundeswehr München	Andreas.Matheus@unibw.de
Ron Lake	Galdos Systems Inc.	rlake@galdosinc.com

iv. Revision history

Date	Release	Author	Paragraph modified	Description
2007-01-22	0.1.0	Andreas Matheus	All	Initial Writing
2007-02-28	0.2.0	Andreas Matheus	All	Formatting
2007-03-19	0.3.0	Michael Mendonca	All	GML corrections

v. Changes to the OGC® Abstract Specification

The OpenGIS® Abstract Specification does not require changes to accommodate this standard.

Even though this document does not require the change of OGC specifications, it has influence to the OpenGIS® Web Service Common Implementation Specification [2], because GeoXACML can be used to establish an Access Control Mechanism to protect the access to OpenGIS Web Services. In that sense, a OWS can reply with exceptions, currently not defined in [2].

A Change Request to [2] shall be developed to specify exceptions, relevant in term of Access Control.

Foreword

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. Open Geospatial Consortium Inc. shall not be held responsible for identifying any or all such patent rights. However, to date, no such rights have been claimed or identified.

This document is not comprehensive by itself, because it defines an extension to an existing OASIS standard, as defined in [1]: “eXtensible Access Control Markup Language (XACML)”. It is therefore mandatory to use this document ONLY together with [1].

Normative Annexes: Annex A

Informative Annexes: Annex B

Please note that all definitions taken from other specifications are shaded in 5% grey.

Introduction

Even though geographic information is often available for free, it might not always be unprotected. Requirements might come from the law, which requires a managed access to geographic information, independent from commercial aspects. However, commercial aspects might bring relevant requirements for protection as well.

In contrast to a „persistent protection mechanism” as it is defined by GeoDRM-RM to be a mechanism that “*remains in force regardless of where the content of the original resource is located or reproduced*” (p. 25, [9]), an Access Control System allows to manage access to information, until it is obtained by the user and stored locally on her computer. Thinking of a service oriented Spatial Data Infrastructure, a GeoDRM System would manage the access at (i) the time the user accesses the geographic information on the service and (ii) the time afterwards, when the geographic information is stored somewhere else. The limitations of an Access Control System are such that access can only be controlled at the time the user initiates a request to the service. After the (geographic) information has left the service, it is out of control and can not be managed any longer.

However there is this distinctive difference between a (Geo)DRM and an Access Control System, requirements exist where the establishment of an Access Control System is sufficient.

The eXtensible Access Control Markup Language (XACML), as defined in the OASIS standard [1], allows establishing an Access Control System which can be used to manage access for Service Oriented Architectures. In that sense, it can be used with limitations to protect geographic information by the declaration of rights through the specified Policy Language. The limitations are based on the fact, that XACML does not have the capabilities to express geo-specific constraints on access rights, as it is relevant for managing access to geographic information.

This document defines the Geospatial eXtensible Access Control Markup Language (GeoXACML) as a geo-specific extension to the existing XACML Policy Language as defined [1] that allows managing access to geographic information.

OpenGIS® Geospatial eXtensible Access Control Markup Language (GeoXACML) Implementation Specification – Version 1.0

1 Scope

The Geospatial eXtensible Access Control Markup Language (GeoXACML) defines an XML encoding extension to the XACML Policy Language that supports the declaration and enforcement of access restrictions on geographic information. GeoXACML is a geospatial extension to the XACML Policy Language, an OASIS standard, defined in [1].

The extension to XACML is based on the extensibility points, as they are introduced in section 8 (p. 89, [1]). GeoXACML defines

- geometry Attribute Values,
- testing functions for topological relationship between geometries and
- OpenGIS Web Service and CRS-specific specific Resource Attribute Designators.

2 Conformance

GeoXACML defines a Policy Language that is schema compliant to the eXtensible Access Control Markup Language (XACML), version 2.0 [1]. Therefore, modifications of the XACML schemata are NOT required.

The XACML Policy Language is defined in the following namespace:

`urn:oasis:names:tc:xacml:1.0:policy`

The GeoXACML extension is defined in the following namespace:

`urn:ogc:def:geoxacml:1.0:function` and `urn:ogc:def:geoxacml:1.0:resource`

Please see normative Annex A.

3 Normative references

- [1] OASIS, *eXtensible Access Control Markup Language (XACML) Version 2.0*, 1 Feb 2005, http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf
- [2] OGC, OpenGIS® Web Service Common Implementation Specification, Version 1.0.0, 2005-11-22, http://portal.opengeospatial.org/files/?artifact_id=8798
- [3] OGC, *OpenGIS® Geography Markup Language(GML) Implementation Specification, Version 3.1.1*, 2004-02-07, http://portal.opengeospatial.org/files/?artifact_id=4700
- [4] OGC, *Open GIS Consortium Inc.: OpenGIS Simple Features Specification For SQL, Revision 1.1*, Release Date: May 5, 1999 (deprecated), http://portal.opengeospatial.org/files/?artifact_id=829

4 Terms and definitions

For the purposes of this document, the following terms and definitions apply. Please note that terms and definition taken from other specifications are shaded 5% grey.

Section 4.1 lists the terms and definitions from [1], section 4.2 from [3] and section 4.3 from [4].

4.1 XACML terms and definitions

Access - Performing an action

Access control - Controlling access in accordance with a policy

Action - An operation on a resource

Applicable policy - The set of policies and policy sets that governs access for a specific decision request

Attribute - Characteristic of a subject, resource, action or environment that may be referenced in a predicate or target (see also – named attribute)

Authorization decision - The result of evaluating applicable policy, returned by the PDP to the PEP. A function that evaluates to “Permit”, “Deny”, “Indeterminate” or “NotApplicable”, and (optionally) a set of obligations

Bag – An unordered collection of values, in which there may be duplicate values

Condition - An expression of predicates. A function that evaluates to "True", "False" or “Indeterminate”

Conjunctive sequence - a sequence of predicates combined using the logical ‘AND’ operation

Context - The canonical representation of a decision request and an authorization decision

Context handler - The system entity that converts decision requests in the native request format to the XACML canonical form and converts authorization decisions in the XACML canonical form to the native response format

Decision – The result of evaluating a rule, policy or policy set

Decision request - The request by a PEP to a PDP to render an authorization decision

Disjunctive sequence - a sequence of predicates combined using the logical ‘OR’ operation

Effect - The intended consequence of a satisfied rule (either "Permit" or "Deny")

Environment - The set of attributes that are relevant to an authorization decision and are independent of a particular subject, resource or action

Named attribute – A specific instance of an attribute, determined by the attribute name and type, the identity of the attribute holder (which may be of type: subject, resource, action or environment) and (optionally) the identity of the issuing authority

Obligation - An operation specified in a policy or policy set that should be performed by the PEP in conjunction with the enforcement of an authorization decision

Policy - A set of rules, an identifier for the rule-combining algorithm and (optionally) a set of obligations. May be a component of a policy set

Policy administration point (PAP) - The system entity that creates a policy or policy set

Policy-combining algorithm - The procedure for combining the decision and obligations from multiple policies

Policy decision point (PDP) - The system entity that evaluates applicable policy and renders an authorization decision. This term is defined in a joint effort by the IETF Policy Framework Working Group and the Distributed Management Task Force (DMTF)/Common Information Model (CIM) in [RFC3198]. This term corresponds to "Access Decision Function" (ADF) in [ISO10181-3].

Policy enforcement point (PEP) - The system entity that performs access control, by making decision requests and enforcing authorization decisions. This term is defined in a joint effort by the IETF Policy Framework Working Group and the Distributed Management Task Force (DMTF)/Common Information Model (CIM) in [RFC3198]. This term corresponds to "Access Enforcement Function" (AEF) in [ISO10181-3].

Policy information point (PIP) - The system entity that acts as a source of attribute values

Policy set - A set of policies, other policy sets, a policy-combining algorithm and (optionally) a set of obligations. May be a component of another policy set

Predicate - A statement about attributes whose truth can be evaluated

Resource - Data, service or system component

Rule - A target, an effect and a condition. A component of a policy

Rule-combining algorithm - The procedure for combining decisions from multiple rules

Subject - An actor whose attributes may be referenced by a predicate

Target - The set of decision requests, identified by definitions for resource, subject and action, that a rule, policy or policy set is intended to evaluate

Type Unification - The method by which two type expressions are "unified". The type expressions are matched along their structure. Where a type variable appears in one expression it is then "unified" to represent the corresponding structure element of the other expression, be it another variable or subexpression. All variable assignments must remain consistent in both structures. Unification fails if the two expressions cannot be aligned, either by having dissimilar structure, or by having instance conflicts, such as a variable needs to represent both "xs:string" and "xs:integer". For a full explanation of type unification, please see [Hancock].

4.2 GML terms and definitions (from GML 3.1.1)

Point - 0-dimensional geometric primitive, representing a position [ISO 19107].

LineString - A LineString is a special curve that consists of a single segment with linear interpolation. It is defined by two or more coordinate tuples, with linear interpolation between them. It is backwards compatible with the LineString of GML 2.

LinearRing - A LinearRing is defined by four or more coordinate tuples, with linear interpolation between them; the first and last coordinates shall be coincident.

Box – Envelope defines an extent using a pair of positions defining opposite corners in arbitrary dimensions. The first direct position is the "lower corner" (a coordinate position consisting of all the minimal ordinates for each dimension for all points within the envelope), the second one the "upper corner" (a coordinate position consisting of all the maximal ordinates for each dimension for all points within the envelope). [Deprecated with GML 3.0]

Polygon - A planar surface defined by 1 exterior boundary and 0 or more interior boundaries

MultiPoint - A MultiPoint is defined by one or more Points, referenced through pointMember elements.

MultiLineString - A MultiLineString is defined by one or more LineStrings, referenced through lineStringMember elements. [Deprecated with GML 3.0 – Use MultiCurve].

MultiPolygon - A MultiPolygon is defined by one or more Polygons, referenced through polygonMember elements. [Deprecated with GML 3.0]

4.2 Topological relations terms and definitions

Based on *OpenGIS Simple Features Specification For SQL* (see [4]), the following definitions are relevant:

Disjoint

Given two (topologically closed) geometries a and b,

$$a.\text{Disjoint}(b) \Leftrightarrow a \cap b = \emptyset$$

Touches

The Touches relation between two geometries a and b applies to the A/A, L/L, L/A, P/A and P/L groups of relationships but not to the P/P group. It is defined as:

$$a.\text{Touches}(b) \Leftrightarrow (I(a) \cap I(b) = \emptyset) \wedge (a \cap b) \neq \emptyset$$

Crosses

The Crosses relation applies to P/L, P/A, L/L and L/A situations. It is defined as:

$$a.\text{Crosses}(b) \Leftrightarrow (\dim(I(a) \cap I(b)) < \max(\dim(I(a)), \dim(I(b)))) \wedge (a \cap b \neq \emptyset) \wedge (a \cap b \neq b)$$

Within

The Within relation is defined as:

$$a.\text{Within}(b) \Leftrightarrow (a \cap b = a) \wedge (I(a) \cap I(b) \neq \emptyset)$$

Contains

$$a.\text{Contains}(b) \Leftrightarrow b.\text{Within}(a)$$

Overlaps

The Overlaps relation is defined for A/A, L/L and P/P situations. It is defined as:

$$a.\text{Overlaps}(b) \Leftrightarrow (\dim(I(a)) = \dim(I(b)) = \dim(I(a) \cap I(b))) \wedge (a \cap b \neq a) \wedge (a \cap b \neq b)$$

Intersects

$$a.\text{Intersects}(b) \Leftrightarrow ! a.\text{Disjoint}(b)$$

5 Conventions

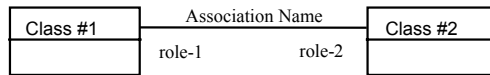
5.1 Symbols (and abbreviated terms)

PAP	Policy Administration Point
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PIP	Policy Information Point
GML	Geography Markup Language
ISO	International Organization for Standardization
OGC	Open Geospatial Consortium
UML	Unified Modeling Language
XML	eXtended Markup Language
1D	One Dimensional
2D	Two Dimensional
3D	Three Dimensional
SAML	Security Assertion Markup Language
XACML	eXtensible Access Control Markup Language
GeoXACML	Geospatial eXtensible Access Control Markup Language

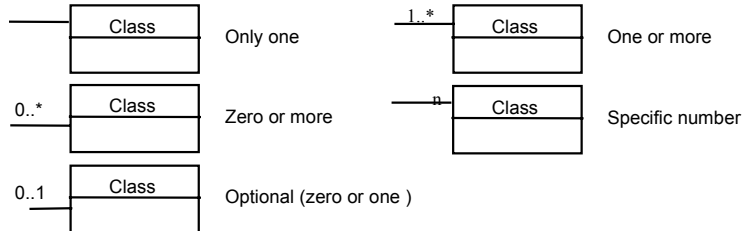
5.2 UML Notation

The diagrams that appear in this standard are presented using the Unified Modeling Language (UML) static structure diagram. The UML notations used in this standard are described in the diagram below.

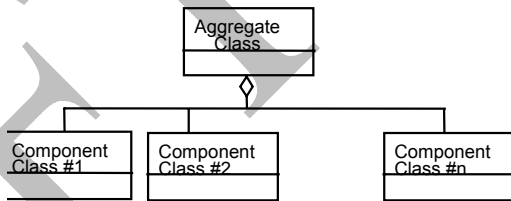
Association between classes



Association Cardinality



Aggregation between classes



Class Inheritance (subtyping of classes)

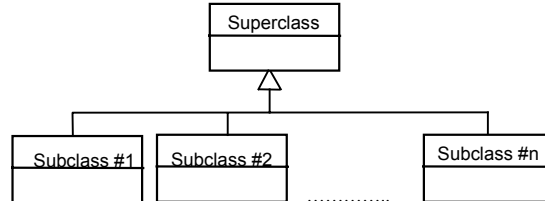


Figure 1 — UML notation

6 Brief Introduction to XACML (informative)

It is the intension of this chapter to give a brief informative introduction of XACML as defined in [1], before GeoXACML is defined in the next chapter.

A short primer on XACML is available as a Technology Report at the Cover Pages; see [7] for more information.

The XACML standard can be separated into two main sections, which are introduced in more detail in the following sections: (i) Policy Language and Authorization Model and (ii) Information Flow Model.

6.1 Policy Language Model and Authorization

The XACML Policy Language Model defines an XML encoding for expressing general purpose access restrictions and extension points to define your own Attribute Values, Functions, etc. The entire set of access restrictions defines an XACML Policy. The Policy is structured, according to the following UML diagram.

The top level element is the <PolicySet>. It can host zero or more <PolicySet> elements, which can be included inline or by reference. This powerful feature allows the reuse of pre-defined policy segments as well as the integration of multiple policies.

Each <PolicySet> element can host one or more <Policy> elements, which is the container for a set of <Rule> elements. Inside the <Rule> element, conditions can be formed to express complex access restrictions, using the <Condition> element.

Each <PolicySet>, <Policy> and <Rule> element have a <Target> element, which can be used to define simple matching conditions for the Subject, Action, Resource and Environment. This allows the effective structuring of a policy into sub-trees, which eases the maintenance of rights defined in a policy. On the other hand, the simple matching in a <Target> element ensures a fast decision making, when it comes to deriving an authorization decision.

The flexible matching of Subjects in the <Target> element supports direct association of access rights to subjects or roles, as defined in the RBAC profile of XACML (“Core and hierarchical role based access control (RBAC) profile of XACML v2.0”, [5]).

In order to derive an authorization decision for a given (XACML authorization decision) request, the XACML policy is traversed from the top (<PolicySet> element) to the leaves (<Rule> elements). For all matching <Rule> elements, their Effect (Permit or Deny) is taken as the most basic driver for the authorization decision. By traversing up the policy the effects of all Rules – accociated to a <Policy> element are combined using the RuleCombiningAlgorithm, which is an attribute of the <Policy> element. The resulting effects of all <Policy> elements are matched on the next level, until at the top

<PolicySet> element, the PolicyCombiningAlgorithm creates the final effect of the entire policy, which represents the authorization decision.

The XACML Policy Language defines four different results for the authorization decision: (i) Permit, (ii) Deny, (iii) Indeterminate and (iv) NotApplicable. Finally, the process of deriving an authorization decision can result in an error, which is documented as additional information in the <Decision> element.

In addition, the decision can be “Permit with Obligation”, which can be expressed in the <Obligation> element, which is attached to the <Policy> or <PolicySet> element.

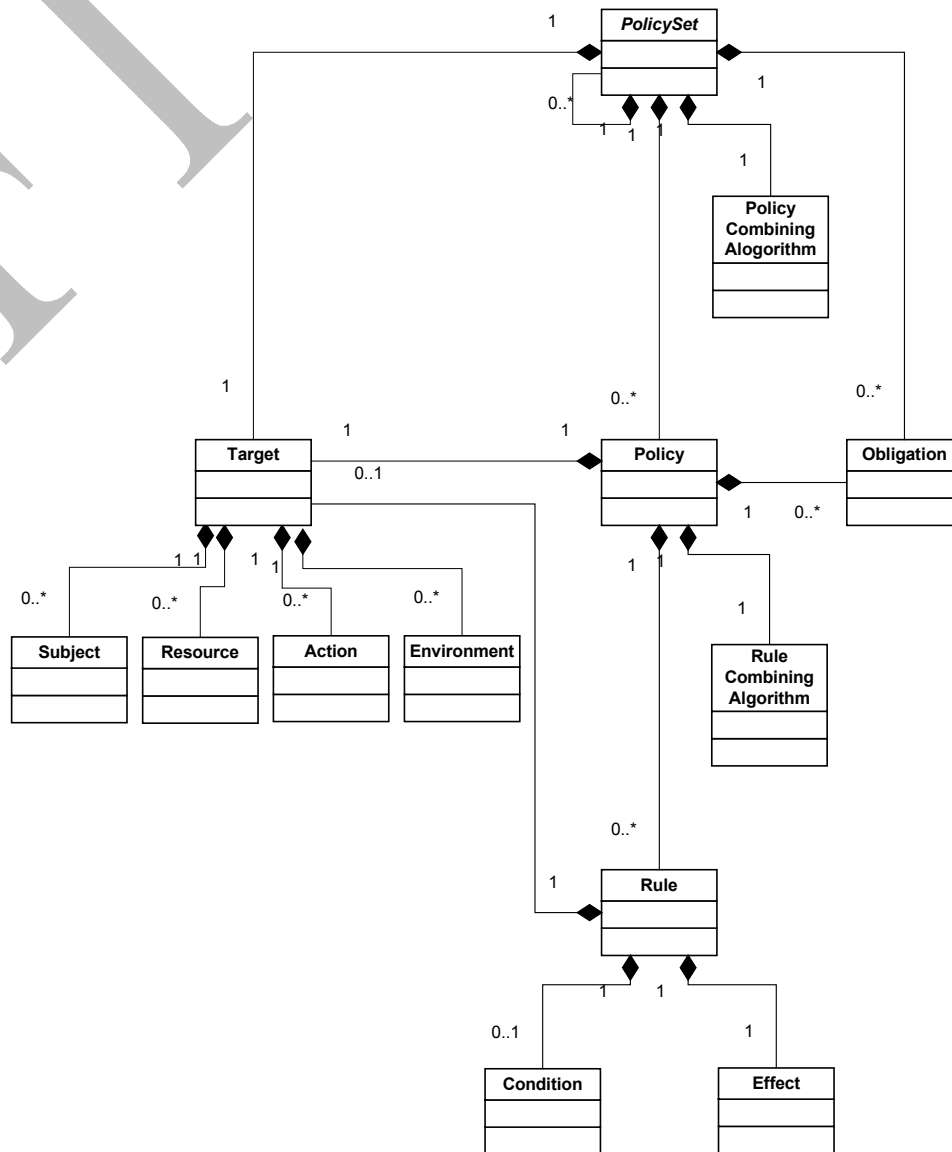


Figure 2 — XACML Policy Language Model

6.2 Information Flow Model

The XACML Information Flow Model defines the architecture of a modular and distributed access control system. In addition, it defines the exchange of messages between the components and the structure of the messages. The following figure illustrates the informative architecture and the sequence of messages, sent between the components of the access control system.

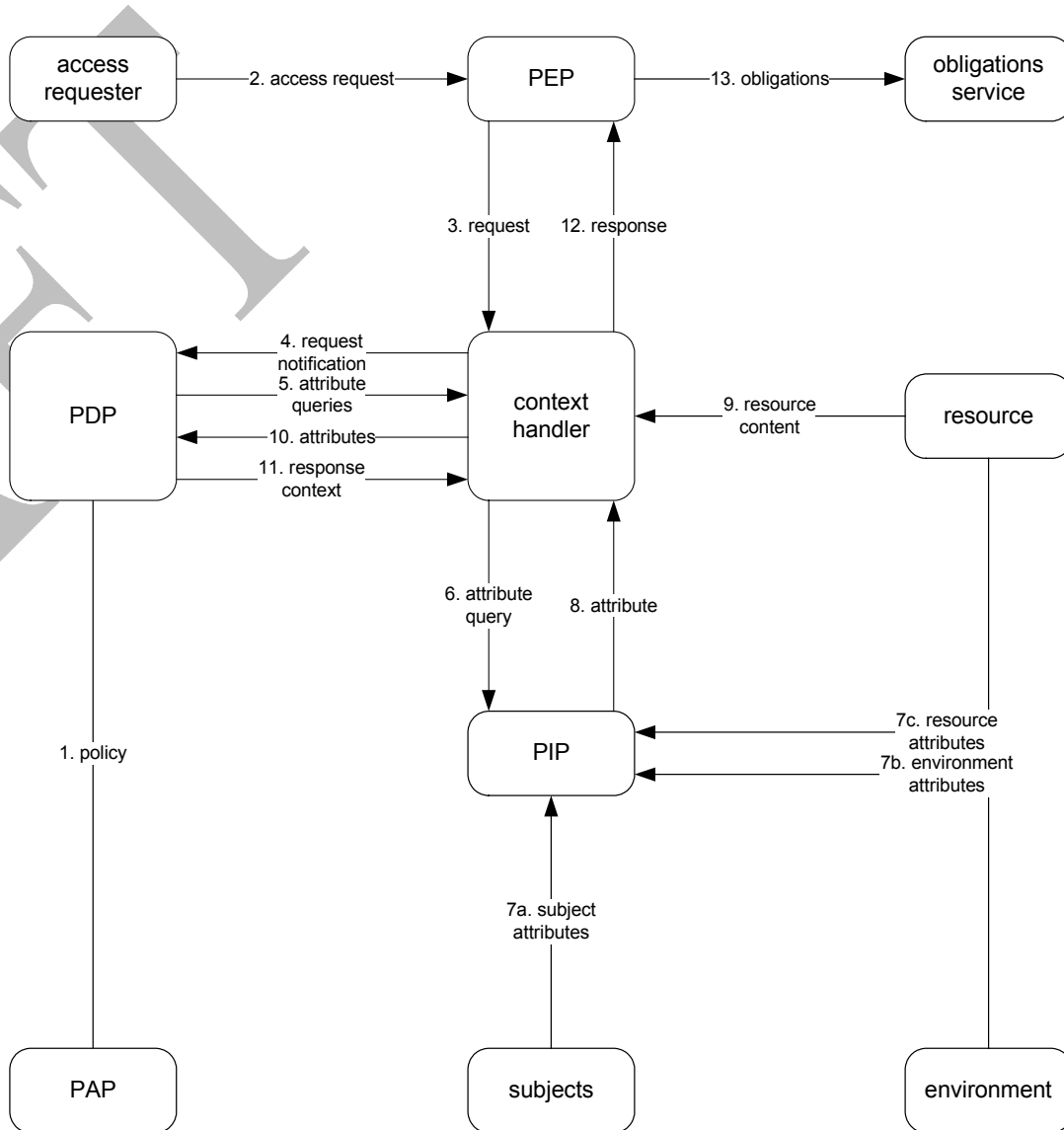


Figure 3 — XACML Information Flow Model

The Policy Administration Point (PAP) is the component that allows one or multiple policy administrators to maintain access rights in a set of policies. In addition, the PAP might provide an interface for requesting policies, as it is defined in the “SAML 2.0 profile of XACML v2.0” of XACML (see [6]).

The Policy Decision Point (PDP) is the component that derives an authorization decision based on a request, received from one or multiple Policy Enforcement Point(s) (PEP). A PDP may request policies from the PAP or use a policy repository on file or in a database.

The Policy Enforcement Point (PEP) can be characterized as a binary switch that either forwards the intercepted request from the client to the service or replies with an adequate error message. The decision if the request is to be forwarded or blocked depends on the authorization decisions, received from the PDP. Because the PEP must request authorization decision in a particular XACML message format, it is the duty of the context handler to collect all relevant information and prepare the authorization decision request message. The information, collected by the context handler can include the identity information about the user, the action to be taken on the resource, information about the resource itself, the IP address of the client, the time of the request, certificate information, etc. In order to collect all relevant information about the user’s identity, it can be required to request such information from the Policy Information Point (PIP).

6.3 Extension capabilities of XACML

The XACML Specification defines the non-normative extensibility points (section 8, [1]). For this specification, it is important to note that the `DataType`, `FunctionId` and `AttributeId` can be extended.

Please see the XACML schema definitions in `access_control-xacml-2.0-policy-schema-os.xsd` for the XML format of the elements.

6.3.1 Defining new `<AttributeValue>` Types using the extension based on `DataType`

A `<AttributeValue>` element has an attribute named `DataType`, which is of type `xs:anyURI`. According to the extension capabilities of XACML, additional attribute values can be defined by associating a unique data type identifier to it.

Section 8.2 of the XACML specification states that a “`<xacml:AttributeValue>` and `<xacml-context:AttributeValue>` elements MAY contain an instance of a structured XML data-type.”. This capability allows the definition of geometry data types, as described in section 7.1.

```
<xs:element name="AttributeValue" type="xacml:AttributeValueType"
substitutionGroup="xacml:Expression"/>
  <xs:complexType name="AttributeValueType" mixed="true">
    <xs:complexContent mixed="true">
      <xs:extension base="xacml:ExpressionType">
        <xs:sequence>
```

```

        <xs:any namespace="##any" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="DataType" type="xs:anyURI" use="required"/>
    <xs:anyAttribute namespace="##any" processContents="lax"/>
</xs:extension>
</xs:complexContent>
</xs:complexType>

```

Figure 4 — XACML schema definition of the <AttributeValue> element

6.3.2 Defining new <Function> Types using the extension based on FunctionId

A <Function> element has an attribute named FunctionID, which is of type xs:anyURI. According to the extension capabilities of XACML, additional functions can be defined by associating a unique FunctionId to it.

The GeoXACML specific function URNs are defined in section 7.2.

```

<xs:element name="Function" type="xacml:FunctionType"/>
<xs:complexType name="FunctionType">
    <xs:attribute name="FunctionId" type="xs:anyURI" use="required"/>
</xs:complexType>

```

Figure 5 — XACML schema definition of the <Function> element

6.3.3 Defining new <AttributeDesignatorTypes> using the extension based on AttributeId

An <AttributeDesignatorType> element has an attribute named AttributeId, which is of type xs:anyURI. According to the extension capabilities of XACML, additional designators can be defined by associating a unique AttributeId to it.

The GeoXACML specific attribute designator URNs are defined in section 7.2.

```

<xs:complexType name="AttributeDesignatorType">
    <xs:complexContent>
        <xs:extension base="xacml:ExpressionType">
            <xs:attribute name="AttributeId" type="xs:anyURI"
use="required"/>
            <xs:attribute name="DataType" type="xs:anyURI" use="required"/>
            <xs:attribute name="Issuer" type="xs:string" use="optional"/>
            <xs:attribute name="MustBePresent" type="xs:boolean"
use="optional" default="false"/>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>

```

Figure 5 — XACML schema definition of the <AttributeDesignatorType> element

7 GeoXACML (normative)

GeoXACML uses the same Policy Language as XACML does. However, a GeoXACML Policy may include specific Attribute Value Elements and Condition Functions, which are defined in GeoXACML only. Therefore a PDP, supporting GeoXACML Policies is capable to also perform authorization decisions on XACML policies; the opposite is not true.

7.2 Geometry type <AttributeValue>

In order to define geometry attribute values, GeoXACML defines the following URNs.

URN	GML Geometry Type	Required ¹⁾
http://www.opengis.net/gml#Point	Point	M
http://www.opengis.net/gml#LineString	LineString	M
http://www.opengis.net/gml#LienarRing	LienarRing	M
http://www.opengis.net/gml#Box	Box [Deprecated with GML 3.0]	M
http://www.opengis.net/gml#Polygon	Polygon	M
http://www.opengis.net/gml#MultiPoint	MultiPoint	O
http://www.opengis.net/gml#MultiLineString	MultiLineString [Deprecated with GML 3.0]	O
http://www.opengis.net/gml#MultiPolygon	MultiPolygon [Deprecated with GML 3.0]	O

¹⁾ M = Mandatory, O = Optional

Table 1 — Geometry type URNs

7.2 Test functions for topological relations

In order to define functions for testing topological relations, GeoXACML defines the following URNs.

URN	Test Function	Required ¹⁾
urn:ogc:def:geoxacml:1.0:function:Disjoint	Disjoint	M
urn:ogc:def:geoxacml:1.0:function:Touces	Touces	M
urn:ogc:def:geoxacml:1.0:function:Crosses	Crosses	M
urn:ogc:def:geoxacml:1.0:function:Within	Within	M
urn:ogc:def:geoxacml:1.0:function:Contains	Contains	M
urn:ogc:def:geoxacml:1.0:function:Overlaps	Overlaps	M
urn:ogc:def:geoxacml:1.0:function:Intersects	Intersects	M
urn:ogc:def:geoxacml:1.0:function:Equals	Equals	M
1) M = Mandatory, O = Optional		

Table 2 — Topological Test Functions

7.3 OpenGIS Web Services specific ResourceAttributeDesignator

In order to protect access to OpenGIS Web Services, it is practicable to allow unique definition of the service and its operation that is to be protected. For this purpose this specification defines two optional ResourceAttributeDesignator elements: Service-Id and Operation-Id.

The Service-Id <ResourceAttributeDesignator > is of type URI and can keep the URL of the service.

The Operation-Id <ResourceAttributeDesignator > is of type URI and defines the operation of the service.

URN	Type	Required ¹⁾
urn:ogc:def:geoxacml:1.0:resource:Service-Id	http://www.w3.org/2001/XMLSchema#anyURI	O
urn:ogc:def:geoxacml:1.0:resource:Operation-Id	http://www.w3.org/2001/XMLSchema# string	O
1) M = Mandatory, O = Optional		

Table 3 — OpenGIS Web Service specific <ResourceAttributeDesignator >

See Annex A for the normative definition of the XML encoding.

7.4 CRS-specific ResourceAttributeDesignator

In order to allow sufficient structuring of access rights, applicable to a specific Coordinate Reference Systems, GeoXACML defines an optional CRS Resource Attribute Descignator. This allows the policy administrator to maintain the same access rights for a OpenGIS Web Service that supports different CRSs by defining an early matching in the <Target> element vs. a late matching by a complex <Condition>.

Please see Annex B for informative examples.

URN	Type	Required ¹⁾
urn:ogc:def:geoxacml:1.0:resource:CRS	http://www.w3.org/2001/XMLSchema#string	O
1) M = Mandatory, O = Optional		

Table 4 — Geo-specific <ResourceAttributeDesignator >

See Annex A for the normative definition of the XML encoding.

Annex A (normative)

GeoXACML ResourceAttributeDesignators

A.1 Service-Id <ResourceAttributeDesignator >

```
<ResourceAttributeDesignator
  xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:policy:schema:os
  access_control-xacml-2.0-policy-schema-os.xsd"
  DataType="http://www.w3.org/2001/XMLSchema#anyURI"
  AttributeId="urn:ogc:def:geoxacml:1.0:resource:Service-Id"/>
```

Figure A.1 — Service-Id <ResourceAttributeDesignator >

A.2 Service-Id <ResourceAttributeDesignator >

```
<ResourceAttributeDesignator
  xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:policy:schema:os
  access_control-xacml-2.0-policy-schema-os.xsd"
  DataType="http://www.w3.org/2001/XMLSchema#string"
  AttributeId="urn:ogc:def:geoxacml:1.0:resource:Operation-Id"/>
```

Figure A.2 — Operation-Id <ResourceAttributeDesignator >

A.3 CRS <ResourceAttributeDesignator >

```
<ResourceAttributeDesignator
  xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:policy:schema:os
  access_control-xacml-2.0-policy-schema-os.xsd"
  DataType="http://www.w3.org/2001/XMLSchema#string"
  AttributeId="urn:ogc:def:geoxacml:1.0:resource:CRS"/>
```

Figure A.3 — CRS <ResourceAttributeDesignator >

Annex B (informative)

GeoXACML Policy Language Examples

B.1 Point Geometry Attribute Value

```
<AttributeValue DataType="http://www.opengis.net/gml#point">
  <gml:Point srsName="urn:ogc:def:crs:EPSG:6.6:4326">
    <gml:pos>45.256 -110.45</gml:pos>
  </gml:Point>
</AttributeValue>
```

Figure B.1 — GeoXACML Point <AttributeValue> Example

B.2 Function

```
<Function FunctionId="urn:ogc:def:geoxacml:1.0:function:within"/>
```

Figure B.2 — GeoXACML <Function> Example

B.3 Condition

```
<Condition FunctionId="urn:oasis:names:tc:xacml:1.0:function:all-of">
  <Function FunctionId="urn:ogc:def:geoxacml:1.0:function:within"/>
  <AttributeValue DataType="http://www.opengis.net/gml#polygon">
    <gml:Polygon gid="P2" srsName="urn:ogc:def:crs:EPSG:6.6:4326">
      <gml:exterior>
        <gml:LinearRing>
          <gml:posList dimension="2">
            -71.41904237001775 42.013443082283366
            -73.509831421403 42.035451388087424
            -74.76430485223416 41.3752022139658
            -75.18246266251121 40.692944734040125
            -74.78631315803823 40.120728783134716
            -70.9568679481326 40.05470386572255
            -71.11092608876098 41.52926035459418
            -71.41904237001775 42.013443082283366
            -71.41904237001775 42.013443082283366
            -71.41904237001775 42.013443082283366
          </gml:posList>
        </gml:LinearRing>
      </gml:exterior>
    </gml:Polygon>
  </AttributeValue>
  <AttributeSelector DataType="http://www.opengis.net/gml#box
    MustBePresent="false" RequestContextPath="//ogc:BBOX/gml:Box"/>
</Condition>
```

Figure B.3 — GeoXACML Condition Example

B.4 GeoXACML Policy Example

The following access rights on MS3D Data are in place for the OWS-4 GeoDRM demo, provided by the Universität der Bundeswehr München and is available under the following URL: <http://iisdemo.informatik.unibw-muenchen.de/ows4/Authorization/Documentation/Demo%20Access%20Restrictions%20for%20MSD3%20Data.htm>

Access Restrictions for the OWS-4 Demo Scenario

AnySubject -- These permissions are granted to all subjects

This enables a simple navigation in the data without seeing the airport features

Operation / Action	Feature Type	Area
GetCapabilities	N/A	N/A
DescribeFeatureType	N/A	N/A
GetFeature / GetFeature	ows4:Road_L	N/A
GetFeature / GetFeature	ows4:River_L	N/A

NGA-Officer – Additional permissions

This enables the Analyst to see the airport features

Operation / Action	Feature Type	Area
GetFeature / GetFeature	ows4:Aerodrome_A	N/A
GetFeature / GetFeature	ows4:Helipad_P	N/A
GetFeature / GetFeature	ows4:Taxiway_A	N/A
GetFeature / GetFeature	ows4:Aircraft_Hangar_A	N/A
GetFeature / GetFeature	ows4:Runway_A	N/A
GetFeature / GetFeature	ows4:Apron_A	N/A

This enables the Analyst to create new and update/delete existing features

Operation / Action	Feature Type	Area
Transaction / Insert, Update, Delete	ows4:Helipad_P	N/A
Transaction / Insert, Update, Delete	ows4:Taxiway_A	N/A
Transaction / Insert, Update, Delete	ows4:Runway_A	N/A

Field-Engineer -- Additional permissions

This enables the Analyst to see the airport features

Operation / Action	Feature Type	Area
GetFeature / GetFeature	ows4:Aerodrome_A	N/A
GetFeature / GetFeature	ows4:Helipad_P	N/A
GetFeature / GetFeature	ows4:Taxiway_A	N/A
GetFeature / GetFeature	ows4:Aircraft_Hangar_A	N/A
GetFeature / GetFeature	ows4:Runway_A	N/A
GetFeature / GetFeature	ows4:Apron_A	N/A

This enables the Analyst to create new and update existing features

Operation / Action	Feature Type	Area
Transaction / Insert	ows4:Helipad_P	WITHIN A1 (see figure below)
Transaction / Update	ows4:Helipad_P	N/A
Transaction / Update	ows4:Taxiway_A	N/A
Transaction / Update	ows4:Runway_A	N/A

Geometry based access restrictions

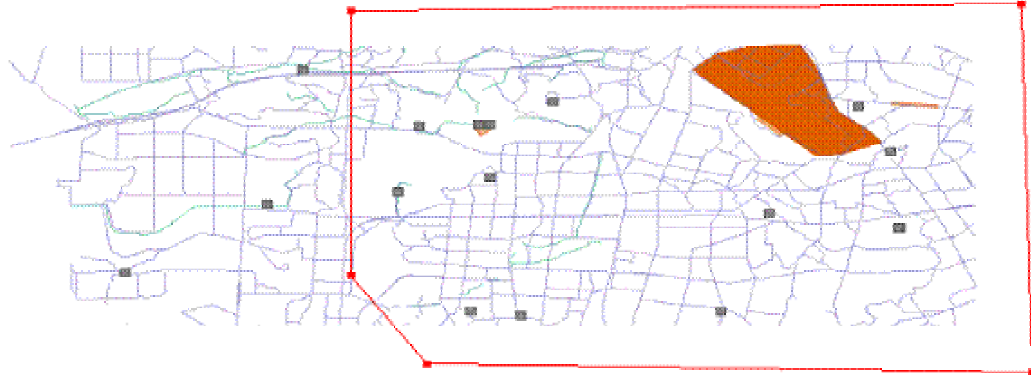


Figure 1: Access Control Area A1 for modification of helipad feature information

(-74.96789132745889, 39.383275615837945), (-74.96789132745889, 39.296675134185634), (-74.94733464747071, 39.268245683138154), (-74.78331858373527, 39.265621426118386), (-74.78638021692498, 39.38546249668775), (-74.96789132745889, 39.383275615837945), (-74.96789132745889, 39.383275615837945), (-74.96789132745889, 39.383275615837945)

Environment

- `<CRS>EPSG:4326</CRS>`
- `<LatLongBoundingBox minx="-75.06011894208314" miny="39.28026350188623" maxx="-74.79843788893288" maxy="39.371523891345134"/>`
- ResourceID: `http://geoserver.itc.nl:8080/geoserver/wfs`

In the following figure is shown the GeoXACML Policy, representing the access rights (as shown above) for the user *Field-Engineer*.

Please note that the GeoXACML namespace for the example policy is `http://www.geoxacml.org`, as it was the actual namespace at the time of OWS-4.


```

<?xml version="1.0" encoding="UTF-8"?>
<PolicySet xmlns="urn:oasis:names:tc:xacml:1.0:policy" xmlns:xacml="urn:oasis:names:tc:xacml:1.0:policy"
xmlns:xacml-context="urn:oasis:names:tc:xacml:1.0:context" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:first-applicable"
PolicySetId="LICENSE_ID_2" xsi:schemaLocation="urn:oasis:names:tc:xacml:1.0:policy cs-xacml-schema-policy-01.xsd">
  <Description>This PolicySet represents the granted rights to Field-Engineer through
LICENSE_ID_2</Description>
  <Target>
    <Subjects>
      <AnySubject/>
    </Subjects>
    <Resources>
      <Resource>
        <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">ID_LICENSE_2</AttributeValue>
          <ResourceAttributeDesignator AttributeId="http://www.geoxacml.org/1.0/resource#license-id"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </ResourceMatch>
      </Resource>
    </Resources>
    <Actions>
      <AnyAction/>
    </Actions>
  </Target>
  <Policy PolicyId="Field-Engineer" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-
algorithm:first-applicable" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <PolicyDefaults>
      <XPathVersion>http://www.w3.org/TR/1999/Rec-xpath-19991116</XPathVersion>
    </PolicyDefaults>
    <Target>
      <Subjects>
        <Subject>
          <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Field-
Engineer</AttributeValue>
            <SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
DataType="http://www.w3.org/2001/XMLSchema#string" SubjectCategory="urn:oasis:names:tc:xacml:1.0:subject-
category:access-subject"/>

```

```

        </SubjectMatch>
    </Subject>
    <Subject>
        <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">CN=Bill Field Engineer,
OU=INF3, O=UniBW, L=Munich, ST=Bavaria, C=DE</AttributeValue>
            <SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
DataType="http://www.w3.org/2001/XMLSchema#string" SubjectCategory="urn:oasis:names:tc:xacml:1.0:subject-
category:access-subject"/>
        </SubjectMatch>
    </Subject>
</Subjects>
<Resources>
    <Resource>
        <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#anyURI">http://geoserver.itc.nl:8080/geoserver/wfs</AttributeValue>
            <ResourceAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
        </ResourceMatch>
    </Resource>
</Resources>
<Actions>
    <AnyAction/>
</Actions>
</Target>
<Rule Effect="Permit" RuleId="rule-2.1">
    <Description>Field-Engineer can request features of type ows4:Aerodrome_A, ows4:Taxiway_A,
ows4:Aircraft_Hangar_A, ows4:Runway_A, ows4:Apron_A</Description>
    <Target>
        <Subjects>
            <AnySubject/>
        </Subjects>
        <Resources>
            <Resource>
                <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:integer-less-than">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#integer">0</AttributeValue>
                    <AttributeSelector DataType="http://www.w3.org/2001/XMLSchema#integer"

```

```

RequestContextPath="count (//wfs:Query[@typeName='ows4:Aerodrome_A']) "/>
  </ResourceMatch>
</Resource>
<Resource>
  <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:integer-less-than">
    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#integer">0</AttributeValue>
    <AttributeSelector DataType="http://www.w3.org/2001/XMLSchema#integer"
RequestContextPath="count (//wfs:Query[@typeName='ows4:Taxiway_A']) "/>
  </ResourceMatch>
</Resource>
<Resource>
  <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:integer-less-than">
    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#integer">0</AttributeValue>
    <AttributeSelector DataType="http://www.w3.org/2001/XMLSchema#integer"
RequestContextPath="count (//wfs:Query[@typeName='ows4:Aircraft_Hangar_A']) "/>
  </ResourceMatch>
</Resource>
<Resource>
  <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:integer-less-than">
    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#integer">0</AttributeValue>
    <AttributeSelector DataType="http://www.w3.org/2001/XMLSchema#integer"
RequestContextPath="count (//wfs:Query[@typeName='ows4:Apron_A']) "/>
  </ResourceMatch>
</Resource>
<Resource>
  <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:integer-less-than">
    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#integer">0</AttributeValue>
    <AttributeSelector DataType="http://www.w3.org/2001/XMLSchema#integer"
RequestContextPath="count (//wfs:Query[@typeName='ows4:Runway_A']) "/>
  </ResourceMatch>
</Resource>
<Resource>
  <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:integer-less-than">
    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#integer">0</AttributeValue>
    <AttributeSelector DataType="http://www.w3.org/2001/XMLSchema#integer"
RequestContextPath="count (//wfs:Query[@typeName='ows4:Administrative_Boundary_L']) "/>
  </ResourceMatch>
</Resource>

```

```

        </Resources>
        <Actions>
          <Action>
            <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue
                DataType="http://www.w3.org/2001/XMLSchema#string">GetFeature</AttributeValue>
              <ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </ActionMatch>
          </Action>
        </Actions>
      </Target>
    </Rule>
    <Rule Effect="Permit" RuleId="rule-2.2">
      <Description>Field-Engineer can request features of type ows4:HeliPad_P2 in the area around the
airport</Description>
      <Target>
        <Subjects>
          <AnySubject/>
        </Subjects>
        <Resources>
          <Resource>
            <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:integer-less-than">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#integer">0</AttributeValue>
              <AttributeSelector DataType="http://www.w3.org/2001/XMLSchema#integer"
                RequestContextPath="count (//wfs:Query[@typeName='ows4:HeliPad_P2'])"/>
            </ResourceMatch>
          </Resource>
        </Resources>
      </Target>
    </Rule>
    <Actions>
      <Action>
        <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue
            DataType="http://www.w3.org/2001/XMLSchema#string">GetFeature</AttributeValue>
          <ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
            DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </ActionMatch>
      </Action>
    </Actions>
  </Policy>

```

```

        </Actions>
    </Target>
    <Condition FunctionId="urn:oasis:names:tc:xacml:1.0:function:all-of">
        <Function FunctionId="http://www.geoxacml.org/1.0/function#within"/>
        <AttributeValue DataType="http://www.opengis.net/gml#polygon">
            <gml:Polygon xmlns:gml="http://www.opengis.net/gml" gid="P2" srsName="EPSG:4326">
                <gml:exterior>
                    <gml:LinearRing>
                        <gml:posList dimension="2">-74.28798767828596,40.72400955310945 -
74.12552621736093,40.722605998371435 -74.12552621736093,40.614883172228936 -74.28939123302396,40.61558494959794 -
74.28798767828596,40.72400955310945 -74.28798767828596,40.72400955310945 -
74.28798767828596,40.72400955310945</gml:posList>
                    </gml:LinearRing>
                </gml:exterior>
            </gml:Polygon>
        </AttributeValue>
        <AttributeSelector DataType="http://www.opengis.net/gml#box" MustBePresent="false"
RequestContextPath="//ogc:BBOX/gml:Box"/>
    </Condition>
</Rule>
<Rule Effect="Permit" RuleId="rule-2.3">
    <Description>Field-Engineer can Update features of type ows4:HeliPad_P2, ows4:Taxiway_A</Description>
    <Target>
        <Subjects>
            <AnySubject/>
        </Subjects>
        <Resources>
            <Resource>
                <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:integer-less-than">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#integer">0</AttributeValue>
                    <AttributeSelector DataType="http://www.w3.org/2001/XMLSchema#integer"
RequestContextPath="count (//wfs:Update [@typeName='ows4:HeliPad_P2'])"/>
                </ResourceMatch>
            </Resource>
            <Resource>
                <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:integer-less-than">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#integer">0</AttributeValue>
                    <AttributeSelector DataType="http://www.w3.org/2001/XMLSchema#integer"

```

```

RequestContextPath="count (//wfs:Update[@typeName='ows4:Taxiway_A'])"/>
    </ResourceMatch>
    </Resource>
  </Resources>
  <Actions>
    <Action>
      <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Update</AttributeValue>
        <ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </ActionMatch>
      </Action>
    </Actions>
  </Target>
</Rule>
<Rule Effect="Permit" RuleId="rule-2.4">
  <Description>Field-Engineer can Insert features of type ows4:HeliPad_P2 WITHIN area around the
airport</Description>
  <Target>
    <Subjects>
      <AnySubject/>
    </Subjects>
    <Resources>
      <Resource>
        <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:integer-less-than">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#integer">0</AttributeValue>
          <AttributeSelector DataType="http://www.w3.org/2001/XMLSchema#integer"
RequestContextPath="count (//wfs:Insert/ows4:HeliPad_P2)"/>
          </ResourceMatch>
        </Resource>
      </Resources>
    <Actions>
      <Action>
        <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Insert</AttributeValue>
          <ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"

```

```

DataType="http://www.w3.org/2001/XMLSchema#string"/>
    </ActionMatch>
    </Action>
  </Actions>
</Target>
<Condition FunctionId="urn:oasis:names:tc:xacml:1.0:function:all-of">
  <Function FunctionId="http://www.geoxacml.org/1.0/function#within"/>
  <AttributeValue DataType="http://www.opengis.net/gml#polygon">
    <gml:Polygon xmlns:gml="http://www.opengis.net/gml" gid="P2" srsName="EPSG:4326">
      <gml:exterior>
        <gml:LinearRing>
          <gml:posList dimension="2">-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 40.72400955310945</gml:posList>
        </gml:LinearRing>
      </gml:exterior>
    </gml:Polygon>
  </AttributeValue>
  <AttributeSelector DataType="http://www.opengis.net/gml#point" MustBePresent="true"
RequestContextPath="//wfs:Transaction/wfs:Insert/ows4:HeliPad_P2/ows4:the_geom/gml:Point"/>
</Condition>
</Rule>
<Rule Effect="Deny" RuleId="rule-2.5">
  <Description>Field-Engineer can NOT delete features of type ows4:HeliPad_P2, ows4:Taxiway_A,
ows4:Runway_A</Description>
  <Target>
    <Subjects>
      <AnySubject/>
    </Subjects>
    <Resources>
      <Resource>
        <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:integer-less-than">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#integer">0</AttributeValue>
          <AttributeSelector DataType="http://www.w3.org/2001/XMLSchema#integer"
RequestContextPath="count (//wfs:Delete [@typeName='ows4:HeliPad_P2']) "/>
        </ResourceMatch>
      </Resource>
    </Resource>
  </Target>
</Rule>

```

```

        <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:integer-less-than">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#integer">0</AttributeValue>
            <AttributeSelector DataType="http://www.w3.org/2001/XMLSchema#integer"
RequestContextPath="count (//wfs:Delete[@typeName='ows4:Taxiway_A']) "/>
        </ResourceMatch>
    </Resource>
    <Resource>
        <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:integer-less-than">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#integer">0</AttributeValue>
            <AttributeSelector DataType="http://www.w3.org/2001/XMLSchema#integer"
RequestContextPath="count (//wfs:Delete[@typeName='ows4:Runway_A']) "/>
        </ResourceMatch>
    </Resource>
</Resources>
<Actions>
    <Action>
        <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Delete</AttributeValue>
            <ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </ActionMatch>
    </Action>
</Actions>
</Target>
</Rule>
<Rule Effect="Deny" RuleId="DenyAll"/>
</Policy>
</PolicySet>

```

Figure B.3 — GeoXACML Policy Example, expressing the Access Rights for the Field Engineer in OWS-4.GeoDRM use case #4

Bibliography

- [5] OASIS, *Core and hierarchical role based access control (RBAC) profile of XACML v2.0*, 2005-02-01, http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-rbac-profile1-spec-os.pdf
- [6] OASIS, *SAML 2.0 profile of XACML v2.0*, 2005-02-01, http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-saml-profile-spec-os.pdf
- [7] Cover Pages, Extensible Access Control Markup Language (XACML), <http://xml.coverpages.org/xacml.html>
- [8] Andreas Matheus, *GeoXACML, a spatial extension to XACML, Version 1.0*, 2005-06-17, http://portal.opengeospatial.org/files/index.php?artifact_id=10471
- [9] OGC, *The OpenGIS® Abstract Specification Topic 18: Geospatial Digital Rights Management Reference Model (GeoDRM RM), Version: 1.0.0*, 2006-12-29, http://portal.opengeospatial.org/files/?artifact_id=17802
- [10] Vivid Solutions, *JTS Topology Suite Technical Specifications, Version 1.4*, <http://www.vividsolutions.com/JTS/bin/JTS%20Technical%20Specs.pdf>