

WFS-T Authorization in OWS4

Implementation of the
University of German Armed Forces in OWS4

OGC TC Meeting, San Diego, December 2006

Agenda

- Overview
- License-based Authorization (for WFS-T)
 - Problem statements
- Technology: SAML & GeoXACML
- Implementation
 - SAML Assertions & License References
 - GeoXACML
 - How our (UniBW) implementation looks like
- Conclusions
- Actions

Overview

- Motto:
“Change the OGC interfaces as little as possible,
use other **existing** standards when possible”
- Implementation based on SAML &
XACML (OASIS)
- We used: Java, Apache Tomcat, AXIS
- Software: OpenSource

1) You need to know your resources (here feature types)!

```
<xs:schema elementFormDefault="qualified"
attributeFormDefault="unqualified" version="1.0">
<xs:import namespace="http://www.unibw.de/inf3/ows4"
schemaLocation="http://blade06.informatik.unibw-
muenchen.de:8080/geoserver/wfs/DescribeFeatureType?typeName=
ows4:River_L,
ows4:Aerodrome_A,
ows4:Taxiway_A,
ows4:HeliPad_P2,
ows4:Road_L,
ows4:Aircraft_Hangar_A,
ows4:Runway_A,
ows4:Administrative_Boundary_L" />
</xs:schema>
```

2) You need to know the identities and how they are represented!

UniBW GeoDRM Client-Side Proxy

SOAP EndPoint
http://iisdemo.informatik.uni-bw-muenchen.de:80/axis/services/MSD3DataProxy

Authentication

Username / Password
 Digital Signature / X509 Certificate

Username / Password
Username: NGA-Officer
Password: *****

Digital Signature / X509 Certificate
 Smartcard Identity: Refresh
 File / Keystore PIN / Password:

File / Keystore
File: keystows4.keystore
Keystore Type: JKS Keystore Password: *****

License Tokens
LicenseID2 - FieldEngineer View
LicenseID1 - NGA Officer Add
Delete

HTTP Proxy
Host:
Port: Apply Changes Exit

[08.12.06 23:03]: Configuration successfully loaded!
[08.12.06 23:03]: Open a browser window and type http://localhost:2727/wfst/

- Username / Password
- X.509 Certificate
- etc. (e.g. Fingerprint)

3) You need to know the actions that can be taken!

- WFS-T GetCapabilities Request

- <Operations>

- <Query/> <!-- read -->

- <Insert/>

- <Update/>

- <Delete/>

- <Lock/> <!-- not relevant here -->

- </Operations>

4) You need to know the permissions per user-license!

UniBW GeoDRM Client-Side Proxy

SOAP EndPoint
http://isdemo.informatik.unibw-muenchen.de:80/axis/services/MSD3DataProxy

Authentication

Username / Password
 Digital Signature / X509 Certificate

Username / Password
Username: NGA-Officer
Passwrod: *****

Digital Signature / X509 Certificate
 Smartcard
 File / Keystore

File / Keystore
File: keyslows4.keystore
Keystore Type: JKS
Keystore Password: *****

License Tokens

LicensesID2 - FieldEngineer	View
LinceselD1 - NGA Officer	Add
	Delete

HTTP Proxy
Host:
Port:

Apply Changes Exit

[08.12.06 23:03]: Configuration successfully loaded!
[08.12.06 23:03]: Open a browser window and type http://localhost:2727/hwfst/

- OWS-4 Script (GeoDRM use case #4)
 - Two users:
 - Field-Engineer
 - NGA-Officer
- License ID-1 (NGA-Officer)
- License ID-2 (Field-Engineer)

5) Don't forget about the „open“ operations / actions

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

- For the purpose of navigating with the data, just allow (additional) access to unrestricted resources
 - ows4:River_L
 - ows4:Road_L

6) Define Permissions for the Restricted Operations / Actions

NGA-Officer – Additional permissions

(License ID-1)

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

6) Define Permissions for the Restricted Operations / Actions

Field-Engineer -- Additional permissions

This enables the Analyst to see the airport features

(License ID-2)

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, Update, Delete	ows4:Helipad_P	WITHIN A1 (see figure below)
Transaction / Update	ows4:Taxiway_A	N/A
Transaction / Update	ows4:Runway_A	N/A

6) Define Permissions for the Restricted Operations / Actions

Geometry based access restrictions

(License ID-2)

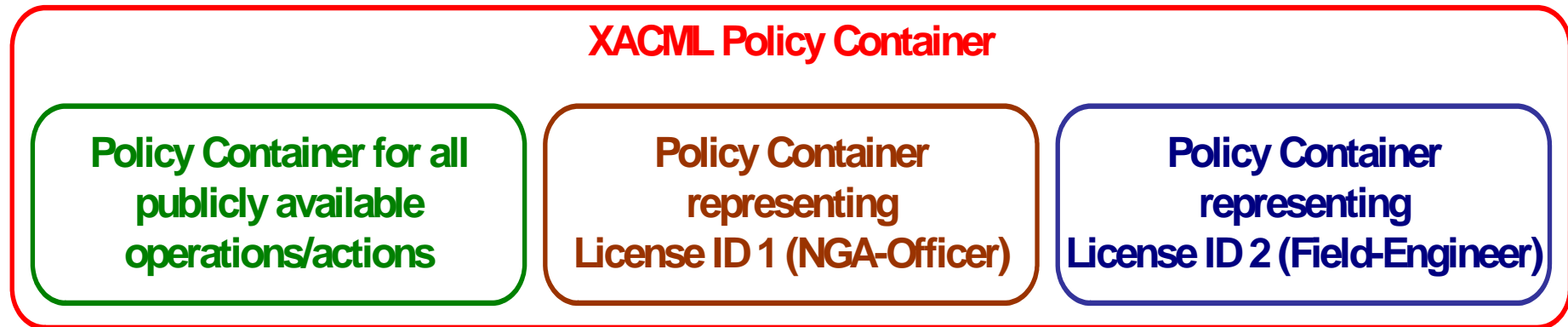


7) Encoding of the Conditions

- Choice **GeoXACML** as an extension to XACML, because it allows to declare and enforce geometry-based permissions

```
- <Condition FunctionId="urn:oasis:names:tc:xacml:1.0:function:all-of">
  <Function FunctionId="http://www.geoxacml.org/1.0/function#within"/>
  - <Attribute Value 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
            -74.28798767828596,40.72400955310945
          </gml:coordinates>
        </gml:LinearRing>
      </gml:outerBoundaryIs>
    </gml:Polygon>
  </Attribute Value>
  <Attribute Selector DataType="http://www.opengis.net/gml#box" MustBePresent="false" RequestContextPath="//ogc:BBOX/gml:Box"/>
</Condition>
```

8) The overall Policy Structure



- <http://iisdemo.informatik.unibw-muenchen.de/ows4/GeoPDP/msd3itc/service?Request=GetPolicy&PolicySetId=msd3>
- http://iisdemo.informatik.unibw-muenchen.de/ows4/GeoPDP/msd3itc/service?Request=GetPolicy&PolicySetId=LICENSE_ID_1
- http://iisdemo.informatik.unibw-muenchen.de/ows4/GeoPDP/msd3itc/service?Request=GetPolicy&PolicySetId=LICENSE_ID_2

Now let's see some examples

1. GetCapabilities and Describe Feature Type is unrestricted for everyone
2. GetFeature action (action == operation) is permitted for Rivers and Roads to everyone
3. Insert of Helipads is only allowed around the area of the Airport for License ID 2
4. Delete of Runways is not allowed for License ID 2
5. Delete of Runways is permitted for License ID 1

1) GetCapabilities and Describe Feature Type is unrestricted for everyone

```
- <Rule Effect="Permit" RuleId="rule-0.1">
- <Description>
  Everybody can make GetCapabilities / DescribeFeatureType
</Description>
- <Target>
- <Subjects>
  <AnySubject/>
</Subjects>
- <Resources>
  <AnyResource/>
</Resources>
- <Actions>
- <Action>
  - <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">GetCapabilities</AttributeValue>
    <ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" DataType="http://www.w3.org/2001/XMLSchema#string"/>
  </ActionMatch>
</Action>
- <Action>
  - <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">DescribeFeatureType</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>
```

2) GetFeature action (action == operation) is permitted for Rivers and Roads to everyone

```
<Rule Effect="Permit" RuleId="rule-0.2">
  - <Description>
    Everybody can make GetFeature requests for ows4:Road_L and ows4:River_L
  </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:Road_L'])"/>
        </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:River_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>
```

Uni

What's this XPath all about?
count(//wfs:Query[@typeName='ows4:Road_L'])

3) Insert of Helipads is only allowed around the area of the Airport for License ID 2

```
- <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">
          <Attribute Value="http://www.w3.org/2001/XMLSchema#integer">0</Attribute Value>
          <Attribute Selector Data Type="http://www.w3.org/2001/XMLSchema#integer" RequestContextPath="count(//wfs:Query[ @typeName='ows4:Road_L'])">
        </ResourceMatch>
      </Resource>
    </Resources>
    - <Actions>
      - <Action>
        - <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <Attribute Value="http://www.w3.org/2001/XMLSchema#string">Insert</Attribute Value>
          <ActionAttribute Designator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" Data Type="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">
    - <Attribute Value Data Type="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 -74.28798767828596,40.72400955310945
            </gml:coordinates>
          </gml:LinearRing>
        </gml:outerBoundaryIs>
      </gml:Polygon>
    </Attribute Value>
    <Attribute Selector Data Type="http://www.opengis.net/gml#point" MustBePresent="true" RequestContextPath="//wfs:Transaction/wfs:Insert/ows4:HeliPad_P2/ows4:the_geom/gml:Point"/>
  </Condition>
</Rule>
```

What's this XPath all about?
count(//wfs:Query[@typeName='ows4:Road_L'])

What's this XPath all about?
//wfs:Transaction/wfs:Insert/ows4:HeliPad_P2/ows4:the_geom/gml:Point

4) Delete of Runways (and Helipads, Taxiways) is not allowed for License ID 2

```
- <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>
- <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-id" DataType="http://www.w3.org/2001/XMLSchema#string"/>
</ActionMatch>
</Action>
</Actions>
</Target>
</Rule>
```

5) Delete of Runways is permitted for License ID 1

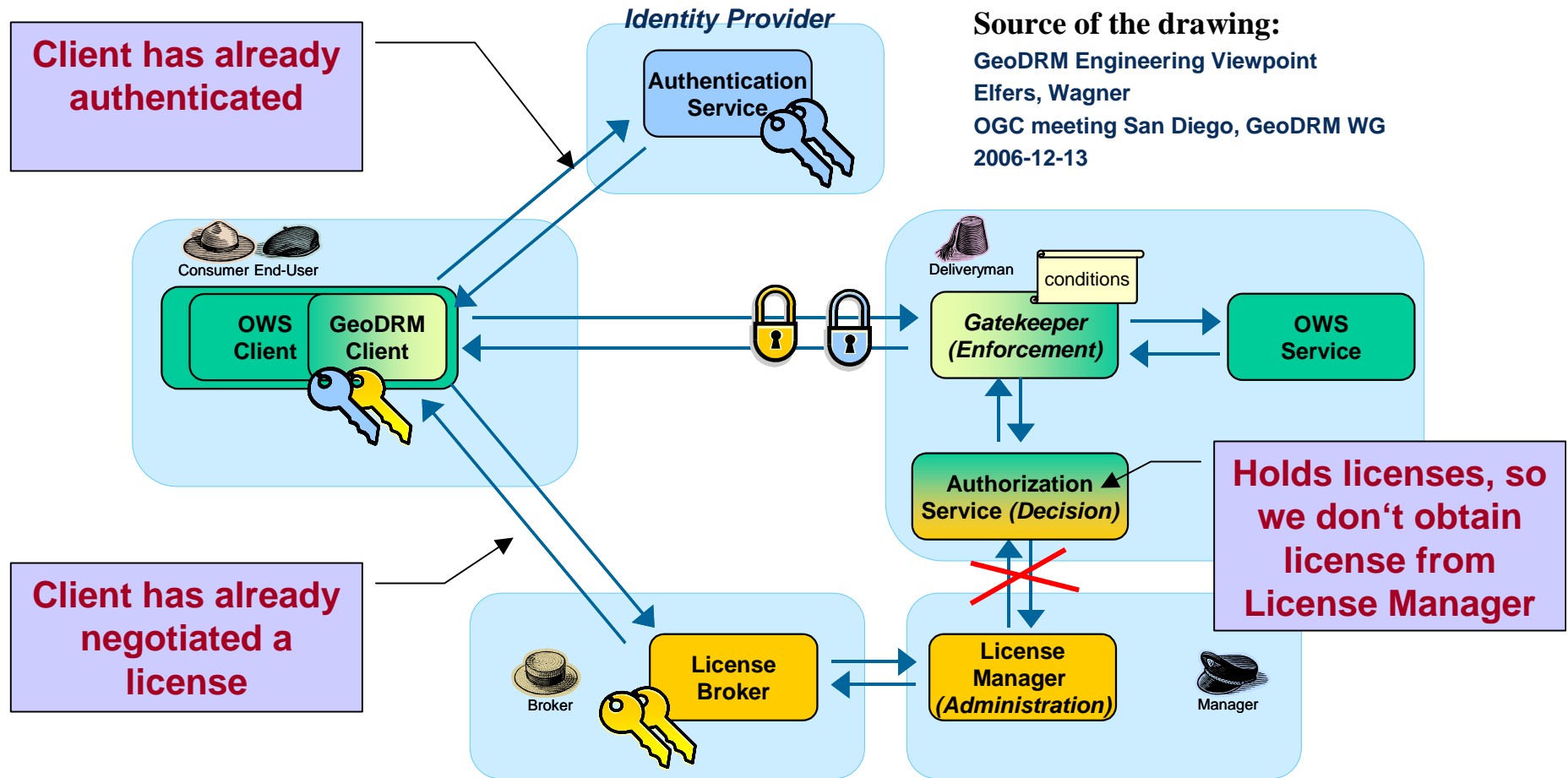
```
- <Rule Effect="Permit" RuleId="rule-1.4">
  - <Description>
    NGA-Officer can Delete features of type ows4:HeliPad_P2, ows4:Taxiway_A, ows4:Runway_A
  </Description>
  - <Target>
    - <Subjects>
      <AnySubject>
      </Subjects>
    - <Resources>
      - <Resource>
        - <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:integer-less-than">
          <Attribute Value DataType="http://www.w3.org/2001/XMLSchema#integer">0</Attribute Value>
          <Attribute Selector DataType="http://www.w3.org/2001/XMLSchema#integer" RequestContextPath="count(/wfs:Delete[@typeName='ows4:HeliPad_P2'])"/>
        </ResourceMatch>
      </Resource>
      - <Resource>
        - <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:integer-less-than">
          <Attribute Value DataType="http://www.w3.org/2001/XMLSchema#integer">0</Attribute Value>
          <Attribute Selector 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">
          <Attribute Value DataType="http://www.w3.org/2001/XMLSchema#integer">0</Attribute Value>
          <Attribute Selector 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">
        <Attribute Value DataType="http://www.w3.org/2001/XMLSchema#string">Delete</Attribute Value>
        <ActionAttribute Designator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" DataType="http://www.w3.org/2001/XMLSchema#string"/>
      </ActionMatch>
    </Action>
  </Actions>
</Target>
</Rule>
```

Un

Now, how does enforcement actually work?

- Let's see the bigger picture first...

Let's see the bigger Picture ...



But back to the question ...

- The WFS-T Request is added to an XACML Authorization Decision Request issued by the Gatekeeper, send to the Authorization Service

```
<Request xmlns="urn:oasis:names:tc:xacml:1.0:context" xmlns:xacml="urn:oasis:names:tc:xacml:1.0:policy" xmlns:xsi="
http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="urn:oasis:names:tc:xacml:1.0:context ps-xacml-schema-context-01.xsd">
  <Subject/>
  <Resource>
    <ResourceContent>
      <!-- Put the WFS-T request here as a CDATA section -->
    </ResourceContent>
  </Resource>
  <Action/>
</Request>
```

XACML Request containing a WFS-T GetFeature Request

```
<xacml-context:ResourceContent><![CDATA[<?xml version="1.0" encoding="UTF-8"?>
<wfs:GetFeature service="WFS" version="1.0.0" xmlns:wfs="http://www.opengis.net/wfs" xmlns:gml="http://www.opengis.net/gml"
xmlns:ogc="http://www.opengis.net/ogc" xmlns:ows4="http://www.opengeospatial.org/ows4" xmlns:xlink="http://www.w3.org/1999/xlink"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://www.opengis.net/wfs
http://schemas.opengis.net/wfs/1.0.0/OWS-basic.xsd">
  <wfs:Query typeName="ows4:Helipad_P2">
    <ogc:BBOX>
      <gml:Box srsName="EPSG:4326">
        <gml:coordinates xmlns:gml="http://www.opengis.net/gml" decimal="." cs="," ts=" ">-73.95533279299448,40.82414581720157
-73.93855481003192,40.832408895114554</gml:coordinates>
      </gml:Box>
    </ogc:BBOX>
  </wfs:Query>
</wfs:GetFeature>]]>
</xacml-context:ResourceContent>
```

- Remember the Xpath(s) in the Policies (Rules)?
 - They are matched inside the WFS-T Request!
 - Question: Is this request for River or Road?
count(//wfs:Query[@typeName='ows4:Road_L'])
- No! This one is for ... **Helipads**

XACML Request containing a WFS-T GetFeature Request

```
<xacml-context:ResourceContent><![CDATA[<?xml version="1.0" encoding="UTF-8"?>
<wfs:GetFeature service="WFS" version="1.0.0" xmlns:wfs="http://www.opengis.net/wfs" xmlns:gml="http://www.opengis.net/gml"
xmlns:ogc="http://www.opengis.net/ogc" xmlns:ows4="http://www.opengeospatial.org/ows4" xmlns:xlink="http://www.w3.org/1999/xlink"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://www.opengis.net/wfs
http://schemas.opengis.net/wfs/1.0.0/ows4-basic.xsd">
  <wfs:Query typeName="ows4:HeliPad_P2">
    <ogc:BBOX>
      <gml:Box srsName="EPSG:4326">
        <gml:coordinates xmlns:gml="http://www.opengis.net/gml" decimal="." cs="," ts=" ">-73.95533279299448,40.82414581720157
-73.93855481003192,40.832408895114554</gml:coordinates>
      </gml:Box>
    </ogc:BBOX>
  </wfs:Query>
</wfs:GetFeature>]]>
</xacml-context:ResourceContent>
```

- Xpath(s)

- `count(//wfs:Query[@typeName='ows4:HeliPad_P2'])`
- `//ogc:BBOX/gml:Box`

The previous request would satisfy the following 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">
          <Attribute Value="http://www.w3.org/2001/XMLSchema#integer">0</Attribute Value>
          <Attribute Selector Data Type="http://www.w3.org/2001/XMLSchema#integer" RequestContextPath="count(/wfs:Query[@typeName='ows4:HeliPad_P2'])"/>
        </ResourceMatch>
      </Resource>
    </Resources>
    - <Actions>
      - <Action>
        - <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <Attribute Value Data Type="http://www.w3.org/2001/XMLSchema#string">GetFeature</Attribute Value>
          <Action Attribute Designator Attribute Id="urn:oasis:names:tc:xacml:1.0:action:action-id" Data Type="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"/>
    - <Attribute Value Data Type="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 -74.28798767828596,40.72400955310945
            </gml:coordinates>
          </gml:LinearRing>
        </gml:outerBoundaryIs>
      </gml:Polygon>
    </Attribute Value>
    <Attribute Selector Data Type="http://www.opengis.net/gml#box" MustBePresent="false" RequestContextPath="//ogc:BBOX/gml:Box"/>
  </Condition>
</Rule>
```

Conclusion on XACML

- **GeoXACML** is very suitable for the declaration of and enforcement of all kinds of access restrictions
 - Because of that, it can get quite complex if you like to enforce very specific and fine-grained restrictions
 - It worked very well for us together with SAML to show a licensed based Authorization, using existing standards
- Performance was never mission critical for these rather simple Policies. So long you know what you do, you can structure them to give good performance.

Warning, Warning, Warning, ...

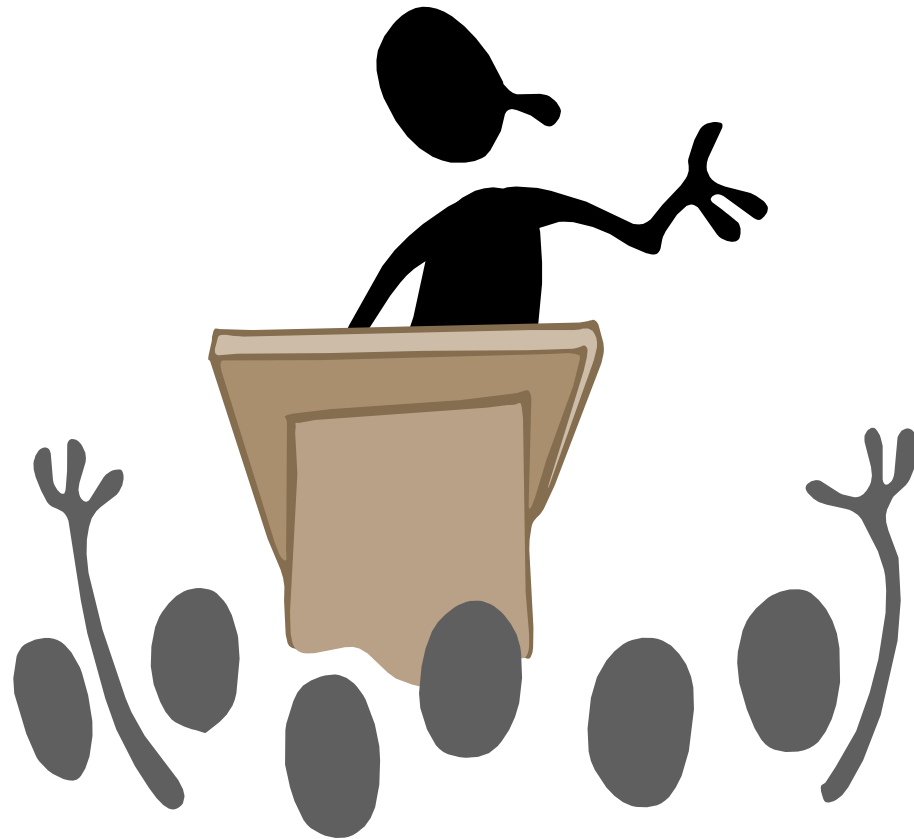
- The current approach derives authorization decisions for some WFS-T operations, based on the service request
- It can get very complicated if you like to support all possible variations of permissions and Transactional Operations

Example: Geometry restriction on Helipads

- So long the request contains a BBOX; fine!
- If not (e.g. `<Filter>Feature-ID=4711</Filter>`) the gatekeeper must resolve the geometry by calling the WFS first.
- This can be controlled by the Status of the XACML Authorization Response (Status: Indeterminate)

keep restrictions SIMPLE at all times!!!

Hope you got the picture ...
Thank you!



Andreas Matheus

University of the German Armed Forces, Munich

Andreas.Matheus@unibw.de