Open Geospatial Consortium

Approved Date: 2013-01-18

Posted Date: 2013-02-06

Reference number of this document: OGC 12-118

External Identifier for this document: http://www.opengis.net/def/doc-type/per/ows9-security

Category: Engineering Report

Editor: Andreas Matheus

OWS-9 Security Engineering Report

Warning

This document is not an OGC Standard. This document is an OGC Public Engineering Report created as a deliverable in an OGC Interoperability Initiative and is not an official position of the OGC membership. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an OGC Standard. Further, any OGC Engineering Report should not be referenced as required or mandatory technology in procurements.

Document type:	OGC® Engineering Report
Document subtype:	NA
Document stage:	Approved for public release
Document language:	English

Abstract

This document presents the results of the work within the OWS-9 Security and Services Interoperability (SSI) thread and results from CCI and Innovations Cross Thread activities.

What is OWS-9?

OWS-9 builds on the outcomes of prior OGC initiatives and is organized around the following threads:

- **Aviation**: Develop and demonstrate the use of the Aeronautical Information Exchange Model (AIXM) and the Weather Exchange Model (WXXM) in an OGC Web Services environment, focusing on support for several Single European Sky ATM Research (SESAR) project requirements as well as FAA (US Federal Aviation Administration) Aeronautical Information Management (AIM) and Aircraft Access to SWIM (System Wide Information Management) (AAtS) requirements.

- **Cross-Community Interoperability (CCI)**: Build on the CCI work accomplished in OWS–8 by increasing interoperability within communities sharing geospatial data, focusing on semantic mediation, query results delivery, data provenance and quality and Single Point of Entry Global Gazetteer.

- **Security and Services Interoperability (SSI)**: Investigate 5 main activities: Security Management, OGC Geography Markup Language (GML) Encoding Standard Application Schema UGAS (UML to GML Application Schema) Updates, Web Services Façade, Reference Architecture Profiling, and Bulk Data Transfer.

- **OWS Innovations**: Explore topics that represent either new areas of work for the Consortium (such as GPS and Mobile Applications), a desire for new approaches to existing technologies to solve new challenges (such as the OGC Web Coverage Service (WCS) work), or some combination of the two.

- **Compliance & Interoperability Testing & Evaluation (CITE)**: Develop a suite of compliance test scripts for testing and validation of products with interfaces implementing the following OGC standards: Web Map Service (WMS) 1.3 Interface Standard, Web Feature Service (WFS) 2.0 Interface Standard, Geography Markup Language (GML) 3.2.1 Encoding Standard, OWS Context 1.0 (candidate encoding standard), Sensor Web Enablement (SWE) standards, Web Coverage Service for Earth Observation (WCS-EO) 1.0 Interface Standard, and TEAM (Test, Evaluation, And Measurement) Engine Capabilities.

The OWS-9 sponsors are: AGC (Army Geospatial Center, US Army Corps of Engineers), CREAF-GeoViQua-EC, EUROCONTROL, FAA (US Federal Aviation Administration), GeoConnections - Natural Resources Canada, Lockheed Martin Corporation, NASA (US National Aeronautics and Space Administration), NGA (US National Geospatial-Intelligence Agency), USGS (US Geological Survey), UK DSTL (UK MoD Defence Science and Technology Laboratory).

License Agreement

Contents

Page

Figures

Tables Page

OGC® OWS-9 Security Engineering Report

1 Introduction

1.1 Scope

This Engineering Report describes the approaches to security taken in the OWS-9 initiative. This document presents the results of the work within the OWS-9 Security and Services Interoperability (SSI) thread and results from CCI and Innovations Cross Thread activities.

The report also describes the various tasks and their results regarding interoperability between different security components provided by different participants.

1.2 Document contributor contact points

All questions regarding this document should be directed to the editor or the contributors:

Name	Organization
Andreas Matheus	University of the Bundeswehr
Jan Drewnak, Rüdiger Gartmann	con terra
Thomas Dineen	LMCO

1.3 Revision history

Date	Release	Editor	Primary clauses modified	Description
20.07.2012	0.1	AM		First working draft
24.09.2012 - 27.11.2012	0.2	AM		Second working draft – incoperating comments received Section 5.4 (diagrams and text) is provided by GEOAxIS and reviewed by con terra Figures 5.2.1 and 5.2.2 are provided by GEOAxIS and reviewed by con terra
07.12.2012	03	JD, RG	5.4.1, 5.6-5.8, 7.3.	Details on the con terra contribution
		TD	5.6.1, 5.7.1, 5.8.1	Details on the GEOAxIS contribution

1.4 Future work

1.5 Forward

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. The Open Geospatial Consortium shall not be held responsible for identifying any or all such patent rights.

Recipients of this document are requested to submit, with their comments, notification of any relevant patent claims or other intellectual property rights of which they may be aware that might be infringed by any implementation of the standard set forth in this document, and to provide supporting documentation.

2 References

The following documents are referenced in this document. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. For undated references, the latest edition of the normative document referred to applies.

OASIS XACML 2.0	https://www.oasis-open.org/committees/xacml/
OGC GeoXACML 1.0.1	http://portal.opengeospatial.org/files/?artifact_id=42734
OGC CSW 2.0.2	http://portal.opengeospatial.org/files/?artifact_id=20555
OGC WFS 2.0	http://portal.opengeospatial.org/files/?artifact_id=39967
OGC OWS Context (used version is not publicaly available)	

3 Terms and definitions

For the purposes of this report, the definitions specified in Clause 4 of the OWS Common Implementation Standard [OGC 06-121r3] and the listed specifications from section 3 (References) shall apply. In addition, the following terms and definitions apply.

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

Obligation - An operation specified in a rule, policy or policySet element that should be performed by the Obligation Handler 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 Decision Point (PDP) - The system entity that evaluates applicable policy and renders an authorization decision.

Policy Enforcement Point (PEP) - The system entity that performs access control, by making decision requests and enforcing authorization decisions.
Policy information point (PIP) - The system entity that acts as a source of attribute values
Rule - A target, an effect, a condition and obligations. A component of a policy

4 Conventions

AD	Authorization decision
ADR	Authorization decision request
CCI	Cross Community Interoperability
CSW	Catalogue Service for the Web
GeoPDP	PDP implementing GeoXACML
GeoXACML	Geospatial eXtensible Access Control Markup Language
GML	Geography Markup Language
HRP	Hierarchical Resource Profile
MRP	Multiple Resource Profile
OASIS	Organization for the Advancement of Structured Information Standards
OGC	Open Geospatial Consortium
OWS	OGC Web Service
OWS-6/7/8/9	OGC Web Services Initiative, Phase 6/7/8/9
PAP	Policy Administration Point
PDP	Policy Decision Point implementing XACML
PEP	Policy Enforcement Point
SDI	Spatial Data Infrastructure
SOA	Service Oriented Architecture
SSI	Security and Services Interoperability
URL	Uniform Resource Locator
URN	Uniform Resource Names
WFS(-T)	Web Feature Service (-Transactional)
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language

5 SSI Thread Security

For the SSI Thread in OWS-9, the security approach focused on testing interoperability of standards based interfaces between software products of different vendors and different security protocols, involving Message Level Security with WS-Security and Transport Level Security.

Also, the execution of XACML 2 based policies on different vendors Policy Decision Points was evaluated regarding interopeability.

5.1 Architecture Overview

The following figure illustrates the initial, high level architecture which is meant to be used for exploring more details.

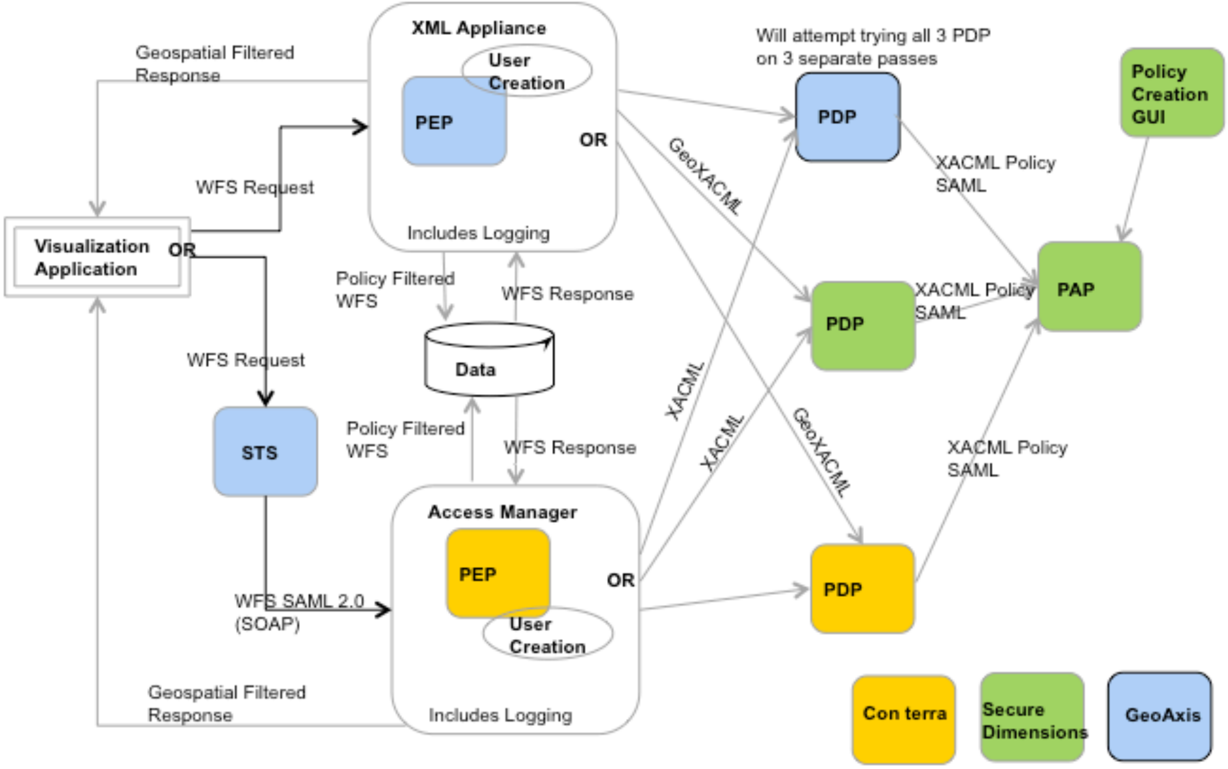
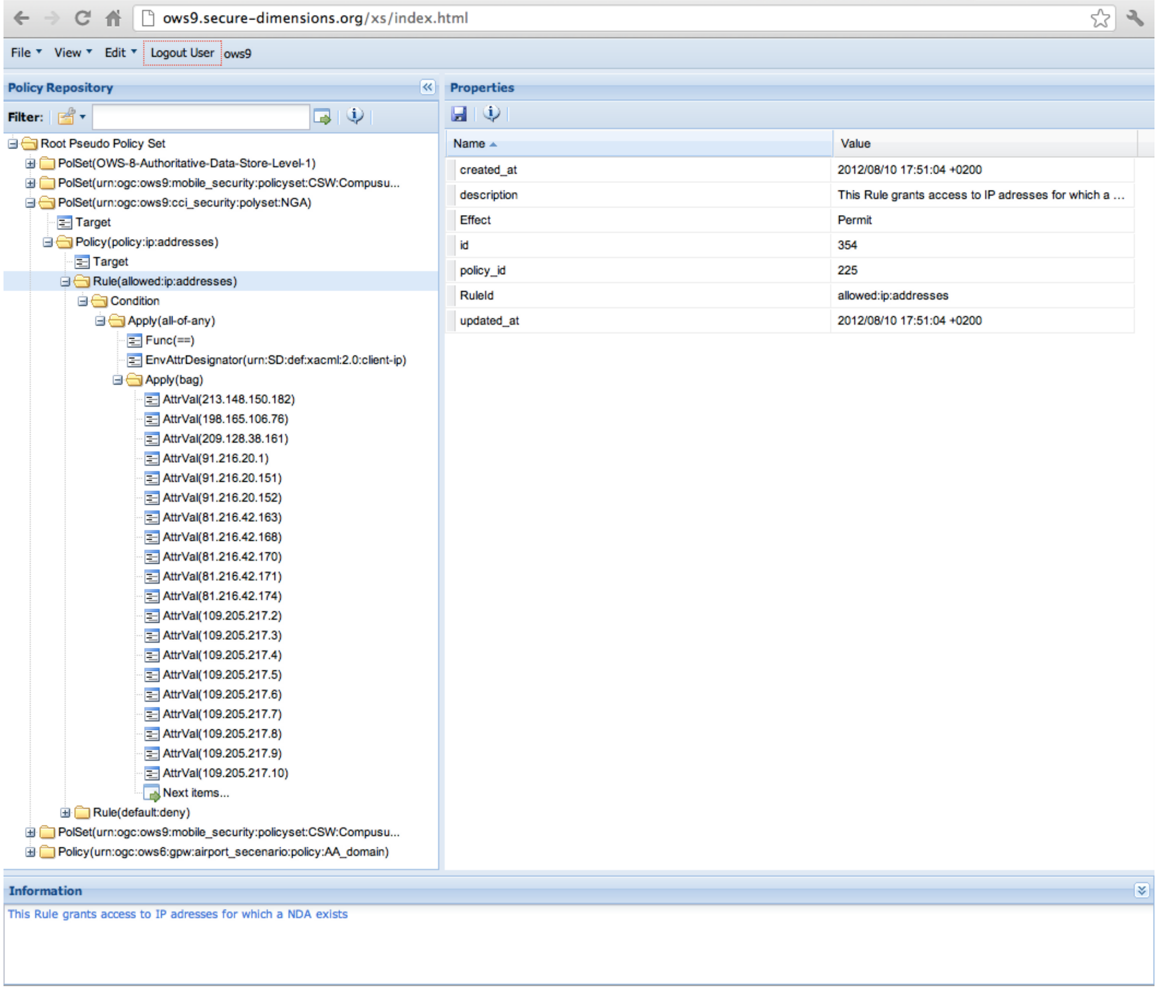


Figure 1— Initial Security Architecture for the SSI thread

As outlined in the figure above, the architecture above comprises of the following software components:

PAP (Policy Administration Point):

This service enables a security administrator to define access rights described in XACML 2.0 or GeoXACML 1.0. For this purpose, a thin client application is available that provides pro-active support for the administrator. The following screen shot illustrates the client:



```
Root Pseudo Policy Set
  PolSet(OWS-8-Authoritative-Data-Store-Level-1)
  PolSet(urn:ogc:ows9:mobile_security:policyset:CSW:Compusu...
  PolSet(urn:ogc:ows9:cci_security:polyset:NGA)
    Target
    Policy(policy:ip:addresses)
      Target
      Rule(allowed:ip:addresses)
        Condition
          Apply(all-of-any)
            Func(==)
            EnvAttrDesignator(urn:SD:def:xacml:2.0:client-ip)
            Apply(bag)
              AttrVal(213.148.150.182)
              AttrVal(198.165.106.76)
              AttrVal(209.128.38.161)
              AttrVal(91.216.20.1)
              AttrVal(91.216.20.151)
              AttrVal(91.216.20.152)
              AttrVal(81.216.42.163)
              AttrVal(81.216.42.168)
              AttrVal(81.216.42.170)
              AttrVal(81.216.42.171)
              AttrVal(81.216.42.174)
              AttrVal(109.205.217.2)
              AttrVal(109.205.217.3)
              AttrVal(109.205.217.4)
              AttrVal(109.205.217.5)
              AttrVal(109.205.217.6)
              AttrVal(109.205.217.7)
              AttrVal(109.205.217.8)
              AttrVal(109.205.217.9)
              AttrVal(109.205.217.10)
              Next items...
      Rule(default:deny)
  PolSet(urn:ogc:ows9:mobile_security:policyset:CSW:Compusu...
  Policy(urn:ogc:ows6:gpw:airport_secenario:policy:AA_domain)
```

Name	Value
created_at	2012/08/10 17:51:04 +0200
description	This Rule grants access to IP adresses for which a ...
Effect	Permit
id	354
policy_id	225
RuleId	allowed:ip:addresses
updated_at	2012/08/10 17:51:04 +0200

This Rule grants access to IP adresses for which a NDA exists

Figure 2 — Initial Security Architecture for the SSI thread

The illustrated example provides a tree view of a XACML 2.0 policy for enforcing access rights to a WFS, where access is restricted to a set of IP adresses (white listing). Using the client to explore the policy in more details would show that the policy gets enforced when the client ip address is one of the listed addresses. The <Condition> evaluates to true and the enclosing <Rule> elements instruments the PDP to derive a "PERMIT" authorization decision. In case that the <Condition> does not match – so a client not having a listed ip address - , the <Rule> "default:deny" would instrument the PDP to return a "DENY" decision.

The PAP does provide a Web Service endpoint that supports requesting a XACML 2.0 or GeoXACML 1.0 policy based on the PolicyId or PolicySetId attribute.

PDP (Policy Decision Point):

The Policy Decision Point is responsbile for deriving an authorization decision based on the information provided in the authorization decision request that was received from the PEP and the Policy that was loaded from the PAP.
If the PDP is a XACML 2.0 compliant implementation, it will accept XACML 2.0 policies. If the PDP is a GeoXACML 1.0 compliant implementation, it will accept a GeoXACML 1.0 or a XACML 1.0 policy.

PEP (Policy Enforcement Point):
The Policy Enforcement Point is responsible for rejecting or accepting requests from a client to a service that is protected by the PEP.
For OWS-9, the PEP is also responsible for modifying intercepted requests to the service or intercepted responses from the service according to XACML 2.0 Obligations that are expressed in the authorization decision that was received from the PDP.

STS (Secure Token Service):
The Secure Token Service is responsible for releasing access tokens to amend messages to the PEP which is expecting WS-Security conforme SOAP messages.

5.2 Use Case / Data Sets / Access Restrictions

The use case defining the access restrictions for the SSI thread are outlined on a OWS-9 wiki page: https://portal.opengeospatial.org/wiki/OWS9/ScenarioAlternative and on various emails. A detailed summary – that covers all relevant details to produce a XACML policy – is available from the OWS-9 portal: https://portal.opengeospatial.org/files/?artifact_id=51106. For the sake of completenes and the ease of reading, this section comprises all the information. Important for the SSI thread are two data sets: Haiti and Monterey. The first data set is hosted on a WFS originally provided by the carbonproject and the second data set is hosted on a WFS originally provided by interactive instruments. For both WFS, the SSI thread participants GEOAxIS and con terra provide through their infrastructure secured endpoints which will enforce the defined access rights. Involved actors are the Chief, the Map Analyst for Monterey and Haiti and the Planner for Monterey and Haiti. All of these users have access rights which are described in more detail below. To demonstrate that any other user on the network has no access to the data sets, the user Placebo (system user Placebo) is in place.
The actor Chief (system user Chief) has unconstrained access to the Haiti data set and for the Monterey data set can see the government buildings regardless of location plus every feature regardless of security tagging inside the airport boundary.

- Access permitted for all features regardless of security marking within the airport boundary (as defined by AeronauticalCurves.2)

- Access permitted to all features of type tds:BuildingGeosurface if the property featureFunction-1 equals government or localGovernment or subnationalGovernment

The actor Monterey Map Analyst (system user MAnalyst) has unconstrained access to the Haiti and Monterey data sets.
The actor Monterey Planner (system user MResponder) has full access to the Haiti data set and limited access to the Monterey data set:

- Access denied for all features statically marked “S” that are within the airport boundary (as defined by AeronauticalCurves.2) StructureSurfaces.19572, AeronauticalPoints.109

- Access denied for features alternatively marked „S“ if request in time 2013-01-12 to 2013-01-13 AeronauticalSurfaces.1054

- Access denied for all features of type tds:BuildingGeosurface if the property featureFunction-1 equals government or localGovernment or subnationalGovernment

The actors Haiti Map Analyst (system user HAnalyst) and Haiti Planner (system user HResponder) both have unconstrained access to the Haiti data set and no access to the Monterey data set.

5.3 Architecture Details

In order to achieve the defined access resrictions on a WFS, this thread practices two methods: (i) WFS request re-writing and (ii) WFS response filtering.

5.3.1 WFS request rewriting

The first practiced method involving the WFS request rewriting takes advantage to extend / modify a simple and security unaware request from the client. The following architecture diagram illustrated the architecture and the flow of interactions between the different components.

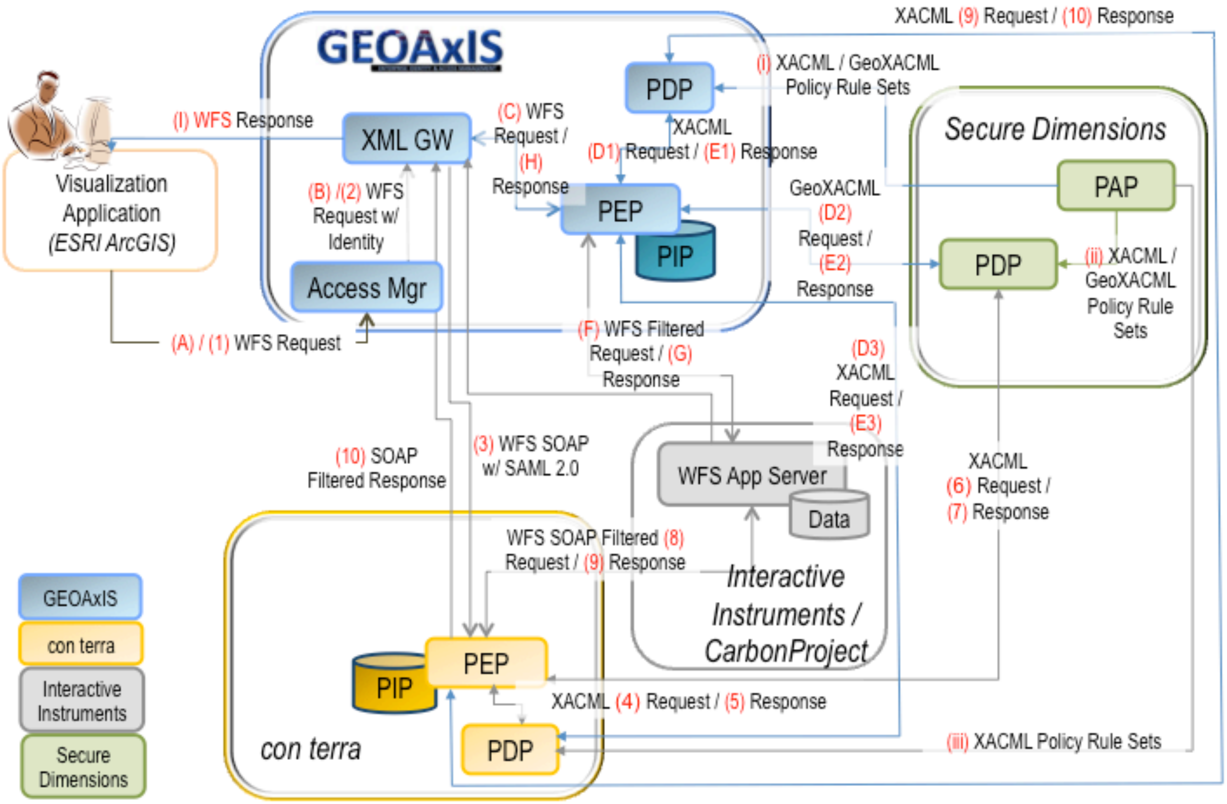


Figure 3 — Architecture for the SSI thread parcticing WFS request rewriting

The complete flow of communication is outlined in more detail in section 5.4

5.3.2 WFS response rewriting

The second practiced method involving the WFS response filtering takes advantage of the fact that the response is XML structured data and that more flexible processing is possible compared to the WFS request options.

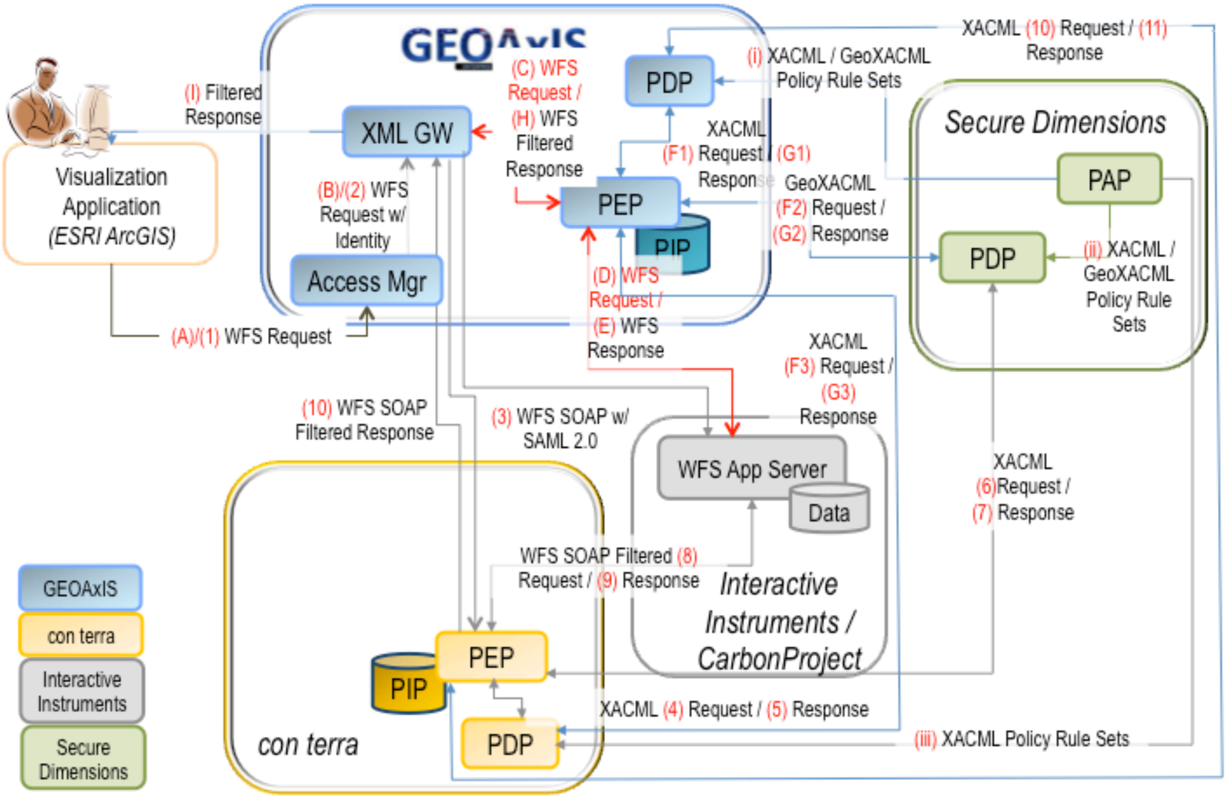

GEOAxIS
XML GW
Access Mgr
PDP
PEP
PIP
(I) Filtered Response
Visualization Application (ESRI ArcGIS)
(A)/(1) WFS Request
(B)/(2) WFS Request w/ Identity
(C) WFS Request / (H) WFS Filtered Response
(D) WFS Request / (E) WFS Response
(i) XACML / GeoXACML Policy Rule Sets
XACML (F1) Request / (G1) Response
GeoXACML (F2) Request / (G2) Response
XACML (10) Request / (11) Response
Secure Dimensions
PAP
PDP
(ii) XACML / GeoXACML Policy Rule Sets
XACML (F3) Request / (G3) Response
XACML (6) Request / (7) Response
(10) WFS SOAP Filtered Response
(3) WFS SOAP w/ SAML 2.0
WFS App Server
Data
WFS SOAP Filtered (8) Request / (9) Response
Interactive Instruments / CarbonProject
PEP
PIP
PDP
con terra
XACML (4) Request / (5) Response
(iii) XACML Policy Rule Sets
GEOAxIS
con terra
Interactive Instruments
Secure Dimensions

Figure 4 — Architecture for the SSI thread parcticing WFS response filtering

The complete flow of communication is outlined in more detail in section 5.4

5.4 Communication Protocols

The outlined architecture comprises of security components from different vendors. It is important to understand that the security information required is carried differently. For an interoperability project like OWS-9 it is of particular importance that the security communication protocol is based on standards whenever a communication link exists between two different vendors. According to the architecture diagrams above, the following security protocols and components can be identified:

1) GEOAxIS PEP – con terra PDP

2) GEOAxIS / con terra PEP – Secure Dimensions PDP

The internal communication between the following components is not documented here:

3) GEOAxIS PEP – GEOAxIS PDP

4) con terra PEP – con terra PDP

5.4.1 GEOAxIS PEP – con terra PDP communication protocol

The con terra PDP accepts XACML 2.0 compliant Authorization Decision Requests (ADR) using HTTP POST. The ADR may be wrapped into a SOAP message or sent as plain HTTP request body. It returns an XACML 2.0 compliant Authorization Decision, again wrapped into a SOAP message or as plain HTTP response body, according to the encoding used for the request.
For this testbed, the con terra PDP is only available to dedicated source IP addresses.

5.4.2 GEOAxIS / con terra PEP – Secure Dimensions PDP communication protocol

The Secure Dimensions PDP accepts XACML 2.0 compliant Authorization Decision Requests (ADR) using HTTP POST. After processing the ADR, it returns a XACML 2.0 compliant Authorization Decision (AD).
The structure of the ADR is defined by the XACML 2.0 schema element RequestType and the structure of the AD is defined by the ResponeType, both defined in the namspace URI urn:oasis:names:tc:xacml:2.0:context:schema:os.
In terms of protection, each PDP prodivded by Secure Dimensions can only be accessed via a cleared IP address. A request from any other IP address will receive a HTTP 403 „Forbidden" status. So in order for GEOAxIS and con terra to leverage the provided PDP, the PEP's outbound IP address must be known.

5.4.3 PAP communication protocol

According to the flow of communication, all PDPs load the policy from the Policy Administration Point. It is therefore required that the PAP provides a web service alike interface in addition to the policy creation and maintenance GUI that can be accessed using login username `ows9` and password `ogcows9`
The PAP service interface for obtaining a policy is not protected. The following service endpoint URL is available
http://ows9.secure-dimensions.org/cgi-bin/PAP
The Web Service interface can be executed via HTTP/Get using Key-Value-Pair encoding to shape the request. Currently, this interface can be executed using the following parameters (keys):

- `PolicySetId=`*`value`* tasks the PAP to return the policy where the attribute "PolicySetId" equals *`value`*. The root element of the returned policy is a <PolicySet> element

- `PolicyId=`*`value`* tasks the PAP to return the policy where the attribute "PolicyId" equals *`value`*. The root element of the returned policy is <Policy> element.

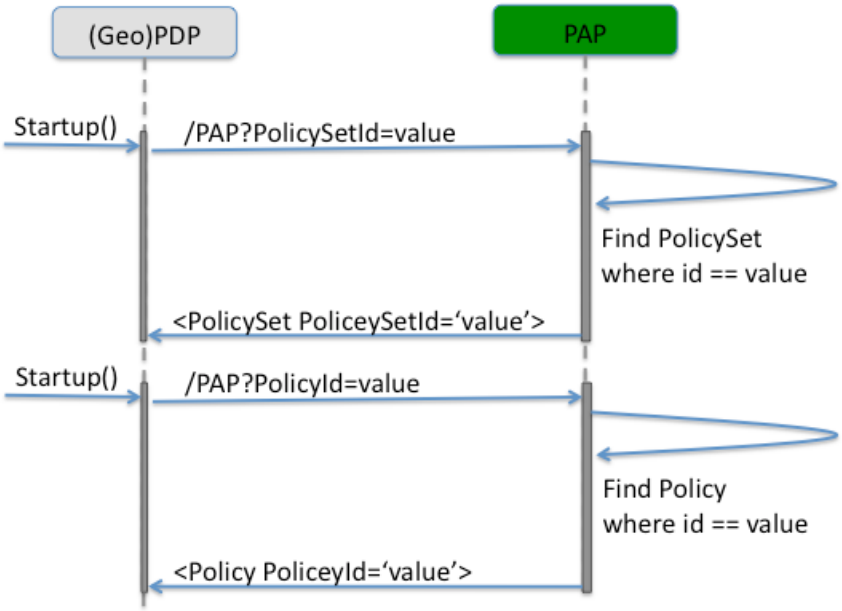


Figure 5 — Interaction with the PAP's Web Service Interface

5.5 Communication between components

As illustated in the architecutre diagrams above, PEPs and PDPs are redundant. From this aspect, different pairings of PEP/PDP are possible as also illustrated above. This sub chapter illustrates the flow of communication between different pairings regarding access control based on client requests with optional request modification.

5.5.1 GEOAxIS PEP and PDP

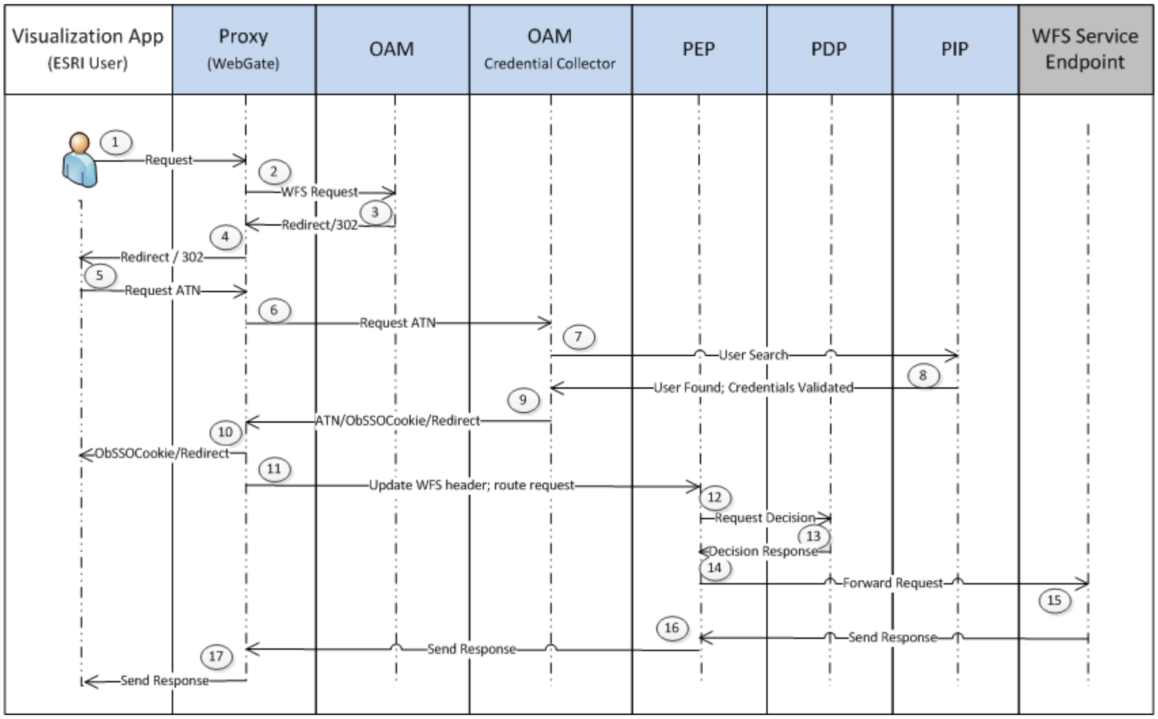


Figure 6 — Flow of communication for GEOAxIS PEP and PDP

1. The User submits a WFS request via the ESRI Visualization Application

2. The Proxy intercepts the request and forwards it to the Oracle Access Manager (OAM).

3. OAM checks if resource is protected and whether an ObSSOCookie exists. In this use case, the resource is protected and there is no ObSSOCookie on the request. As the result, an HTTP 302 (redirect) response is returned.

4. Proxy forwards HTTP 302 response to the Visualization Application

5. Authentication (ATN) request is generated.

6. Proxy intercepts ATN request and forwards it to the OAM Credential Collector (CC)

7. User credentials (uid/pwd) must be validated, thus OAM CC forwards the request to the Policy Information Point (PIP).

8. PIP returns credential successful validation.

9. OAM CC generates a session token with a URL that contains the ObSSOCookie. User is athenticated and ObSSOCookie is forwarded to the Proxy.

10. Proxy forwards HTTP 302 + authenticated response

11. Proxy appends the userid into the WFS header and forwards to the Policy Enforcement Point (PEP).

12. PEP sends information to the Policy Decision Point (PDP) to determine if user request is permitted to be sent to the WFS endpoint.

13. PDP makes decision and returns response to PEP.

14. Upon receipt of a successful response from the PDP, the PEP routes the WFS request to the WFS service endpoint

15. – 17. WFS endpoint response is routed to requester (end user).

5.5.2 GEOAxIS PEP and Secure Dimensions PDP

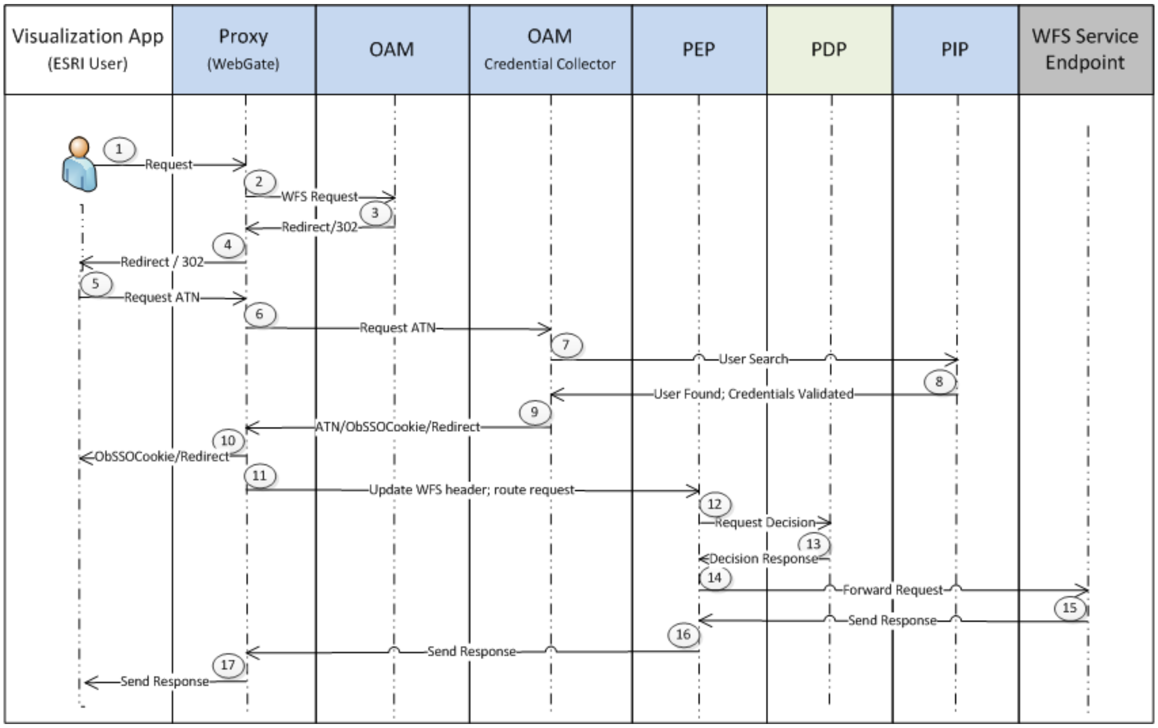


Figure 7 — Flow of communication for GEOAxIS PEP and Secure Dimensions PDP

The flow of communication is identical to 5.2.1. even though another participant provides the PDP.

5.5.3 GEOAxIS PEP and con terra PDP

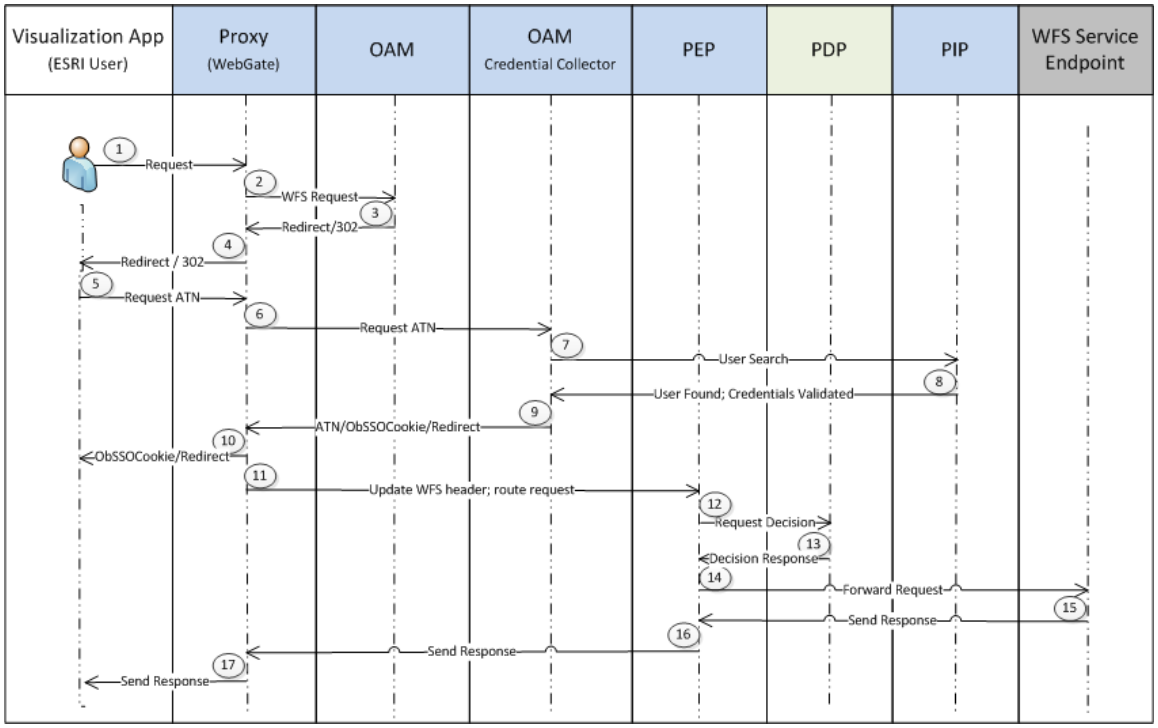


Figure 8 — Flow of communication for GEOAxIS PEP and con terra PDP

The flow of communication is identical to 5.2.1. even though another participant provides the PDP.

5.5.4 con terra PEP con terra PDP

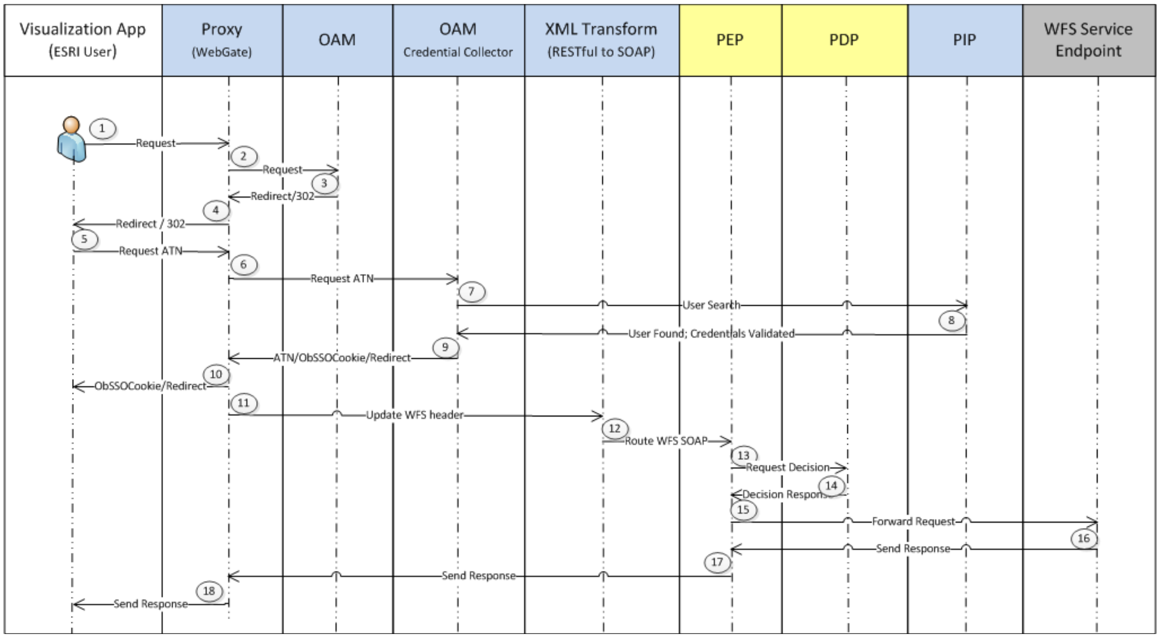


Figure 9 — Flow of communication for con terra PEP and PDP

1. User submits a WFS request via the Visualization Application.
2. Proxy intercepts request and forwards it to Oracle Access Manager (OAM).
3. OAM checks if resource is protected and whether an ObSSOCookie exists. In this use case, the resource is protected and there is no ObSSOCookie on the request, as a result, an HTTP 302 (redirect) response is forwarded to the browser.
4. Proxy forwards HTTP 302 response to the browser.
5. Authentication request is generated.
6. Proxy intercepts ATN request and forwards to the OAM Credential Collector (CC).
7. User credentials (uid/pwd) must be validated, thus OAM CC forwards the request to the Policy Information Point (PIP).
8. PIP returns successful credential validation.
9. OAM Credential Collector generates a session token with a URL that contains the ObSSOCookie. User is athenticated and ObSSOCookie is forwarded to Proxy/WebGate.
10. Proxy forwards HTTP 302 + authenticated response.
11. OAM WebGate appends the userid into the WFS header and forwards to the Policy Enforcement Point (PEP).
12. WFS SOAP is routed to con terra PEP.
13. PEP sends information to the Policy Decision Point (PDP) to determine if user request is permitted to be sent to the WFS Service Endpoint.
14. PDP makes decision and returns response to PEP.
15. Upon receipt of a successful response from the PDP, the PEP routes the WFS request to the WFS endpoint.
16. – 18. WFS endpoint returns the response to the end user.

5.5.5 con terra PEP and Secure Dimensions PDP

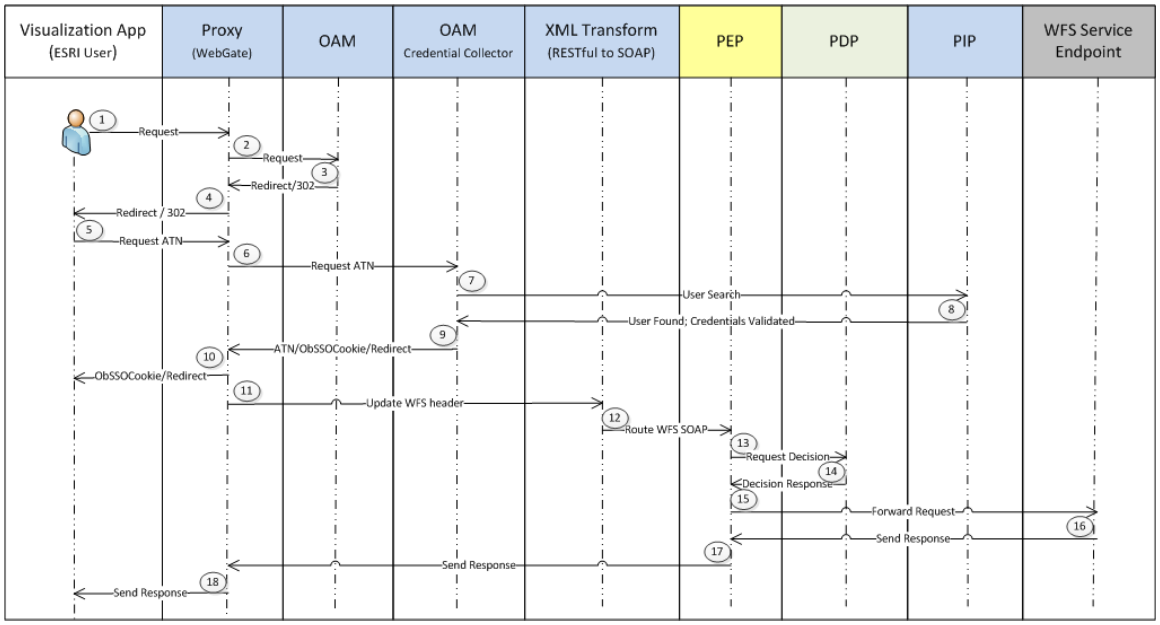


Figure 10 — Flow of communication for con terra PEP and Secure Dimensions PDP

The flow of communication is identical to 5.2.4. even though another participant provides the PDP.

5.5.6 con terra PEP and GEOAxIS PDP

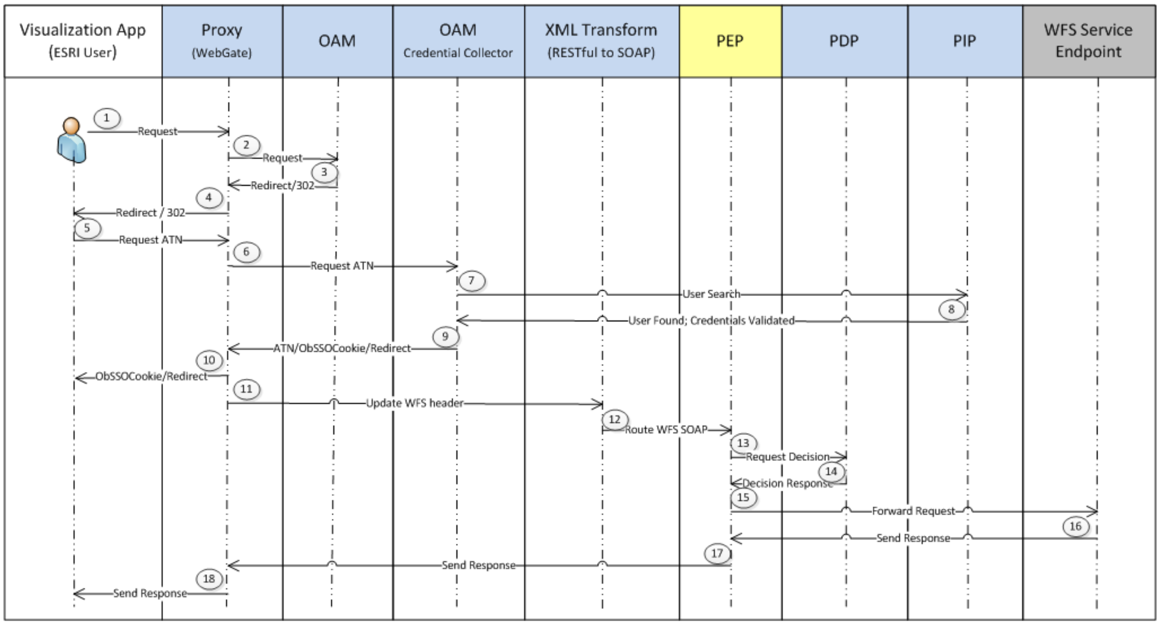


Figure 11 — Flow of communication for con terra PEP and GEOAxIS PDP

The flow of communication is identical to 5.2.4. even though another participant provides the PDP.

5.5.7 con terra PEP and Secure Dimensions PDP

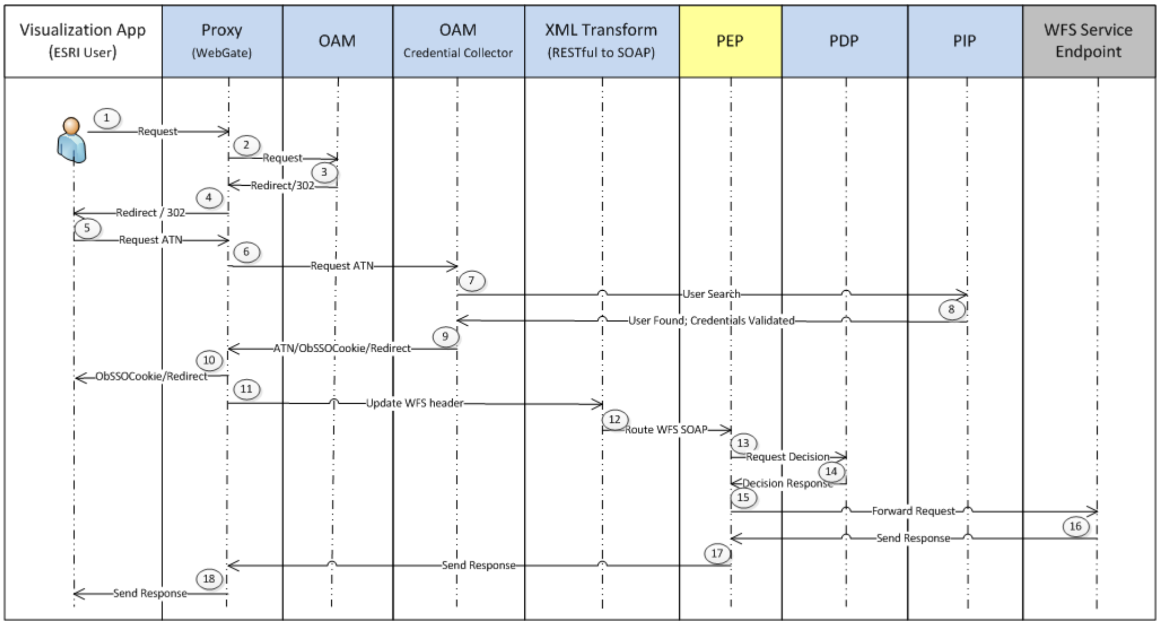


Figure 12 — Flow of communication for con terra PEP and GEOAxIS PDP

The flow of communication is identical to 5.2.4. even though another participant provides the PDP.

5.6 Interoperability Test PDP / Policy

One interoperability test undertaken during OWS-9 focuses on the ability to share policies. This is a vital pre-requisite to support the decision making where the PEP and the PDP is not provided by the same participant. As illustrated in figure 5.2.1, the GEOAxIS PEP leverages the con terra PDP (interactions 4/5) and Secure Dimensions PDP (interactions D2/E2); and the con terra PEP leverages the GEOAxIS PDP (interacitons 9/10) and Secure Dimensions PDP (interactions 6/7).
It is important to understand that it is essential that the policy, associated to a particular PEP supports the processing semantics of that particular PEP. For OWS-9, GEOAxIS and con terra created their own policies which was loaded by their own PDP but also by the other participants PDPs.
The following matrix introduces the tested combinations and the results.

PDP \ Policy provider	GEOAxIS	con terra
GEOAxIS PDP	n/a[1)]	∞
con terra PDP	∞	n/a[1)]
Secure Dimensions PDP	∞	√

Table 1 — PDP / Policy interoperability

These symbols used in the matrix have the following meaning:

√: PDP loads and executes other participant policy with no errors

×: PDP loads and executes other participant policy with errors

∞: PDP loading other participant policy was not tested

1) There is no interoperability proof if the policy and the PDP is provided by the same participant; so this is n/a.

5.6.1 GEOAxIS XACML Import/Export

GEOAxIS PDP supports XACML 2.0 and is compliant with XACML 3.0 specifications. It currently does not support the capability to import or export XACML policy. This capability is expected to be provided by the vendor in a future release. The GEOAxIS PAP was used to construct policies to mirror those that were created by the SecureDimensions PAP.

n/a There is no interoperability proof if the policy and the PDP is provided by the same participant.

5.6.2 con terra PDP with GEOAxIS Policy

∞ Since no XACML 2.0-compliant policy from GEOAxIS was available during the implementation phase of this testbed the con terra PDP was not tested with policies originating from GEOAxIS.

5.6.3 Secure Dimensions PDP with con terra Policy

√ The Secure Dimensions PDP was successfully tested with con terra-created policies. ADR's are accepted and AD's are issues as expected.

5.7 Interoperability Test Results for PEP / PDP Communication

In order to capture the results concerning the interoperability tests between the PEP and PDP components provided by different participants, the following matrix shows the test results in a compact fashion.

PDP \ PEP Interoperability	GEOAxIS PEP	con terra PEP
GEOAxIS PDP	n/a[1)]	√
con terra PDP	√	n/a[1)]
Secure Dimensions PDP	∞	√

Table 2 — PDP / PEP communication interoperability

These symbols used in the matrix have the following meaning:

√: PEP and PDP communication was tested and works as expected

×: PEP and PDP communication was tested but does not work.

∞: PEP and PDP communication was not tested

5.7.1 GEOAXiS PEP with con terra and Secure Dimensions PDP

In support of interoperability, connectivity testing was performed between ESRI, GEOAxIS, Carbon Services, Conterra, Interactive Instruments and Secure Dimensions to identify and correct any network and firewall related issues. Connectivity with WFS providers was demonstrated using simple invocations of GetCapabilities and GetFeature WFS requests for each service provider.

During this effort the visualization application was tested to determine that it could successfully authenticate with the GEOAxIS infrastructure and maintain session state. Without this capability, user identity could not be propagated and security policy enforcement would ultimately fail. Client applications need to support HTTP redirects (302) as well as session persistence mechanisms with cookies and headers. It was discovered that the ESRI client was not able to support this protocol. As a result, an instance of a SilverLight client was modified to act as the visualization application.

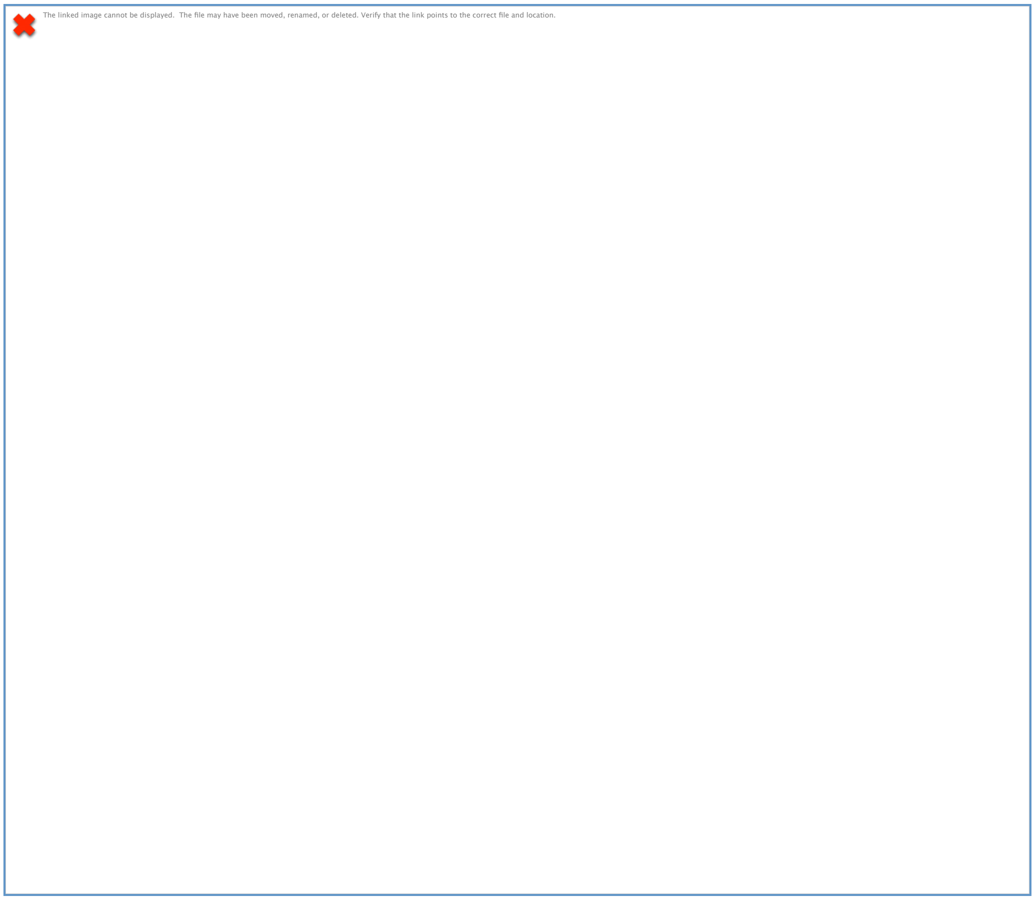
Additional testing was conducted to ensure that XACML request and response messages could be exchanged and successfully processed by partners.

5.7.1.1 Interoperability Testing Issues

During testing, it was discovered that PEP clients needed to understand the encoding scheme of their PDP partners. Specifically, PEP and PDP needed to agree upon the format of data contained within the <Resource> and <Action> elements in the XACML request messages. If a PEP client did not encode the data in a manner that the PDP expected, the result would either be a XACML Deny or NotApplicable response. These were the only two instances where this situation was encountered during testing, however, there may be other instances if additional XACML components are configured.

In this case, it appears that the encoding scheme provides the PDP with the ability to parse the input strings in a consistent manner and map them to internal data structures, stored policies and resources.

This discovery resulted in development of custom transformations implemented at the GEOAxIS PEP to accommodate the various data encoding requirements of the participating PDPs. Transformations were performed on both inbound and outbound XACML message flows to reconcile these structural differences. Although this situation was encountered in a small test environment with limited impact, in a large scale enterprise deployment, this could have considerable impacts on scalability, performance and maintainability of an enterprise security solution that relies heavily on XACML. According to the XACML standard, there is the concept of a Context Handler. The context handler, as identified in Figure 1 in the XACML standard, is described as a component that sits between any interface with a PDP. The interface could be a resource, a PEP, or a PIP.


The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the correct file and location.

According to the XACML specification, the Context Handler is 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. Within the scope of this exercise, the Context Handler function is provided by the GEOAxIS PEP. However, it does not conform to the strict definition of the Context Handler within the specification. It does not perform translation from non-XACML authorization requests to XACML, but rather, is responsible for initiating the the interaction to the PDP by generating XACML request messages and forwarding them onto the PDP and enforcing decision responses.

Additionally, the GEOAxIS PEP is responsible for performing translation services for each PDP it interacts with. It also provides application and protocol translation, for example, converting OGC RESTful formatted request messages to SOAP messages. Based upon insight gained during this effort, GEOAxIS believes that the XACML standard should be enhanced to provide guidance on how to resolve such interoperability issues. Options to address this issue in the XACML standard include:

- Require PDP service providers to include data and encoding constraints in a service definition

- Provide guidance on a common data structure format that PDP providers can publish to PEPs to reduce or eliminate exposing internal data mapping schemes to PEP consumers
- Expand the description of the Context Handler to introduce a translation service component that provides, among other things, message structure translation capability, protocol translation services and syntax or semantics checking

5.7.1.2 Obligation Processing

Additional transformations were created to accommodate the use of obligations in the XACML PDP responses. These obligations were returned as Base64 encoded strings containing OGC Filters. Base64 was used to simplify persistence options at the PDP. These transformations decoded the Base64 encoded obligation strings and redacted the WFS POST request to contain the OGC filter XML segment.

5.7.2 con terra PEP with GEOAxIS PDP

√ One separate instance of a con terra PEP was set up to request AD's from the GEOAxIS PDP. The PEP was able to connect to the PDP, send ADR's, and process the AD's.

5.7.3 con terra PEP with Secure Dimensions PDP

√ One separate instance of a con terra PEP was set up to request AD's from the Secure Dimensions PDP working on the con terra created policy. The PEP was able to connect to the PDP, send ADR's, and process the AD's.

5.8 Functionality Test Results for PEP / PDP

In terms of functionality, it is important that each possible PEP / PDP pair enforces the identified access rights correctly. The following TIE matrix captures the test results regarding the correct enforcement of the defined access rights.

PDP \ PEP	GEOAxIS PEP	con terra PEP
GEOAxIS PDP		×
con terra PDP		√
Secure Dimensions PDP	∞	√

Table 3 — PDP / PEP functional results

These symbols used in the matrix have the following meaning:

√: this combination of PEP/PDP enforces the access rights as defined
×: this combination of PEP/PDP does not enforce the access rights as defined
∞: this combination of PEP/PDP was not tested

5.8.1 GEOAxIS PEP with con terra and Secure Dimensions PDP

The PEP and PDP communications testing was driven by the SilverLight client application. The application was hosted on a GEOAxIS server and protected by the

GEOAxIS infrastructure. Users were challenged to authenticate and issued security tokens and headers as described above.

Once a user was authenticated, they would register the WFS using a widget on the client. The user would input the URL of the target service, then search on that service. That search action would result in a GetCapabilities call to the target service. The result on the client was a display of the available layers and features. The user would then select the desired features from the layer and enable them to be visible. The selection of the feature resulted in a GetFeature POST call to the GEOAxIS infrastructure and routed accordingly. Additionally, the GET and POST links in the GetCapabilities needed to be transformed on the response to the client to contain the GEOAxIS URL instead of the service provider URL.

The GEOAxIS proxy servers were configured to route traffic to different servers based upon URI. For example, the /xsprojects URI would map Interactive Instrument requests to an XML Firewall instance installed on GEOAxIS that routed PDP requests to Conterra. URI patterns for /wfs would route Carbon Service PDP requests to the GEOAxIS PDP. Changing routing to backends was simply a matter of reconfiguring the proxy server to hit the appropriate XML Firewall.

Additional XML Firewall configurations were enabled to demonstrate functionality that converted RESTful service calls to SOAP with SAML headers, responded to XACML requests from Conterra, and called out to Secure Dimensions PDP.

5.8.2 con terra PEP with con terra PDP

√ The con terra PEP was able to enforce the PDP's authorization decisions as expected. This includes enforcement of access restrictions to single feature types as well as request rewriting (application of Filter Encoding statements) and request filtering (removing denied feature types from a capabilities document).

5.8.3 con terra PEP with GEOAxIS PDP

√ The con terra PEP was able to enforce the PDP's authorization decisions as expected. The enforcement of obligations was not tested due to lack of an according policy.

5.8.4 con terra PEP with Secure Dimensions PDP

√ The con terra PEP was able to enforce the PDP's authorization decisions as expected. This includes enforcement of access restrictions to single feature types as well as request rewriting (application of Filter Encoding statements) and request filtering (removing denied feature types from a capabilities document).

6 Cross Thread Security

As defined in the OWS9 master scenario, different actors must discover data sets, partically served by protected Web Feature Services. According to that scenario, the security approach for the CCI cross thread security includes two major objectives:

- Filtering of Catalogue responses in a coarse grained fashion, according to the need-to-know principle: The user can query the catalogue service, but the response is going to be filtered, matching the user's ability to not see restricted service endpoints.

- Access Control in place for Web Feature Services in a fine grained fashion to ensure that denied data sets, down to the location of a feature or characteristics of the feature, are not accessible.

6.1 Use Case

The full use case description – as a 100% copy from the OWS9 portal – can be found in the annex A to this document.

Regarding security, the following sub sequence of the use case is important: An actor of the Integrated Client undertakes a catalogue search for determining Web Feature Services that provide data sets on Haiti and Monterey. The user leverages a Cataloge Service for the Web (CSW) interface. The result of the search is presented as an OWSContext document where particular portions are filtered according to the need-to-know principle.

The user can leverage the received information to either have a client to execute a semantic mediator or execute the protected Web Feature Services (WFSs) directly.

6.2 Architecture and Deployment

A user is making a Catalogue search from a mobile application using the CSW 2.0.2 interface. The response retuned to the application is an OWSContext document containing all service / resource offerings matching the request for which the user has the clearance to see. In other word, the actual response is a subset of response the service produces. All service / resource offerings for which the user has no need-to-know get removed from the service response.

In order to achieve this, the following architecture is used:

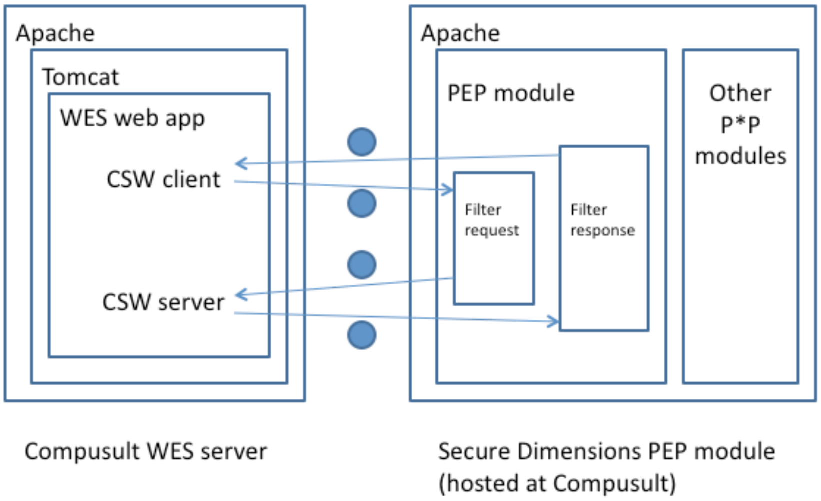


Figure 13 —Architecture to filter CSW responses based on user clearance

The sequence of interactions between the modules is described in the following sequence diagram.

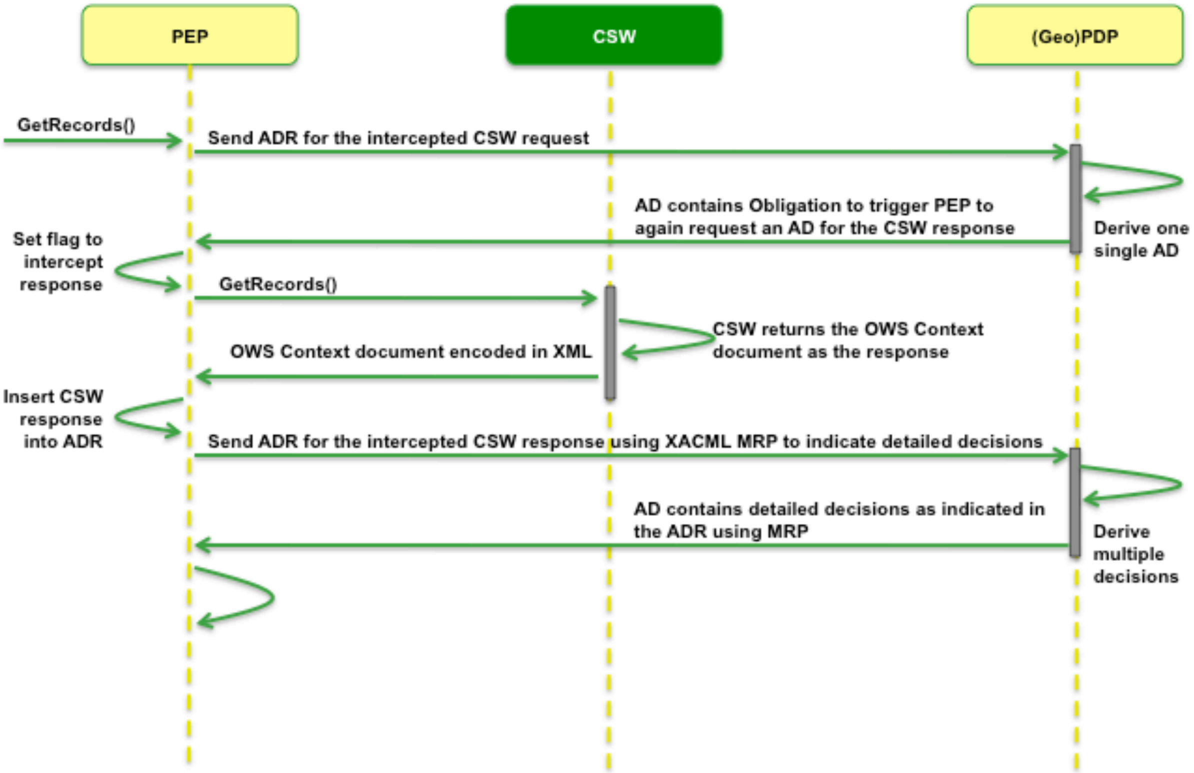

PEP
CSW
(Geo)PDP
GetRecords()
Send ADR for the intercepted CSW request
AD contains Obligation to trigger PEP to again request an AD for the CSW response
Derive one single AD
Set flag to intercept response
GetRecords()
CSW returns the OWS Context document as the response
OWS Context document encoded in XML
Insert CSW response into ADR
Send ADR for the intercepted CSW response using XACML MRP to indicate detailed decisions
AD contains detailed decisions as indicated in the ADR using MRP
Derive multiple decisions

Figure 14 — Interactions between the security components and the CSW

The following are the details for the interactions

1. A client submits a "Get Records" operation. This request is not directly executed at the CSW, instead it is intercepted by the PEP.

2. The PEP analyses the request and creates a XACML 2.0 compliant Authorization Decision Request (ADR). This ADR contains information about the user Role, all parameters of the CSW request and environment information such as Date and Time. In addition, the ADR contains information about the HTTP method and the request context -> CSW request.

3. The PEP sends the ADR to the PDP.

4. The PDP analysis the ADR and applies the policy which matches the request context (CSW request) plus user Role, CSW operation, etc.

5. The PDP finds a matching Policy and derives the Authorization Decision (AD). Because the ADR was a XACML 2.0 Core request, only one decision is included into the AD. However, the AD must be PERMIT but in order to task the PEP to request authorization decisions based on the CSW response for

the purpose of filtering, an Obligation must be included. For the Secure Dimensions PEP, this Obligation must indicate the ObligationID=to-do.

6. The PEP receives the AD and analysis it. Because the decision is PERMIT, it will continue processing the AD and find the Obligation. Processing of the Obligation id has the side effect that a flag is set to construct a XACML 2.0 MRP ADR based on the CSW response.

7. The PEP forwards the intercepted request to the CSW and receives the CSW response, e.g. a OWS Context document.

8. The further processing of the CSW response is under the flag for XACML 2.0 MRP. This requires that a ADR including MRP is constructed and that the two required parameters are copied from the Obligation, received in the AD for the CSW request. Also, the PEP must include the received CSW response into the <Resource Content> element of the ADR and the request context must be set to CSW response.

9. The ADR is send to the PDP.

10. The PDP analysis the ADR and understands, that XACML 2.0 MRP compliant processing is required. In order to do that, it must produce individual authorization decisions for each XML element of the <Resource Content> that matches the provided xpath expression in the resource-id attribute.

11. For each matching XML element, the PDP creates an individual authorization decision by analyzing the existing policy. A decision for each element comprises the resulting AD.

12. The PEP receives the AD for the intercepted CSW response and removes all those XML elements for which the authorization decision is Deny. After all authorization decisions are processed, the CSW response is filtered, meaning that all XML elements got removed for which the user has no permission to see.

13. After error free processing, the PEP forwards the shrunk CSW response to the client. It is important to note that the security was applied in an opaque fashion, so the user does not know.

This processing implies that certain criteria are met when writing the policy.

6.3 Approach to Policy writing for CSW response filtering

In order to control the sequence of interactions, as illustrated above, it is important that the Policy “deals” with an ADR concerning the intercepted CSW request. This ADR must contain an indication to the PEP that it shall allow processing of the CSW request or return a “not authorized” exception. Assuming the user indicates thru a particular role that a certain clearance is involved, then the response from the CSW is to be processed.

This is indicated to the PEP by returning an Obligation with the identifier "`urn:SD:Obligation:Response:Filter`". This will kick off PEP processing according to the XACML 2.0 Multiple Resources Profile with the semantics that "at the end" XML elements get removed from the response, for which a Deny decision exists. The required parameters for shaping the ADR using the intercepted CSW response (the OWS Context document) are contained in the Obligation.

In order to derive the desired authorization decisions, the Policy must "deal" with the XACML 2.0 MRP compliant ADR. The structure must be such that the AD comprises of many individual authorization decisions, according to the request. These decisions indicate to the PEP which XML elements are to e removed from the OWS Context document by Xpath expressions.

6.3.1 CSW Request example

http://ows9.secure-dimensions.org/service/CSW/Compusult?

REQUEST=GetRecords&SERVICE=CSW&VERSION=2.0.2&CONSTRAINTLANGUAGE=CQL_TEXT&TYPENAMES=csw:Record&RESULTTYPE=results&OUTPUTSCHEMA=http://www.isotc211.org/2005/gmd&ELEMENTSETNAME=brief

This example request will be transformed into the following ADR assuming a user with RoleA issued the request:

```
<?xml version='1.0' encoding="ISO-8859-1" standalone="no" ?>
<Request xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:os"
  xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:context:schema:os
  http://docs.oasis-open.org/xacml/access_control-xacml-2.0-context-schema-os.xsd">
  <Subject>
    <Attribute DataType="http://www.w3.org/2001/XMLSchema#string"
      AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id">
      <AttributeValue>Alice</AttributeValue>
    </Attribute>
    <Attribute DataType="http://www.w3.org/2001/XMLSchema#anyURI"
      AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role">
      <AttributeValue>A</AttributeValue>
    </Attribute>
  </Subject>
  <Resource>
    <Attribute DataType="http://www.w3.org/2001/XMLSchema#string"
      AttributeId="urn:SD:def:xacml:2.0:context">
      <AttributeValue>urn:SD:def:xacml:2.0:request</AttributeValue>
    </Attribute>
    <Attribute DataType="http://www.w3.org/2001/XMLSchema#anyURI"
      AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id">
      <AttributeValue/>
    </Attribute>
    <Attribute DataType="http://www.w3.org/2001/XMLSchema#anyURI"
      AttributeId="urn:SD:def:xacml:2.0:uri">
      <AttributeValue>/service/CSW/Compusult</AttributeValue>
    </Attribute>
    <Attribute DataType="http://www.w3.org/2001/XMLSchema#string"
      AttributeId="urn:SD:def:xacml:2.0:service">
      <AttributeValue>CSW</AttributeValue>
    </Attribute>
    <Attribute DataType="http://www.w3.org/2001/XMLSchema#string"
      AttributeId="urn:SD:def:xacml:2.0:request">
      <AttributeValue>GetRecords</AttributeValue>
    </Attribute>
    <Attribute DataType="http://www.w3.org/2001/XMLSchema#string"
      AttributeId="urn:SD:def:xacml:2.0:version">
      <AttributeValue>2.0.2</AttributeValue>
    </Attribute>
    <Attribute DataType="http://www.w3.org/2001/XMLSchema#string"
      AttributeId="urn:SD:def:xacml:2.0:resulttype">
      <AttributeValue>results</AttributeValue>
    </Attribute>
    <Attribute DataType="http://www.w3.org/2001/XMLSchema#string"
      AttributeId="urn:SD:def:xacml:2.0:">
      <AttributeValue>http://www.isotc211.org/2005/gmd</AttributeValue>
    </Attribute>
    <Attribute DataType="http://www.w3.org/2001/XMLSchema#string"
      AttributeId="urn:SD:def:xacml:2.0:elementsetname">
      <AttributeValue>brief</AttributeValue>
    </Attribute>
    <Attribute DataType="http://www.w3.org/2001/XMLSchema#string"
      AttributeId="urn:SD:def:xacml:2.0:constraintlanguage">
      <AttributeValue>CQL_TEXT</AttributeValue>
    </Attribute>
  </Resource>
  <Action>
    <Attribute DataType="http://www.w3.org/2001/XMLSchema#string"
      AttributeId="urn:SD:def:xacml:2.0:request">
      <AttributeValue>GetRecords</AttributeValue>
    </Attribute>
    <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
      DataType="http://www.w3.org/2001/XMLSchema#string">
      <AttributeValue>GET</AttributeValue>
    </Attribute>
  </Action>
  <Environment>
    <Attribute DataType="http://www.w3.org/2001/XMLSchema#date"
      AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-date">
      <AttributeValue>2012-06-12</AttributeValue>
    </Attribute>
    <Attribute DataType="http://www.w3.org/2001/XMLSchema#time"
      AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-time">
      <AttributeValue>19:54:11Z</AttributeValue>
    </Attribute>
    <Attribute DataType="http://www.w3.org/2001/XMLSchema#dateTime"
      AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-dateTime">
      <AttributeValue>2012-06-12T19:54:11Z</AttributeValue>
    </Attribute>
    <Attribute DataType="http://www.w3.org/2001/XMLSchema#string"
      AttributeId="urn:SD:def:xacml:2.0:protocol">
      <AttributeValue>HTTP/1.1</AttributeValue>
    </Attribute>
    <Attribute DataType="http://www.w3.org/2001/XMLSchema#string"
      AttributeId="urn:SD:def:xacml:2.0:hostname">
      <AttributeValue>localhost</AttributeValue>
    </Attribute>
  </Environment>
</Request>
```

Table 4 — XACML request example

6.3.2 Policy snippet

Depending on the policy in place, the ADR above can result in any authorization decision. But in order to filter the CSW response, the matching policy must return Permit and the appropriate Obligation. The following policy snippet ensures that.

```
<?xml version="1.0" encoding="UTF-8"?>
<Policy PolicyId="urn:ogc:ows9:mobile_security:policy:request:RoleA"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-
overrides">
  <Description>Policy for matching the REQUEST context -> PEP will receive an obligation
to request MRP on the RESULT context ...</Description>
  <Target>
    <Actions>
      <Action>
        <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">GetRecords</AttributeValue>
          <ActionAttributeDesignator AttributeId="urn:SD:def:xacml:2.0:request"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </ActionMatch>
      </Action>
    </Actions>
  </Target>
  <Rule RuleId="AllPermit" Effect="Permit">
    <Description>All service requests are permitted but are subject to
Obligations</Description>
    <Target>
      <Resources>
        <Resource>
          <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">urn:SD:def:xacml:2.0:request</Attribu
teValue>
            <ResourceAttributeDesignator AttributeId="urn:SD:def:xacml:2.0:context"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </ResourceMatch>
        </Resource>
      </Resources>
    </Target>
  </Rule>
  <Obligations>
    <Obligation ObligationId="urn:SD:Obligation:Response:Filter" FulfillOn="Permit">
      <AttributeAssignment AttributeId="urn:SD:def:xacml:2.0:profile:identifier"

DataType="http://www.w3.org/2001/XMLSchema#string">urn:oasis:names:tc:xacml:2.0:profile:
multiple:xpath-expression</AttributeAssignment>
      <AttributeAssignment AttributeId="urn:oasis:names:tc:xacml:2.0:resource:scope"
        DataType="http://www.w3.org/2001/XMLSchema#string">XPath-
expression</AttributeAssignment>
      <AttributeAssignment AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-
id"
        DataType="urn:oasis:names:tc:xacml:2.0:data-type:xpath-expression">./*[local-
name()='OWSContext']/*[local-name()='ResourceList']/*[local-
name()='Layer']</AttributeAssignment>
    </Obligation>
  </Obligations>
</Policy>
```

Table 5 — XACML policy snippet

6.3.3 AD for the CSW request

The following snippet illustrates the AD derived by the PDP.

```
<Response xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:os"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:context:schema:os
  access_control-xacml-2.0-context-schema-os.xsd
urn:oasis:names:tc:xacml:2.0:policy:schema:os access_control-xacml-2.0-policy-schema-
os.xsd"
```

```
  xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
  xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os">
  <Result ResourceId="">
    <Decision>Permit</Decision>
    <Status>
      <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
    </Status>
    <xacml:Obligations>
      <xacml:Obligation ObligationId="urn:SD:Obligation:Response:Filter"
FulfillOn="Permit">
        <xacml:AttributeAssignment AttributeId="urn:SD:def:xacml:2.0:profile:identifier"
          DataType="http://www.w3.org/2001/XMLSchema#string"
          >urn:oasis:names:tc:xacml:2.0:profile:multiple:xpath-
expression</xacml:AttributeAssignment>
        <xacml:AttributeAssignment
AttributeId="urn:oasis:names:tc:xacml:2.0:resource:scope"
          DataType="http://www.w3.org/2001/XMLSchema#string"
          >XPath-expression</xacml:AttributeAssignment>
        <xacml:AttributeAssignment
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
          DataType="urn:oasis:names:tc:xacml:2.0:data-type:xpath-expression"
          >/*[local-name()='OWSContext']/*[local-name()='ResourceList']/*[local-
name()='Layer']</xacml:AttributeAssignment>
      </xacml:Obligation>
    </xacml:Obligations>
  </Result>
</Response>
```

Table 6 — XACML response example

6.3.4 ADR for the CSW response

The following snippet illustrated the example ADR for the CSW response.

```
<?xml version="1.0" encoding="UTF-8"?>
<Request xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:os"
  xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:context:schema:os
  http://docs.oasis-open.org/xacml/access_control-xacml-2.0-context-schema-os.xsd">
  <Subject>
    <Attribute DataType="http://www.w3.org/2001/XMLSchema#anyURI"
      AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role">
      <AttributeValue>A</AttributeValue>
    </Attribute>
  </Subject>
  <Resource>
    <ResourceContent>
      <OWSContext version="0.2.1"
        id="ows-context"
        xmlns="http://www.opengis.net/ows-context/0.2.1"
        xmlns:xlink="http://www.w3.org/1999/xlink"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xmlns:sld="http://www.opengis.net/sld"
        xmlns:ogc="http://www.opengis.net/ows-context/0.2.1"
        xmlns:ows="http://www.opengis.net/ows"
        xmlns:param="http;//www.opengis.net/param"
        xsi:schemaLocation="http://www.opengis.net/ows-context/0.2.1 ./owsContext.xsd">
        <General>
          <Window width="500" height="300"/>
          <ows:BoundingBox crs="EPSG:4326">
            <ows:LowerCorner>-71.1485566986829 42.2593928033786</ows:LowerCorner>
            <ows:UpperCorner>-71.0016725358029 42.4399863588876</ows:UpperCorner>
          </ows:BoundingBox>
          <ows:Title>OWS Context Document</ows:Title>
          <ows:Abstract>The OpenGIS Web Services Context Document</ows:Abstract>
          <ows:Keywords>
            <ows:Keyword>MassGIS</ows:Keyword>
            <ows:Keyword>Boston</ows:Keyword>
            <ows:Keyword>Massachusetts</ows:Keyword>
          </ows:Keywords>
          <LogoURL width="140" height="65" format="image/gif">
            <OnlineResource xlink:type="simple"
              xlink:href="http://www.opengis.org/img/ogc_header_top_left.gif"/>
          </LogoURL>
          <DescriptionURL format="text/html">
            <OnlineResource xlink:type="simple"

xlink:href="http://www.opengis.org/press/?page=pressrelease&amp;view=20040525_ContextIE_PR
"/>
          </DescriptionURL>
          <ows:ServiceProvider>
            <ows:ProviderName>Environment Canada</ows:ProviderName>

            <ows:ProviderSite xlink:type="simple" xlink:href="http://www.ec.gc.ca/"/>
            <ows:ServiceContact>
              <ows:IndividualName>Tom Kralidis</ows:IndividualName>
              <ows:PositionName>Senior Systems Scientist</ows:PositionName>
              <ows:ContactInfo>
                <ows:Phone>
                  <ows:Voice>+01-905-336-4409</ows:Voice>

                  <ows:Facsimile>+01-905-336-4499</ows:Facsimile>
                </ows:Phone>
                <ows:Address>
                  <ows:DeliveryPoint>867 Lakeshore Road</ows:DeliveryPoint>
                  <ows:City>Burlington</ows:City>
                  <ows:AdministrativeArea>Ontario</ows:AdministrativeArea>
                  <ows:PostalCode>L7R4A6</ows:PostalCode>

                  <ows:Country>Canada</ows:Country>

<ows:ElectronicMailAddress>tom.kralidis@ec.gc.ca</ows:ElectronicMailAddress>
                </ows:Address>
                <ows:OnlineResource xlink:type="simple"
xlink:href="http://www.ec.gc.ca/"/>
                <ows:HoursOfService>0700h - 1500h (EST), Monday -
Friday</ows:HoursOfService>
                <ows:ContactInstructions>Just call or email</ows:ContactInstructions>
              </ows:ContactInfo>

              <ows:Role>Senior Systems Scientist</ows:Role>
            </ows:ServiceContact>
          </ows:ServiceProvider>
        </General>
        <ResourceList>
          <Coverage hidden="0" group="Coverages" id="93278">
            <ows:Title>MOD_Grid_L2g_2d Coverage Offering</ows:Title>
            <ows:Abstract>MOD_Grid_L2g_2d Coverage Offering, MOD09GHK data</ows:Abstract>
            <ows:Identifier>MOD_Grid_L2g_2d</ows:Identifier>
            <ows:OutputFormat>image/tiff</ows:OutputFormat>
            <ows:AvailableCRS>EPSG:4326</ows:AvailableCRS>
            <ows:BoundingBox crs="EPSG:4326">
              <ows:LowerCorner>-71.1485566986829 42.2593928033786</ows:LowerCorner>
              <ows:UpperCorner>-71.0016725358029 42.4399863588876</ows:UpperCorner>
            </ows:BoundingBox>
            <Server service="WCS" version="1.0.0" title="Boston Indexed Geotiff imagery">
              <OnlineResource method="GET" xlink:type="simple"

xlink:href="http://webservices.ionicsoft.com/ionicwcs/coverage/BOSTONPOOL"/>
            </Server>
            <MetadataURL format="text/xml">
              <OnlineResource xlink:type="simple"

xlink:href="http://webservices.ionicsoft.com/ionicwcs/coverage/BOSTONPOOL/REQUEST/getdir/D
IR/metadata/DATA/LPR/BOSTONPOOL/MOD_Grid_L2g_2d.xml"/>
```

```
            </MetadataURL>
            <DimensionList>
              <Dimension name="time" units="ISO8601">2003-12-01T14:55:00Z/2003-12-
03T20:50:00Z</Dimension>
            </DimensionList>
            <ParameterList>
              <Parameter>
                <param:kvp name="band" value="band1"/>
              </Parameter>
              <Parameter>
                <param:kvp name="interpolation" value="nearest neighbor"/>
              </Parameter>
            </ParameterList>
          </Coverage>
          <FeatureType hidden="0" group="Features" id="92756">
            <ows:Title>Landuse</ows:Title>
            <ows:Abstract>Boston Landuse Polygons</ows:Abstract>
            <ows:Identifier>Landuse</ows:Identifier>
            <ows:AvailableCRS>EPSG:26986</ows:AvailableCRS>
            <ows:BoundingBox crs="EPSG:4326">
              <ows:LowerCorner>-71.1485566986829 42.2593928033786</ows:LowerCorner>
              <ows:UpperCorner>-71.0016725358029 42.4399863588876</ows:UpperCorner>
            </ows:BoundingBox>
            <Server service="GML" version="2.1.2" title="Cadcorp GeognoSIS.NET Web Feature
Service">
              <OnlineResource xlink:type="simple"
xlink:href="http://www.cadcorpdev.co.uk/gml/MassGIS/LandUse.gml"/>
            </Server>
            <sld:MinScaleDenominator>5000</sld:MinScaleDenominator>
            <sld:MaxScaleDenominator>50000</sld:MaxScaleDenominator>
            <MaxFeatures>99</MaxFeatures>
          </FeatureType>
          <Layer queryable="0" hidden="0" group="Layers" id="2957">
            <ows:Title>hydro</ows:Title>
            <ows:Abstract>hydro</ows:Abstract>
            <ows:Identifier>hydro</ows:Identifier>
            <ows:OutputFormat>image/gif</ows:OutputFormat>
            <ows:OutputFormat>image/png</ows:OutputFormat>
            <ows:OutputFormat>image/jpeg</ows:OutputFormat>
            <ows:AvailableCRS>EPSG:4326</ows:AvailableCRS>
            <ows:BoundingBox crs="EPSG:4326">
              <ows:LowerCorner>-71.1485566986829 42.2593928033786</ows:LowerCorner>
              <ows:UpperCorner>-71.0016725358029 42.4399863588876</ows:UpperCorner>
            </ows:BoundingBox>
            <Server service="WMS" version="1.1.1" title="Boston on Oracle">
              <OnlineResource xlink:type="simple"
xlink:href="http://webservices2.ionicsoft.com/ionicweb/wfs/BOSTON_ORA"/>
            </Server>
            <sld:MinScaleDenominator>5000</sld:MinScaleDenominator>
            <sld:MaxScaleDenominator>50000</sld:MaxScaleDenominator>
            <StyleList>
              <Style current="1">
                <Name>default</Name>
                <Title>default</Title>
              </Style>
            </StyleList>
          </Layer>
          <Layer .../>
        </ResourceList>
      </OWSContext>
    </ResourceContent>
    <Attribute DataType="urn:oasis:names:tc:xacml:2.0:data-type:xpath-expression"
      AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id">
      <AttributeValue>/*[local-name()='OWSContext']/*[local-
name()='ResourceList']/*[local-name()='Layer']</AttributeValue>
    </Attribute>
    <Attribute DataType="http://www.w3.org/2001/XMLSchema#string"
      AttributeId="urn:oasis:names:tc:xacml:2.0:profile:multiple:scope">
      <AttributeValue>XPath-expression</AttributeValue>
    </Attribute>
    <Attribute DataType="http://www.w3.org/2001/XMLSchema#string"
```

```
      AttributeId="urn:SD:def:xacml:2.0:hostname">
      <AttributeValue>localhost</AttributeValue>
    </Attribute>
    <Attribute DataType="http://www.w3.org/2001/XMLSchema#anyURI"
      AttributeId="urn:SD:def:xacml:2.0:uri">
      <AttributeValue>/service/CSW/Compusult</AttributeValue>
    </Attribute>
    <Attribute DataType="http://www.w3.org/2001/XMLSchema#string"
      AttributeId="urn:SD:def:xacml:2.0:context">
      <AttributeValue>urn:SD:def:xacml:2.0:response</AttributeValue>
    </Attribute>
  </Resource>
  <Action>
    <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
      DataType="http://www.w3.org/2001/XMLSchema#string">
      <AttributeValue>Post</AttributeValue>
    </Attribute>
    <Attribute AttributeId="urn:SD:def:xacml:2.0:request"
      DataType="http://www.w3.org/2001/XMLSchema#string">
      <AttributeValue>GetRecords</AttributeValue>
    </Attribute>
  </Action>
  <Environment>
    <Attribute DataType="http://www.w3.org/2001/XMLSchema#date"
      AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-date">
      <AttributeValue>2012-06-08</AttributeValue>
    </Attribute>
    <Attribute DataType="http://www.w3.org/2001/XMLSchema#time"
      AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-time">
      <AttributeValue>09:28:27Z</AttributeValue>
    </Attribute>
    <Attribute DataType="http://www.w3.org/2001/XMLSchema#dateTime"
      AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-dateTime">
      <AttributeValue>2012-06-08T09:28:27Z</AttributeValue>
    </Attribute>
  </Environment>
</Request>
```

Table 7 — XACML MRP request example

6.3.5 AD for the CSW response ADR

The following snippet illustrates the details of the AD received from the PDP.

```
<Response xmlns='urn:oasis:names:tc:xacml:2.0:context:schema:os'
  xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'
  xsi:schemaLocation='urn:oasis:names:tc:xacml:2.0:context:schema:os
  access_control-xacml-2.0-context-schema-os.xsd
  urn:oasis:names:tc:xacml:2.0:policy:schema:os
  access_control-xacml-2.0-policy-schema-os.xsd'
  xmlns:xacml='urn:oasis:names:tc:xacml:2.0:policy:schema:os'
  xmlns:xacml-context='urn:oasis:names:tc:xacml:2.0:context:schema:os'>
<Result ResourceId="/*[local-name()='OWSContext'][1]/*[local-
name()='ResourceList'][1]/*[local-name()='Layer'][3]">
<Decision>Permit</Decision>
<Status>
<StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
</Status>
</Result>
<Result ResourceId="/*[local-name()='OWSContext'][1]/*[local-
name()='ResourceList'][1]/*[local-name()='Layer'][1]">
<Decision>Deny</Decision>
<Status>
<StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
</Status>
</Result>
<Result ResourceId="/*[local-name()='OWSContext'][1]/*[local-
name()='ResourceList'][1]/*[local-name()='Layer'][2]">
<Decision>Permit</Decision>
<Status>
<StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
</Status>
</Result>
</Response>
```

Table 8 — XACML MRP response example

Processing of the AD above has the effect that the PEP removes that XML element from the CSW response, which is referenced by the following xpath expression:

```
/*[local-name()='OWSContext'][1]/*[local-name()='ResourceList'][1]/*[local-
name()='Layer'][1]">
```

This XML element actually represents the following resource listing in the OWS Context document:

```
<?xml version="1.0" encoding="UTF-8"?>
<Layer queryable="0" hidden="0" group="Layers" id="2957">
  <ows:Title>hydro</ows:Title>
  <ows:Abstract>hydro</ows:Abstract>
  <ows:Identifier>hydro</ows:Identifier>
  <ows:OutputFormat>image/gif</ows:OutputFormat>
  <ows:OutputFormat>image/png</ows:OutputFormat>
  <ows:OutputFormat>image/jpeg</ows:OutputFormat>
  <ows:AvailableCRS>EPSG:4326</ows:AvailableCRS>
  <ows:BoundingBox crs="EPSG:4326">
    <ows:LowerCorner>-71.1485566986829 42.2593928033786</ows:LowerCorner>
    <ows:UpperCorner>-71.0016725358029 42.4399863588876</ows:UpperCorner>
  </ows:BoundingBox>
  <Server service="WMS" version="1.1.1" title="Boston on Oracle">
    <OnlineResource xlink:type="simple"
xlink:href="http://webservices2.ionicsoft.com/ionicweb/wfs/BOSTON_ORA"/>
  </Server>
  <sld:MinScaleDenominator>5000</sld:MinScaleDenominator>
  <sld:MaxScaleDenominator>50000</sld:MaxScaleDenominator>
  <StyleList>
    <Style current="1">
      <Name>default</Name>
      <Title>default</Title>
    </Style>
  </StyleList>
</Layer>
```

Table 9 — OWS Context example

6.4 Access Management to the CSW and the WFSs

For the CCI cross thread security, the same users and access rights are defined as for the SSI thread. However, additional access constraints refering to the need-to-know principle are defined for the CSW.

6.4.1 Protected data sets and services

For the CCI cross thread security activity, the following Web Feature Service instances are deployed:

Haiti data sets:

WFS abbreviation	WFS URL
USGS	http://ows9.secure-dimensions.org/service/WFS/USGS
VGI	http://ows9.secure-dimensions.org/service/WFS/VGI
MINUSTAH	http://ows9.secure-dimensions.org/service/WFS/MINUSTAH

Table 10 — Haiti data set WFS URLs

Monterey data sets:

WFS abbreviation	WFS URL
NGA	http://ows9.secure-dimensions.org/service/WFS/NGA

Table 11 — Monterey data set WFS URLs

Each service endpoint enforces the access rights as defined for the SSI thread as it got introduced in the SSI security section above.

6.4.2 CSW Access Rights

The concern with the catalogue is that a user must only see records according to the need-to-know principle. In order to enforce these access constraints, the CSW for the CCI cross thread activity is protected and the response is filtered based on the rights of the user. The protected services for the Haiti and Montrey data set can be discovered through the following CSW end point:

http://ows-9-ext.compusult.net/service/CSW/CCI

The discovery of the different service records is constrained as follows:

User	Access Rights	How is the CSW response modified?

Chief	All WFS can be discovered	n/a
Placebo	Cannot discover any of the WFS above	All records of the above WFSs (USGS, VGI, MINUSTAH, NGA) are removed from the response and the attribute "numberofMatchesReturned" is modified accordingly.
HResponder HAnalyst	Can discover the USGS, VGI and MINUSTAH WFS Can discover the NGA WFS but **not** the service endpoint.	The service endpoint for the NGA WFS is removed from the result record if present. So the user can see the NGA WFS record but not execute it because the service endpoint is missing.
Mresponder MAnalyst	All WFS can be discovered	n/a

Table 12 — Access Rights for CSW

6.5 Deployment and Flow of Information

As we can see in the illustration of the deployment below, different flows of information are possible:

1) The Integrated Client interacts with the Catalogue service (CSW) and the user searches for applicable services. The client then excutes the WFS directly, hence bypassing the middleware service.

2) The Integrated Client interacts with the middleware service, eg. a semantic mediation service or a WPS, which acts on the client's behalf. In order to get the user identity to the CSW and the WFS, it is required that the middleware service forwards the user identity, e.g. as a dedicated HTTP header. If the middleware service is secured by HTTP basic authentication for example, it could use that information and insert it into the decicated HTTP header when executing the CSW or the WFSs.

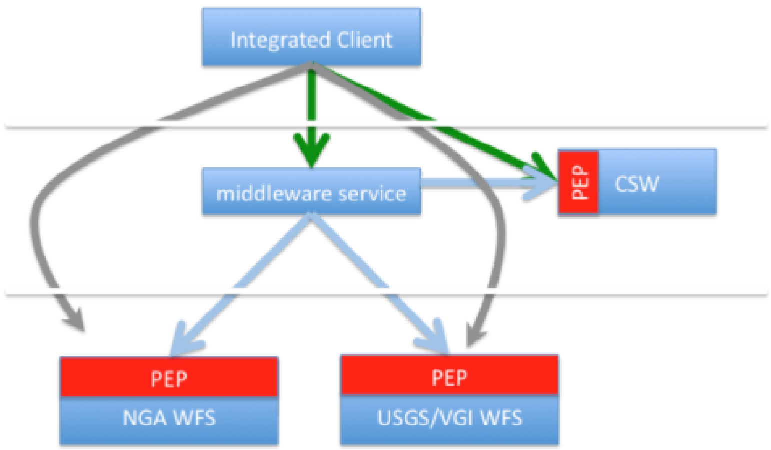


Figure 15 — CCI Cross-Thread Architecture including security components

6.6 Security Requirements

For the sake of enforcing access rights based on the user identity, it is required that each protected service – hence the PEP – receives user identity information with each request. For the service architecture illustrated above, two different interaction patterns – according to OGC Topic 12 - can be identified:

- Transparent Chaining: The client has a direct communication with the protected service and it is the user controlling the interaction.

- Opaque Chaining: The client has only direct communication with the middleware service (e.g. a workflow service) and then the middleware service executes the backend services; the WFSs in this case.

In terms of authentication, the transparent chaining is straight forward: Each PEP endpoint can be setup to require HTTP Basic Authentication. This requires the client to provide the HTTP Header "Authorization" as recommended by IETF 2617. But for the opaque chaining, the question is how does the identity information make it to the underlying WFSs. Various options exist that invlove WS-Security or the use of custom HTTP headers. For OWS9, the recommendation to use HTTP headers was named in favor over WS-Security at the kick-of meeting.

The proposal for the CCI cross thread security activity is to use the HTTP header named `SUBJECT_ROLE` to carry the information of the user's role. As an alternative, if user roles are not supported, the user identity could be placed inside that custom HTTP header.

An example flow of communication involving the WFS Semantic Mediator service is outlined in the sequence diagram below.

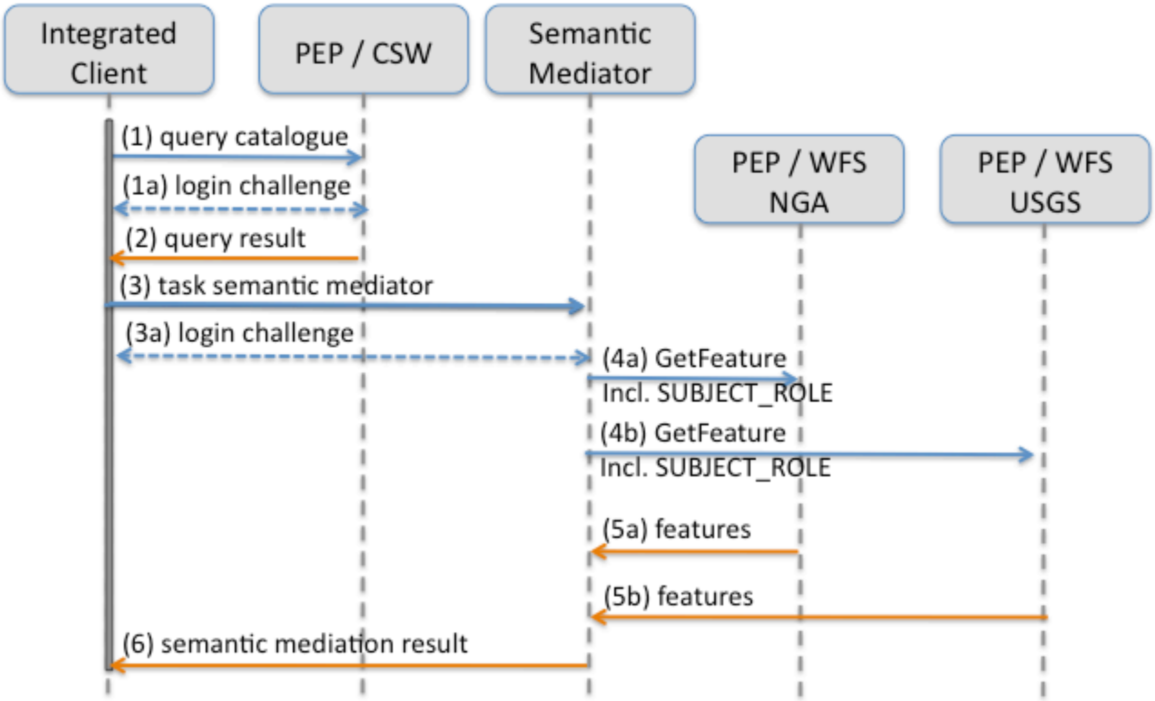


Figure 16 — CCI Cross-Thread example interactions between components

In more detail, the sequence of interactions are such:

- (1) The Integrated Client is executing the CSW to undertake a catalogue query. Because this service endpoint is protected by a PEP which enforces access constraints upon a user role, the user must login first.

- (1a) The PEP sends the Integrated client the basic authentication challenge. After the user has logged in, she must select a role that is to be used on any future requests, in particular to the CSW and the Semantic Mediator.

- (2) The CSW returns the FILTERED query result. Because the user is unaware of how much of the matching records gets filtered, this response can potentially be empty!

- (3) Based on the result from the catalogue, the user selects the resources to be used and tasks the semantic mediator. Because this service is protected, the user must login in.

- (3a) The Semantic Mediator is sending the Integrated Client the login challenge. After a successful login, the user's role gets attached to the request as an HTTP Header named SUBJECT_ROLE.

- (4a, 5a) The Semantic Mediator executes the WFSs. Because these services are Back-Office services, the Semantic Mediator must not response to a http basic login challenge. However, in order to enforce access rights based on the user's role, the request must contain the HTTP Header named SUBJECT_ROLE.

- (4b, 5b) The WFS / PEP returns the filtered response to the Semantic Mediator. It is important to note that the result could not contain a feature at all, depending on the request and the access constraints in place.
- (6) The Semantic Mediator returns the result to the Integrated Client.

6.7 Pros / Cons of the security approach above

The big pro of the approach is that it uses simplified authentication (HTTP Basic Authentication). The direct cons resulting from that is that the user must login with the CSW and the Semantic Mediator separately. Because of that, the use of the "services" is not seamless. The direct implication from that is the access control in place with the CSW and the WFS MUST be harmonized. But because it is not possible with the separate user management (at the CSW and the Semantic Mediator) to ensure that the user takes the same login at both services such that the access right enforcement fits. It is also a con that the role management is kept separate with each service's user management.

In any case where a user does pick different roles with using the CSW and the Semantic Mediator, there is a good likelihood that the user cannot use the system at all or the result is bogus. In the extreme case, where the user picks two different roles which have disjoint access rights on the CSW and the WFSs, the user may (i) receive CSW results containing WFS endpoints that cannot be executed; (ii) user may not receive records for WFSs even though she had access rights.

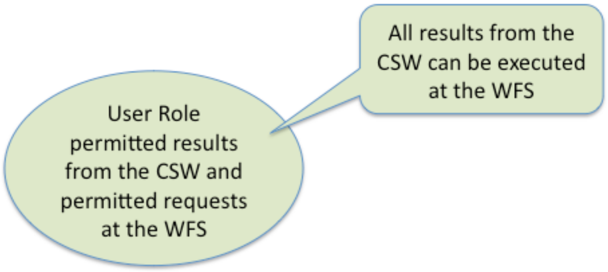

All results from the CSW can be executed at the WFS
User Role permitted results from the CSW and permitted requests at the WFS

Figure 17 — Roles and Access Rights for CSW and WFS are harmonized

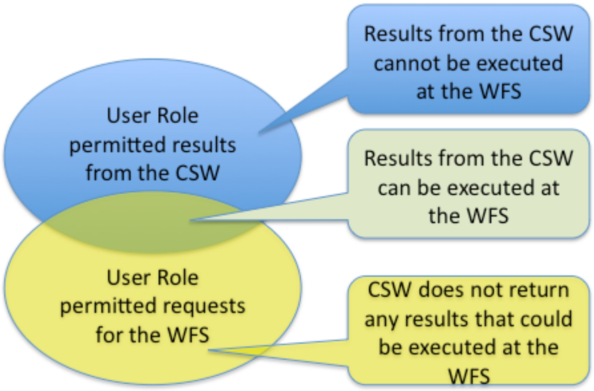

User Role permitted results from the CSW
User Role permitted requests for the WFS
Results from the CSW cannot be executed at the WFS
Results from the CSW can be executed at the WFS
CSW does not return any results that could be executed at the WFS

Figure 18 — Roles and Access Rights for CSW and WFS are not harmonized

6.8 Possible way to improve the security approach above

In order to improve the situation above for the user, a single-sign-on would ensure that the services could be used more seamlessly. But the more important point is that the single-sign-on with another entity, and sharing the user credentials among the CSW and the Semantic Mediator, would guarantee the possibility to harmonize access rights at the CSW and the Semantic Mediator. This is because with single sign on, always the same user credentials are used with the CSW and the Semantic Mediator and therefore the WFSs. In order to enable this guarantee, that always the same credentials are used among different services is considered an access management federation. A possible implementation can be based on the OASIS standard Security Assertion Markup Language (SAML).

The other improvement would be that the user / role management must not take place at each service provider. Instead the commonly trusted entity, called an Identity Provider, would take care about this. At login, the user must select the role which is going to be used on all services of the federation.

Single-Sign-On would also allow the separation of the login flow from the interactions with the services. Such, the user could use the Integrated Client first to authenticate with the Identity Provider. Once that step is completed, the user could commence the CSW and then the Semantic Mediator which no additional login.

Because SAML enables to separate the communication required to exchange security assertions (e.g. user credentials) and the actual OGC service requests, the Semantic Mediator must not provide Role management; instead it could "simply" use the user Role provided in the user credentials and forward that to the WFSs. However, the client might have to implement some security, depending if it is a Web Browser based client or not. In case the Integrated Client where some Web Browser based client using JavaScript, potentially no changes to the client where required. In case the client where a desktop client (e.g. C++ or Java implementation), the implementation of the SAML2 Profile ECP and the PAOS Binding where required.

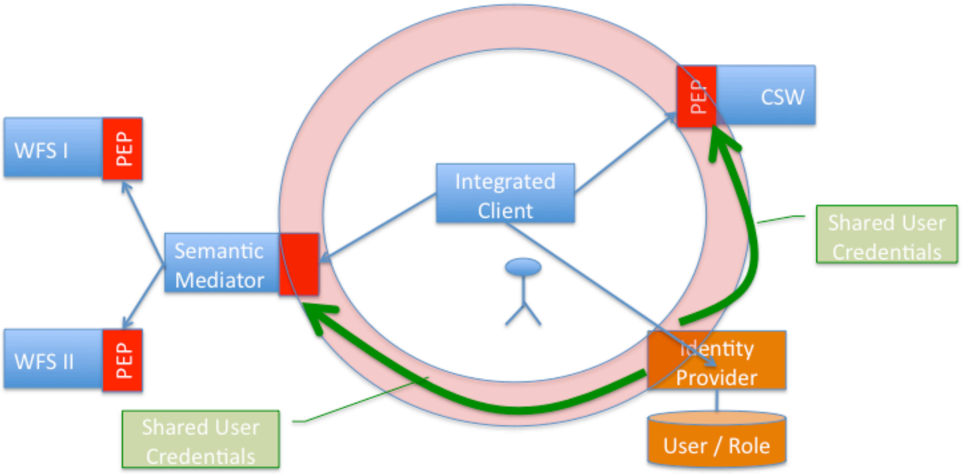


Figure 19 — Federated Approach

7 WFS Request Rewriting vs. Response Filtering (SSI Thread Scenario)

For the SSI thread, the master scenario requires from the access control system in place for the Monterey data to enforce conditions on spatial and temporal characteristics of features. Because the features are served by a WFS 2.0, it is the main goal of the security solution in place to "challenge" the WFS standard interface such, that the conditions can be enforced.

Different feature types are served by one WFS instance. But, different access restrictions are in place for different feature types. For example, a Monterey Analyst can see all features regardless of type and regardles of the security tagging. However, a Monterey Responder can not see those features that are tagged secret or tagged alternatively secret and the request is within a given time window.

7.1 Motivation for an Access Control System with Request Rewriting

Even though the WFS supports a request where all those features are not fetched which property has a certain value using the OWS Filter mechanism, the client will not create the request as such.

The problem is that the client is not aware of any access restrictions at the service side and therefore would simply issue WFS requests regardless if they meet the access rights of the current user. It is therefore the job of the security component – to be placed within the information flow between the client and the service – to modify the client request such that it meets the access rights of the user before forwarded to the WFS.

WFS request rewriting has its limitations. The limitations arrive from the WFS implementation / the version implemented. Basically, all those access rights could be enforced that can be represented by a standard compliant WFS request. Understanding the WFS request as a SQL select statement, the important bit is the WHERE clause. For a WFS, this is represented by the OWS Filter. Basically, all access rights could be enforced for which a OWS FILTER expression can be created.

Constraints on	Rewriting requirement	Can be enforced using request rewriting
Feature type	Requires to modify the parameter `typeNames`	Yes
Feature instance through string property value condition	Requires to modify the parameter `FILTER` or to create one reflecting the conditions	Yes
Feature instance through spatial	Requires to modify the parameter `FILTER`	Yes, but limited to topological conditions

property value condition	or to create one reflecting the conditions	(must be implemented by WFS)
Feature instance through temporal property value condition	Requires to modify the parameter `FILTER` or to create one reflecting the conditions	Maybe[1]
Feature instance but only certain properties	Requires to modify the parameter `propertyNames`	Yes, but restricted properties must not be mandatory in the schema[2]

Table 13 — OWS Filter outreach on WFS request re-writing

The following simplified arechitecture illustrates the security solution invloving the XACML 2.0 standard and the recommended components

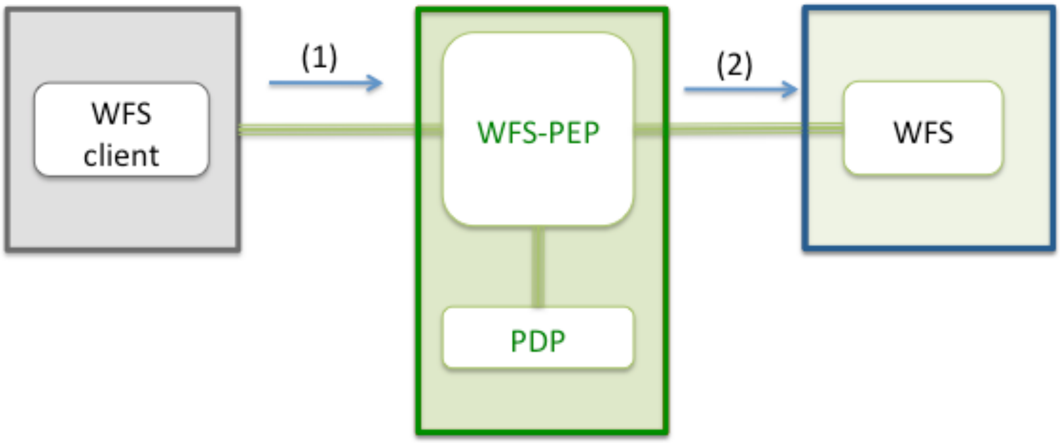


Figure 20 — WFS Access Control **(request rewriting)**

Presuming that a constrain exists for the feature type `tds:BuildingGeosurface` and that the user may only see those feature instances that are not marked secret through security marking on property `tds:restriction.securityAttributesGroup_resClassification`, the following request rewriting must take place inside the green box:

(1) – Request from the client:

[1] Depending on the implemented FILTER condition functions. In case no temporal condition functions are implemented, the use of date or time related conditions in the Filter is not possible.

[2] WFS must return a valid response and therefore include all those properties which are mandatory in the schema, regardless if explicitly requested.

```
/…/wfs?service=WFS&request=GetFeature&version=2.0.0&srsName=urn:ogc:def:crs:EPSG::4326&ty
peNames=tds:BuildingGeosurface&namespaces=xmlns(tds,http%3A%2F%2Fmetadata.dod.mil%2Fmdr%2
Fns%2FGSIP%2F3.0%2Ftds%2F3.0
```

(2) – Request to the WFS

```
/…/wfs?service=WFS&request=GetFeature&version=2.0.0&srsName=urn:ogc:def:crs:EPSG::4326&ty
peNames=tds:BuildingGeosurface&namespaces=xmlns(tds,http%3A%2F%2Fmetadata.dod.mil%2Fmdr%2
Fns%2FGSIP%2F3.0%2Ftds%2F3.0)&
       FILTER=<fes:Filter xmlns:fes="http://www.opengis.net/fes/2.0"
xmlns:tds="http://metadata.dod.mil/mdr/ns/GSIP/3.0/tds/3.0"><fes:PropertyIsNotEqualTo><fe
s:ValueReference>tds:restriction.securityAttributesGroup_resClassification</fes:ValueRefe
rence><fes:Literal>S</fes:Literal></fes:PropertyIsNotEqualTo></fes:Filter>
```

Presuming tha a constraint exists regarding security tagging but only being effective for a certain time window, the corresponding filter expression would look like this[3]:

```
<fes:Filter xmlns:fes="http://www.opengis.net/fes/2.0"
xmlns:gml="http://www.opengis.net/gml/3.2"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.opengis.net/fes/2.0
  http://schemas.opengis.net/filter/2.0/filterAll.xsd
  http://www.opengis.net/gml/3.2
  http://schemas.opengis.net/gml/3.2.1/gml.xsd">
  <fes:Not>
    <fes:And>
      <fes:PropertyIsEqualTo>
<fes:ValueReference>tds:restriction.securityAttributesGroup_resClassification</fes:Value
Reference>
        <fes:Literal>S</fes:Literal>
      </fes:PropertyIsEqualTo>
      <fes:After>
<fes:ValueReference>tds:restriction.securityAttributesGroup_resClassificationAlternateDa
teInterval_low</fes:ValueReference>
        <gml:TimeInstant gml:id="now.1">
          <gml:timePosition>2012-10-22T10:00:00Z</gml:timePosition>
        </gml:TimeInstant>
      </fes:After>
      <fes:Before>
<fes:ValueReference>tds:restriction.securityAttributesGroup_resClassificationAlternateDa
teInterval_high</fes:ValueReference>
        <gml:TimeInstant gml:id="now.2">
          <gml:timePosition>2012-10-22T10:00:00Z</gml:timePosition>
        </gml:TimeInstant>
      </fes:Before>
    </fes:And>
  </fes:Not>
</fes:Filter>
```

Table 14 — OWS Filter example leveraging dateTime functions

The above filter expression leverages from the Filter specification logical operands (**fes:Not** and **fes:And**), string operand (**fes:PropertyIsEqualTo**) and temporal operands (**fes:Before** and **fes:After**).

But, if such a filter expression is accepted by the WFS depends on the implementation. The capabilities document can be consulted to see which filter condition functions are implemented.

[3] Request URL for the FILTER expression:

```
/…/wfs?service=WFS&request=GetFeature&version=2.0.0&srsName=urn:ogc:def:crs:EPSG::4326&ty
peNames=tds:LandAerodromeGeosurface&namespaces=xmlns(tds,http%3A%2F%2Fmetadata.dod.mil%2F
mdr%2Fns%2FGSIP%2F3.0%2Ftds%2F3.0)&filter=
```

The following capabilities snippet exploits that the WFS has implemented some geometry, spatial, temporal and string comparison functions but not the logical condtion functions:

```
<fes:Scalar_Capabilities>
      <fes:LogicalOperators/>
      <fes:ComparisonOperators>
        <fes:ComparisonOperator name="PropertyIsEqualTo"/>
        <fes:ComparisonOperator name="PropertyIsNotEqualTo"/>
        <fes:ComparisonOperator name="PropertyIsLessThan"/>
        <fes:ComparisonOperator name="PropertyIsGreaterThan"/>
        <fes:ComparisonOperator name="PropertyIsLessThanOrEqualTo"/>
        <fes:ComparisonOperator name="PropertyIsGreaterThanOrEqualTo"/>
        <fes:ComparisonOperator name="PropertyIsLike"/>
        <fes:ComparisonOperator name="PropertyIsNull"/>
        <fes:ComparisonOperator name="PropertyIsNil"/>
        <fes:ComparisonOperator name="PropertyIsBetween"/>
      </fes:ComparisonOperators>
    </fes:Scalar_Capabilities>
    <fes:Spatial_Capabilities>
      <fes:GeometryOperands>
        <fes:GeometryOperand name="gml:Point"/>
        <fes:GeometryOperand name="gml:MultiPoint"/>
        <fes:GeometryOperand name="gml:LineString"/>
        <fes:GeometryOperand name="gml:Curve"/>
        <fes:GeometryOperand name="gml:MultiCurve"/>
        <fes:GeometryOperand name="gml:Polygon"/>
      </fes:GeometryOperands>
      <fes:SpatialOperators>
        <fes:SpatialOperator name="BBOX"/>
        <fes:SpatialOperator name="Equals"/>
        <fes:SpatialOperator name="Disjoint"/>
        <fes:SpatialOperator name="Intersects"/>
        <fes:SpatialOperator name="Touches"/>
        <fes:SpatialOperator name="Crosses"/>
        <fes:SpatialOperator name="Within"/>
        <fes:SpatialOperator name="Contains"/>
        <fes:SpatialOperator name="Overlaps"/>
        <fes:SpatialOperator name="Beyond"/>
        <fes:SpatialOperator name="DWithin"/>
      </fes:SpatialOperators>
    </fes:Spatial_Capabilities>
    <fes:Temporal_Capabilities>
      <fes:TemporalOperands>
        <fes:TemporalOperand name="gml:TimeInstant"/>
        <fes:TemporalOperand name="gml:TimePeriod"/>
      </fes:TemporalOperands>
      <fes:TemporalOperators>
        <fes:TemporalOperator name="During"/>
      </fes:TemporalOperators>
    </fes:Temporal_Capabilities>
```

Table 15 — OWS Filter options implemented by the Monterey WFS

Basically, the WFS behind the above capabilities is not capabele to support the example conditions as only the `fes:PropertyIsEqualTo` operand is supported.

7.2 Motivation for an Access Control System with Response Filtering

In cases where access restrictions cannot be implemented due to filter expression limitations or due to not supported filter operands by the WFS, the access control system could filter / modify the WFS response before it is sent to the client.

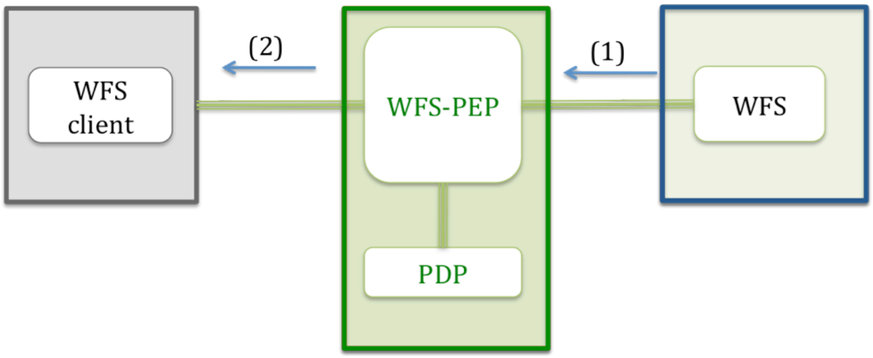


Figure 21 — WFS Access Control **(response filtering)**

Using the same infrastructure as above, the PEP must intercept the response from the WFS, apply changes and then forward the response to the client. Regarding the options that could be supported, the limitations are no longer caused by the Filter specification nor by the WFS implementation. It actually does not even matter which service is protected as long the output from the service is XML and its structure (schema) is known.

7.3 XACML 2.0 Policy Implications (con terra)

The con terra implementations of PEP and PDP make use of request rewriting and response filtering techniques based on authorization decisions to implement the security policies defined by XACML 2.0 policies. The mechanism used to enforce a policy decision highly depends on the requested WFS operation. In the scope of this testbed, the con terra PEP authorizes access to the WFS operations GetCapabilities, DescribeFreatureType, and GetFeature.

7.3.1 Underlying Policy Model and General Access

con terra's PEP/PDP solution, called 'securityManager' is based on a policy model, where access operations are mapped to XACML actions. Additionally, for each supported service type securityManager defines resource types provided by that service, like 'service' or 'feature type'. Instances of any resource type are expressed as resources within an XACML policy. A valid target element, identifying the WFS operation 'GetFeature' in conjunction with a feature type 'ControlTowerGeopoint' would look like this:

```
<Target>
  <Subjects>
    <Subject>
      <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
          >MAnalyst</AttributeValue>
        <SubjectAttributeDesignator
          AttributeId="urn:conterra:names:sdi-suite:policy:attribute:role"
          DataType="http://www.w3.org/2001/XMLSchema#string"/>
      </SubjectMatch>
    </Subject>
  </Subjects>
  <Resources>
    <Resource>
      <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
          >service.wfs#featuretype::http://services.interactive-instruments.de/xsprojects/ows9-
tds/services/ltds/wfs#ControlTowerGeopoint</AttributeValue>
        <ResourceAttributeDesignator
          AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
          DataType="http://www.w3.org/2001/XMLSchema#string"/>
      </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"
          >service.wfs::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>
```

Table 16 -- securityManager sample target

Please note, that this target also requires a subject’s role membership information to be present. It only applies to subjects who belong to the role ‘MAnalyst’.

7.3.2 GetCapabilites

For a GetCapabilities request securityManager acts upon the request path as well as on the response path. First, it checks whether a policy exists granting the requesting subject to perform the action ‘GetCapabilities’ on the requested service ‘http://services.interactive-instruments.de/xsprojects/ows9-tds/services/ltds/wfs’. If so, the request is forwarded to the protected WFS.
The response of the WFS is then intercepted and filtered. securityManager identifies all feature types referenced in the capabilities document and sends an ADR for each feature type instance as a resource and action type ‘GetCapabilities’. If the AD is not ‘permit’, securityManager removes the feature type from the list of advertised feature types inside the capabilities document.

7.3.3 DescribeFeatureType

Generally, authorization of DescribeFeatureType WFS operations works the same as with the GetCapabilities operation. First securityManager checks, whether the action ‘DescribeFeatureType’ is permitted on the requested service. Unlike for the GetCapabilities request, feature type authorization for DescribeFeatureType operation calls takes place on the request path. securityManager checks, if ‘DescribeFeatureType’ is allowed for each requested feature type and removes all denied feature types from the request. securityManager can handle WFS key value pair-encoded requests as well as XML POST requests.

7.3.4 GetFeature

Similar to the DescribeFeatureType operation, securityManager first checks the general permission to call the GetFeature operation before authorizing and potentially removing queries to denied feature types. In case of GetFeature, the AD for a certain feature type may contain an obligation requiring to apply an OGC filter expression to the query to that feature type.

```
<Response xmlns="urn:oasis:names:tc:xacml:1.0:context">
  <Result ResourceId="service.wfs#featuretype::http://services.interactive-instruments.de/xsprojects/ows9-
tds/services/ltds/wfs#BuildingGeosurface">
    <Decision>Permit</Decision>
    <Status>
      <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
    </Status>
    <Obligations xmlns="urn:oasis:names:tc:xacml:1.0:policy">
      <Obligation FulfillOn="Permit" ObligationId="urn:conterra:names:sdi-
suite:policy:obligation:filterexpression::not_S">
        <AttributeAssignment AttributeId="filterexpression.featuretype"
```

```
DataType="http://www.w3.org/2001/XMLSchema#string">BuildingGeosurface</AttributeAssignment>
        <AttributeAssignment AttributeId="filterexpression.expression"
DataType="http://www.w3.org/2001/XMLSchema#string">PG9nYzpOb3QgeG1sbnM6b2djPSJodHRwOi8vd3d3Lm9wZW5naXMubmV0L29nYyI+PG9n
YzpQcm9wZXJ0eUlzRXF1YWxUbz48b2djOlByb3BlcnR5TmFtZT50ZHM6cmVzdHJpY3Rpb24uc2VjdXJpdHlBdHRyaWJ1dGVzR3JvdXBfcmVzQ2xhc3NpZml
jYXRpb248L29nYzpQcm9wZXJ0eU5hbWU+PG9nYzpMaXRlcmFsPlM8L29nYzpMaXRlcmFsPjwvb2djOlByb3BlcnR5SXNFcXVhbFRvPjwvb2djOk5vdD4=</
AttributeAssignment>
      </Obligation>
    </Obligations>
  </Result>
</Response>
```

Table 17 -- PDP response example

The above PDP response example demonstrates the use of obligations. The obligation's attribute 'filterexpression.expression' contains a base64-encoded OGC filter expression to be applied to queries for the feature type 'BuildingGeosurface'. In this case the filter would limit the returned features set to only contain those features where the property 'tds:restriction.securityAttributesGroup_resClassification' is not equal to 'S'.

7.4 XACML 2.0 Policy Implications (GEOAxIS)

7.5 XACML 2.0 Policy Implications (Secure Dimensions)

The Secure Dimensions implementation for the CCI cross thread leverages WFS request rewriting in favor over WFS response filtering where possible. If a WFS request shall be modified by the PEP or the WFS response shall be filtered is controlled by the Policy. The Authorization Decision of the PDP triggers the appropriate processing routines in the PEP.

7.5.1 WFS Request Re-writing

WFS request re-writing is triggered by an Authorization Decision that contains an Obligation called "urn:SD:Obligation:Response:Filter". The following XACML AD illustrates the AS including an Obligation returned by the PDP that causes the PEP to extend the intercepted WFS request by the provided ows:filter expression.

As an example, let's assume the user Chief wants to execute the GetFetaure operation of the NGA WFS for the feature type tds:BuildingGeopoint. The access restriction of the Chief to only see those buildings which are considered government, subnationalGovernment or localGovernment, is represented by the ows:Filter expression outlined in the xacml:Obligation.

```
<Response xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:os"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:context:schema:os access_control-
xacml-2.0-context-schema-os.xsd urn:oasis:names:tc:xacml:2.0:policy:schema:os
access_control-xacml-2.0-policy-schema-os.xsd"
  xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
  xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os">
  <!-- Authorization Decision derived by Secure Dimensions GeoXACML 1.0 / XACML 2.0
Policy Decision Point-->
  <Result ResourceId="">
    <Decision>Permit</Decision>
    <Status>
      <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
    </Status>
    <xacml:Obligations>
      <xacml:Obligation ObligationId="urn:SD:Obligation:OWS:Filter" FulfillOn="Permit">
        <xacml:AttributeAssignment AttributeId="urn:SD:Obligation:OWS:Filter:Definition"
          DataType="http://www.w3.org/2001/XMLSchema#string">
```

```
           <fes:Filter xmlns:fes="http://www.opengis.net/fes/2.0"
             xmlns:tds="http://metadata.dod.mil/mdr/ns/GSIP/3.0/tds/3.0"
             xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
             xsi:schemaLocation="http://www.opengis.net/fes/2.0
http://schemas.opengis.net/filter/2.0/filterAll.xsd">&lt;fes:Filter
xmlns:fes=&quot;http://www.opengis.net/fes/2.0&quot;
xmlns:tds=&quot;http://metadata.dod.mil/mdr/ns/GSIP/3.0/tds/3.0&quot;&gt; &lt;fes:Or&gt;
&lt;fes:PropertyIsEqualTo&gt; &lt;fes:ValueReference&gt;tds:featureFunction-
1&lt;/fes:ValueReference&gt; &lt;fes:Literal&gt;government&lt;/fes:Literal&gt;
&lt;/fes:PropertyIsEqualTo&gt; &lt;fes:PropertyIsEqualTo&gt;
&lt;fes:ValueReference&gt;tds:featureFunction-1&lt;/fes:ValueReference&gt;
&lt;fes:Literal&gt;localGovernment&lt;/fes:Literal&gt; &lt;/fes:PropertyIsEqualTo&gt;
&lt;fes:PropertyIsEqualTo&gt; &lt;fes:ValueReference&gt;tds:featureFunction-
1&lt;/fes:ValueReference&gt; &lt;fes:Literal&gt;subnationalGovernment&lt;/fes:Literal&gt;
&lt;/fes:PropertyIsEqualTo&gt; &lt;/fes:Or&gt; &lt;/fes:Filter&gt;</fes:Filter>
        </xacml:AttributeAssignment>
      </xacml:Obligation>
    </xacml:Obligations>
  </Result>
</Response>
```

Table 18 — ADR with OWS Filter for WFS request rewriting

As highlighted above, the decision is Permit which tasks the PEP to forward the intercepted WFS request after the attached Obligation is processed. The Obligation id "`urn:SD:Obligation:OWS:Filter`" instruments the PEP to extend the WFS request using the outlined owsFilter expression. Assuming that the intercepted WFS request was not instrumenting a ows:Filter expression, the request re-writing aspect is high-lighted in gray:

```
http://ows9.secure-dimensions.org/service/WFS/NGA
?REQUEST=GetFeature
&VERSION=2.0.0
&SERVIcE=WFS
&TYPENAMES=tds:BuildingGeopoint
&NAMESPACES=xmlns(tds,http://metadata.dod.mil/mdr/ns/GSIP/3.0/tds/3.0)
&FILTER=&lt;fes:Filter xmlns:fes=&quot;http://www.opengis.net/fes/2.0&quot;
xmlns:tds=&quot;http://metadata.dod.mil/mdr/ns/GSIP/3.0/tds/3.0&quot;
xmlns:xsi=&quot;http://www.w3.org/2001/XMLSchema-instance&quot;
xsi:schemaLocation=&quot;http://www.opengis.net/fes/2.0
http://schemas.opengis.net/filter/2.0/filterAll.xsd&quot;&gt;&lt;fes:Or&gt;&lt;fes:Prop
ertyIsEqualTo&gt;&lt;fes:ValueReference&gt;tds:featureFunction-
1&lt;/fes:ValueReference&gt;&lt;fes:Literal&gt;government&lt;/fes:Literal&gt;&lt;/fes:P
ropertyIsEqualTo&gt;&lt;fes:PropertyIsEqualTo&gt;&lt;fes:ValueReference&gt;tds:featureF
unction-
1&lt;/fes:ValueReference&gt;&lt;fes:Literal&gt;localGovernment&lt;/fes:Literal&gt;&lt;/
fes:PropertyIsEqualTo&gt;&lt;fes:PropertyIsEqualTo&gt;&lt;fes:ValueReference&gt;tds:fea
tureFunction-
1&lt;/fes:ValueReference&gt;&lt;fes:Literal&gt;subnationalGovernment&lt;/fes:Literal&gt
;&lt;/fes:PropertyIsEqualTo&gt;&lt;/fes:Or&gt;&lt;/fes:Filter&gt;
```

Table 19 — HTTP GET GetFeature request re-written

```
<wfs:GetFeature
  service="WFS"
  version="2.0.0"
  outputFormat="application/gml+xml; version=3.2"
  xmlns:myns="http://www.someserver.com/myns"
  xmlns:wfs="http://www.opengis.net/wfs/2.0"
  xmlns:tds="http://metadata.dod.mil/mdr/ns/GSIP/3.0/tds/3.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.opengis.net/wfs/2.0
http://schemas.opengis.net/wfs/2.0.0/wfs.xsd">
  <wfs:Query typeName="tds:BuildingGeosurface">
    <fes:Filter xmlns:fes="http://www.opengis.net/fes/2.0"
```

```
      xmlns:tds="http://metadata.dod.mil/mdr/ns/GSIP/3.0/tds/3.0"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation="http://www.opengis.net/fes/2.0
http://schemas.opengis.net/filter/2.0/filterAll.xsd">
      <fes:Or>
        <fes:PropertyIsEqualTo>
          <fes:ValueReference>tds:featureFunction-1</fes:ValueReference>
          <fes:Literal>government</fes:Literal>
        </fes:PropertyIsEqualTo>
        <fes:PropertyIsEqualTo>
          <fes:ValueReference>tds:featureFunction-1</fes:ValueReference>
          <fes:Literal>localGovernment</fes:Literal>
        </fes:PropertyIsEqualTo>
        <fes:PropertyIsEqualTo>
          <fes:ValueReference>tds:featureFunction-1</fes:ValueReference>
          <fes:Literal>subnationalGovernment</fes:Literal>
        </fes:PropertyIsEqualTo>
      </fes:Or>
    </fes:Filter>
  </wfs:Query>
</wfs:GetFeature>
```

Table 20 — HTTP POST GetFeature request re-written

7.5.2 WFS Response Filtering

The limitations with WFS response filtering depend on the expressiveness of the XACML 2.0 / GeoXACML 1.0 standard where the resources are described as a XML based hierarchy. Because the basic requirements how to apply response rewriting is already illustrated in a previous chapter, here only the WFS and SSI specificness is described.
For the purpose of filtering all those feature instances of type **tds:LandAerodromeGeosurface** with the alternate security tagging "S" for a certain time window, lets take a look at the response first (reduced[4] properties and two features only for readability):

```
<wfs:FeatureCollection> <wfs:member> <tds:LandAerodromeGeosurface
gml:id="AeronauticalSurfaces.1054">

<tds:restriction.securityAttributesGroup_resClassification>U</tds:restriction.securityAtt
ributesGroup_resClassification>
    <tds:restriction.securityAttributesGroup_resNonIntelComMarkings>No
Information</tds:restriction.securityAttributesGroup_resNonIntelComMarkings>
    <tds:restriction.securityAttributesGroup_resOwnerProducer>No
Information</tds:restriction.securityAttributesGroup_resOwnerProducer>

<tds:restriction.securityAttributesGroup_resClassificationAlternate>S</tds:restriction.se
curityAttributesGroup_resClassificationAlternate>

<tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterval_low>2013-
01-
12T00:00:00Z</tds:restriction.securityAttributesGroup_resClassificationAlternateDateInter
val_low>

<tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterval_high>2013
-01-
13T00:00:00Z</tds:restriction.securityAttributesGroup_resClassificationAlternateDateInter
val_high>

<tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterval_closure>g
teToLtInterval</tds:restriction.securityAttributesGroup_resClassificationAlternateDateInt
erval_closure>
```

[4] Complete FeatureCollection is listed in the Annex A

```
    </tds:LandAerodromeGeosurface> </wfs:member>
  <wfs:member> <tds:LandAerodromeGeosurface gml:id="AeronauticalSurfaces.1055">

<tds:restriction.securityAttributesGroup_resClassification>U</tds:restriction.securityAtt
ributesGroup_resClassification>
    <tds:restriction.securityAttributesGroup_resNonIntelComMarkings>No
Information</tds:restriction.securityAttributesGroup_resNonIntelComMarkings>
    <tds:restriction.securityAttributesGroup_resOwnerProducer>No
Information</tds:restriction.securityAttributesGroup_resOwnerProducer>
    <tds:restriction.securityAttributesGroup_resClassificationAlternate>No
Information</tds:restriction.securityAttributesGroup_resClassificationAlternate>

<tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterval_low>No
Information</tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterv
al_low>

<tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterval_high>No
Information</tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterv
al_high>

<tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterval_closure>c
losedInterval</tds:restriction.securityAttributesGroup_resClassificationAlternateDateInte
rval_closure>
    </tds:LandAerodromeGeosurface> </wfs:member></wfs:FeatureCollection>
```

Table 21 — WFS response example for tds:AerodromeGeosurface

In order for the PEP to remove the unwanted elements () from the XML document, it must request individual decisions for each element matching the following xpath expression: **`/wfs:FeatureCollection/wfs:member/*`**

One option is to leverage the XACML 2.0 Multiple Resource Profile (as already described in the chapter on CSW Filtering). The corresponsding request looks like the following (snippet only):

```
<Request>
  <Subject SubjectCategory="urn:oasis:names:tc:xacml:1.0:subject-category:access-
subject">
    <Attribute AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
      DataType="http://www.w3.org/2001/XMLSchema#anyURI">
      <AttributeValue>MResponder</AttributeValue>
    </Attribute>
  </Subject>
  <Resource>
    <ResourceContent>
<wfs:FeatureCollection><wfs:member> <tds:LandAerodromeGeosurface
gml:id="AeronauticalSurfaces.1054">

<tds:restriction.securityAttributesGroup_resClassification>U</tds:restriction.securityAtt
ributesGroup_resClassification>
    <tds:restriction.securityAttributesGroup_resNonIntelComMarkings>No
Information</tds:restriction.securityAttributesGroup_resNonIntelComMarkings>
    <tds:restriction.securityAttributesGroup_resOwnerProducer>No
Information</tds:restriction.securityAttributesGroup_resOwnerProducer>

<tds:restriction.securityAttributesGroup_resClassificationAlternate>S</tds:restriction.se
curityAttributesGroup_resClassificationAlternate>

<tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterval_low>2013-
01-
12T00:00:00Z</tds:restriction.securityAttributesGroup_resClassificationAlternateDateInter
val_low>

<tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterval_high>2013
-01-
13T00:00:00Z</tds:restriction.securityAttributesGroup_resClassificationAlternateDateInter
val_high>
```

```
<tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterval_closure>g
teToLtInterval</tds:restriction.securityAttributesGroup_resClassificationAlternateDateInt
erval_closure>
    </tds:LandAerodromeGeosurface> </wfs:member>
  <wfs:member> <tds:LandAerodromeGeosurface gml:id="AeronauticalSurfaces.1055">

<tds:restriction.securityAttributesGroup_resClassification>U</tds:restriction.securityAtt
ributesGroup_resClassification>
    <tds:restriction.securityAttributesGroup_resNonIntelComMarkings>No
Information</tds:restriction.securityAttributesGroup_resNonIntelComMarkings>
    <tds:restriction.securityAttributesGroup_resOwnerProducer>No
Information</tds:restriction.securityAttributesGroup_resOwnerProducer>
    <tds:restriction.securityAttributesGroup_resClassificationAlternate>No
Information</tds:restriction.securityAttributesGroup_resClassificationAlternate>

<tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterval_low>No
Information</tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterv
al_low>

<tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterval_high>No
Information</tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterv
al_high>

<tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterval_closure>c
losedInterval</tds:restriction.securityAttributesGroup_resClassificationAlternateDateInte
rval_closure>
    </tds:LandAerodromeGeosurface>
</wfs:member></wfs:FeatureCollection></ResourceContent>
    <Attribute AttributeId="urn:SD:def:xacml:2.0:uri"
      DataType="http://www.w3.org/2001/XMLSchema#anyURI">
      <AttributeValue>/service/WFS/NGA</AttributeValue>
    </Attribute>
    <Attribute AttributeId="urn:oasis:names:tc:xacml:2.0:profile:multiple:scope"
      DataType="http://www.w3.org/2001/XMLSchema#string">
      <AttributeValue>XPath-expression</AttributeValue>
    </Attribute>
    <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
      DataType="urn:oasis:names:tc:xacml:2.0:data-type:xpath-expression">
      <AttributeValue>/*[local-name()='FeatureCollection']/*[local-
name()='member']/*[local-name()='LandAerodromeGeosurface']</AttributeValue>
    </Attribute>
  </Resource>  <Action>
    <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
      DataType="http://www.w3.org/2001/XMLSchema#string">
      <AttributeValue>GetFeature</AttributeValue>
    </Attribute>
  </Action>
<Environment>
    <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-date"
      DataType="http://www.w3.org/2001/XMLSchema#date">
      <AttributeValue>2013-01-12</AttributeValue>
    </Attribute>
    <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-time"
      DataType="http://www.w3.org/2001/XMLSchema#time">
      <AttributeValue>14:37:22+00:00</AttributeValue>
    </Attribute>
    <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-dateTime"
      DataType="http://www.w3.org/2001/XMLSchema#dateTime">
      <AttributeValue>2013-01-12T14:37:02+00:00</AttributeValue>
    </Attribute>
    <Attribute AttributeId="urn:SD:def:xacml:2.0:client-ip"
      DataType="http://www.w3.org/2001/XMLSchema#string">
      <AttributeValue>188.111.111.60</AttributeValue>
    </Attribute>
  </Environment>
```

Table 22 — ADR using MRP leveraging the WFS response example

The important aspects that make the request a compliant MRP request are highlighted: The XACML attribute urn:oasis:names:tc:xacml:2.0:profile:multiple:scope instruct the PDP to derive a single authorization decision for each XML element that matches the xpath expression provided with the XACML attribute urn:oasis:names:tc:xacml:1.0:resource:resource-id. As we can see, the xpath references the feature instances in the feature collection.
From the above request, the PDP derives the following decision:

```
<Response xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:os"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:context:schema:os access_control-
xacml-2.0-context-schema-os.xsd urn:oasis:names:tc:xacml:2.0:policy:schema:os
access_contr
  ol-xacml-2.0-policy-schema-os.xsd"
  xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
  xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os">
  <Result
    ResourceId="/*[local-name()='FeatureCollection'][1]/*[local-
name()='member'][1]/*[local-name()='LandAerodromeGeosurface'][1]">
    <Decision>Deny</Decision>
    <Status>
      <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
    </Status>
  </Result>
  <Result
    ResourceId="/*[local-name()='FeatureCollection'][1]/*[local-
name()='member'][2]/*[local-name()='LandAerodromeGeosurface'][1]">
    <Decision>Permit</Decision>
    <Status>
      <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
    </Status>
  </Result>
  </Response>
```

Table 23 — AD using MRP

The authorization decision above would cause the PEP to remove that XML element for which the xpath ="/*[local-name()='FeatureCollection'][1]/*[local-name()='member'][1]/*[local-name()='LandAerodromeGeosurface'][1] evaluates. This references the feature with alternative security marking "S" during the period Jan 12-13 2013 at the given time of the request at 2013-01-12T14:37:02+00:00.
At the end, the PEP must adopt the attribute numberReturned in the <wfs:FeatureCollection> element to reflect that filtering of feature instances took place. For example, <wfs:FeatureCollection timeStamp="2012-10-10T07:48:09.763-02:00" numberReturned="5" ...> must ge changed to <wfs:FeatureCollection timeStamp="2012-10-10T07:48:09.763-02:00" numberReturned="4" ...> based on the example authorization decision from above.
The illustrated request rewriting and the response filtering takes place in the PEP. However, it could be the PDP that indicates (dictates[5]) the PEP what should be done. In order for the PDP to differenciate if the PEP requests an authorization for the request or the response, this context information must be presented in the XACML Authorization Decision Request (ADR). The Secure Dimensions PEP uses the attribute urn:SD:def:xacml:2.0:context for that. Its value could be

[5] This is true for the Secure Dimensions PDP.

`urn:SD:def:xacml:2.0:request` indicating that the ADR is referencing a WFS request and `urn:SD:def:xacml:2.0:response` indicating that the ADR is referencing a WFS response. In order to dictate that the PEP must intercept the WFS response and undertake it a XML processing, the Authorization Deicsion (AD) returned by the Secure Dimensions PDP must contain an Obligation with the identifier `urn:SD:Obligation:Response:Filter`.

The following is an example of the AD reflecting that response processing is required for the feature type `LandAerodromeGeosurface`:

```
<Response xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:os"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:context:schema:os access_control-
xacml-2.0-context-schema-os.xsd urn:oasis:names:tc:xacml:2.0:policy:schema:os
access_control-xacml-2.0-policy-schema-os.xsd"
  xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
  xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os">
  <Result ResourceId="">
    <Decision>Permit</Decision>
    <Status>
      <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
    </Status>
    <xacml:Obligations>
      <xacml:Obligation ObligationId="urn:SD:Obligation:Response:Filter"
FulfillOn="Permit">
        <xacml:AttributeAssignment AttributeId="urn:SD:def:xacml:2.0:profile:identifier"
          DataType="http://www.w3.org/2001/XMLSchema#string"
          >urn:oasis:names:tc:xacml:2.0:profile:multiple:xpath-
expression</xacml:AttributeAssignment>
        <xacml:AttributeAssignment
AttributeId="urn:oasis:names:tc:xacml:2.0:resource:scope"
          DataType="http://www.w3.org/2001/XMLSchema#string"
          >XPath-expression</xacml:AttributeAssignment>
        <xacml:AttributeAssignment
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
          DataType="urn:oasis:names:tc:xacml:2.0:data-type:xpath-expression"
          >./*[local-name()='FeatureCollection']/*[local-name()='member']/*[local-
name()='LandAerodromeGeosurface']</xacml:AttributeAssignment>
      </xacml:Obligation>
    </xacml:Obligations>
  </Result>
</Response>
```

Table 24 — AD instrumenting the PEP to undertake WFS response filtering

The important part is that the Obligation is to executed if the AD is “Permit”, which it is. The Id `urn:SD:Obligation:Response:Filter` indicates, that response processing must take place. The attribute `urn:SD:def:xacml:2.0:profile:identifier` indicates, that a XACML profile shall be used. The attribute value `urn:oasis:names:tc:xacml:2.0:profile:multiple:xpath-expression` indicates that MRP shall be used exactly as defined in the XACML 2.0 MRP: The individual decisions shall be derived with the scope `XPath-expression` as expressed in the attrbute `urn:oasis:names:tc:xacml:2.0:resource:scope`. The xpath expression that references the XML elements for which the decisions are to be derived are indicated by the attribute `urn:oasis:names:tc:xacml:1.0:resource:resource-id` thru the value `./*[local-name()='FeatureCollection']/*[local-name()='member']/*[local-name()='LandAerodromeGeosurface']`.

As we can see, the xpath expression references exactly those XML elements which represent feature instances of type `LandAerodromeGeosurface`.

Based on the request as illustated above, a Policy must be in place that makes the PDP to derive the above decision. This is very simple, as the <Target> element must only match for the userid == MResponder and the feature type **tds:LandAerodromeGeosurface**. The following Policy resolves to Permit and the comprised Obligation is part of the AD:

```
<Policy PolicyId="urn:ogc:ows9:ssi:policy:request:GET:LandAerodromeGeosurface"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-
applicable">
        <Description>Policy for matching the REQUEST context and feature type
tds:LandAerodromeGeosurface -> PEP will receive an obligation to request MRP on the
RESULT context ...</Description>
        <PolicyDefaults>
          <XPathVersion>http://www.w3.org/TR/1999/Rec-xpath-19991116</XPathVersion>
        </PolicyDefaults>
        <Target>
          ...
        </Target>
        <Rule RuleId="PermitWithObligationForLandAerodromeGeoSurface1" Effect="Permit">
          <Description>All service requests for feature type tds:LandAerodromeGeosurface
are permitted but are subject to Obligations</Description>
          <Target>
            <Resources>
              <Resource>
                <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
equal">
                  <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">urn:SD:def:xacml:2.0:request</Attribu
teValue>
                  <ResourceAttributeDesignator
AttributeId="urn:SD:def:xacml:2.0:context"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
                </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:SD:def:xacml:2.0:request"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
                </ActionMatch>
              </Action>
            </Actions>
          </Target>
          <Condition>
            <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">
              <Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-
equal"/>
              <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">tds:LandAerodromeGeosurface</Attribut
eValue>
              <ResourceAttributeDesignator AttributeId="urn:SD:def:xacml:2.0:typenames"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </Apply>
          </Condition>
        </Rule>
        <Obligations>
          <Obligation ObligationId="urn:SD:Obligation:Response:Filter"
FulfillOn="Permit">
            <AttributeAssignment AttributeId="urn:SD:def:xacml:2.0:profile:identifier"

DataType="http://www.w3.org/2001/XMLSchema#string">urn:oasis:names:tc:xacml:2.0:profile:
multiple:xpath-expression</AttributeAssignment>
            <AttributeAssignment
AttributeId="urn:oasis:names:tc:xacml:2.0:resource:scope"
              DataType="http://www.w3.org/2001/XMLSchema#string">XPath-
```

```
expression</AttributeAssignment>
            <AttributeAssignment
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
              DataType="urn:oasis:names:tc:xacml:2.0:data-type:xpath-
expression">./*[local-name()='FeatureCollection']/*[local-name()='member']/*[local-
name()='LandAerodromeGeosurface']</AttributeAssignment>
          </Obligation>
        </Obligations>
      </Policy>
```

Table 25 — Policy snippet to issue Obligation for WFS response filtering

Based on that PDP response, the PEP intercepts the response from the WFS, which then contains the feature collection of type `tds:LandAerodromeGeosurface`. The following Policy snippet takes care of deriving individual decisions for each XML element matching the provided xpath expression:

```
<Rule RuleId="LandAerodromeGeosurface" Effect="Deny">
        <Description>All classified features of type LandAerodromeGeosurface that are
marked "S" and the the request is in range with the defined timewindow</Description>
        <Target/>
        <Condition>
          <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
            <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">S</AttributeValue>
              <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-
only">
                <Apply FunctionId=" urn:SD:def:xacml:2.0:xpath-string-selector">
                  <Apply FunctionId="urn:oasis:names:tc:xacml:2.0:function:xpath-
expression-concatenate">
                    <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:xpath-
expression-one-and-only">
                      <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="urn:oasis:names:tc:xacml:2.0:data-type:xpath-expression"/>
                    </Apply>
                    <AttributeValue DataType="urn:oasis:names:tc:xacml:2.0:data-
type:xpath-expression">/*[local-name() =
'restriction.securityAttributesGroup_resClassificationAlternate']/text()</AttributeValue
>
                  </Apply>
                </Apply>
              </Apply>
            </Apply>
            <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:dateTime-greater-
than">
              <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:dateTime-one-and-
only">
                <EnvironmentAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-dateTime"
DataType="http://www.w3.org/2001/XMLSchema#dateTime"/>
              </Apply>
              <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:dateTime-one-and-
only">
                <Apply FunctionId="urn:SD:def:xacml:2.0:xpath-dateTime-selector">
                  <Apply FunctionId="urn:oasis:names:tc:xacml:2.0:function:xpath-
expression-concatenate">
                    <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:xpath-
expression-one-and-only">
                      <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="urn:oasis:names:tc:xacml:2.0:data-type:xpath-expression"/>
                    </Apply>
                    <AttributeValue DataType="urn:oasis:names:tc:xacml:2.0:data-
type:xpath-expression">/*[local-name() =
'restriction.securityAttributesGroup_resClassificationAlternateDateInterval_low']/text()
</AttributeValue>
```

```
                  </Apply>
                </Apply>
              </Apply>
            </Apply>
            <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:dateTime-less-
than">
              <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:dateTime-one-and-
only">
                <EnvironmentAttributeDesignator 
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-dateTime" 
DataType="http://www.w3.org/2001/XMLSchema#dateTime"/>
              </Apply>
              <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:dateTime-one-and-
only">
                <Apply FunctionId="urn:SD:def:xacml:2.0:xpath-dateTime-selector">
                  <Apply FunctionId="urn:oasis:names:tc:xacml:2.0:function:xpath-
expression-concatenate">
                    <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:xpath-
expression-one-and-only">
                      <ResourceAttributeDesignator 
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" 
DataType="urn:oasis:names:tc:xacml:2.0:data-type:xpath-expression"/>
                    </Apply>
                    <AttributeValue DataType="urn:oasis:names:tc:xacml:2.0:data-
type:xpath-expression">/*[local-name() = 
'restriction.securityAttributesGroup_resClassificationAlternateDateInterval_high']/text(
)</AttributeValue>
                  </Apply>
                </Apply>
              </Apply>
            </Apply>
          </Apply>
        </Condition>
        </Rule>
```

Table 26 — Rule snippet that uses dateTime functions to filter WFS response

The outermost Apply statement of the <Condition> provides a logical AND containing three individual conditions to be checked:

1) Check if the property, referenced by xPath `/*[local-name() = 'restriction.securityAttributesGroup_resClassificationAlternate']/text()` has the value S

2) Check if the current request time prepresented by attribute **`urn:oasis:names:tc:xacml:1.0:environment:current-dateTime`** is after the begin time of the alternative security tagging represented by the xPath **`/*[local-name() = 'restriction.securityAttributesGroup_resClassificationAlternateDateInterval_low']/text()`**

3) Check if the current request time prepresented by attribute **`urn:oasis:names:tc:xacml:1.0:environment:current-dateTime`** is before the end time of the alternative security tagging represented by the xPath **`/*[local-name() = 'restriction.securityAttributesGroup_resClassificationAlternateDateInterval_high']/text()`**

If all three conditions do evaluate to true, the Rule will return a "Deny" decision which is processed by the PDP to derive the individual decisions. The following AD illustates the derived decisions for five feature instances:

```
<Response xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:os"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:context:schema:os access_control-
xacml-2.0-context-schema-os.xsd urn:oasis:names:tc:xacml:2.0:policy:schema:os
```

```
access_control-xacml-2.0-policy-schema-os.xsd"
  xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
  xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os">
  <Result
    ResourceId="/*[local-name()='FeatureCollection'][1]/*[local-
name()='member'][5]/*[local-name()='LandAerodromeGeosurface'][1]">
    <Decision>Permit</Decision>
    <Status>
      <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
    </Status>
  </Result>
  <Result
    ResourceId="/*[local-name()='FeatureCollection'][1]/*[local-
name()='member'][1]/*[local-name()='LandAerodromeGeosurface'][1]">
    <Decision>Permit</Decision>
    <Status>
      <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
    </Status>
  </Result>
  <Result
    ResourceId="/*[local-name()='FeatureCollection'][1]/*[local-
name()='member'][2]/*[local-name()='LandAerodromeGeosurface'][1]">
    <Decision>Permit</Decision>
    <Status>
      <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
    </Status>
  </Result>
  <Result
    ResourceId="/*[local-name()='FeatureCollection'][1]/*[local-
name()='member'][3]/*[local-name()='LandAerodromeGeosurface'][1]">
    <Decision>Permit</Decision>
    <Status>
      <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
    </Status>
  </Result>
  <Result
    ResourceId="/*[local-name()='FeatureCollection'][1]/*[local-
name()='member'][4]/*[local-name()='LandAerodromeGeosurface'][1]">
    <Decision>Permit</Decision>
    <Status>
      <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
    </Status>
  </Result>
</Response>
```

Table 27 — AD instrumenting the PEP to not remove feature instances

As we can see, none of the requested features meet the criteria at the time of request `2012-10-22T12:00:00Z`. Chaning the request time to `2013-01-12T12:00:00Z` cause the AD to change as follows (the xpath instance for the denied element represent the feature instance with `gml:id` `AeronauticalSurfaces.1054`):

```
<Response xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:os"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:context:schema:os access_control-
xacml-2.0-context-schema-os.xsd urn:oasis:names:tc:xacml:2.0:policy:schema:os
access_control-xacml-2.0-policy-schema-os.xsd"
  xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
  xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os">
  <Result
    ResourceId="/*[local-name()='FeatureCollection'][1]/*[local-
name()='member'][5]/*[local-name()='LandAerodromeGeosurface'][1]">
    <Decision>Permit</Decision>
    <Status>
      <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
    </Status>
  </Result>
  <Result
```

```
    ResourceId="/*[local-name()='FeatureCollection'][1]/*[local-
name()='member'][1]/*[local-name()='LandAerodromeGeosurface'][1]">
    <Decision>Permit</Decision>
    <Status>
      <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
    </Status>
  </Result>
  <Result
    ResourceId="/*[local-name()='FeatureCollection'][1]/*[local-
name()='member'][2]/*[local-name()='LandAerodromeGeosurface'][1]">
    <Decision>Permit</Decision>
    <Status>
      <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
    </Status>
  </Result>
  <Result
    ResourceId="/*[local-name()='FeatureCollection'][1]/*[local-
name()='member'][3]/*[local-name()='LandAerodromeGeosurface'][1]">
    <Decision>Deny</Decision>
    <Status>
      <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
    </Status>
  </Result>
  <Result
    ResourceId="/*[local-name()='FeatureCollection'][1]/*[local-
name()='member'][4]/*[local-name()='LandAerodromeGeosurface'][1]">
    <Decision>Permit</Decision>
    <Status>
      <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
    </Status>
  </Result>
</Response>
```

Table 28 — AD instrumenting the PEP to remove one feature instance

7.6 Practical considerations when using WFS response filtering

As explained before, there are potentially more options of how access could be restricted to a WFS by applying general XML processing on the WFS response. But two arguments should not be forgotten: Assurance and Performance

7.6.1 Assurance Considerations

With response filtering, the content goes to the client after the PEP has applied the XML processing it was instructed to do; perhaps through an AD received from the PDP.

In any case, the final result of that XML processing is sent to the client. Any glitch in the processing may cause an unwanted / unintended exploitation of restricted content.

7.6.2 Performance Considerations

Another important aspect is processing performance in the PEP and the PDP and network load when using the XACML 2.0 MRP.

It requires that the entire WFS response is included inline in the ADR (as illustrated above). In order to get this, the PEP must fetch the entire WFS response in memory and then marshall it (inside the ADR) to the PDP. Depending on the number of returned features and the complexity of the features, and in particular the accuracy of the feature geometry, cause a quick increase of size.

Network load for transporting the ADR from the computer which runs the PEP to the computer which runs the PDP becomes the next performance issue. Assuming that the PEP resides in the DMZ and the PDP inside the private network, this is not too much of an issue. But in cases where the PDP is hosted remotely at some other computing center, network load my become an issue.

The PDP, receiving the XACML MRP compliant request must create a DOM representation for the WFS response in order to apply the xpath expressions as included into the ADR. This requires heap meomory. Processing all XML nodes referenced by the xpath expression from the ADR – which potentially invloves more xpath expressions to be evaluated from the policy, requires CPU power.

When the PEP does XML processing on the WFS response based on the AD received from the PDP, the PEP must evaluate all the xpath expression from the AD and remove all those nodes for which the decision is Deny. This requires main memory and CPU power as the entire WFS response must be in main memory using a DOM representation.

Even tough performance testing was not done in OWS-9, some sources indicate that Xerces DOM processing requires 5x more main memory compared to the actual size of the XML. Looking at the Monterey Data Set, the WFS response for features of the type tds:BuildingGeocurve is approx 10MB. This requires main memory allocation for each request on that feature type roughly about 50MB. With 10 parallel users, the main memory consumption is already 500MB. So the final stage where the PEP must decline new requests because of main memory defizit can easily be estimated.

7.7 XACML 2.0 Short Comings and Standardization Option

A closer look at the Rule snippet using XACML MRP unveils that non standard XACML 2.0 functions had been used. The reason for that is a short coming of the XACML 2.0 standard regarding the AttributeSelector. The AttributeSelector as defined in XACML 2.0 can only select XML nodes based on a static xpath expression.

```
<xs:element name="AttributeSelector" type="xacml:AttributeSelectorType"
substitutionGroup="xacml:Expression"/>
<xs:complexType name="AttributeSelectorType">
        <xs:complexContent>
                <xs:extension base="xacml:ExpressionType">
                        <xs:attribute name="RequestContextPath" type="xs:string" use="required"/>
                        <xs:attribute name="DataType" type="xs:anyURI" use="required"/>
                        <xs:attribute name="MustBePresent" type="xs:boolean" use="optional" default="false"/>
                </xs:extension>
        </xs:complexContent>
</xs:complexType>
```

The short coming is that it is not possible to provide a xpath expression as a parameter to the AttributeSelector. However, this is not sufficient for the requirement in MRP where it is required to derive an authorization decision for individual XML node(s).

Therefore, the above not XACML 2.0 compliant Rule requires none standard functions such as

1) `urn:SD:def:xacml:2.0:xpath-string-selector` which is a function that returns a bag of string attributes for a given parameter: a xpath expression.

2) `urn:SD:def:xacml:2.0:xpath-dateTime-selector` which is a function that returns a bag of dateTime attributes for a given parameter: a xpath expression.

In cases where a spatial condition shall be placed on a child element, a function like `urn:SD:def:xacml:2.0:xpath-geometry-selector` is required: The function returns a bag of geometry attributes from an xpath expression.
A possible way forward would be to standardize these attribute selector functions. The questions is whether this change request should be targeted at OASIS or OGC. Clearly, the shortcoming is in the XACML 2.0 specification and therefore a Change Request should be targeted at OASIS. However, OASIS has fixed this shortcoming in the XACML 3.0 version, which reduces the acceptance likelihood for a CR on XACML 2.0 dramatically.

An alternative would be to provide a Change Request to GeoXACML to include these attribute selector functions. One strong argument for targeting at OGC is that one of the data types that must be returned by the attribute selector functions is of type **`urn:ogc:def:dataType:geoxacml:1.0:geometry`**. Therefore, the requirement for such a specification extension seems reasonable be OGC centric. The change request to GeoXACML 1.0 could – however - incorperate a `urn:ogc:def:function:geoxacml:1.1:xpath-<data-type>-selector` function where data-type are all XACML 2.0 data types plus the GeoXACML data type geometry.

The other alternative is to use XACML 3.0, as the improved attribute selector version is available. However, this seems to require to upgrade GeoXACML to be based on XACML 3.0 in order to allow the return of attributes of data type **`urn:ogc:def:dataType:geoxacml:1.0:geometry`**.

Bibliography

[1] SSI Access Rights: https://portal.opengeospatial.org/files/?artifact_id=51106

8 ANNEX A

This is the text of the full CCI use case as of 27 Nov. 2012.

Introduction

This is the scenario for OWS9. It integrates work from the CCI, IO and Aviation scenarios in a single one.

Motivation: Presidential Escape Route

The OGC president is evacuated from Haiti to Florida due to a hurricane. Once in Florida the OGC President is taken to a secret building location where he is safe. *The optimal escape route needs to be identified in Haiti and in Escape routes to the airport are needed, as well as the best One in Road data is combined from several sources (conflation) and new data is made available. Data is sent to in-field mobile devices for verification and determining the best route. Best route is sent to OGC central to prepare airplane.*

Overview

1. Hurricane approaches Haiti
2. Information about Haiti is gathered to help identified optimum escape plan.
   - VGI data
   - OWS Context
3. Information is analyzed and the plan is developed. (Plan captures current location of President, best roads and best airport)
   - VGI data
   - OWS Context
4. Aviation Thread
5. Security Policy is generated, while the President is in the air
   - SSI Thread
6. President lands in Florida (using Monterey data) and plan to get to secure building is design
   - Entire security flow done in this stage (Filtered context)
   - Conflation
   - Data Quality including VGI data
7. Route planned to move President from Monterey Florida Airport to classified location (buildings with security markings)

Conventions

□ Black text are main flow/CCI contributions

□ Blue text are Innovations contributions

□ Red text are Aviation contributions

□ Green text are SSI contributions

- Orange text are open issues

Actors

- National Hurricane Center operator - (**NHC-OP)**
- Haiti Emergency Response Center - **(ERC)**
- Haiti Emergency Response Center - **Emergency Responder (ERC-ER)**
- Haiti Emergency Response Center - **Haiti Operator (ERC-OP)**
- Florida Emergency Response Center Planner - **Florida Planner (FERC-PLAN)**
- Florida Emergency Response Center - **Map Analysis Expert (FERC-MAP)**
- Florida Emergency Response Center - **Florida Operator (FERC-OP)**
- Presidential Support Lead Team - **Policy Builder (POL)**
- Someone in Puerto Rico **Juan**
- Hacker in Jamaica **Jamcker**
- OGC President as **Marco (PRES)**
- Presidential Support Lead Team as **Steve (PRESLEAD)**
- **TC Member**

Steps

Haiti

1. **NHC-OP**(NOAA) discovers a hurricane approaching Haiti
    - **NHC-OP** explores NASA weather data related to the hurricane warning.
        - Plan A: NHC-OP sees the approaching hurricane on-screen and draws a line (path) showing the expected track of the storm. [time series GMU WCS with Envitia client]. [Envitia/Luciad client] **NHC-OP** - circles the eye of the storm on the image, which creates an embedded SVG imagery annotation in a context document (or in the image itself) -- TBD if possible by Raj - Context document is registered in the catalog
        - Plan B: [Envitia WMTS client]
    - [Envitia/Luciad Component] creates a WMS for the data and registers the WMS in the catalog;
2. NHC-OP issues a warning with an OWS Context document [Compusult]
    - **NHC-OP** sends notification to **ERC** as email with a link to OWS Context document from the CSW with the hurricane imagery included as WCS and WMTS, and the actual hurricane track included as KML.
3. **ERC** verifies the situation
    - Opens [Pyxis Client] and views the Context document to view hurricane map
    - Adds Haiti imagery (generic basemap; landsat; etc) with [NASA WMTS or OPeNDAP WCS] -- note that Haiti imagery is unprojected.
    - Event is verified, and triggers a "situation" response: Evacuate the OGC President.

4. **ERC-ER**builds a best-of-source roads basemap upon which evacuation plans can be developed
    - Discovers data from Haiti
        - Submits query in the [Pyxis Client] to retrieve: data from Haiti to the [Compusult CSW]
    - [Pyxis Client] gets Context document with the data sources and visualizes
        - [Envitia WFS Twitter Broker]
            - Geocodes [OpenGeo WFS VGI Twitter] with Gazetteer data, providing points that can be obstructions.
        - [OpenGeo WFS VGI OSM]
        - [OpenGeo WFS VGI Usahidi]
        - [Cubewerx WFS Haiti - maybe]
        - [Intergraph WFS Haiti - maybe]
5. ***To:Raj please complete - Pyxis has limited support for GeoPackage***
    - Raj: what does limited support mean? All the GeoPackages are the same so maybe drop GeoPackage visualization from this step?
        - GeoPackages from [who??]
6. **ERC-ER** uses yesterday's LiDAR? survey of a remote area to assess the condition of roads there
    - **ERC-ER** accesses browser-based [Rasdaman LiDAR? visualization client] *(Use sample LIDAR HRE and zoom to fake that it's in Haiti)*
    - **ERC-ER**, after doing some imagery manipulation, sees that this road is closed and should be marked as obstructed, then updates the obstruction point layer.
7. **ERC-ER**sends best-of-source roads data to evacuation planners for route development.
    - **ERC-ER** using [Pyxis Client] updates Context document to include additional data sources (images, LiDAR?, etc.)
        - ***To:Raj: who is going to to this context document. Can we generate it based on this?** _-- Raj: Yes this is fine._*
    - **ERC-ER** re-posts Context document to web which updates the document's last modified date in the CSW
8. **PRESLEAD** accesses Context document and develops presidential escape route.
    - **adds** point on the map as identification of the President location (as annotation?)
    - line as escape route,
    - point as airport for departure.
    - **PRESLEAD** asks her team to perform a field check of route to ensure safety of President during evacuation.
    - **PRESLEAD** team uses [Luciad mobile app] with the GeoPackage for determining line of sight along the route (for personal safety concerns?)

- **PRESLEAD** team uses [GIS.FCU mobile app] to edit the route to avoid a recent flood that didn't appear in the data. Also takes pictures of the flood and attaches them to appropriate places on the map.
- **PRESLEAD** uses [Compusult] to encrypt the final GeoPackage and then distributes to the team. Show in [Envitia mobile app] that the encrypted one can be viewed.

9. **ERC-ER** plans a generic escape route for **TC Members**
   - **ERC-OP** uses [Carbon Project] mobile app to identify a good route (using all that good VGI data and field verification) and Geosynchronizes data back to **ERC**
   - [SigmaBravo] creates an open GeoPackage which is posted to the web for **TC Member**s who view in [Compusult mobile app]
   - **ERC-OP** requests data to be streamed using [LM client]
   - [LM Client] contacts [XX WFS]
     - **ERC-OP** gets GML stream via WFS in his cool mobile device [who??] **ALTERNATE FLOW: The president's escape route is sent via GML stream to *Field Operator. Carbon packages route and enable GML stream via WFS.***The Stream can be received and rendered by any WFS system. Show LM's tool receiving the data and being rendered real-time.
   - GML can also be streamed to a GeoPackage and accessed on a mobile app...
10. A nod to Aviation - Flight from Haiti to Monterey
    - *While in flight, **Florida Planner** receives notice from Presidential support team to identify suitable airport for special flight landing along with best available GEOINT data to provide a “common operational picture”.*
    - Security Policies are generated based on Presidential Support Team Needs
      - _Presidential support team lead recognizes need to restrict some data from open access based on potential landing sites and possible buildings for President to be housed temporarily._
      - **Policy Builder**(SD) creates policy stating that
        - access to the WFS airport feature (everything inside the AeronauticalSurfaces? boundary) is restricted based on security tag of (S) during the time frame 01-12-2013 to 01-13-2013. This policy is distributed to PEP for NGA data (Geoaxis) and PEP for USGS data (SD). (Same policy applied to different PEPs).(in other words the Policy is on the data and it’s availability) (from IO Scenario)
        - Access restriction to Federal building FFN1 = Government, ZSAX_RS0 = S and State building

FFN1 = Subnational Government, ZSAX_RS0 = S based on individuals security clearance level

- Identification of best route from Florida Airport to Temporary Secured housing. - Part 1 - investigation of data by **Florida Planner**(Data used is Monterey but we will say is Florida)
    - **Florida Planner**queries using [Pyxis Client] the [Compusult CSW] to discover GEOINT data sources
        - The date is 01-12-2013
        - [Compusult CSW] responds to data/service with a filtered OWS Context based on the credentials of the Planner.?? *Double check with Jenn and Andreas ??
    - [Pyxis Client] shows the following
        - [CubeWerx WFS USGS] is identified
        - [OpenGeo WFS VGI] is identified
        - [ii WFS NGA] is NOT discovered or is discovered and a restriction messages is presented
            - e.g. error message stating insufficient authorization for some data. ??
    - **Florida Planner** selects to preview all of them (the non restricted ones)
    - [Pyxis Client] request WFS request and presents the data from:
        - [Cube Werx WFS USGS]
        - [OpenGeo WFS VGI]
    - ***Florida Planner*** knows that there is complementary data that they do not have access to. She is not cleared and is not a GIS expert and will need help of a ***Map Analysis Expert***
    - **Florida Planner** passes a Context Document to the **Map Analysis Expert**
- Identification of best route from Florida Airport to Temporary Secured housing. - Part 2 - investigation of data by **Map Analysis Expert**
    - **Map Analysis Expert** is tasked to identify best route to get President from airport to secret building location.
    - **Map Analysis Expert**queries CSW to discover GEOINT data sources
        - the date is 01-12-2013
        - [Compusult CSW] provides result in OWS Context*
        - [Pyxis Client] shows the following
            - [CubeWerx WFS USGS] is identified
            - [OpenGeo WFS VGI] is identified
            - [ii WFS NGA] - It is discovered now because of the credentials of **Map Analysis Expert**
    - **Map analysis expert** investigates sources
        - views FGDC metadata

    - views in more comprehensive ISO metadata
  - **Map analysis expert**requests data
    - via [Pyxis Client] to view [ii WFS NGA]via [Pyxis Client] to view CubeWerx? WFS USGS TNM
      - **The Pyxis Client only can issue a WFS SOAP POST while the Cubewerx WFS provider can only understad a WFS KVP GET. The Lisasoft Web Service Facade will translate both the request and the response. ---** double check with pyxis.
- Demonstration of filtered secured features
  - [Esri Client] contacts WFSs
    - GeoAxis? (using con terra PDP and SD PAP)
    - Interactive instruments WFS.
    - Client [Esri Client] displays NGA WFS results that have been "filtered". WFS responds with error message stating insufficient authorization.
      - Airport is discovered because they are authorized access even though query falls within 01-12-2013 and 01-13-2013 when this feature is classified
      - Control tower, Federal Building, State building are discovered
- Demonstration of filtered secured features - with Broker
  - US sources are being secured (USGS WFS, NGA WFS).
  - They can both be access using NGA WFS schema via a WFS broker [CNR NGA (USGS) WFS].
  - An outside user wants to access buildings from the region of interest
  - The buildings from USGS are filtered based on the NGA rules
  - [Pyxis Client] request USGS data based on the NGA WFS [CNR NGA (USGS) WFS]
  - The broker gets the request (based on NGA WFS) translates the request to USGS WFS and responds based on NGA WFS
  - The magic secure component intercepts the respond and filters the respond removing features that are secured.
  - [Pyxis Client] shows the filtered results
- Continuation **Map Analysis Expert**interaction with [Pyxis Client] to perform conflation
  - **Map Analysis Expert** sees that there is overlapping and complementary road data
  - in [Pyxis Client] selects to conflate the sources
    - selects a target source: [ii WFS NGA TDS]
    - selects a source to be conflated first: [Cube Werx

WFS USGS TNM]

- [Pyxis Client] submits the conflation process to the conflation WPS [52North WPS Conflation]
    - WPS [52North WPS Conflation] conflates
        - Performs geometry conflation by invoking the [GMU WPS Conflation]
        - Performs attribute conflation by invoking the [Envitia WPS SPARQL]
        - Prepares the results using the target schema
        - Provides the provenance results in TBD ???
    - WPS [52North WPS Conflation] makes available the result
        - feature data with a WFS [52North WFS Conflation Results]
        - metadata and provenance in TBD ??
- Client [Pyxis Client] presents the resulting conflated data.

- **Map Analysis Expert**interacts with the data and make small adjustments
    - This can be pre-processed. Maybe nothing else needs to be added or removed.
- Via [Pyxis Client] **Map Analysis Expert** registers the result in the catalog as OWSContext
- **Map Analysis Expert** sends the new context map to the **Steve** OGC Support Team (who is cleared to see restricted data)
- **Steve** opens the OWS Context in the Client [Pyxis Client] and sees the new conflated data.
- **Steve** sees the conflation details as a provenance graph in the [Pyxis Client]

- **Steve**drives the OGC president to the secured facility
    - The world is saved !

9 ANNEX B

```
<?xml version="1.0" encoding="utf-8"?>

<wfs:FeatureCollection timeStamp="2012-11-27T14:41:20.11-02:00" numberReturned="5"
  numberMatched="unknown" xmlns:tds="http://metadata.dod.mil/mdr/ns/GSIP/3.0/tds/3.0"
  xmlns:gml="http://www.opengis.net/gml/3.2" xmlns:wfs="http://www.opengis.net/wfs/2.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://metadata.dod.mil/mdr/ns/GSIP/3.0/tds/3.0 http://services.interactive-instruments.de/xsprojects/ows9-
tds/schema/TDS_v3.0_SF0_GML321/TDS_v3.0_SF0_GML321.xsd http://www.opengis.net/wfs/2.0 http://services.interactive-instruments.de/xsprojects/ows9-
tds/schema/ogc/wfs/2.0/wfs.xsd http://www.opengis.net/gml/3.2 http://services.interactive-instruments.de/xsprojects/ows9-
tds/schema/ogc/gml/3.2.1/gml.xsd http://www.opengis.net/gml/3.2 http://services.interactive-instruments.de/xsprojects/ows9-
tds/schema/ogc/gml/3.2.1/gml.xsd">
  <wfs:boundedBy>
    <gml:Envelope srsName="http://metadata.ces.mil/mdr/ns/GSIP/crs/WGS84E_2D" srsDimension="2">
      <gml:lowerCorner>36.5817352780001 -121.862459283</gml:lowerCorner>
      <gml:upperCorner>36.9415407990001 -121.595448459</gml:upperCorner>
    </gml:Envelope>
  </wfs:boundedBy>
  <wfs:member> <tds:LandAerodromeGeosurface gml:id="AeronauticalSurfaces.1052">
    <tds:geometry>
      <gml:Polygon gml:id="AeronauticalSurfaces.ObjectID.1052.SHAPE.Geom_0">
        <gml:exterior>
          <gml:LinearRing>
            <gml:posList>36.6324007110001 -121.694346767 36.632309338 -121.694632804 36.632376875
              -121.694895005 36.6324801660001 -121.695224743 36.632643048 -121.695399544
              36.632782094 -121.695546535 36.6328613040001 -121.69558614 36.6329604200001
              -121.695562352 36.633020011 -121.695510707 36.6330478200001 -121.695451116
              36.633067684 -121.695363715 36.632833292 -121.694616839 36.6327141100001
              -121.694195729 36.632662538 -121.694144157 36.6325834570001 -121.694144157
              36.632484139 -121.694199775 36.6324007110001 -121.694346767</gml:posList>
          </gml:LinearRing>
        </gml:exterior>
      </gml:Polygon>
    </tds:geometry>
    <tds:address>No Information</tds:address>
    <tds:aerodromeElevation>-999999</tds:aerodromeElevation>
    <tds:aerodromeOfficialName>No Information</tds:aerodromeOfficialName>
    <tds:airfieldSymbolType>abandonedClosedNotUsable</tds:airfieldSymbolType>
    <tds:airfieldType>minor</tds:airfieldType>
    <tds:area>6307</tds:area>
    <tds:conditionOfFacility>abandoned</tds:conditionOfFacility>
    <tds:controllingAuthority>civilian</tds:controllingAuthority>
    <tds:facilityOperationalStatus>notInOperation</tds:facilityOperationalStatus>
```

```
<tds:geointAssuranceMetadata.processStep.source.resourceContentOrigin>noInformation</tds:geointAssuranceMetadata.processStep.source.resourceConte
ntOrigin>
    <tds:geoNameCollection.memberGeoName.fullName>No Information</tds:geoNameCollection.memberGeoName.fullName>
    <tds:geoNameCollection.memberGeoName.nameIdentifier>-999999</tds:geoNameCollection.memberGeoName.nameIdentifier>
    <tds:highestElevation>-999999</tds:highestElevation>
    <tds:icaoLocationIndicator>No Information</tds:icaoLocationIndicator>
    <tds:length>133</tds:length>
    <tds:note.memorandum>No Information</tds:note.memorandum>
    <tds:portOfEntry>false</tds:portOfEntry>
    <tds:restriction.securityAttributesGroup_resClassification>U</tds:restriction.securityAttributesGroup_resClassification>
    <tds:restriction.securityAttributesGroup_resNonIntelComMarkings>No
Information</tds:restriction.securityAttributesGroup_resNonIntelComMarkings>
    <tds:restriction.securityAttributesGroup_resOwnerProducer>No Information</tds:restriction.securityAttributesGroup_resOwnerProducer>
    <tds:restriction.securityAttributesGroup_resClassificationAlternate>No
Information</tds:restriction.securityAttributesGroup_resClassificationAlternate>
    <tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterval_low>No
Information</tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterval_low>
    <tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterval_high>No
Information</tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterval_high>

<tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterval_closure>closedInterval</tds:restriction.securityAttributesGroup_r
esClassificationAlternateDateInterval_closure>
    <tds:specifiedEnumerants>No Information</tds:specifiedEnumerants>
    <tds:uniqueEntityIdentifier>No Information</tds:uniqueEntityIdentifier>
    <tds:width>57</tds:width>
    </tds:LandAerodromeGeosurface> </wfs:member>
  <wfs:member> <tds:LandAerodromeGeosurface gml:id="AeronauticalSurfaces.1053">
    <tds:geometry>
      <gml:Polygon gml:id="AeronauticalSurfaces.ObjectID.1053.SHAPE.Geom_0">
        <gml:exterior>
          <gml:LinearRing>
            <gml:posList>36.6824270430001 -121.759332736 36.6816130280001 -121.757754374
              36.6815247280001 -121.757500512 36.6809894090001 -121.757277002 36.680478925
              -121.756267071 36.6794524370001 -121.755177118 36.6789640280001 -121.754661115
              36.6779016690001 -121.753496659 36.6777333470001 -121.753328337 36.6773442750001
              -121.752980656 36.67657165 -121.752279775 36.6763122690001 -121.752056266 36.675252669
              -121.752221828 36.674565585 -121.754026459 36.67264506 -121.755555153 36.6711743130001
              -121.756722368 36.672780269 -121.759840461 36.6721290570001 -121.760350946
              36.6724850160001 -121.761032511 36.6727306010001 -121.761520921 36.6727857880001
              -121.761672686 36.6728575320001 -121.761932067 36.673310069 -121.762837142
              36.6736660290001 -121.763526986 36.6737764040001 -121.763449723 36.67392541
              -121.763722902 36.6739679930001 -121.763688515 36.674807107 -121.763035535
              36.6748553190001 -121.762986148 36.6752692250001 -121.762696414 36.675109182
              -121.762387364 36.675569997 -121.76200933 36.6757686720001 -121.761835489 36.675967347
              -121.762210764 36.6760915190001 -121.762119705 36.676171541 -121.762252155
              36.676453919 -121.762061541 36.676254252 -121.761667973 36.676557023 -121.761426243
              36.67675669 -121.761819811 36.6770352250001 -121.761570589 36.677082134 -121.761542996
              36.6768613840001 -121.761104255 36.6769745190001 -121.761029752 36.6768089560001
              -121.760717943 36.677482244 -121.760179864 36.6780286000001 -121.761173239
              36.6785777150001 -121.762238358 36.677926503 -121.762787474 36.6786825720001
              -121.764252701 36.678828819 -121.764318926 36.6789220590001 -121.764256716
              36.678675334 -121.763771104 36.679047403 -121.763465096 36.6792942930001
              -121.763966499 36.679358619 -121.763921576 36.6794883090001 -121.764167161
              36.679342062 -121.764288573 36.6798221930001 -121.765188129 36.6797973590001
              -121.765251595 36.6796787060001 -121.765350933 36.680169875 -121.766286361
              36.6803161220001 -121.766167707 36.6810777090001 -121.767630176 36.6804844430001
              -121.768113067 36.680931462 -121.768976751 36.6810308 -121.768996066 36.681243271
              -121.768985029 36.6813301780001 -121.768940226 36.6816334150001 -121.769196859
              36.681822868 -121.769637058 36.6810316240001 -121.770249994 36.6808978930001
              -121.769993675 36.6803518230001 -121.770328004 36.6818863390001 -121.773339263
              36.6819624820001 -121.773491548 36.6820005530001 -121.773505825 36.682038624
              -121.773496307 36.6837375590001 -121.772135256 36.6846535920001 -121.77140153
              36.6856744410001 -121.770583847 36.6874904960001 -121.769139554 36.686739946
              -121.767652251 36.685611361 -121.765483383 36.6849242770001 -121.764150605
              36.6840247210001 -121.762423236 36.683163796 -121.760734499 36.6824270430001
              -121.759332736</gml:posList>
          </gml:LinearRing>
        </gml:exterior>
      </gml:Polygon>
    </tds:geometry>
    <tds:address>No Information</tds:address>
    <tds:aerodromeElevation>-999999</tds:aerodromeElevation>
    <tds:aerodromeOfficialName>No Information</tds:aerodromeOfficialName>
    <tds:airfieldSymbolType>noInformation</tds:airfieldSymbolType>
    <tds:airfieldType>noInformation</tds:airfieldType>
    <tds:area>-999999</tds:area>
    <tds:conditionOfFacility>noInformation</tds:conditionOfFacility>
    <tds:controllingAuthority>noInformation</tds:controllingAuthority>
    <tds:facilityOperationalStatus>noInformation</tds:facilityOperationalStatus>

<tds:geointAssuranceMetadata.processStep.source.resourceContentOrigin>noInformation</tds:geointAssuranceMetadata.processStep.source.resourceConte
ntOrigin>
    <tds:geoNameCollection.memberGeoName.fullName>No Information</tds:geoNameCollection.memberGeoName.fullName>
    <tds:geoNameCollection.memberGeoName.nameIdentifier>-999999</tds:geoNameCollection.memberGeoName.nameIdentifier>
    <tds:highestElevation>-999999</tds:highestElevation>
    <tds:icaoLocationIndicator>No Information</tds:icaoLocationIndicator>
    <tds:length>-999999</tds:length>
    <tds:note.memorandum>No Information</tds:note.memorandum>
    <tds:portOfEntry>noInformation</tds:portOfEntry>
    <tds:restriction.securityAttributesGroup_resClassification>U</tds:restriction.securityAttributesGroup_resClassification>
    <tds:restriction.securityAttributesGroup_resNonIntelComMarkings>No
Information</tds:restriction.securityAttributesGroup_resNonIntelComMarkings>
    <tds:restriction.securityAttributesGroup_resOwnerProducer>No Information</tds:restriction.securityAttributesGroup_resOwnerProducer>
    <tds:restriction.securityAttributesGroup_resClassificationAlternate>No
```

```
Information</tds:restriction.securityAttributesGroup_resClassificationAlternate>
    <tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterval_low>No
Information</tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterval_low>
    <tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterval_high>No
Information</tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterval_high>

<tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterval_closure>closedInterval</tds:restriction.securityAttributesGroup_r
esClassificationAlternateDateInterval_closure>
    <tds:specifiedEnumerants>No Information</tds:specifiedEnumerants>
    <tds:uniqueEntityIdentifier>No Information</tds:uniqueEntityIdentifier>
    <tds:width>-999999</tds:width>
    </tds:LandAerodromeGeosurface> </wfs:member>
  <wfs:member> <tds:LandAerodromeGeosurface gml:id="AeronauticalSurfaces.1054">
    <tds:geometry>
      <gml:Polygon gml:id="AeronauticalSurfaces.ObjectID.1054.SHAPE.Geom_0">
        <gml:exterior>
          <gml:LinearRing>
            <gml:posList>36.5918880140001 -121.847980296 36.5918737380001 -121.847837528
              36.591945121 -121.847580547 36.592006987 -121.847038029 36.5920307820001 -121.84659545
              36.5920022280001 -121.846381298 36.5919213270001 -121.846186182 36.591726211
              -121.845905406 36.5915501310001 -121.845724567 36.5913883280001 -121.845653183
              36.5912550780001 -121.845634147 36.591136105 -121.845676978 36.5909362300001
              -121.845757879 36.5908077390001 -121.845786433 36.590664971 -121.845791192
              36.590545998 -121.845762638 36.5904079900001 -121.845696013 36.5902081150001
              -121.845519933 36.5900510700001 -121.845267711 36.589813124 -121.844929827
              36.589684633 -121.84465381 36.5896132500001 -121.844363515 36.589584696 -121.844054185
              36.5896132500001 -121.843564016 36.5898036070001 -121.842997705 36.5900034810001
              -121.842412357 36.5900891420001 -121.842022126 36.590136731 -121.841679483
              36.590189079 -121.841136966 36.590260463 -121.840346985 36.5902319100001
              -121.839923441 36.5901272130001 -121.839557004 36.5899892040001 -121.839304781
              36.589798848 -121.839024005 36.589556143 -121.838728952 36.58938958 -121.8385148
              36.589289643 -121.838367274 36.5892135 -121.838210229 36.589161152 -121.838091256
              36.5890897680001 -121.838038908 36.5889470010001 -121.837991319 36.588761403
              -121.837958006 36.588566287 -121.837967524 36.5884330370001 -121.838005596
              36.588322197 -121.83749556 36.5876987140001 -121.835940519 36.5870825650001
              -121.834517509 36.5869358630001 -121.834077404 36.5868771820001 -121.834033393
              36.5867671560001 -121.834026058 36.5865764430001 -121.834040728 36.586437077
              -121.834048063 36.586268369 -121.833938037 36.5861510080001 -121.833754659
              36.586055651 -121.833556611 36.585886944 -121.833189856 36.585740242 -121.833043154
              36.5855568650001 -121.832911123 36.5853441470001 -121.832837772 36.5850507430001
              -121.832837772 36.5847059930001 -121.832837772 36.58448594 -121.832757086
              36.5842878920001 -121.832632389 36.5841118500001 -121.832522362 36.583928472
              -121.832434341 36.5837524300001 -121.83237566 36.583547047 -121.832302309
              36.5834076800001 -121.832184948 36.5832463080001 -121.832038246 36.583150952
              -121.831950225 36.583048261 -121.831920884 36.582938234 -121.83195756 36.5828868880001
              -121.832060251 36.582813537 -121.832280304 36.582747521 -121.832830437 36.582740186
              -121.83348326 36.5826741700001 -121.834282786 36.5826741700001 -121.834810913
              36.5826521650001 -121.835162998 36.5826154900001 -121.83562511 36.5825494740001
              -121.835757141 36.582432112 -121.835815822 36.5823074150001 -121.835808487
              36.5821167030001 -121.835823157 36.5819479960001 -121.835903843 36.581874645
              -121.836006535 36.5818086290001 -121.836380625 36.5817352780001 -121.837033449
              36.58230008 -121.838683846 36.5831362820001 -121.840994402 36.5832022980001
              -121.841236461 36.583771676 -121.840885977 36.5840119650001 -121.840861948
              36.5842162100001 -121.840970077 36.5843964260001 -121.841126265 36.5846367140001
              -121.841498712 36.584768873 -121.841787057 36.5850812470001 -121.842652095
              36.585333797 -121.843494079 36.585136699 -121.843592628 36.584841053 -121.843783566
              36.584773301 -121.843888274 36.5847486640001 -121.844060734 36.5848040970001
              -121.844245513 36.5850011950001 -121.844812169 36.584767141 -121.844935355
              36.5849827170001 -121.845569763 36.5849703980001 -121.845791497 36.5850504690001
              -121.846111781 36.5851221180001 -121.846314787 36.5841681520001 -121.846809082
              36.5843363540001 -121.847578004 36.584192181 -121.847626062 36.5841080800001
              -121.847794263 36.5841080800001 -121.84805858 36.583987936 -121.848334912 36.583850581
              -121.848426482 36.5838604480001 -121.848466771 36.5839389700001 -121.848979782
              36.583965144 -121.849403802 36.5839756130001 -121.84975977 36.5842203660001
              -121.849711593 36.5844392760001 -121.849587861 36.585284232 -121.848968022
              36.5858098460001 -121.848555175 36.585962131 -121.848464756 36.5860811040001
              -121.848440961 36.5863857310001 -121.849561799 36.587038555 -121.851424914
              36.587141246 -121.852195099 36.5867891610001 -121.852356472 36.587163251
              -121.853559428 36.587185257 -121.85369146 36.5872806130001 -121.853830827
              36.5874713260001 -121.853933518 36.5876106920001 -121.853962858 36.5877647300001
              -121.854043544 36.5878454160001 -121.854146236 36.5879114320001 -121.854402964
              36.5879774470001 -121.854696368 36.587992118 -121.854975102 36.587992118 -121.85518782
              36.5879554420001 -121.855730617 36.5879701120001 -121.856134048 36.588006788
              -121.85664017 36.5879994530001 -121.856977584 36.587962777 -121.857190302
              36.5879187670001 -121.85737368 36.587838081 -121.857476371 36.5878014050001
              -121.857872466 36.587265943 -121.860461756 36.5873172880001 -121.860769831
              36.587531663 -121.861053045 36.5875497970001 -121.861057062 36.587613047
              -121.861160562 36.587843047 -121.861396312 36.5885194310001 -121.861958058 36.58901066
              -121.862459283 36.5894233930001 -121.860759794 36.5896965250001 -121.860456314
              36.5901820940001 -121.858253048 36.5919180000001 -121.857093753 36.592130437
              -121.856668881 36.5921182970001 -121.856159034 36.592027253 -121.855819137
              36.5912989010001 -121.853506617 36.591226066 -121.852936075 36.5912199960001
              -121.852232001 36.5912746220001 -121.852140957 36.591341388 -121.852116678
              36.591432432 -121.852122748 36.591748051 -121.852207722 36.5922275500001
              -121.852201653 36.592409638 -121.851612901 36.5926066120001 -121.851796951
              36.5930894200001 -121.852001926 36.593427971 -121.852322658 36.5935413 -121.851839117
              36.5935591460001 -121.8512502 36.59363053 -121.850197289 36.5932676620001
              -121.84975114 36.592906424 -121.849360383 36.592806486 -121.849222375 36.592535228
              -121.848903527 36.5921021660001 -121.848375287 36.5919641570001 -121.848175412
              36.5919118090001 -121.848070716 36.5918880140001 -121.847980296</gml:posList>
          </gml:LinearRing>
        </gml:exterior>
      </gml:Polygon>
    </tds:geometry>
    <tds:address>No Information</tds:address>
    <tds:aerodromeElevation>-999999</tds:aerodromeElevation>
    <tds:aerodromeOfficialName>No Information</tds:aerodromeOfficialName>
    <tds:airfieldSymbolType>noInformation</tds:airfieldSymbolType>
    <tds:airfieldType>major</tds:airfieldType>
    <tds:area>-999999</tds:area>
    <tds:conditionOfFacility>fullyFunctional</tds:conditionOfFacility>
    <tds:controllingAuthority>noInformation</tds:controllingAuthority>
    <tds:facilityOperationalStatus>noInformation</tds:facilityOperationalStatus>

<tds:geointAssuranceMetadata.processStep.source.resourceContentOrigin>noInformation</tds:geointAssuranceMetadata.processStep.source.resourceConte
ntOrigin>
    <tds:geoNameCollection.memberGeoName.fullName>No Information</tds:geoNameCollection.memberGeoName.fullName>
    <tds:geoNameCollection.memberGeoName.nameIdentifier>-999999</tds:geoNameCollection.memberGeoName.nameIdentifier>
    <tds:highestElevation>-999999</tds:highestElevation>
    <tds:icaoLocationIndicator>No Information</tds:icaoLocationIndicator>
    <tds:length>-999999</tds:length>
    <tds:note.memorandum>No Information</tds:note.memorandum>
    <tds:portOfEntry>noInformation</tds:portOfEntry>
    <tds:restriction.securityAttributesGroup_resClassification>U</tds:restriction.securityAttributesGroup_resClassification>
    <tds:restriction.securityAttributesGroup_resNonIntelComMarkings>No
Information</tds:restriction.securityAttributesGroup_resNonIntelComMarkings>
    <tds:restriction.securityAttributesGroup_resOwnerProducer>No Information</tds:restriction.securityAttributesGroup_resOwnerProducer>
    <tds:restriction.securityAttributesGroup_resClassificationAlternate>S</tds:restriction.securityAttributesGroup_resClassificationAlternate>
    <tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterval_low>2013-01-
12T00:00:00Z</tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterval_low>
    <tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterval_high>2013-01-
13T00:00:00Z</tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterval_high>

<tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterval_closure>gteToLtInterval</tds:restriction.securityAttributesGroup_
resClassificationAlternateDateInterval_closure>
    <tds:specifiedEnumerants>No Information</tds:specifiedEnumerants>
    <tds:uniqueEntityIdentifier>No Information</tds:uniqueEntityIdentifier>
    <tds:width>-999999</tds:width>
    </tds:LandAerodromeGeosurface> </wfs:member>
  <wfs:member> <tds:LandAerodromeGeosurface gml:id="AeronauticalSurfaces.1055">
    <tds:geometry>
      <gml:Polygon gml:id="AeronauticalSurfaces.ObjectID.1055.SHAPE.Geom_0">
        <gml:exterior>
          <gml:LinearRing>
            <gml:posList>36.6682753790001 -121.608620248 36.6665407520001 -121.607213987
              36.6665121990001 -121.607178295 36.6665121990001 -121.607114049 36.6683511530001
              -121.604562379 36.668498679 -121.604721803 36.6684988580001 -121.604721459
              36.6685077760001 -121.604704309 36.668578129 -121.604569014 36.6690245400001
              -121.603710532 36.669429048 -121.602944346 36.6688746340001 -121.60239469 36.667808635
              -121.601331071 36.6674421980001 -121.600955116 36.6672684980001 -121.600824246
              36.667189976 -121.600877784 36.6668366260001 -121.601484546 36.666322662
          -121.601074089 36.6653595760001 -121.600258242 36.6634030540001 -121.598557402
          36.662936157 -121.598138677 36.661854141 -121.59725676 36.661413182 -121.596641641
          36.6613724210001 -121.596578647 36.661246433 -121.595448459 36.6601533 -121.595611502
          36.66022 -121.596274793 36.660194061 -121.596541592 36.660034723 -121.597857056
          36.6600087850001 -121.598046038 36.6599791400001 -121.598075683 36.6594233100001
          -121.598501819 36.6592936170001 -121.598638924 36.659241739 -121.598790851
          36.659241739 -121.599072471 36.6592565610001 -121.599457847 36.6590972230001
          -121.600158193 36.6585154540001 -121.600084082 36.6577150590001 -121.599702412
          36.6563699500001 -121.59968759 36.6559475190001 -121.600454636 36.6558400590001
          -121.60051763 36.6557288930001 -121.60072514 36.656344011 -121.601217976 36.656503349
          -121.602040604 36.656699743 -121.602959577 36.656729387 -121.603085565
          36.6566589820001 -121.603237492 36.6564725050001 -121.603545235 36.6563958890001
          -121.603674745 36.6567145650001 -121.604260219 36.6570851180001 -121.605820249
          36.6574334380001 -121.606476129 36.657744703 -121.606424251 36.657781759 -121.60679851
          36.657707648 -121.606824449 36.6576187150001 -121.606909676 36.657585365
          -121.607046781 36.6575927760001 -121.607228352 36.6575334880001 -121.607402512
          36.6573926770001 -121.607532206 36.657255573 -121.607776771 36.657174051
          -121.607843471 36.6571110570001 -121.607858293 36.6570554740001 -121.60780271
          36.6568405530001 -121.607584084 36.656788675 -121.607580378 36.6567442090001
          -121.607598906 36.6566775090001 -121.607658194 36.656392183 -121.608147325
          36.656484822 -121.608895843 36.656803498 -121.609622127 36.657077707 -121.610252068
          36.657147932 -121.610380216 36.657282878 -121.610670349 36.6573919420001
          -121.610984697 36.6575061560001 -121.611522455 36.6575204330001 -121.611684259
          36.6577356180001 -121.612181243 36.6578032140001 -121.612346737 36.658106231
          -121.612321097 36.6581505180001 -121.612710358 36.658600382 -121.612682387
          36.6588964060001 -121.61333737 36.6586190290001 -121.613535497 36.658915053
          -121.614234767 36.659329954 -121.61519976 36.659723876 -121.616099487 36.660169078
          -121.617176363 36.6607075160001 -121.618421064 36.660866347 -121.618796126
          36.661178358 -121.619532904 36.661639876 -121.620556169 36.6617954640001
          -121.620424145 36.662104689 -121.6200581 36.6621023100001 -121.619931988 36.662118966
          -121.619767806 36.662140381 -121.61965835 36.6623854650001 -121.619379953
          36.6627281080001 -121.619648832 36.6632730040001 -121.620050961 36.66355616
          -121.619501306 36.6637179640001 -121.619603623 36.664262874 -121.618509893
          36.664242255 -121.618435663 36.665157761 -121.616678881 36.6653020970001
          -121.616390208 36.6654057800001 -121.616447552 36.6663081070001 -121.614613632
          36.6669568070001 -121.613340619 36.6670190900001 -121.61321939 36.66732419
          -121.613493979 36.668659662 -121.614677761 36.669233707 -121.615186371
          36.6696471390001 -121.614537968 36.6696054980001 -121.614511199 36.6698374960001
          -121.614109665 36.6697125740001 -121.614002589 36.6696560620001 -121.614079922
          36.6688886860001 -121.613422595 36.6689392490001 -121.613351212 36.667859569
          -121.612399427 36.667791159 -121.612212045 36.667826851 -121.612042508 36.668082579
          -121.611570085 36.668391973 -121.61099852 36.6684365880001 -121.610924161
          36.6684633570001 -121.610906315 36.669281891 -121.611325695 36.6696673640001
          -121.61073321 36.669895792 -121.610183554 36.6694603510001 -121.609562515
          36.6682753790001 -121.608620248</gml:posList>
      </gml:LinearRing>
    </gml:exterior>
```

```
      </gml:Polygon>
    </tds:geometry>
    <tds:address>No Information</tds:address>
    <tds:aerodromeElevation>-999999</tds:aerodromeElevation>
    <tds:aerodromeOfficialName>No Information</tds:aerodromeOfficialName>
    <tds:airfieldSymbolType>noInformation</tds:airfieldSymbolType>
    <tds:airfieldType>major</tds:airfieldType>
    <tds:area>1971728</tds:area>
    <tds:conditionOfFacility>noInformation</tds:conditionOfFacility>
    <tds:controllingAuthority>noInformation</tds:controllingAuthority>
    <tds:facilityOperationalStatus>continuous</tds:facilityOperationalStatus>

<tds:geointAssuranceMetadata.processStep.source.resourceContentOrigin>noInformation</tds:geointAssuranceMetadata.processStep.source.resourceConte
ntOrigin>
    <tds:geoNameCollection.memberGeoName.fullName>No Information</tds:geoNameCollection.memberGeoName.fullName>
    <tds:geoNameCollection.memberGeoName.nameIdentifier>-999999</tds:geoNameCollection.memberGeoName.nameIdentifier>
    <tds:highestElevation>-999999</tds:highestElevation>
    <tds:icaoLocationIndicator>No Information</tds:icaoLocationIndicator>
    <tds:length>2063</tds:length>
    <tds:note.memorandum>No Information</tds:note.memorandum>
    <tds:portOfEntry>noInformation</tds:portOfEntry>
    <tds:restriction.securityAttributesGroup_resClassification>U</tds:restriction.securityAttributesGroup_resClassification>
    <tds:restriction.securityAttributesGroup_resNonIntelComMarkings>No
Information</tds:restriction.securityAttributesGroup_resNonIntelComMarkings>
    <tds:restriction.securityAttributesGroup_resOwnerProducer>No Information</tds:restriction.securityAttributesGroup_resOwnerProducer>
    <tds:restriction.securityAttributesGroup_resClassificationAlternate>No
Information</tds:restriction.securityAttributesGroup_resClassificationAlternate>
    <tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterval_low>No
Information</tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterval_low>
    <tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterval_high>No
Information</tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterval_high>

<tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterval_closure>closedInterval</tds:restriction.securityAttributesGroup_r
esClassificationAlternateDateInterval_closure>
    <tds:specifiedEnumerants>No Information</tds:specifiedEnumerants>
    <tds:uniqueEntityIdentifier>No Information</tds:uniqueEntityIdentifier>
    <tds:width>1537</tds:width>
    </tds:LandAerodromeGeosurface> </wfs:member>
  <wfs:member> <tds:LandAerodromeGeosurface gml:id="AeronauticalSurfaces.1056">
    <tds:geometry>
      <gml:Polygon gml:id="AeronauticalSurfaces.ObjectID.1056.SHAPE.Geom_0">
        <gml:exterior>
          <gml:LinearRing>
            <gml:posList>36.940691332 -121.785826105 36.9391956360001 -121.784599963
              36.9393279010001 -121.784441258 36.939156579 -121.784041509 36.939277932 -121.78394871
              36.938992397 -121.783192041 36.9381928980001 -121.781414584 36.9374290910001
              -121.781985655 36.9371007250001 -121.779986907 36.937272046 -121.779851278 36.93685802
              -121.778859043 36.9363077620001 -121.779260584 36.936103948 -121.779474589
              36.9358797520001 -121.779759929 36.9357370820001 -121.780004506 36.93565799
              -121.780183781 36.935584222 -121.78035099 36.935431361 -121.780870716 36.9352377380001
              -121.781533112 36.9349727790001 -121.78208341 36.9345243880001 -121.782908858
              36.9341170020001 -121.78365278 36.9335868430001 -121.784620896 36.932068428
              -121.787423341 36.931875867 -121.787774076 36.931497748 -121.788462793
              36.9312837430001 -121.788911184 36.9311818360001 -121.789237287 36.9311116220001
              -121.789652278 36.931061653 -121.78995209 36.9309270690001 -121.790745511 36.930865924
              -121.79116333 36.930818948 -121.79158678 36.9307454450001 -121.791871955
              36.9306739620001 -121.792149293 36.930521775 -121.792544979 36.9303188580001
              -121.792889937 36.9300601400001 -121.793199384 36.9297050370001 -121.793498686
              36.9294997470001 -121.793660387 36.9289643920001 -121.79408207 36.9284875390001
              -121.794462538 36.927660302 -121.795153251 36.926985958 -121.79566989 36.9268084070001
              -121.795786567 36.92613371 -121.796126452 36.925585557 -121.79636784 36.925727877
              -121.796968554 36.925798898 -121.797359168 36.92601196 -121.798150542 36.9261387830001
              -121.798804947 36.926328905 -121.798925037 36.926593025 -121.798882207 36.926742931
              -121.798739439 36.9268999760001 -121.79856098 36.9270570200001 -121.798432489
              36.9273068640001 -121.798289721 36.9277922740001 -121.798111262 36.9286988480001
              -121.797782896 36.9288487540001 -121.797640128 36.9289558300001 -121.797490222
              36.9290700440001 -121.797226102 36.929248504 -121.79688346 36.9293484410001
              -121.796676447 36.9299409270001 -121.796191037 36.9300694180001 -121.796091099
              36.9302336010001 -121.796005439 36.930404922 -121.795976885 36.930661904 -121.79595547
              36.930783256 -121.795905501 36.930926024 -121.795655658 36.9310902070001
              -121.795384399 36.9312115590001 -121.795255909 36.931411434 -121.795091726
              36.9316041700001 -121.795020342 36.9318825670001 -121.795063172 36.9321181340001
              -121.795091726 36.9323679770001 -121.795234493 36.932546437 -121.795341569
              36.9327463110001 -121.795391538 36.9328533870001 -121.795313016 36.932960463
              -121.795063172 36.9330604 -121.79476336 36.9331531990001 -121.794406441
              36.9342667870001 -121.793535558 36.9357801240001 -121.793621219 36.9356444950001
              -121.794791914 36.9360442440001 -121.794920405 36.937022203 -121.794934681
              36.9370364800001 -121.795869809 36.9370436180001 -121.795962608 36.937155906
              -121.795946278 36.938055981 -121.795905366 36.939031062 -121.795843997
              36.9394470060001 -121.795809903 36.9398254020001 -121.79575945 36.9398561310001
              -121.795755353 36.939747255 -121.795459137 36.939693606 -121.795186761 36.939652337
              -121.794749308 36.939627575 -121.793647424 36.939624893 -121.792933899
              36.9396234480001 -121.792549666 36.9396151940001 -121.790733826 36.9396193210001
              -121.789809398 36.9396151940001 -121.7894875 36.9396358290001 -121.789277027
              36.9396605900001 -121.78909957 36.939689479 -121.789021159 36.93974203 -121.788941756
              36.9409980230001 -121.787774076 36.9410041420001 -121.787768387 36.941046441
              -121.787729062 36.941168729 -121.787066666 36.9412706360001 -121.78654694 36.94132159
              -121.7862616 36.9415407990001 -121.785233619 36.940691332 -121.785826105</gml:posList>
          </gml:LinearRing>
        </gml:exterior>
      </gml:Polygon>
    </tds:geometry>
    <tds:address>No Information</tds:address>
    <tds:aerodromeElevation>-999999</tds:aerodromeElevation>
    <tds:aerodromeOfficialName>No Information</tds:aerodromeOfficialName>
    <tds:airfieldSymbolType>noInformation</tds:airfieldSymbolType>
    <tds:airfieldType>noInformation</tds:airfieldType>
    <tds:area>-999999</tds:area>
    <tds:conditionOfFacility>noInformation</tds:conditionOfFacility>
    <tds:controllingAuthority>noInformation</tds:controllingAuthority>
    <tds:facilityOperationalStatus>noInformation</tds:facilityOperationalStatus>

<tds:geointAssuranceMetadata.processStep.source.resourceContentOrigin>noInformation</tds:geointAssuranceMetadata.processStep.source.resourceConte
ntOrigin>
    <tds:geoNameCollection.memberGeoName.fullName>No Information</tds:geoNameCollection.memberGeoName.fullName>
    <tds:geoNameCollection.memberGeoName.nameIdentifier>-999999</tds:geoNameCollection.memberGeoName.nameIdentifier>
    <tds:highestElevation>-999999</tds:highestElevation>
    <tds:icaoLocationIndicator>No Information</tds:icaoLocationIndicator>
    <tds:length>-999999</tds:length>
    <tds:note.memorandum>No Information</tds:note.memorandum>
    <tds:portOfEntry>noInformation</tds:portOfEntry>
    <tds:restriction.securityAttributesGroup_resClassification>U</tds:restriction.securityAttributesGroup_resClassification>
    <tds:restriction.securityAttributesGroup_resNonIntelComMarkings>No
Information</tds:restriction.securityAttributesGroup_resNonIntelComMarkings>
    <tds:restriction.securityAttributesGroup_resOwnerProducer>No Information</tds:restriction.securityAttributesGroup_resOwnerProducer>
    <tds:restriction.securityAttributesGroup_resClassificationAlternate>No
Information</tds:restriction.securityAttributesGroup_resClassificationAlternate>
    <tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterval_low>No
Information</tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterval_low>
    <tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterval_high>No
Information</tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterval_high>

<tds:restriction.securityAttributesGroup_resClassificationAlternateDateInterval_closure>closedInterval</tds:restriction.securityAttributesGroup_r
esClassificationAlternateDateInterval_closure>
    <tds:specifiedEnumerants>No Information</tds:specifiedEnumerants>
    <tds:uniqueEntityIdentifier>No Information</tds:uniqueEntityIdentifier>
    <tds:width>-999999</tds:width>
    </tds:LandAerodromeGeosurface> </wfs:member>
</wfs:FeatureCollection>
```

Listing 8.2.5-1