OGC Testbed-15

Data Centric Security

Table of Contents

Publication Date: 2019-12-19

Approval Date: 2019-11-22

Submission Date: 2019-10-21

Reference number of this document: OGC 19-016r1

Reference URL for this document: http://www.opengis.net/doc/PER/t15-D004

Category: OGC Public Engineering Report

Editor: Name(s) Michael A. Leedahl

Title: OGC Testbed-15: Data Centric Security

OGC Public Engineering Report

COPYRIGHT

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 Public Engineering Report should not be referenced as required or mandatory technology in procurements. However, the discussions in this document could very well lead to the definition of an OGC Standard.

LICENSE AGREEMENT

Permission is hereby granted by the Open Geospatial Consortium, ("Licensor"), free of charge and subject to the terms set forth below, to any person obtaining a copy of this Intellectual Property and any associated documentation, to deal in the Intellectual Property without restriction (except as set forth below), including without limitation the rights to implement, use, copy, modify, merge, publish, distribute, and/or sublicense copies of the Intellectual Property, and to permit persons to whom the Intellectual Property is furnished to do so, provided that all copyright notices on the intellectual property are retained intact and that each person to whom the Intellectual Property is furnished agrees to the terms of this Agreement.

If you modify the Intellectual Property, all copies of the modified Intellectual Property must include, in addition to the above copyright notice, a notice that the Intellectual Property includes modifications that have not been approved or adopted by LICENSOR.

THIS LICENSE IS A COPYRIGHT LICENSE ONLY, AND DOES NOT CONVEY ANY RIGHTS UNDER ANY PATENTS THAT MAY BE IN FORCE ANYWHERE IN THE WORLD. THE INTELLECTUAL PROPERTY IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE DO NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE INTELLECTUAL PROPERTY WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE INTELLECTUAL PROPERTY WILL BE UNINTERRUPTED OR ERROR FREE. ANY USE OF THE INTELLECTUAL PROPERTY SHALL BE MADE ENTIRELY AT THE USER’S OWN RISK. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR ANY CONTRIBUTOR OF INTELLECTUAL PROPERTY RIGHTS TO THE INTELLECTUAL PROPERTY BE LIABLE FOR ANY CLAIM, OR ANY DIRECT, SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM ANY ALLEGED INFRINGEMENT OR ANY LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR UNDER ANY OTHER LEGAL THEORY, ARISING OUT OF OR IN CONNECTION WITH THE IMPLEMENTATION, USE, COMMERCIALIZATION OR PERFORMANCE OF THIS INTELLECTUAL PROPERTY.

This license is effective until terminated. You may terminate it at any time by destroying the Intellectual Property together with all copies in any form. The license will also terminate if you fail to comply with any term or condition of this Agreement. Except as provided in the following sentence, no such termination of this license shall require the termination of any third party end-user sublicense to the Intellectual Property which is in force as of the date of notice of such termination. In addition, should the Intellectual Property, or the operation of the Intellectual Property, infringe, or in LICENSOR’s sole opinion be likely to infringe, any patent, copyright, trademark or other right of a third party, you agree that LICENSOR, in its sole discretion, may terminate this license without any compensation or liability to you, your licensees or any other party. You agree upon termination of any kind to destroy or cause to be destroyed the Intellectual Property together with all copies in any form, whether held by you or by any third party.

Except as contained in this notice, the name of LICENSOR or of any other holder of a copyright in all or part of the Intellectual Property shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Intellectual Property without prior written authorization of LICENSOR or such copyright holder. LICENSOR is and shall at all times be the sole entity that may authorize you or any third party to use certification marks, trademarks or other special designations to

indicate compliance with any LICENSOR standards or specifications.

This Agreement is governed by the laws of the Commonwealth of Massachusetts. The application to this Agreement of the United Nations Convention on Contracts for the International Sale of Goods is hereby expressly excluded. In the event any provision of this Agreement shall be deemed unenforceable, void or invalid, such provision shall be modified so as to make it valid and enforceable, and as so modified the entire Agreement shall remain in full force and effect. No decision, action or inaction by LICENSOR shall be construed to be a waiver of any rights or remedies available to it.

None of the Intellectual Property or underlying information or technology may be downloaded or otherwise exported or reexported in violation of U.S. export laws and regulations. In addition, you are responsible for complying with any local laws in your jurisdiction which may impact your right to import, export or use the Intellectual Property, and you represent that you have complied with any regulations or registration procedures required by applicable law to make this license enforceable.

Chapter 1. Subject

The OGC Testbed-15 Data Centric Security Engineering Report (ER) discusses the current state of security in protecting data in a geospatial environment. The ER examines the use of encrypted container formats such as NATO STANAG 4778 "Information on standard Metadata Binding" with metadata as defined in NATO STANAG 4774 "Confidentiality Metadata Label Syntax" in combination with geospatial data using the encoding for an OGC Web Feature Service (WFS) FeatureCollection structure. This report also makes a recommendation for the creation of new media types to support output container formats such as STANAG 4778. The report then discusses various implementation scenarios in which a STANAG 4778 (eXtensible Markup Language (XML) container maintains encrypted data from author to service to viewer. These implementations use the new OGC API - Features - Part 1: Core with features encrypted using keys supplied by feature authors and users.

Chapter 2. Executive Summary

OGC members can derive business value from this ER in the following three areas:

1. Where Data Centric Security fits in with proposed standards such as OGC API for Features.
2. Techniques to use and issues that impact implementation of Data Centric Security.
3. The continuing work that remains in the area of Data Centric Security.

The motivation for data centric security is a response to the possibility of an unauthorized user who intercepts network traffic or hacks systems storing sensitive data. When looking at drafting OGC standards such as OGC API - Features in a data centric security scenario, standards need to include ways to classify the security requirements around data access. This classification can exist as additional metadata fields. The requirement stems from the need to limit different consumers to a different subset of data. Additional requirements include the need for representation of the source of the information as well as an assurance that the information has not been tampered with. A fundamental requirement for data centric security is that the data is always in an encrypted form until an authorized actor makes use of the data. As the data could pass through systems that do not belong to the data consumer nor the producer, the data must remain encrypted throughout the geospatial environment. The geospatial environment includes all infrastructure that touches the geospatial data (services, networks, storage, clients, etc.).

For the purposes of the Testbed 15 Data Centric Security (DCS) activity as documented in this ER, a requirement existed to use an open source implementation of OGC API - Features.

The Testbed-15 findings show that it is possible to support data centric security within the OGC API service framework. The ER documents three DCS scenarios:

- Scenario 1: Starts with a user requesting features, with a security proxy intercepting and modifying the request before forwarding to a vanilla OGC API – Features service. The proxy service intercepts the response to filter, encrypt and sign the response in a STANAG 4778 output format. Annex A provides additional details for this scenario.
- Scenario 2: This scenario includes a security proxy that contains a geospatial policy of classified and unclassified data. The scenario is similar to the one above in that a request is intercepted, filtered, encrypted and signed by the security proxy. The difference is that temporal decisions and spatial filtering is performed on the results of the request by the security proxy. See Annex B for more details.
- Scenario 3: Starts with a user requesting features which a security proxy intercepts, and modifies before forwarding to an OGC API - Features service that understands the STANAG 4778 output format. The security proxy intercepts the response to filter, encrypt metadata and sign the feature collection. In this scenario, the OGC API - Features service returns a feature collection with STANAG 4778 encoded feature objects. See Annex C for more details.

The first challenge, an implementer encounters, occurs when sending the request. The current code lists do not support a STANAG 4778 output format. The STANAG 4778 output format is a container format that contains encrypted portions of sensitive data and associated metadata. A sub-challenge is that the OGC API set of standards needs a way to specify both the container encoding and the format of the data in the container. Once standards such as OGC API - Features support the

documentation of containers and data and get agreement by the implementing and OGC membership communities, then interoperability with 4778 is possible. However, this may not be the only factor in interoperability. STANAG 4778 may not be an appropriate output format, especially when there may be a variety of different DCS formats in the future. One of the issues that different DCS formats may expose in the future is how to express a feature collection where items could be in different DCS formats. This could be caused by different content authors contributing to the feature collection.

The next challenge for implementation, which is outside the scope of OGC API standards work, of Key Management. In the first and second scenarios, the OGC API service does not know anything about keys. The feature data is either not encrypted in the storage container or the data is encrypted by the file system or the database system. The security proxy (PDP/PEP) encrypts the data as the data is returned to the authorized actor. This allows the OGC API - Features service to search the data that are visible to the service. In the third scenario, the OGC API - Features service either needs authorization to access keys or the services ability to filter data is limited. One challenge that is within the scope of OGC API standards is the description and negotiation of key management. Currently there are no markings in the service to specify whether the metadata is encrypted with the public key of the client or if the metadata contains the key for the sensitive encrypted feature data. There are potentially other key management methods which client and service implementations may use in negotiation and description of key management.

Another challenge that an OGC Standards Working Group (SWG) should address is the inclusion of a digital signature element in the scheme of a feature collection. Current standards, such as OGC API - Features, do not contain a digital signature as part of the scheme. The testbed participants were able to add one for the purposes of demonstrating Data Centric Security. However, the resulting feature collection will fail in the WFS FeatureCollection schema validation. This issue is demonstrated in scenario three where the OGC API - Features service returns a feature collection with STANAG 4778 encoded features.

Future testbeds should investigate:

- Additional container formats for encoding output formats. In this testbed, STANAG 4778 was chosen because of its use by NATO Partner Nations for exchanging data. The STANAG XML format is useful for systems that are working with XML data. Other encoding formats exist and some applications, particularly in the commercial sector, may not be as keen to support XML. An investigation in using a JavaScript Object Notation (JSON) based encoding would be beneficial as many applications today exchange information using JSON.
- Key management markings. When running the tests in the testbed, notice that the metadata contains the symmetric key for decrypting the feature data and the metadata is encrypted with the public key of the user. An alternative key management scenario may store the keys in a key management service and require the client to fetch the key via a key identifier stored in the metadata. There should be some indication to the client of where to fetch the keys from and how to decrypt the features and metadata.
- Authentication and Authorization Protocols. To run the tests in this testbed, OAuth 2 was used to issue a bearer token for access delegation. OAuth 2 scopes are validated along with GeoXACML to define authorization. Future implementations should evaluate data provenance using assertions, Blockchain technologies, or other standards.

- Using XML Digital Signature in OGC encoding standards. Scenario Three demonstrates the ability to include a set of STANAG 4778 container objects in a WFS FeatureCollection result. Putting a STANAG 4778 container object in as a feature works because the feature collection schema allows for a type of `xs:any`. Applying a digital signature to the final feature collection results in an invalid structure as the schema defined in `wfs.xsd` does not support the insertion of a W3C XML Digital Signature element. From the testbed results, the participants encourage OGC SWGs working on OGC API standards to add optional schema elements that allow the use of XML Digital Signatures. See the OGC Change Request #614 [http://ogc.standardstracker.org/show_request.cgi?id=614] for more information.

2.1. Document contributor contact points

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

Contacts

Name	Organization	Role
Michael Leedahl	Maxar Technologies, Inc.	Editor
Andreas Matheus	Secure Dimensions	Contributor
George Elphick	Helyx Secure Information Systems	Contributor
Donovan Dall	Helyx Secure Information Systems	Contributor
Matt Knight	Helyx Secure Information Systems	Contributor

2.2. Foreword

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.

Chapter 3. References

The following normative documents are referenced in this document.

- NATO: "ADatP-4774" Confidentiality Metadata Label Syntax, edition A version 1, NSO, 2017. [https://nso.nato.int/nso/zPublic/ap/PROM/ADatP-4774%20EDA%20V1%20E.pdf]
- NATO: "ADatP-4778" Metadata Binding Mechanism, edition A version 1, NSO, 2018. [https://nso.nato.int/nso/zPublic/ap/PROM/ADatP-4778%20EDA%20V1%20E.pdf]
- OGC: OGC 17-069r1, OGC® API - Features - Part 1:Core Standard [http://docs.opengeospatial.org/DRAFTS/17-069r1.html]
- OGC: OGC 09-025r2, OGC® Web Feature Service 2.0 Interface Standard [http://docs.opengeospatial.org/is/09-025r2/09-025r2.html]
- IETF: The OAuth 2.0 Authorization Framework [https://tools.ietf.org/html/rfc6749]
- IETF: The OAuth 2.0 Authorization Framework: Bearer Token Usage [https://tools.ietf.org/html/rfc6750]
- OGC: GeoXACML 1.0, OGC Implementation Specification [http://portal.opengeospatial.org/files/?artifact_id=42734]
- OGC: GeoXACML3 - Core, OGC Discussion Paper [http://www.opengis.net/doc/DP/GEOXACML-CORE]
- OGC: GeoXACML3 - GML 3.2.1 Encoding Extension, OGC Discussion Paper [http://www.opengis.net/doc/DP/GEOXACML/GML3-Extension]
- OASIS: XACML 3, OASIS Standard [http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html]

Chapter 4. Terms and definitions

For the purposes of this report, the definitions specified in Clause 4 of the OWS Common Implementation Standard OGC 06-121r9 [https://portal.opengeospatial.org/files/?artifact_id=38867&version=2] shall apply. In addition, the following terms and definitions apply.

- **AS**

  OAuth2 Authorization Server — a component that dispatches, validates manages bearer access tokens.

- **GeoPDP**

  Geospatial Policy Decision Point — a component of a policy-based system that uses a request, attributes about a request (including geospatial attributes) and a policy document to make an access decision to allow access to a resource. The GeoPDP implements the OGC GeoXACML implementation specification.

- **GeoPEP**

  Geospatial Policy Enforcement Point — a component of a geospatial aware policy-based system that works with a GeoPDP to enforce access decision and perform obligations requested by the GeoPDP.

- **OGC API - Features**

  OGC API - Features - Part 1: Core — is a new OGC standard for a feature service application programming interface that provides access to feature collections and the items in them. This standard was formally known as WFS3 for Web Feature Service version 3.

- **LDProxy**

  LDProxy — An Open Source product by Interactive Instruments which provides most of the REST implementation specified in the OGC API - Features Standard.

- **PDP**

  Policy Decision Point — a component of a policy-based system that uses a request, attributes about a request (including geospatial attributes) and a policy document to make an access decision to allow access to a resource. The PDP implements the OASIS XACML3 standard.

4.1. Abbreviated terms

- AD - Authorization Decision
- ADR - Authorization Decision Request
- AS - Authorization Server
- DCS - Data Centric Security
- DWG - Domain Working Group
- GeoPDP - Geospatial Policy Decision Point
- GeoPEP - Geospatial Policy Enforcement Point

- GeoXACML - Geospatial eXtensible Access Control Markup Language
- OAPIF - Short form of OGC API - Features - Part 1 - Core
- OGC - Open Geospatial Consortium
- PDP - Policy Decision Point
- SAML - Security Assertion Markup Language
- SWG - Standard Working Group
- TB15 - OGC Testbed-15
- WFS3 - Web Feature Service version 3 (Also known as OGC API Features)
- XACML - eXtensible Access Control Markup Language
- XML - eXtensible Markup Language
- XSLT - eXtensible Stylesheet Language Template

Chapter 5. Overview

This section provides a brief overview and description of the key sections of this Engineering Report.

Section 6 provides a look at the landscape of data centric security technologies and techniques. The section also covers considerations of implementing data centric security on performance of a feature retrieval service such as OGC API - Features.

Section 7 outlines scenarios, requirements and architecture used in the Testbed for Data Centric Security. The first of three scenarios defined in this testbed works with a proxy solution. The proxy deals with authentication, authorization and converting to a STANAG 4778 container format. The proxy is put in front of a vanilla implementation of an OGC API - Features service. The second scenario is similar to the first scenario with the exception that the proxy service applies a spatial filter on the request. The third scenario looks at an authentication and authorization system that passes through a request to an OGC API - Features service which already stores the features in a STANAG 4778 format encoding. Next the section covers requirements and presents a mapping of requirements to architectural elements. This is followed by the engineering aspects of the architecture and infrastructure setup for the Data Centric Security portion of Testbed-15.

Section 10 presents the results of the Technology Integration Experiment (TIE) testing. In general the TIEs show what happens when you call an OGC API - Features service with and without adding a security proxy in front for each scenario.

Section 11 provides a summary of the main findings. This section shows that adding data centric security using containers that conform to STANAG 4778 is possible.

Section 12 looks at additional the aspects of key management, authentication/authorization and filtering that were not covered in this testbed.

Annex A provides a demonstration and implementation instructions for scenario one.

Annex B provides a demonstration and implementation instructions for scenario two.

Annex C provides a demonstration and implementation instructions for scenario three.

Chapter 6. Data Centric Security

6.1. State of Art in Data Centric Security

When implementing a platform for data centric security, data providers and distributors need a way to:

- Authenticate agents/users;
- Prove the authenticity and Integrity of data;
- Provide the provenance and data history;
- Classify data;
- Manage rights and policies for accessing data;
- Manage keys for encrypting and decrypting data;
- Automation of encryption and decryption of data;
- Automation of data masking and unmasking;
- Discovery or cataloging of encrypted data.

Data Centric Security requires some sort of agent or client that runs on endpoints where data is being created that can assess the data and perform actions on the data as defined in policies. Often these policies are centrally managed and pushed out to the agent or client. Users or automated processes that create or use data should not be aware that the data is encrypted when they access the data.

There are many technologies and standards that are used to accomplish data centric security such as:

- Digital Rights Management (DRM)
- Data Loss Prevention (DLP)
- Key Management Interoperability Protocol (KMIP)
- Public-Key Cryptography Standards (PKCS #11)
- Information Flow Control
- Attribute-Based Access Control
- Role-Based Access Control
- W3C PROV
- Digital Signatures
- Transport Layer Security (TLS)
- Secured Hyper-Text Transfer Protocol (HTTPS)

Many of the aforementioned technologies and standards have been applied to various solutions for file and email management. When looking for solutions to these problems in a geospatial context, data centric security seems to be behind other infrastructures. There was some OGC work done on

Data Provenance in Testbed 10 [https://portal.opengeospatial.org/files/?artifact_id=58967]. Some companies published papers on various ways to record providence in metadata. Most products support HTTPS using TLS. However, this approach is a transport security model as opposed to a data centric security model. There are products available as a proxy service to provide authentication, authorization and policy access controls based on Attributes or Roles. These solutions may and often are placed in front of geospatial solutions today.

There are a number of solutions available to inspect network traffic to and from a web service or to and from a database that provide DLP and threat assessment services. These proxy services may and often are put in front of geospatial services. The common thread that all of these services have for geospatial implementations is that they are done on the network transport layer and not on the data and services themselves. This suggests that more work and experiments are needed to create and extend standards that implement DRM, DLP and Policy decisions. For example, adding markings in the data would support better decision making by the services that serve data.

6.2. Data Burden

Adding encryption will always create some additional overhead to any web implementation. This overhead is comprised of two components. The first component of overhead comes from the size of the network packets. The second component of overhead comes from performance impacts due to additional processing time on servers and clients. Returning an entire feature collection as an encrypted section in a container format could be quite large. Encryption creates binary results that are converted to base 64 encoding when put into an XML container. This conversion may expand the data volume to as much a twice its original size. This creates a burden on network communications. This reporter examines scenarios in which a proxy service in front of an OGC API Features service provides data centric security. The OGC API - Features service may or may not be aware of encrypted data stored in a data centric security container format. In both cases, a data burden is placed on the client application as it has to decrypt the data to use or present the data.

In the service that is unaware of Data Centric Security, all the encryption is done in the proxy service at request time. This could impose a burden on the data over a classic service that does not provide data centric security. However, in many classic implementations security is still enforced and encryption is applied in other forms that add a burden in terms of performance of data retrieval. The big difference is that in a classic scenario, the encryption is done on the transport layer and is communicated in a binary form. In the Data Centric Security scenario, the data is expanded to convert to an ASCII format for inclusion into a container. For example, in a classic implementation whole disk encryption or database encryption may be applied. This adds additional latency to the delivery of data in that it must be decrypted from the storage before being delivered. An additional source of overhead in a classic implementation is imposed on the transport layer as the data is often encrypted through the communication protocol such as Transport Layer Security (TLS). By using a proxy to provide data centric security, using TLS as the data is already encrypted is no longer important. However, the proxy scenario solution we present in this ER does use both asymmetric and symmetric keys to encrypt portions of the data as does TLS. In effect a classic implementation and the data centric security implementation should be similar in performance in cases where transport and storage encryption are used on a classic service.

In contrast, a data centric security aware OGC API - Features service has containers with encryption

already applied to the data in the database or on the data storage. In this scenario, the data creator had a burden to encrypt the data before putting it into the service. For this ER and testbed experiments the participants did not encrypt the metadata portion in the containers stored in the service. This allowed a proxy server to make classification and filtering decisions based on the metadata. The proxy service then used an asymmetric key to encrypt the metadata as was done in the unaware scenarios.

Another alternative to be considered for future testbeds is using a key to decrypt the metadata in the proxy service thus allowing the ability to store the metadata encrypted as well. As to data burden and performance, this solution is potentially more performant in that the proxy service is not applying encryption to the bulk of the data as it is already encrypted. There is still a burden on the client side to decrypt the data. A classic solution with network and storage encryption makes the encryption seamless to the client where a data centric security model imposes work on the client to decrypt. However, performance testing could demonstrate that it is quite possible that the scenario where features are stored as encrypted containers may actually perform a little faster than the classic solution.

In summary, encryption will always add a burden to data and performance of a system. That is certainly the case in geospatial data solutions. In this testbed, the participants did not perform any performance testing so there are no metrics to report on. Perhaps that is something best left for future testbeds. However, we can work out the data burden in a logical manner and looking at it logically, the data burden should be similar to a classic implementation where data is encrypted at rest and in motion. The client will have more of a burden in a data centric security model to decrypt data than a classic implementation would impose. A data centric aware service, such as OGC API - Features, could logically decrease some of the performance burden placed on the data.

Chapter 7. Scenarios, Requirements and Architecture

7.1. Scenarios

The driving use case for the Testbed-15 Data Centric Security activity is enabling NATO partner countries to share geodata across potentially insecure networks. To accomplish this use case, data must be secure from storage through delivery. This involves storing the data in an encrypted form in the spatial database and leaving it encrypted in transit. For a client to use this data, the client needs the ability to retrieve a key to decrypt the data. To support the NATO use case, the decision was made to encode the data in a transfer protocol format defined in STANAG 4778. This decision provides the developers with three implementation scenarios:

7.1.1. Scenario One

In this scenario, a default GeoServer implementation is put behind a Geospatial Policy Enforcement Point (GeoPEP). The GeoPEP acts as a proxy server to apply generic metadata. Further, the proxy server packages and encrypts geo-data (features) into the STANAG 4778 format. Further, the GeoPEP returns the data to the client. Figure 1 shows an example of a typical flow from client request to response using the GeoPEP proxy. This scenario leverages XACML to consider processing geographic properties of the request and response.

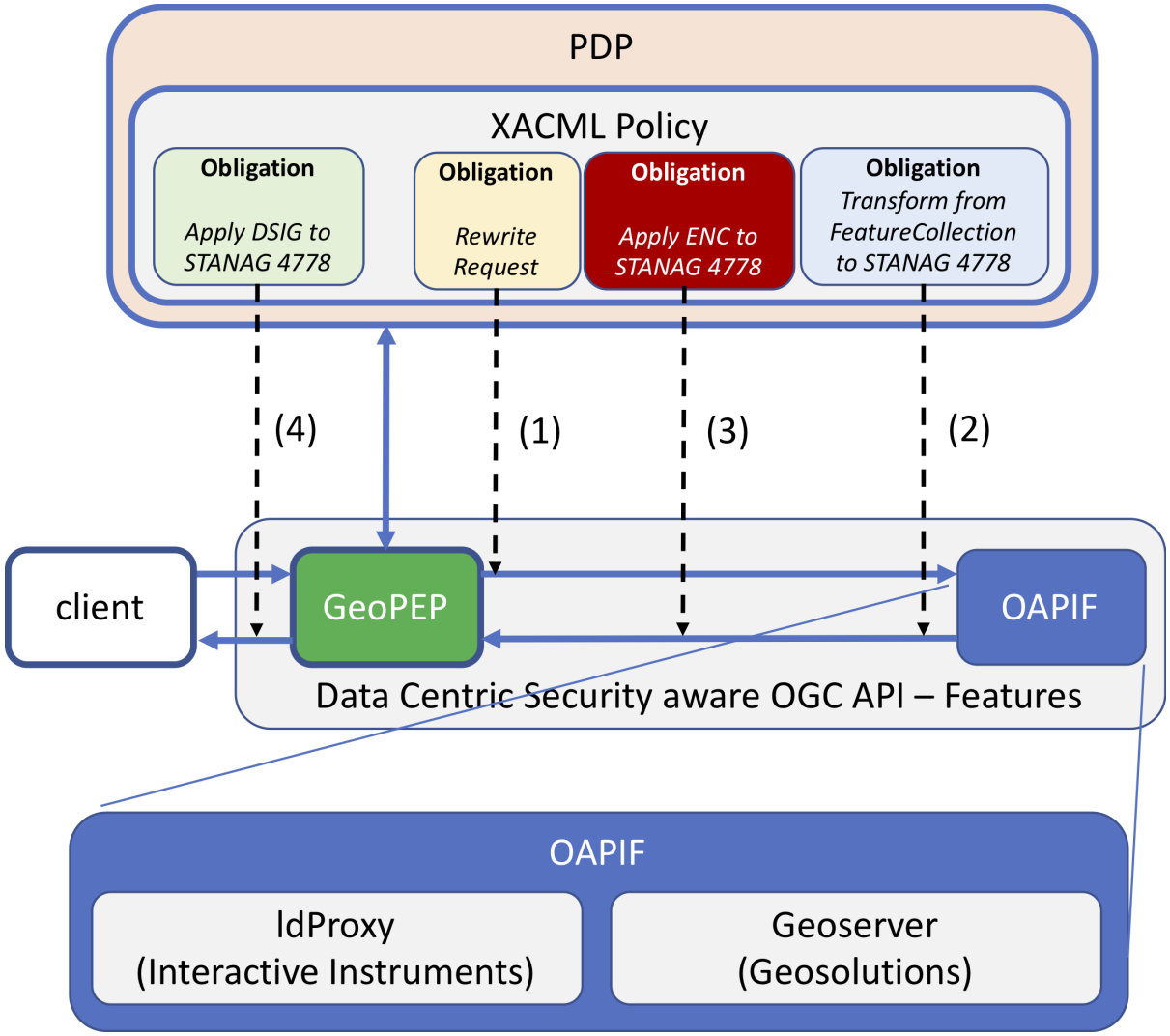

Figure 1. GeoPEP as a Proxy for STANAG 4778

1. Client sends an OGC API Features (WFS3) request.
2. The GeoPEP intercepts the request and asks the PDP if the request is allowed. The Policy Decision Point (PDP) uses a XACML Policy for a list of obligations that apply to the request parameters. XACML is an XML document that contains access control rules and obligations. The PDP responds with filter obligations on the request, a STANAG 4778 transformation with digital signature and encryption obligations on the response.
3. The GeoPEP applies the filters specified in the filter obligation to the request and sends the modified request to the OGC API Features (WFS3) service.
4. The GeoPEP receives a response from the OGC API Features (WFS3) service and applies the STANAG 4778 transformation to the response.
5. The GeoPEP creates a symmetric key to encrypt the STANAG 4778 objects, uses the public key of the user to encrypt the symmetric key for inline distribution. This step is not shown on the diagram.
6. The GeoPEP calculates the digital signature for the response and sends it to the client.

7.1.2. Scenario Two

This scenario uses the same setup as scenario one except that the GeoXAML Policy contains conditions for geographic and temporal access conditions as well as filtering. Figure 2 shows a

similar flow to scenario one except that the GeoPEP may deny the request based on spatial condition with temporal requirements. The flow in scenario two may rewrite the request to filter off of spatial requirements and ignore classification due to policy overrides for emergency situations. Lastly the flow may result in classification-based filtering as in scenario once when time and location are not a consideration.

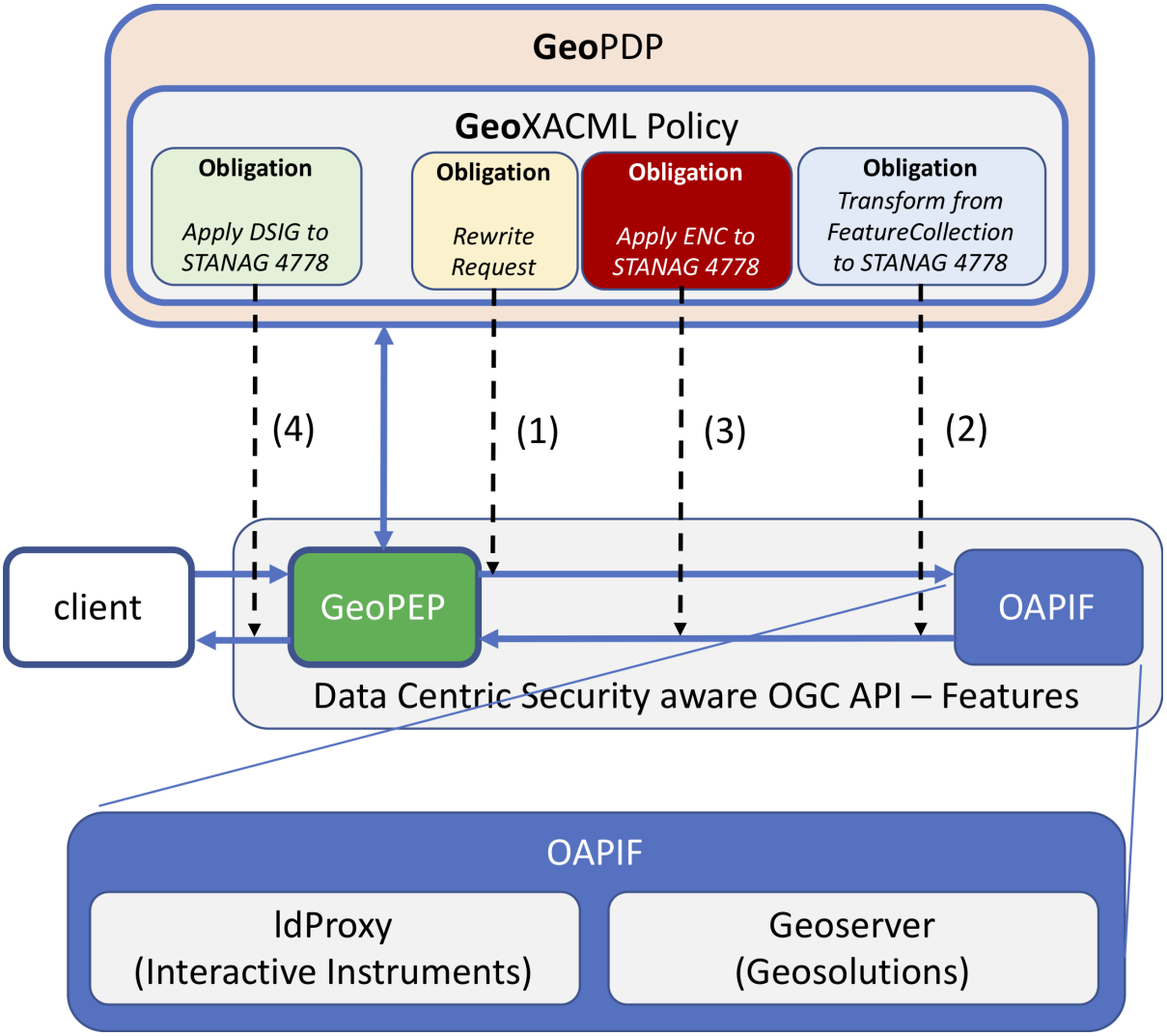

Figure 2. GeoPEP as a Proxy for STANAG 4778 with Spatial and Temporal Filtering

The steps illustrated in Figure 2 are explained as follows:

1. As in scenario one, the client sends an OGC API Features (WFS3) request.
2. The GeoPEP intercepts the request and asks the GeoPDP if the request is allowed. The GeoPDP responds with a geographic and temporal filter obligation on the request and a STANAG 4778 transformation with digital signature obligations on the response. GeoPEP applies the filters specified in the filter obligation to the request and sends the modified request to the OGC API - Features (WFS3) service.
3. The GeoPEP receives a response from the OGC API Features (WFS3) service and applies the STANAG 4778 transformation to the response.
4. The GeoPEP creates a symmetric key to encrypt the STANAG 4778 objects, uses the public key of the user to encrypt the symmetric key for inline distribution. This step is not shown on the diagram.

5. The GeoPEP calculates the digital signature for the response and sends it to the client.

7.1.3. Scenario Three

This scenario involves an OGC API - Features service that supports the STANAG 4778 format as an output format. Figure 3 shows an example of a flow from client to request to response using an OGC API - Features service supporting STANAG 4778.

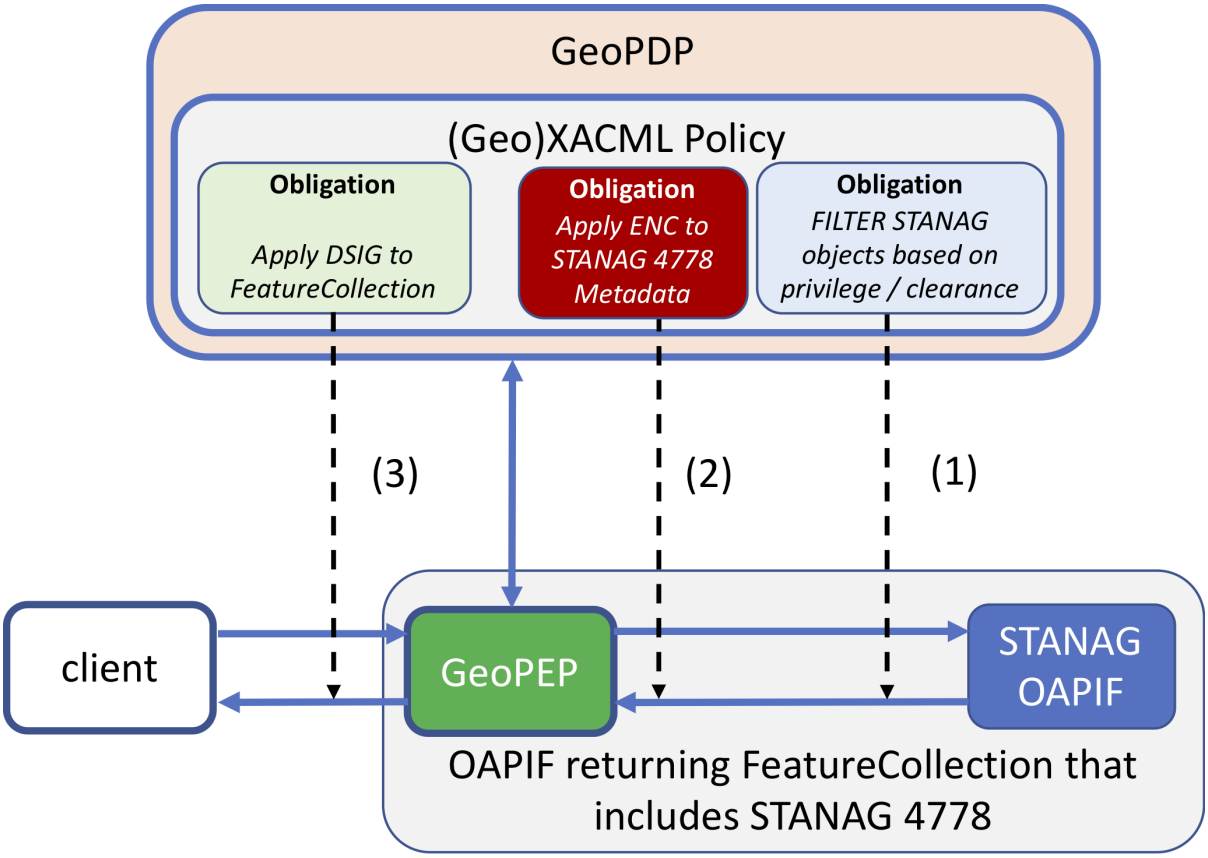

Figure 3. GeoPEP as a pass through where OGC API Features Service supports output as STANAG 4778

The steps illustrated in Figure 3 are explained as follows:

1. Client sends an OGC API Features (WFS3) request.
2. The GeoPEP intercepts the request and asks the GeoPDP if the request is allowed. The GeoPDP responds with a filter obligation on the request and a digital signature obligation on the response.
3. GeoPEP applies the filters specified in the filter obligation to the request and sends the modified request to the OGC API Features (WFS3) service.
4. The GeoPEP receives a response from the OGC API Features (WFS3) service that is already in a STANAG 4778 format. The data part is encrypted and the metadata part contains the object classification based on STANAG 4774 marking.
5. The GeoPEP first filters the STANAG objects (features) based on their classification markings and the user's clearance. Then encrypts the metadata with the public key from the user. This is not shown on the diagram.
6. The GeoPEP calculates the digital signature, applies it to the FeatureCollection and sends the response to the client.

7.2. Requirements & Implementation Mapping

7.2.1. Requirements

- **Encryption:** Features and metadata about the features shall be separately encrypted with different keys.
- **Privileges:** Different users have different access privileges and as such the system shall filter the features returned by the privilege level of the user.
- **Implementation:** The feature service shall be an implementation of the OGC API - Features service (WFS 3.0).

7.2.2. Implementation Mapping

7.2.2.1. Requirement Encryption

Features and metadata about the features shall be separately encrypted with different keys.

To implement a system with encryption for both metadata and features, this testbed is using a STANAG 4778 and 4774 data format. The STANAG 4778 specification describes an XML binding.

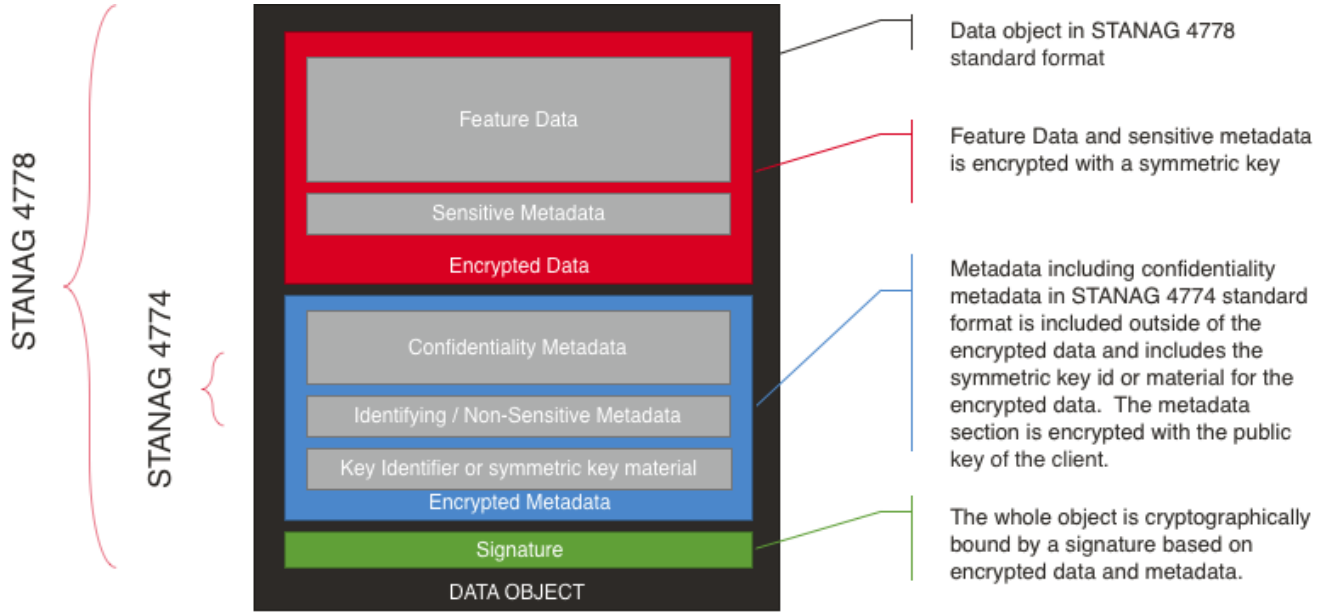

Figure 4. Data Object Format

7.2.2.2. Requirement Privileges

Different users have different access privileges and as such the system shall filter the features returned by the privilege level of the user.

Privileges are handed by a Geo-Aware Policy Enforcement Point (PEP) service and a Geo-Aware Policy Decision Point (PDP) service. GeoPDP uses GeoXACML Policy to create a set of filters to pass to the OGC API Features service and obligations to apply at the GeoPEP. For more information see the scenario section.

7.2.2.3. Requirement Implementation

The feature service shall be an implementation of the OGC API - Features service (formerly named WFS 3.0).

The implementation of the feature service should either be a …

- Vanilla OGC API Features service, as in the use case scenario one or a
- Customized OGC API - Features service that supports an XML output format that follow STANAG 4778, as in use case scenario three.

7.3. Engineering Aspects

7.3.1. Introduction

The architecture defined for the OGC Testbed 15 Data Centric Security Thread used a typical setup to enable security for exploring new innovative objectives. The objectives for the Thread were to use STANAG 4778 and 4774 combined with a WFS FeatureCollection object accessible via the implementation of OGC API - Features.

To achieve a generic setup, a Security Proxy (GeoPEP) was deployed as an OAuth2 Resource Server that operated as an interceptor to requests and responses to different backend services. For scenario one and two, the backend service was a vanilla WFS3 comprised of a Geoserver and ldproxy [https://interactive-instruments.github.io/ldproxy/] whereas for scenario three, the backend service was a STANAG 4778 aware WFS3.

This section provides a summary of the functioning of the security proxy to achieve the different objectives of the Data Centric Security Thread. More details on the functionality can be found in the Annexes A, B and C.

7.3.2. Architectural Summary

Best practices for controlling access to services or APIs involve the use of access tokens. An access - or Bearer - token represents a particular security context which can be used to undertake the required processing. For Testbed-15, the Security Proxy is setup as an RFC 6750 compliant OAuth2 Resource Server. The security context that a Bearer token represents includes the user's clearance and the public key. The user's clearance, together with the classification of the features, is used to evaluate access conditions. The security proxy, in addition to access rules, is setup to allow request rewriting and filtering of responses before the response is sent to the client.

For scenario one and two, the Security Proxy provides the functionality to transform a WFS FeatureCollection of a DCS unaware WFS3 into STANAG 4778 data format. In addition, the proxy applies encryption and a digital signature to the response. In other words, the security proxy upgrades the OGC API - Features (WFS3) to be operated as a Data Centric Security aware WFS3 exposing STANAG 4778 and FeatureCollection responses.

In order to do this, the Security Proxy must support flexible processing. This is achieved by controlling the appropriate processing via Obligations received from a Policy Decision Point. Obligation handlers used for Testbed-15 DCS are:

- Request rewriting (HTTP GET or HTTP POST with XML payload);
- Response filtering on XML payload;
- Digital Signature on the XML response;
- Encryption on the XML response.

All the different requirements in terms of processing in the Security Proxy - the GeoPEP provided by Secure Dimensions - are controlled by GeoXACML policies. For each scenario / alternative implementation, a different policy was in place that contained conditions for making access decisions but also provided processing instructions for the Security Proxy. In order to better craft GeoXACML policies, the Abbreviation Language for Authorization (ALFA) was used. ALFA is an OASIS Working Draft. The Axiomatics ALFA plugin for Eclipse was used to generate full GeoXACML policies from ALFA input (https://www.axiomatics.com).

The authorization decisions were created by a GeoPDP that has loaded different policies for the different scenarios. The GeoPDP is a GeoXACML 3 implementation which is an extension to the AuthZForce PDP. In the AuthZForce Authorization Server, different XACML functions were implemented and are available for Testbed-15 to manage policies:

- PAP: The Policy Administration Point API allows uploading and/or modifying and deletion policies that are used by the PDP.
- PDP: The PDP - extended by the GeoXACML capabilities - is the stateless service that returns GeoXACML authorization decisions

For making authorization decisions and providing GeoPEP function handler input, the GeoPEP sends collected information to the GeoPDP. The information collected by the GeoPEP comes from the intercepted request as well as information about the user from the Authorization Server. The user information is obtained by an OAuth2 / OpenID Connect enabled Authorization Server.

For illustration purposes in this testbed, the Authorization Server allows some fictitious users to login and the user claims are made available to the Security Proxy. The Security Proxy obtains the user claims from the Authorization Server via the standard OpenID Connect UserInfo endpoint. For Testbed-15, two user claims were specifically created to meet the needs for Data Centric Security: (i) the user has a claim expressing the user's clearance and (ii) another claim contains the public key of the user.

Feature filtering uses the user's clearance based on the classification marking of the features in the response. Basically, the PDP returns an Obligation to transform the response through XSLT where the user's clearance and the feature's classification are compared. All features that do not meet the 'need-to-know' principle get removed.

Chapter 8. Technology Integration Experiments (TIE)

The TIE for the Data Centric Security enabled OGC API - Features (WFS3) breaks down into multiple tests for each scenario. Also, the TIE separates into sub-TIEs as follows:

- Client → WFS3 (unprotected endpoint): Any request from the client to the endpoint results in a response - a FeatureCollection - that was produced by the WFS3 that is unaware of the Data Centric Security.
- Client → DCS WFS3 (protected endpoint): The same request as submitted to the unprotected WFS3 does return - from this endpoint - a valid STANAG 4778 data container.

8.1. TIE to the unprotected WFS3

The following figure illustrates the TIE to the unprotected WFS3.

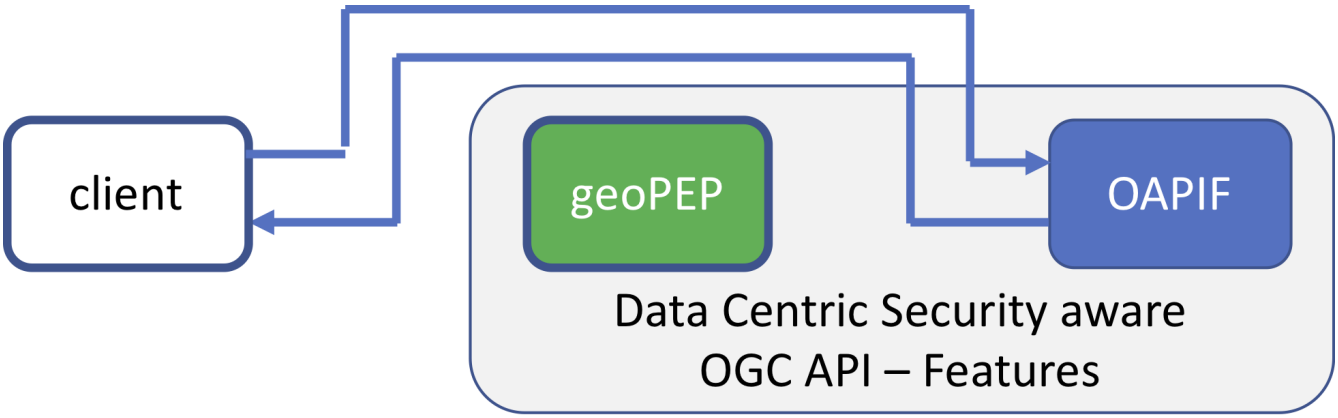

Figure 5. The TIE to the unprotected WFS3

8.2. TIE to the protected DCS aware WFS3

The following figure illustrates the TIE to the protected WFS3.

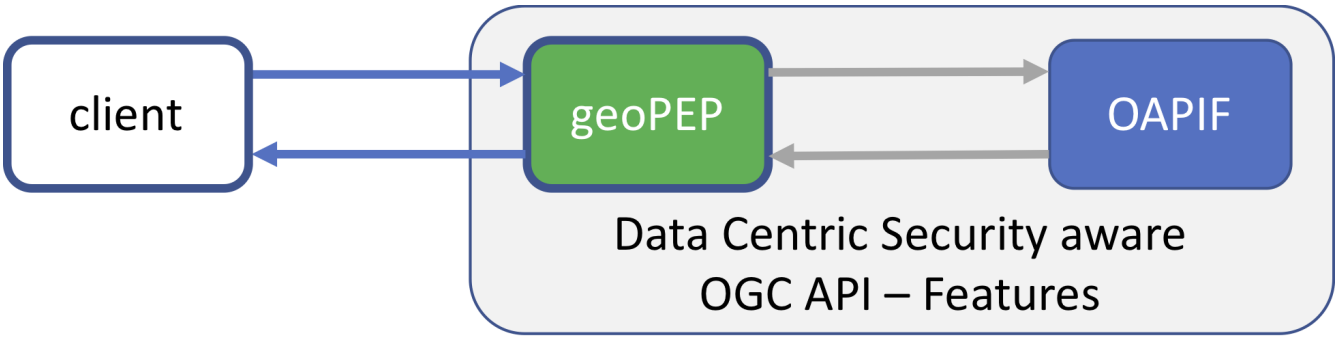

Figure 6. The TIE to the protected WFS3

8.3. Legends for tables below

- - The user receives what was requested - No DCS processing.
- - The user requested features of a classification type at or below own clearance.
- - The user requested features of a classification type above own clearance - no read up.
- - The request does not qualify for DCS processing based on subject-location. Requests are processed according to Scenario One.
- - The request qualifies for DCS processing based on subject-location and time ⇒ Spatio-temporal condition overrides the static feature classification. All users receive features of all feature types (as for the yellow case) but the metadata is marked "n/a" to prevent the user knowing the actual classification of the feature type.

All the TIE scenarios assume that the users have permissions to view the following layers as is documented in Appendix A.

Table 1. Access Control

User	Read
jane	poly_landmarks, poi, tiger_roads, states
bob	poi, tiger_roads, states
alice	tiger_roads, states
joe	states

8.4. TIEs for Scenario One

This set of TIEs summarize the result when executing the implementation of scenario one as described in Appendix A.

8.4.1. TIE to the unprotected WFS3

Table 2. Client to Unprotected WFS3

User	States	Roads	PoIs	Landmarks
ALL	OPEN	OPEN	OPEN	OPEN

Because there is no DCS to the unprotected WFS3, the response is according to the request.

8.4.2. TIE to the protected DCS aware WFS3

Table 3. Client to DCS protected WFS3

User	States	Roads	PoIs	Landmarks
Jane	YES	YES	YES	YES
Bob	YES	YES	YES	NO
Alice	YES	YES	NO	NO

User	States	Roads	PoIs	Landmarks
Joe	YES	NO	NO	NO

According to the Information Flow Control, resulting from the fictitious data classification marking and the clearance ranking of the fictitious user, a response content gets filtered. The diagonal green/red split is the result of the geoPEP enforcing the Bell-La Padula information flow control policy "no read up".

8.5. TIEs for Scenario Two

This set of TIEs summarize the result when executing the implementation for scenario two as described in Appendix B. Compared to the TIE results from scenario one, this TIE represents the differences caused by the spatio-temporal policy.

8.5.1. TIE to the unprotected WFS3

Table 4. Client to Unprotected WFS3

User	States	Roads	PoIs	Landmarks
ALL	OPEN	OPEN	OPEN	OPEN

Because there is no DCS to the unprotected WFS3, the response is according to the request.

8.5.2. TIE to the protected DCS aware WFS3

Table 5. Client to Unprotected WFS3

	Outside Geometry	Inside Geometry
Before time condition	Alt 1	Alt 1
During time condition	Alt 1	STO
After time condition	Alt 1	Alt 1

In this scenario, a spatio-temporal condition overrides the static information flow control policy ("no read up"). One way to execute a DCS based on such a spatio-temporal policy is to manage a disaster at a given location (boundary) and time window. In this policy, any user making a request within the time window and within the defined boundary receives the data requested. However, in order to hide the classification marking of the data (that would not have been returned under the standard policy) the value returned is "n/a".

In that sense, any request with a user (mobile device) location outside the given boundary (midtown Manhattan) or outside the time window (either before or after) results in processing according to the TIE illustrated above. The policy "no read up" with static classification and user clearance is enforced (Alt 1).

In case a request is made with a user (mobile device) location within the boundary and within the time window, the requested data is returned but the classification marking in the metadata is set to "n/a" (STO).

8.6. TIEs for Scenario Three

The TIE for scenario three uses the user's clearance and public key. The public key is used to encrypt the STANAG 4774 metadata that is returned by the DCS enabled WFS3. The DCS enabled WFS3 - the backend service - returns STANAG data objects encrypted but leaves the metadata in the clear. This allows the Security Proxy to filter the response based on feature type classification and user clearance. Appendix C provides more details.

8.7. TIE to the STANAG aware WFS3

The following figure illustrates the TIE to the STANAG aware WFS3.

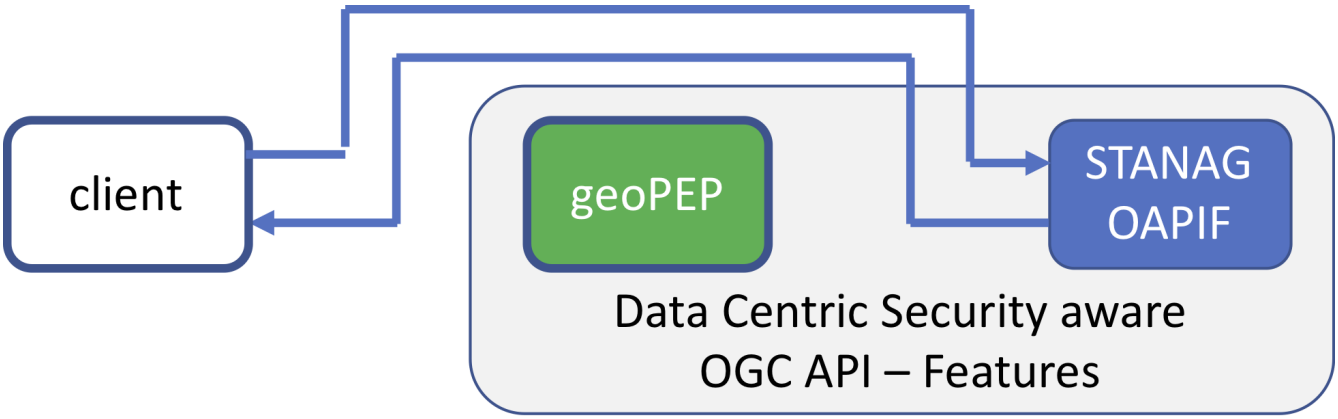

Figure 7. TIE to the STANAG aware WFS3

The result of the TIE shows the output of the WFS3 being in a STANAG 4778 format with unencrypted Metadata even though the security proxy is bypassed.

8.8. TIE to the DCS aware Security Proxy

The following figure illustrates the TIE to the DCS aware Security Proxy.

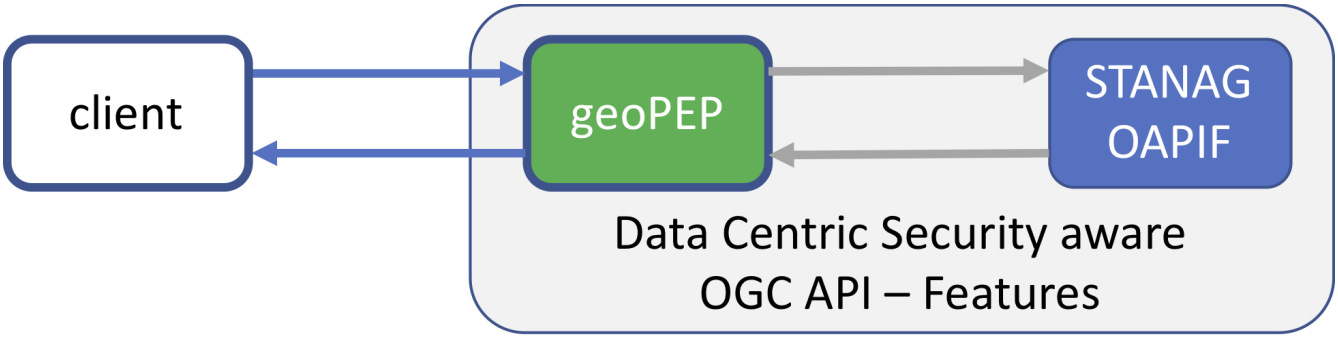

Figure 8. TIE to the DCS aware Security Proxy

Table 6. Client to Security Proxy and DCS aware WFS3

	Data Encrypted	Metadata Encrypted
Client to DCS aware WFS3	yes	no
Client to Security Proxy	yes	yes

The GeoPEP enforces the Information Flow Policy "no read up" by processing the STANAG 4774 metadata that is returned by the WFS3 along with the encrypted features. Because there is one metadata element per encrypted data element, the GeoPEP could filter those elements that would violate the "no read up" policy. To ensure the confidentiality of the metadata, the GeoPEP encrypts all metadata elements of the response before returning to the client.

Note: The result of this implementation returns a FeatureCollection that includes a Digital Signature element. The response is therefore no longer schema compliant. As a consequence, allowing a Digital Signature to exist in an instance XML document in OGC Standards is recommended. An OGC Change Request (CR) was created that requests putting an optional element `ds:DigitalSignature` in relevant OGC schemas.

Chapter 9. Results

In general, the work performed in Testbed 15 was able to demonstrate that with a security proxy and an OGC API - Features service, an implementation can satisfy the requirements for a data centric security model. Scenarios one and two show a backward compatible method for implementing data centric security. One requirement that was not completely investigated in the first two scenarios was encryption of the data from the author to storage. One could implement disk encryption. However, the features are not individually encrypted. Further disk encryption would be imposed by a service provider who is not necessarily the feature author. However, the results show that from the service to the end users the features are encrypted and a digital signature is verifiable from the user's point of view.

For scenarios one and two, another important note is that if HTML responses from the OGC API Features service are not limited, you are left with a security vulnerability in the implementation. A vanilla OGC API Features service does not understand data centric security. This is more important in scenario two than for scenario one. Scenario one bases access solely on an attribute in the metadata of the feature. Thus, the resulting map is limited to your classification level. Scenario two puts additional restrictions via geographic and temporal filtering which are not restricted by the vanilla OGC API Features service. In addition, HTML is not encrypted or packaged in an encrypted container and thus provides a potential for a "man in the middle" attack.

Scenario three is an implementation in which an OGC API - Features service is aware of STANAG 4778 as a feature storage type. In this scenario the testbed demonstrates that when an author of a feature packages and encrypts the feature in a STANAG 4778 container, the OGC API Features service can store the encrypted features. The use of the security proxy in this model is to provide authentication and authorization of the user. The proxy also encrypts the feature metadata and adds a digital signature. The major difference with this approach is that the individual features are encrypted in a container but the overall feature collection is not encrypted and is not in a container. Thus, the response is what a developer would expect from an OGC API Features service.

There are a few things to note about scenario three. The WFS 2.0 FeatureClass scheme does not support digital signatures. The implementation in Testbed-15 does add a digital signature to the end of the feature class. However, a validation against the scheme would fail. Features are encrypted with a key provided by the author of the features. Thus, the OGC API - Features service has no way to query against any of the encrypted data. If the metadata or a portion of the metadata is not encrypted, the service can query against the unencrypted portion. However, spatial queries are not available to the service. There are issues with key management that need to be addressed in future testbeds.

For more details about the implementation of each scenario and how to run the tests yourself, please see the appendices. Appendix A contains information about scenario one. Appendix B contains information about scenario two. Appendix C contains information about scenario three.

Chapter 10. Future Work

This testbed did not examine key management in any detail. The experiments used static private/public key pairs based on user attributes that were assigned by either the PEP or OGC API - Features. Future experiments should look at a variety of key management topics. For example, the use of hardware generated tokens could limit the lifetime of a token. Another possible scenario could be having a service that would store keys and having the return message contain a link or identifier of the key to use. Another area of further investigation is temporal or location specific keys. This would limit the time frame and/or locations that a key could be used to decrypt data.

Another area of future work revolves around the use of more sophisticated authentication and authorization schemes. The current experiments used OAuth where it was assumed that the client had received an authorization token from an authorization server prior to making a request. There was no attempt to use SAML or Open ID Connect. Future work could also make use of assertions to aid the PDP to make decisions about granting access or the PEP to enforce an assertion made be the authorization server.

The other area for future work that the participants considered important were efforts to search or catalog encrypted data. In the tests in which searching was possible, the PEP applied the encryption after fetching data from an unencrypted database. This deviated from the premise that data centric security ensures the data is encrypted at all times except when viewed in a client by the consumer of the data. The scenario in which the OGC API - Features service stores data the author encrypts renders the data mostly unsearchable. If the metadata is unencrypted some filtering is possible but encrypted geometry data is still unsearchable.

Future work should consider the management of different data centric security schemes in OGC APIs. There is much work taking place in a variety of organizations using Trusted Data Format (TDF) of different flavors and TFD would be of benefit to ensure that DCS development takes this into consideration.

Consideration should be given to the granularity at which data centric security is applied to features, feature collections and services. The ability to filter based on encrypted data should be cognizant of the computational time and overhead associated with any re-encryption and re-wrapping of objects. The traditional approach to security with OGC services is to externalize the security enforcing functions. However, with data centric security approaches it is arguable that having object release functions embedded within the OGC service itself may provide benefits in computational overhead, transformation speed, security and reliability.

Future work may wish to examine the concepts of obfuscation and transformation of potentially-sensitive spatial, temporal and other metadata, such as allowing otherwise sensitive data to be stored and used for querying/filtering in an unencrypted format. Data centric security approaches make use of linked or encapsulated data. These approaches may direct the client to obtain information from a data centric security store, which centralize the authentication, authorization and key release processes. There may be benefit in this approach especially when linked with obfuscation/translation since it might allow OGC API servers and clients to operate with minimal changes. This approach will also minimize the risk surface area of an integrated solution, of which the OGC API may only be a part.

Future work should examine the use of JSON to deliver the output from the APIs. OGC APIs should enable a variety of different formats or encodings of data centric security objects. DCS objects may be encoded in XML, JSON, YAML or some sort of binary format such as protocol buffers. This should also consider digital signatures as part of its scope.

Spatial querying of feature services is carried out by a number of optimizations made to the underlying data store, such as a database, and algorithms that act over them, such as spatial indexing. There may be benefit in further research in how the optimizations might be performed where the spatial query parameters and the spatial tree data themselves are all encrypted. Possibly a limited range of spatial queries may be permitted on encrypted data in this fashion. Similarly, encrypted filter parameters may be able to act on encrypted values in the underlying data store.

In a system that demonstrates aspects of key management with stronger forms of authentication, the ability to make assertions and facilitates searching for encrypted data will provide for a more robust and useful service in the future.

Appendix A: Data Centric Security - Scenario One

Introduction

Scenario #1 uses a vanilla WFS3 API (ldproxy for Geoserver for this demonstration) that has nothing to do with Data Centric Security. The GeoPEP transforms the WFS3 features into a STANAG 4778 encoding including STANAG 4774 classification marking, encryption, and digital signature. This is illustrated in Figure 9.

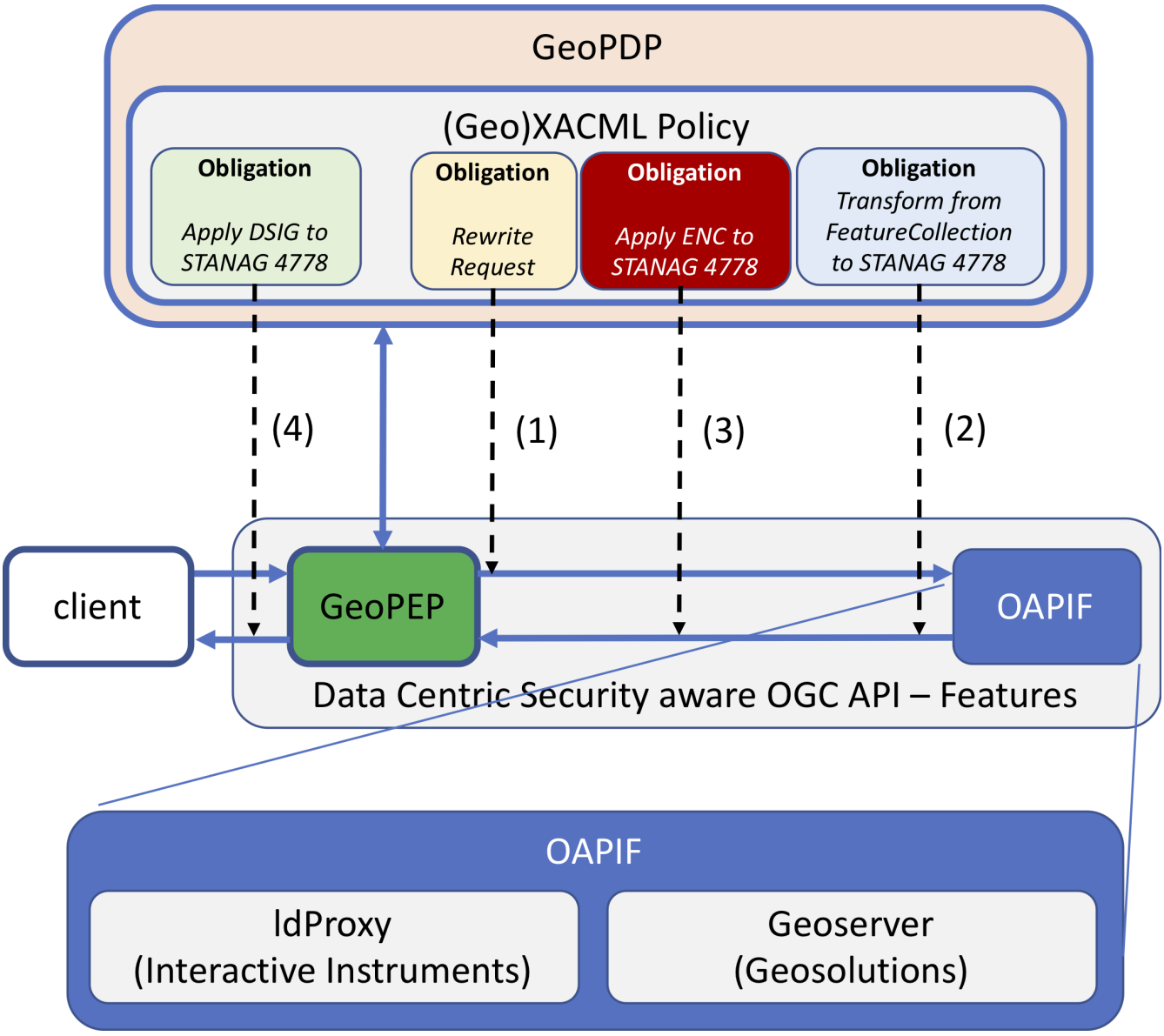

Figure 9. Illustration of the components involved in Scenario One

The client sends a regular OGC API - Features request to ldproxy/Geoserver which then returns the result. ldproxy translates an OGC API - Features request into a traditional WFS 2.0 request which goes to GeoServer and visa-versa. The GeoPEP produces a STANAG 4778 compliant result and sends it to the client.

Upgrade to Data Centric Security

In order to provide Data Centric Security based on the deployment described above, the GeoPEP acts as a security proxy in front of the ldproxy. The main objective of this approach is to provide the required functions to serve Data Centric Security packaged in the STANAG 4778 format.

The STANAG 4778 format has multiple features that need to be addressed:

1. A bundle of metadata and data per asset.
2. Support for digital signature and encryption of metadata, data or both either with the same or different keys.

The GeoPEP acts as an enforcement proxy that is controlled by GeoXACML policies. In order to return STANAG 4778 encoded content to the client (instead of a FeatureCollection), the following functions must be provided:

1. request rewriting
    - query parameter change from f=stanag ⇒ f=xml
2. XSLT from FeatureCollection to STANAG 4778 merging in Metadata
    - XSLT from GeoXACML policy
3. Encryption
    - encrypt data (features - private symmetric key)
    - encrypt metadata (public key of actor[user/automated process])
4. Digital Signature
    - Apply Digital Signature to STANAG 4778 encoded result

Demonstration Use Cases

For demonstration purposes, the metadata consisted of the classification of the data which is determined by feature type as indicated in the table below:

Table 7. Classifications

Feature Type	Classification
poly_landmarks	top_secret
poi	secret
tiger_roads	classified
states	unclassified

Any user requesting features of a particular type must have the appropriate clearance. If not, the GeoPEP returns a 403 (forbidden). Which feature types a user can read is determined by the Bell - La Padula information flow control policy. The following users with fictitious clearance were made available for Testbed-15 demonstration (password: `secret`):

Table 8. Users

User	Clearance
jane	top_secret
bob	secret
alice	classified
joe	unclassified

This means that the GeoPEP had to enforce the following Access Control Matrix for feature instances from a particular type.

Table 9. Access Control

User	Read
jane	poly_landmarks, poi, tiger_roads, states
bob	poi, tiger_roads, states
alice	tiger_roads, states
joe	states

Demonstration

Getting an Access Token

Each user logged into the OAuth2/OpenID Connect Authorization Server (AS) and obtained an access token for accessing the GeoPEP.

The following CURL request was used to do this operation:

```
curl -k -i -L -X POST \
   -H "Authorization:Basic
ZmEwMGVmNGYtMTQzZC1kYTUzLWM4MTQtYWMxODY2ZDU5MmM1QG9nYy5zZWN1cmUtZGltZW5zaW9ucy5jb206Yj
BkZWM0Zjg1MzI3YzlhZjgwZjk2NjlmMGM4Zjk2NmViYzNmZmFhMGY1YzU2YzI0NGJhYzc2ODAyZDZiYTllZg==
" \
   -H "Content-Type:application/x-www-form-urlencoded" \
   -d "grant_type=password" \
   -d "username=<username>" \
   -d "password=secret" \
   -d "scope=openid saml tb15" \
   -d "response_type=token" \
 'https://ogc.secure-dimensions.com/oauth/token'
```

Response:

```
{
"access_token": "187639d3971831fbef7f5590d57dd746f24ab51,
"expires_in": 1800,
"token_type": "bearer",
"scope": "openid saml tb15",
"refresh_token": "7f6886d39560d3c06e6b5173aa85a6cd21a028"
}
```

TIP The Authorization Header contains the BASIC authentication credentials for the client application, registered with the AS:

```
client_id = fa00ef4f-143d-da53-c814-ac1866d592c5@ogc.secure-dimensions.com
client_secret = b0dec4f85327c9af80f9669f0c8f966ebc3ffaa0f5c56c244bac76802d6ba9ef
```

The OAuth2 `grant_type = password` had to be used as CURL cannot use any other `grant_type` because they all are required to interact with a Web Browser.

The scope variable containing `tb15` enables the user claims `subject_clearance` and `public_key`, which are required for executing the different GeoXACML policies.

Verifying the token (which the GeoPEP will do)

```
curl -X GET -k -H 'Authorization: Basic
ZmEwMGVmNGYtMTQzZC1kYTUzLWM4MTQtYWMxODY2ZDU5MmM1QG9nYy5zZWN1cmUtZGltZW5zaW9ucy5jb206Yj
BkZWM0Zjg1MzI3YzlhZjgwZjk2NjlmMGM4Zjk2NmViYzNmZmFhMGY1YzU2YzI0NGJhYzc2ODAyZDZiYTllZg==
' -i 'https://ogc.secure-dimensions.com/oauth/tokeninfo?token=<access_token>'
```

Verifying the user claims (which the GeoPEP will obtain). The following CURL request can be used to fetch the user claims:

```
curl -X POST -k -H 'Content-Type: application/x-www-form-urlencoded' -H
'Authorization: Bearer <access_token>' -i 'https://ogc.secure-
dimensions.com/oauth/userinfo' --data 'client_id=fa00ef4f-143d-da53-c814-
ac1866d592c5@ogc.secure-
dimensions.com&client_secret=b0dec4f85327c9af80f9669f0c8f966ebc3ffaa0f5c56c244bac76802
d6ba9ef'
```

TIP Please replace <access_token> with the actual access token received.

Accessing the GeoPEP

The GeoPEP was setup as an RFC 6750 compliant OAuth2 Resource Server that accepts the access token either as part of the HTTP request header or as a query parameter.

As such the following URL (not containing a bearer token) will return an OAuth2 compliant error:

https://ogc.secure-dimensions.com/rest/services/DCS/collections/poi/items?f=xml

Obtain the `poi` feature type with the following URL including an access token as a query parameter):

https://ogc.secure-dimensions.com/rest/services/DCS/collections/poi/items?f=xml&access_token=<access_token>

The preferred way to submit the bearer access token would be as part of the HTTP header (see RFC 6750 and 2396):

```
curl -X GET -k -H 'Authorization: Bearer <access_token>' -i 'https://ogc.secure-
dimensions.com/rest/services/DCS/collections/poi/items?f=xml'
```

Requesting STANAG 4778 encoded responses according to the Testbed-15 demonstration of Scenario 1, the GeoPEP returns STANAG 4778 encoded data fetched from a Geoserver. In order to activate this, the requested format must be “stanag”:

```
curl -X GET -k -H 'Authorization: Bearer <access_token>' -i 'https://ogc.secure-
dimensions.com/rest/services/DCS/collections/poi/items?f=stanag'
```

TIP An attempt to request any other format (e.g. xml, html, json, etc.) will result in a response, not processed by the GeoPEP. These formats can be used to validate the original responses produced by the OGC API for Features (WFS3).

The GeoPEP will rewrite the request query from `f=stanag` to `f=xml` to ensure that the WFS3 returns an XML encoded response. This will be further processed in the GeoPEP…

Response:

```
<?xml version="1.0"?>
<mb:BindingInformation xmlns:xsi="https://www.w3.org/2001/XMLSchema-instance.xsd"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:xmime=
"http://www.w3.org/2005/05/xmlmime"
  xmlns:mb="urn:nato:stanag:4778:bindinginformation:1:0"
  xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0"
  xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd"
  xsi:schemaLocation="urn:nato:stanag:4778:bindinginformation:1:0 4778.xsd">
  <mb:MetadataBindingContainer xml:id="WFS">
    <mb:MetadataBinding>
      <mb:Metadata><slab:originatorConfidentialityLabel>
          <slab:ConfidentialityInformation>
            <slab:PolicyIdentifier>TB15</slab:PolicyIdentifier>
            <slab:Classification>SECRET</slab:Classification>
          </slab:ConfidentialityInformation>
          <slab:CreationDateTime>30.06.2019T12:00:00Z</slab:CreationDateTime>
```

```
        </slab:originatorConfidentialityLabel></mb:Metadata>
      <mb:Data><EncryptedData xmlns="http://www.w3.org/2001/04/xmlenc#"
          Type="http://www.w3.org/2001/04/xmlenc#Element">
          <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc
"/>
          <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
            <EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#">
              <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
              <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
                <KeyName>Dr. No</KeyName>
              </KeyInfo>
              <CipherData>

<CipherValue>GbvEvGtuH08lP8u8oeGisvEd1MR5HqnwtUef9ItPBOYT2XXyM3/3T0VdtzLx2Q5k
hN6125pj7sxIaj1QK+A6F+5o9EZj99/II6QMMgFGijkNiDXA4X9477xGO9AIVIpD
99mI4rL6YDnHR2Xy60mcjQ6vTrR/KnIBQhjhm5Gj6GygHGUeX/xC125UwdQffo/S
RNckmKal65DFourb14CB/x1YD34kl2rzH73CqMH8x+E0LSsrZfhS1XLwacm5tRCc
bLQU9J4oFnvcx3UTzg9XO45X07hwTVyqWVAuxBaFGcVR2lH2/n4n160NAaTlKCVJ
VxiF6yxWkkSB5WmrtnFeyA==</CipherValue>
              </CipherData>
            </EncryptedKey>
          </KeyInfo>
          <CipherData>

<CipherValue>05VP07tS/AutzFnEjxasYXVReUf7liUxGHXoBywY5VIs1TWmyoPp4zBSDZr8D7MR
gJ5pgrN4UGFot83Pfmr29LZlfZ68PdbD+4UaPG3dp1F2DaR0TExITLaUWPBbjnZl
PgCGT05MD1EMc8a6XD8uV8wNVQ9WegH4Ht1nelX+bYmgvH3nMuK21GxJNdhA1AFh
xuUVeqMDS2nv7mpP3CuVU4C8z++fFsbxGcc39Ax3fubco5W/Ml/uJ+VxARg5uoJe
lpxWXe7del1WWR/fHK3QQ4psqPsjDB4ZoBNdYv80JDCU31NLFuGF9T3psaDo2b8u
hOIQZiPiAhmE1Xn/NSJwEoG1aSqI0VfghGS1LPutqFh0yzIOqzW7qr96xbU/ECL7
0EmPy7Y1Abgfs93BbBwQyHMOhE+9snIDlgwJxfegXjG7zVZsJBHR8Uv+afNIBbA+
9+VNjJeLjIwdrs9cI7q9GtwVLVEK9HRGW4TRafDrH11KN+yKvYvUIZxFjRhXCcmH
PmLq91ABxZHLFAn33VTMwsh5olfb909U1EBUtNDI8FfJ7VJi8vRMeG77OZVgOskR
oDpDxmD0FwK/M8STB77+zKpuF5DRbwEnLAw+o5HVA14mIiFhkMa2oh1/bOI4f2aO
5YNUNTuGETAsRBelMLJLkLBhsdv6mPYACNEL7DtBQgBJDgkFwz8jKlE0mSJSOeWh
1/DQe9Pyg9PYnM/5PIg9vEZbUwze3J19dtUaxnH4G0z5x6QuuVhihc7nQbHfU/MO
6NppWxPMqYjBBVzI+tSHR0A+I5Z+Aj3VVlfcjPwbcWuOjku0UzcZBC1TCdIyvt+A
LA0aXKCVN27EGknFCnl7NqmluHWG9E3cUS1I5ONmOaTpRkZKy+QtJKjMA4kZcRAQ
0YJOWnS3W5oL/MiBypO96zzWZt8HTAabuSwZda+OMAlSasrpZHGNQjy06tnB9nVY
Ttgk4KqWyKdRhIi1xZSvWxUfLWQZJMtSOsInkrCXLFsV8tNycnxI1WwFvb5PUuad
f49wCamBB9qSJKS+mWHihQVJqhDYuX4vT6Van56JowlQVZHTIzi7/S+c3pUbvnqg
x8HCYpHxZqESt7e2MD+B9J8DXFq3goKZMenlFgr3i4tuZmHBJfn1uNoKOujYngGM
BvRSLsnsRbOZhttswdcFRmqXapO/1zMEMxtemA3HakriAtxETGOmB427iZBCXpxH
S/Y5m5MirgQKeugEItcbZ4CXIk7j325j/8d8BxeS0seX0nHKwiWfJyZpLG9Lp9qG
kuyMx2B1s1dTlTfETsJV2/zu00e7OIcDv6RwBn7EwwEDUGlD95Vb7/3xW33yWRVx</CipherValue>
          </CipherData>
        </EncryptedData></mb:Data>
    </mb:MetadataBinding>
    <mb:MetadataBinding>
      <mb:Metadata><slab:originatorConfidentialityLabel>
          <slab:ConfidentialityInformation>
```

```
            <slab:PolicyIdentifier>TB15</slab:PolicyIdentifier>
            <slab:Classification>SECRET</slab:Classification>
          </slab:ConfidentialityInformation>
          <slab:CreationDateTime>30.06.2019T12:00:00Z</slab:CreationDateTime>
        </slab:originatorConfidentialityLabel></mb:Metadata>
      <mb:Data><EncryptedData xmlns="http://www.w3.org/2001/04/xmlenc#"
          Type="http://www.w3.org/2001/04/xmlenc#Element">
          <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc
"/>
          <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
            <EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#">
              <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
              <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
                <KeyName>Dr. No</KeyName>
              </KeyInfo>
              <CipherData>

<CipherValue>yHiGy9BgHkUu+Qr3XPAMQmbzkVzu+eISABYunx/oXtSI+QWssm+2i6LgvdYclDgE
ORoscMRxCv/O7pJ6IAGATAyDo0Vz5rsbzaBdzMUB6CuQnGrPVPFZZQi5SJfxxTHJ
7ng5QpApj0Wd1qlEa2T9cM45WBUXK3IAr+z9nl0la8gORdH1l6WWsr9t6M6bH3Np
0J37oYni4JI5+DGUk7CasZsfogRuYDxzok7xVL5rdAiVL4u88/klw7nkQMT44lrP
Lk73OV6xf61+8C7dvCeVCD/FxbFtkCi+Wl2p4njq2P4eTywPGWiNtXg5uc748syG
L2oX9qYeZ5CVODoPTRdqVg==</CipherValue>
              </CipherData>
            </EncryptedKey>
          </KeyInfo>
          <CipherData>

<CipherValue>YUgl88EgJKsk6v+8lEB2SXpIGmRAv7r5XXRJ7EptIBbwGGH2lJSa3VBniVV+qsL2
oxPSVRVIFy3NUIRcoet6zWjFflhD6vcUIvEbi6KyX6LH/5cgWJ4nKjmfUITvDTWS
u5tpCBv3+cn0KrJsrtTB7di+QWLQhAbXx8qZcKX9io7U8jOFh4VgQ1h3fTDD3O1L
suSEI1sWEesEEIQVK42nGwgjCaqN8PyFK7wU+1rpP8nLmZw2lRzCbFT3s+bs0W8D
8SvmsUeSidr+AVFWcy/dRa6wcVj7us4wEPBc3LmvAi3vgbwi46VBtaqCQ4Dk6th3
+BPGqRLWYSsg776cEG6Op/BSbCkqmJFKqbyCbp8n2o9rd8S07mWlitZopxd9xhdU
fhIaptlr9W/VzkGXc0KEAsLgqOl6xw+E2ePXG+eScLRifvtR+WjLFdTwnhzSHSIU
M9ieVEXb2juPDsdJ/ST3gAswBNq1fkcPN6l2gX78lTuxe03DRxggoLgQZEKDMT32
iXNmyLPUTlJHlgIjgolC6DPalOZHHOE/EUFHG9ZVlyig5kRL4FcWUSnw1qlDRRVe
3tSEJNqqmK6sQ/CE1+PbrsjhIFirKYkIe2ph1jf1dm74yh2aMjYumovyb64Q/PvL
Z9nDQPsu9By7W6SEL9J6WLuZODOeGNOd/NDZAbPiqLrzYlcrtS9PtIuJQoWsfpmh
tWwMT1fR0MOJm4cpkI2uaYIZr2WdGLMePLpPcMPWvMfJexmujTfEF53twniOyppL
uFcfhS/XWsxkaUpL29D5Mgi7sw4xYRsrDqQIa7w+36tyUA+wxkYAHkm7jfpUzM9f
0RrWLpgk29qTqg7TZWijQ7gfQgtDKDXdgV5iH+ozhSr8E5NhmHRFT5MZfUWG1lTU
lbJcNJFN8GX1g+GfBVVnOnPeRjqsBX03gz+IMfdt9/3Un+/HL0yTCHMbcKa+qtXE
Tq1i4xyc68kb2E0RkqLa7ydtAwJJRHNUFXW1vChMxBIB8wxXyx26K/XOjkc4YsQV
WedMmfOuRuRip0Jn2eqe3L+Nsx0poAn4G8LxZ85r0P+sg33JpGII5A439vfu+fAR
lbPrQqCaPhuGt5caCkC+9D2PoTkaFUYQGwOqSE69LaAzaQymXPA8VgawqjYDoFXR
RrqP7FMkHL3wU9YUGVV0ACEt3nmhl+2AvRNT466CTJmeMfO/6Vhiscj8bKluNy8x
GzA8LIxe9NGzbZhgKpy1jvvsgtoVMTWhGf4lOAPOCJtIcVobXUXNdvKkxivM+ryY
5fQ5q3UGkGsQ4DJZd7pMiNdnZJGiUWEQcftNNku4lQAhyC2U3kphoYEtaNfyJz3B</CipherValue>
          </CipherData>
        </EncryptedData></mb:Data>
```

```
    </mb:MetadataBinding>
    <mb:MetadataBinding>
      <mb:Metadata><slab:originatorConfidentialityLabel>
          <slab:ConfidentialityInformation>
            <slab:PolicyIdentifier>TB15</slab:PolicyIdentifier>
            <slab:Classification>SECRET</slab:Classification>
          </slab:ConfidentialityInformation>
          <slab:CreationDateTime>30.06.2019T12:00:00Z</slab:CreationDateTime>
        </slab:originatorConfidentialityLabel></mb:Metadata>
      <mb:Data><EncryptedData xmlns="http://www.w3.org/2001/04/xmlenc#"
          Type="http://www.w3.org/2001/04/xmlenc#Element">
          <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc
"/>
          <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
            <EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#">
              <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
              <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
                <KeyName>Dr. No</KeyName>
              </KeyInfo>
              <CipherData>

<CipherValue>IBAmku4wHl+wLyautj98CRQ6/uib/8uCjVM4/aM7SMK8B3fQknVFWEuH7MHYukGa
PO+4jbqjRulFk0b8CA+lc+irVxG8AaWa6E7i251t+La5Uvj2l2vcNb/GpdGRoVnT
FoS99eNbS+CfZ2PnuRHU9qBVuzPM6BeqqCyuzXhQePr9pmlTb4LJkpA6mFD+Ky30
Im4MDpix8PxYCkdna18QNKYjoCfcJzOzxC53+Zi6XeqxfD1Ynfywt6dIwyIk40fa
0S5wGL8xxBOX2LpqedfdfTYuRxFyABFZ5+SGZ9DzacrHkLsUSyb9ranXGQz7O+pK
6a57JUBGZ9o+b1ZOqHmreQ==</CipherValue>
              </CipherData>
            </EncryptedKey>
          </KeyInfo>
          <CipherData>

<CipherValue>rS2IRKEakG+04GVXBV1zEdETxHJ1LzwgbWLlR1m1At0mhObBeQ4xM/V7lqPc957C
b7gMlKGcGVAXyKvufsKN2Pa5t7Cjj9Om9IObB7y/LVq4ZtLsZJLiGDcOl/pse1oz
GF7FA4ts+uBbYKLpRFhTSPLvNNAcXwirf15KumZ70n2YEqZ4bdRVfPGXc7jrE8f5
AXaz4nLgvcgRDe4y0Ab0fwpJDf6uv66Ke1on9po7bkTmLxy8SvzLB4u5O0X5RJUM
SnnZrY9MkO9nIU7eBMsYO/B+tZ2wgYgzVdMAnTYgX0i0jm7X3DxAkhJHkLpgxwQe
EA4O/0N3lHZBtUKdc41+ZZ7SKMSQ5NBkl84tSq5HPrUNRRdI7LhZbN9Z5o8kSbRL
2ET1mh0tJwSG1/LGzhjf34YUmgmmm29IswCsBEicdLD8321M0UhZTXjhnDPU4lyI
JV72np/oH3cdjCKfE84i0GNHucMuEGmrUjHRwSmKTplssi440Rpmho9RU4g855qe
qqHG9MlWtTePqk3HRFwx1YduhHAtWLA3WJJXIhGXVROPk3cPHGn00RBY/TkEWbew
6OwxUEmcEi6qqlwickS+aUFoA11/jkLfTZK5L27yEBRY9BNxhOpFWaz8PYykupEe
ECfDwZ+qUNFplA2JcPra7NKSlMLj0mqzRcGiWaV9xxeTJDiDmGLLBrdoYd1NEuyw
5GAz6Nf2h271lAD26F51kK4nolUqmfURrSq1vyK7SpqxEycnsNa4aOzHYJjomSR0
zeCjIAb4x1Dipf/KuNQ8Jm7/AKtTcIXxuvfcof86qfLAozEl12AAZHN94wpRHBuu
pRb96Ea+uDsKQYwVIxAVslnl+m8ir9su1bewXOwz4cpxRXR7j1O8ZdBHcU6dm0fZ
CO18GnjLju3CoKbAsSj0wpnyzaCR/AJM1Ezmr6a+lT1d0PrlPCmt0ogWTwwiiIEL
Ly8CyuvYJr0jNfqpwGB2IUlb1qzOf1/D0xtgE1pecwqCixVROgaEYTHyr8hdcA5i
qxHB8B1Xg/DE8L9+kY5L++rEgkFt8FeTQDZ1cQx9PUybzYSkL30E4FnPWD/ZJv7u
SXhAGqyYm+WjWBc6+EME+UGdvG5EMibByBPuhhgl6d/l/HWkHgAQ0I0T9/Z7TBOv
e9RrYwX1JSKBPmdVg4cWQou+WF9GHYVZc4oxHZykICFDMafCTPEnuGaeSNGXmzt4
```

```
VKt+lbidFsv6t5hhUDuPi8ulFRmtweL5AJpQCFNelHslgmRJYojC2aXNoR9VMLrK
4F9QT3ftrkOehHz0eUiq7MUu2aUpQw0nsPBhzQmmWgVvdZ8ecKI5PcdheR3jA+SP</CipherValue>
          </CipherData>
        </EncryptedData></mb:Data>
    </mb:MetadataBinding>
    <mb:MetadataBinding>
      <mb:Metadata><slab:originatorConfidentialityLabel>
          <slab:ConfidentialityInformation>
            <slab:PolicyIdentifier>TB15</slab:PolicyIdentifier>
            <slab:Classification>SECRET</slab:Classification>
          </slab:ConfidentialityInformation>
          <slab:CreationDateTime>30.06.2019T12:00:00Z</slab:CreationDateTime>
        </slab:originatorConfidentialityLabel></mb:Metadata>
      <mb:Data><EncryptedData xmlns="http://www.w3.org/2001/04/xmlenc#"
          Type="http://www.w3.org/2001/04/xmlenc#Element">
          <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc
"/>
          <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
            <EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#">
              <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
              <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
                <KeyName>Dr. No</KeyName>
              </KeyInfo>
              <CipherData>

<CipherValue>TS8bTwhVKEl+JCbrjSWRtkTOJSXM4rYps6WlPR7OdFnFF1fEeaqaO5FG60RwbUFC
oAun3K9z0+j/EPS9YUv0veVx4Aa1O/mhD7eE3bY9IMwDdb9xkrQbpc4RzjI8WdCL
4OL5u4ywiLAX0L36sMdwX5rwpungOnnfjqtf/x1hzHWGj29qTBZxP2E0lfs9JJc7
le6QhORQv51RpEH/oleQTbxemBNEtV1hTb80iZJVcacr32PWK82k5DyOWKHfpGlx
0isBwHE3VgWVY4nT3YG4QjVsD2wYqFLL3YvvnaF/OsHQglPWCA84G18FF5j8d4iy
lAC0Q0rOgTpbDBwy3Cw5xA==</CipherValue>
              </CipherData>
            </EncryptedKey>
          </KeyInfo>
          <CipherData>

<CipherValue>Bgoo202out8zZrXI21Rfmduoa84Z+jfr2jGc0lF9RTX3kNy0UquTzd7aRWtzuO/T
AeOetOU3JOTguTR2hI+PPE2SEEk6VeZAUj/0g3R1CfKCAOXpLb1pxoIidmj3qKKF
KpDyR5n6soRIAZS+0T6PLFhc5Zgoc0t2uvflSj94dZ1zInaALyyUb3IgMr6L2Tv8
7j3ZUgy6RlGZ7Cqb71OXaOjuuV143A2Wsoa+9B3E4VpQDGVIMKoXRR0CqY/S5z3o
lPWmpESgdN1yH6upOT9LPBBO/V4d3DGqXUBs/yU4jfVXDM4Qa4enJuGS22RZe9z9
InwUuLxIf4bYc+M7cETLbMd2thrrdlNXNvKBvbCijgtS5md9KhgRy6SlfO3J68L2
QciFJu+x/jOPKtICPTNO7axrRNIOTzosQQWK5ZatympkkBytcxM7YOQ3U06p4535
ZIkUHzKqcbtgXq4b9z7koRvO/UidpkmDuNuPLmJoBuIHltjlVBdA5ZpdCi8cm+zr
er00bmXpjbHjn/qo+kxaSfy3kPaZuwUVcAocDrFUP0Zezky/RAWYCUulXo156BH2
OT28rpdD4lOvVgevRRhcgcIaudv70VKo+JPFcYWVOZ7EmxfnD8PEkiokBFLYms+e
PYUNdZx6ZEhv0q6lNRIZOJHBT1/vtO2/yYreyvtV6jzY4zSniisw9dAhVRME8yJD
DWab5u9S6weggwjn429St6FMmcYCToRoRnjVl68LNdDzLcWYaUuznaI/BC+I5d4o
TOGSn1kJylPc4Rx+WWlCHjW190KcuzTyMLBkes00vw3D3jcvEW9Ga4F8ITGjbEoj
IJpvyS2h6Zs4ehke981luibSbZe+1ly4Dmf8VAM8bBm6/BJu4r4nIz3fYeYQu9Gm
lx9z80HMPKMa99EXznoyd23BDWcQq9YUY7naPhIQ94355azl4jI2s6tzEm+EI+wV
```

```
o29m2dcnTvfuSw/ta8hf765ZW64mfQW/Hp8gfaTcDzgkn3PRG9uRqdgj3X55magO
U5gmcKpTt9rcqR2A8H5skIUvFkf4SBM9VP2wj195VU/VgRA50uraIYU2stlZcRmf
vwUXXjpjGmX7fB+WZqGEZILv+zg2XnQFvIoKAO2xM73saSTq/HRMIs5Byc/N9NMU
unR6X2Pvy9WkY8CXz/WljQIizswA69yz5ohwCWkGg8QgHr7XM1RX40SmzQQ0KHgW
9UNRK+NBQZQ80WlZQgAo548h0FYAdh5QiZhJa52bGWdDuIwLEszjAGyzIQRJKxsC
81DPRTg1HfNuekJwacOf8BE0n7zjh5eTPCxlJf95A8G4IEkafkI0s0myjwy9/cJU</CipherValue>
          </CipherData>
        </EncryptedData></mb:Data>
    </mb:MetadataBinding>
    <mb:MetadataBinding>
      <mb:Metadata><slab:originatorConfidentialityLabel>
          <slab:ConfidentialityInformation>
            <slab:PolicyIdentifier>TB15</slab:PolicyIdentifier>
            <slab:Classification>SECRET</slab:Classification>
          </slab:ConfidentialityInformation>
          <slab:CreationDateTime>30.06.2019T12:00:00Z</slab:CreationDateTime>
        </slab:originatorConfidentialityLabel></mb:Metadata>
      <mb:Data><EncryptedData xmlns="http://www.w3.org/2001/04/xmlenc#"
          Type="http://www.w3.org/2001/04/xmlenc#Element">
          <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc
"/>
          <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
            <EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#">
              <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
              <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
                <KeyName>Dr. No</KeyName>
              </KeyInfo>
              <CipherData>

<CipherValue>dsuQYd51N1u8galpFPcQYPk2GIY+U097WB2elU16gjOMfhaBiuLvgwxelP2cqm9K
YqNq09CbyrP3G/uozzIVyxv+QKsvCOV393LjB0p0lNbVz7dItZfiw8UwAsORAlaq
llC3xRWJf/IFMypBQpQD/Vc6cMWN/WOXfZRr7JsWeN2tFgLy9oPPZFQgbUUgkJwm
eB7aCokaQ0wq64ZHIElX3ijwFfnV7zmwqLnX43JRS7AF06QzvBvIvr9UjtgU1k+R
IQXLSTI6eg/eLqNAf8HQJaredLYp+ur3aOXi12uiqoyUZm2tMCyIB6gPSDpZJPk7
fBHCQlovzLbtSeoEpPVjPg==</CipherValue>
              </CipherData>
            </EncryptedKey>
          </KeyInfo>
          <CipherData>

<CipherValue>pPcsHl2KP2N2CHTj0yVjLaQ7D26Rh/20vHqm5DPUI/Jq1kopNVdO6iqYnEJuYeMS
1o0eiKOh73Z94DcmgX776+MArQWvLE5AypEAbme1XDhvrfVp6YDy1lShQmlcGGKl
zOEmzMhApAu5umJO+yOS/UIxxGKFvElOnbmYYSujsWRnxtR6wYX+s6NbC5+bBlMG
91jGIBNaahxL2O0wr5IoySoc138Bhq8ZfO3iXNAT3/ZxK1YT9KNPsDXKOxRSSj8I
vROruUtIvY+lbv/T5ogWFqVN0TP1EnUB5zrW2mZYG9PJtSH46iRffponpyNPxvtb
iAMHH4GdJEXNrpydBVmgbOJ16mO3x6h/nr+1/EhAaqBR6TcL/SOsGTEkXG5zW7/l
rfMqYKefJBdHJVK5KX/KH/t56QAbH91MiMtw4gc+CZJZmzc38Ue4KO5qpydkwK9M
mnsn8YSYp83Qkqb8b8ptsnt44MJFZJnxVxz7IFLAFqBtbwGHlhC8S69c5Fif2iW1
bJ0p/jtpF59Xd3Hyz3kxumzm59qHrcbN/1NbpBxQyOHRPkICKewrG5ADsv+7C/L9
Tgw+KmKvs4zobQJYmP/80WckWYrHvWy17rH8O6BOdhgjweTr24U5YDMz9tI08qCG
NmAi0uPgZbYPzV8IO7epZVBsUvkQ3HqRvIeIW/1I1Vfgebskis4m/2K8LZZ7L8S0
```

```
Ju6pmraFXPYVdMBQaEG43FlVSb3hSkE4jlo8JbLal/mXBcizlXJcsPQgkYqbyXRF
WBSQOF8gSeyN4FnBUi7Rb8aAKKv3TOemU08NaHXaVqVIxY7B2ikUDe7MegkXWJaE
HpcovYT81Sfhjk19mUX4CPcvIbz2vVxlFheEs4kHET9K7fgW8Y2NT8c47aYfL4Iy
Ur7OFHg6ouwJfRuUGA5X2agWU+GEhNYgbFJcyq70RPNU40NRY1tWIm/JaVCZx4Zu
hb74UJRcPngR459aLfWCIGo3wNx2S3ZdH7uOrBJWWOmw/Fjm0p8XfdPv3fe4g+uj
l7lLTKnt+rE//uNAdJIISfC9loHnV6qtg7faLRr/laJKQ/Uj4Lr03Bk4H7H0DPjy
45xmNlFK0yXgNP/QmyGxdxR00ixAhAWr1dLY7uVeNBu+v4K8E0wY2EQE9yqQhAtu
w3TzGnED/eXyo+bC0tMN275GgT1+opODJwaLcIaEvyadvLlWVS2/hxgwUxIMHrv6
EhlU7g+cStYFRrxH1eSYAEiGxa9lj8NRnVj7TvqVyj2PMKe57+mA0Hq8iTxu7SJF
Ede8nCUAy99Qu7lLbIq9m5YCQr+IStE9r6gr1f7Zsd32qwHJiA2M1xAcYrgQmpxz
VaSb+yY31J8=</CipherValue>
          </CipherData>
        </EncryptedData></mb:Data>
    </mb:MetadataBinding>
    <mb:MetadataBinding>
      <mb:Metadata><slab:originatorConfidentialityLabel>
          <slab:ConfidentialityInformation>
            <slab:PolicyIdentifier>TB15</slab:PolicyIdentifier>
            <slab:Classification>SECRET</slab:Classification>
          </slab:ConfidentialityInformation>
          <slab:CreationDateTime>30.06.2019T12:00:00Z</slab:CreationDateTime>
        </slab:originatorConfidentialityLabel></mb:Metadata>
      <mb:Data><EncryptedData xmlns="http://www.w3.org/2001/04/xmlenc#"
          Type="http://www.w3.org/2001/04/xmlenc#Element">
          <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc
"/>
          <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
            <EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#">
              <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
              <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
                <KeyName>Dr. No</KeyName>
              </KeyInfo>
              <CipherData>

<CipherValue>q++RiNAWqMXSElyejIy5liT+g4Zldm4CnPQ8xRZsk+mbswXQkoe94m6NbahYUduj
UM3OQnTdUeap8y/d/rwb/mRR/4IrWiKSCmuNpEwcvp6t+sJenehIeOtpNmOg+t1k
EdEkT/rdWyL3zpI9h+A7ygD3gSU9kPm6kgMapp3pRRZf5goOR759GoMh508SJrcV
hQKPKOE5UYuuTC7LntVnDOelKG7EQpjLm2J8k4IEXy5CuGk71QfJSgMZ8GNxzPDZ
lvysVwB3VoeBPgWxGAJwyJptlv3y0/mPmG5k/ak7hmHrpoIbBlOgVCWRLMQEdqAj
nAE6Kqh9B5KMDKjYWWb0+Q==</CipherValue>
              </CipherData>
            </EncryptedKey>
          </KeyInfo>
          <CipherData>

<CipherValue>tRTf//uK2YO5s8daH6sOzccVm7PgpSVAs/p0tM9s8GpouhioYxTDeeyw/hRyXpWI
Hrq91jK1mAdI5AQ605YNaCbiu5oOhMsWvuMeUdN0+2+KgY1hkhhcJJVNSt/rpPpJ
T5j+SeLxce8VvoanYPCX9NUiLD1fsBOmsuJy8gjVVbZCRHaGSHmkgsKYBqp7s1zm
hL2LkpthokVHRpeBEBUrW/VkiAZU8lZiHIVAg7SRe+T1vjvqp4ecFpS6mwWN/sid
eGh1UimgZzXhdaweRrIXyNHxSuGVRGcGA4HF7GGoGWvhjR4IR/iWQEfXzxWzHrwv
0CguUm2XdR0m4JdA0NG34C6N/sv627qH3cyPbeTavvNbjPmkEgEOvmnk3WgFEP4k
```

```
1tXEGarWFpHTLqEMO44VI3EZmjRrW7Dqku9QrCv7L9xB0zsMlvmFbHYKbzTKjwR4
4VAQXW+1nsRFXQpMCN/xq/v+ajXK/Ym0oluj6smZMWPm5oM1XzTPGMykJt6RaXyV
1UNShuJRd2tpNbcE/Qe0/gRD/olQCzucmOW7j1uO5TOJaOL57W6nVevah02jva9X
iELLFKOzU0r/hRra60LrHKs328Qi/c1ENkBeZ9WhcXGQqAQ4uIzoKSHEtb+A6IND
fz5eJCmToI6nF0uMQppIYOJxJLfKXQxoleAijy3lWhHaFMAuzs2hpQDxsExdQmqQ
fpsZIYYPOnTFlQ9MbQq6uZQsYJ/exW55IITON0o61ZvAQTO0wQf/SLukT/A6EYTO
DNpfYhpa0YocaJ5G3acYUiX2IMRZgKT6uKicU6PZVFY4MJzYGqOTnvVlCTd3Xxx+
pkSVR/fo5RDRNHwm4XuyWRVwrrvVkQfDWNH9CvyY0JRrr8kPE2QkzYwYjv4yMcyO
IDCag32SYlBdSfFA6lG4/qk7M5kfmppMLQ3M25oG6tIwlSYoKGMXjGMS+BKEVtgJ
ghpsI3Bj2aSiCs/0+19O3A1TeGkWYq+Y3oez98bfv9b4US445ACEl84adodgQtWh
rkwCNC2qhQ3y4gb0pleYD1WMk+ThbXgMODx/Qb+5UWHWSfDZ1YpTR7GR1nNnrb9Y
4Ln7mmYW8gi+yTLmnI2JHPF1A6RA13P61tQUuRSaB9X2yMU0owNumJjDDTkieXld
Q9rZEA5xHYZ07aKXFpX7LZxwoKtvq9Al9U+oza29IIHHDtzATZxMKawsF/SgqAWT
da0EJWlGrZRNCJKXC1ILIh2LMMvv2ElNqMN0dANBIgFDbmBIK0bLWe3n3NWGbI1G
Z2tfVtXGkK3Q1qFtT7y++N4aJwms4z3JGt7CIUd+pGUXRu5lrc1SIjDvC0yY8pKn</CipherValue>
          </CipherData>
        </EncryptedData></mb:Data>
    </mb:MetadataBinding>
  </mb:MetadataBindingContainer>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"/>
      <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
      <ds:Reference Id="xml:id" URI="#WFS">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <ds:DigestValue>8tcwOOincWXzmthLcYshy1hfeNo=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>

<ds:SignatureValue>NjgCX+HRx/yjoO11GEqwVe0x80gIzMUcz+f7Ttqik8sXxHEGIZQQVApi7WyARZgy
sT2EGvUR6LJPdDmv1vfOG/M+o4oVuEsP0iTASwDr2BFMQrAIk9KOQkxW5ta4eCsv
agaOU4Ct98YpyYtmYG4mgTgfgDyih45Tf5FMSlnIbw75H5VLnPeLXwMOvvACmopx
4Bje+e7Rr9J/haq439RdjYn/LIsg+Rj7zvu5lAjvZ8RTT1M1CMQWXQ5m05bNn+G4
4Xg9a7wMKqh2SDmfOwrViduK7wvZaxCUrvBSc0FZlQYrs/iEu5JDSAWfQzNSDmdO
7ummsMOs3ipEXMo9xV7Ufw==</ds:SignatureValue>
    <ds:KeyInfo>
      <ds:KeyName>Dr. No</ds:KeyName>
      <ds:X509Data>



<ds:X509Certificate>MIIDuTCCAqGgAwIBAgIEYpLJdjANBgkqhkiG9w0BAQsFADCBjDELMAkGA1UEBhMC
REUxEDAOBgNVBAgTB0JhdmFyaWExDzANBgNVBAcTBk11bmljaDEfMB0GA1UEChMW
U2VjdXJlIERpbWVuc2lvbnMgR21iSDEfMB0GA1UECxMWU2VjdXJlIERpbWVuc2lv
bnMgR21iSDEYMBYGA1UEAxMPQW5kcmVhcyBNYXRoZXVzMB4XDTE1MTAyNTE0NDEw
MVoXDTE2MDEyMzE0NDEwMVowgYwxCzAJBgNVBAYTAkRFMRAwDgYDVQQIEwdCYXZh
```

```
cmlhMQ8wDQYDVQQHEwZNdW5pY2gxHzAdBgNVBAoTFlNlY3VyZSBEaW1lbnNpb25z
IEdtYkgxHzAdBgNVBAsTFlNlY3VyZSBEaW1lbnNpb25zIEdtYkgxGDAWBgNVBAMT
D0FuZHJlYXMgTWF0aGV1czCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AJBxrjwhMmOGnSKT4DLsOx+R+c4dN3gA74/03NdsxUdy2r6QB65AvF8Rm3YF5pJy
Hzdrlf43IObjOHK2yRn6p0tXpc5yYwBGd3tZMGTkyj4qhqqy/ug4LxYy4HYfCXE/
ec9UOTCDu7vfkbvmEfg8V0M2DfT6t5XnvFZmkUkSAi4L4vQ9PJthsFLyJXq2nNlh
tOMQeBWxcOzbog6EBAB7qaUyumlrrIojksHd9Tb4Om/BIp+JxcocRjGmSq7XoKZ1
GuXmWXSnrc877AnET/+Kbea4zqH+Oo44zP2G0XdCCMiKtL7nxqIAfwucp3SEGtqH
XGNv61RGsqihQbtlbhRkprcCAwEAAaMhMB8wHQYDVR0OBBYEFIVLBZDvNUo/OX9F
MKRLz7OFaUXXMA0GCSqGSIb3DQEBCwUAA4IBAQCA7FkGI0EOkJPr4yjCT8HxJvAd
lzNW539tl/SVYe4ducBm4J523G6POKvz6kVHbS30J2HiNd2FoQL9s2DMPN2ag9Q3
myzI8E9x8dowNKhaupmTJI/Edneqnp7pr/8/o612qBXTf00T4j8QP9mZxUreqC+x
TCV9GCO0XuIVpBM6sGbEiFfjg0xLs3HO7kBHla78WAb8EyZGv9aoHCsqoIE+A/L9
e++xrY09TN/wjJKrv665iRF3XG+WHj0lrUvzlPZzNHbLykqSo48DhDc/JmaadiqZ
cNFF8NBHOLzicsSo+GpeEnSJBKnCYwxStWJ+dFWoHQxwyHrkn+Om+EiQ6/2w</ds:X509Certificate>
        <ds:X509SubjectName>CN=Andreas Matheus,OU=Secure Dimensions GmbH,O=Secure
Dimensions GmbH,L=Munich,ST=Bavaria,C=DE</ds:X509SubjectName>
      </ds:X509Data>
    </ds:KeyInfo>
  </ds:Signature>
</mb:BindingInformation>
```

This is the original output from the WFS3:

```
<?xml version="1.0" encoding="utf-8"?>
<wfs:FeatureCollection xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:ows="http://www.opengis.net/ows/1.1" xmlns:gml="
http://www.opengis.net/gml/3.2"
  xmlns:fes="http://www.opengis.net/fes/2.0" xmlns:xlink="
http://www.w3.org/1999/xlink"
  xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xml=
"http://www.w3.org/XML/1998/namespace"
  xmlns:cite="http://www.opengeospatial.net/cite" xmlns:tiger="http://www.census.gov"
  xmlns:nurc="http://www.nurc.nato.int" xmlns:sde="http://geoserver.sf.net"
  xmlns:it.geosolutions="http://www.geo-solutions.it" xmlns:topp=
"http://www.openplans.org/topp"
  xmlns:sf="http://www.openplans.org/spearfish" xmlns:wfs=
"http://www.opengis.net/wfs/3.0"
  xmlns:atom="http://www.w3.org/2005/Atom" numberReturned="6" numberMatched="6"
  timeStamp="2019-06-27T08:03:42Z"
  xsi:schemaLocation="http://www.census.gov http://demo.secure-
dimensions.de:80/geoserver/wfs?service=WFS&amp;version=2.0.0&amp;request=DescribeFeatu
reType&amp;typeName=tiger%3Apoi http://www.opengis.net/gml/3.2 http://demo.secure-
dimensions.de:80/geoserver/schemas/gml/3.2.1/gml.xsd http://www.opengis.net/wfs/3.0
https://raw.githubusercontent.com/opengeospatial/WFS_FES/master/core/xml/wfs.xsd
http://www.w3.org/2005/Atom http://schemas.opengis.net/kml/2.3/atom-author-link.xsd">
  <atom:link rel="self" title="this document"
    type="application/gml+xml;profile=
&quot;http://www.opengis.net/def/profile/ogc/2.0/gml-sf2&quot;;version=3.2"
    href="http://wfs3.secure-
```

```
dimensions.de/rest/services/geoserver/collections/poi/items?f=xml"/>
  <atom:link rel="alternate" title="this document as GeoJSON" type=
"application/geo+json"
    href="http://wfs3.secure-
dimensions.de/rest/services/geoserver/collections/poi/items?f=json"/>
  <atom:link rel="alternate" title="this document as HTML" type="text/html"
    href="http://wfs3.secure-
dimensions.de/rest/services/geoserver/collections/poi/items?f=html"/>
  <wfs:member>
    <tiger:poi gml:id="poi.1">
      <tiger:the_geom>
        <gml:Point srsName="http://www.opengis.net/def/crs/OGC/1.3/CRS84"
srsDimension="2">
          <gml:pos>-74.0104611 40.70758763</gml:pos>
        </gml:Point>
      </tiger:the_geom>
      <tiger:NAME>museam</tiger:NAME>
      <tiger:THUMBNAIL>pics/22037827-Ti.jpg</tiger:THUMBNAIL>
      <tiger:MAINPAGE>pics/22037827-L.jpg</tiger:MAINPAGE>
    </tiger:poi>
  </wfs:member>
  <wfs:member>
    <tiger:poi gml:id="poi.2">
      <tiger:the_geom>
        <gml:Point srsName="http://www.opengis.net/def/crs/OGC/1.3/CRS84"
srsDimension="2">
          <gml:pos>-74.01083751 40.70754684</gml:pos>
        </gml:Point>
      </tiger:the_geom>
      <tiger:NAME>stock</tiger:NAME>
      <tiger:THUMBNAIL>pics/22037829-Ti.jpg</tiger:THUMBNAIL>
      <tiger:MAINPAGE>pics/22037829-L.jpg</tiger:MAINPAGE>
    </tiger:poi>
  </wfs:member>
  <wfs:member>
    <tiger:poi gml:id="poi.3">
      <tiger:the_geom>
        <gml:Point srsName="http://www.opengis.net/def/crs/OGC/1.3/CRS84"
srsDimension="2">
          <gml:pos>-74.01053024 40.70938712</gml:pos>
        </gml:Point>
      </tiger:the_geom>
      <tiger:NAME>art</tiger:NAME>
      <tiger:THUMBNAIL>pics/22037856-Ti.jpg</tiger:THUMBNAIL>
      <tiger:MAINPAGE>pics/22037856-L.jpg</tiger:MAINPAGE>
    </tiger:poi>
  </wfs:member>
  <wfs:member>
    <tiger:poi gml:id="poi.4">
      <tiger:the_geom>
        <gml:Point srsName="http://www.opengis.net/def/crs/OGC/1.3/CRS84"
```

```
srsDimension="2">
          <gml:pos>-74.00857344 40.71194565</gml:pos>
        </gml:Point>
      </tiger:the_geom>
      <tiger:NAME>lox</tiger:NAME>
      <tiger:THUMBNAIL>pics/22037884-Ti.jpg</tiger:THUMBNAIL>
      <tiger:MAINPAGE>pics/22037884-L.jpg</tiger:MAINPAGE>
    </tiger:poi>
  </wfs:member>
  <wfs:member>
    <tiger:poi gml:id="poi.5">
      <tiger:the_geom>
        <gml:Point srsName="http://www.opengis.net/def/crs/OGC/1.3/CRS84"
srsDimension="2">
          <gml:pos>-74.01183158 40.70852996</gml:pos>
        </gml:Point>
      </tiger:the_geom>
      <tiger:NAME>church</tiger:NAME>
      <tiger:THUMBNAIL>pics/22037839-Ti.jpg</tiger:THUMBNAIL>
      <tiger:MAINPAGE>pics/22037839-L.jpg</tiger:MAINPAGE>
    </tiger:poi>
  </wfs:member>
  <wfs:member>
    <tiger:poi gml:id="poi.6">
      <tiger:the_geom>
        <gml:Point srsName="http://www.opengis.net/def/crs/OGC/1.3/CRS84"
srsDimension="2">
          <gml:pos>-74.00153046 40.71988512</gml:pos>
        </gml:Point>
      </tiger:the_geom>
      <tiger:NAME>fire</tiger:NAME>
      <tiger:THUMBNAIL>pics/28640984-Ti.jpg</tiger:THUMBNAIL>
      <tiger:MAINPAGE>pics/28640984-L.jpg</tiger:MAINPAGE>
    </tiger:poi>
  </wfs:member>
</wfs:FeatureCollection>
```

Appendix B: Data Centric Security - Scenario Two

Introduction

This annex demonstrates the ability to verify spatiotemporal aspects of the DCS WFS3 in Testbed-15 as an extension to Scenario One (From vanilla Geoserver to STANAG 4778). Figure 10 illustrates the scenario described in this section.

The main feature of the GeoPDP configuration is to support the disaster management requirement. Normal authorization decisions are paused for the area of interest and the time window of a disaster. Basically, one or more XACML conditions regulate the access of a user with clearance to features with static classification marking. With GeoXACML spatiotemporal conditions, it is possible to "lift" these restrictions by defining one or more areas of interest and time windows that are associated with the disaster.

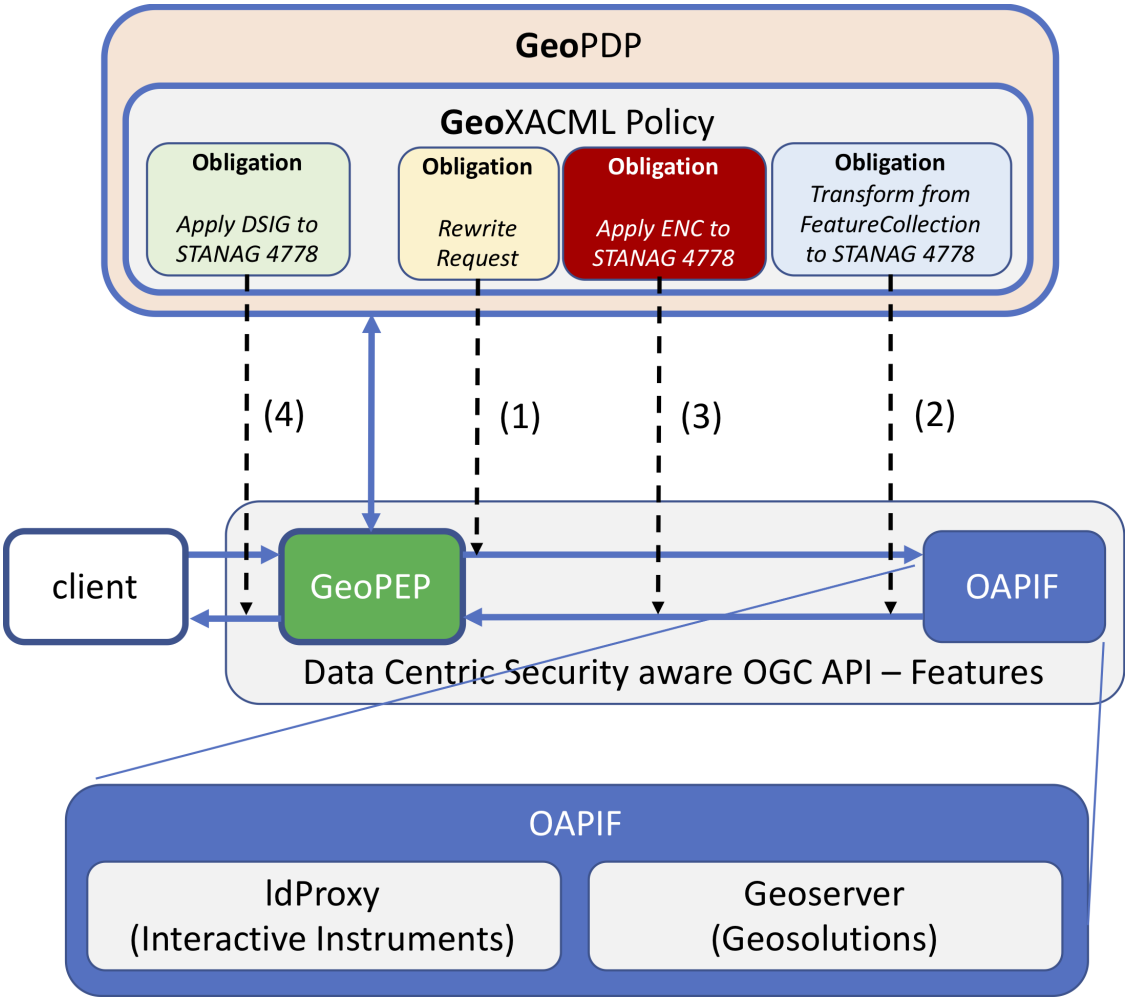

Figure 10. Illustration of the components involved in Scenario Two

The DCS WFS3 accepts different format parameters:

- `f=html`: Allow preview of responses from the WFS3 without the GeoPEP processing (response is a HTML page with map preview of returned features)

- `f=json`: The response in GeoJSON
- `f=xml`: The response as FeatureCollection including GML
- `f=stanag`: The STANAG 4778 response including filtered, encrypted features with an overall digital signature

First, get an access token as a user that has lower clearance as the classification of the feature type. (access token is valid for 30 minutes).

Table 10. Classifications

Feature Type	Classification
poly_landmarks	top_secret
poi	secret
tiger_roads	classified
states	unclassified

Table 11. Users

User	Clearance
jane	top_secret
bob	secret
alice	classified
joe	unclassified

In addition to the static association feature_type < - > classification, the classification for the feature_type `poly_landmarks` is downgraded to classification secret if the user's location is within New York City (Manhattan). The subject's location can be supplied in the client request by submitting the query_string parameter: `urn:sd:subject_location=LAT,LON` In this case if no location is provided with the client request, the static association is used.

Second, fix the subject location for a given (example BBOX that is located mid-town Manhattan).

- Point within the given incident `BBOX: CRS=EPSG:4326;POINT(40.75 -74.00)`
- Point outside the given incident `BBOX: CRS=EPSG:4326;POINT(40.73 -73.50)`

Spatio-temporal access Policy:

```
rule requestLocationRule
{
  permit
  target
    clause
      GeoXACML3.subject_location <= "CRS=EPSG:4326;POLYGON((40.704586878965245
-74.0361785888672,40.76962180287486 -74.0361785888672,40.76962180287486
-73.94966125488283,40.704586878965245 -73.94966125488283,40.704586878965245
-74.0361785888672))":geometry
      and
      time <= "12:00:00Z":time
  on permit {
    obligation requestKVP {
      action = "insert"
      key = "bbox"
      value = "40.704586878965245,-74.0361785888672,40.76962180287486,-
73.94966125488283"
    }
  }
}
```

A SpatioTemporal Rule is expressed in ALFA limits including the BBOX for selecting features. This Rule is responsible for the request rewriting. Another matching rule exists that takes care of the response filtering, visualized in the next figure. (Full TB15 patio-temporal policy is available from the TB15 wiki).

```
rule responseLocationRule
{
  permit
  target
    clause
      GeoXACML3.subject_location <= "CRS=EPSG:4326;POLYGON((40.704586878965245
-74.0361785888672,40.76962180287486 -74.0361785888672,40.76962180287486
-73.94966125488283,40.704586878965245 -73.94966125488283,40.704586878965245
-74.0361785888672))":geometry
      and
      time <= "12:00:00Z":time
  on permit {
    obligation responseXSLT {
      document =
"PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz4KPCEtLSAKICBUaGlzIFhTTFQgd3JhcHMgY
W55IFdGUyByZXNwb25zZSBpbnRvIFNUQU5BRyA0Nzc4IAogIFRoZSBNZXRhZGF0YSBpcyBzZXQgdG8gbnVsbCB
iZWNhdXNlIHRoaXMgdHJhbnNmb3JtYXRpb24gaXMgdXNlZCBieSBsb2NhdGlvbiBvdmVyd3JpdGUKICBUaGUgZ
mVhdHVyZSB0eXBlcyB0aGF0IGNvcnJlc3BvZCB0byBhIGNsYXNzaWZpY2F0aW9uIGFyZSBvYnRhaW5lZCBmcm9
tIGEgZ2xvYmFsIHBhcmFtCiAgVGhlIFhBQ01MIHBvbGljeSBlbnN1cmVzIHRoYXQgdGhlIHJlcXVlc3RlZCBmZ
WF0dXJlIHR5cGUgbWF0Y2hlcyB0aGUgY2xhc3NpZmljYXRpb24gaW4gdGhpcyBYU0xUCiAgYnkgc2V0dGluZyB
0aGUgZmVhdHVyZSB0eXBlcyB2aWEgdGhlIGdsb2JhbCBwYXJhbXMKLS0+Cjx4c2w6dHJhbnNmb3JtIHZlcnNpb
249IjEuMCIgeG1sbnM6eHNsPSJodHRwOi8vd3d3LnczLm9yZy8xOTk5L1hTTC9UcmFuc2Zvcm0iIGV4dGVuc2l
vbi1lbGVtZW50LXByZWZpeGVzPSJkYXRlIiB4bWxuczpkYXRlPSJodHRwOi8vZXhzbHQub3JnL2RhdGVzLWFuZ

```
rule requestLocationRule
{
  permit
  target
    clause
      GeoXACML3.subject_location <= "CRS=EPSG:4326;POLYGON((40.704586878965245
-74.0361785888672,40.76962180287486 -74.0361785888672,40.76962180287486
-73.94966125488283,40.704586878965245 -73.94966125488283,40.704586878965245
-74.0361785888672))":geometry
      and
      time <= "12:00:00Z":time
  on permit {
    obligation requestKVP {
      action = "insert"
      key = "bbox"
      value = "40.704586878965245,-74.0361785888672,40.76962180287486,-
73.94966125488283"
    }
  }
}
```

A SpatioTemporal Rule is expressed in ALFA limits including the BBOX for selecting features. This Rule is responsible for the request rewriting. Another matching rule exists that takes care of the response filtering, visualized in the next figure. (Full TB15 patio-temporal policy is available from the TB15 wiki).

```
rule responseLocationRule
{
  permit
  target
    clause
      GeoXACML3.subject_location <= "CRS=EPSG:4326;POLYGON((40.704586878965245
-74.0361785888672,40.76962180287486 -74.0361785888672,40.76962180287486
-73.94966125488283,40.704586878965245 -73.94966125488283,40.704586878965245
-74.0361785888672))":geometry
      and
      time <= "12:00:00Z":time
  on permit {
    obligation responseXSLT {
      document =
"PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz4KPCEtLSAKICBUaGlzIFhTTFQgd3JhcHMgY
W55IFdGUyByZXNwb25zZSBpbnRvIFNUQU5BRyA0Nzc4IAogIFRoZSBNZXRhZGF0YSBpcyBzZXQgdG8gbnVsbCB
iZWNhdXNlIHRoaXMgdHJhbnNmb3JtYXRpb24gaXMgdXNlZCBieSBsb2NhdGlvbiBvdmVyd3JpdGUKICBUaGUgZ
mVhdHVyZSB0eXBlcyB0aGF0IGNvcnJlc3BvZCB0byBhIGNsYXNzaWZpY2F0aW9uIGFyZSBvYnRhaW5lZCBmcm9
tIGEgZ2xvYmFsIHBhcmFtCiAgVGhlIFhBQ01MIHBvbGljeSBlbnN1cmVzIHRoYXQgdGhlIHJlcXVlc3RlZCBmZ
WF0dXJlIHR5cGUgbWF0Y2hlcyB0aGUgY2xhc3NpZmljYXRpb24gaW4gdGhpcyBYU0xUCiAgYnkgc2V0dGluZyB
0aGUgZmVhdHVyZSB0eXBlcyB2aWEgdGhlIGdsb2JhbCBwYXJhbXMKLS0+Cjx4c2w6dHJhbnNmb3JtIHZlcnNpb
249IjEuMCIgeG1sbnM6eHNsPSJodHRwOi8vd3d3LnczLm9yZy8xOTk5L1hTTC9UcmFuc2Zvcm0iIGV4dGVuc2l
vbi1lbGVtZW50LXByZWZpeGVzPSJkYXRlIiB4bWxuczpkYXRlPSJodHRwOi8vZXhzbHQub3JnL2RhdGVzLWFuZ
```
```

```
C10aW1lcyI+CiAgPHhzbDpvdXRwdXQgbWV0aG9kPSJ4bWwiIGluZGVudD0ieWVzIi8+CiAgCiAgPHhzbDpzdHJ
pcC1zcGFjZSBlbGVtZW50cz0iKiIgLz4KICAKICA8eHNsOnBhcmFtIG5hbWU9InVuY2xhc3NpZmllZEZlYXR1c
mVUeXBlIj48L3hzbDpwYXJhbT4KICA8eHNsOnBhcmFtIG5hbWU9ImNsYXNzaWZpZWRGZWF0dXJlVHlwZSI+PC9
4c2w6cGFyYW0+CiAgPHhzbDpwYXJhbSBuYW1lPSJzZWNyZXRGZWF0dXJlVHlwZSI+PC94c2w6cGFyYW0+CiAgP
HhzbDpwYXJhbSBuYW1lPSJ0b3BzZWNyZXRGZWF0dXJlVHlwZSI+PC94c2w6cGFyYW0+CiAgCiAgPHhzbDp0ZW1
wbGF0ZSBuYW1lPSJVTkNMQVNTSUZJRUQiPiAgCiAgICA8bWI6TWV0YWRhdGFCaW5kaW5nIHhtbG5zOm1iPSJ1c
m46bmF0bzpzdGFuYWc6NDc3ODpiaW5kaW5naW5mb3JtYXRpb246MTowIj4KICAgICAgPG1iOk1ldGFkYXRhPgo
gICAgICAgIDxzbGFiOm9yaWdpbmF0b3JDb25maWRlbnRpYWxpdHlMYWJlbAogICAgICAgICAgeG1sbnM6c2xhY
j0idXJuOm5hdG86c3RhbmFnOjQ3NzQ6Y29uZmlkZW50aWFsaXR5bWV0YWRhdGFsYWJlbDoxOjAiPgogICAgICA
gICAgPHNsYWI6Q29uZmlkZW50aWFsaXR5SW5mb3JtYXRpb24+CiAgICAgICAgICAgIDxzbGFiOlBvbGljeUlkZ
W50aWZpZXI+VEIxNTwvc2xhYjpQb2xpY3lJZGVudGlmaWVyPgogICAgICAgICAgICA8c2xhYjpDbGFzc2lmaWN
hdGlvbj5OL0E8L3NsYWI6Q2xhc3NpZmljYXRpb24+CiAgICAgICAgICA8L3NsYWI6Q29uZmlkZW50aWFsaXR5S
W5mb3JtYXRpb24+CiAgICAgICAgICA8c2xhYjpDcmVhdGlvbkRhdGVUaW1lPjx4c2w6dmFsdWUtb2Ygc2VsZWN
0PSJkYXRlOmRhdGUtdGltZSgpIi8+PC9zbGFiOkNyZWF0aW9uRGF0ZVRpbWU+CiAgICAgICAgPC9zbGFiOm9ya
WdpbmF0b3JDb25maWRlbnRpYWxpdHlMYWJlbD4KICAgICAgPC9tYjpNZXRhZGF0YT4KICAgICAgPG1iOkRhdGE
+CiAgICAgICAgPHhzbDpjb3B5LW9mIHNlbGVjdD0iLiIvPgogICAgICA8L21iOkRhdGE+CiAgICA8L21iOk1ld
GFkYXRhQmluZGluZz4KICA8L3hzbDp0ZW1wbGF0ZT4KICAKICA8eHNsOnRlbXBsYXRlIG5hbWU9IkNMQVNTSUZ
JRUQiPgogICAgPG1iOk1ldGFkYXRhQmluZGluZyB4bWxuczptYj0idXJuOm5hdG86c3RhbmFnOjQ3Nzg6YmluZ
GluZ2luZm9ybWF0aW9uOjE6MCI+CiAgICAgIDxtYjpNZXRhZGF0YT4KICAgICAgICA8c2xhYjpvcmlnaW5hdG9
yQ29uZmlkZW50aWFsaXR5TGFiZWwKICAgICAgICAgIHhtbG5zOnNsYWI9InVybjpuYXRvOnN0YW5hZzo0Nzc0O
mNvbmZpZGVudGlhbGl0eW1ldGFkYXRhbGFiZWw6MTowIj4KICAgICAgICAgIDxzbGFiOkNvbmZpZGVudGlhbGl
0eUluZm9ybWF0aW9uPgogICAgICAgICAgICA8c2xhYjpQb2xpY3lJZGVudGlmaWVyPlRCMTU8L3NsYWI6UG9sa
WN5SWRlbnRpZmllcj4KICAgICAgICAgICAgPHNsYWI6Q2xhc3NpZmljYXRpb24+Ti9BPC9zbGFiOkNsYXNzaWZ
pY2F0aW9uPgogICAgICAgICAgPC9zbGFiOkNvbmZpZGVudGlhbGl0eUluZm9ybWF0aW9uPgogICAgICAgICAgP
HNsYWI6Q3JlYXRpb25EYXRlVGltZT48eHNsOnZhbHVlLW9mIHNlbGVjdD0iZGF0ZTpkYXRlLXRpbWUoKSIvPjw
vc2xhYjpDcmVhdGlvbkRhdGVUaW1lPgogICAgICAgIDwvc2xhYjpvcmlnaW5hdG9yQ29uZmlkZW50aWFsaXR5T
GFiZWw+CiAgICAgIDwvbWI6TWV0YWRhdGE+CiAgICAgIDxtYjpEYXRhPgogICAgICAgIDx4c2w6Y29weS1vZiB
zZWxlY3Q9Ii4iLz4KICAgICAgPC9tYjpEYXRhPgogICAgPC9tYjpNZXRhZGF0YUJpbmRpbmc+CiAgPC94c2w6d
GVtcGxhdGU+CiAgCiAgPHhzbDp0ZW1wbGF0ZSBuYW1lPSJTRUNSRVQiPgogICAgPG1iOk1ldGFkYXRhQmluZGl
uZyB4bWxuczptYj0idXJuOm5hdG86c3RhbmFnOjQ3Nzg6YmluZGluZ2luZm9ybWF0aW9uOjE6MCI+CiAgICAgI
DxtYjpNZXRhZGF0YT4KICAgICAgICA8c2xhYjpvcmlnaW5hdG9yQ29uZmlkZW50aWFsaXR5TGFiZWwKICAgICA
gICAgIHhtbG5zOnNsYWI9InVybjpuYXRvOnN0YW5hZzo0Nzc0OmNvbmZpZGVudGlhbGl0eW1ldGFkYXRhbGFiZ
Ww6MTowIj4KICAgICAgICAgIDxzbGFiOkNvbmZpZGVudGlhbGl0eUluZm9ybWF0aW9uPgogICAgICAgICAgICA
8c2xhYjpQb2xpY3lJZGVudGlmaWVyPlRCMTU8L3NsYWI6UG9saWN5SWRlbnRpZmllcj4KICAgICAgICAgICAgP
HNsYWI6Q2xhc3NpZmljYXRpb24+Ti9BPC9zbGFiOkNsYXNzaWZpY2F0aW9uPgogICAgICAgICAgPC9zbGFiOkN
vbmZpZGVudGlhbGl0eUluZm9ybWF0aW9uPgogICAgICAgICAgPHNsYWI6Q3JlYXRpb25EYXRlVGltZT48eHNsO
nZhbHVlLW9mIHNlbGVjdD0iZGF0ZTpkYXRlLXRpbWUoKSIvPjwvc2xhYjpDcmVhdGlvbkRhdGVUaW1lPgogICA
gICAgIDwvc2xhYjpvcmlnaW5hdG9yQ29uZmlkZW50aWFsaXR5TGFiZWw+CiAgICAgIDwvbWI6TWV0YWRhdGE+C
iAgICAgIDxtYjpEYXRhPgogICAgICAgIDx4c2w6Y29weS1vZiBzZWxlY3Q9Ii4iLz4KICAgICAgPC9tYjpEYXR
hPgogICAgPC9tYjpNZXRhZGF0YUJpbmRpbmc+CiAgPC94c2w6dGVtcGxhdGU+CgogIDx4c2w6dGVtcGxhdGUgb
mFtZT0iVE9QU0VDUkVUIj4KICAgIDxtYjpNZXRhZGF0YUJpbmRpbmcgeG1sbnM6bWI9InVybjpuYXRvOnN0YW5
hZzo0Nzc4OmJpbmRpbmdpbmZvcm1hdGlvbjoxOjAiPgogICAgICA8bWI6TWV0YWRhdGE+CiAgICAgICAgPHNsY
WI6b3JpZ2luYXRvckNvbmZpZGVudGlhbGl0eUxhYmVsCiAgICAgICAgICB4bWxuczpzbGFiPSJ1cm46bmF0bzp
zdGFuYWc6NDc3NDpjb25maWRlbnRpYWxpdHltZXRhZGF0YWxhYmVsOjE6MCI+CiAgICAgICAgICA8c2xhYjpDb
25maWRlbnRpYWxpdHlJbmZvcm1hdGlvbj4KICAgICAgICAgICAgPHNsYWI6UG9saWN5SWRlbnRpZmllcj5UQjE
1PC9zbGFiOlBvbGljeUlkZW50aWZpZXI+CiAgICAgICAgICAgIDxzbGFiOkNsYXNzaWZpY2F0aW9uPk4vQTwvc
2xhYjpDbGFzc2lmaWNhdGlvbj4KICAgICAgICAgIDwvc2xhYjpDb25maWRlbnRpYWxpdHlJbmZvcm1hdGlvbj4
KICAgICAgICAgIDxzbGFiOkNyZWF0aW9uRGF0ZVRpbWU+PHhzbDp2YWx1ZS1vZiBzZWxlY3Q9ImRhdGU6ZGF0Z
S10aW1lKCkiLz48L3NsYWI6Q3JlYXRpb25EYXRlVGltZT4KICAgICAgICA8L3NsYWI6b3JpZ2luYXRvckNvbmZ
pZGVudGlhbGl0eUxhYmVsPgogICAgICA8L21iOk1ldGFkYXRhPgogICAgICA8bWI6RGF0YT4KICAgICAgICA8e
HNsOmNvcHktb2Ygc2VsZWN0PSIuIi8+CiAgICAgIDwvbWI6RGF0YT4KICAgIDwvbWI6TWV0YWRhdGFCaW5kaW5
```

```
nPgogIDwveHNsOnRlbXBsYXRlPgogIAogIDx4c2w6dGVtcGxhdGUgbWF0Y2g9Im5vZGUoKSI+CiAgICA8eHNsO
mNob29zZT4KICAgICAgPHhzbDp3aGVuIHRlc3Q9InNlbGY6OiogYW5kIGNvbnRhaW5zKCR1bmNsYXNzaWZpZWR
GZWF0dXJlVHlwZSwgbG9jYWwtbmFtZSgpKSI+CiAgICAgICAgIDx4c2w6Y2FsbC10ZW1wbGF0ZSBuYW1lPSJVT
kNMQVNTUZJRUQiLz4gICAgICAgIAogICAgICA8L3hzbDp3aGVuPgogICAgICA8eHNsOndoZW4gdGVzdD0ic2V
sZjo6KiBhbmQgY29udGFpbnMoJGNsYXNzaWZpZWRGZWF0dXJlVHlwZSwgbG9jYWwtbmFtZSgpKSI+CiAgICAgI
CAgPHhzbDpjYWxsLXRlbXBsYXRlIG5hbWU9IkNMQVNTUZJRUQiLz4KICAgICAgPC94c2w6d2hlbj4KICAgICA
gPHhzbDp3aGVuIHRlc3Q9InNlbGY6OiogYW5kIGNvbnRhaW5zKCRzZWNyZXRGZWF0dXJlVHlwZSwgbG9jYWwtb
mFtZSgpKSI+CiAgICAgICAgPHhzbDpjYWxsLXRlbXBsYXRlIG5hbWU9IlNFQ1JFVCIvPgogICAgICA8L3hzbDp
3aGVuPgogICAgICA8eHNsOndoZW4gdGVzdD0ic2VsZjo6KiBhbmQgY29udGFpbnMoJHRvcHNlY3JldEZlYXR1c
mVUeXBlLCBsb2NhbC1uYW1lKCkpIj4KICAgICAgICAgPHhzbDpjYWxsLXRlbXBsYXRlIG5hbWU9IlVE9QU0VDUkV
UIi8+CiAgICAgIDwveHNsOndoZW4+CiAgICA8L3hzbDpjaG9vc2U+ICAgIAogICAgPHhzbDphcHBseS10ZW1wb
GF0ZXMgc2VsZWN0PSJub2RlKCkiLz4KICA8L3hzbDp0ZW1wbGF0ZT4KICAKICA8eHNsOnRlbXBsYXRlIG1hdGN
oPSIvIj4KICAgICAgPG1iOkJpbmRpbmdJbmZvcm1hdGlvbiB4bWxuczp4c2k9Imh0dHBzOi8vd3d3LnczLm9yZ
y8yMDAxL1hNTFNjaGVtYS1pbnN0YW5jZS54c2QiCiAgICAgIHhtbG5zOmRzPSJodHRwOi8vd3d3LnczLm9yZy8
yMDAwLzA5L3htbGRzaWcjIiB4bWxuczp4bWltZT0iaHR0cDovL3d3dy53My5vcmcvMjAwNS8wNS94bWxtaW1lI
gogICAgICB4bWxuczptYj0idXJuOm5hdG86c3RhbmFnOjQ3Nzg6YmluZGluZ2luZm9ybWF0aW9uOjE6MCIKICA
gICAgeG1sbnM6c2xhYj0idXJuOm5hdG86c3RhbmFnOjQ3NzQ6Y29uZmlkZW50aWFsaXR5bWV0YWRhdGFsYWJlb
DoxOjAiCiAgICAgIHhtbG5zOndzdT0iaHR0cDovL2RvY3Mub2FzaXMtb3Blbi5vcmcvd3NzLzIwMDQvMDEvb2F
zaXMtMjAwNDAxLXdzcy13c3NlY3VyaXR5LXV0aWxpdHktMS4wLnhzZCIKICAgICAgICAgeG1sbnM6eG1sPSJodHRwO
i8vd3d3LnczLm9yZy9YTUwvMTk5OC9uYW1lc3BhY2UiCiAgICAgIHhtbG5zOmRzPSJodHRwOi8vd3d3LnczLm9yZ
GF0YUJpbmRpbmdDb250YWluZXIgeG1sOmlkPSJXRlMiPgogICAgICAgICAgIDx4c2w6YXBwbHktdGVtcGxhdGVzIHN
lbGVjdD0iQCp8bm9kZSgpIi8+CiAgICAgICAgICAgICA8bWI6QmFzZTY0VHRhdGFCaW5kaW5nIHhtbG5zOm1iPSJ1cm46b
mF0bzpzdGFuYWc6NDc3ODpiaW5kaW5naW5mb3JtYXRpb246MTowIj4KICAgICAgICAgICAgICAgICAgPG1iOk1ldGFkYXR
hPgogICAgICAgICAgICAgICAgICAgIDxudWxsLz4KICAgICAgICAgICAgICAgICAgPC9tYjpNZXRhZGF0YT4KICAgICAgICAgICAgICA
8L21iOkJpbmRpbmdJbmZvcm1hdGlvbj4KICA8L3hzbDp0ZW1wbGF0ZT4KICAKPC94c2w6c3R5bGVzaGVldD4="
      parameter = "unclassifiedFeatureType=states tiger_roads poly_landmarks poi"
    }
  }

}
```

The Spatial Filter Rule that tasks the GeoPEP to run the WFS3 response through the XSLT provided is specified below.

The temporal aspect:

Testing the spatio-temporal policy requires making requests BEFORE 12:00UTC and after.

- 00:00 - 12:00UTC ⇒ The response will contain all requested features of the given type but marked with classification "N/A"
- 12:00 - 23:59UTC ⇒ The response does not contain features.

Demonstration

This demonstration uses the same deployment as Scenario 1. Please see Annex A for details how to obtain an access token.

Executing the geoPEP enforcing spatio-temporal policy

To obtain an access token for user "joe", please use the following CURL:

```
curl -k -i -X POST -H "Authorization:Basic
ZmEwMGVmNGYtMTQzZC1kYTUzLWM4MTQtYWMxODY2ZDU5MmM1QG9nYy5zZWN1cmUtZGltZW5zaW9ucy5jb206Yj
BkZWM0Zjg1MzI3YzlhZjgwZjk2NjlmMGM4Zjk2NmViYzNmZmFhMGY1YzU2YzI0NGJhYzc2ODAyZDZiYTllZg==
" -H "Content-Type:application/x-www-form-urlencoded" -d "grant_type=password" -d
"username=jane" -d "password=secret" -d "scope=openid saml tb15" -d
"response_type=token" 'https://ogc.secure-dimensions.com/oauth/token'
```

With the access token for the user, the following requests simulates a subject location inside and outside the policy BBOX:

- example request for subject location **within** the policy's BBOX:

```
https://ogc.secure-
dimensions.com/rest/services/DCS/collections/poi/items?f=stanag&subjectlocation=CRS=EP
SG:4326;POINT(40.75 -74.00)&access_token=<access token>
```

- example request for subject location **outside** the policy's BBOX:

```
https://ogc.secure-
dimensions.com/rest/services/DCS/collections/poi/items?f=stanag&subjectlocation=CRS=EP
SG:4326;POINT(40.73 -73.5)&access_token=<access token>
```

Verifying the original WFS3 response with ldproxy from Interactive Instruments

In order to verify what the original Feature Collection is going to look like - BEFORE it is processed by the GeoPEP - please use the XML or JSON formats:

Visualizing the original WFS3 responses when applying the subject location.

Client requests can be visualized by the following URL template:

```
https://ogc.secure-
dimensions.com/rest/services/DCS/collections/<feature_type>/items?f=html&access_token=
<access token>&subjectlocation=<location>
```

For making requests in the format "html", all users are able to fetch the same features for any type. The WFS3 itself is NOT DCS aware!

So first, fetch an access token of your favorite user.

Then make a request and either provide a subject location OUTSIDE the BBOX or do NOT provide a

subject location. Example URLs:

- subject location **outside** the policy BBOX

```
https://ogc.secure-
dimensions.com/rest/services/DCS/collections/tiger_roads/items?f=html&access_token=<ac
cess token>&subjectlocation=CRS=EPSG:4326;POINT(40.73 -73.5)
```

- subject location **omitted**

```
https://ogc.secure-
dimensions.com/rest/services/DCS/collections/tiger_roads/items?f=html&access_token=<ac
cess token>
```

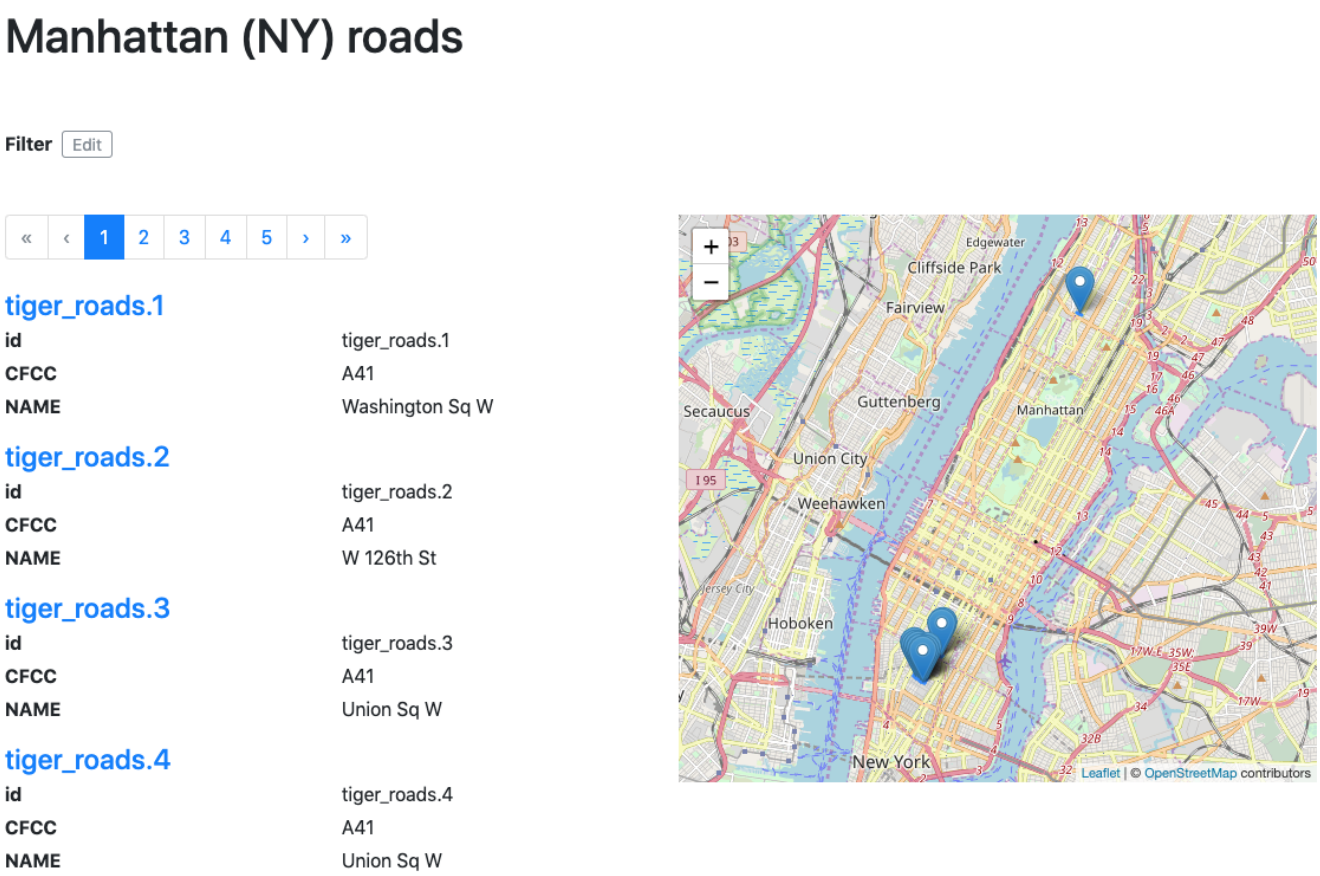

Figure 11. The features got returned for the given request - note that tiger_roads.2 (W 126th St.) is returned; it is located north of the BBOX.

Then make a request with the user location WITHIN the given BBOX. You will see that only features in the BBOX - specified in the GeoPolicy - are returned by the WFS3. This is caused by the GeoPEP doing the request rewriting!

```
https://ogc.secure-
dimensions.com/rest/services/DCS/collections/tiger_roads/items?f=html&access_token=<ac
cess token>&subjectlocation=CRS=EPSG:4326;POINT(40.75%20-74.00)
```

Manhattan (NY) roads

Filter Edit

« ‹ 1 2 3 4 5 › »

tiger_roads.1

id	tiger_roads.1
CFCC	A41
NAME	Washington Sq W

tiger_roads.3

id	tiger_roads.3
CFCC	A41
NAME	Union Sq W

tiger_roads.4

id	tiger_roads.4
CFCC	A41
NAME	Union Sq W

tiger_roads.5

id	tiger_roads.5
CFCC	A41
NAME	Washington Sq E

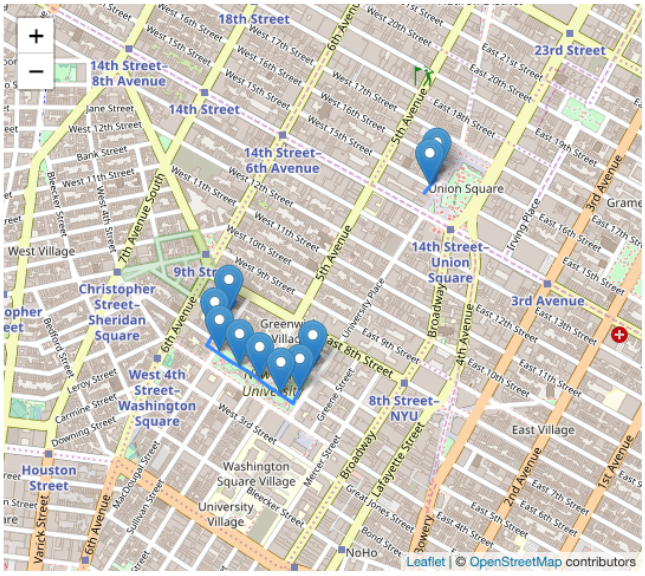

Figure 12. The features got returned for the given BBOX - note that tiger_roads.2 is not returned as it is located north of the BBOX as you can see in the figure above.

Appendix C: Data Centric Security - Scenerio Three

Intro

This annex demonstrates the ability to process STANAG 4778 encoded DCS objects inside a WFS FeatureCollection. A WFS FeatureCollection is an XML data structure that is defined (for WFS 2.0) in the XSD `wfs.xsd`. Essentially, the root element `<wfs:FeatureCollection>` contains zero or more `<wfs:member>` elements where the content can be (i) `<wfs:FeatureCollection>` or `<xsd:any>`. The described DCS alternative here leverages the `<xsd:any>` choice to place a STANAG 4778 encoded DCS object into the `<wfs:member>` element.

Each STANAG DCS object returned by the WFS3 has the `< Metadata>` element in the clear and the `<Data>` element encrypted. This ensures (i) that the GeoPEP can process the response according to the user's privilege / object classification and (ii) that the data is always encrypted.

```
<wfs:member>
    <dcs:dcs_object xml:id="feature_1" dcs:encoding_type="stanag4778">
      <mb:BindingInformation>
        <mb:MetadataBindingContainer>
          <mb:MetadataBinding>
            <mb:Metadata>
              <slab:originatorConfidentialityLabel>
                <slab:ConfidentialityInformation>
                  <slab:PolicyIdentifier>TB15</slab:PolicyIdentifier>
                  <slab:Classification>SECRET</slab:Classification>
                </slab:ConfidentialityInformation>
                <slab:CreationDateTime>2019-08-
19T09:12:04.520Z</slab:CreationDateTime>
              </slab:originatorConfidentialityLabel>
            </mb:Metadata>
            <mb:Data>
              <enc:EncryptedData>
                <enc:EncryptionMethod Algorithm=
"http://www.w3.org/2001/04/xmlenc#aes128"/>
                <enc:EncryptionKeyInfo>
                  <enc:EncryptedKey>
                    <enc:SignatureMethod
                      Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
                    <enc:KeyInfo>
                      <enc:KeyName>Jane Bond 128</enc:KeyName>
                    </enc:KeyInfo>
                    <enc:CipherData>
                      <enc:CipherValue>YaYjKMQsccm6...gcGOJCbQ==</enc:CipherValue>
                    </enc:CipherData>
                  </enc:EncryptedKey>
                </enc:EncryptionKeyInfo>
                <CipherData>
                  <CipherValue>
+BBWAwnfFLaZG9ONeK0O/kiJ1wvRiyDwMtP...FL9VsSQyg==</CipherValue>
                </CipherData>
              </enc:EncryptedData>
            </mb:Data>
          </mb:MetadataBinding>
        </mb:MetadataBindingContainer>
      </mb:BindingInformation>
    </dcs:dcs_object>
  </wfs:member>
```

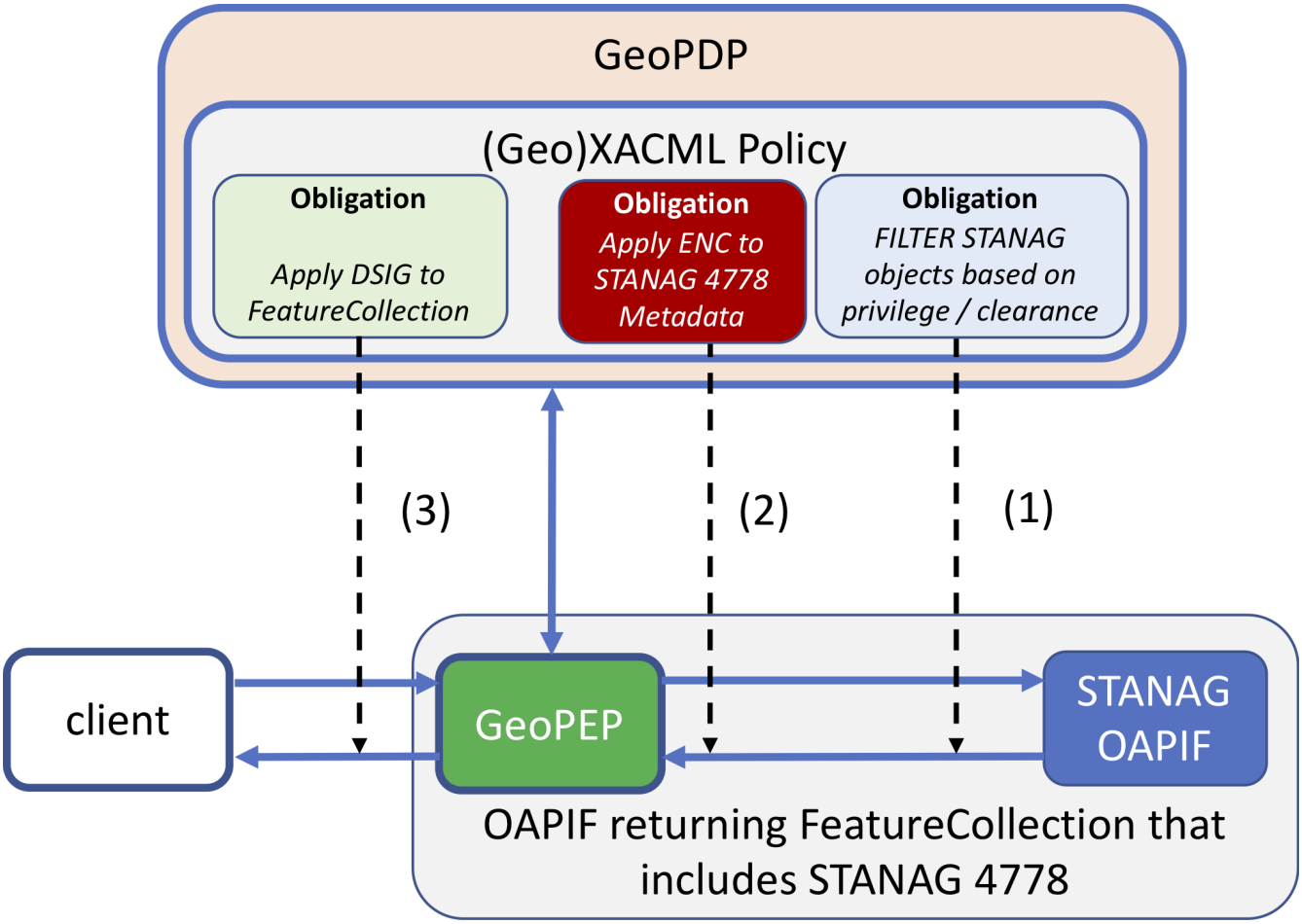

Figure 13. Illustration of a FeatureCollection including STANAG 4778 objects (metadata in the clear and data encrytped).

The GeoPEP forwards the incoming request from the client to the WFS3. The response gets processed in the following order:

- XSLT processing: Based on the user's clearance, each STANAG object gets inspected and removed in case the user's clearance is less than the classification level expressed in the `<slab:Classification>` element. So as an example, for users jane and bob, the response would contain the example data object above; however for users alice and joe the entire `<wfs:member>` element gets removed.
- XML Encryption: Once the XSLT based response filtering is finished, the content of the remaining `<mb:Metadata>` elements is encrypted based on the user's public key.
- XML Digital Signature: The final FeatureCollection is digitally signed using the GeoPEP's private key. Attention: The result of this step produces an invalid FeatureCollection structure, as the inserted DigitalSignature element is not supported by the schema of the WFS FeatureCollection!

```
<wfs:member>
  <dcs:dcs_object xml:id="feature_1" dcs:encoding_type="stanag4778">
    <mb:BindingInformation>
      <mb:MetadataBindingContainer>
        <mb:MetadataBinding>
          <mb:Metadata>
            <EncryptedData xmlns="http://www.w3.org/2001/04/xmlenc#" Type=
"http://www.w3.org/2001/04/xmlenc#Element">
```

```
              <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-
cbc"/>
              <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
                <EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#">
                  <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-
1_5"/>
                  <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
                    <KeyName>138af896-3487-32d6-8171-c4a51c416424</KeyName>
                  </KeyInfo>
                  <CipherData>

<CipherValue>k1fLcibV4QOu1gZRL3HsbCmv3Uu/cApMfu09FlD8N98OCB4Cv4Y4Xl0qm0b2p7uo
                      OuJQeLJWwhMLPg3vnIqhlo5LESQpkWGHIdwOrzamd58Z83IgUQUoT04yLmTi6s4m
                      +IZncYHyz57uJYcVlFsEoTU0l0fCMufbVX6rp6p+ZoIc6xK4RfpYWTPxBLwkEfhc
                      qzcN6lmcSQ5OUkHUPf5O33fqDcfFTDAMGtPdWkn/YY2djwSe8/iZQDZ9B6tcXgUm
                      ajMMup5rFnavkjdI60NwTM/FHT3fpex2HCUgsyzePB4fdN03wGN2WdjxrF/x4Wd0
                      4C9oMP2duUfzDeuHyZ6Axw==</CipherValue>
                  </CipherData>
                </EncryptedKey>
              </KeyInfo>
              <CipherData>

<CipherValue>p7vlvSGvbzpgR7ly5AmTi3TdsrudznhFA8kFb6KpyCnX28WDyUEO7+7bSR2ZlA7B
                    6vpuzFQoIrvgqVAhxrunPVXzUlRq6QCfv6HN4+orP2qDzmOlCnZ3C1b4ju8yE00r
                    xeJN2ix4JMqPSfFBr6zjAVyT3HORPlzZKlzeU2CeVe4B0+FgBBfFcIKB1C/M3JLj
                    8W2ytQBjGFTdTRC/BJyJfotGd7zpRQ9PJSIvLr+u2UiJEnAOadV5ozMmvu+M2xk8
                    fAIeh33qoVBkzLbSUjWVfWuU/J8cstSESEjBPWx96hj1go0CWIyY7gDTihP2mwki
                    n6XLEPS9tZ3W4VO0jWVMisx9OLGPyRCs1Omn7FkfRZtrWM1lEl0qJ4Bwm4eUmMvu

2jFA8AGUnq9S+0f7YqC0nMN/dXNUDSLxZWOqUPyU6IoWuD0i9Nv+Mg==</CipherValue>
              </CipherData>
            </EncryptedData>
          </mb:Metadata>
          <mb:Data>
            <enc:EncryptedData>
              <enc:EncryptionMethod Algorithm="
http://www.w3.org/2001/04/xmlenc#aes128"/>
              <enc:EncryptionKeyInfo>
                <enc:EncryptedKey>
                  <enc:SignatureMethod
                    Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
                  <enc:KeyInfo>
                    <enc:KeyName>Jane Bond 128</enc:KeyName>
                  </enc:KeyInfo>
                  <enc:CipherData>
                    <enc:CipherValue>YaYjKMQsccm6...gcGOJCbQ==</enc:CipherValue>
                  </enc:CipherData>
                </enc:EncryptedKey>
              </enc:EncryptionKeyInfo>
              <CipherData>
                <CipherValue>
```

```
+BBWAwnfFLaZG9ONeK0O/kiJ1wvRiyDwMtP...FL9VsSQyg==</CipherValue>
              </CipherData>
            </enc:EncryptedData>
          </mb:Data>
        </mb:MetadataBinding>
      </mb:MetadataBindingContainer>
    </mb:BindingInformation>
  </dcs:dcs_object>
</wfs:member>
```

The following XML snippet illustrates the resulting FeatureCollection after the XML Digital Signature is applied:

```
<?xml version="1.0"?>
<wfs:FeatureCollection xmlns:wfs="http://www.opengis.net/wfs/3.0"
  xmlns:gml="http://www.opengis.net/gml" xmlns:mb=
"urn:nato:stanag:4778:bindinginformation:1:0"
  xmlns:dcs="urn:tb15:dcs:1:0" xmlns:enc="http://www.w3.org/2001/04/xmlenc#Element"
  xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0">
  <gml:boundedBy>
    <gml:Null>missing</gml:Null>
  </gml:boundedBy>
  <wfs:member>
    <dcs:dcs_object xml:id="feature_1" dcs:encoding_type="stanag4778">
      <mb:BindingInformation>
        <mb:MetadataBindingContainer>
          <mb:MetadataBinding>
            <mb:Metadata>
              <EncryptedData xmlns="http://www.w3.org/2001/04/xmlenc#"
                Type="http://www.w3.org/2001/04/xmlenc#Element">
                <EncryptionMethod Algorithm=
"http://www.w3.org/2001/04/xmlenc#tripledes-cbc"/>
                <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
                  <EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#">
                    <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-
1_5"/>
                    <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
                      <KeyName>138af896-3487-32d6-8171-c4a51c416424</KeyName>
                    </KeyInfo>
                    <CipherData>
                      <CipherValue>k1fLci...Z6Axw==</CipherValue>
                    </CipherData>
                  </EncryptedKey>
                </KeyInfo>
                <CipherData>
                  <CipherValue>p7vlvSG...9Nv+Mg==</CipherValue>
                </CipherData>
              </EncryptedData>
            </mb:Metadata>
            <mb:Data>
```

```
              <enc:EncryptedData>
                <enc:EncryptionMethod Algorithm=
"http://www.w3.org/2001/04/xmlenc#aes128"/>
                <enc:EncryptionKeyInfo>
                  <enc:EncryptedKey>
                    <enc:SignatureMethod
                      Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
                    <enc:KeyInfo>
                      <enc:KeyName>Jane Bond 128</enc:KeyName>
                    </enc:KeyInfo>
                    <enc:CipherData>
                      <enc:CipherValue>NpzsfRXr2/...YwlnSr9xw==</enc:CipherValue>
                    </enc:CipherData>
                  </enc:EncryptedKey>
                </enc:EncryptionKeyInfo>
                <CipherData>
                  <CipherValue>++//jkiBKMi3Nvh6BCCSL...PbaLW/dtgAmraeQ==</CipherValue>
                </CipherData>
              </enc:EncryptedData>
            </mb:Data>
          </mb:MetadataBinding>
        </mb:MetadataBindingContainer>
      </mb:BindingInformation>
    </dcs:dcs_object>
  </wfs:member>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"/>
      <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
      <ds:Reference Id="id" URI="#feature_1">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <ds:DigestValue>WApjIBfE4PBiaEeQvgQRgLeN4CQ=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>

<ds:SignatureValue>di8sRClAsEWh9YR9sict4bHCCFlSPGVy5g/mhBzcS/oUqt4ix3qx1AFUIALoBCLQ
    0EGy60IKAKBQ7m47mIhOEjWwrfiY7fIODwue9Ze90zsJvvlUMv8x2rAng4bZodhU
    4CztFrV9iAR8yNnD9hnOfSnweG26ow9Eq74PqmEDoWIBnTGU7/3QmoglinCUvCsQ
    wGagndTyPKSM2ABvEnMMlOwDYNyXEgDEbtN7eLw17B7unlyQc3CY9lUCnJu9Xg2y
    E6Q5BWjTdHCiS24aFlB6OqF0zc2rqnjQkgVonWdtIujgGNctO+c2/gl36V0vVidx
    P7uVarSDtNd3XVVZLZa/9g==</ds:SignatureValue>
    <ds:KeyInfo>
      <ds:KeyName>Dr. No</ds:KeyName>
      <ds:X509Data>
```

```
<ds:X509Certificate>MIIDuTCCAqGgAwIBAgIEYpLJdjANBgkqhkiG9w0BAQsFADCBjDELMAkGA1UEBhMC
        REUxEDAOBgNVBAgTB0JhdmFyaWExDzANBgNVBAcTBk11bmljaDEfMB0GA1UEChMW
        U2VjdXJlIERpbWVuc2lvbnMgR21iSDEfMB0GA1UECxMWU2VjdXJlIERpbWVuc2lv
        bnMgR21iSDEYMBYGA1UEAxMPQW5kcmVhcyBNYXRoZXVzMB4XDTE1MTAyNTE0NDEw
        MVoXDTE2MDEyMzE0NDEwMVowgYwxCzAJBgNVBAYTAkRFMRAwDgYDVQQIEwdCYXZh
        cmlhMQ8wDQYDVQQHEwZNdW5pY2gxHzAdBgNVBAoTFlNlY3VyZSBEaW1lbnNpb25z
        IEdtYkgxHzAdBgNVBAsTFlNlY3VyZSBEaW1lbnNpb25zIEdtYkgxGDAWBgNVBAMT
        D0FuZHJlYXMgTWF0aGV1czCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
        AJBxrjwhMmOGnSKT4DLsOx+R+c4dN3gA74/03NdsxUdy2r6QB65AvF8Rm3YF5pJy
        Hzdrlf43IObjOHK2yRn6p0tXpc5yYwBGd3tZMGTkyj4qhqqy/ug4LxYy4HYfCXE/
        ec9UOTCDu7vfkbvmEfg8V0M2DfT6t5XnvFZmkUkSAi4L4vQ9PJthsFLyJXq2nNlh
        tOMQeBWxcOzbog6EBAB7qaUyumlrrIojksHd9Tb4Om/BIp+JxcocRjGmSq7XoKZ1
        GuXmWXSnrc877AnET/+Kbea4zqH+Oo44zP2G0XdCCMiKtL7nxqIAfwucp3SEGtqH
        XGNv61RGsqihQbtlbhRkprcCAwEAAaMhMB8wHQYDVR0OBBYEFIVLBZDvNUo/OX9F
        MKRLz7OFaUXXMA0GCSqGSIb3DQEBCwUAA4IBAQCA7FkGI0EOkJPr4yjCT8HxJvAd
        lzNW539tl/SVYe4ducBm4J523G6POKvz6kVHbS30J2HiNd2FoQL9s2DMPN2ag9Q3
        myzI8E9x8dowNKhaupmTJI/Edneqnp7pr/8/o612qBXTf00T4j8QP9mZxUreqC+x
        TCV9GCO0XuIVpBM6sGbEiFfjg0xLs3HO7kBHla78WAb8EyZGv9aoHCsqoIE+A/L9
        e++xrY09TN/wjJKrv665iRF3XG+WHj0lrUvzlPZzNHbLykqSo48DhDc/JmaadiqZ

cNFF8NBHOLzicsSo+GpeEnSJBKnCYwxStWJ+dFWoHQxwyHrkn+Om+EiQ6/2w</ds:X509Certificate>
        <ds:X509SubjectName>CN=Andreas Matheus,OU=Secure Dimensions GmbH,O=Secure
Dimensions GmbH,L=Munich,ST=Bavaria,C=DE</ds:X509SubjectName>
      </ds:X509Data>
    </ds:KeyInfo>
  </ds:Signature>
</wfs:FeatureCollection>
```

Demo

Secure Dimensions GeoPEP setup for the Helyx Secure Information Systems WFS3

The Secure Dimensions GeoPEP is an Apache Web Server module. For the demonstration of this flow - as well as the others - the Apache Web Server is configured as a reverse proxy that loads the GeoPEP module. The following Apache 2.4 configuration snippet illustrates that:

```
# Helyx WFS
RewriteRule ^/features$ /features/ [qsappend,L]
RewriteRule ^$ /features/ [qsappend,L]
ProxyPass /features http://wfs-helyx.westeurope.azurecontainer.io:5601/features
ProxyPassReverse /features http://wfs-helyx.westeurope.azurecontainer.io:5601/features
<Location /features/collections/tripledes/landsat8__B3_index/items>
    AllowMethods GET POST OPTIONS

    <LimitExcept OPTIONS>
                AuthType Basic
                AuthName "OAuth Bearer"
                Require valid-user
    </LimitExcept>

    PerlAuthenHandler SD::OpenIDBearerHandler
    PerlOptions +ParseHeaders +SetupEnv +GlobalRequest
    PerlSetVar ClientId fa00ef4f-143d-da53-c814-ac1866d592c5@ogc.secure-dimensions.com
    PerlSetVar ClientSecret
b0dec4f85327c9af80f9669f0c8f966ebc3ffaa0f5c56c244bac76802d6ba9ef
    PerlSetVar ValidateURL https://ogc.secure-dimensions.com/oauth/tokeninfo
    PerlSetVar UserinfoURL https://ogc.secure-dimensions.com/oauth/userinfo

    GeoPEP.API      on
    GeoPDP.Host     116.202.106.215
    GeoPDP.Port     80
    GeoPDP.Path     /geopdp/domains/JeuDTcMdEemN8MEvpJG-Sw/pdp
    GeoPDP.Scheme   http

    ProxyPass http://wfs-
helyx.westeurope.azurecontainer.io:5601/features/collections/tripledes/landsat8__B3_in
dex/items
    ProxyPassReverse http://wfs-
helyx.westeurope.azurecontainer.io:5601/features/collections/tripledes/landsat8__B3_in
dex/items

</Location>
```

The PerlAuthenHandler `SD::OpenIDBearerHandler` is an authentication handler that acts as a RFC 6750 (The OAuth 2.0 Authorization Framework: Bearer Token Usage) compliant OAuth2 Resource Server. It inspects the incoming HTTP header, query parameters for a GET and payload for a POST request to find the bearer access token. In case no access token is found, the response is a HTTP status of 401 with message "Unauthorized". In case an access token is found but it is invalid, the response is 401 with "Access Token invalid". For a valid access token, the handler requests the user claims from the Authorization Server via the `UserinfoURL`. The user claims are key-value-pairs that get associated with the intercepted request as Apache 2 Environment variables. As such, they become available to other Apache modules, such as the GeoPEP.

The GeoPEP interacts with the GeoPDP as configured by the `GeoPDP.*` directives. The `JeuDTcMdEemN8MEvpJG-Sw` domain holds the GeoXACML policies associated with the Helyx WFS3. The

directive `GeoPEP.API on` instruments the GeoPEP to act as a WFS3 API interceptor. (Other options are WMS, WFS, WCS, etc. which would instruct the GeoPEP to interpret query string parameters accordingly).

The GeoPEP

The GeoPEP - as an Apache Web Server module - gets executed by the Apache Web Server as an authorization handler. It has access to the Apache request including all HTTP headers plus any Apache 2 Environment Variables. From this Apache2 domain specific set of information, a GeoXACML specific request is created in the XACML3 structure. The default encoding leverages the JSON Request / Response profile for XACML 3. The following is a JSON encoded Authorization Decision Request sent to the GeoPDP:


```
{
  "Request": {
    "ReturnPolicyIdList": false,
    "CombinedDecision": false,
    "Category": [
      {
        "CategoryId": "urn:oasis:names:tc:xacml:1.0:subject-category:access-subject",
        "Attribute": [
          {
            "IncludeInResult": false,
            "AttributeId": "urn:oasis:names:tc:xacml:1.0:subject:subject-id",
            "DataType": "http://www.w3.org/2001/XMLSchema#string",
            "Value": ["af4f2285-979d-389a-892a-90aa9d776476"]
          }
        ]
      },
      {
        "CategoryId": "urn:oasis:names:tc:xacml:3.0:attribute-category:resource",
        "Attribute": [
          {
            "IncludeInResult": false,
            "AttributeId": "urn:sd:path",
            "DataType": "http://www.w3.org/2001/XMLSchema#string",
            "Value": ["/features/collections/tripledes/landsat8__B3_index/items"]
          },
          {
            "IncludeInResult": false,
            "AttributeId": "urn:sd:hostname",
            "DataType": "http://www.w3.org/2001/XMLSchema#string",
            "Value": ["ogc.secure-dimensions.com"]
          }
        ]
      },
      {
        "CategoryId": "urn:oasis:names:tc:xacml:3.0:attribute-category:action",
        "Attribute": [
          {
```

```
            "IncludeInResult": false,
            "AttributeId": "urn:sd:method",
            "DataType": "http://www.w3.org/2001/XMLSchema#string",
            "Value": ["GET"]
          }
        ]
      },
      {
        "CategoryId": "urn:oasis:names:tc:xacml:3.0:attribute-category:environment",
        "Attribute": [
          {
            "IncludeInResult": false,
            "AttributeId": "urn:sd:method",
            "DataType": "http://www.w3.org/2001/XMLSchema#string",
            "Value": ["GET"]
          },
          {
            "IncludeInResult": false,
            "AttributeId": "urn:sd:query_string",
            "DataType": "http://www.w3.org/2001/XMLSchema#string",
            "Value": ["access_token=42333cafd91f7fd22f24b6a003b2a66202619cc3"]
          },
          {
            "IncludeInResult": false,
            "AttributeId": "urn:oasis:names:tc:xacml:1.0:subject:subject-id",
            "DataType": "http://www.w3.org/2001/XMLSchema#string",
            "Value": ["af4f2285-979d-389a-892a-90aa9d776476"]
          },
          {
            "IncludeInResult": false,
            "AttributeId": "urn:sd:datetime",
            "DataType": "http://www.w3.org/2001/XMLSchema#dateTime",
            "Value": ["2019-08-20T12:20:18Z"]
          },
          {
            "IncludeInResult": false,
            "AttributeId": "urn:sd:date",
            "DataType": "http://www.w3.org/2001/XMLSchema#date",
            "Value": ["2019-08-20"]
          },
          {
            "IncludeInResult": false,
            "AttributeId": "urn:sd:time",
            "DataType": "http://www.w3.org/2001/XMLSchema#time",
            "Value": ["12:20:18Z"]
          },
          {
            "IncludeInResult": false,
            "AttributeId": "urn:sd:host",
            "DataType": "http://www.w3.org/2001/XMLSchema#string",
            "Value": ["ogc.secure-dimensions.com"]
```

```
          },
          {
            "IncludeInResult": false,
            "AttributeId": "urn:sd:user-agent",
            "DataType": "http://www.w3.org/2001/XMLSchema#string",
            "Value": ["Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:67.0)
Gecko/20100101 Firefox/67.0"]
          },
          {
            "IncludeInResult": false,
            "AttributeId": "urn:sd:accept",
            "DataType": "http://www.w3.org/2001/XMLSchema#string",
            "Value": [
              "text/html",
              "application/xhtml+xml",
              "application/xml;q=0.9",
              "*/*;q=0.8"
            ]
          },
          {
            "IncludeInResult": false,
            "AttributeId": "urn:sd:accept-language",
            "DataType": "http://www.w3.org/2001/XMLSchema#string",
            "Value": [
              "de",
              "en;q=0.7",
              "en-US;q=0.3"
            ]
          },
          {
            "IncludeInResult": false,
            "AttributeId": "urn:sd:accept-encoding",
            "DataType": "http://www.w3.org/2001/XMLSchema#string",
            "Value": [
              "gzip",
              " deflate",
              " br"
            ]
          },
          {
            "IncludeInResult": false,
            "AttributeId": "urn:sd:dnt",
            "DataType": "http://www.w3.org/2001/XMLSchema#string",
            "Value": ["1"]
          },
          {
            "IncludeInResult": false,
            "AttributeId": "urn:sd:connection",
            "DataType": "http://www.w3.org/2001/XMLSchema#string",
            "Value": ["keep-alive"]
          },
```

```
          {
            "IncludeInResult": false,
            "AttributeId": "urn:sd:cookie",
            "DataType": "http://www.w3.org/2001/XMLSchema#string",
            "Value": ["language=en; SimpleSAML=7f736e5c0eee4d3c03c9d87691b346e4;
AuthToken=_9e0d349ac383969f4de52d12b40aff68b006364dbc"]
          },
          {
            "IncludeInResult": false,
            "AttributeId": "urn:sd:upgrade-insecure-requests",
            "DataType": "http://www.w3.org/2001/XMLSchema#string",
            "Value": ["1"]
          },
          {
            "IncludeInResult": false,
            "AttributeId": "urn:sd:unique_id",
            "DataType": "http://www.w3.org/2001/XMLSchema#string",
            "Value": ["XVvlgmM-a0tJIBus4NsxxwAAAAY"]
          },
          {
            "IncludeInResult": false,
            "AttributeId": "urn:sd:script_url",
            "DataType": "http://www.w3.org/2001/XMLSchema#string",
            "Value": ["/features/collections/tripledes/landsat8__B3_index/items"]
          },
          {
            "IncludeInResult": false,
            "AttributeId": "urn:sd:script_uri",
            "DataType": "http://www.w3.org/2001/XMLSchema#string",
            "Value": ["https://ogc.secure-
dimensions.com/features/collections/tripledes/landsat8__B3_index/items"]
          },
          {
            "IncludeInResult": false,
            "AttributeId": "urn:sd:subject-id",
            "DataType": "http://www.w3.org/2001/XMLSchema#string",
            "Value": ["af4f2285-979d-389a-892a-90aa9d776476"]
          },
          {
            "IncludeInResult": false,
            "AttributeId": "urn:sd:subject-clearance",
            "DataType": "http://www.w3.org/2001/XMLSchema#string",
            "Value": ["unclassified"]
          },
          {
            "IncludeInResult": false,
            "AttributeId": "urn:sd:public-key",
            "DataType": "http://www.w3.org/2001/XMLSchema#string",
            "Value": ["-----BEGIN PUBLIC KEY-----\\
\\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwfA+788fVX5ls2ZzdcbB\\\\nAK5CGgXSdjDDce
AHDkhxOQqNrwP0mH2obMqLBji8dgo1Fg++TEIDf4kvRBGaPUA5\\\\nSBYNwisBTjY1/4YzFJCz2bvWbH2hMjW
```

```
cmlCRC2ZMSHxsdK/KnwGOkRhOOfXdvs6H\\\\nRbwr0lisBdZHVWmisAWwHG4i0BFu1lchS0Px1YLfej5C89SD
vMcz1POn6SQxeL07\\\\nUkbsY9OAls/j70NwaGkVuW9C+2SAMxa1wdAHsA4oRLxPzA1jiOm2MJ5GQbivpijX\
\\\nmMJPMakWF/WDI6bJW85vgIP8yvdNScZBPfgFQPSC1xcEFwE446zx4kJ8pShi19TO\\\\nQQIDAQAB\\\\n
-----END PUBLIC KEY-----"]
          },
          {
            "IncludeInResult": false,
            "AttributeId": "urn:sd:simplesamlphp_config_dir",
            "DataType": "http://www.w3.org/2001/XMLSchema#string",
            "Value": ["/opt/saml2-authorization-
server/vendor/simplesamlphp/simplesamlphp/config"]
          },
          {
            "IncludeInResult": false,
            "AttributeId": "urn:sd:https",
            "DataType": "http://www.w3.org/2001/XMLSchema#string",
            "Value": ["on"]
          },
          {
            "IncludeInResult": false,
            "AttributeId": "urn:sd:ssl_tls_sni",
            "DataType": "http://www.w3.org/2001/XMLSchema#string",
            "Value": ["ogc.secure-dimensions.com"]
          },
          {
            "IncludeInResult": false,
            "AttributeId": "urn:sd:access_token",
            "DataType": "http://www.w3.org/2001/XMLSchema#string",
            "Value": ["42333cafd91f7fd22f24b6a003b2a66202619cc3"]
          }
        ]
      }
    ]
  }
}
```


Examining the ADR a bit further unveils that the different XACML 3 categories are leveraged to capture information representing the Apache 2 request in an XACML 3 compliant way. (In XACML 3 terminology, the Context Handler included in the GeoPEP generated the Apache2 into XACML 3 information transformation).

Based on the Authorization Decision (AD) received from the GeoPDP, the GeoPEP processes the Apache 2 request based on XACML 3 Obligations. The GeoPEP understands the following Obligations of which the `redact obligation` is not instrumented in this testbed:

- `urn:SD:Obligation:Redact:Image` enables the GeoPEP to modify images before send to the caller (typically the client application)
- `urn:SD:Obligation:Request:KVP` enables the GeoPEP to modify the HTTP GET query string parameters

- `urn:SD:Obligation:Request:XSLT` enables the GeoPEP to modify a HTTP POST request encoded in XML (WFS, WCS, etc.)
- `urn:SD:Obligation:Response:XSLT` enables the GeoPEP to modify a response encoded in XML (GML, STANAG, etc.)
- `urn:SD:Obligation:Response:DSIG` enables the GeoPEP to apply a Digital Signature to an XML encoded response
- `urn:SD:Obligation:Response:ENC` enables the GeoPEP to apply XML Encryption to an XML encoded response

The following is a policy snippet in ALFA notation for the `urn:SD:Obligation:Response:XSLT` obligation which is used to filter the response in this demo.

```
obligation responseXSLT {
    document =
"PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz4KPCEtLSAKICBUaGlzIFhTTFQgZmlsdGVyc
yBhbnkgV0ZTIHJlc3BvbnNlIC0gYWthIGEgRmVhdHVyZUNvbGxlY3Rpb24gLSBpbmNsdWRpbmcgU1RBTkFHIDQ
3NzggZmVhdHVyZXMgYmFzZWQgb24gdGhlIGNsYXNzaWZpY2F0aW9uIGxldmVsIGRlZmluZWQgaW4gdGhlIFNUQ
U5BRyBNZXRhZGF0YQogIGFuZCB0aGUgcGFyYW1ldGVyKHMpIGZvciBmZWF0dXJlIGNsYXNzaWZpY2F0aW9uOiB
VTkNMQVNTUZJRUQsIENMQVNTUZJRUQsIFNFQ1JFVCBhbmQgVE9QX1NFQ1JFVAogIEluIGNhc2UgdGhhdCB0a
GUgdXNlciBpcyBub3QgZW50aXRsZWQgdG8gc2VlIGFueSBvZiB0aGUgU1RBTkFHIGZlYXR1cmVzLCBhbiBlbXB
0eSBGZWF0dXJlQ29sbGVjdGlvbiBpcyBjcmVhdGVkLgotLT4KPHhzbDp0cmFuc2Zvcm0gdmVyc2lvbj0iMS4wI
iB4bWxuczp4c2w9Imh0dHA6Ly93d3cudzMub3JnLzE5OTkvWFNML1RyYW5zZm9ybSIgeG1sbnM6d2ZzPSJodHR
wOi8vd3d3Lm9wZW5naXMubmV0L3dmcy8zLjAiIHhtbG5zOmdtbD0iaHR0cDovL3d3dy5vcGVuZ2lzLm5ldC9nb
WwiCiAgeG1sbnM6bWI9InVybjpuYXRvOnN0YW5hZzo0Nzc4OmJpbmRpbmdpbmZvcm1hdGlvbjoxOjAiIHhtbG5
zOmRjcz0idXJuOnRiMTU6ZGNzOjE6MCIgeG1sbnM6ZW5jPSJodHRwOi8vd3d3LnczLm9yZy8yMDAxLzA0L3htb
GVuYyNFbGVtZW50IiB4bWxuczpzbGFiPSJ1cm46bmF0bzpzdGFuYWc6NDc3NDpjb25maWRlbnRpYWxpdHltZXR
hZGF0YWxhYmVsOjE6MCIgeG1sbnM6ZXh0PSJodHRwOi8vZXhzbHQub3JnL2NvbW1vbiIgZXh0ZW5zaW9uLWVsZ
W1lbnQtcHJlZml4XM9ImV4dCI+CiAgPHhzbDpvdXRwdXQgbWV0aG9kPSJ4bWwiIGluZGVudD0ieWVzIi8+CiA
gCiAgPHhzbDpzdHJpc1zcGFjZSBlbGVtZW50cz0iKiIgLz4KICAKICA8eHNsOnBhcmFtIG5hbWU9InVzZXJDb
GVhcmFuY2UiLz4KICAKICA8eHNsOnRlbXBsYXRlIG5hbWU9IkNPUFkiPgogICA8eHNsOnBhcmFtIG3B5LW9mIHNlbGV
jdD0iLiIvPgogIDwveHNsOnRlbXBsYXRlPgogICA8eHNsOnRlbXBsYXRlIG1hdGNoPSJub2RlKCkiPgogICAgP
HhzbDpjaG9vc2U+CiAgICAgIDx4c2w6d2hlbiB0ZXN0PSJzZWxmOjoqW2xvY2FsLW5hbWUoKT0nbWVtYmVyJ10
gYW5kIHNlbGY6OiovZGNzOmRjc19vYmplY3QvbWI6QmluZGluZ0luZm9ybWF0aW9uL21iOk1ldGFkYXRhQmluZ
GluZ0NvbnRhaW5lci9tYjpNZXRhZGF0YUJpbmRpbmcvbWI6TWV0YWRhdGEvc2xhYjpvcmlnaW5hdG9yQ29uZml
kZW50aWFsaXR5TGFiZWwvc2xhYjpDb25maWRlbnRpYWxpdHlJbmZvcm1hdGlvbi9zbGFiOkNsYXNzaWZpY2F0a
W9uL3RleHQoKSA9ICdVTkNMQVNTUZJRUQnIGFuZCAoJHVzZXJDbGVhcmFuY2UgPSAndW5jbGFzc2lmaWVkJyB
vciAkdXNlckNsZWFyYW5jZSA9ICdjbGFzc2lmaWVkJyBvciAkdXNlckNsZWFyYW5jZSA9ICdzZWNyZXQnIG9yI
CR1c2VyQ2xlYXJhbmNlID0gJ3RvcF9zZWNyZXQnKSI+CiAgICAgICAgPHhzbC10ZW1wbGF0ZSBuYW1
lPSJDT1BZIi8+ICAgICAgICAKICAKPC94c2w6d2hlbj4KICAgICAgPC94c2w6Y2hvb3NlPgogICA8L3hzbDp0
ipbbG9jYWwtbmFtZSgpPSdtZW1iZXInXSBhbmQgc2VsZjo6Ki9kY3M6ZGNzX29iamVjdC9tYjpCaW5kaW5nSW5
mb3JtYXRpb24vbWI6TWV0YWRhdGFCaW5kaW5nUnVudGFpbmVyL21iOk1ldGFkYXRhQmluZGluZy9tYjpNZXRhZ
GF0YS9zbGFiOm9yaWdpbmF0b3JDb25maWRlbnRpYWxpdHlMYWJlbC9zbGFiOkNvbmZpZGVudGlhbGl0eUluZm9
ybWF0aW9uL3NsYWI6Q2xhc3NpZmljYXRpb24vdGV4dCgpID0gJ0NMQVNTUZJRUQnIGFuZCAoJHVzZXJDbGVhc
mFuY2UgPSAnY2xhc3NpZmllZCcgb3IgJHVzZXJDbGVhcmFuY2UgPSAnc2VjcmV0JyBvciAkdXNlckNsZWFyYW5
jZSA9ICd0b3Bfc2VjcmV0JykiPgogICAgICAgIDx4c2w6Y2FsbC10ZW1wbGF0ZSBuYW1lPSJDT1BZIi8+CiAgI
CAgIDwveHNsOndoZW4+CiAgICAgICAgPHhzbDp4c2w6d2hlbiB0ZXN0PSJzZWxmOjoqW2xvY2FsLW5hbWUoKT0nbWVtYmV
yJ10gYW5kIHNlbGY6OiovZGNzOmRjc19vYmplY3QvbWI6QmluZGluZ0luZm9ybWF0aW9uL21iOk1ldGFkYXRhQ
mluZGluZ0NvbnRhaW5lci9tYjpNZXRhZGF0YUJpbmRpbmcvbWI6TWV0YWRhdGEvc2xhYjpvcmlnaW5hdG9yQ29
uZmlkZW50aWFsaXR5TGFiZWwvc2xhYjpDb25maWRlbnRpYWxpdHlJbmZvcm1hdGlvbi9zbGFiOkNsYXNzaWZpY

```

```
2F0aW9uL3RleHQoKSA9ICdTRUNSRVQnIGFuZCAoJHVzZXJDbGVhcmFuY2UgPSAnc2VjcmV0JyBvciAkdXNlckN
sZWFyYW5jZSA9ICd0b3Bfc2VjcmV0JykiPgogICAgICAgIDx4c2w6Y2FsbC10ZW1wbGF0ZSBuYW1lPSJDT1BZI
i8+CiAgICAgICAgDwveHNsOndoZW4+CiAgICAgICAgIDx4c2w6d2hlbiB0ZXN0PSJzZWxmOjoqW2xvY2FsLW5hbWUoKT0
nbWVtYmVyJ10gYW5kIHNlbGY6OiovZGNzOmRjc19vYmplY3QvbWI6QmluZGluZ0luZm9ybWF0aW9uL21iOk1ld
GFkYXRhQmluZGluZ0NvbnRhaW5lci9tYjpNZXRhZGF0YUJpbmRpbmcvbWI6TWV0YWRhdGEvc2xhYjpvcmlnaW5
hdG9yQ29uZmlkZW50aWFsaXR5TGFiZWwvc2xhYjpDb25maWRlbnRpYWxpdHlJbmZvcm1hdGlvbi9zbGFiOkNsY
XNzaWZpY2F0aW9uL3RleHQoKSA9ICdUT1BfU0VDUkVUJyBhbmQgKCR1c2VyQ2xlYXJhbmNlID0gJ3RvcF9zZWN
yZXQnKSI+CiAgICAgICAgPHhzbDpjYWxsLXRlbXBsYXRlIG5hbWU9IkNPUFkiLz4KICAgICAgICAgPC94c2w6d2hlb
j4KICAgICAgICAgDwveHNsOmNob29zZT4gICAgICAgICA8eHNsOmFwcGx5LXRlbXBsYXRlcyBzZWxlY3Q9Im5vZGUoKSI
vPgogICAgICAgIDwveHNsOnRlbXBsYXRlPgogICAgICAgPHhzbDp0ZW1wbGF0ZSBtYXRjaD0iQCp8LyI+CiAgICAgICA8d2ZzOkZlY
XR1cmVDb2xsZWN0aW9uPgogICAgICAgICA8eHNsOmNvcHktb2Ygc2VsZWN0PSJAKiIgLz4KICAgICAgICAgPGdtbDpib3V
uZGVkQnk+CiAgICAgICAgICAgPGdtbDpOdWxsPm1pc3Npbmc8L2dtbDpOdWxsPgogICAgICAgICAgPC9nbWw6Ym91bmRlZ
nk+CiAgICAgICAgICAgPDx4c2w6YXBwbHktdGVtcGxhdGVzIHNlbGVjdD0iQCp8bm9kZSgpIi8+CiAgICAgICA8L3dmczpGZWF
0dXJlQ29sbGVjdGlvbj4gICAgICAgICA8eHNsOnRlbXBsYXRlPgogICAgICAgICAgIDwvc3hzbDp0cmFuc2Zvcm0+"
    parameter = "userClearance=unclassified"
}
```

The `document` contains the base64 encoded XSLT and the `parameter` contains the XSLT parameter.

The following is a policy snippet in ALFA notation for the `urn:SD:Obligation:Response:DSIG` obligation which is used to apply a Digital Signature to the response in this demo.

```
obligation responseDSIG {
    private_key_file = "/etc/pki/tls/private/testbed15.pem"
    private_key_name = "Dr. No"
    certificate_file = "/etc/pki/tls/certs/testbed15.crt"
    id_element_value = "#feature_1"
    id_element_qname = "id"
}
```

For verification of the digital signature, the `testbed15.crt` certificate is available online: https://ogc.secure-dimensions.com/testbed15.crt

The following is a policy snippet in ALFA notation for the `urn:SD:Obligation:Response:ENC` obligation which is used to apply XML Encryption to the response in this demo.

```
obligation responseENC {
    public_key_value = subject_public_key
    public_key_name = subject_id
    xpath = "//*[local-name() = 'originatorConfidentialityLabel']"
}
```

The ALFA notation `public_key_value = subject_public_key` instruments the GeoPDP to insert the value of the designated attribute `subject_public_key` from the ADR to the obligation parameter `public_key_name`. The same applies to the ALFA notation `public_key_name = subject_id `. The `xpath` value is used by the GeoPEP to find the XML elements that are to be encrypted. For this flow, it is the XML element `slab:originatorConfidentialityLabel`.

The Helyx WFS3 dedicated GeoPDP

As described in the GeoPDP github pages, a domain was created for service authorization decisions for the Helyx WFS3. The necessary steps are:

- send a HTTP POST request to the PDP's domain management API endpoint: https://ogc.secure-dimensions.com/geopdp/domains

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<domainProperties xmlns="http://authzforce.github.io/rest-api-model/xmlns/authz/5"
 externalId="Helyx">
 <description>TB15 Helyx WFS PDP</description>
</domainProperties>
```

The response contains the identifier for the created domain `JeuDTcMdEemN8MEvpJG-Sw`:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<ns3:linkxmlns="http://authzforce.github.io/pap-dao-flat-file/xmlns/properties/3.6
"xmlns:ns2="http://authzforce.github.io/rest-api-model/xmlns/authz/5"xmlns:ns3=
"http://www.w3.org/2005/Atom"xmlns:ns4="http://authzforce.github.io/core/xmlns/pdp/6.0
"xmlns:ns5="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"rel="item"href=
"JeuDTcMdEemN8MEvpJG-Sw"title="JeuDTcMdEemN8MEvpJG-Sw"/>
```

- send a HTTP POST request to the PDP's policy management API endpoint: https://ogc.secure-dimensions.com/geopdp/domains/JeuDTcMdEemN8MEvpJG-Sw/pap/policies

```
<?xml version="1.0" encoding="UTF-8"?>
 <!--This file was generated by the ALFA Plugin for Eclipse from Axiomatics AB
(http://www.axiomatics.com).
 Any modification to this file will be lost upon recompilation of the source ALFA
file-->
<xacml3:PolicySet xmlns:xacml3="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
    PolicySetId="urn:secd:policyset:tb15:helyx"
    PolicyCombiningAlgId="urn:oasis:names:tc:xacml:3.0:policy-combining-
algorithm:deny-overrides"
    Version="1.0">
    <xacml3:Description />
    <xacml3:PolicySetDefaults>
        <xacml3:XPathVersion>http://www.w3.org/TR/1999/REC-xpath-
19991116</xacml3:XPathVersion>
    </xacml3:PolicySetDefaults>
    <xacml3:Target />
    <xacml3:Policy xmlns:xacml3="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
       PolicyId="urn:secd:policyset:tb15:helyx:features"
        RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-
algorithm:permit-overrides"
        Version="1.0">
```

```
        <xacml3:Description />
        <xacml3:PolicyDefaults>
            <xacml3:XPathVersion>http://www.w3.org/TR/1999/REC-xpath-
19991116</xacml3:XPathVersion>
        </xacml3:PolicyDefaults>
        <xacml3:Target>
            <xacml3:AnyOf>
                <xacml3:AllOf>
                    <xacml3:Match MatchId=
"urn:oasis:names:tc:xacml:1.0:function:string-equal">
                        <xacml3:AttributeValue
                            DataType="http://www.w3.org/2001/XMLSchema#string"
>/features/</xacml3:AttributeValue>
                        <xacml3:AttributeDesignator
                            AttributeId="urn:sd:path"
                            DataType="http://www.w3.org/2001/XMLSchema#string"
                            Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:resource"
                            MustBePresent="false"
                        />
                    </xacml3:Match>
                </xacml3:AllOf>
            </xacml3:AnyOf>
        </xacml3:Target>
        <xacml3:Rule
                Effect="Permit"
                RuleId=
"http://axiomatics.com/alfa/identifier/ogc.tb15helyx.features.permitAll">
            <xacml3:Description />
            <xacml3:Target />
        </xacml3:Rule>
    </xacml3:Policy>
    <xacml3:Policy xmlns:xacml3="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
       PolicyId="urn:secd:policyset:tb15:helyx:collections"
        RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-
algorithm:permit-overrides"
        Version="1.0">
        <xacml3:Description />
        <xacml3:PolicyDefaults>
            <xacml3:XPathVersion>http://www.w3.org/TR/1999/REC-xpath-
19991116</xacml3:XPathVersion>
        </xacml3:PolicyDefaults>
        <xacml3:Target>
            <xacml3:AnyOf>
                <xacml3:AllOf>
                    <xacml3:Match MatchId=
"urn:oasis:names:tc:xacml:1.0:function:string-equal">
                        <xacml3:AttributeValue
                            DataType="http://www.w3.org/2001/XMLSchema#string"
>/features/collections</xacml3:AttributeValue>
                        <xacml3:AttributeDesignator
```

```
                            AttributeId="urn:sd:path"
                            DataType="http://www.w3.org/2001/XMLSchema#string"
                            Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:resource"
                            MustBePresent="false"
                        />
                    </xacml3:Match>
                </xacml3:AllOf>
            </xacml3:AnyOf>
        </xacml3:Target>
        <xacml3:Rule
                Effect="Permit"
                RuleId=
"http://axiomatics.com/alfa/identifier/ogc.tb15helyx.collections.permitAll">
            <xacml3:Description />
            <xacml3:Target />
        </xacml3:Rule>
    </xacml3:Policy>
    <xacml3:Policy xmlns:xacml3="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
       PolicyId="urn:secd:policyset:tb15:helyx:api"
        RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-
algorithm:permit-overrides"
        Version="1.0">
        <xacml3:Description />
        <xacml3:PolicyDefaults>
            <xacml3:XPathVersion>http://www.w3.org/TR/1999/REC-xpath-
19991116</xacml3:XPathVersion>
        </xacml3:PolicyDefaults>
        <xacml3:Target>
            <xacml3:AnyOf>
                <xacml3:AllOf>
                    <xacml3:Match MatchId=
"urn:oasis:names:tc:xacml:1.0:function:string-equal">
                        <xacml3:AttributeValue
                            DataType="http://www.w3.org/2001/XMLSchema#string"
>/features/api</xacml3:AttributeValue>
                        <xacml3:AttributeDesignator
                            AttributeId="urn:sd:path"
                            DataType="http://www.w3.org/2001/XMLSchema#string"
                            Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:resource"
                            MustBePresent="false"
                        />
                    </xacml3:Match>
                </xacml3:AllOf>
            </xacml3:AnyOf>
        </xacml3:Target>
        <xacml3:Rule
                Effect="Permit"
                RuleId=
"http://axiomatics.com/alfa/identifier/ogc.tb15helyx.api.permitAll">
```

```
            <xacml3:Description />
            <xacml3:Target />
        </xacml3:Rule>
    </xacml3:Policy>
    <xacml3:PolicySet xmlns:xacml3="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
        PolicySetId="urn:secd:policyset:tb15:helyx:landsat8__B3"
        PolicyCombiningAlgId="urn:oasis:names:tc:xacml:3.0:policy-combining-
algorithm:deny-overrides"
        Version="1.0">
        <xacml3:Description />
        <xacml3:PolicySetDefaults>
            <xacml3:XPathVersion>http://www.w3.org/TR/1999/REC-xpath-
19991116</xacml3:XPathVersion>
        </xacml3:PolicySetDefaults>
        <xacml3:Target>
            <xacml3:AnyOf>
                <xacml3:AllOf>
                    <xacml3:Match MatchId=
"urn:oasis:names:tc:xacml:1.0:function:string-equal">
                        <xacml3:AttributeValue
                            DataType="http://www.w3.org/2001/XMLSchema#string"
>/features/collections/aes/landsat8__B3_index/items</xacml3:AttributeValue>
                        <xacml3:AttributeDesignator
                            AttributeId="urn:sd:path"
                            DataType="http://www.w3.org/2001/XMLSchema#string"
                            Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:resource"
                            MustBePresent="false"
                        />
                    </xacml3:Match>
                </xacml3:AllOf>
                <xacml3:AllOf>
                    <xacml3:Match MatchId=
"urn:oasis:names:tc:xacml:1.0:function:string-equal">
                        <xacml3:AttributeValue
                            DataType="http://www.w3.org/2001/XMLSchema#string"
>/features/collections/tripledes/landsat8__B3_index/items</xacml3:AttributeValue>
                        <xacml3:AttributeDesignator
                            AttributeId="urn:sd:path"
                            DataType="http://www.w3.org/2001/XMLSchema#string"
                            Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:resource"
                            MustBePresent="false"
                        />
                    </xacml3:Match>
                </xacml3:AllOf>
            </xacml3:AnyOf>
        </xacml3:Target>
        <xacml3:Policy xmlns:xacml3="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
           PolicyId="urn:secd:policy:tb15:helyx:xslt"
            RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-
```

```
algorithm:permit-overrides"
            Version="1.0">
            <xacml3:Description />
            <xacml3:PolicyDefaults>
                <xacml3:XPathVersion>http://www.w3.org/TR/1999/REC-xpath-
19991116</xacml3:XPathVersion>
            </xacml3:PolicyDefaults>
            <xacml3:Target />
            <xacml3:Rule
                    Effect="Permit"
                    RuleId=
"http://axiomatics.com/alfa/identifier/ogc.tb15helyx.landsat8__B3.xsltPolicy.topsecret
">
                <xacml3:Description />
                <xacml3:Target>
                    <xacml3:AnyOf>
                        <xacml3:AllOf>
                            <xacml3:Match MatchId=
"urn:oasis:names:tc:xacml:1.0:function:string-equal">
                                <xacml3:AttributeValue
                                    DataType="http://www.w3.org/2001/XMLSchema#string
">top_secret</xacml3:AttributeValue>
                                <xacml3:AttributeDesignator
                                    AttributeId="urn:sd:subject-clearance"
                                    DataType="http://www.w3.org/2001/XMLSchema#string"
                                    Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:environment"
                                    MustBePresent="false"
                                />
                            </xacml3:Match>
                        </xacml3:AllOf>
                    </xacml3:AnyOf>
                </xacml3:Target>
                <xacml3:ObligationExpressions>
                    <xacml3:ObligationExpression ObligationId=
"urn:SD:Obligation:Response:XSLT"
                    FulfillOn="Permit">
                        <xacml3:AttributeAssignmentExpression AttributeId=
"urn:SD:Obligation:Response:XSLT:Document" Category=
"urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
                            <xacml3:AttributeValue
                                DataType="http://www.w3.org/2001/XMLSchema#string"
>PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz4KPCEtLSAKICBUaGlzIFhTTFQgZmlsdGVyc
yBhbnkgV0ZTIHJlc3BvbnNlIC0gYWthIGEgRmVhdHVyZUNvbGxlY3Rpb24gLSBpbmNsdWRpbmcgU1RBTkFHIDQ
3NzggZmVhdHVyZXMgYmFzZWQgb24gdGhlIGNsYXNzaWZpY2F0aW9uIGxldmVsIGRlZmluZWQgaW4gdGhlIFNUQ
U5BRyBNZXRhZGF0YQogIGFuZCB0aGUgcGFyYW1ldGVyKHMpIGZvciBmZWF0dXJlIGNsYXNzaWZpY2F0aW9uOiB
VTkNMQVNTSUZJRUQsIENMQVNTSUZJRUQsIFNFQ1JFVCBhbmQgVE9QX1NFQ1JFVAogIEluIGNhc2UgdGhhdCB0a
GUgdXNlciBpcyBub3QgZW50aXRsZWQgdG8gc2VlIGFueSBvZiB0aGUgU1RBTkFHIGZlYXR1cmVzLCBhbiBlbXB
0eSBGZWF0dXJlQ29sbGVjdGlvbiBpcyBjcmVhdGVkLgotLT4KPHhzbDp0cmFuc2Zvcm0gdmVyc2lvbj0iMS4wI
iB4bWxuczp4c2w9Imh0dHA6Ly93d3cudzMub3JnLzE5OTkvWFNML1RyYW5zZm9ybSIgeG1sbnM6d2ZzPSJodHR
wOi8vd3d3Lm9wZW5naXMubmV0L3dmcy8zLjAiIHhtbG5zOmdtbD0iaHR0cDovL3d3dy5vcGVuZ2lzLm5ldC9nb
```

```
WwiCiAgeG1sbnM6bWI9InVybjpuYXRvOnN0YW5hZzo0Nzc4OmJpbmRpbmdpbmZvcm1hdGlvbjoxOjAiIHhtbG5
zOmRjcz0idXJuOnRiMTU6ZGNzOjE6MCIgeG1sbnM6ZW5jPSJodHRwOi8vd3d3LnczLm9yZy8yMDAxLzA0L3htb
GVuYyNFbGVtZW50IiB4bWxuczpzbGFiPSJ1cm46bmF0bzpzdGFuYWc6NDc3NDpjb25maWRlbnRpYWxpdHltZXR
hZGF0YWxhYmVsOjE6MCIgeG1sbnM6ZXh0PSJodHRwOi8vZXhzbHQub3JnL2NvbW1vbiIgZXh0ZW5zaW9uLWVsZ
W1lbnQtcHJlZml4ZXM9ImV4dCI+CiAgPHhzbDpvdXRwdXQgbWV0aG9kPSJ4bWwiIGluZGVudD0ieWVzIi8+CiA
gCiAgPHhzbDpzdHJpcC1zcGFjZSBlbGVtZW50cz0iKiIgLz4KICAKICA8eHNsOnBhcmFtIG5hbWU9InVzZXJDb
GVhcmFuY2UiLz4KICAKICA8eHNsOnRlbXBsYXRlIG5hbWU9IkNPUFkiPgogICAgPHhzbDpjb3B5LW9mIHNlbGV
jdD0iLiIvPgogIDwveHNsOnRlbXBsYXRlPgoKICA8eHNsOnRlbXBsYXRlIG1hdGNoPSJub2RlKCkiPgogICAgP
HhzbDpjaG9vc2U+CiAgICAgIDx4c2w6d2hlbiB0ZXN0PSJzZWxmOjoqW2xvY2FsLW5hbWUoKT0nbWVtYmVyJ10
gYW5kIHNlbGY6OiovZGNzOmRjc19vYmplY3QvbWI6QmluZGluZ0luZm9ybWF0aW9uL21iOk1ldGFkYXRhQmluZ
GluZ0NvbnRhaW5lci9tYjpNZXRhZGF0YUJpbmRpbmcvbWI6TWV0YWRhdGEvc2xhYjpvcmlnaW5hdG9yQ29uZml
kZW50aWFsaXR5TGFiZWwvc2xhYjpDb25maWRlbnRpYWxpdHlJbmZvcm1hdGlvbi9zbGFiOkNsYXNzaWZpY2F0a
W9uL3RleHQoKSA9ICdVTkNMQVNTSUZJRUQnIGFuZCAoJHVzZXJDbGVhcmFuY2UgPSAndW5jbGFzc2lmaWVkJyB
vciAkdXNlckNsZWFyYW5jZSA9ICdjbGFzc2lmaWVkJyBvciAkdXNlckNsZWFyYW5jZSA9ICdzZWNyZXQnIG9yI
CR1c2VyQ2xlYXJhbmNlID0gJ3RvcF9zZWNyZXQnKSI+CiAgICAgICAgIDx4c2w6Y2FsbC10ZW1wbGF0ZSBuYW1
lPSJDT1BZIi8+ICAgICAgICAKICAgICAgPC94c2w6d2hlbj4KICAgICAgPHhzbDp3aGVuIHRlc3Q9InNlbGY6O
ipbbG9jYWwtbmFtZSgpPSdtZW1iZXInXSBhbmQgc2VsZjo6Ki9kY3M6ZGNzX29iamVjdC9tYjpCaW5kaW5nSW5
mb3JtYXRpb24vbWI6TWV0YWRhdGFCaW5kaW5nQ29udGFpbmVyL21iOk1ldGFkYXRhQmluZGluZy9tYjpNZXRhZ
GF0YS9zbGFiOm9yaWdpbmF0b3JDb25maWRlbnRpYWxpdHlMYWJlbC9zbGFiOkNvbmZpZGVudGlhbGl0eUluZm9
ybWF0aW9uL3NsYWI6Q2xhc3NpZmljYXRpb24vdGV4dCgpID0gJ0NMQVNTSUZJRUQnIGFuZCAoJHVzZXJDbGVhc
mFuY2UgPSAnY2xhc3NpZmllZCcgb3IgJHVzZXJDbGVhcmFuY2UgPSAnc2VjcmV0JyBvciAkdXNlckNsZWFyYW5
jZSA9ICd0b3Bfc2VjcmV0JykiPgogICAgICAgIDx4c2w6Y2FsbC10ZW1wbGF0ZSBuYW1lPSJDT1BZIi8+CiAgI
CAgIDwveHNsOndoZW4+CiAgICAgIDx4c2w6d2hlbiB0ZXN0PSJzZWxmOjoqW2xvY2FsLW5hbWUoKT0nbWVtYmV
yJ10gYW5kIHNlbGY6OiovZGNzOmRjc19vYmplY3QvbWI6QmluZGluZ0luZm9ybWF0aW9uL21iOk1ldGFkYXRhQ
mluZGluZ0NvbnRhaW5lci9tYjpNZXRhZGF0YUJpbmRpbmcvbWI6TWV0YWRhdGEvc2xhYjpvcmlnaW5hdG9yQ29
uZmlkZW50aWFsaXR5TGFiZWwvc2xhYjpDb25maWRlbnRpYWxpdHlJbmZvcm1hdGlvbi9zbGFiOkNsYXNzaWZpY
2F0aW9uL3RleHQoKSA9ICdTRUNSRVQnIGFuZCAoJHVzZXJDbGVhcmFuY2UgPSAnc2VjcmV0JyBvciAkdXNlckN
sZWFyYW5jZSA9ICd0b3Bfc2VjcmV0JykiPgogICAgICAgIDx4c2w6Y2FsbC10ZW1wbGF0ZSBuYW1lPSJDT1BZI
i8+CiAgICAgIDwveHNsOndoZW4+CiAgICAgIDx4c2w6d2hlbiB0ZXN0PSJzZWxmOjoqW2xvY2FsLW5hbWUoKT0
nbWVtYmVyJ10gYW5kIHNlbGY6OiovZGNzOmRjc19vYmplY3QvbWI6QmluZGluZ0luZm9ybWF0aW9uL21iOk1ld
GFkYXRhQmluZGluZ0NvbnRhaW5lci9tYjpNZXRhZGF0YUJpbmRpbmcvbWI6TWV0YWRhdGEvc2xhYjpvcmlnaW5
hdG9yQ29uZmlkZW50aWFsaXR5TGFiZWwvc2xhYjpDb25maWRlbnRpYWxpdHlJbmZvcm1hdGlvbi9zbGFiOkNsY
XNzaWZpY2F0aW9uL3RleHQoKSA9ICdUT1BfU0VDUkVUJyBhbmQgKCR1c2VyQ2xlYXJhbmNlID0gJ3RvcF9zZWN
yZXQnKSI+CiAgICAgICAgPHhzbDpjYWxsLXRlbXBsYXRlIG5hbWU9IkNPUFkiLz4KICAgICAgPC94c2w6d2hlb
j4KICAgIDwveHNsOmNob29zZT4gICAgCiAgICA8eHNsOmFwcGx5LXRlbXBsYXRlcyBzZWxlY3Q9Im5vZGUoKSI
vPgogIDwveHNsOnRlbXBsYXRlPgogCiAgPHhzbDp0ZW1wbGF0ZSBtYXRjaD0iQCp8LyI+CiAgICA8d2ZzOkZlY
XR1cmVDb2xsZWN0aW9uPgogICAgICA8eHNsOmNvcHktb2Ygc2VsZWN0PSJAKiIgLz4KICAgICAgPGdtbDpib3V
uZGVkQnk+CiAgICAgICAgPGdtbDpOdWxsPm1pc3Npbmc8L2dtbDpOdWxsPgogICAgICA8L2dtbDpib3VuZGVkQ
nk+CiAgICAgIDx4c2w6YXBwbHktdGVtcGxhdGVzIHNlbGVjdD0iQCp8bm9kZSgpIi8+CiAgICA8L3dmczpGZWF
0dXJlQ29sbGVjdGlvbj4gIAogIDwveHNsOnRlbXBsYXRlPgogIAo8L3hzbDp0cmFuc2Zvcm0+</xacml3:Attr
ibuteValue>
                        </xacml3:AttributeAssignmentExpression>
                        <xacml3:AttributeAssignmentExpression AttributeId=
"urn:SD:Obligation:Response:XSLT:Parameter" Category=
"urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
                            <xacml3:AttributeValue
                                DataType="http://www.w3.org/2001/XMLSchema#string"
>userClearance=top_secret</xacml3:AttributeValue>
                        </xacml3:AttributeAssignmentExpression>
                    </xacml3:ObligationExpression>
                </xacml3:ObligationExpressions>
```

```
            </xacml3:Rule>
            <xacml3:Rule
                    Effect="Permit"
                    RuleId=
"http://axiomatics.com/alfa/identifier/ogc.tb15helyx.landsat8__B3.xsltPolicy.secret">
                <xacml3:Description />
                <xacml3:Target>
                    <xacml3:AnyOf>
                        <xacml3:AllOf>
                            <xacml3:Match MatchId=
"urn:oasis:names:tc:xacml:1.0:function:string-equal">
                                <xacml3:AttributeValue
                                    DataType="http://www.w3.org/2001/XMLSchema#string
">secret</xacml3:AttributeValue>
                                <xacml3:AttributeDesignator
                                    AttributeId="urn:sd:subject-clearance"
                                    DataType="http://www.w3.org/2001/XMLSchema#string"
                                    Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:environment"
                                    MustBePresent="false"
                                />
                            </xacml3:Match>
                        </xacml3:AllOf>
                    </xacml3:AnyOf>
                </xacml3:Target>
                <xacml3:ObligationExpressions>
                    <xacml3:ObligationExpression ObligationId=
"urn:SD:Obligation:Response:XSLT"
                    FulfillOn="Permit">
                        <xacml3:AttributeAssignmentExpression AttributeId=
"urn:SD:Obligation:Response:XSLT:Document" Category=
"urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
                            <xacml3:AttributeValue
                                DataType="http://www.w3.org/2001/XMLSchema#string"
>PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz4KPCEtLSAKICBUaGlzIFhTTFQgZmlsdGVyc
yBhbnkgV0ZTIHJlc3BvbnNlIC0gYWthIGEgRmVhdHVyZUNvbGxlY3Rpb24gLSBpbmNsdWRpbmcgU1RBTkFHIDQ
3NzggZmVhdHVyZXMgYmFzZWQgb24gdGhlIGNsYXNzaWZpY2F0aW9uIGxldmVsIGRlZmluZWQgaW4gdGhlIFNUQ
U5BRyBNZXRhZGF0YQogIGFuZCB0aGUgcGFyYW1ldGVyKHMpIGZvciBmZWF0dXJlIGNsYXNzaWZpY2F0aW9uOiB
VTkNMQVNTUZJRUQsIENMQVNTUZJRUQsIFNFQ1JFVCBhbmQgVE9QX1NFQ1JFVAogIEluIGNhc2UgdGhhdCB0a
GUgdXNlciBpcyBub3QgZW50aXRsZWQgdG8gc2VlIGFueSBvZiB0aGUgU1RBTkFHIGZlYXR1cmVzLCBhbiBlbXB
0eSBGZWF0dXJlQ29sbGVjdGlvbiBpcyBjcmVhdGVkLgotLT4KPHhzbDp0cmFuc2Zvcm0gdmVyc2lvbj0iMS4wI
iB4bWxuczp4c2w9Imh0dHA6Ly93d3cudzMub3JnLzE5OTkvWFNML1RyYW5zZm9ybSIgeG1sbnM6d2ZzPSJodHR
wOi8vd3d3Lm9wZW5naXMubmV0L3dmcy8zLjAiIHhtbG5zOmdtbD0iaHR0cDovL3d3dy5vcGVuZ2lzLm5ldC9nb
WwiCiAgeG1sbnM6bWI9InVybjpuYXRvOnN0YW5hZzo0Nzc4OmJpbmRpbmdpbmZvcm1hdGlvbjoxOjAiIHhtbG5
zOmRjcz0idXJuOnRiMTU6ZGNzOjE6MCIgeG1sbnM6ZW5jPSJodHRwOi8vd3d3LnczLm9yZy8yMDAxLzA0L3htb
GVuYyNFbGVtZW50IiB4bWxuczpzbGFiPSJ1cm46bmF0bzpzdGFuYWc6NDc3NDpjb25maWRlbnRpYWxpdHltZXR
hZGF0YWxhYmVsOjE6MCIgeG1sbnM6ZXh0PSJodHRwOi8vZXhzbHQub3JnL2NvbW1vbiIgZXh0ZW5zaW9uLWVsZ
W1lbnQtcHJlZml4ZXM9ImV4dCI+CiAgPHhzbDpvdXRwdXQgbWV0aG9kPSJ4bWwiIGluZGVudD0ieWVzIi8+CiA
gCiAgPHhzbDpzdHJpcC1zcGFjZSBlbGVtZW50cz0iKiIgLz4KICAKICA8eHNsOnBhcmFtIG5hbWU9InVzZXJDb
GVhcmFuY2UiLz4KICAKICA8eHNsOnRlbXBsYXRlIG5hbWU9IkNPUFkiPgogICAgPHhzbDpjb3B5LW9mIHNlbGV
jdD0iLiIvPgogIDwveHNsOnRlbXBsYXRlPgogIAogIDx4c2w6dGVtcGxhdGUgbWF0Y2g9IioiPgogICAgPHhzb
CP
```

```
HhzbDpjaG9vc2U+CiAgICAgIDx4c2w6d2hlbiB0ZXN0PSJzZWxmOjoqW2xvY2FsLW5hbWUoKT0nbWVtYmVyJ10
gYW5kIHNlbGY6OiovZGNzOmRjc19vYmplY3QvbWI6QmluZGluZ0luZm9ybWF0aW9uL21iOk1ldGFkYXRhQmluZ
GluZ0NvbnRhaW5lci9tYjpNZXRhZGF0YUJpbmRpbmcvbWI6TWV0YWRhdGEvc2xhYjpvcmlnaW5hdG9yQ29uZml
kZW50aWFsaXR5TGFiZWwvc2xhYjpDb25maWRlbnRpYWxpdHlJbmZvcm1hdGlvbi9zbGFiOkNsYXNzaWZpY2F0a
W9uL3RleHQoKSA9ICdVTkNMQVNTSUZJRUQnIGFuZCAoJHVzZXJDbGVhcmFuY2UgPSAndW5jbGFzc2lmaWVkJyB
vciAkdXNlckNsZWFyYW5jZSA9ICdjbGFzc2lmaWVkJyBvciAkdXNlckNsZWFyYW5jZSA9ICdzZWNyZXQnIG9yI
CR1c2VyQ2xlYXJhbmNlID0gJ3RvcF9zZWNyZXQnKSI+CiAgICAgICAgIDx4c2w6Y2FsbC10ZW1wbGF0ZSBuYW1
lPSJDT1BZIi8+ICAgICAgICAKICAgICAgPC94c2w6d2hlbj4KICAgICAgPHhzbDp3aGVuIHRlc3Q9InNlbGY6O
ipbbG9jYWwtbmFtZSgpPSdtZW1iZXInXSBhbmQgc2VsZjo6Ki9kY3M6ZGNzX29iamVjdC9tYjpCaW5kaW5nSW5
mb3JtYXRpb24vbWI6TWV0YWRhdGFCaW5kaW5nQ29udGFpbmVyL21iOk1ldGFkYXRhQmluZGluZy9tYjpNZXRhZ
GF0YS9zbGFiOm9yaWdpbmF0b3JDb25maWRlbnRpYWxpdHlMYWJlbC9zbGFiOkNvbmZpZGVudGlhbGl0eUluZm9
ybWF0aW9uL3NsYWI6Q2xhc3NpZmljYXRpb24vdGV4dCgpID0gJ0NMQVNTSUZJRUQnIGFuZCAoJHVzZXJDbGVhc
mFuY2UgPSAnY2xhc3NpZmllZCcgb3IgJHVzZXJDbGVhcmFuY2UgPSAnc2VjcmV0JyBvciAkdXNlckNsZWFyYW5
jZSA9ICd0b3Bfc2VjcmV0JykiPgogICAgICAgIDx4c2w6Y2FsbC10ZW1wbGF0ZSBuYW1lPSJDT1BZIi8+CiAgI
CAgIDwveHNsOndoZW4+CiAgICAgIDx4c2w6d2hlbiB0ZXN0PSJzZWxmOjoqW2xvY2FsLW5hbWUoKT0nbWVtYmV
yJ10gYW5kIHNlbGY6OiovZGNzOmRjc19vYmplY3QvbWI6QmluZGluZ0luZm9ybWF0aW9uL21iOk1ldGFkYXRhQ
mluZGluZ0NvbnRhaW5lci9tYjpNZXRhZGF0YUJpbmRpbmcvbWI6TWV0YWRhdGEvc2xhYjpvcmlnaW5hdG9yQ29
uZmlkZW50aWFsaXR5TGFiZWwvc2xhYjpDb25maWRlbnRpYWxpdHlJbmZvcm1hdGlvbi9zbGFiOkNsYXNzaWZpY
2F0aW9uL3RleHQoKSA9ICdTRUNSRVQnIGFuZCAoJHVzZXJDbGVhcmFuY2UgPSAnc2VjcmV0JyBvciAkdXNlckN
sZWFyYW5jZSA9ICd0b3Bfc2VjcmV0JykiPgogICAgICAgIDx4c2w6Y2FsbC10ZW1wbGF0ZSBuYW1lPSJDT1BZI
i8+CiAgICAgIDwveHNsOndoZW4+CiAgICAgIDx4c2w6d2hlbiB0ZXN0PSJzZWxmOjoqW2xvY2FsLW5hbWUoKT0
nbWVtYmVyJ10gYW5kIHNlbGY6OiovZGNzOmRjc19vYmplY3QvbWI6QmluZGluZ0luZm9ybWF0aW9uL21iOk1ld
GFkYXRhQmluZGluZ0NvbnRhaW5lci9tYjpNZXRhZGF0YUJpbmRpbmcvbWI6TWV0YWRhdGEvc2xhYjpvcmlnaW5
hdG9yQ29uZmlkZW50aWFsaXR5TGFiZWwvc2xhYjpDb25maWRlbnRpYWxpdHlJbmZvcm1hdGlvbi9zbGFiOkNsY
XNzaWZpY2F0aW9uL3RleHQoKSA9ICdUT1BfU0VDUkVUJyBhbmQgKCR1c2VyQ2xlYXJhbmNlID0gJ3RvcF9zZWN
yZXQnKSI+CiAgICAgICAgPHhzbDpjYWxsLXRlbXBsYXRlIG5hbWU9IkNPUFkiLz4KICAgICAgPC94c2w6d2hlb
j4KICAgIDwveHNsOmNob29zZT4gICAgCiAgICA8eHNsOmFwcGx5LXRlbXBsYXRlcyBzZWxlY3Q9Im5vZGUoKSI
vPgogIDwveHNsOnRlbXBsYXRlPgogCiAgPHhzbDp0ZW1wbGF0ZSBtYXRjaD0iQCp8LyI+CiAgICA8d2ZzOkZlY
XR1cmVDb2xsZWN0aW9uPgogICAgICA8eHNsOmNvcHktb2Ygc2VsZWN0PSJAKiIgLz4KICAgICAgPGdtbDpib3V
uZGVkQnk+CiAgICAgICAgPGdtbDpOdWxsPm1pc3Npbmc8L2dtbDpOdWxsPgogICAgICA8L2dtbDpib3VuZGVkQ
nk+CiAgICAgIDx4c2w6YXBwbHktdGVtcGxhdGVzIHNlbGVjdD0iQCp8bm9kZSgpIi8+CiAgICA8L3dmczpGZWF
0dXJlQ29sbGVjdGlvbj4gIAogIDwveHNsOnRlbXBsYXRlPgogIAo8L3hzbDp0cmFuc2Zvcm0+</xacml3:Attr
ibuteValue>
                        </xacml3:AttributeAssignmentExpression>
                        <xacml3:AttributeAssignmentExpression AttributeId=
"urn:SD:Obligation:Response:XSLT:Parameter" Category=
"urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
                            <xacml3:AttributeValue
                                DataType="http://www.w3.org/2001/XMLSchema#string"
>userClearance=secret</xacml3:AttributeValue>
                        </xacml3:AttributeAssignmentExpression>
                    </xacml3:ObligationExpression>
                </xacml3:ObligationExpressions>
            </xacml3:Rule>
            <xacml3:Rule
                    Effect="Permit"
                    RuleId=
"http://axiomatics.com/alfa/identifier/ogc.tb15helyx.landsat8__B3.xsltPolicy.classifie
d">
                <xacml3:Description />
                <xacml3:Target>
```

```
                    <xacml3:AnyOf>
                        <xacml3:AllOf>
                            <xacml3:Match MatchId=
"urn:oasis:names:tc:xacml:1.0:function:string-equal">
                                <xacml3:AttributeValue
                                    DataType="http://www.w3.org/2001/XMLSchema#string
">classified</xacml3:AttributeValue>
                                <xacml3:AttributeDesignator
                                    AttributeId="urn:sd:subject-clearance"
                                    DataType="http://www.w3.org/2001/XMLSchema#string"
                                    Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:environment"
                                    MustBePresent="false"
                                />
                            </xacml3:Match>
                        </xacml3:AllOf>
                    </xacml3:AnyOf>
                </xacml3:Target>
                <xacml3:ObligationExpressions>
                    <xacml3:ObligationExpression ObligationId=
"urn:SD:Obligation:Response:XSLT"
                    FulfillOn="Permit">
                        <xacml3:AttributeAssignmentExpression AttributeId=
"urn:SD:Obligation:Response:XSLT:Document" Category=
"urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
                            <xacml3:AttributeValue
                                DataType="http://www.w3.org/2001/XMLSchema#string"
>PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz4KPCEtLSAKICBUaGlzIFhTTFQgZmlsdGVyc
yBhbnkgV0ZTIHJlc3BvbnNlIC0gYWthIGEgRmVhdHVyZUNvbGxlY3Rpb24gLSBpbmNsdWRpbmcgU1RBTkFHIDQ
3NzggZmVhdHVyZXMgYmFzZWQgb24gdGhlIGNsYXNzaWZpY2F0aW9uIGxldmVsIGRlZmluZWQgaW4gdGhlIFNUQ
U5BRyBNZXRhZGF0YQogIGFuZCB0aGUgcGFyYW1ldGVyKHMpIGZvciBmZWF0dXJlIGNsYXNzaWZpY2F0aW9uOiB
VTkNMQVNTUZJRUQsIENMQVNTUZJRUQsIFNFQ1JFVCBhbmQgVE9QX1NFQ1JFVAogIEluIGNhc2UgdGhhdCB0a
GUgdXNlciBpcyBub3QgZW50aXRsZWQgdG8gc2VlIGFueSBvZiB0aGUgU1RBTkFHIGZlYXR1cmVzLCBhbiBlbXB
0eSBGZWF0dXJlQ29sbGVjdGlvbiBpcyBjcmVhdGVkLgotLT4KPHhzbDp0cmFuc2Zvcm0gdmVyc2lvbj0iMS4wI
iB4bWxuczp4c2w9Imh0dHA6Ly93d3cudzMub3JnLzE5OTkvWFNML1RyYW5zZm9ybSIgeG1sbnM6d2ZzPSJodHR
wOi8vd3d3Lm9wZW5naXMubmV0L3dmcy8zLjAiIHhtbG5zOmdtdCB0aHR0cDovL3d3dy5vcGVuZ2lzLm5ldC9nb
WwiCiAgeG1sbnM6bWI9InVybjpuYXRvOnN0YW5hZzo0Nzc4OmJpbmRpbmdpbmZvcm1hdGlvbjoxOjAiIHhtbG5
zOmRjcz0idXJuOnRiMTU6ZGNzOjE6MCIgeG1sbnM6ZW5jPSJodHRwOi8vd3d3LnczLm9yZy8yMDAxLzA0L3htb
GVuYyNFbGVtZW50IiB4bWxuczpzbGFiPSJ1cm46bmF0bzpzdGFuYWc6NDc3NDpjb25maWRlbnRpYWxpdHltZXR
hZGF0YWxhYmVsOjE6MCIgeG1sbnM6ZXh0PSJodHRwOi8vZXhzbHQub3JnL2NvbW1vbiIgZXh0ZW5zaW9uLWVsZ
W1lbnQtcHJlZml4ZXM9ImV4dCI+CiAgPHhzbDpvdXRwdXQgbWV0aG9kPSJ4bWwiIGluZGVudD0ieWVzIi8+CiA
gCiAgPHhzbDpzdHJpcC1zcGFjZSBlbGVtZW50cz0iKiIgLz4KICAKICA8eHNsOnBhcmFtIG5hbWU9InVzZXJDb
GVhcmFuY2UiLz4KICAKICA8eHNsOnRlbXBsYXRlIG5hbWU9IkNPUFkiPgogICAgPHhzbDpjb3B5LW9mIHNlbGV
jdD0iLiIvPgogIDwveHNsOnRlbXBsYXRlPgogIAogIDx4c2w6d2hlbiB0ZXN0PSJzZWxmOjoqW2xvY2FsLW5hbWUoKT0nbWVtYmVyJ10
gYW5kIHNlbGY6OiovZGNzOmRjc19vYmplY3QvbWI6QmluZGluZ0luZm9ybWF0aW9uL21iOk1ldGFkYXRhQmluZ
GluZ0NvbnRhaW5lci9tYjpNZXRhZGF0YUJpbmRpbmcvbWI6TWV0YWRhdGEvc2xhYjpvcmlnaW5hdG9yQ29uZml
kZW50aWFsaXR5TGFiZWwvc2xhYjpDb25maWRlbnRpYWxpdHlJbmZvcm1hdGlvbi9zbGFiOkNsYXNzaWZpY2F0a
W9uL3RleHQoKSA9ICdVTkNMQVNTUZJRUQnIGFuZCAoJHVzZXJDbGVhcmFuY2UgPSAndW5jbGFzc2lmaWVkJyB
vciAkdXNlckNsYWFyYW5jZSA9ICdjbGFzc2lmaWVkJyBvciAkdXNlckNsYWFyYW5jZSA9ICdzZWNyZXQnIG9yI
CR1c2VyQ2xlYXJhbmNlID0gJ3RvcF9zZWNyZXQnKSI+CiAgICA8c2w6dGV4dD48bGFiZWw6bGF0ZSBuYW1
```

```
lPSJDT1BZIi8+ICAgICAgICAKICAgICAgPC94c2w6d2hlbj4KICAgICAgPHhzbDp3aGVuIHRlc3Q9InNlbGY6O
ipbbG9jYWwtbmFtZSgpPSdtZW1iZXInXSBhbmQgc2VsZjo6Ki9kY3M6ZGNzX29iamVjdC9tYjpCaW5kaW5nSW5
mb3JtYXRpb24vbWI6TWV0YWRhdGFCaW5kaW5nQ29udGFpbmVyL21iOk1ldGFkYXRhQmluZGluZy9tYjpNZXRhZ
GF0YS9zbGFiOm9yaWdpbmF0b3JDb25maWRlbnRpYWxpdHlMYWJlbC9zbGFiOkNvbmZpZGVudGlhbGl0eUluZm9
ybWF0aW9uL3NsYWI6Q2xhc3NpZmljYXRpb24vdGV4dCgpID0gJ0NMQVNTSUZJRUQnIGFuZCAoJHVzZXJDbGVhc
mFuY2UgPSAnY2xhc3NpZmllZCcgb3IgJHVzZXJDbGVhcmFuY2UgPSAnc2VjcmV0JyBvciAkdXNlckNsZWFyYW5
jZSA9ICd0b3Bfc2VjcmV0JykiPgogICAgICAgIDx4c2w6Y2FsbC10ZW1wbGF0ZSBuYW1lPSJDT1BZIi8+CiAgI
CAgIDwveHNsOndoZW4+CiAgICAgIDx4c2w6d2hlbiB0ZXN0PSJzZWxmOjoqW2xvY2FsLW5hbWUoKT0nbWVtYmV
yJ10gYW5kIHNlbGY6OiovZGNzOmRjc19vYmplY3QvbWI6QmluZGluZ0luZm9ybWF0aW9uL21iOk1ldGFkYXRhQ
mluZGluZ0NvbnRhaW5lci9tYjpNZXRhZGF0YUJpbmRpbmcvbWI6TWV0YWRhdGEvc2xhYjpvcmlnaW5hdG9yQ29
uZmlkZW50aWFsaXR5TGFiZWwvc2xhYjpDb25maWRlbnRpYWxpdHlJbmZvcm1hdGlvbi9zbGFiOkNsYXNzaWZpY
2F0aW9uL3RleHQoKSA9ICdTRUNSRVQnIGFuZCAoJHVzZXJDbGVhcmFuY2UgPSAnc2VjcmV0JyBvciAkdXNlckN
sZWFyYW5jZSA9ICd0b3Bfc2VjcmV0JykiPgogICAgICAgIDx4c2w6Y2FsbC10ZW1wbGF0ZSBuYW1lPSJDT1BZI
i8+CiAgICAgIDwveHNsOndoZW4+CiAgICAgIDx4c2w6d2hlbiB0ZXN0PSJzZWxmOjoqW2xvY2FsLW5hbWUoKT0
nbWVtYmVyJ10gYW5kIHNlbGY6OiovZGNzOmRjc19vYmplY3QvbWI6QmluZGluZ0luZm9ybWF0aW9uL21iOk1ld
GFkYXRhQmluZGluZ0NvbnRhaW5lci9tYjpNZXRhZGF0YUJpbmRpbmcvbWI6TWV0YWRhdGEvc2xhYjpvcmlnaW5
hdG9yQ29uZmlkZW50aWFsaXR5TGFiZWwvc2xhYjpDb25maWRlbnRpYWxpdHlJbmZvcm1hdGlvbi9zbGFiOkNsY
XNzaWZpY2F0aW9uL3RleHQoKSA9ICdUT1BfU0VDUkVUJyBhbmQgKCR1c2VyQ2xlYXJhbmNlID0gJ3RvcF9zZWN
yZXQnKSI+CiAgICAgICAgPHhzbDpjYWxsLXRlbXBsYXRlIG5hbWU9IkNPUFkiLz4KICAgICAgPC94c2w6d2hlb
j4KICAgIDwveHNsOmNob29zZT4gICAgCiAgICA8eHNsOmFwcGx5LXRlbXBsYXRlcyBzZWxlY3Q9Im5vZGUoKSI
vPgogIDwveHNsOnRlbXBsYXRlPgogCiAgPHhzbDp0ZW1wbGF0ZSBtYXRjaD0iQCp8LyI+CiAgICA8d2ZzOkZlY
XR1cmVDb2xsZWN0aW9uPgogICAgICA8eHNsOmNvcHktb2Ygc2VsZWN0PSJAKiIgLz4KICAgICAgPGdtbDpib3V
uZGVkQnk+CiAgICAgICAgPGdtbDpOdWxsPm1pc3Npbmc8L2dtbDpOdWxsPgogICAgICA8L2dtbDpib3VuZGVkQ
nk+CiAgICAgIDx4c2w6YXBwbHktdGVtcGxhdGVzIHNlbGVjdD0iQCp8bm9kZSgpIi8+CiAgICA8L3dmczpGZWF
0dXJlQ29sbGVjdGlvbj4gIAogIDwveHNsOnRlbXBsYXRlPgogIAo8L3hzbDp0cmFuc2Zvcm0+</xacml3:Attr
ibuteValue>
                        </xacml3:AttributeAssignmentExpression>
                        <xacml3:AttributeAssignmentExpression AttributeId=
"urn:SD:Obligation:Response:XSLT:Parameter" Category=
"urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
                            <xacml3:AttributeValue
                                DataType="http://www.w3.org/2001/XMLSchema#string"
>userClearance=classified</xacml3:AttributeValue>
                        </xacml3:AttributeAssignmentExpression>
                    </xacml3:ObligationExpression>
                </xacml3:ObligationExpressions>
            </xacml3:Rule>
            <xacml3:Rule
                    Effect="Permit"
                    RuleId=
"http://axiomatics.com/alfa/identifier/ogc.tb15helyx.landsat8__B3.xsltPolicy.unclassif
ied">
                <xacml3:Description />
                <xacml3:Target>
                    <xacml3:AnyOf>
                        <xacml3:AllOf>
                            <xacml3:Match MatchId=
"urn:oasis:names:tc:xacml:1.0:function:string-equal">
                                <xacml3:AttributeValue
                                    DataType="http://www.w3.org/2001/XMLSchema#string
">unclassified</xacml3:AttributeValue>
```

```
                                <xacml3:AttributeDesignator
                                    AttributeId="urn:sd:subject-clearance"
                                    DataType="http://www.w3.org/2001/XMLSchema#string"
                                    Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:environment"
                                    MustBePresent="false"
                                />
                            </xacml3:Match>
                        </xacml3:AllOf>
                    </xacml3:AnyOf>
                </xacml3:Target>
                <xacml3:ObligationExpressions>
                    <xacml3:ObligationExpression ObligationId=
"urn:SD:Obligation:Response:XSLT"
                    FulfillOn="Permit">
                        <xacml3:AttributeAssignmentExpression AttributeId=
"urn:SD:Obligation:Response:XSLT:Document" Category=
"urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
                            <xacml3:AttributeValue
                                DataType="http://www.w3.org/2001/XMLSchema#string"
>PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz4KPCEtLSAKICBUaGlzIFhTTFQgZmlsdGVyc
yBhbnkgV0ZTIHJlc3BvbnNlIC0gYWthIGEgRmVhdHVyZUNvbGxlY3Rpb24gLSBpbmNsdWRpbmcgU1RBTkFHIDQ
3NzggZmVhdHVyZXMgYmFzZWQgb24gdGhlIGNsYXNzaWZpY2F0aW9uIGxldmVsIGRlZmluZWQgaW4gdGhlIFNUQ
U5BRyBNZXRhZGF0YQogIGFuZCB0aGUgcGFyYW1ldGVyKHMpIGZvciBmZWF0dXJlIGNsYXNzaWZpY2F0aW9uOiB
VTkNMQVNTUZJRUQsIENMQVNTUZJRUQsIFNFQ1JFVCBhbmQgVE9QX1NFQ1JFVAogIEluIGNhc2UgdGhhdCB0a
GUgdXNlciBpcyBub3QgZW50aXRsZWQgdG8gc2VlIGFueSBvZiB0aGUgU1RBTkFHIGZlYXR1cmVzLCBhbiBlbXB
0eSBGZWF0dXJlQ29sbGVjdGlvbiBpcyBjcmVhdGVkLgotLT4KPHhzbDp0cmFuc2Zvcm0gdmVyc2lvbj0iMS4wI
iB4bWxuczp4c2w9Imh0dHA6Ly93d3cudzMub3JnLzE5OTkvWFNML1RyYW5zZm9ybSIgeG1sbnM6d2ZzPSJodHR
wOi8vd3d3Lm9wZW5naXMubmV0L3dmcy8zLjAiIHhtbG5zOmdtbD0iaHR0cDovL3d3dy5vcGVuZ2lzLm5ldC9nb
WwiCiAgeG1sbnM6bWI9InVybjpuYXRvOnN0YW5hZzo0Nzc4OmJpbmRpbmdpbmZvcm1hdGlvbjoxOjAiIHhtbG5
zOmRjcz0idXJuOnRiMTU6ZGNzOjE6MCIgeG1sbnM6ZW5jPSJodHRwOi8vd3d3LnczLm9yZy8yMDAxLzA0L3htb
GVuYyNFbGVtZW50IiB4bWxuczpzbGFiPSJ1cm46bmF0bzpzdGFuYWc6NDc3NDpjb25maWRlbnRpYWxpdHltZXR
hZGF0YWxhYmVsOjE6MCIgeG1sbnM6ZXh0PSJodHRwOi8vZXhzbHQub3JnL2NvbW1vbiIgZXh0ZW5zaW9uLWVsZ
W1lbnQtcHJlZml4ZXM9ImV4dCI+CiAgPHhzbDpvdXRwdXQgbWV0aG9kPSJ4bWwiIGluZGVudD0ieWVzIi8+CiA
gCiAgPHhzbDpzdHJpcC1zcGFjZSBlbGVtZW50cz0iKiIgLz4KICAKICA8eHNsOnRlbXBsYXRlIG5hbWU9InVzZXJDb
GVhcmFuY2UiLz4KICAKICA8eHNsOnRlbXBsYXRlIG5hbWU9IkNPUFkiPgogICAgPHhzbDpjb3B5LW9mIHNlbGV
jdD0iLiIvPgogIDwveHNsOnRlbXBsYXRlPgoKICA8eHNsOnRlbXBsYXRlIG1hdGNoPSJub2RlKCkiPgogICAgP
HhzbDpjaG9vc2U+CiAgICAgIDx4c2w6d2hlbiB0ZXN0PSJzZWxmOjoqW2xvY2FsLW5hbWUoKT0nbWVtYmVyJ10
gYW5kIHNlbGY6OiovZGNzOmRjc19vYmplY3QvbWI6QmluZGluZ0luZm9ybWF0aW9uL21iOk1ldGFkYXRhQmluZ
GluZ0NvbnRhaW5lci9tYjpNZXRhZGF0YUJpbmRpbmcvbWI6TWV0YWRhdGEvc2xhYjpvcmlnaW5hdG9yQ29uZml
kZW50aWFsaXR5TGFiZWwvc2xhYjpDb25maWRlbnRpYWxpdHlJbmZvcm1hdGlvbi9zbGFiOkNsYXNzaWZpY2F0a
W9uL3RleHQoKSA9ICdVTkNMQVNTUZJRUQnIGFuZCAoJHVzZXJDbGVhcmFuY2UgPSAndW5jbGFzc2lmaWVkJyB
vciAkdXNlckNsZWFyYW5jZSA9ICdjbGFzc2lmaWVkJyBvciAkdXNlckNsZWFyYW5jZSA9ICdzZWNyZXQnIG9yI
CR1c2VyQ2xlYXJhbmNlID0gJ3RvcF9zZWNyZXQnKSI+CiAgICAgICAgPHhzbC10ZW1wbGF0ZSBuYW1
lPSJDT1BZIi8+ICAgICAgICAKICAgPC94c2w6d2hlbj4KICAgPHhzbDp3aGVuIHRlc3Q9InNlbGY6
ipbbG9jYWwtbmFtZSgpPSdtZW1iZXInXSBhbmQgc2VsZjo6Ki9kY3M6ZGNzX29iamVjdC9tYjpCaW5kaW5nSW5
mb3JtYXRpb24vbWI6TWV0YWRhdGFCaW5kaW5nQ29udGFpbmVyL21iOk1ldGFkYXRhQmluZGluZy9tYjpNZXRhZ
GF0YS9zbGFiOm9yaWdpbmF0b3JDb25maWRlbnRpYWxpdHlMYWJlbC9zbGFiOkNvbmZpZGVudGlhbGl0eUluZm9
ybWF0aW9uL3NsYWI6Q2xhc3NpZmljYXRpb24vdGV4dCgpID0gJ0NMQVNTUZJRUQnIGFuZCAoJHVzZXJDbGVhc
mFuY2UgPSAnY2xhc3NpZmllZCcgb3IgJHVzZXJDbGVhcmFuY2UgPSAnc2VjcmV0JyBvciAkdXNlckNsZWFyYW5
jZSA9ICd0b3Bfc2VjcmV0JykiPgogICAgICAgICAgICAgICAgICAgIDx4c2w6ZW1wbGF0ZSBuYW1lPSJDT1BZIi8+CiAgI
```

```
CAgIDwveHNsOndoZW4+CiAgICAgIDx4c2w6d2hlbiB0ZXN0PSJzZWxmOjoqW2xvY2FsLW5hbWUoKT0nbWVtYmV
yJ10gYW5kIHNlbGY6OiovZGNzOmRjc19vYmplY3QvbWI6QmluZGluZ0luZm9ybWF0aW9uL21iOk1ldGFkYXRhQ
mluZGluZ0NvbnRhaW5lci9tYjpNZXRhZGF0YUJpbmRpbmcvbWI6TWV0YWRhdGEvc2xhYjpvcmlnaW5hdG9yQ29
uZmlkZW50aWFsaXR5TGFiZWwvc2xhYjpDb25maWRlbnRpYWxpdHlJbmZvcm1hdGlvbi9zbGFiOkNsYXNzaWZpY
2F0aW9uL3RleHQoKSA9ICdTRUNSRVQnIGFuZCAoJHVzZXJDbGVhcmFuY2UgPSAnc2VjcmV0JyBvciAkdXNlckN
sZWFyYW5jZSA9ICd0b3Bfc2VjcmV0JykiPgogICAgICAgIDx4c2w6Y2hsbC10ZW1wbGF0ZSBuYW1lPSJDT1BZI
i8+CiAgICAgIDwveHNsOndoZW4+CiAgICAgIDx4c2w6d2hlbiB0ZXN0PSJzZWxmOjoqW2xvY2FsLW5hbWUoKT0
nbWVtYmVyJ10gYW5kIHNlbGY6OiovZGNzOmRjc19vYmplY3QvbWI6QmluZGluZ0luZm9ybWF0aW9uL21iOk1ld
GFkYXRhQmluZGluZ0NvbnRhaW5lci9tYjpNZXRhZGF0YUJpbmRpbmcvbWI6TWV0YWRhdGEvc2xhYjpvcmlnaW5
hdG9yQ29uZmlkZW50aWFsaXR5TGFiZWwvc2xhYjpDb25maWRlbnRpYWxpdHlJbmZvcm1hdGlvbi9zbGFiOkNsY
XNzaWZpY2F0aW9uL3RleHQoKSA9ICdUT1BfU0VDUkVUJyBhbmQgKCR1c2VyQ2xlYXJhbmNlID0gJ3RvcF9zZWN
yZXQnKSI+CiAgICAgICAgPHhzbDpjYWxsLXRlbXBsYXRlIG5hbWU9IkNPUFkiLz4KICAgICAgPC94c2w6d2hlb
j4KICAgIDwveHNsOmNob29zZT4gICAgICAgICA8eHNsOmFwcGx5LXRlbXBsYXRlcyBzZWxlY3Q9Im5vZGUoKSI
vPgogIDwveHNsOnRlbXBsYXRlPgogICAgPHhzbDp0ZW1wbGF0ZSBtYXRjaD0iQCp8LyI+CiAgICA8d2ZzOkZlY
XR1cmVDb2xsZWN0aW9uPgogICAgICA8eHNsOmNvcHktb2Ygc2VsZWN0PSJAKiIgLz4KICAgICAgPHhzbDpjb3Vu
ZGVkQnk+CiAgICAgICAgPGdtbDpQc3Npbmc8L2dtbDpOdWxsPgogICAgICA8L2dtbDpjb3VuZGVkQ
nk+CiAgICAgIDx4c2w6YXBwbHktdGVtcGxhdGVzIHNlbGVjdD0iQCp8bm9kZSgpIi8+CiAgICA8L3dmczpGZWF
0dXJlQ29sbGVjdGlvbj4gIAogIDwveHNsOnRlbXBsYXRlPgogIAo8L3hzbDpzdHlsZXNoZWV0PA==</xacml3:Attr
ibuteValue>
                        </xacml3:AttributeAssignmentExpression>
                        <xacml3:AttributeAssignmentExpression AttributeId=
"urn:SD:Obligation:Response:XSLT:Parameter" Category=
"urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
                            <xacml3:AttributeValue
                                DataType="http://www.w3.org/2001/XMLSchema#string"
>userClearance=unclassified</xacml3:AttributeValue>
                        </xacml3:AttributeAssignmentExpression>
                    </xacml3:ObligationExpression>
                </xacml3:ObligationExpressions>
            </xacml3:Rule>
            <xacml3:Rule
                    Effect="Deny"
                    RuleId=
"http://axiomatics.com/alfa/identifier/ogc.tb15helyx.landsat8__B3.xsltPolicy.denyAll">
                <xacml3:Description />
                <xacml3:Target />
            </xacml3:Rule>
        </xacml3:Policy>
        <xacml3:ObligationExpressions>
            <xacml3:ObligationExpression ObligationId="urn:SD:Obligation:Response:ENC"
            FulfillOn="Permit">
                <xacml3:AttributeAssignmentExpression AttributeId=
"urn:SD:Obligation:Response:ENC:RSA:PublicKey:Value" Category=
"urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
                    <xacml3:AttributeDesignator
                        AttributeId="urn:sd:public-key"
                        DataType="http://www.w3.org/2001/XMLSchema#string"
                        Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:environment"
                        MustBePresent="false"
                    />
```

```
                </xacml3:AttributeAssignmentExpression>
                <xacml3:AttributeAssignmentExpression AttributeId=
"urn:SD:Obligation:Response:ENC:RSA:PublicKey:Name" Category=
"urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
                    <xacml3:AttributeDesignator
                        AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
                        DataType="http://www.w3.org/2001/XMLSchema#string"
                        Category="urn:oasis:names:tc:xacml:1.0:subject-
category:access-subject"
                        MustBePresent="false"
                    />
                </xacml3:AttributeAssignmentExpression>
                <xacml3:AttributeAssignmentExpression AttributeId=
"urn:SD:Obligation:Response:ENC:Xpath" Category=
"urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
                    <xacml3:AttributeValue
                        DataType="http://www.w3.org/2001/XMLSchema#string">//*[local-
name() = 'originatorConfidentialityLabel']</xacml3:AttributeValue>
                </xacml3:AttributeAssignmentExpression>
            </xacml3:ObligationExpression>
            <xacml3:ObligationExpression ObligationId="
urn:SD:Obligation:Response:DSIG"
            FulfillOn="Permit">
                <xacml3:AttributeAssignmentExpression AttributeId=
"urn:SD:Obligation:Response:DSIG:RSA:PrivateKey:File" Category=
"urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
                    <xacml3:AttributeValue
                        DataType="http://www.w3.org/2001/XMLSchema#string"
>/etc/pki/tls/private/testbed15.pem</xacml3:AttributeValue>
                </xacml3:AttributeAssignmentExpression>
                <xacml3:AttributeAssignmentExpression AttributeId=
"urn:SD:Obligation:Response:DSIG:RSA:PrivateKey:Name" Category=
"urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
                    <xacml3:AttributeValue
                        DataType="http://www.w3.org/2001/XMLSchema#string">Dr.
No</xacml3:AttributeValue>
                </xacml3:AttributeAssignmentExpression>
                <xacml3:AttributeAssignmentExpression AttributeId=
"urn:SD:Obligation:Response:DSIG:X509:Certificate:File" Category=
"urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
                    <xacml3:AttributeValue
                        DataType="http://www.w3.org/2001/XMLSchema#string"
>/etc/pki/tls/certs/testbed15.crt</xacml3:AttributeValue>
                </xacml3:AttributeAssignmentExpression>
                <xacml3:AttributeAssignmentExpression AttributeId=
"urn:SD:Obligation:Response:DSIG:Id:Value" Category=
"urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
                    <xacml3:AttributeValue
                        DataType="http://www.w3.org/2001/XMLSchema#string">
#feature_1</xacml3:AttributeValue>
                </xacml3:AttributeAssignmentExpression>
```

```
                <xacml3:AttributeAssignmentExpression AttributeId=
"urn:SD:Obligation:Response:DSIG:Id:QName" Category=
"urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
                    <xacml3:AttributeValue
                        DataType="http://www.w3.org/2001/XMLSchema#string">
id</xacml3:AttributeValue>
                </xacml3:AttributeAssignmentExpression>
            </xacml3:ObligationExpression>
        </xacml3:ObligationExpressions>
    </xacml3:PolicySet>
</xacml3:PolicySet>
```

Operational XACML3 policy that controls access to the Helyx WFS3.

- This domain must be "updated" with GeoXACML functions. This can be achieved using the following HTTP PUT request: https://ogc.secure-dimensions.com/geopdp/domains/JeuDTcMdEemN8MEvpJG-Sw/pap/pdp.properties

```
<?xml version="1.0" encoding="UTF-8"?>
<pdpPropertiesUpdate xmlns="http://authzforce.github.io/rest-api-model/xmlns/authz/5">
  <feature type="urn:ow2:authzforce:feature-type:pdp:core" enabled="true"
    >urn:ow2:authzforce:feature:pdp:core:xpath-eval</feature>
  <feature type="urn:ow2:authzforce:feature-type:pdp:data-type" enabled="true"
    >urn:ogc:def:dataType:geoxacml:1.0:geometry</feature>
  <feature type="urn:ow2:authzforce:feature-type:pdp:function" enabled="true"
    >urn:ogc:def:function:geoxacml:1.0:geometry-intersects</feature>
  <feature type="urn:ow2:authzforce:feature-type:pdp:function" enabled="true"
    >urn:ogc:def:function:geoxacml:1.0:geometry-one-and-only</feature>
  <feature type="urn:ow2:authzforce:feature-type:pdp:function" enabled="true"
    >urn:ogc:def:function:geoxacml:1.0:geometry-disjoint</feature>
  <feature type="urn:ow2:authzforce:feature-type:pdp:function" enabled="true"
    >urn:ogc:def:function:geoxacml:1.0:geometry-is-within-distance</feature>
  <feature type="urn:ow2:authzforce:feature-type:pdp:function" enabled="true"
    >urn:ogc:def:function:geoxacml:1.0:geometry-is-simple</feature>
  <feature type="urn:ow2:authzforce:feature-type:pdp:function" enabled="true"
    >urn:ogc:def:function:geoxacml:1.0:geometry-touches</feature>
  <feature type="urn:ow2:authzforce:feature-type:pdp:function" enabled="true"
    >urn:ogc:def:function:geoxacml:1.0:geometry-contains</feature>
  <feature type="urn:ow2:authzforce:feature-type:pdp:function" enabled="true"
    >urn:ogc:def:function:geoxacml:1.0:geometry-sym-difference</feature>
  <feature type="urn:ow2:authzforce:feature-type:pdp:function" enabled="true"
    >urn:ogc:def:function:geoxacml:1.0:geometry-crosses</feature>
  <feature type="urn:ow2:authzforce:feature-type:pdp:function" enabled="true"
    >urn:ogc:def:function:geoxacml:1.0:geometry-bag-intersection</feature>
  <feature type="urn:ow2:authzforce:feature-type:pdp:function" enabled="true"
    >urn:ogc:def:function:geoxacml:1.0:geometry-bag-at-least-one-member-of</feature>
  <feature type="urn:ow2:authzforce:feature-type:pdp:function" enabled="true"
    >urn:ogc:def:function:geoxacml:1.0:geometry-within</feature>
  <feature type="urn:ow2:authzforce:feature-type:pdp:function" enabled="true"
    >urn:ogc:def:function:geoxacml:1.0:geometry-is-rectangle</feature>
```

```
  <feature type="urn:ow2:authzforce:feature-type:pdp:function" enabled="true"
    >urn:ogc:def:function:geoxacml:1.0:geometry-is-empty</feature>
  <feature type="urn:ow2:authzforce:feature-type:pdp:function" enabled="true"
    >urn:ogc:def:function:geoxacml:1.0:geometry-is-closed</feature>
  <feature type="urn:ow2:authzforce:feature-type:pdp:function" enabled="true"
    >urn:ogc:def:function:geoxacml:1.0:geometry-union</feature>
  <feature type="urn:ow2:authzforce:feature-type:pdp:function" enabled="true"
    >urn:ogc:def:function:geoxacml:1.0:geometry-bag-size</feature>
  <feature type="urn:ow2:authzforce:feature-type:pdp:function" enabled="true"
    >urn:ogc:def:function:geoxacml:1.0:geometry-is-in</feature>
  <feature type="urn:ow2:authzforce:feature-type:pdp:function" enabled="true"
    >urn:ogc:def:function:geoxacml:1.0:geometry-boundary</feature>
  <feature type="urn:ow2:authzforce:feature-type:pdp:function" enabled="true"
    >urn:ogc:def:function:geoxacml:1.0:geometry-equals</feature>
  <feature type="urn:ow2:authzforce:feature-type:pdp:function" enabled="true"
    >urn:ogc:def:function:geoxacml:1.0:geometry-intersection</feature>
  <feature type="urn:ow2:authzforce:feature-type:pdp:function" enabled="true"
    >urn:ogc:def:function:geoxacml:1.0:geometry-set-equals</feature>
  <feature type="urn:ow2:authzforce:feature-type:pdp:function" enabled="true"
    >urn:ogc:def:function:geoxacml:1.0:geometry-buffer</feature>
  <feature type="urn:ow2:authzforce:feature-type:pdp:function" enabled="true"
    >urn:ogc:def:function:geoxacml:1.0:geometry-bag</feature>
  <feature type="urn:ow2:authzforce:feature-type:pdp:function" enabled="true"
    >urn:ogc:def:function:geoxacml:1.0:geometry-length</feature>
  <feature type="urn:ow2:authzforce:feature-type:pdp:function" enabled="true"
    >urn:ogc:def:function:geoxacml:1.0:geometry-area</feature>
  <feature type="urn:ow2:authzforce:feature-type:pdp:function" enabled="true"
    >urn:ogc:def:function:geoxacml:1.0:geometry-centroid</feature>
  <feature type="urn:ow2:authzforce:feature-type:pdp:function" enabled="true"
    >urn:ogc:def:function:geoxacml:1.0:geometry-is-valid</feature>
  <feature type="urn:ow2:authzforce:feature-type:pdp:function" enabled="true"
    >urn:ogc:def:function:geoxacml:1.0:geometry-difference</feature>
  <feature type="urn:ow2:authzforce:feature-type:pdp:function" enabled="true"
    >urn:ogc:def:function:geoxacml:1.0:geometry-bag-union</feature>
    <feature type="urn:ow2:authzforce:feature-type:pdp:function" enabled="true"
    >urn:ogc:def:function:geoxacml:1.0:geometry-bag-subset</feature>
  <feature type="urn:ow2:authzforce:feature-type:pdp:function" enabled="true"
    >urn:ogc:def:function:geoxacml:1.0:geometry-overlaps</feature>
  <feature type="urn:ow2:authzforce:feature-type:pdp:function" enabled="true"
    >urn:ogc:def:function:geoxacml:1.0:geometry-distance</feature>
  <feature type="urn:ow2:authzforce:feature-type:pdp:function" enabled="true"
    >urn:ogc:def:function:geoxacml:1.0:convert-to-metre</feature>
  <feature type="urn:ow2:authzforce:feature-type:pdp:function" enabled="true"
    >urn:ogc:def:function:geoxacml:1.0:convert-to-square-metre</feature>
  <feature type="urn:ow2:authzforce:feature-type:pdp:function" enabled="true"
    >urn:ogc:def:function:geoxacml:1.0:geometry-convex-hull</feature>
  <rootPolicyRefExpression>urn:secd:policyset:tb15:helyx</rootPolicyRefExpression>
</pdpPropertiesUpdate>
```

The XML above, shows the update of the policy with the id `urn:secd:policyset:tb15:helyx`.

Users

Same users and clearance as created for alternative one.

Table 12. Users

User	Clearance
jane	top_secret
bob	secret
alice	classified
joe	unclassified

Once obtained an access token for a user, e.g. "joe"

```
curl -k -i -X POST -H "Authorization:Basic
ZmEwMGVmNGYtMTQzZC1kYTUzLWM4MTQtYWMxODY2ZDU5MmM1QG9nYy5zZWN1cmUtZGltZW5zaW9ucy5jb206Yj
BkZWM0Zjg1MzI3YzlhZjgwZjk2NjlmMGM4Zjk2NmViYzNmZmFhMGY1YzU2YzI0NGJhYzc2ODAyZDZiYTllZg==
" -H "Content-Type:application/x-www-form-urlencoded" -d "grant_type=password" -d
"username=jane" -d "password=secret" -d "scope=openid saml tb15" -d
"response_type=token" 'https://ogc.secure-dimensions.com/oauth/token'
```

the DCS WFS3 can be executed to fetch landsat8 features: https://ogc.secure-dimensions.com/features/collections/tripledes/landsat8__B3_index/items?mode=geowise&access_token=<access_token>

The following is a complete response for the user "joe":

```
<?xml version="1.0"?>
<wfs:FeatureCollection xmlns:wfs="http://www.opengis.net/wfs/3.0" xmlns:gml=
"http://www.opengis.net/gml" xmlns:mb="urn:nato:stanag:4778:bindinginformation:1:0"
xmlns:dcs="urn:tb15:dcs:1:0" xmlns:enc="http://www.w3.org/2001/04/xmlenc#Element"
xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0"><gml:boundedBy><gml
:Null>missing</gml:Null></gml:boundedBy><wfs:member><dcs:dcs_object xml:id="feature_1"
dcs:encoding_type="stanag4778"><mb:BindingInformation><mb:MetadataBindingContainer><mb
:MetadataBinding><mb:Metadata><EncryptedData xmlns="http://www.w3.org/2001/04/xmlenc#"
Type="http://www.w3.org/2001/04/xmlenc#Element">
<EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc"/>
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#">
<EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<KeyName>138af896-3487-32d6-8171-c4a51c416424</KeyName>
</KeyInfo>
<CipherData>
<CipherValue>k1fLcibV4QOu1gZRL3HsbCmv3Uu/cApMfu09FlD8N98OCB4Cv4Y4Xl0qm0b2p7uo
OuJQeLJWwhMLPg3vnIqhlo5LESQpkWGHIdwOrzamd58Z83IgUQUoT04yLmTi6s4m
+IZncYHyz57uJYcVlFsEoTU0l0fCMufbVX6rp6p+ZoIc6xK4RfpYWTPxBLwkEfhc
qzcN6lmcSQ5OUkHUPf5O33fqDcfFTDAMGtPdWkn/YY2djwSe8/iZQDZ9B6tcXgUm
```

```
ajMMup5rFnavkjdI60NwTM/FHT3fpex2HCUgsyzePB4fdN03wGN2WdjxrF/x4Wd0
4C9oMP2duUfzDeuHyZ6Axw==</CipherValue>
</CipherData>
</EncryptedKey>
</KeyInfo>
<CipherData>
<CipherValue>p7vlvSGvbzpgR7ly5AmTi3TdsrudznhFA8kFb6KpyCnX28WDyUEO7+7bSR2ZlA7B
6vpuzFQoIrvgqVAhxrunPVXzUlRq6QCfv6HN4+orP2qDzmOlCnZ3C1b4ju8yE00r
xeJN2ix4JMqPSfFBr6zjAVyT3HORPlzZKlzeU2CeVe4B0+FgBBfFcIKB1C/M3JLj
8W2ytQBjGFTdTRC/BJyJfotGd7zpRQ9PJSIvLr+u2UiJEnAOadV5ozMmvu+M2xk8
fAIeh33qoVBkzLbSUjWVfWuU/J8cstSESEjBPWx96hj1go0CWIyY7gDTihP2mwki
n6XLEPS9tZ3W4VO0jWVMisx9OLGPyRCs1Omn7FkfRZtrWM1lEl0qJ4Bwm4eUmMvu
2jFA8AGUnq9S+0f7YqC0nMN/dXNUDSLxZWOqUPyU6IoWuD0i9Nv+Mg==</CipherValue>
</CipherData>
</EncryptedData></mb:Metadata><mb:Data><enc:EncryptedData><enc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#aes128"/><enc:EncryptionKeyInfo><enc:Encry
ptedKey><enc:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256"/><enc:KeyInfo><enc:KeyName>Jane Bond 128</enc:KeyName>
</enc:KeyInfo><enc:CipherData><enc:CipherValue>NpzsfRXr2/aH4jvmq90PhVpv4u4SqMBfqh2FRId
ME9feDYx5wqGOFTiOsi3PVkPE6w8BELvAui4mNYkyzyTmSF4AT8rhQfoNOa7F//3CTUjeKAeD3bEdwzZY6YJxO
wFFOgciR/eVCA+sctF+codqGBJhjgDRQqaNIXZDP6FZuhjvxy+TuvB8C9UJgkoNMg2Sx3F3fveycwOapOkF+qD
abQhHFtc8sRH6iyWlA487up5evkR5mAIte9656zajxJdkEZ+uLjmdvcK0ZNqHGluG2CTxiznBhJbHTA1nvdo3M
vYDvSF/Nubszp/AVL/zmBrORjBH+DS0TrNEIYwlnSr9xw==</enc:CipherValue></enc:CipherData></en
c:EncryptedKey></enc:EncryptionKeyInfo><CipherData><CipherValue>++//jkiBKMi3Nvh6BCCSLi
B3OMDpldke31xwotLT8/Qbob8h2GHgHO0lJQyl+ou8Aov/3SjSYyEwybTTquqJ67+m8jGJ4UUzV3oNNkWeCguq
pb0njC71nNvgn3O/T3mQH71HDDmXFJJOQxIJb/eqzUvCQV5DBGfujbjZSFlr1LUH/B6Z7vrL0f/viqYlpnJuea
2mKLwJSlBVCIqn3L943u0gDDM84hQeEpgFaSdnr0GD8SW0AZXGfMFKIJN9hMETV09AOnfESyN6vOboJ9987ECS
2GObyMzbJMkvyYjXeeYJ3q2IzsB86gidP2aSpWtxCgUpMQl+cgbuvFSqqOx4koPxJbQBlcZ8wUogk32EwROZpe
siufTYRoTW2Ts44xfsMWNTKYUk1bK+oO6gK2Ng2LR20zMFwT306sOzhOoq2FuUgv7EMElNOJf7GuW62BMxn+7c
++zauXCRun35RezdizK1szb84+nWCTp5X0j3yhbbG7kIOQDDjg20CS5V8LaVFBYtAHzphLTAJ6YphMaShZsFof
J/LN/RznrSr3QRFu6ZEbxBr32fCNaLxJ+Dhr2MvzvmnXN2txQEomwLs4w++1+wE92v1E5HqLvAudAUzy14wOCX
mi4BeeSiLU1CvC3jLMrDaTdOCtNIcjeTjOu8GSTJ9u2V80rA3NE6GbUAJo+eyQ6QmYVEey0PzpPZB8mfG3YTTm
+xlzazSsznPzyggQZyyKLSgr+qz+Lf57NcXuaxvj7gHc6qzGjm+x/COnWTbL+/kMc83L15BiJIvWRURvXplZ7g
VfKuL/jNUZXA5hYIcxe16ElOeEX1nhuI/4dAcmIEI0biZzqVjVMSbXLF7Q0uyBvXLGRldHFTdSnkmaTYynEvMi
3Kn+vV2NAPx29XPzpPMzx3qyy9P3kQVeMw4LjJZa6l/YwpnI4gbVHxLlnQ4ULULpQkWwd+upkLCdqPp0s+p2En
671xhfO1oLmP2io/ocrDa+TOdK0fBq51dOWACUt6iiRCcTy3vpbPNgMJMvg5Tpx/8C2A9BqcZYBEUVc3NWKwO4
eFV5XjgL16rbVAi+29WNEt9GHEqacuTiHv4VjqmWC2TxBPgFuz4L3L9BBUg905HpGlo64/Ko5FonpBS3g6CUHl
IhHc8I1RykwbyiWx3EAS4IQ7IHnuh94RFLpa21hYHs/KGjCjGpDr9vjvDlmIZUCzxbYVIOZHs/BTGbRtJgJttl
HrtzWAgUhLdFmk9CF0GpqZZyzXXSUU3uQAeBLh6BYUJ3395YY0OCWeu7es+1/YU+vlQiCt++c3TPT0Iui3CgAt
Br03Io6A0S8XaQKgaB/Q1lCateYECVGDNBrWjo0wMQ4VZ5uyMet4ZBH64DniMgbh7ZrR/nNsNnARwG5UNfwchD
Z5VXzFrOngkhPZMcJgzRUyNCF3Trqia7d0eDZHqG6gnuG17llhgKf69rnVkLeu/qdAepzyL7Q5ok4ZDVicldTR
4N9PFQrE9qrazdg1EysAxXeyzwyAlmISON1aQjpuRtCuYxVvE4V+CSk55KnmQ9ADVSOdl7ESv9b8EkIDpvjh7w
rcCUvV/tQTcj93iVgUAN+Q3sik263X0+zayir+/1qwvbEGQkTpJ/YPQwmoPzby6IexGpV8m9Ig7prgjtVATaOo
bvJJ6FSJf0R2/uM//jFYk13pY4zb84/MAhAlSI9hroXLS20wJOopF6+p5Hb6ylpEQyevlnrOUqA70SJmG4zl+1
S5rk/5IKokvhjNku6Zx5WRz3oRp/x/RHb+4z/+MViTXeljjNvzBhIIK03RugjOhNtKD1K6pfo0B8xrccE4xjiw
kL2ij+8kpz98oz7UjzyHA+MWdZcsB6xJbxbc8dkOePju6SuG0o3ZY/cj3Ypxusg8l9fBOB0XvdqY22PeOaR/aT
rE2IiH3LBgR8DzIEerpB3wYVZJIiSWGqmo5negF1y3tyb7oneS7PItDTPg8rv+U85Oll9GqWHVECsZ1FsZd2rm
IMVmDtpOUfohvq4bnbfvoVpJLewcfZyUyANemU8T9WSHdSj3nyMDV4I7Ld7MewjQnaX0ZVyKcQFKwFPcL5GyVA
MDkrVTvP91ydzgSBmBZ6k4ZXJZhau0CtURKA7UCZATlxGF2Fl/iY6LkxGbnD+P9Z1BGnvvtatgniFosgSDVCKi
/yDNmdAA7gAAc4wx+uF7WWv4lqP/Sn4nv5bE8+uLmsfvzTx8yvYJaEWtyBYUYPuyQnOymUz6r0IvYUvO1j2I2K
t/TFfaIq9qo5NfZzVC64+jhmRW7WJEwR+fjdBPkJ4aHIYaz+bb96C6e1+bg55cpZNofryCBPI27G26MXqz5c/v
```

```
cwva/7tVgCDY9H4k+l8UzyzzJRryfbkHEY5K8/LrSBnGrqB6CxGo/fk49fR/YJguOitI/8x+VuCNUwLy6SQMyp
CM58qEZb+HPzzevuRfGomJkyuyvWZy1glqnOzlIpxFQpElGvJ9uQcRjkrz8utIGcauE3GNIkrfR0vYfd6MFwBc
oT8mNHPdQPYCQpRF364dCNFjlJs7KAXHAejAa7yTGbmCo7BKxRDJzOW/CqFIAw8d3zBCbPVwlHdv8rhpDL6TQS
nw3uwx3VvPJR8zLvKunUiOLUuyV6s7e9BvY8UYRhtc3eTxXNkEvnGKLZGB559NW3qWaLmuvsvGSBhm4Qi1wp93
keBrGgQmb6GT+hIICf4x/kRCkpZcgj/0WBM9dbMta5MuLX98q2GaHso0snF+ju9iHgAev3I9khdE1prFzDWGHz
vNwSaV7XKkr51XuDy7sRSmigYDd02/9dVyQh7WBqoD/qPqqAC46pdsY6bdvA1r3Nr/u1WAINj0fiT6XxTPLPOH
jZ34bv933ajAJv8lYp4hdvYxn2IaxJA2XlIGrF9khrlXVyqU7DOp7rocDiKPp/uIT3Gs8950uZqSBrLQwbYw+9
2LGv+hgrvJpSFZmtBBuZDujD0LdRjH5EYvVJ7Nayctbus8NiQ7I1x9f3zytQsjlXHfrgFmlYrV6NekRJG8heN6
2RYhQKxO9BCi0NmePmlN3zsfjn2U2XJu/p2JV1M/zQazJxhBPj3A6QqiIKbeBRzBG4gH1KsKk47dzIpz4kyQ/f
3txOpLbRQvTdwCJJEGtidrltkTNkmLOE0BdAH0Dc5tiAULWITGZ10Fc3ZE6d09CDX4iwba0qG+ebaKTXCB5TTM
v1CnUtgAlbICYaL5qT8mNHPdQPYCQpRF364dCNFjlJs7KAXHAejAa7yTGbmCo7BKxRDJzOW/CqFIAw8d3zBCbP
VwlHdv8rhpDL6TQSnw3uwx3VvPJR8zLvKunUiOLUuyV6s7e9BvY8UYRhtc3eTxXNkEvnGKLZGB559NW3qWaLmu
vsvGSBhm4Qi1wp93keBrGgQmb6GT+hIICf4x/ugzqM+QhB1Ewp8SxNwf2Fnv23FAjf/pgn3aQLiHcjlpHgAev3
I9khdE1prFzDWGH025QEYZqOV5zRscZ3B+VEimigYDd02/9dVyQh7WBqoDHymrm7hAuq4zkjYKzj+wuuDu3/tE
njsQE76E36qZuJcB0PCwe9sLH7wkF6jEJVkjasqLvXCBOpqRm44odjsfePa+c6mkvhK0NENJ+UC3updGGwaSfK
0Qb7LI8QM57+qXDB0NvSrl0sQ+H4ve7kTrcFa1S/EguR2Eg95v2cPhaymd2E/gE17PT2OA0ha6Bqzpo3VcZXPa
uU/yppoCjlrjPZgRuDfCfIczNs955PbI2Wqu7mDddcDquHXwsAgt10yTdYr6Q1N8Ftf6yE0bxslTjGiUbo5brc
aSC9ilXNQZgouCxHs28SFms3hJ7e2svRjr0mIPb+OFXeH+5reT6B/OVhwA7+UejwrBGqXXw5fT7gB1ivpDU3wW
1/rITRvGyVOM3IhFK+R5wzDlTdGFOlN2D6+F10WCiDNuMeOalDW4L3XzWmHasVOJGW6HoJ4AjBNKLfUENwWHaX
e5rP3TOFhzYVfireFH78enBHNzYtFBPwOb1y7uwPbKq0bmeD/WNLKgIDFkQS/X45HGiAdQq7grRwPP38IJ9b0t
Mb4k6qBKAbA+00nWfRbK2VBUYw6FzNa+aWiT87CO4UyErXqdmHOMD4vFcdjgjZKkZPT9w7DiDdz8lRms5Zn3tC
mLbn/4IhyY1Ps4YS4IrlRhZxQncP0+PvrLt2I+Dzsz7FAO6/Tcs4uXgQRyI+zWwmVOXIdmWLvHbPrYIRu28Kgx
LZHToHJsBq7uYN11wOq4dfCwCC3XTJN70qBYvvPbd60I2vX2Hkvqy43lNzhuqnC99iKIza9mUPvv/45IgSjItz
b4egQgki7k11beuFmEqB5RP3efWrFcPmiXRoZ4S7OpNVaR8GKxsOUzYoMRDAX6PFeYP1W7mmHKxVqqXI8iiCNB
dHn34U6eX0u786spTe2TTB8rn9mffLE83pRJMkfuZFiG35BBFRoKi/4SVg+KTLvqNRqkJGrYeWV1kYWOg4+Epm
l3Xu2TZSnS8Eqkw55C5epFy9v9lFcpGh1x62MObMEHHfj9h3NYls9YRHLM5Jn9ESFp3GQindtbuLhRm54lbat1
bN9QEsJ5ZXWRhY6Dj4SmaXde7ZNlElQSSqIw5vqzlVs1uBwQJ+zRs/bshWY9bd/Nimr6xCu5kMkUewpr9CvQnq
hA4UW9xR6WxX7dvMS+VJnm5LznWMRjp8P4sGFlsTwtye0ide3ZP6qFIsggOgiaILmh6/mhy7IXjXc0n81HVFPf
nzP1nbMTqjAVKX5tn5i4c8TRypwXGf153+9AA/GSDun+sIoDO+BWfXesHFGccnH5AGrX+l/r8cGBXgcJV3VpKb
ZilzLmOFPvddpIRPKdJpCM3tX63ahtLd94ocobenQ0JdUG32lX1eOr31GN6XjCYSv4vocJ+agKZOR9kg1vsnmO
WGOzp3QK1nqQ98xB2+AUmzZAfwqL/hJWD4pMu+o1GqQkatgKicCqF2jp1GaUiGC9MeuRJSxNwvNnWCW+24CfgO
ECbLsvSq38uqew0+L3gmgcG929k1nW1J5YmJ5qnLvkIlcvl23EDSAEDyrT2koAuHb3U8KNOViu389KgSqSA0Zf
miZUgVyoFkQaJEx2x+zRe0WYT6QL74idXHn/Yi5anHjYpZZSmFQ7AbyTuGSY2ubkOKjjwDwd7I2T9k0ySOv/p8
ApXBRNWDcFR9tgMocnKqjVwgvzZhdAa/XRJQOMDjL5TD/CstWnuA1gD6D/5ehvT3B3jPJR9IFLxO2XrdFNoBwg
WUrh3KHJ+AZ0pbrex/3/xFT8TpJVuQcykHOSY0mlgkQA+zz2/eemm0N8TBwTzi4LcD8mNHPdQPYCQpRF364dCN
FjlJs7KAXHAejAa7yTGbmCo7BKxRDJzOW/CqFIAw8d3zBCbPVwlHdv8rhpDL6TQSnw3uwx3VvPJR8zLvKunUiO
LUuyV6s7e9BvY8UYRhtc3eTxXNkEvnGKLZGB559NW3qWaLmuvsvGSBhm4Qi1wp93keBrGgQmb6GT+hIICf4x/l
ygRLSdzw8z7Uij+j588Ijha3pyg9P4k/oGQqWo5sphHgAev3I9khdE1prFzDWGHzgQoQid3nkdc4be2j+o7oOm
igYDd02/9dVyQh7WBqoDsJQGpai6uTJw0uXVzoerD6Z9XtokRx8aD//4KU/fboEEcMQw0NqG8FHwSqNx3PO3R4
sAx3EWsIrENQYf2jKAQ6P/Sn4nv5bE8+uLmsfvzTx8yvYJaEWtyBYUYPuyQnOy1wXtltZ6T+bRvj4x8EnHAVfa
Iq9qo5NfZzVC64+jhmRW7WJEwR+fjdBPkJ4aHIYaz+bb96C6e1+bg55cpZNofsvtFA/h0ArWPVEExKnrjBJMyp
FCkbUABO63bRiYbyP+L6+6ezy6hAhSTRcJBP5mPW5K4S2UClcfGd15Kkz13HzbF8Eg9iwRFS8KkBx3JoWztLEX
NNfAH0FLle+W99a29hA/ucC4oZzNmoX0FmwORfkvr7p7PLqECFJNFwkE/mY9yiXwy3cYFBGW2vka30U+Bz8mNH
PdQPYCQpRF364dCNFjlJs7KAXHAejAa7yTGbmCo7BKxRDJzOW/CqFIAw8d3zBCbPVwlHdv8rhpDL6TQSnw3uwx
3VvPJR8zLvKunUiOLUuyV6s7e9BvY8UYRhtc3eTxXNkEvnGKLZGB559NW3qWaLmuvsvGSBhm4Qi1wp93keBrGg
Qmb6GT+hIICf4x/qo24XDX22+qfzNkTRlkkpfv23FAjf/pgn3aQLiHcjlpHgAev3I9khdE1prFzDWGH025QEYZ
qOV5zRscZ3B+VEimigYDd02/9dVyQh7WBqoDHQO6jtXiRoMbK2yjLgUfl0zKkUKRtQAE7rdtGJhvI/5e1MRgjK
GvpfD8EnaiETE/sO01dPaHb83IhCMCgEw/WQOXExfXhQ3pmhlKP9UZ3y9/U8FVjUVt2zNiEetri6RX11Rm55nk
aG3PEkj22e//sYIS1qsyl8Ixg5nn+vofIDoBqn+hyj0rQYEJf24mKY26aMtj+0tlQL5zhxjuoZJG7wauA78/ZH
FnBAF//4Zc6roNs342LPXPZZu3+1kCeKbybw2ts1gHYtK84tE/acbquj1qDclGZxiT2PTgAjULprZv6wmDNgL4
haBm3jW7yFs9R/sGArv5WY1Pum3wr0vt166V7dmFtIKgRzLMJO4YuCWfnsQrR2YQRAngRfBAmVoBIrGF1m7VCQ
```

```
+lSMHtr/74Y7ZoF5yAWrRedQjUhuyxJKFG9ZsJuXeGfoJGq5tRK/RaK7JHAGQ6A14h08rY2/QdHV8yqYuRt8yV
AGgroQgjGPG2nfu/XTV+WF1a1xm+MU2zGrbERODgOhfXkUjHI6gYaPULsPDQqnSlWpPVT/w6br+OqLKll08ecs
wmaQd4HTWthDK5PYvpTQpoT1zot1uz4OiqBayTU6aK1GxYgHlE2Hj4+dqymEev3hWNsFeBl+87BFhdaFtadPTm
9Poy1rN73adb7Y+yxI8BVkuf2h8ACrGAX+Tk3zdK8tL7xcQCFYZwDZuzgooQPyKdutjN9m0wHNHS5fFFZedTGh
BkXE6Rer69ojJud/UWMjbo0ScE3B3jAiUSCkM1h4hqEK14EuitU9t8NuoNmL+ILX9hG62VJ0dh54yHJGl6fdjb
AkFPQIvp2M0S/YPE6X0TVC+laXQffJjMLmLf1Xs5bIT+GmlvFKoB/bRrZvQ3T9E2cFgPWGXY4KtyB7YsOQnSaD
7MQKNayelP3N6Y1KWYGr9MD5hlOF27OHV1E2xc0k7lGVIlTsGO7rFWGpHkhlI55DRrz15OcR91+2j5YK345czC
RD0nBT3mhsvMt89qx7z3an1IGzzlIB6JCW/qaKe32G7e78MN3HYIsjDKf1ciw5Ui68A8Q8kW13v7W9ficIEQep
F/MIL2M/eZYpPAUdenlSQU9hU2Y+RNqF0l/BihvMPh4BW8gcLFgvaG/hXIQRf9aU/5mpohUSU6wbpcXfmjvB6I
A1Tg7DALCFSZvMWmEKsXMEmH/bbJIYN7n9geoM5pdOVOltloUF9zhK4EfM5KxRuZceP7xEBuEqaISCuIOZSU90
VzXFB2cS3uPimeh/pv5XmlBDIX7T/YEOTV3cE09ZbUaiTbG2fVxLNvDvDepQnb5LtDdckUwVSfUcasudoBhMiG
n2E8Co5yPxbBDH9U0i+mkkK3syuyRwBkOgNeIdPK2Nv0HR1fMqmLkbfMlQBoK6EIIxjxtp37v101flhdWtcZvj
FNsxq2xETg4DoX15FIxyOoGGj1C7Dw0Kp0pVqT1U/8Om6/jqiypZdPHnLMJmkHeB01rYQyuT2L6U0KaE9c6Ldb
s+DoqgWsk1OmitRsWIB5RNh44e1R/aX9aMot72lohJRpssPemukX2arrJkSNOoojzQyONJVQAt6i6XAsVhqBny
HB8Yc+XSMYL09OxFZYLZZEiu64Lbz5ogk0Ls7duzoyH55vDa2zWAdi0rzi0T9pxuq6OOL5vAvrsw32FSIw1yBJ
86ZWMVlRYiEJYdf0XFYx4e6ZBUW5VDn5iOLCE9/X+bC30IBCncbHdc5viN4jRZagyFL9kQFXWVL7nIxNcQy8Gj
NB4Qu648fD4Ror2mNezuoiJgWkKRGJyR8sG/imnDao94nPgjhtqF7yJ+JR8Tb5bWwD9b8d9wzR8y+Ob3hZFGHr
67eqe7Qbi32M+QDKPKwtVJkdKGReu5TrzBSF3JdTeyEHFcluf8+g3QZwHQnW94EPc1WbzSrq3YpfICRZSKCDaF
Ss2EGtg9O4Kaw9+ImLTN0mWYybIHhhEx4VCDQNQRQ3Z6bz/vk7h1csVSNjj79k/E2Su3d06cfe4jaZKS4xGUf5
oghBpu+XL1IyqJQzkC0zPG/QUR15tvU24ubG3WQv5Mkhg3uf2B6gzml05U6W2WgtIyx+eEl429WO2oHiEdpHyM
qxs3QhahYPhqLjwtfuf4ixCvm9ukCvyS4Kzd9iHaMaz/0jUyVMRkqT2q9kTl7xDSreSyYCSW8ia3JSVEfNj8XR
qxTsxK6ltJJ6UWda1fRUywgBtdNurkKXn2lVeJ9jv7udEatUqKiKoCSDSPoqxrp3+MTlVVhiHTlan/XbrzbLe4
GmCbDSC2hOZOs8xy3glbtda0QhCEMgm3kskqIoKWukzLur6bWMb7KyhodSJOsvcULGBjgLYuT2vmUFFdVhsUPh
0jb7YjsCxS1mMVLTyfKF3JgJeUPoNCl95P6prcIa7HZlmyY9NrYkPBZNddEZ49Woac91l+LAI3OFmCyrNu2kEJ
MJBtzsIiT3beRWKWdLA8tJpGQp55N1GD7mucNy218CY786OL5j90Z0HMTmkfXA/cIVHZ25fBenfeiiJsTR0uXx
RWXnUxoQZFxOkXq+odWyN0RG9PfSSsPla6+6wP2R3MXYu5U5tJJeWfzjmXfIulsyuImdDlTVsJxATf7R9OGDb6
MxkLgjl7gGG+yN24LlFSyRGwuKNV6R51rg7N/whm7U91tiGnmTOa7EcJ7ZmkGKRF+elFTLemGBDTFXYXUlMeCm
jxMN5SjvJdBmh6cb8mzSYztsu4hgc8asFi/sS2CjyhHV8A4WAVVJdUZ7d99/o8mrBHDUhnjXCAEgbHuSrnbCO5
kqEXkz7fnfSsbeGmNDFHCwgWaWOuOcRPzCrpWVfSS6LbAKJZlJZs7bjaJOEZmCeH9aVPLYkNNJn1QV8shQsiLA
/w4mXR1vzHS1pCEzYyijvbDdPNLCT5jrbOmlNjynPoeRG/DkuzUZWLMc9cD9whUdnbl8F6d96KImxNHS5fFFZe
dTGhBkXE6Rer69ojJud/UWMjbo0ScE3B3j8F3RLfkhyYt9ywUIv4Br1L2U47pyBNY8JkJj7Ij0qcnGkF4PYKyq
IIBddwtXRMJU+bUl35dq6xF9DnLmDe0hcnQh1pMn4j/HeCmr4DWcO3AcVdFVa0xRwWtAPI0Q0ZJKQwdtTGI+3M
lsOC3THYfleXBUatO+N4Kin53up311wqS5XbkMbpTaEnc+8fyBD8nmLUIUHqPDW9DT7i6bar99gr0qQIguAHfH
22OkOT5K9EJUONw4IzqKo9Xyg+gOSJMeJxbaZN72PHdPT7ZxHUcpVge1IkpRkF9mbaYKOXRK9ZXtU2ZA25/NTz
FJo/zRcM1Tr5A1Cd/vDvsE60PE+rrVmwBvlmj1h3plnQakMsQpFjifnsQrR2YQRAngRfBAmVoB5Ki7Jjmnesr Q
WtQI+yCxw7B165ZQfGYtYrgfidrwLjq7OHV1E2xc0k7lGVIlTsGO7rFWGpHkhlI55DRrz15OcR91+2j5YK345c
zCRD0nBT3mhsvMt89qx7z3an1IGzzlIB6JCW/qaKe32G7e78MN3HYIsjDKf1ciw5Ui68A8Q8kW13v7W9ficIEQ
epF/MIL2M/eZYpPAUdenlSQU9hU2Y+RNqF0l/BihvMPh4BW8gcLavAlc51/zg9f6zJTFynv/e1OYDqgTn+vncz
4Irz8GKJxmf9MEGb12DOSOqp2s3AyZxObBa0MjtOjZHvmkVMlZWSyJw8f2GEmEiMu8wfICdB5QwbjouUeqIQOa
qAZ1kY2809DfqRV7hSIV4sVKAPDRAMmOSzJ/abkvFpYEnmuOFwrLBlUwsn2S7siLwbixIXib/sbyJY5FJh+68x
fnOknnCoy3PdbDhNf3l3QWHKMbdKpBU+kwcLxPdx9r9t/E1HjQsFqUey8oj57cNblNq/p6XfSbJH/nfu72HovY
jVIM9slh51f91I/54rN/fD8Xfj73s5waLTxkTyfhL4YV8jBamJq8S6j6R9A8q5czEe5bk8khg3uf2B6gzml05U
6W2WgtIyx+eEl429WO2oHiEdpHyMqxs3QhahYPhqLjwtfuf7o+GEuOwKYKMSPYbEpxGUKpI4elL6OJN3XkKTsT
METnkMOTOKy0wqraUGGWGLeMB76o7RfDoJYgQxu1LpElEwauok4k3aH26xkx+li8g5+RBJCqEzD6LIA1xURQCf
RCDxuXAgcslOOiGcAg9EOGD9CfnsQrR2YQRAngRfBAmVoBxBXEaYkVwL600zo5chnnCy6YgOJKwLBiVdKOxmXV
/ep1u4qhhEPwsrf6FYxV57ruBkF3NKFHUPJ1bbex6WyfXHzPRLmim3sxgNnyK1xZ/Z3iPcWqiV0vmQblkJ2L0D
+yxfA/P6TxiSCVKTslYdzmNCYFpCkRickfLBv4ppw2qPeJz4I4bahe8ifiUfE2+W1sA/W/HfcM0fMvjm94WRRh
6+u3qnu0G4t9jPkAyjysLVSZHShkXruU68wUhdyXU3shBxXJbn/PoN0GcB0J1veBD3NVm80q6t2KXyAkWUigg2
hUrNhBrYPTuCmsPfiJi0zdJlmMmyB4YRMeFQg0DUEUN5M7k2Pms4f+oY39e/vAXTrI67eK9rxT5X5P3SfyanQz
bvXam24T7qX3+saOrrNJJjmvqlKvGKpGjK9COGYRpIYjCBzCHvESujJaAatlJK0nQinvkhELzr3u2TlNyKTuqq
bdKcBOqPPrvW0MErkxWFxfgksPw7Vh3rvHG6tV74b+CD842TQc/H3BcBXwSgpde9K0JR0kpSuj5kfTPNf54R2V
```

```
6sQJpOPyPBHnFqyhVHMd0dLl8UVl51MaEGRcTpF6vr2iMm539RYyNujRJwTcHePmZ7FgimJn8ZDQjNbX6uEsFX
30pLtpIg+L9Yli2L1gzN8epWnL8sq3+fGLrKpIz6Q7jShirVtQtjF74FtImLTYsoOLjxDTiOEc+kvpReSyG5E0
s6OdtpRbwJcfoJ66fxybf24t+OvIu3HsK1iZFca8dCHWkyfiP8d4KavgNZw7cBxV0VVrTFHBa0A8jRDRkkpDB2
1MYj7cyWw4LdMdh+V5cFRq0743gqKfne6nfXXCpLlduQxulNoSdz7x/IEPyeYtQhQeo8Nb0NPuLptqv32CvSpA
iC4Ad8fbY6Q5Pkr0QlQ43DgjOoqj1fKD6A5Ikx4nFtpk3vY8d09PtnEdRylWN+N+Tnw9H3Jq9ZVcJSo9spL/2w
6nA2E6W9+Q29EwTq71Z57AZZiTTkDkSIRSGiOBhZaplgoE1yLRM98Vh8Wfj4MPgGowCy10GDafYaCmttl5ivO1
gxNHBZPhIGe2jzWY12q/DCSOYVXqDKv9SecB6m92uTFcC/iksifqT2y5vfK2ELubloPZJ7XBBptuVoNL2M0S/Y
PE6X0TVC+laXQffAWbsTspDxamXzNn65LhpWaW8nQ+8iq5hjHKzcci1kbesUyHC/n1M7GYNFwbMiPq4LzT0N+p
FXuFIhXixUoA8NEAyY5LMn9puS8WlgSea44XCssGVTCyfZLuyIvBuLEheJv+xvIljkUmH7rzF+c6SecKjLc91s
OE1/eXdBYcoxt0qkFT6TBwvE93H2v238TUeNCwWpR7LyiPntw1uU2r+npd9Jskf+d+7vYei9iNUgz2yWHnV/3U
j/nis398Pxd+PtV55ktPOOhR9Z5xt5yra+87aQ05jO5lfDVbc4vQxiLPChTBqP4MvNZMtV3zeRgVlyCCYk4Gt0
ElriYv6FMu1dJAvaZUNv2+9wMfURk+nj0pzJPRigkoV5UMbByV0CuCCH9xXii6FFhRFk/sRRUWMtX18KUzbTzH
L9S4vvwPrdcdSY4+Jz95rxqJ+16mmAsS3N6mkdu10Vuizn7xWBk0y27ycRRtTdHPrvHGj02cJ4r27upeyU8dMm
wte+x4NC03De0OVeYHPh5Cdi5+hzwEvOieSgBwXITwZLDQ9LHp3wPkdOk4wtKTmOAvUVXg7jdmewEhGjWrekrQ
SMiXmcCP59MFcsRV6A5Qz++LoFCt1owLiz6lLk4zlR4aw+Nkwr9/mDjwB/Eg1cjcynzmasVGODtx1AM6NVm4BK
enkQznERvfu/krMd3WHcEjhBpRw2AlWUZmM7TcW5kSnG+B/ObsQnovyr+OkuWbItZShf4qGc148WFyMpN31Ejv
irvV+KyGcWaJxg3uRxVHG9+iLwHSYmx1s+b1LolGXFLiaGamBkLMJ5wnBywVJHCzOBxLlqefMxkJB4++ete9Xz
ZYNDxzcpP2Id/QNC4brldgpIaSEVMNsmQ3izK2nIEKIk7CDSbkF8riQxXVJzN8/jCVI6UES2AeQ1WlhK03hhWT
DOtCQTgfG/Js0mM7bLuIYHPGrBYv7Etgo8oR1fAOFgFVSXVGe3fff6PJqwRw1IZ41wgBIGx7kq52wjuZKhF5M+
3530rG3hpjQxRwsIFmljrjnET8wq6VlX0kui2wCiWZSWbO242ite3xjtWQP20h8rYB5+66tjEfQK6XrM6hWSDK
wPCfNagJxxYS6QsHMspmsXGjYEHdzJPRigkoV5UMbByV0CuCCH9xXii6FFhRFk/sRRUWMtX18KUzbTzHL9S4vv
wPrdcd9p6V6puU/Pw0/5yEsmHG+hkJB4++ete9XzZYNDxzcpP2Id/QNC4brldgpIaSEVMNTz6m2YAkrcCl8Lx8
B9L9kQoPTLdcQgQ+DYZq5TUkk1IFeoMES16UxdNiTQFO8oNKlripe/MXMOLzGWDyw5IDdHuyVceGTDgsr7LxSr
2aEiQeelzJpfAMGz0TWkpcrmgm5ELilvbL5NWKVUTmIaxsCOip9qrZpoIXy0EYDmiB54Md42JcqgtQa0X5y8QC
X9/2V9+joS4SNxYutGWwIe40i0kaRQxMSAivOsF6MWzJr1/uuC28+aIJNC7O3bs6Mh+e+2lwtk/R0KP1ISPvPY
DZdl2wpWAkbZMWdqLXNT434IPzmFJXOt2WjWgc1CI4E13yGQkHj756171fNlg0PHNyk482FoENAoCgRdidLFb4
nRSdOyeOn9QAmliCTw+Bm4hbI5cJD+1jUw3vewECyDd4HgrLBlUwsn2S7siLwbixIXib/sbyJY5FJh+68xfnOk
nnCoy3PdbDhNf3l3QWHKMbdKpBU+kwcLxPdx9r9t/E1HjQsFqUey8oj57cNblNq/p6XfSbJH/nfu72HovYjVIM
9tAQnJj206tsv4fss6jk6oHkFymh6NeuUvfJnzi1ZySPgpNHDRFPbaLW/dtgAmraeQ==</CipherValue></Ci
pherData></enc:EncryptedData></mb:Data></mb:MetadataBinding></mb:MetadataBindingContai
ner></mb:BindingInformation></dcs:dcs_object></wfs:member><ds:Signature xmlns:ds=
"http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315
"/>
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<ds:Reference Id="id" URI="#feature_1">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue>WApjIBfE4PBiaEeQvgQRgLeN4CQ=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>di8sRClAsEWh9YR9sict4bHCCFlSPGVy5g/mhBzcS/oUqt4ix3qx1AFUIALoBCLQ
0EGy60IKAKBQ7m47mIhOEjWwrfiY7fIODwue9Ze90zsJvvlUMv8x2rAng4bZodhU
4CztFrV9iAR8yNnD9hnOfSnweG26ow9Eq74PqmEDoWIBnTGU7/3QmoglinCUvCsQ
wGagndTyPKSM2ABvEnMMlOwDYNyXEgDEbtN7eLw17B7unlyQc3CY9lUCnJu9Xg2y
E6Q5BWjTdHCiS24aFlB6OqF0zc2rqnjQkgVonWdtIujgGNctO+c2/gl36V0vVidx
P7uVarSDtNd3XVVZLZa/9g==</ds:SignatureValue>
<ds:KeyInfo>
```

```
<ds:KeyName>Dr. No</ds:KeyName>
<ds:X509Data>


<ds:X509Certificate>MIIDuTCCAqGgAwIBAgIEYpLJdjANBgkqhkiG9w0BAQsFADCBjDELMAkGA1UEBhMC
REUxEDAOBgNVBAgTB0JhdmFyaWExDzANBgNVBAcTBk11bmljaDEfMB0GA1UEChMW
U2VjdXJlIERpbWVuc2lvbnMgR21iSDEfMB0GA1UECxMWU2VjdXJlIERpbWVuc2lv
bnMgR21iSDEYMBYGA1UEAxMPQW5kcmVhcyBNYXRoZXVzMB4XDTE1MTAyNTE0NDEw
MVoXDTE2MDEyMzE0NDEwMVowgYwxCzAJBgNVBAYTAkRFMRAwDgYDVQQIEwdCYXZh
cmlhMQ8wDQYDVQQHEwZNdW5pY2gxHzAdBgNVBAoTFlNlY3VyZSBEaW1lbnNpb25z
IEdtYkgxHzAdBgNVBAsTFlNlY3VyZSBEaW1lbnNpb25zIEdtYkgxGDAWBgNVBAMT
D0FuZHJlYXMgTWF0aGV1czCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AJBxrjwhMmOGnSKT4DLsOx+R+c4dN3gA74/03NdsxUdy2r6QB65AvF8Rm3YF5pJy
Hzdrlf43IObjOHK2yRn6p0tXpc5yYwBGd3tZMGTkyj4qhqqy/ug4LxYy4HYfCXE/
ec9UOTCDu7vfkbvmEfg8V0M2DfT6t5XnvFZmkUkSAi4L4vQ9PJthsFLyJXq2nNlh
tOMQeBWxcOzbog6EBAB7qaUyumlrrIojksHd9Tb4Om/BIp+JxcocRjGmSq7XoKZ1
GuXmWXSnrc877AnET/+Kbea4zqH+Oo44zP2G0XdCCMiKtL7nxqIAfwucp3SEGtqH
XGNv61RGsqihQbtlbhRkprcCAwEAAaMhMB8wHQYDVR0OBBYEFIVLBZDvNUo/OX9F
MKRLz7OFaUXXMA0GCSqGSIb3DQEBCwUAA4IBAQCA7FkGI0EOkJPr4yjCT8HxJvAd
lzNW539tl/SVYe4ducBm4J523G6POKvz6kVHbS30J2HiNd2FoQL9s2DMPN2ag9Q3
myzI8E9x8dowNKhaupmTJI/Edneqnp7pr/8/o612qBXTf00T4j8QP9mZxUreqC+x
TCV9GCO0XuIVpBM6sGbEiFfjg0xLs3HO7kBHla78WAb8EyZGv9aoHCsqoIE+A/L9
e++xrY09TN/wjJKrv665iRF3XG+WHj0lrUvzlPZzNHbLykqSo48DhDc/JmaadiqZ
cNFF8NBHOLzicsSo+GpeEnSJBKnCYwxStWJ+dFWoHQxwyHrkn+Om+EiQ6/2w</ds:X509Certificate>
<ds:X509SubjectName>CN=Andreas Matheus,OU=Secure Dimensions GmbH,O=Secure Dimensions
GmbH,L=Munich,ST=Bavaria,C=DE</ds:X509SubjectName>
</ds:X509Data>
</ds:KeyInfo>
</ds:Signature></wfs:FeatureCollection>
```

For user "jane", the FeatureCollection is empty:

```
<?xml version="1.0"?>
<wfs:FeatureCollection xmlns:wfs="http://www.opengis.net/wfs/3.0" xmlns:gml=
"http://www.opengis.net/gml" xmlns:mb="urn:nato:stanag:4778:bindinginformation:1:0"
xmlns:dcs="urn:tb15:dcs:1:0" xmlns:enc="http://www.w3.org/2001/04/xmlenc#Element"
xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0"><gml:boundedBy><gml
:Null>missing</gml:Null></gml:boundedBy><ds:Signature xmlns:ds=
"http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315
"/>
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<ds:Reference Id="id" URI="#feature_1">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue/>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue/>
<ds:KeyInfo>
<ds:KeyName/>
<ds:X509Data>
<ds:X509SubjectName/>
<ds:X509Certificate/>
</ds:X509Data>
</ds:KeyInfo>
</ds:Signature></wfs:FeatureCollection>
```

Invalid FeatureCollection Issue

As illustrated in the example for user "joe", the `<ds:Signature>` element is included in the XML as last child of root, aka the `<wfs:FeatureCollection>` element. According to the current OGC WFS schema, this is **invalid**.

Appendix D: Revision History

Table 13. Revision History

Date	Editor	Release	Primary clauses modified	Descriptions
August 15, 2019	M. Leedahl	.1	all	initial version
August 21, 2019	A. Matheus	.2	annex-c	initial version
August 29, 2019	D. Dall	.3	multiple	updates and spell checks
Sept. 12, 2019	C. Reed	.4	all	Internal Review
Oct. 8, 2019	A. Matheus	.5	multiple	Review and changes
Oct. 9, 2019	M. Leedahl	.6	all	Edits & Publish to Pending
Dec. 16, 2019	C. Reed	.7	All	Final edits for publications as a PER