Open Geospatial Consortium

Publication Date: 2015-01-25

Approval Date: 2015-09-17

Posted Date: 2015-10-13

Reference number of this document: OGC 15-050r3

Reference URL for this document: http://www.opengis.net/doc/PER/ tb11-niem-ic-data

Category: Public Engineering Report

Editor(s): Jeff Harrison

OGC Testbed-11 Test and Demonstration Results for NIEM using IC Data Encoding Specifications Engineering Report

Warning

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

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

Contents

Page

Figures

Page

Abstract

The goal of the Geo4NIEM thread in Testbed 11 was to gain Intelligence Community (IC) concurrence of the National Information Exchange Model (NIEM) Version 3.0 architecture through the development, implementations, test, and robust demonstration making use of IC specifications, Geography Markup Language (GML), and NIEM in a simulated "real-world" scenario. The demonstration scenario begins with NIEM-conformant Information Exchange Packages (IEPs) containing operational data and IC security tags from the Information Security Marking (ISM) and Need-To-Know (NTK) access control metadata, and the Trusted Data Format (TDF) for binding assertion metadata with data resource(s). Those instance documents are deployed using Open Geospatial Consortium (OGC) standards enabled Web Services for use by client applications. Access control is based on attributes of the end-user and the instance data.

Recommendations to update these information exchanges were provided to reflect NIEM 3.0 architecture and security tags in a 'NIEM/IC Data Encoding'. The assessment tested this data encoding in OGC Web Feature Services (WFS) and Policy Enforcement Points (PEP) accessed by multiple client applications. Results from this task provided a preliminary architecture that was tested and demonstrated in Testbed 11, and summarized in other OGC Testbed 11 Engineering Reports. The demonstrations also highlighted how NIEM and IC data encodings together may support more agile and customer-centric frameworks driven by collaborative partnerships. This transformation is vital to confronting the security challenges of the future.

Business Value

Geospatial information technologies are increasingly a foundation for supporting homeland security, law enforcement, emergency management, and public safety missions in the U.S. While these technologies rely upon much of the same data, they are typically developed in silos within a specific mission area. As a result, data duplication and data exchange delays occur.

In addition, many Information Sharing Environment (ISE), Homeland Security (HLS) and Law Enforcement (LE) mission partners have developed stand-alone geospatial information systems (GIS) or Common Operating Picture (COP)/Situational Awareness (SA) applications to support their stakeholder communities during incidents and for daily operational support. While different missions, these GIS or COP/SA capabilities rely upon much of the same data or generate specific data during an event. The data are often stove-piped and not exposed to a broader community that could benefit from these data, resulting in duplication and delayed or incorrect decisions. While mission partners do not need to use the same GIS or COP/SA tools, they could benefit from shared access to the

common operating data and services used within these systems if they were exposed and exchanged using open standards.

To meet this challenge, the Program Manager for the Information Sharing Environment (PM-ISE) is funding work to enhance NIEM. One focus of these efforts is to enhance NIEM's geospatial exchange capabilities to improve inter-government information sharing. Validating and testing the NIEM (Version 3.0) technical architecture related to the IC Data Encoding Specifications (i.e. security tags such as ISM, NTK, and TDF), aligned to OGC Web Services was identified as a need. Specifically, if the framework's geospatial exchange capability is enhanced with security and standards issued by the OGC it will significantly improve inter-government information sharing.

Keywords

ogcdocs, testbed-11, Geo4NIEM, NIEM, WFS, WFS-T, GML, PEP, security, access control, ISM, NTK and TDF

OGC Testbed-11 Test and Demonstration Results for NIEM using IC Data Encoding Specifications Engineering Report

1 Introduction

1.1 Scope

The focus of the Geo4NIEM thread in OGC Testbed 11 was to assess the potential for security tagging and access control from Intelligence Community (IC) Data Encoding Specifications to be combined with NIEM for information exchange. The purpose was to determine if the current NIEM architecture can be aligned with the IC Data Encoding Specifications, which include (but are not limited to) ISM, NTK and Trusted Data Format (TDF). This alignment would enable secure information exchange and enhance user/developer understanding. The assessment included review of real world data exchanges defined in the form of a NIEM Information Exchange Package Documentation (IEPD). A number of Extensible Markup Language (XML) instance documents from those real-world exchanges, populated with operational data and IC security tags, were deployed on OGC Web Services for testing.

This effort builds on the previous work of the Geo4NIEM Pilot Project. Much of the work was focused on the GML (ISO 19136) data exchange standard and the mechanisms by which GML and NIEM data could be intermingled. A key driver was to clarify how data conforming to one framework could be included or "embedded" in the other using various encapsulation strategies. A secondary goal was to conduct various software demonstrations in order to assess the feasibility of the various approaches and to explore the prospects for making use of fundamental OGC web service standards such as Web Feature Service (WFS).

Based on the results of the Geo4NIEM Pilot the sponsors of the Geo4NIEM thread in Testbed worked with OGC staff to articulate specific functional requirements in order to meet the following objectives:

- Validating the NIEM (Version 3.0) technical architecture related to the IC Data Encoding Specifications (i.e. ISM, NTK, and TDF) aligned to OGC Web Services, Phase 9 (OWS-9) Testbed related work.

- Testing and demonstrating use of 1) NIEM 3.0 architecture, and access control and security tagging metadata defined by the IC Data Encoding Specifications leveraging OWS-9; and 2) full round tripping of NIEM-conformant information

exchanges to GML feature(s) and back to a NIEM-conformant information exchange.

- Testing and demonstrating use of an application programming interface (API) for operating primarily on GML feature representations leveraging NIEM components; features may be searched, retrieved, inserted, updated, and deleted.

- Reviewing and documenting recommendations to enable full round tripping from NIEM-conformant information exchange to Geography Markup Language (GML) feature(s) and back to NIEM-conformant information exchange.

To accomplish these objectives, five primary tasks were identified:

Task 1: *NIEM & IC Data Encoding Specification Assessment and Recommendations*

This task assessed the potential for security tagging and access control from the IC Data Encoding Specifications to be leveraged with NIEM in support of information exchange. The purpose was to determine if the current architecture of NIEM can support IC specification alignment. The IC Data Encoding Specifications include but are not limited to ISM, NTK, TDF.

The assessment included review of real world IEPDs, where the Extensible Markup Language (XML) schema and NIEM instance documents were populated with relevant content and IC security tags. IEPDs assessed were:

- Notice of Arrival IEPD
- Incidents IEPD
- Resources IEPD

Recommendations to update these information exchanges were provided to reflect NIEM 3.0 architecture and included sample security and dissemination control markings. The assessment exercised OGC web services to test NIEM Version 3.0 conformant IEPDs containing the appropriate IC security markings. Results from this task provided a preliminary proposed architecture structure that was tested and demonstrated in Task 2.

This task produced one document:

- Testbed 11 NIEM IC Data Encoding Specification Assessment and Recommendations ER

Task 2: *NIEM & IC Data Encoding Specification Test and Demonstration*

This task used preliminary findings and recommended architectures for IC Data Encoding Specification support identified in Task 1, and performed a Test and Demonstration of the recommended architecture leveraging the results of Testbed 9 and previous Geo4NIEM initiatives where appropriate. Results of this task provided updates to the proposed architecture prepared in Task 1.

Results of this test and demonstration were documented in an Engineering Report containing the Findings and Recommendations with reference to refinements to the originally proposed architecture prepared in Task 1.

This task produced one document:

- Testbed 11 Results of Test and Demonstration of NIEM Using IC Data Encoding Specifications ER

Task 3: *NIEM-GML-NIEM Round-trip Assessment and Recommendations*

This task assessed the NIEM and GML support for geospatial data exchange round-trip workflow process to include: creation, transfer, receipt, modification, return, and acceptance of XML content originating as NIEM IEPDs.

This task produced one document:

- Testbed 11 NIEM-GML-NIEM Round Trip Assessment and Recommendations ER (Preliminary)

Task 4: *NIEM-GML-NIEM Round-trip Test and Demonstration*

This task used the findings and recommended architecture structure supporting NIEM-GML-NIEM round-trip assessment identified in Task 3 and performs a Test and Demonstration of the recommended architecture.

This task produced one document:

- Testbed 11 NIEM-GML-NIEM Round Trip Assessment and Recommendations ER (Final)

Task 5: *Test and Demonstration of an API for Processing GML Feature Representations*

This task performed Test and Demonstrations using OGC web services, such as Basic and Transactional Web Feature Service (WFS-T) and Policy Enforcement Points (PEPs), to process GML feature representations leveraging NIEM components. The Test and Demonstration included, but are not limited to feature retrieval, insert, update and delete.

This task produced one document:

- Testbed 11 NIEM-GML Feature Processing API using OGC Web Services ER.

1.2 Participating organizations

1.2.1 Sponsoring Organizations

Geo4NIEM in Testbed 11 was sponsored by the following organizations:

- US Department of Homeland Security (DHS)

1.2.2 Participating Organizations

The following organizations played one or more roles in Geo4NIEM in Testbed 11 as participants (i.e. responded to the RFQ/CFP)

- The Carbon Project
- Secure Dimensions
- con terra
- Jericho Systems

This document also integrates comments and content from MITRE and Safe Software.

1.3 Document contributor contact points

The following participants (listed in alphabetical order by surname) made substantial contributions to the content of this report. All questions regarding this document should be directed to the editor or any of the contributors.

Name	Organization
Jan Drewnak	con terra

Rüdiger Gartmann	con terra
Jeff Harrison	The Carbon Project
Dean Hintz	Safe Software
Andreas Matheus	Secure Dimensions
Mark Mattson	The Carbon Project
Scott Renner	MITRE
Tim Schmoyer	Jericho Systems

Many thanks are extended to the reviewers who submitted comments over the course of the project.

1.4 Future work

Improvements in this document are desirable and will be included based on ongoing interoperability engineering activities.

1.5 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.

2 References

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

- *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA)

- *Guidelines and Requirements in Support of the Information Sharing Environment*, Presidential Memo, December 2005.
- Open Geospatial Consortium (OGC), Summary and Recommendations of the Geospatial Enhancement for the National Information Exchange Model (Geo4NIEM) Interoperability Program Pilot (http://www.opengeospatial.org/standards/per)
- Open Geospatial Consortium (OGC), Geography Markup Language (GML) Encoding Standard (http://www.opengeospatial.org/standards/gml)
- Open Geospatial Consortium (OGC), Web Feature Service (WFS) (http://www.opengeospatial.org/standards/wfs)
- Open Geospatial Consortium (OGC), Filter Encoding Implementation Specification (http://www.opengeospatial.org/standards/filter)
- Intelligence Community (IC) Data Encoding Specifications (http://www.dni.gov/index.php/about/organization/chief-information-officer/ic-cio-enterprise-integration-architecture)
- IC Enterprise Authorization Attribute Exchange between IC Attribute Services, Authorization Attribute Set (http://www.dni.gov/index.php/about/organization/chief-information-officer/idam-authorization-attribute-set)
- XML Data Encoding Specifications for Information Security Marking Metadata (http://www.dni.gov/index.php/about/organization/chief-information-officer/information-security-marking-metadata)
- XML Data Encoding Specification for Need-To-Know Metadata (http://www.dni.gov/index.php/about/organization/chief-information-officer/need-to-know-metadata)
- XML Data Encoding Specification for Trusted Data Format (http://www.dni.gov/index.php/about/organization/chief-information-officer/trusted-data-format)
- NIEM Version 3.0 (http://release.niem.gov/niem/3.0)
- NIEM.gov (http://www.niem.gov)
- Open Geospatial Consortium (OGC), Web Services Common Standard (http://www.opengeospatial.org/standards/common)

NOTE The OWS Common Standard contains a list of normative references that are also applicable to this Implementation Standard.

In addition to this document, this report includes several XML Document files as specified in Annexes A and B.

3 Terms and definitions

For the purposes of this report, the definitions specified in Clause 4 of the OWS Common Implementation Standard [OGC 06-121r3] shall apply.

3.1 Abbreviated Terms

ABAC	Access Based Access Control
AIXM	Aeronautical Information Exchange Model
ARH	Access Rights and Handling
DES	Data Encoding Specification
EDH	Enterprise Data Header
GML	Geography Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over SSL/TLS
IC	Intelligence Community
IEP	Information Exchange Package
IEPD	Information Exchange Package Documentation
ISM	Information Security Markings
MDA	Maritime Domain Awareness
NIEM	National Information Exchange Model
NTK	Need to Know
OAS	OGC Attribute Store
OWS	OGC Web Services
PDP	Policy Decision Point
PEP	Policy Enforcement Points
PM-ISE	Program Manager for the Information Sharing Environment
SSL	Secure Sockets Layer
TDF	Trusted Data Format
TDO	Trusted Data Objects
TLS	Transport Layer Security
UAAS	Unified Attribute and Authorization Service

UIAS	Unified Identity Attribute Set
WFS	OGC Web Feature Service
WFS-T	OGC Web Feature Service – Transactional
XLink	XML Linking Language
XML	Extensible Markup Language

4 Testing

For the OGC Testbed 11, Geo4NIEM thread Participants assessed IC Security Markings and Need to Know tagging. They also investigated how to provide access control to NIEM IEPs served through an OGC Web Feature Service (WFS) instance. The assessment was conducted by implementing prototype components that use NIEM/IC Data Encodings and Feature Processing APIs[1] in a functional test environment. Access control was conducted via one of several Policy Enforcement Points that filter based upon the user attributes stored in the OGC Attribute Store. Details on the prototype test environment and test results are provided in the sections below.

[1] See OGC IP ERs 15-047 and 15-048

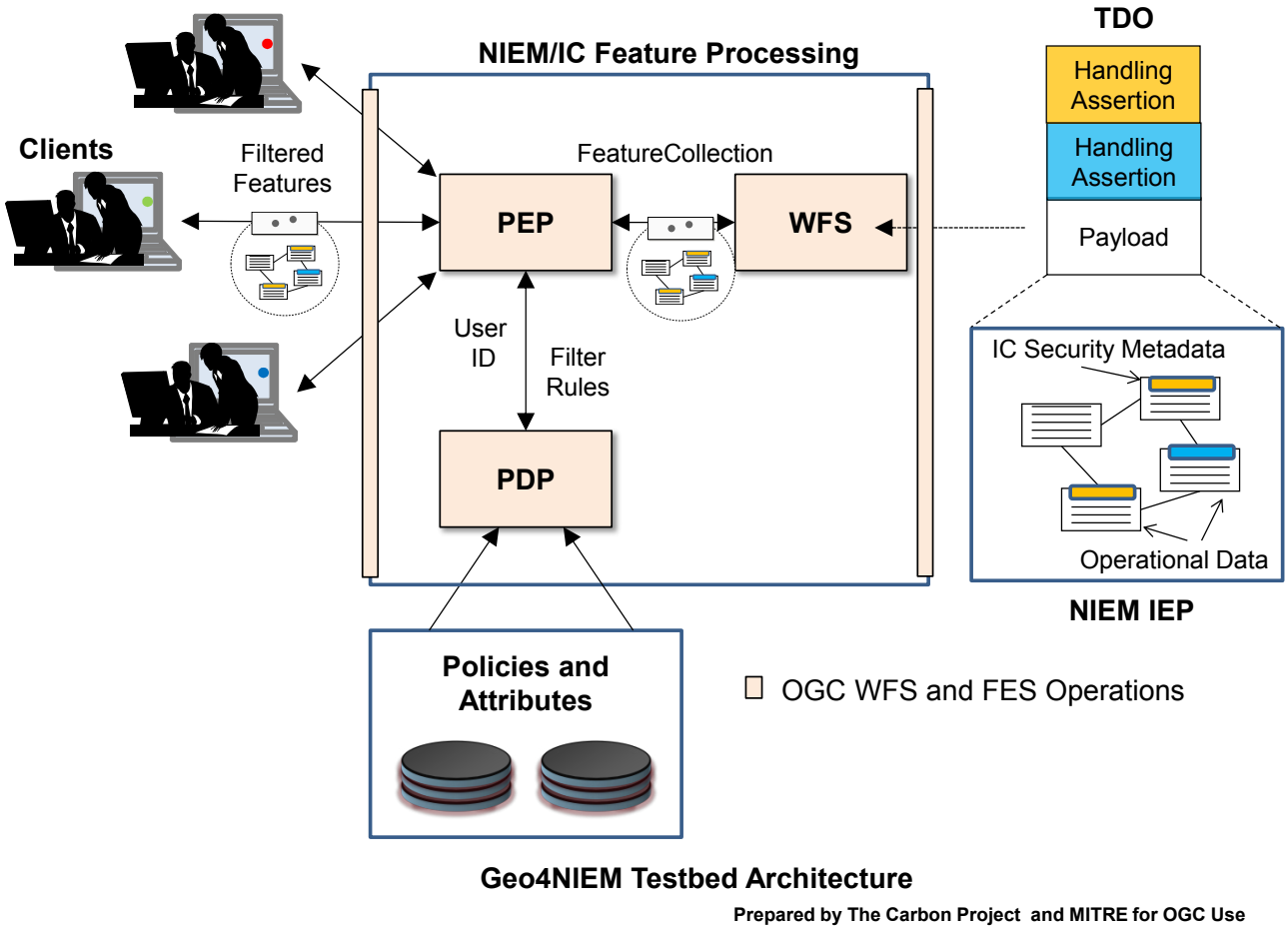


Figure 1 – Geo4NIEM Testbed Architecture [2]

For this testbed four service interfaces, encodings and information exchange frameworks were considered during testing and demonstration:

- IC Data Encoding & Service Specifications
- NIEM 3.0
- OGC Web Services, WFS

[2] User attributes created to support the Geo4NIEM Testbed 11 architecture were extended from the IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set (UIAS) to support fine-grained access control using NTK.

4.1 IC Data Encoding & Service Specifications

The success of intelligence, defense, homeland security, and law enforcement missions are dependent on information producers and consumers being able to share, manage, discover, retrieve, and access information across national and international boundaries. The IC Data Encoding Specifications (DES) are the result of IC collaboration and coordination in response to public law, executive orders, policy and guidance, and change requests submitted by IC elements. Data encoding specifications define agreed upon digital encodings or formats for information being shared or exchanged within the enterprise. These specifications should be viewed as component modules. Many of the specifications are tightly integrated and dependent on each other. They can be integrated into other data encoding specifications or profiled (i.e., configured or constrained) to achieve a particular mission or business objective - such as supporting security tagging within the NIEM.

While this flexibility exists, users of the IC Data Encoding Specifications are required to maintain conformance to the relevant specification. An instance document is considered conformant to an IC DES if it passes all of the normative validation steps. The IC DES XML schemas (unless noted otherwise) CVE values from the XML CVE files, and the Schematron code version of the constraint rules are normative for the specifications.

4.1.1 XML Data Encoding Specification for Information Security Marking (ISM) Metadata

The XML Data Encoding Specification (DES) for Information Security Markings (ISM.XML) defines detailed implementation guidance for using XML to encode Information Security Markings (ISM) metadata. This DES defines the XML attributes, associated structures and relationships, restrictions on cardinality, permissible values, and constraint rules for representing electronic information security markings.

4.1.2 XML Data Encoding Specification for Need-To-Know (NTK) Metadata

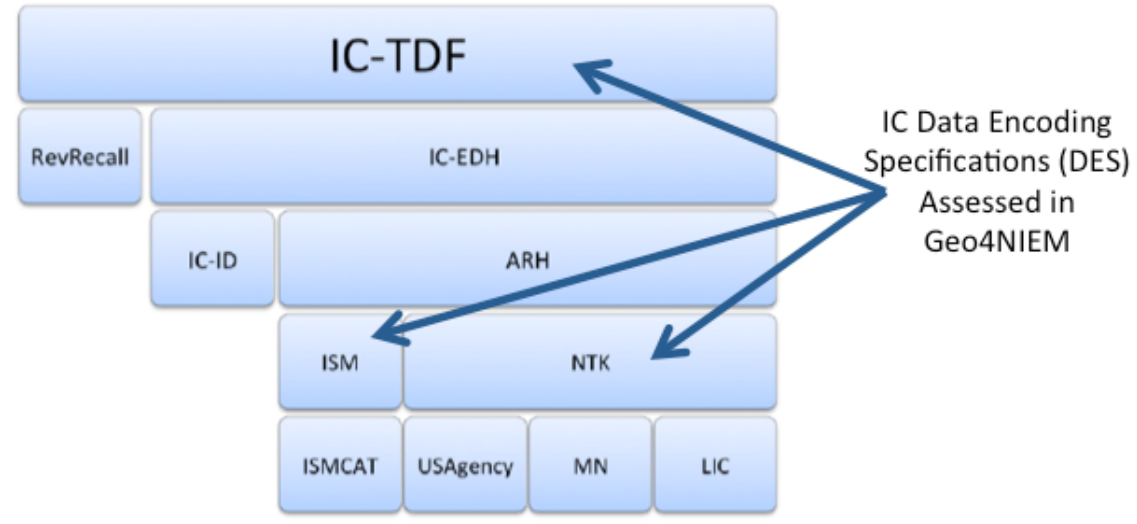
The XML Data Encoding Specification (DES) for Need-to-Know Metadata (NTK.XML) defines detailed implementation guidance for using XML to encode metadata necessary to facilitate automated systems making access control decisions. This DES defines the XML elements and attributes, associated structures and relationships, restrictions on cardinality, and permissible values for representing access control data concepts using XML.

The metadata, are used to represent the system-specific properties assigned to an information resource that will be used, in conjunction with information about the user, and possibly other information, to determine the user’s access to the data. A single information resource may include multiple occurrences of these metadata in order to specify access control information according to multiple, different access systems.

4.1.3 XML Data Encoding Specification for Trusted Data Format (TDF)

The XML Data Encoding Specification (DES) for Trusted Data Format (IC-TDF.XML) defines detailed implementation guidance for using XML to encode IC-TDF data. This Data Encoding Specification (DES) defines the XML elements and attributes, associated structures and relationships, mandatory and cardinality requirements, and permissible values for representing trusted data format data concepts using XML.

The Intelligence Community (IC) has standardized the various classification and control markings established for information sharing within the Information Security Markings (ISM), Need-To-Know (NTK), Enterprise Data Header (EDH), and Access Rights and Handling (ARH) XML specifications of the Intelligence Community Enterprise Architecture (ICEA) Data Standards. The IC-TDF.XML specification further expands on this body of work, adapting and extending it as necessary for TDF to function as the IC submission format for binding assertion metadata with data resource(s). This TDF functionality supports the IC way-ahead strategy of implementing secure cloud-based information exchange and discovery on the IC Enterprise



IC-TDF Dependencies[3]

The IC-TDF.XML specification has a consistent and simple concept of Assertions and Payloads. There are two options for root elements: Trusted Data Object (TDO) and

[3] Graphic provided by the Office of the Director of National Intelligence (ODNI) Office of the Chief Information Officer (OCIO) with annotations provided by Defense Information Systems Agency (DISA) and the NIEM Program Management Office (PMO).

Trusted Data Collection (TDC). A TDO contains some data (the payload) and some statements about that data (the assertions). In the context of TDF, an ‘assertion’ is defined as a statement providing handling, discovery, or mission metadata describing a payload, TDO, or TDC, depending on the scope of the assertion. To facilitate handling and access control decisions, each TDO and TDC must contain at least one Handling Assertion. A Handling Assertion is a special type of structured assertion that contains the IC Enterprise Data Header (EDH) for the TDO or payload, providing the attributes needed for policy decisions regarding access control and how the data must be handled. ISM and NTK markings are contained in Handling Assertions, as part of the Access Rights and Handling (ARH) block. Additional discovery and mission assertions may also be provided. A TDC contains a list of TDOs (the payload) and some statements about those TDOs (the assertions). A TDC may also be a collection of collections, and contain other TDCs.

Each TDO consists of one or more assertions and a payload. Assertions may optionally be cryptographically bound to the payload to provide assurance over the integrity of the assertion, the payload, and the relationship between the assertion and payload. Each IC-TDF requires at least one handling assertion, optional discovery and mission assertions, and a payload. The handling assertion must consist of a structured IC-EDH block. Mission specific metadata may consist of a structured block (XML) or unstructured data (binary). The payload may be structured XML, unstructured data, or a reference. A TDC consists of a collection of TDOs or TDCs. It is expected but not required that the child TDOs and TDCs within a TDC are in some way related, with relationships encoded in the TDC assertions.

Information sharing within the national intelligence enterprise increasingly relies on information assurance metadata to allow interagency access control, automated exchanges, and appropriate protection of shared intelligence. This requires a structured, verifiable representation of security metadata bound to the intelligence data in order for the enterprise to become inherently "smarter" about the information flowing in and around it. This representation when implemented with other data formats, improved user interfaces, and data processing utilities, can provide part of a larger robust information assurance infrastructure capable of automating some of the management and exchange decisions now requiring human involvement. These specifications are in operational usage outside of the IC currently for other missions such as Defense and Law Enforcement. In Geo4NIEM they were successfully applied to a disaster management scenario.

4.1.4 IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set (UIAS)

The IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set (UIAS) codifies the minimum set of enterprise-level authorization attributes

that IC elements are expected to provide if they participate in the Intelligence Community Unified Authorization and Attribute Service (UAAS) architecture. It provides a common, consistent way to identify IC enterprise authorization attributes of IC persons produced by, stored within, or shared throughout the IC's information domain. The name, definition, cardinality, and controlled vocabulary for each attribute are defined in order to promote interoperability between UAAS-compliant attribute services established by participating Agencies.

Defining the mandatory minimum set of IC enterprise authorization attributes and values for sharing through the IC UAAS federation supports consistent and assured information sharing across the enterprise. The IC UAAS supports Attribute-Based Access Control (ABAC) to promote on-demand access to information and other resources by IC users and services, and reduces authorization vulnerabilities by strengthening the access control decision process.

IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set (UIAS) specification is implemented by the OGC Attribute Store to define the user attributes used for the Testbed 11. While the UIAS specification codifies the minimum set of enterprise-level authorization attributes that IC elements are expected to provide if they participate in the Intelligence Community Unified Authorization and Attribute Service (UAAS) architecture, Testbed 11 applies the specification to state and local emergency responder participants. These attributes are explicitly used as parameters for access to the data assets tagged with NTK.XML.

4.2 NIEM 3.0

NIEM is a standards-based approach to the design of structured information exchange specifications. Figure 2 illustrates the process, which is described in reverse order (right to left) as follows: Producer and consumer software applications exchange structured information in the form of XML documents known as information exchange packages (IEPs). Developers of that software understand the expected content of those IEPs by understanding the exchange specification, which in NIEM is called an information exchange package documentation (IEPD). The designers of the IEPD follow the NIEM process, reusing data components from the NIEM data model and extending their exchange with new components as needed. The NIEM community [3] creates shared data components for those concepts on which they can agree and for which they believe a common definition will be useful.

An IEPD consists of a minimal but complete set of artifacts (XML schemas, documentation, sample XML instances, etc.) that defines and describes an implementable NIEM information exchange. A complete and conforming IEPD will contain all the schema definitions and instructional material necessary to:

- Understand information exchange content, semantics, and structure.
- Create and validate information exchanges defined by the IEPD.
- Identify the lineage of the IEPD and optionally its artifacts.

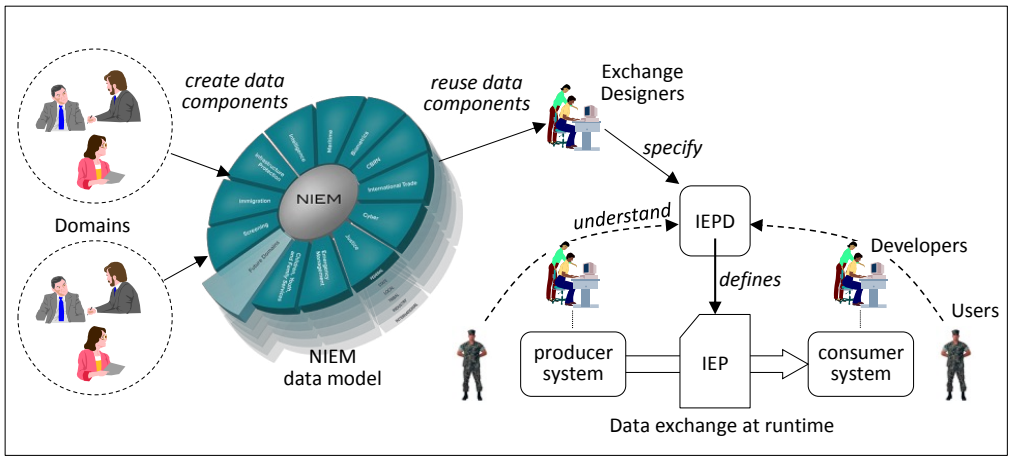


Figure 2 - The NIEM Process

4.3 Web Feature Service (WFS)

The OGC Web Feature Service (WFS) Implementation Specification allows a client to retrieve geospatial data encoded in Geography Markup Language (GML) from multiple Web Feature Services. The standard defines interfaces for data access and manipulation operations on geographic features, using HTTP as the distributed computing platform. Via these interfaces, a Web user or service can combine, use and manage geodata -- the feature information behind a map image -- from different sources. A Transactional Web Feature Service allows a client to send messages relating to making changes to a geospatial database.

4.4 Testing Process – Pre-Security TIEs

The first step in testing was to establish a 'Pre-Security' Technology Integrations Experiments (TIEs). The TIEs consisted of a cloud-based test WFS from The Carbon Project and Policy Enforcement Points (PEPs) from multiple Testbed Participants including Secure Dimensions, con terra and Jericho Systems, with no security tagged

NIEM/IC Data Encodings. The purpose of the Pre-Security TIEs were to ensure data flows functioned properly before implementing a stringent filtering regime with security tagged NIEM/IC Data. Multiple client applications were implemented to test connection to the services including Gaia, QGIS, FME and Web Clients from The Carbon Project.

The Pre-Security TIE environment is shown in the representational flow diagram below.

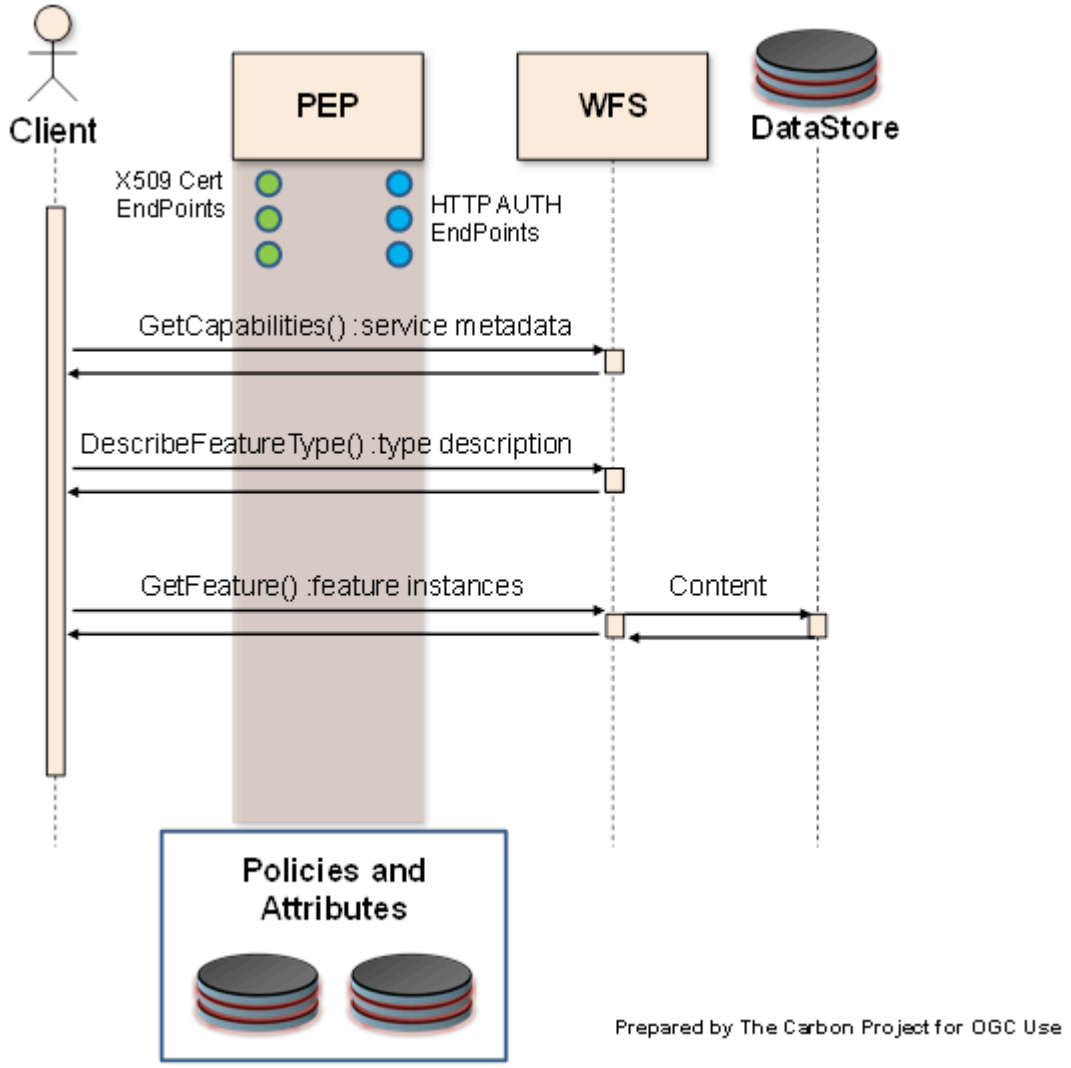


Figure 3 – Pre-Security TIE Flow Diagram

Hands-on collaborative engineering yielded the following set of results summarized in the figure below. No major issues were noted during testing and examples of the Pre-Security TIE results with non-security tagged data over San Francisco are shown in the

flow diagrams below. Please note some clients implemented HTTP AUTH only when connected to PEPs.

Component	CC WFS	OGC IdP	ct PEP	JS PEP	SD PEP
con terra PEP	S	S *			
Jericho Systems PEP	S				
Secure Dimensions PEP	S	S *			
Gaia Client	S		S	S	F
QGIS Client	S		S	S	S
ArcGIS Client					
FME Client	S		S	S	F
Web Browser Client	S				

Legend:
S - Successful Test Complete
F - Test Fail
R - Remediation
N - Not Tested

* - see post-security tag filtering tie

Figure 4 - Results of Pre-Security TIEs

Primary client applications tested in the pre-security environment included Gaia desktop client, CarbonCloud web client, QGIS desktop client and FME. Results of this testing with data from the city of San Francisco are shown below. Direct connection to the WFS instance was also tested using multiple client applications including desktop and web applications shown below.

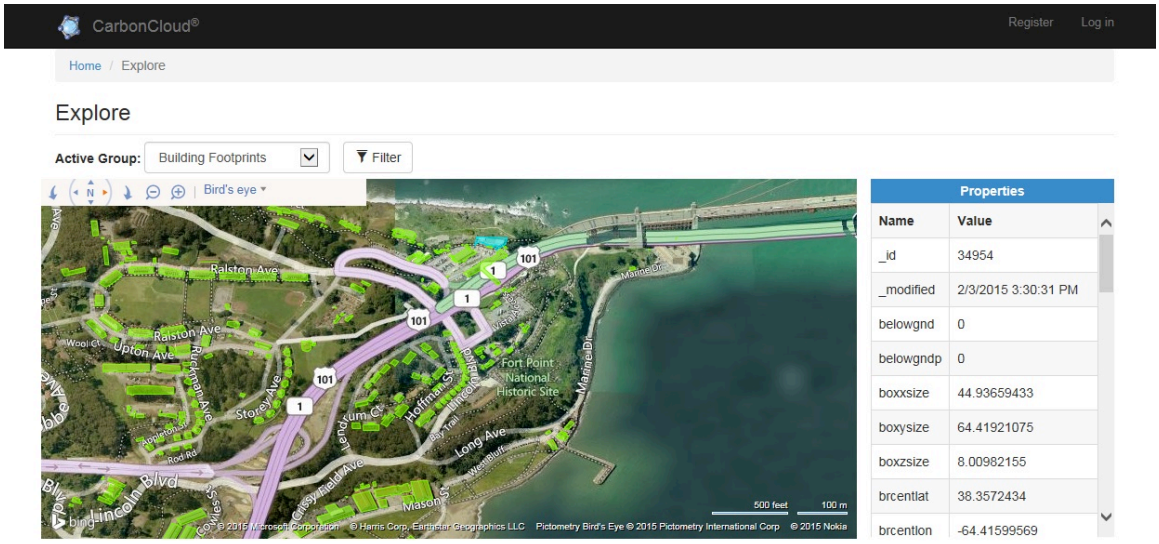


Figure 5 - Web Client from The Carbon Project connecting to Pre-Security WFS with Building Footprint Data

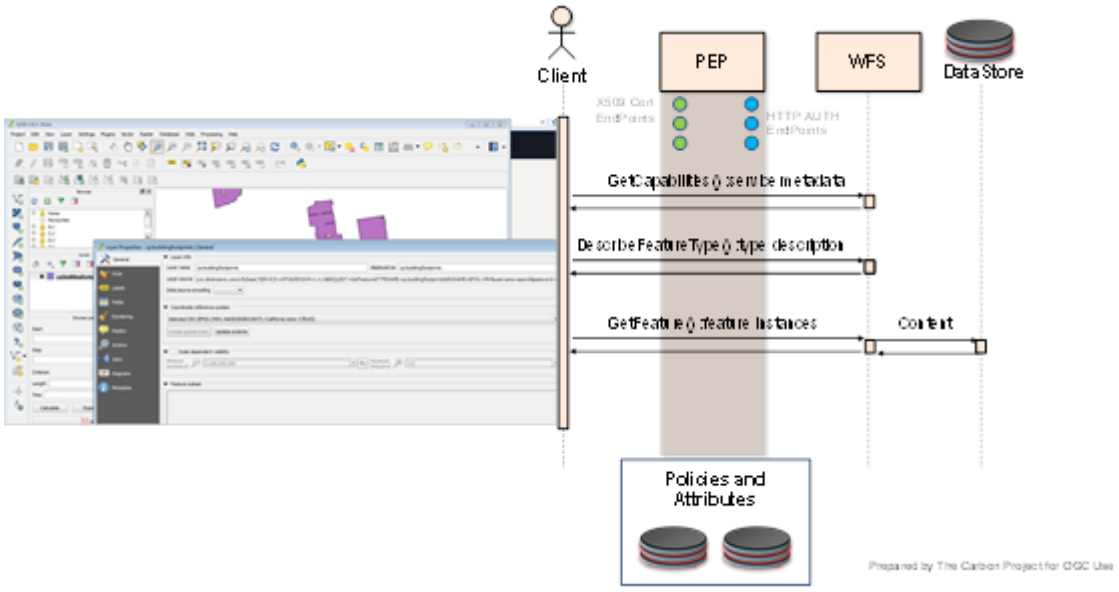


Figure 6 - QGIS connecting to Secure Dimensions, con terra and Jericho Systems PEPs and Pre-Security WFS

4.5 Testing Process – Post-Security TIEs

The next step in testing was to add Trusted Data Objects (TDO), especially IC Security Markings (ISM) and Need to Know (NTK) security tags, to the NIEM IEP documents. An example of a NIEM/IC IEP with security tags is provided as Annex A. The security-tagged NIEM/IC Data Encoding was then loaded into a cloud-based server and provided as GML feature geometries through an OGC WFS-T. This process is summarized in the Figure below and discussed in detail in other Testbed 11 reports.[4] An example of a NIEM/IC Data Encoding with security tags is provided as Annex B.

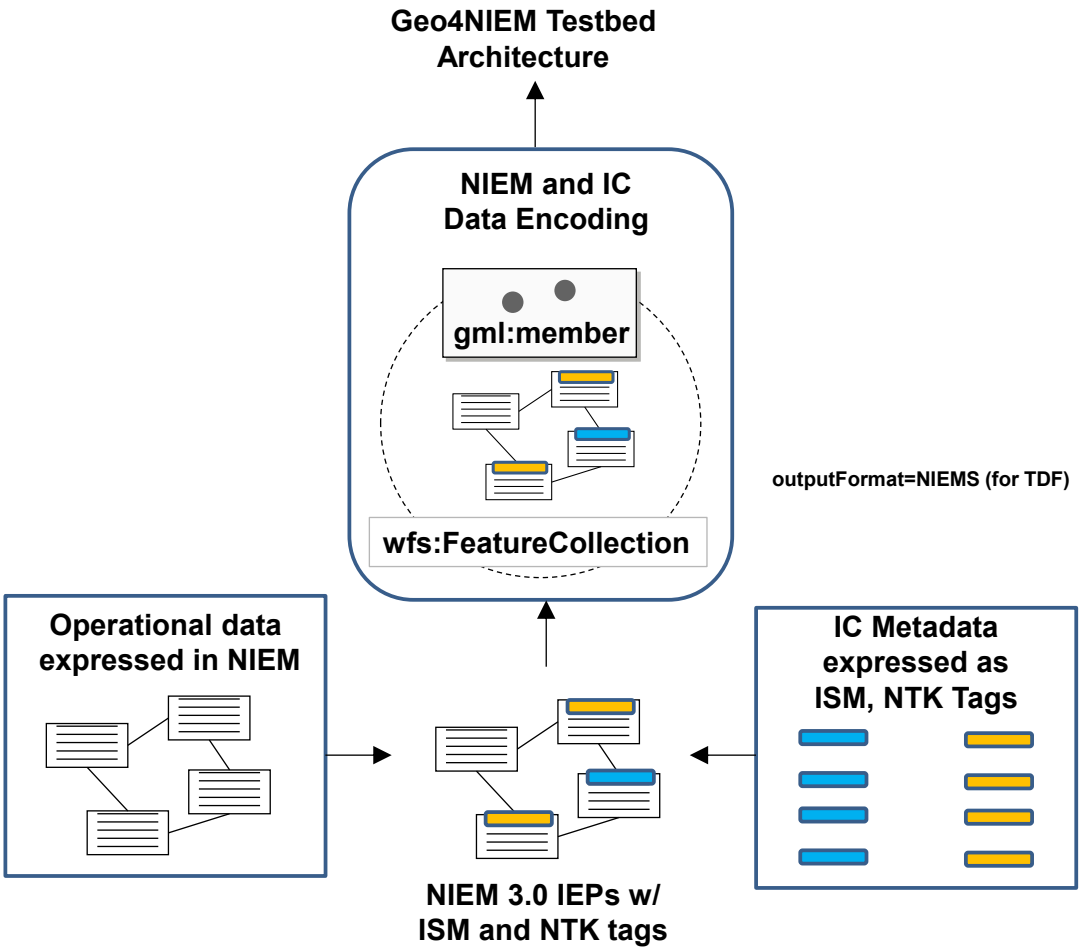


Figure 7 – Converting NIEM IEP with ISM/NTK tags into wfs:FeatureCollections

[4] See OGC IP ERs 15-047 and 15-048

To support flexibility, guiding principles were applied to the development of the NIEM/IC Data Encoding. For example, it must support multiple namespaces and complex nested schema. It must also be discoverable, self-describing and support interactive query and update. Finally, it must support multiple security tagged IEP instance documents. The OGC Web Feature Service – Transactional (WFS-T) was selected as a template to test the NIEM/IC Data Encoding since it supports all these principles.

Using these principles and WFS-T as a template, the project assessed two ways of delivering the data encoding:

- NIEM IEP containing ISM and NTK metadata as a member of wfs:FeatureCollection (called the 'NIEM/IC WFS')

- NIEM IEP with ISM and NTK metadata, appearing as the structured payload in a TDO, which in turn is a member of wfs:FeatureCollection. (This encoding was made available via the outputFormat parameter called 'NIEMS')

This approach provided the NIEM/IC WFS as a default option since it was assessed this model may be more readily handled by server and client applications during initial testing. Three IEPs were converted, Notice of Arrival, Incident and Resource, into NIEM/IC wfs:FeatureCollection and tested during hands-on collaborative engineering. From that engineering a set of candidate rules were developed to guide the development of NIEM/IC Data Encoding in an environment where there may be hundreds of potential IEP instance documents, each with security tags. These rules are summarized in separate Engineering Reports.

The Post-Security TIEs were conducted by implementing prototype components that use NIEM/IC Data Encodings in a functional test environment. Access control was conducted via one of several Policy Enforcement Points that filter based upon the user attributes stored in the OGC Attribute Store (discussed below).

4.5.1 Access Control Frameworks

A key consideration at this phase in the project was describing the implementation of various ISM and NTK metadata in NIEM/IC Data Encodings and Service API. A key principal was that many different access control frameworks may be implemented on NIEM/IC Data Encodings and Services. Common in these approaches is the need to specify, maintain and manage roles, groups and policies in a NIEM-IC information exchange – for secure data exchange. By specifying Roles, ntk:AccessGroups, ism:classification and AccessPolicy PEPs, leveraging attributes defined in alignment of UIAS, can grant access to geospatial information exchange resources to some users,

limited kinds of access to other users, and completely deny access to yet another set of users.

Each access control rule implemented by a different PEP grants (or denies) requests made by an individual or group of individuals, possibly depending on details associated with the request. Referring to one or more web services, rules can specify, for a given set of users, the conditions under which access is to be granted to them. A user can be associated with roles within an organization or with a group whose membership is known throughout the system.

The responsibility for implementing this access control is delegated to the PEP in this prototype NIEM/IC information exchange. NIEM/IC API responses and response pass through the PEPs, and each access control rule implemented by different PEPs grants (or denies) requests made by an individual or group of individuals, depending on the Roles, ntk:AccessGroups, ism:classification and AccessPolicy associated with the user making the request.

In addition, because rules will refer to user roles and names, security within the NIEM/IC information exchange test and demonstration implementation provides a way to name users and mechanisms to manage user identities, including the means by which users can be authenticated. A person is authenticated and assumes an identity by demonstrating knowledge of a secret (such as a password), or possession of some other information, that is associated with that identity.

NIEM/IC information exchange has a flexible authentication framework that supports multiple authentication methods. To authenticate a user known to an organization, and uses systems already used to authenticate users. This allows an organization to use existing authentication methods. For example, a user might be authenticated at an organization by providing a username/password (HTTP AUTH) that is recognized in the organization, or via X.509 certificates.

Key within this test and demonstration implementation is the OGC Attribute Store. The OGC Attribute Store implements the IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set (UIAS) specification. The specification documents a set of IC enterprise identity attributes and associated values that are required for participation in Intelligence Community Unified Authorization and Attribute Service (UAAS) architecture. Information about user and role assignment is stored in an LDAP. The data can be accessed via the OGC IdP Attribute Service interface.

With this access control framework in place the project also assessed how the principals of Attribute Based Access Control (ABAC) may be applied to NIEM/IC information exchange. ABAC is an access control method where subject requests to perform operations on objects are granted or denied based on assigned attributes of the subject, assigned attributes of the object, environment conditions, and a set of policies that are specified in terms of those attributes and conditions. Attributes are characteristics of the subject, object, or environment conditions. Attributes contain information given by a

name-value pair. A subject is a human user or NPE, such as a device that issues access requests to perform operations on objects. Subjects are assigned one or more attributes. An object is a system resource for which access is managed by the ABAC system, such as devices, files, records, tables, processes, programs, networks, or domains containing or receiving information. An operation is the execution of a function at the request of a subject upon an object. Operations include read, write, edit, delete, copy, execute, and modify. Policy is the representation of rules or relationships that makes it possible to determine if a requested access should be allowed, given the values of the attributes of the subject, object, and possibly environment conditions.[5]

The Post-Security TIE environment is shown in the representational flow diagram below.

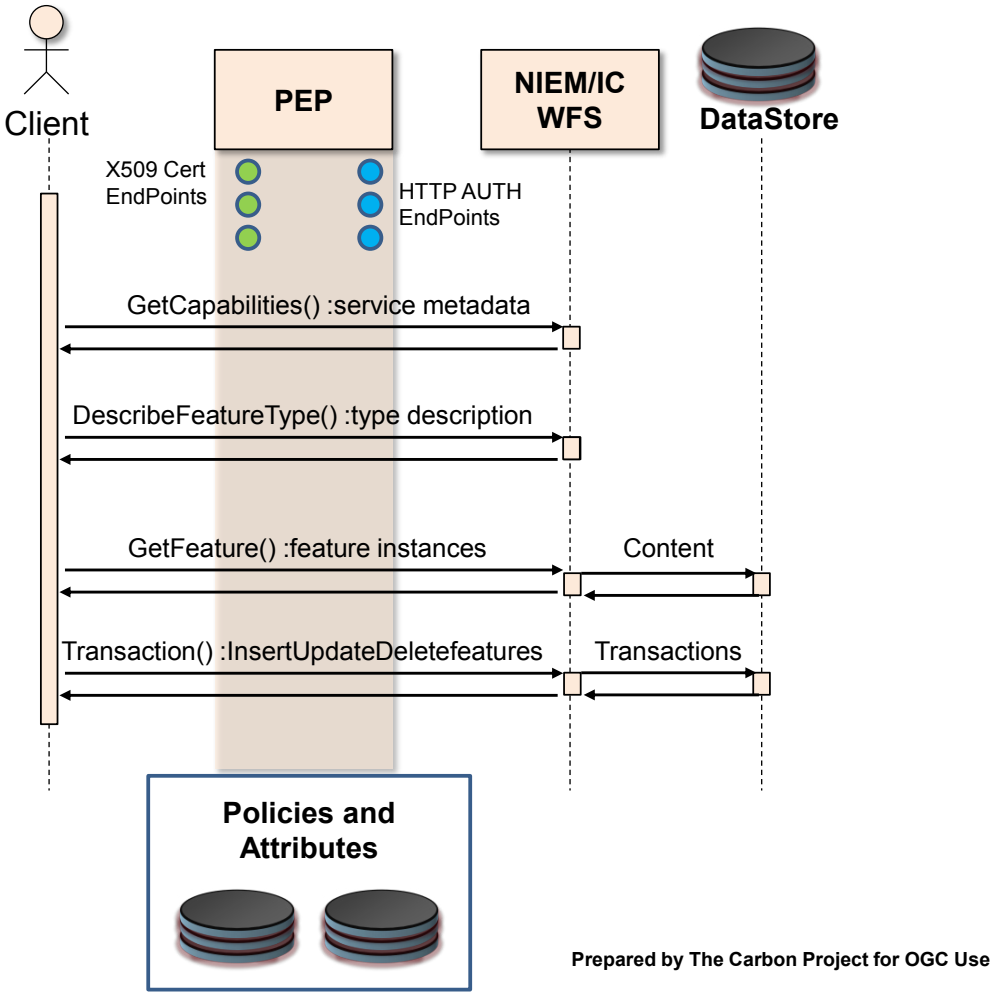


Figure 8 – Post-Security TIE Flow Diagram

[5] Guide to Attribute Based Access Control (ABAC) Definition and Considerations
http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf

4.5.1.1 OGC Attribute Store

Key within the 'Post-Security' test and demonstration implementation was the OGC Attribute Store (OAS) for Policies and Attributes. Information about user and role assignment was stored in an LDAP directory, and the data was accessed via the OGC IdP Attribute Service interface. The following LDAP entries for PEP/PDP/PIPs were created using first initial and last name of Testbed 11 Participants as shown below:

```
---> uid=amatheus
---> uid=jdrewnak
---> uid=jtolbert
---> uid=mqueralt
---> uid=rgartmann
---> uid=tschmoyer
```

The test and demonstration simulated users representing actors in the scenario Use Cases were:

```
---> uid=apond | cn=Amy Pond
---> uid=asmith | cn=Anna Smith
---> uid=dbrown | cn=Daniel Brown
---> uid=jdoe | cn=Jane Doe
---> uid=mhess | cn=Mark Hess
---> uid=tjacobs | cn=Tim Jacobs
---> uid=kandrews | cn=Kristen Andrews
---> uid=ematthews | cn=Eric Matthews
---> uid=bjones | cn=Bill Jones
---> uid=drose | cn=Dave Rose
```

To connect through the x509 secured endpoints, applications had the option to install valid user certificates in their browser. The following sample URLs were used to download certificates for the demonstration users described above:

http://geo4niem.opengeospatial.org/ssl/apond.p12

http://geo4niem.opengeospatial.org/ssl/asmith.p12

http://geo4niem.opengeospatial.org/ssl/dbrown.p12

http://geo4niem.opengeospatial.org/ssl/jdoe.p12

http://geo4niem.opengeospatial.org/ssl/mhess.p12

http://geo4niem.opengeospatial.org/ssl/tjacobs.p12

http://geo4niem.opengeospatial.org/ssl/kandrews.p12

http://geo4niem.opengeospatial.org/ssl/ematthews.p12

A sample of the attributes for one of the demonstration users is shown below:

```
# Entry 12: cn=Tim Jacobs,dc=opengeospatial,dc=org
dn: cn=Tim Jacobs,dc=opengeospatial,dc=org
adminorganization: SLT
aicp: FALSE
clearance: U
cn: Tim Jacobs
countryofaffiliation: US
digitalidentifier: cn=Tim Jacobs,ou=SolanoOES,o=Solano
County,c=US
dutyorganization: SLT
entitytype: GOV
fineaccesscontrols: Restricted
isicmember: FALSE
mail: tjacobs@geo4niem.example.com
o: Solano County
objectclass: organizationalPerson
objectclass: geo4NIEMAccessControl
objectclass: inetOrgPerson
ou: SolanoOES
role: SEMS-CA-Msn-SolanoCounty-MAC
sn: Jacobs
uid: tjacobs
```

The OGC Attribute Store also stored information about valid values for security Clearance and Roles in the Geo4NIEM Test and Demonstration scenario, shown below:

Valid Values for Clearance
U
C
S
TS

Valid Values for Role
SEMS-CA-Msn-ContraCostaCounty-MAC
SEMS-CA-Msn-SolanoCounty-MAC
SEMS-CA-Ent-StateOperationsCenter-MAC
SEMS-CA-Ent-CoastalRegion-MAC
SEMS-CA-Ent-InlandRegion-MAC
NIMS-FEMA-Msn-RegionIX-ICS
MDA-USCG-Msn-District11-ROC
RedCross-EmergencyResponder-05332
HomeDepot-EmergencyResponder

Figure 9 - Sample Clearance and Role information used in Geo4NIEM Testing and Demonstration

4.5.1.2 Filter Rules

In the Testbed 11: Geo4NIEM thread, participants assessed multiple aspects of IC Security Markings (ISM) and Need to Know (NTK) tagging and how to provide appropriate access control to information served through an OGC Web Feature Service – Transactional. The access control was conducted via one of several Policy Enforcement Points that filter based upon the user attributes that are stored in the OGC Attribute Store.

The user attribute categories that are stored for the demonstration users are listed in section Table 1 in the figure below. The attributes that were filtered on were Clearance, Role, and possibly EntityType.

LDAP Store	SAML Attribute Name	SAML Friendly Name
CountryOfAffiliation	urn:ogc:def:testbed11:geo4niem:countryofaffiliation	CountryOfAffiliation
FineAccessControls	urn:ogc:def:testbed11:geo4niem:fineaccesscontrols	FineAccessControls
AICP	urn:ogc:def:testbed11:geo4niem:aicp	AICP
DigitalIdentifier	urn:ogc:def:testbed11:geo4niem:digitalidentifier	DigitalIdentifier
Role	urn:ogc:def:testbed11:geo4niem:role	Role
EntityType	urn:ogc:def:testbed11:geo4niem:entitytype	EntityType
DutyOrganization	urn:ogc:def:testbed11:geo4niem:dutyorganization	DutyOrganization
Clearance	urn:ogc:def:testbed11:geo4niem:clearance	Clearance
AdminOrganization	urn:ogc:def:testbed11:geo4niem:adminorganization	AdminOrganization
isICMember	urn:ogc:def:testbed11:geo4niem:isicmember	isICMember

Figure 10 - User Attribute Categories for the test and demonstration users

4.5.1.2.1 Authentication Methods

The method of security authentication that a client performs was the first criteria for access control. If a client uses no authentication (ie a web browser with no login), the access to all capabilities and features from the protected WFS was denied [deny all].

Should the client use HTTP Basic Authentication to the PEP and that user is validated against the OGC Attribute Store, the access to all capabilities from the protected WFS was allowed [allow all]. Features from the protected WFS were filtered based on the filtering rules.

Clients with HTTP Basic Authentication over TLS to the PEP, and validated against the OGC Attribute Store, should be given the access to all capabilities from the protected WFS [allow all]. Features from the protected WFS should be filtered based on the filtering rules.

4.5.1.2.2 Clearance maps to classification and filtering

Trusted Data Objects (TDO) were added to the NIEM IEPs for this project, along with geospatial feature geometries for testing. Each document included an “ism:classification” attribute in the TDO headers, as well as, nested in various tags throughout the rest of the document. Generally, the TDO header information in the <tdf:HandlingAssertion> tags should be unclassified, meaning all viewers of the document can see those portions. Any tag in the document payload or <tdf:StructuredPayload>, and all of its children tags

should be filtered from being sent to the client based upon the “ism:classification” attribute for that tag.

The most restrictive classification was TS (Top Secret), followed in order by, S (Secret), C (Confidential), and followed lastly with the least restrictive classification of Clearance being: U (Unclassified).

An example of a <tdf:StructuredPayload> is shown below. Notice that the classification attribute in the mda:noticeofarrival tag is equal to "C" (line 9). This is the roll-up from the entire payload. Any Classification markings anywhere below this tag (lines 12 and on) should be identified and filtered based upon the user attributes. If the user is "Unclassified", lines 26 through 36 should be stripped, but line 37 would remain.

```
1                <mda:noticeofarrival
2                   xmlns:mda="http://release.niem.gov/niem/domains/maritime/3.0/mda/"
3                   xmlns:ntk="urn:us:gov:ic:ntk" xmlns:ism="urn:us:gov:ic:ism"
4                   xmlns:nc="http://release.niem.gov/niem/niem-core/3.0/"
5                   xmlns:mda-codes="http://release.niem.gov/niem/domains/maritime/3.0/mda/codes/"
6                   xmlns:m="http://release.niem.gov/niem/domains/maritime/3.0/"
7                   xmlns:geo="http://release.niem.gov/niem/adapters/geospatial/3.0/"
8                   ntk:DESVersion="9" ism:DESVersion="11" ism:ownerProducer="USA"
9                   ism:classification="C" ism:resourceElement="true" ism:classifiedBy="USCG"
10                 ism:classificationReason="Classified due to sensitive maritime security information."
11                 ism:declassDate="2050-12-01" fid="noticeofarrival.1">
12                   <mda:Voyage ism:ownerProducer="USA" ism:classification="U">
13                      <m:VoyageCategoryText>Foreign to US</m:VoyageCategoryText>
14                      <m:VoyageIdentification>
15                           <nc:IdentificationID>1</nc:IdentificationID>
16                       </m:VoyageIdentification>
17                       <mda:VoyageClosedLoopIndicator>false</mda:VoyageClosedLoopIndicator>
18                   </mda:Voyage>
19                   <mda:Vessel ism:ownerProducer="USA" ism:classification="U">
20                       <m:VesselAugmentation ism:ownerProducer="USA" ism:classification="U">
21                           <m:VesselCallSignText>H3LP</m:VesselCallSignText>
22                           <m:VesselCargoCategoryText>Harmful
23                               Substances</m:VesselCargoCategoryText>
24                           <m:VesselCategoryText>Container Ship</m:VesselCategoryText>
25                           <mda:VesselCDCCargoOnBoardIndicator>true</mda:VesselCDCCargoOnBoardIndicator>
26                           <mda:VesselCharterer ism:ownerProducer="USA" ism:classification="C"
27                               ntk:access="#Roles|Group^MDA-USCG-Msn-District11-ROC">
28                               <nc:EntityOrganization>
29                                   <nc:OrganizationLocation>
30                                       <nc:Address>
31                                           <nc:LocationCountryISO3166Alpha2Code>KR</nc:LocationCountryISO3166Alpha2Code>
32                                       </nc:Address>
33                                   </nc:OrganizationLocation>
34                                   <nc:OrganizationName>SK Shipping</nc:OrganizationName>
35                               </nc:EntityOrganization>
36                           </mda:VesselCharterer>
37                           <m:VesselClassText>Bulk Carrier</m:VesselClassText>
```

4.5.1.2.3 ism:classification="TS"

In filtering a document based on the “Clearance” attribute, the user with a user attribute of Clearance equal to TS can see all tags and information that are contained in a document that is not filtered out by any of the other filters.

4.5.1.2.4 ism:classification="S"

A user with a user attribute of Clearance equal to “S” can see all tags and information that are contained in a document, after all ism:classification=”TS” tags have been removed, and that are not filtered out by any of the other filters.

4.5.1.2.5 ism:classification="C"

A user with a user attribute of Clearance equal to “C” can see all tags and information that are contained in a document, after all ism:classification=”TS” and ism:classification=”S” tags have been removed, and that are not filtered out by any of the other filters.

4.5.1.2.6 ism:classification="U"

A user with a user attribute of Clearance equal to “U” can see all tags and information that are contained in a document, after all ism:classification=”TS”, ism:classification=”S”, and ism:classification=”C” tags have been removed, and that are not filtered out by any of the other filters.

4.5.1.2.7 Role maps to ntk:access="#Roles|Group”

Roles in the OGC Attribute Store were one-to-one. Each user only had at most one role.

Each document included an <ntk:Access /> tag and various <ntk:AccessGroup /> and <ntk:AccessGroupValue /> information in the TDO headers, as well as nested in various tags throughout the document. Any tag in the document payload, and all of its children tags, should be filtered from being sent to the client based upon the ntk:access="#Roles|Group^{role list}" attribute for that tag. These role attributes are specific and need exact pattern match to allow the tag and its children to pass. *More specifically, if a tag has a ntk:access attribute that does not match exactly the user attribute Role, then that information should not be sent to the client.*

4.5.1.2.8 EntityTypes

The EntityTypes were not coded into the IEPs and therefore, the project tested these rules to see how external attribute filters could work. For example, all the Government users in the OGC Attribute Store might have a larger need to know than say an NGO or a private company employee (here codified as PVT). There are examples in the past, during

disaster response, where agencies like FEMA have allowed NGOs or even private companies special access to critical information to allow for a better response.

If a user has a valid OGC Attribute Store record and is listed as EntityType of NGO or PVT, the system should filter on classification for their Clearance, but disregard their Role. This filter would require the Role filter to read the user attribute Role as a wildcard.

4.5.1.2.9 Geospatial Filtering

Several scenarios were tested where the system provided or denied access based upon the simulated location of the client. In these tests the Carbon Project web client passed a location (lat/lon) to the PEP. By comparing the location with an allowed polygon, if the client is in the polygon(s), access was allowed, based upon the filtering rules. If the client is outside the polygon(s) all access should be denied, based upon the filtering rules.

The location header, or GeoHeader, followed this format:

```
Location: <gml:Point xmlns:gml="http://www.opengis.net/gml"
gml:id="TownHallSF" srsName="EPSG:4326"><gml:pos
srsDimension="2">37.77925 -122.419222</gml:pos></gml:Point>
```

or

```
Location: <gml:Point xmlns:gml="http://www.opengis.net/gml"
gml:id="WashingtonMonument" srsName="EPSG:4326"><gml:pos
srsDimension="2">38.889444 -77.035278</gml:pos></gml:Point>
```

4.5.1.3 Results of Post-Security TIEs

Using the Access Control Frameworks discussed above, the TIEs consisted of a cloud-based test WFS from The Carbon Project and PEPs from multiple Participants including Secure Dimensions, con terra and Jericho Systems, with no security tagged NIEM/IC Data Encodings. The purpose of the Post-Security TIEs were to ensure data flows functioned properly before implementing a stringent filtering regime with security tagged NIEM/IC Data. Multiple client applications were implemented to test connection to the services including Gaia, QGIS, FME and Web Clients from The Carbon Project. Hands-on collaborative engineering yielded the following set of results summarized in the figure below:

Component	CC WFS	OGC <nop>IdP	ct PEP	JS PEP	SD PEP
con terra PEP		S			
Jericho Systems PEP					
Secure Dimensions PEP		S			
Gaia Client	S		NT	NT	
QGIS Client	NT		NT	NT	
<nop>ArcGIS Client					
FME Client	R		N	S	R
Web Browser Client	S		S	S	NT

Legend:
S - Successful Test Complete
F - Test Fail
R - Remediation
N - Not Tested

Figure 11 - Results of Post-Security TIEs

5 Demonstration

The work done in the Geo4NIEM thread and benefits gained by the technology were demonstrated in simulated real-world scenarios. This section describes the Use Cases and Demonstration results.

5.1 Scenario

To support national climate-change preparedness OGC's Testbed 11 demonstrated technology based on the scenario of spatial information needed when a population is displaced due to coastal inundation. To support this objective the Testbed 11 Demonstration Scenario was coastal flooding in densely populated region.

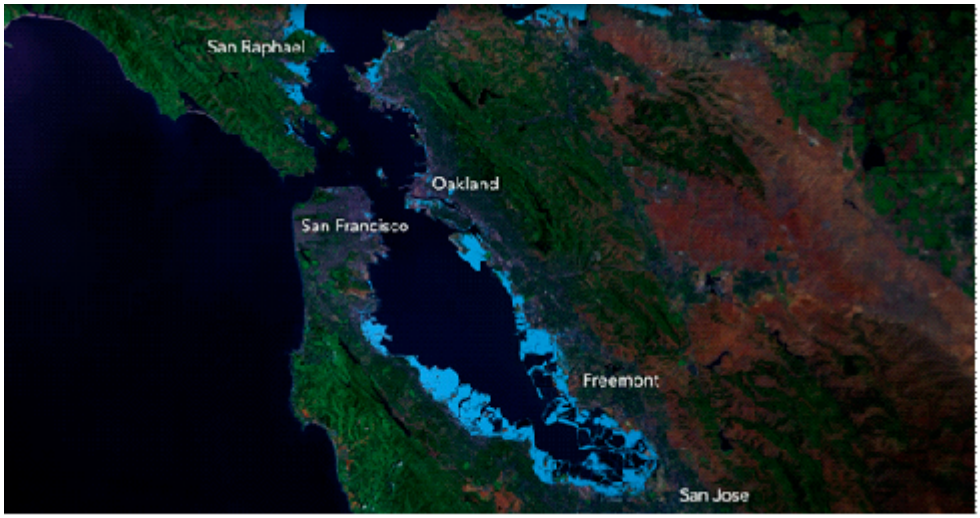


Figure 12 - Testbed 11 Demonstration Scenario: Coastal flooding in densely populated region

In this environment many communities need to coordinate, including:

- First Responders
- Law Enforcement
- Emergency Management
- Govt Decision Makers
- NGOs
- Military Support Personnel
- Intelligence Community

5.2 Geo4NIEM Use Cases

The vignettes below are the portions of the June 4th Testbed Demonstration at the OGC Boulder TC meeting. Those demonstrations were used to explain work done in the Geo4NIEM thread.

5.2.1 Use Case #2 – Maritime Domain Awareness Event

Use Case #2 – Maritime Domain Awareness event by Port Authority, USCG and civilian merchant vessels to sortie from San Francisco Harbor/Bay in view of increasing flooding and impending tropical storm.

Title: San Francisco Port Authority advises seaworthy merchant vessels to sortie from SF Bay for open ocean or safe havens.

Description: Using the National Information Exchange Model (NIEM 3.0) the Maritime Domain Awareness packages augmented with geospatial location using OGC GML and Information Communities Security Markings for Role-based Access Control, the United States Coast Guard queries the NIEM conformant information exchange Notice of Arrival messages to determine what vessels are scheduled to be in the Bay Region within the next two weeks.

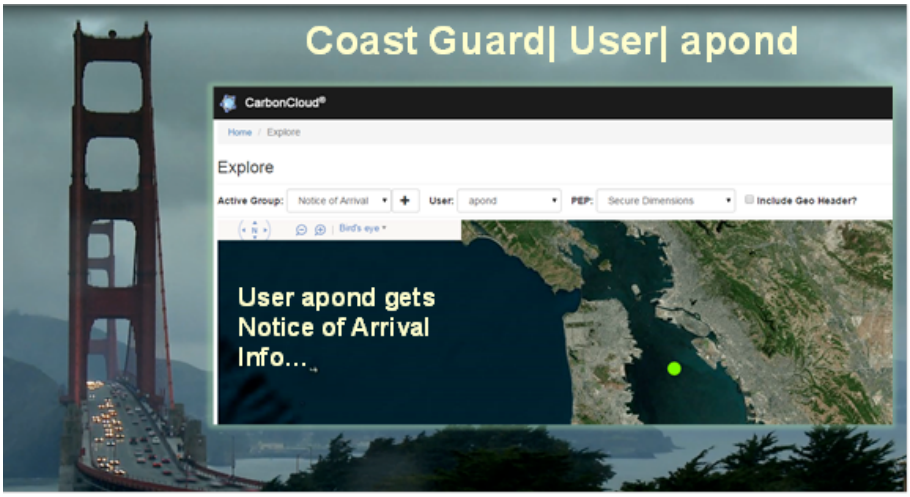
By including GML features into NIEM 3.0, and serving these messages via an OGC Web Feature Service, spatial and other filters can be invoked to receive a list of vessels that will be within the region (and with certain criteria). This allows the Port Authority to focus in on the ships that they really need to work with to get them to a safe position.

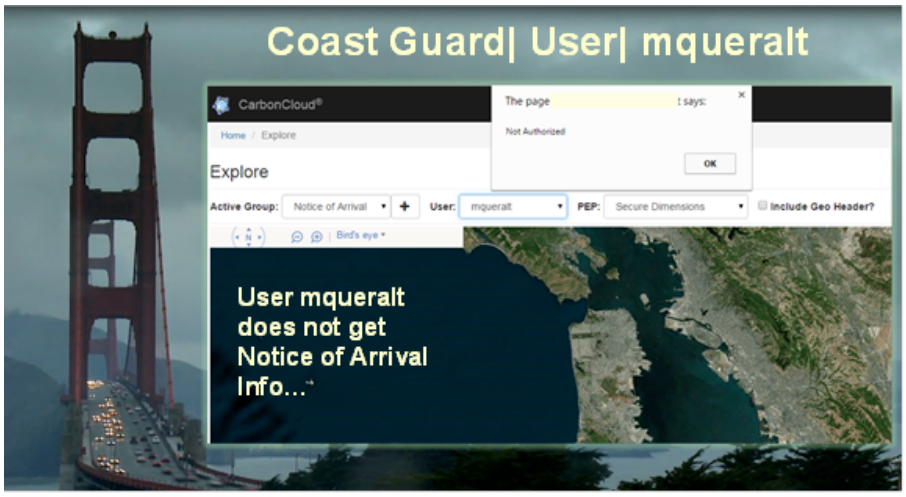
Some of the Notice of Arrival information is classified such as cargo type, some of this information might even be "top secret", and the system cannot pass this information around to others, especially for cross-jurisdictional purposes, but they do need the minimum set of information for each feature in question.

In order to accomplish this, Participants tagged the message fields with security tags that are filtered through the security policy enforcement points that are proxying the Web Feature Server. These PEPs are checking the attribute store to provide that role-based access based upon OASIS's SAML specification. Some PEPs are able to limit or allow access based upon the geographic location of the user.

5.2.1.1 Geo4NIEM Use Case 2 – Demonstration Example

The following examples provide a brief overview of the Testbed 11 Geo4NIEM demonstration Use Case #2, Maritime Domain Awareness, as described above.





5.2.2 Use Case #4 - Mutual Aid / Evacuation

Use Case #4 - Mutual Aid / Evacuation of municipal hospital by National Guard air assets and coordination with local air traffic control

Title: Evacuation of a municipal hospital requiring mutual aid and National Guard

Description: Here we are using NIEM 3.0 for Mutual Aid and the Incident and Resource messages to provide situational awareness for cross-jurisdictional information sharing. The messages that are being exchanged through the OGC Web Feature Service – Transactional, and have OGC GML features and Information Communities security markings. Again the messages are being filtered to provide only the appropriate level of classified data based upon the users security attributes.

Due to the flooding in the area and the proximity to the bay, the area around Pier 90 has lost power, Pacific Gas and Electric has been spread thin, units are coming from other states to help, but it is estimated to be days before crews can restore power to this sector. It is now reported that the backup generator at the Bayview Child Health Center has blown and its patients are in need of immediate evacuation. Eighteen of the 46 beds are in need of Air Medivac. The Hospital shares one Lifeline Helicopter with the California Pacific Medical Center.

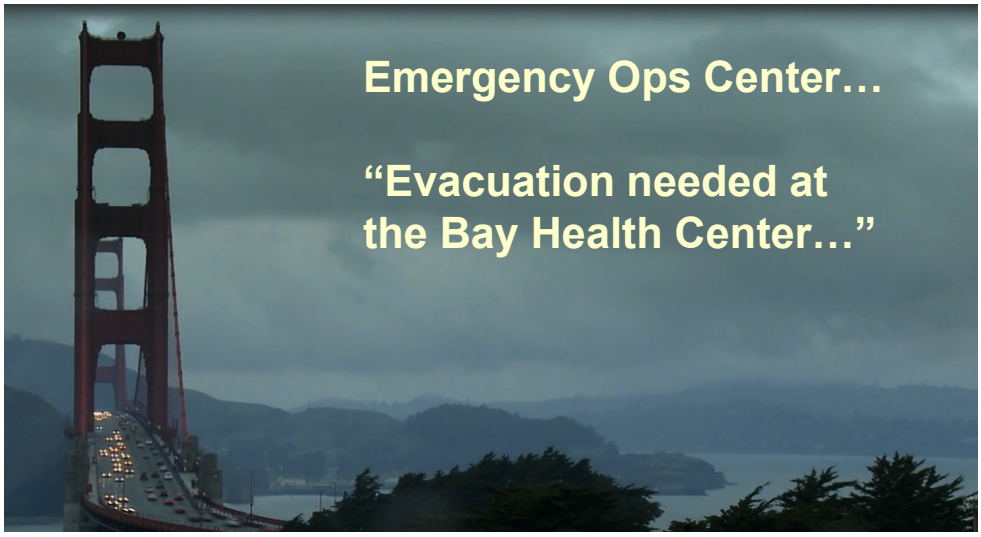
There are limited resources in the area due to all the responses that are in progress throughout the Bay Area. After the evacuation order has been given the Emergency Operations Center will need to notify others in the region of the incident, and request air resources to assist in the Air Ambulance evacuation from the National Guard and others.

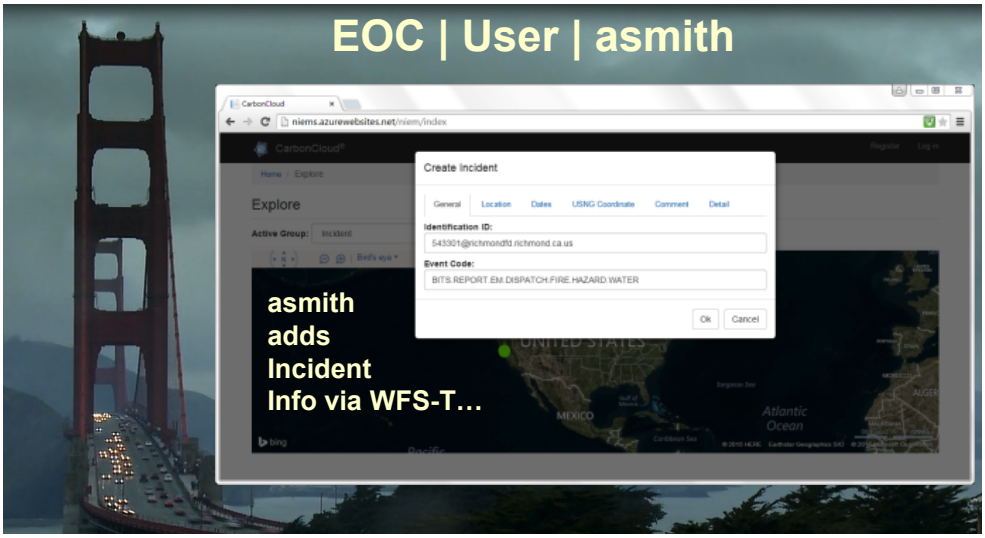
Knowing the geographical location of specific resources is now easier with the inclusion of OGC GML into the NIEM documents that allow for spatial filtering through the Web Feature Service.

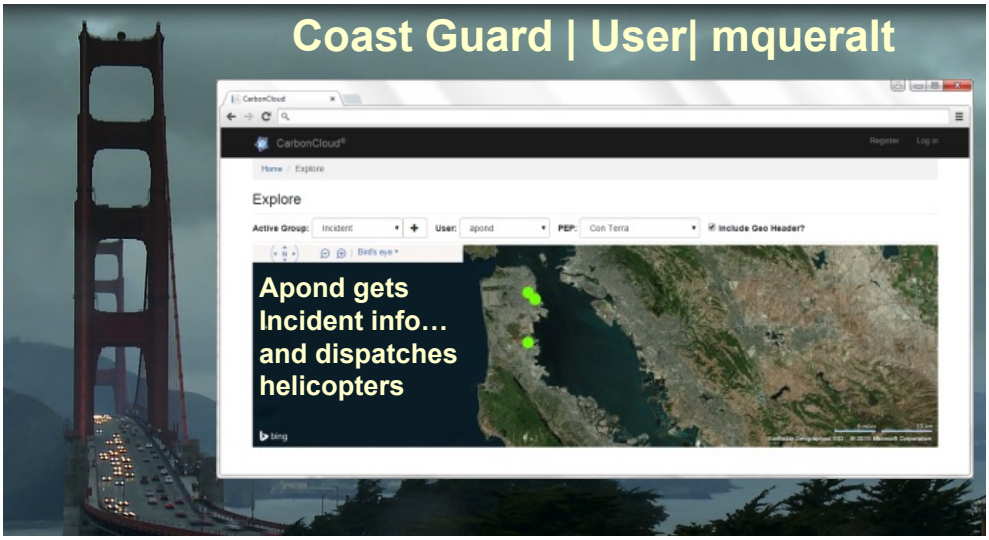
The back and forth nature of requesting resources and receiving responses regarding those resources stresses the requirements for the creation, search and retrieve, edit and update, and deletion of NIEM instance documents.

5.2.2.1 Geo4NIEM Use Case 4 – Demonstration Example

The following examples provide a brief overview of the Testbed 11 Geo4NIEM demonstration Use Case #4, Mutual Aid, described above.







5.3 Technical Flow of Events and Additional Examples

This section provides additional examples of the implemented technology in use by applications and services provided by Testbed 11 participants including a cloud-based test WFS from The Carbon Project and PEPs from multiple Participants including Secure Dimensions, con terra and Jericho Systems.

The basic flow of events in the demonstration was:

1. The PEP requests user attributes via a SAML attribute query to the OGC Identity Provider (IdP) Testbed Attribute Service.
2. The OGC IdP returns the user attributes to the PEP in the form of a SAML response; the PEP then associates the attributes with the client session. In this scenario instance, the user attributes are

uid	tjacobs
CountryOfAffiliation	US
FineAccessControls	Restricted
AICP	FALSE
DigitalIdentifier	cn=Tim Jacobs,ou=SolanoOES,o=Solano County,c=US
Role	SEMS-CA-Msn-SolanoCounty-MAC
EntityType	GOV
DutyOrganization	SLT
Clearance	U
AdminOrganization	SLT
isICMember	FALSE
mail	tjacobs@geo4niem.example.com

3. The client sends GetCapabilities, DescribeFeatureType, and GetFeature requests to the PEP (which is acting as a WFS proxy). Steps 4-9 describe the handling of the GetFeature request. (Handling of the other service invocations is similar and simpler.)

4. The PEP issues a XACML 2.0 compliant Authorization Decision Request to the PDP, including the user attributes from step 2 and the geolocation of the client.
5. The PDP retrieves the GeoXACML Policy from the Testbed Policy Store. In this scenario, the policy rules are expressed in terms of the user attributes for location, clearance, and role.
6. The PDP creates the Authorization Decision based on the policy and the user attributes. This may be Deny, Permit, or Permit with Obligations for rewriting rules that must be applied to the response from the WFS before the featureCollection is sent to the client. In this scenario, the rewriting rule removes elements classified C or above, and removes elements that have NTK portion marks which do not grant access for the role SEMS-CA-Msn-SolanoCounty-MAC.
7. If permitted, the PEP forwards the GetFeature request to the WFS server.
8. The WFS server returns a featureCollection to the PEP. Depending on the outputFormat parameter of the GetFeatureCollection request, the members of the featureCollection may be NIEM IEPs (the default), or TDOs with a NIEM IEP payload (with "niems" outputFormat).
9. The PEP executes any Obligations by applying any required rewriting rules to the featureCollection. These rules can have the effect of redacting elements that are classified above the user's clearance. In this scenario, the rewriting rule removes elements classified C or above, and removes elements that have NTK portion marks which do not grant access for the role SEMS-CA-Msn-SolanoCounty-MAC. The result is returned to the client as the output of the GetFeature request.

An architecture for this demonstration flow is provided below.

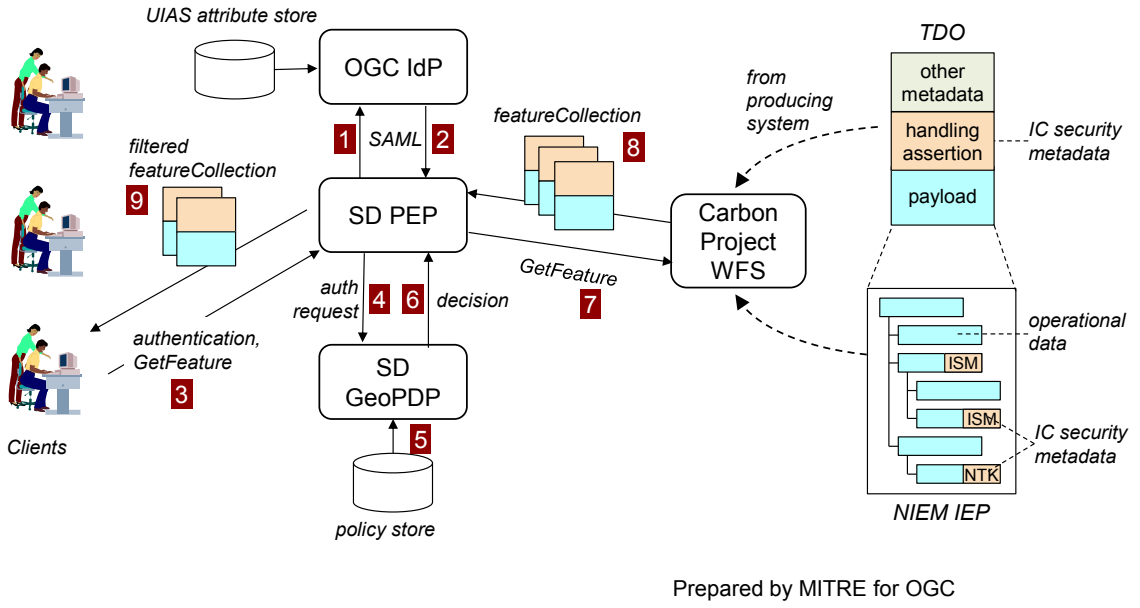


Figure 13 - Sample Geo4NIEM Testbed 11 Demonstration Flow for one PEP

5.3.1 The Carbon Project

The Carbon Project implemented the NIEM/IC Feature Processing API, the NIEM/IC Data Encoding in OGC WFS and multiple client applications, including a new web client developed for Testbed 11. The Web Feature Service (WFS) provided NIEM/IC Data Encoding as wfs:FeatureCollections to Policy Enforcement Point (PEP) services form Secure Dimensions, con terra and Jericho Systems. In addition, the WFS provided NIEM/IC Data Encoding directly to client applications such as Gaia, an older geospatial application.

The Carbon Project also developed a new web client able to access the NIEM/IC Data Encoding via PEP from Secure Dimensions, con terra and Jericho Systems, and NIEM/IC WFS from The Carbon Project cloud. An example of this new web client for NIEM/IC is shown in the first graphic below. The Carbon Project web client able for NIEM/IC also served as a test platform for WFS Transactions, as described in Section 5.2.2.1 above.

In addition, new tools were developed to create and manage NIEM/IC Feature services in a cloud-based environment. An example of this new CarbonCloud® toolset for NIEM/IC is shown in the second graphic below.

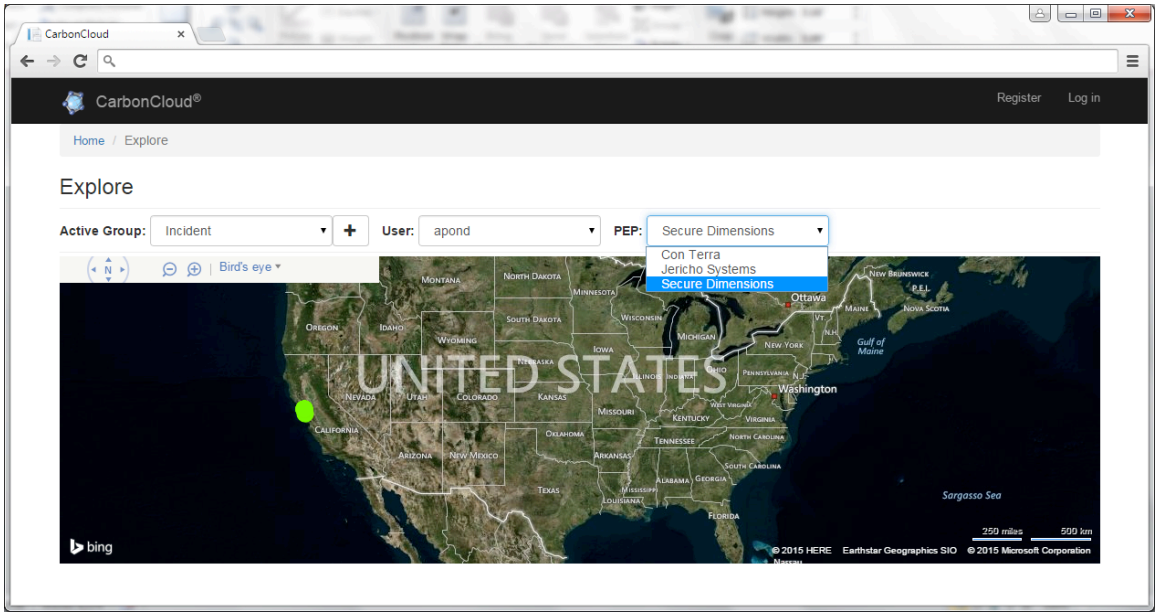


Figure 14 - Web Client from The Carbon Project accessing NIEM/IC Data Encoding from Secure Dimensions, con terra and Jericho Systems PEP

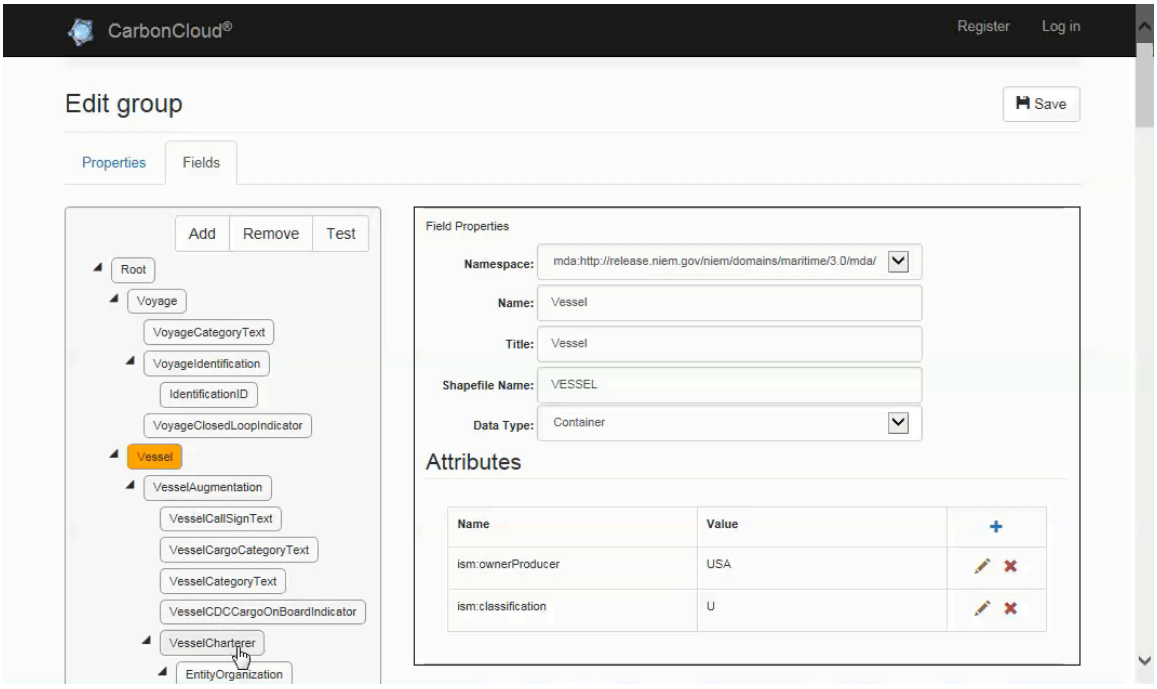


Figure 15 - Web Client from The Carbon Project managing cloud-based NIEM/IC WFS

5.4 Secure Dimensions

Secure Dimensions implemented and tested the NIEM/IC Data Encoding and Feature Processing API in PEP services. Examples with simulated geographic location and geographic access control rules implemented are shown below.

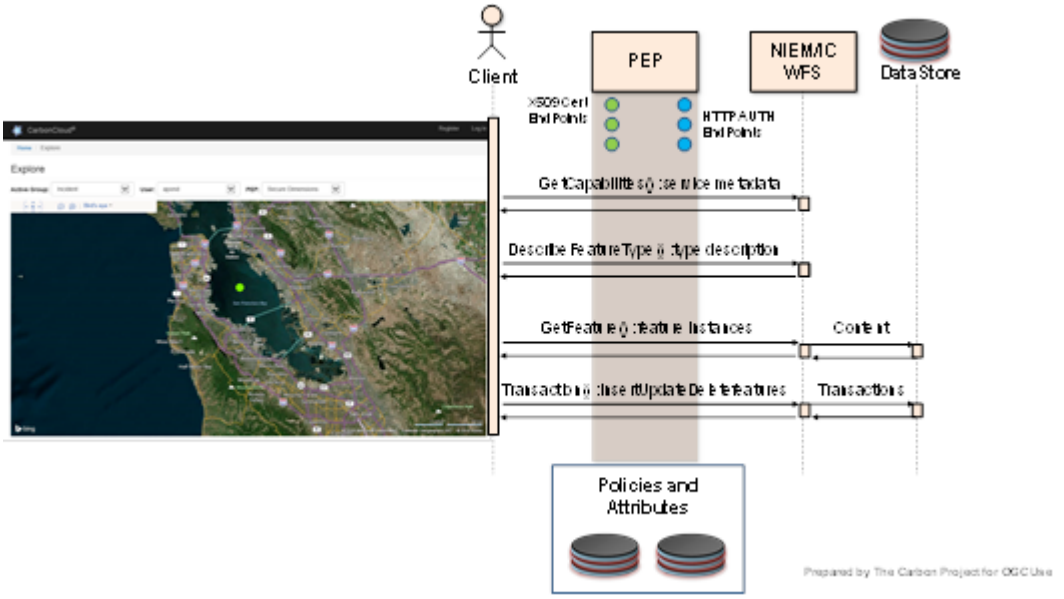


Figure 16 - Secure Dimensions PEP in The Carbon Project web client, implementing GeoHeader

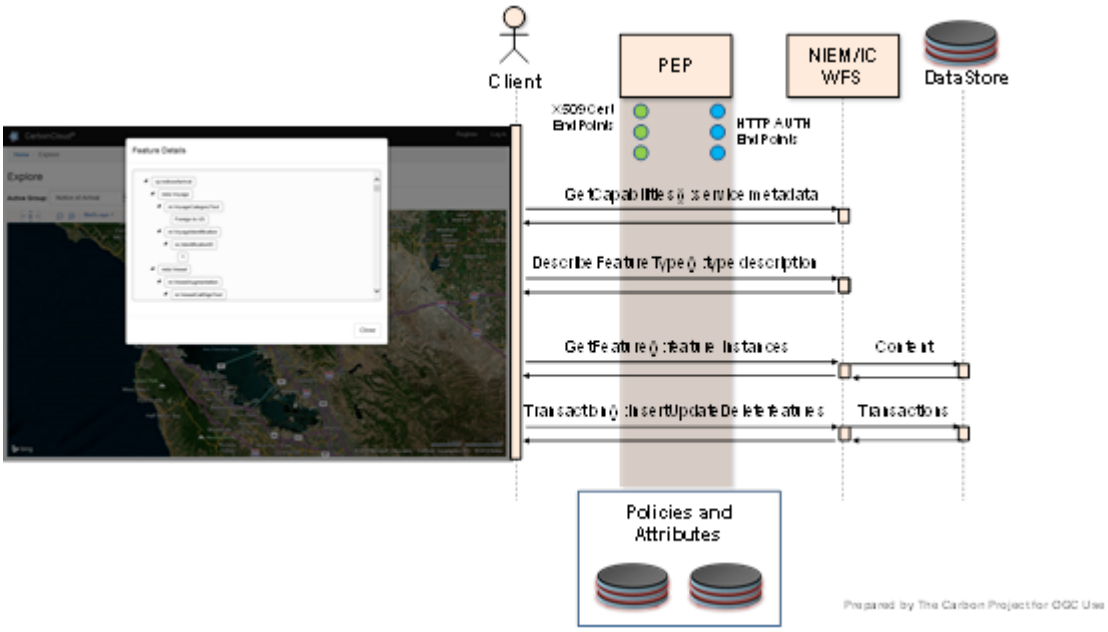


Figure 17 - Secure Dimensions PEP in web client, feature detail displayed

The Secure Dimensions architecture for implementing and testing the NIEM/IC Data Encoding and Feature Processing API in PEP services is shown below.

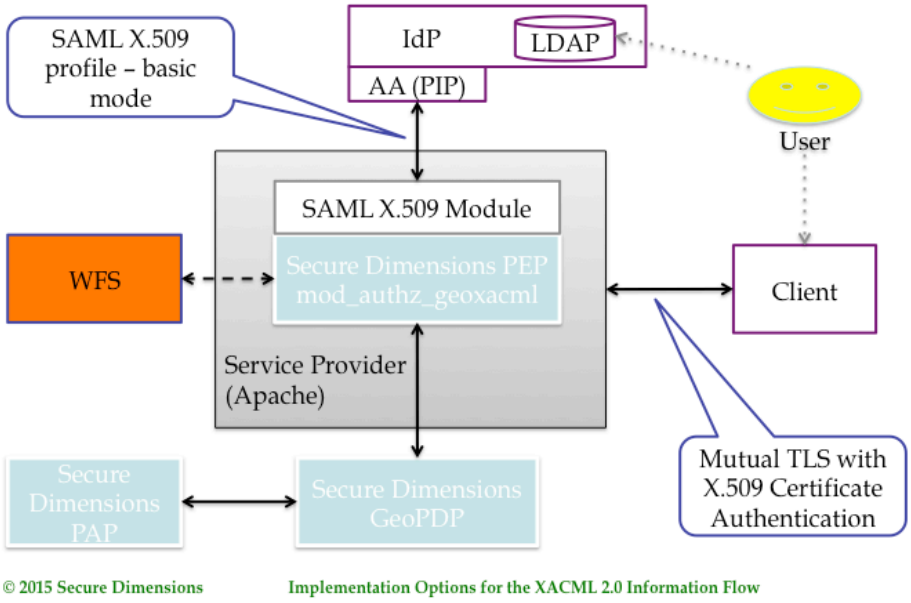


Figure 18 - Secure Dimensions architecture for implementing and testing the NIEM/IC Data Encoding and Feature Processing API in PEP services

5.5 Con terra

con terra implemented and tested the NIEM/IC Data Encoding and Feature Processing API in PEP services. An example in the Post-Security Architecture is provided below.

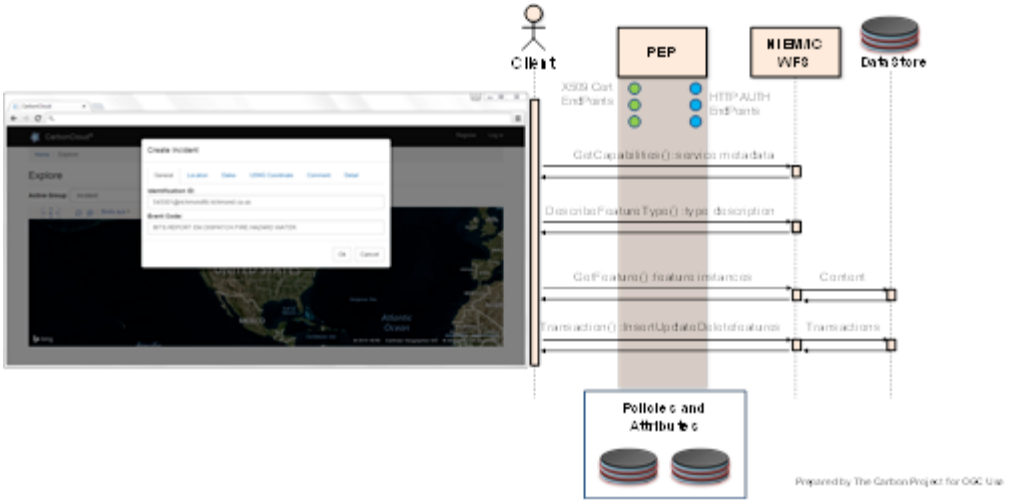


Figure 19 – con terra PEP in web client, executing WFS Transactions

The con terra security.manager architecture for implementing and testing the NIEM/IC Data Encoding and Feature Processing API in PEP services is shown below.

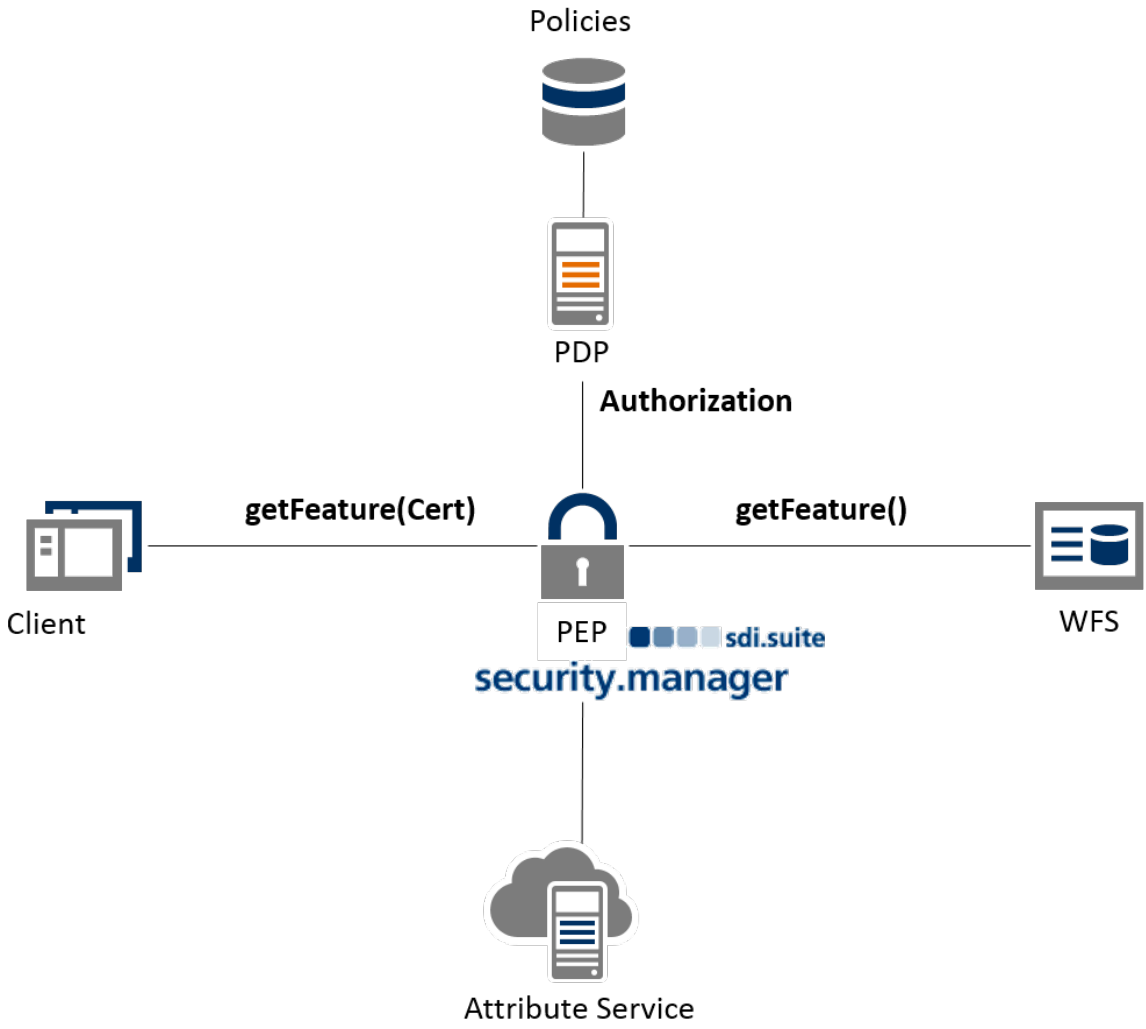


Figure 20 - con terra security.manager architecture for implementing and testing the NIEM/IC Data Encoding and Feature Processing API in PEP services

5.6 Jericho Systems

Jericho Systems implemented and tested the NIEM/IC Data Encoding and Feature Processing API in PEP services. An example of accessing a Resource encoding in the Post-Security Geo4NIEM Architecture is shown below.

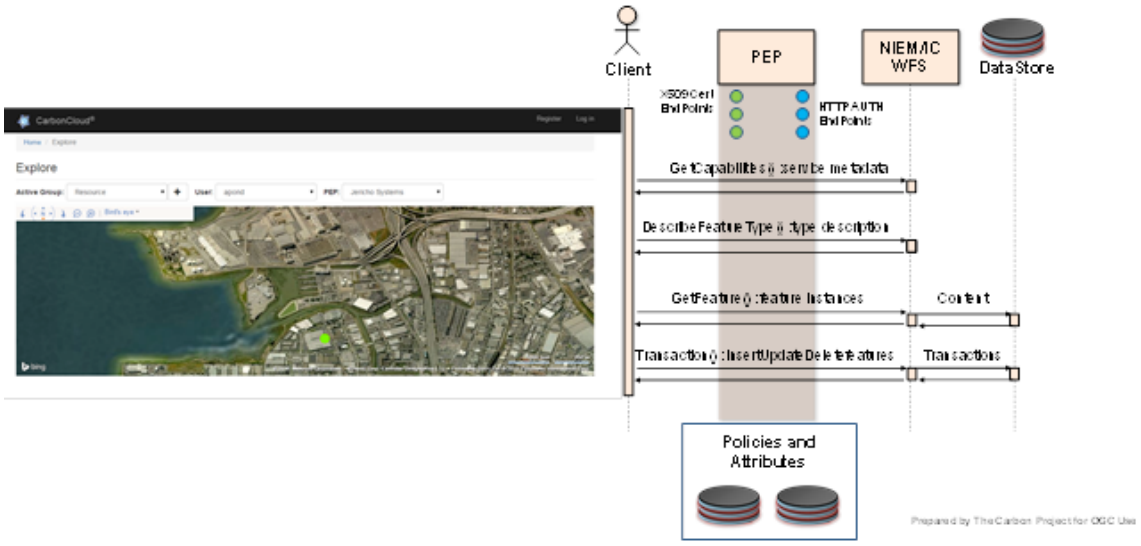


Figure 21 – Jericho Systems PEP in web client, accessing Resource encoding

The Jericho Systems EnterSpace® architecture for implementing and testing the NIEM/IC Data Encoding and Feature Processing API in PEP services is shown below.

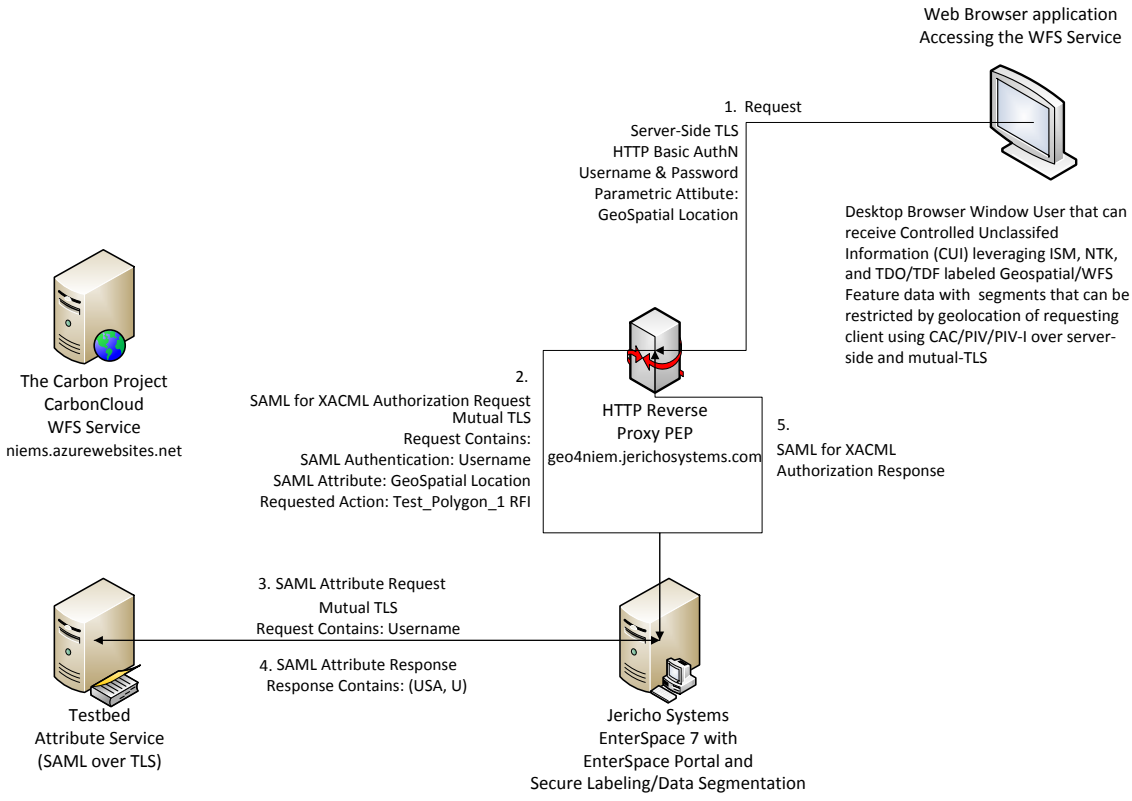


Figure 22 - Jericho Systems EnterSpace® architecture for PEP services

6 Findings and Recommendations

The evidence obtained through the Testbed 11:Geo4NIEM thread supports three main findings:

- First, with reasonable effort it is possible to combine NIEM, IC security specifications, OGC Web Service components, and GML-aware clients to support information exchange with authorized users.

- Second, implementing such an exchange requires extra work, compared to a typical exchange of features that conform to the GML Simple Features profile. However, this level of effort is not greater than encodings already in OGC, such as Aeronautical Information Exchange Model (AIXM), where a community of interest has defined a standard GML application schema for exchanging geographic data.

- Finally, it is possible to simplify the implementation of NIEM and IC security specifications and still meet information exchange needs. This simplification can reduce the technical overhead required to broadly implement secure information exchanges and emerging collaborative partnerships. Simplification options include NIEM IEPD development guidance or recommended practices that reduce the impact of generating excessive namespaces.

The following sections describe these findings and any associated recommendations.

6.1 Combining NIEM, IC security, and OGC Web Services OWS is feasible

The demonstration used real-world NIEM IEPs, containing embedded GML elements, properly tagged with IC access control and security metadata and optionally enclosed within the IC's dissemination format for binding assertion metadata with data resources (i.e. IC-TDF.XML/TDO).. The demonstration was constructed using a cloud-based WFS server, multiple Policy Enforcement Points that provide access controls and filters based upon the user attributes stored in the OGC Attribute Store and multiple GML-aware clients. Major OGC operations in a simulated distributed information exchange were assessed including:

- WFS server with GetCapabilities, DescribeFeatureType, GetFeature, and Transaction operations
- Access control engines enforcing access policy based on user attributes and IC metadata attributes in the WFS FeatureCollection payload
- Clients interpreting the WFS FeatureCollection elements and performing transaction operations

NIEM 3.0 was compatible with the IC security, access control and dissemination specifications (ISM, NTK, and TDF) and supported the access control policies for the demonstration scenario. There is no evidence to suggest incompatibility with more complex policies, schemas and security markings. Access control engines can work with NIEM/IC Data Encoding, with or without the NIEM/IC Feature Processing API.

The participants spent most of their time learning about the NIEM exchange specifications and the IC security specifications. Implementation of the second and third information exchanges (based on Incident and Resource IEPs) took less development time since specialized tools were created to speed the 'cloning' of the first WFS instance (based on the Notice of Arrival IEP).

Recommendation 1: Develop, test and demonstrate tools that clone and adjust data elements of WFS instances of NIEM/IC Data Encodings to simplify and speed development and deployment of service-based information exchanges. Assess tools that promote export of NIEM/IC Data Encodings.

Recommendation 2: Assess how IC security specifications (ISM, NTK, and TDF) may further enable WFS and GML-based data exchange.

6.2 Extra effort relative to typical use of Simple Features profile

The GML Simple Features profile defines fixed coding patterns for the use of a subset of XML Schema and GML constructs. It is intended to address the case where a client interacts with a previously unknown server offering. This is the typical case for many OWS components. Relative to that typical case, the demonstration implementation for the NIEM/IC Feature Processing API and NIEM/IC Data Encoding (Testbed 11 ER 15-048) required extra effort in three areas: complex non-spatial properties, multiple namespaces and DescribeFeatureType, and context-dependent value references in filter encodings.

6.2.1 Complex non-spatial properties

Information exchanges implementing the draft NIEM/IC Feature Processing API required schemas in wfs:FeatureCollections roughly equivalent to those that comply with level two (2) of the OGC GML Simple Features Profile (SF-2 for GMLsf). This finding means that some current WFS and GML applications and services expecting GMLsf Level 0 or 1 tools may not able to fully operate with the NIEM/IC Feature Processing API 'out of the box'. This finding also means that exporting NIEM/IC Data Encoding from a WFS

implementing NIEM/IC Feature Processing API may not be possible in common GIS formats such as Shapefiles.

The SF-0 profile does not allow complex non-spatial properties, while these are permitted but unusual in the SF-1 profile. This simplicity can be exploited in server and client software, allowing off-the-shelf components to handle new application schemas with little or no special effort. However, this simplicity is not present in the NIEM/IC Feature Processing API and NIEM/IC Data Encoding. For example, the Notice of Arrival IEPD defines a complex property with six levels of nested elements, resulting in data like this:

```
<mda:Vessel ...>
  <m:VesselAugmentation ...>
    <m:VesselCallSignText>H3LP</m:VesselCallSignText>
    <m:VesselCargoCategoryText>Harmful Substances ...
    <m:VesselCategoryText>Container Ship ...
    <m:VesselCDCCargoOnBoardIndicator>true ...
    <m:VesselCharterer ...>
      <nc:EntityOrganization>
        <nc:OrganizationLocation>
          <nc:Address>
            <nc:LocationCountryISO3166Alpha2Code>KR ...
          </nc:Address> ...
```

From the perspective of an Information Exchange designer or implementer, this level of complexity may require effort in the WFS server implementations when compared with less extensive SF-0 and SF-1 schemas, especially when implementing the WFS-T functions. It also requires extra effort in the client applications, where specialized Filter Encodings using XPath expressions are necessary to retrieve values from the complex properties.

Recommendation 3: Develop and test a Best Practice that defines more limited, but useful, subsets of NIEM/IC schema components (including location as GML), with required IC DES components, to lower the 'implementation bar' of time and resources required for developing software that supports the NIEM/IC Feature Processing API. By lowering the level of effort, Information Exchange designers, geospatial developers and access control software implementers will be encouraged to take greater advantage of the rich functionality in NIEM/IC. The Best Practice should be designed around the business elements needed by Information Exchange Designers.

6.2.2 Multiple namespaces, and DescribeFeatureType

The WFS DescribeFeatureType operation returns an XML Schema document containing a complex type definition for the specified feature type. In order to form a complete schema, the client must then either retrieve or already possess a separate schema document for each imported namespace. This is essential for WFS servers and GML clients implemented with validating parsers. On the other hand, implementations based on non-validating parsers do not need the schema and do not rely on DescribeFeatureType. Both approaches were tested in Testbed 11 Geo4NIEM Thread.

For application schemas conforming to the Simple Features profile, implementing the DescribeFeatureType operation is relatively simple. These schemas typically define features within a single namespace, and clients usually have schema documents for the imported GML namespaces.

Implementing the DescribeFeatureType operation for the NIEM/IC Feature Processing API is more complicated. The schema for such a feature type will have many namespaces, and clients may not always have the corresponding schema document. This can greatly complicate the implementation of the DescribeFeatureType operation.

Two aspects of NIEM IEPDs may be exploited in future work to reduce much of this complexity. A conforming IEPD contains the complete set of schema documents. It also contains a set of OASIS XML Catalog files providing a mapping between namespace URI and schema document file name. A WFS server could use the catalog to rewrite every <import> schema element so that the schemaLocation attribute resolves to a schema document on the server.

Recommendation 4: Develop, test and demonstrate the feasibility of making schemas available from WFS implementing the NIEM/IC Feature Processing API. This may or may not be part of the DescribeFeatureType operation so PEPs can create filter rules based upon them. This recommendation may also include assessing methods by which PEPs may process security tag information from the DescribeFeatureType.

Recommendation 5: Assess, develop, test and demonstrate governance methods to provide complete sets of public-accessible schema document. In particular, assess methods to assist IEPD developers in maintaining and accessing schemas.

6.2.3 Context-dependent value references in Filter Encodings

From the perspective of an OGC software developer or user the nested structure in the data encodings associated with the NIEM/IC Feature Processing API means

implementing fully capable OGC Filter Encodings for WFS will require a subset of XPath. For example, the Notice of Arrival NIEM IEPD describes data like this:

```
<m:VesselDOCCertificate>
  <nc:DocumentExpirationDate>
    <nc:Date>2028-04-24T00:00:00</nc:Date>
  </nc:DocumentExpirationDate>
  <nc:CertificateIssueDate>
    <nc:Date>2026-03-11T00:00:00</nc:Date>
  </nc:CertificateIssueDate>
```

XPath is required to distinguish between the `nc:Date` of document expiration and certificate issue. There is a similar context dependency in NTK, where XPath is required to distinguish between the `ntk:AccessGroupList` element within `ntk:RequiresAnyOf`, and the same element within `ntk:RequiresAllOf` . Therefore, the use of either NIEM or IC security requires Filter processing with XPath enabled.

XPath is accounted for in the Filter Encoding specification, but it is a specialized case and not as broadly implemented as the standard spatial, logical and comparison operators of WFS.

Recommendation 6: Develop, test and demonstrate the feasibility of fully capable OGC Filter Encodings for WFS using a subset of XPath. This approach provides the potential for high fidelity queries on the NIEM/IC Feature Processing API in support of mission and community requirements.

6.3 Simplifying use of NIEM and IC security and meeting exchange needs

The extra effort required to implement the NIEM/IC Feature Processing API is not unique to either of those standards. It is common in situations where a community of interest has defined a standard GML application schema for exchanging geographic data, and presumes understanding on the part of all community participants. For example, the Aeronautical Information Exchange Model (AIXM) provides a standard GML application schema for aeronautical information exchange. This application schema defines many complex non-spatial properties, uses multiple namespaces, and includes context-dependent element values. Implementing AIXM-based exchanges with off-the-shelf components requires the same sort of extra effort needed for the NIEM/IC encoding. For example, the Gaia client requires a special "AIXM extender" in order to process AIXM data.

This extra effort can be reduced by careful NIEM-conformant IEPD design. Instead of using all available NIEM objects designers can carefully construct IEPD schemas using just enough NIEM objects to meet the community's information exchange need. It may be possible to satisfy a large set of information exchange needs with a simple "what, where, when" IEPD that approaches the Simple Feature profile, using reduced nesting and a subset of location designations and security tags.

Achieving broad implementation of these approaches will make it possible for the NIEM/IC Feature Processing API to support emerging agile information exchanges driven by collaborative partnerships. This transformation is vital to confronting the security challenges of the future.

Recommendation 7: Develop, test, and demonstrate the feasibility of a 'Generic' IEPD with location, time, what, who information as 'core' elements in simple GMLsf.

Recommendation 8: Develop, test and demonstrate the feasibility of a generic GML Application Schema leveraging NIEM-conformant components and IC specification components. This would extend the usefulness of NIEM components from an OGC implementation stand-point within a particular community of interest.

Annex A

Sample IEP Instance Document with Security Tags

```
<?xml version="1.0" encoding="UTF-8"?>
<!--All classification marks in this example are for illustrative
purposes only.-->
<!--There are no actual classified data elements contained in
this example.-->
<mda:LOAReport

xsi:schemaLocation="http://release.niem.gov/niem/domains/maritime
/3.0/mda/ ../xsd/extension/mda.xsd"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:ntk="urn:us:gov:ic:ntk"
    xmlns:ism="urn:us:gov:ic:ism"
    xmlns:gml="http://www.opengis.net/gml/3.2"
    xmlns:nc="http://release.niem.gov/niem/niem-core/3.0/"
    xmlns:m="http://release.niem.gov/niem/domains/maritime/3.0/"

xmlns:mda="http://release.niem.gov/niem/domains/maritime/3.0/mda/
" ntk:DESVersion="9" ism:DESVersion="11" ism:createDate="2025-12-
10" ism:ownerProducer="USA" ism:classification="S"
ism:resourceElement="true" ism:classifiedBy="USCG"
ism:classificationReason="Classified due to sensitive maritime
security information." ism:declassDate="2050-12-01">
    <mda:Access>
        <ntk:Access ism:classification="U"
ism:ownerProducer="USA">
            <ntk:RequiresAnyOf ism:classification="U"
ism:ownerProducer="USA">
                <ntk:AccessGroupList>
                    <ntk:AccessGroup ism:classification="U"
ism:ownerProducer="USA">
                        <ntk:AccessPolicy ism:classification="U"
ism:ownerProducer="USA">Roles</ntk:AccessPolicy>
                        <ntk:AccessGroupValue
ism:classification="U" ism:ownerProducer="USA">NIMS-FEMA-Msn-
RegionIX-ICS</ntk:AccessGroupValue>
                        <ntk:AccessGroupValue
ism:classification="U" ism:ownerProducer="USA">MDA-USCG-Msn-
District11-ROC</ntk:AccessGroupValue>
                        <ntk:AccessGroupValue
ism:classification="U" ism:ownerProducer="USA">SEMS-CA-Ent-
CoastalRegion-MAC</ntk:AccessGroupValue>
```

```
                        <ntk:AccessGroupValue
ism:classification="U" ism:ownerProducer="USA">SEMS-CA-Ent-
StateOperationsCenter-MAC</ntk:AccessGroupValue>
                    </ntk:AccessGroup>
                </ntk:AccessGroupList>
                <ntk:AccessProfileList ism:classification="U"
ism:ownerProducer="USA">
                    <ntk:AccessProfile ism:classification="U"
ism:ownerProducer="USA">
                        <ntk:AccessPolicy ism:classification="U"
ism:ownerProducer="USA">slt-ntk.aces</ntk:AccessPolicy>
                        <ntk:AccessProfileValue
ism:classification="U" ism:ownerProducer="USA"
ntk:vocabulary="urn:us:gov:ic:cvenum:usagency:agencyacronym">SLT<
/ntk:AccessProfileValue>
                    </ntk:AccessProfile>
                </ntk:AccessProfileList>
            </ntk:RequiresAnyOf>
        </ntk:Access>
    </mda:Access>
    <mda:LevelOfAwarenessCode ism:ownerProducer="USA"
ism:classification="S" ntk:access="#Roles|Group^MDA-USCG-Msn-
District11-ROC Roles|Group^NIMS-FEMA-Msn-RegionIX-
ICS">1</mda:LevelOfAwarenessCode>
    <mda:Vessel ism:ownerProducer="USA" ism:classification="U">
        <m:VesselAugmentation>
            <m:VesselBeamMeasure>
                <nc:MeasureValueText>120.0</nc:MeasureValueText>
            </m:VesselBeamMeasure>
            <m:VesselCallSignText>H3LP</m:VesselCallSignText>
            <m:VesselCargoCategoryText>Harmful
Substance</m:VesselCargoCategoryText>
            <m:VesselCategoryText>Container
Ship</m:VesselCategoryText>
            <m:VesselCharterer ism:ownerProducer="USA"
ism:classification="C" ntk:access="#Roles|Group^MDA-USCG-Msn-
District11-ROC">
                <nc:EntityOrganization>
                    <nc:OrganizationLocation>
                        <nc:Address>

<nc:LocationCountryISO3166Alpha2Code>KR</nc:LocationCountryISO316
6Alpha2Code>
                        </nc:Address>
                    </nc:OrganizationLocation>
                    <nc:OrganizationName>SK
Shipping</nc:OrganizationName>
                </nc:EntityOrganization>
            </m:VesselCharterer>
            <m:VesselClassText>Bulk Carrier</m:VesselClassText>
```

```
            <m:VesselClassificationSocietyName>Germanischer
Lloyd</m:VesselClassificationSocietyName>
            <m:VesselContactInformation ism:ownerProducer="USA"
ism:classification="C" ntk:access="#Roles|Group^MDA-USCG-Msn-
District11-ROC">
                <nc:ContactTelephoneNumber>
                    <nc:InternationalTelephoneNumber>
                        <nc:TelephoneNumberID>800-555-
1212</nc:TelephoneNumberID>
                    </nc:InternationalTelephoneNumber>

<nc:TelephoneNumberCategoryCode>work</nc:TelephoneNumberCategoryC
ode>
                </nc:ContactTelephoneNumber>
                <nc:ContactTelephoneNumber>
                    <nc:InternationalTelephoneNumber>
                        <nc:TelephoneNumberID>800-555-
1213</nc:TelephoneNumberID>
                    </nc:InternationalTelephoneNumber>

<nc:TelephoneNumberCategoryCode>fax</nc:TelephoneNumberCategoryCo
de>
                </nc:ContactTelephoneNumber>
                <nc:ContactEntity>
                    <nc:EntityPerson>
                        <nc:PersonName>
                            <nc:PersonFullName>James
Smith</nc:PersonFullName>
                        </nc:PersonName>
                    </nc:EntityPerson>
                    <nc:EntityOrganization>
                        <nc:OrganizationName>Horizon
Lines</nc:OrganizationName>
                    </nc:EntityOrganization>
                </nc:ContactEntity>
            </m:VesselContactInformation>
            <m:VesselDOCCertificate>
                <nc:DocumentExpirationDate>
                    <nc:Date>2028-04-24</nc:Date>
                </nc:DocumentExpirationDate>
                <m:CertificateIssueDate>
                    <nc:Date>2018-04-25</nc:Date>
                </m:CertificateIssueDate>
                <m:CertificateIssuingAgency>
                    <nc:EntityOrganization>
                        <nc:OrganizationName>U.S. Coast
Guard</nc:OrganizationName>
                    </nc:EntityOrganization>
                </m:CertificateIssuingAgency>
            </m:VesselDOCCertificate>
```



```
            <m:VesselDraftMeasure>
                <nc:MeasureValueText>12.1</nc:MeasureValueText>
                <nc:MeasureUnitText>m</nc:MeasureUnitText>
            </m:VesselDraftMeasure>

<m:VesselGrossTonnageValue>54881</m:VesselGrossTonnageValue>

<m:VesselIMONumberText>9278155</m:VesselIMONumberText>
            <m:VesselISSC ism:ownerProducer="USA"
ism:classification="C" ntk:access="#Roles|Group^MDA-USCG-Msn-
District11-ROC">
                <m:CertificateIssueDate>
                    <nc:Date>2022-06-22</nc:Date>
                </m:CertificateIssueDate>
                <m:CertificateIssuingAgency>
                    <nc:EntityOrganization>
                        <nc:OrganizationName>Government of
Bermuda, Department of Maritime
Administration</nc:OrganizationName>
                    </nc:EntityOrganization>
                </m:CertificateIssuingAgency>
                <m:RecognizedISSCSecurityEntity>
                    <nc:EntityOrganization>
                        <nc:OrganizationName>Government of
Bermuda, Department of Maritime
Administration</nc:OrganizationName>
                    </nc:EntityOrganization>
                </m:RecognizedISSCSecurityEntity>
                <m:VesselSecurityOfficerContactInformation>
                    <nc:ContactTelephoneNumber>
                        <nc:InternationalTelephoneNumber>
                            <nc:TelephoneNumberID>888-234-
5432</nc:TelephoneNumberID>
                        </nc:InternationalTelephoneNumber>

<nc:TelephoneNumberCategoryCode>work</nc:TelephoneNumberCategoryC
ode>
                    </nc:ContactTelephoneNumber>
                    <nc:ContactTelephoneNumber>
                        <nc:InternationalTelephoneNumber>
                            <nc:TelephoneNumberID>888-234-
5431</nc:TelephoneNumberID>
                        </nc:InternationalTelephoneNumber>

<nc:TelephoneNumberCategoryCode>fax</nc:TelephoneNumberCategoryCo
de>
                    </nc:ContactTelephoneNumber>

<nc:ContactEmailID>ftest@test.com</nc:ContactEmailID>
                    <nc:ContactEntity>
                        <nc:EntityPerson>
```

```
                            <nc:PersonName>
                                <nc:PersonFullName>Frank
Test</nc:PersonFullName>
                            </nc:PersonName>
                        </nc:EntityPerson>
                    </nc:ContactEntity>
                </m:VesselSecurityOfficerContactInformation>

<m:VesselSecurityPlanImplementedIndicator>true</m:VesselSecurityP
lanImplementedIndicator>
            </m:VesselISSC>
            <m:VesselMMSIText>352948000</m:VesselMMSIText>
            <m:VesselName>MSC NERISSA</m:VesselName>

<m:VesselNationalFlagISO3166Alpha2Code>PA</m:VesselNationalFlagIS
O3166Alpha2Code>

<m:VesselOfficialCoastGuardNumberText>US878N2</m:VesselOfficialCo
astGuardNumberText>

<m:VesselOperationalConditionOfEquipmentDescriptionText>Operation
al</m:VesselOperationalConditionOfEquipmentDescriptionText>
            <m:VesselOperator ism:ownerProducer="USA"
ism:classification="C" ntk:access="#Roles|Group^MDA-USCG-Msn-
District11-ROC">
                <nc:EntityPerson>
                    <nc:PersonName>
                        <nc:PersonFullName>Dan
James</nc:PersonFullName>
                    </nc:PersonName>
                </nc:EntityPerson>
            </m:VesselOperator>
            <m:VesselOverallLengthMeasure>
                <nc:MeasureValueText>294.08</nc:MeasureValueText>
                <nc:MeasureUnitText>m</nc:MeasureUnitText>
            </m:VesselOverallLengthMeasure>
            <m:VesselOwner ism:ownerProducer="USA"
ism:classification="C" ntk:access="#Roles|Group^MDA-USCG-Msn-
District11-ROC">
                <nc:EntityOrganization>
                    <nc:OrganizationLocation>
                        <nc:Address>

<nc:LocationCountryISO3166Alpha2Code>US</nc:LocationCountryISO316
6Alpha2Code>
                        </nc:Address>
                    </nc:OrganizationLocation>
                    <nc:OrganizationName>American Shipping
Company</nc:OrganizationName>
                </nc:EntityOrganization>
```



```
            </m:VesselOwner>
            <m:VesselSafetyManagementCertificate
ism:ownerProducer="USA" ism:classification="C"
ntk:access="#Roles|Group^MDA-USCG-Msn-District11-ROC">
                <nc:DocumentExpirationDate>
                    <nc:Date>2027-12-01</nc:Date>
                </nc:DocumentExpirationDate>
                <m:CertificateIssueDate>
                    <nc:Date>2017-03-12</nc:Date>
                </m:CertificateIssueDate>
                <m:CertificateIssuingAgency>
                    <nc:EntityOrganization>
                        <nc:OrganizationName>U.S. Coast
Guard</nc:OrganizationName>
                    </nc:EntityOrganization>
                </m:CertificateIssuingAgency>
            </m:VesselSafetyManagementCertificate>
        </m:VesselAugmentation>
    </mda:Vessel>
    <mda:Position ism:ownerProducer="USA" ism:classification="C"
ntk:access="#Roles|Group^MDA-USCG-Msn-District11-ROC
Roles|Group^NIMS-FEMA-Msn-RegionIX-IC Roles|Group^SEMS-CA-Ent-
StateOperationsCenter-MAC">
        <m:LocationPoint>
            <gml:Point gml:id="p1"
srsName="http://www.opengis.net/def/crs/EPSG/0/4326">
                <gml:pos>36.79771 -122.5665</gml:pos>
            </gml:Point>
        </m:LocationPoint>
        <mda:PositionSpeedMeasure>
            <nc:MeasureValueText>3.2</nc:MeasureValueText>
            <nc:SpeedUnitCode>KNT</nc:SpeedUnitCode>
        </mda:PositionSpeedMeasure>
        <mda:PositionCourseMeasure>
            <nc:MeasureValueText>17</nc:MeasureValueText>
        </mda:PositionCourseMeasure>
        <mda:PositionDateTime>
            <nc:DateTime>2025-12-07T00:00:00Z</nc:DateTime>
        </mda:PositionDateTime>
    </mda:Position>
    <mda:Arrival ism:ownerProducer="USA" ism:classification="U">
        <mda:VisitAnchorageText>Main
Anchorage</mda:VisitAnchorageText>
        <mda:VisitExpectedArrivalDateTime>
            <nc:DateTime>2025-12-10T14:30:00Z</nc:DateTime>
        </mda:VisitExpectedArrivalDateTime>
        <mda:VisitLocationInPort>
            <m:PortName>Oakland</m:PortName>
            <nc:LocationStateName>CA</nc:LocationStateName>
            <nc:LocationCityName>Oakland</nc:LocationCityName>
            <mda:PortAugmentation>
```

```
                <m:LocationPoint>
                    <gml:Point gml:id="p2"
srsName="http://www.opengis.net/def/crs/EPSG/0/4326">
                        <gml:pos>37.7955 122.2846</gml:pos>
                    </gml:Point>
                </m:LocationPoint>
            </mda:PortAugmentation>
        </mda:VisitLocationInPort>
        <mda:VisitReceivingFacilityName>Pier
57</mda:VisitReceivingFacilityName>
    </mda:Arrival>
    <mda:LastPortOfCall ism:ownerProducer="USA"
ism:classification="U" ntk:access="#Roles|Group^MDA-USCG-Msn-
District11-ROC">
        <mda:VisitActualArrivalDateTime>
            <nc:DateTime>2025-11-25T00:00:00Z</nc:DateTime>
        </mda:VisitActualArrivalDateTime>
        <mda:VisitActualDepartureDateTime>
            <nc:DateTime>2025-11-30T00:00:00Z</nc:DateTime>
        </mda:VisitActualDepartureDateTime>
        <mda:VisitLocationInPort>
            <m:PortName>Port of Portland, Oregon</m:PortName>

<nc:LocationCountryISO3166Alpha2Code>US</nc:LocationCountryISO316
6Alpha2Code>
            <nc:LocationStateName>OR</nc:LocationStateName>
            <nc:LocationCityName>Portland</nc:LocationCityName>
        </mda:VisitLocationInPort>
    </mda:LastPortOfCall>
    <mda:NextPortOfCallList ism:ownerProducer="USA"
ism:classification="U" ntk:access="#Roles|Group^MDA-USCG-Msn-
District11-ROC">
        <mda:NextPortOfCall>
            <mda:VisitExpectedArrivalDateTime>
                <nc:DateTime>2026-01-02T00:00:00Z</nc:DateTime>
            </mda:VisitExpectedArrivalDateTime>
            <mda:VisitExpectedDepartureDateTime>
                <nc:DateTime>2026-01-07T00:00:00Z</nc:DateTime>
            </mda:VisitExpectedDepartureDateTime>
            <mda:VisitLocationInPort>
                <m:PortName>Port of Long Beach</m:PortName>

<nc:LocationCountryISO3166Alpha2Code>US</nc:LocationCountryISO316
6Alpha2Code>
                <nc:LocationStateName>CA</nc:LocationStateName>
                <nc:LocationCityName>Long
Beach</nc:LocationCityName>
            </mda:VisitLocationInPort>
        </mda:NextPortOfCall>
    </mda:NextPortOfCallList>
```



```
    <mda:PreviousForeignPortOfCallList ism:ownerProducer="USA"
ism:classification="U" ntk:access="#Roles|Group^MDA-USCG-Msn-
District11-ROC">
        <mda:PreviousForeignPortOfCall>
            <mda:VisitLocationInPort>
                <m:PortName>Port of St. John's</m:PortName>

<nc:LocationCountryISO3166Alpha2Code>CA</nc:LocationCountryISO316
6Alpha2Code>
            </mda:VisitLocationInPort>
        </mda:PreviousForeignPortOfCall>
    </mda:PreviousForeignPortOfCallList>
    <mda:Interest ism:ownerProducer="USA" ism:classification="S"
ntk:access="#Roles|Group^MDA-USCG-Msn-District11-ROC">

<mda:CANUSLexiconAPR07CategoryCode>1a</mda:CANUSLexiconAPR07Categ
oryCode>
        <mda:InterestDateRange>
            <nc:StartDate>
                <nc:Date>2022-01-10</nc:Date>
            </nc:StartDate>
            <nc:EndDate>
                <nc:Date>2027-01-17</nc:Date>
            </nc:EndDate>
        </mda:InterestDateRange>

<mda:CANUSLexiconAPR07ThreatCode>High</mda:CANUSLexiconAPR07Threa
tCode>

<mda:InterestNotificationCategoryCode>Notification:Warning</mda:I
nterestNotificationCategoryCode>
    </mda:Interest>
    <mda:Interest ism:ownerProducer="USA" ism:classification="S"
ntk:access="#Roles|Group^MDA-USCG-Msn-District11-ROC">

<mda:InterestCategoryText>A5312</mda:InterestCategoryText>
        <mda:InterestDateRange>
            <nc:StartDate>
                <nc:Date>2022-01-10</nc:Date>
            </nc:StartDate>
            <nc:EndDate>
                <nc:Date>2027-01-17</nc:Date>
            </nc:EndDate>
        </mda:InterestDateRange>
        <mda:InterestDescriptionText>Hazardous
Materials</mda:InterestDescriptionText>
        <mda:InterestLevelText>5</mda:InterestLevelText>
        <mda:InterestLexiconSourceText>Lexicon LT-004; US
Standard Codes for Generalized Threat
Levels</mda:InterestLexiconSourceText>
```

```
<mda:InterestNotificationCategoryCode>Notification:Warning</mda:I
nterestNotificationCategoryCode>
    </mda:Interest>
    <mda:CDCCargoList ism:ownerProducer="USA"
ism:classification="C" ntk:access="#Roles|Group^MDA-USCG-Msn-
District11-ROC Roles|Group^NIMS-FEMA-Msn-RegionIX-IC">
        <mda:CDCCargo>
            <m:CargoHazmatDeclaration>
                <m:HazmatDeclarationDescriptionText>Division 2.3
Poisonous Gas</m:HazmatDeclarationDescriptionText>
                <m:HazmatDeclarationMaterialAmountMeasure>

<nc:MeasureValueText>100</nc:MeasureValueText>

<nc:MeasureUnitText>Barrel</nc:MeasureUnitText>
                </m:HazmatDeclarationMaterialAmountMeasure>

<m:HazmatDeclarationUNHazmatCode>UN3018</m:HazmatDeclarationUNHaz
matCode>
            </m:CargoHazmatDeclaration>
        </mda:CDCCargo>
    </mda:CDCCargoList>
    <mda:CrewNationalityList ism:ownerProducer="USA"
ism:classification="C" ntk:access="#Roles|Group^MDA-USCG-Msn-
District11-ROC">
        <mda:CrewNationalityCount>

<mda:CrewNationalityISO3166Alpha2Code>US</mda:CrewNationalityISO3
166Alpha2Code>

<mda:CrewNationalityQuantity>20</mda:CrewNationalityQuantity>
        </mda:CrewNationalityCount>
        <mda:CrewNationalityCount>

<mda:CrewNationalityISO3166Alpha2Code>CA</mda:CrewNationalityISO3
166Alpha2Code>

<mda:CrewNationalityQuantity>30</mda:CrewNationalityQuantity>
        </mda:CrewNationalityCount>
    </mda:CrewNationalityList>
    <mda:NonCrewNationalityList ism:ownerProducer="USA"
ism:classification="C" ntk:access="#Roles|Group^MDA-USCG-Msn-
District11-ROC">
        <mda:NonCrewNationalityCount>

<mda:NonCrewNationalityISO3166Alpha2Code>US</mda:NonCrewNationali
tyISO3166Alpha2Code>
```



```
<mda:NonCrewNationalityQuantity>250</mda:NonCrewNationalityQuanti
ty>
        </mda:NonCrewNationalityCount>
        <mda:NonCrewNationalityCount>

<mda:NonCrewNationalityISO3166Alpha2Code>CA</mda:NonCrewNationali
tyISO3166Alpha2Code>

<mda:NonCrewNationalityQuantity>120</mda:NonCrewNationalityQuanti
ty>
        </mda:NonCrewNationalityCount>
    </mda:NonCrewNationalityList>
</mda:LOAReport>
```

Annex B

NIEM/IC WFS - wfs:FeatureCollection Sample

This annex provides a sample NIEM/IC wfs:FeatureCollection.

```
<?xml version="1.0" encoding="UTF-8"?>
<wfs:FeatureCollection xmlns:wfs="http://www.opengis.net/wfs"
xmlns:gml="http://www.opengis.net/gml"
xmlns:mda="http://release.niem.gov/niem/domains/maritime/3.0/mda/
" xmlns:m="http://release.niem.gov/niem/domains/maritime/3.0/"
xmlns:nc="http://release.niem.gov/niem/niem-core/3.0/">
  <gml:featureMember>
    <mda:noticeofarrival
mda="http://release.niem.gov/niem/domains/maritime/3.0/mda/"
ntk="urn:us:gov:ic:ntk" ism="urn:us:gov:ic:ism"
nc="http://release.niem.gov/niem/niem-core/3.0/" mda-
codes="http://release.niem.gov/niem/domains/maritime/3.0/mda/code
s/" m="http://release.niem.gov/niem/domains/maritime/3.0/"
geo="http://release.niem.gov/niem/adapters/geospatial/3.0/"
DESVersion="11" ownerProducer="USA" classification="C"
resourceElement="true" classifiedBy="USCG"
classificationReason="Classified due to sensitive maritime
security information." declassDate="2050-12-01"
id="noticeofarrival.1" p7="http://www.opengis.net/gml">
      <mda:Voyage ownerProducer="USA" classification="U">
        <m:VoyageCategoryText>Foreign to
US</m:VoyageCategoryText>
        <m:VoyageIdentification>
          <nc:IdentificationID>1</nc:IdentificationID>
        </m:VoyageIdentification>

<mda:VoyageClosedLoopIndicator>false</mda:VoyageClosedLoopIndicat
or>
      </mda:Voyage>
      <mda:Vessel ownerProducer="USA" classification="U">
        <m:VesselAugmentation ownerProducer="USA"
classification="U">
          <m:VesselCallSignText>H3LP</m:VesselCallSignText>
          <m:VesselCargoCategoryText>Harmful
Substances</m:VesselCargoCategoryText>
          <m:VesselCategoryText>Container
Ship</m:VesselCategoryText>
```



```
<mda:VesselCDCCargoOnBoardIndicator>true</mda:VesselCDCCargoOnBoa
rdIndicator>
          <mda:VesselCharterer ownerProducer="USA"
classification="C" access="#Roles|Group^MDA-USCG-Msn-District11-
ROC">
            <nc:EntityOrganization>
              <nc:OrganizationLocation>
                <nc:Address>

<nc:LocationCountryISO3166Alpha2Code>KR</nc:LocationCountryISO316
6Alpha2Code>
                </nc:Address>
              </nc:OrganizationLocation>
              <nc:OrganizationName>SK
Shipping</nc:OrganizationName>
            </nc:EntityOrganization>
          </mda:VesselCharterer>
          <m:VesselClassText>Bulk Carrier</m:VesselClassText>
          <m:VesselClassificationSocietyName>Germanischer
Lloyd</m:VesselClassificationSocietyName>
          <m:VesselContactInformation>
            <nc:ContactTelephoneNumber>
              <nc:InternationalTelephoneNumber>
                <nc:TelephoneNumberID>800-555-
1212</nc:TelephoneNumberID>
              </nc:InternationalTelephoneNumber>

<nc:TelephoneNumberCategoryCode>work</nc:TelephoneNumberCategoryC
ode>
            </nc:ContactTelephoneNumber>
            <nc:ContactEntity>
              <nc:EntityPerson>
                <nc:PersonName>
                  <nc:PersonFullName>James
Smith</nc:PersonFullName>
                </nc:PersonName>
              </nc:EntityPerson>
            </nc:ContactEntity>
          </m:VesselContactInformation>
          <m:VesselDOCCertificate>
            <nc:DocumentExpirationDate>
              <nc:Date>2028-04-24T00:00:00</nc:Date>
            </nc:DocumentExpirationDate>
            <nc:CertificateIssueDate>
              <nc:Date>2028-04-25T00:00:00</nc:Date>
            </nc:CertificateIssueDate>
            <m:CertificateIssuingAgency>
              <nc:EntityOrganization>
                <nc:OrganizationName>U.S. Coast
Guard</nc:OrganizationName>
```

```
              </nc:EntityOrganization>
            </m:CertificateIssuingAgency>
          </m:VesselDOCCertificate>
          <m:VesselISSC ownerProducer="USA" classification="C"
access="#Roles|Group^MDA-USCG-Msn-District11-ROC">
            <m:CertificateIssueDate>
              <nc:Date>2022-06-22T00:00:00</nc:Date>
            </m:CertificateIssueDate>
            <m:CertificateIssuingAgency>
              <nc:EntityOrganization>
                <nc:OrganizationName>Government of Bermuda,
Department of Maritime Administration</nc:OrganizationName>
              </nc:EntityOrganization>
            </m:CertificateIssuingAgency>
            <m:RecognizedISSCSecurityEntity>
              <nc:EntityOrganization>
                <nc:OrganizationName>Government of Bermuda,
Department of Maritime Administration</nc:OrganizationName>
              </nc:EntityOrganization>
            </m:RecognizedISSCSecurityEntity>
            <m:VesselSecurityOfficerContactInformation>
              <m:ContactTelephoneNumber>
                <nc:InternationalTelephoneNumber>
                  <nc:TelephoneNumberID>888-234-
5432</nc:TelephoneNumberID>
                </nc:InternationalTelephoneNumber>

<nc:TelephoneNumberCategoryCode>work</nc:TelephoneNumberCategoryC
ode>
              </m:ContactTelephoneNumber>

<nc:ContactEmailID>ftest@test.com</nc:ContactEmailID>
              <nc:ContactEntity>
                <nc:EntityPerson>
                  <nc:PersonName>
                    <nc:PersonFullName>Frank
Test</nc:PersonFullName>
                  </nc:PersonName>
                </nc:EntityPerson>
              </nc:ContactEntity>
            </m:VesselSecurityOfficerContactInformation>

<m:VesselSecurityPlanImplementedIndicator>true</m:VesselSecurityP
lanImplementedIndicator>
          </m:VesselISSC>
          <m:VesselMMSIText>352948000</m:VesselMMSIText>
          <m:VesselName>MSC NERISSA</m:VesselName>

<m:VesselNationalFlagISO3166Alpha2Code>PA</m:VesselNationalFlagIS
O3166Alpha2Code>
```



```
<m:VesselOfficialCoastGuardNumberText>US878N2</m:VesselOfficialCo
astGuardNumberText>
          <m:VesselOperator ownerProducer="USA"
classification="C" access="#Roles|Group^MDA-USCG-Msn-District11-
ROC">
            <nc:EntityPerson>
              <nc:PersonName>
                <nc:PersonFullName>Dan James</nc:PersonFullName>
              </nc:PersonName>
            </nc:EntityPerson>
          </m:VesselOperator>
          <m:VesselOwner>
            <nc:EntityOrganization>
              <nc:OrganizationName>MSC Mediterranean Shipping
Company</nc:OrganizationName>
            </nc:EntityOrganization>
          </m:VesselOwner>
          <m:VesselSafetyManagementCertificate
ownerProducer="USA" classification="C" access="#Roles|Group^MDA-
USCG-Msn-District11-ROC">
            <nc:DocumentExpirationDate>
              <nc:Date>2027-12-01T00:00:00</nc:Date>
            </nc:DocumentExpirationDate>
            <nc:CertificateIssueDate>
              <nc:Date>2017-03-12T00:00:00</nc:Date>
            </nc:CertificateIssueDate>
            <m:CertificateIssuingAgency>
              <nc:EntityOrganization>
                <nc:OrganizationName>U.S. Coast
Guard</nc:OrganizationName>
              </nc:EntityOrganization>
            </m:CertificateIssuingAgency>
          </m:VesselSafetyManagementCertificate>
        </m:VesselAugmentation>

<mda:VesselCargoOnBoardIndicator>true</mda:VesselCargoOnBoardIndi
cator>
        <mda:VesselCertificateOfFinancialResponsibilityOperator
ownerProducer="USA" classification="U" access="#Roles|Group^MDA-
USCG-Msn-District11-ROC">

<mda:VesselCertificateOfFinancialResponsibilityOperator>
            <nc:EntityOrganization>
              <nc:OrganizationName>MSC Mediterranean Shipping
Company</nc:OrganizationName>
            </nc:EntityOrganization>

</mda:VesselCertificateOfFinancialResponsibilityOperator>
        </mda:VesselCertificateOfFinancialResponsibilityOperator>
```

```
        <mda:VesselSubCategoryText>Anhydrous
Ammonia</mda:VesselSubCategoryText>
      </mda:Vessel>
      <mda:Arrival ownerProducer="USA" classification="U">
        <mda:VisitAnchorageText>Main
Anchorage</mda:VisitAnchorageText>
        <mda:VisitExpectedArrivalDateTime>
          <nc:DateTime>2025-12-10T14:30:00</nc:DateTime>
        </mda:VisitExpectedArrivalDateTime>
        <mda:VisitLocationInPort>
          <m:PortName>Oakland</m:PortName>
          <nc:LocationStateName>CA</nc:LocationStateName>
          <nc:LocationCityName>Oakland</nc:LocationCityName>
          <mda:PortAugmentation>
            <m:LocationPoint>
              <gml:Point gml="http://www.opengis.net/gml"
srsName="EPSG::4326">
                <gml:pos srsName="EPSG::4326" srsDimension="2">-
122.295 37.6965</gml:pos>
              </gml:Point>
            </m:LocationPoint>
          </mda:PortAugmentation>
        </mda:VisitLocationInPort>
        <mda:VisitReceivingFacilityName>Pier
57</mda:VisitReceivingFacilityName>
      </mda:Arrival>
      <mda:Departure ownerProducer="USA" classification="U">
        <mda:VisitExpectedDepartureDateTime>
          <mda:DateTime>2025-12-16T00:00:00</mda:DateTime>
        </mda:VisitExpectedDepartureDateTime>
      </mda:Departure>
      <mda:LastPortOfCall ownerProducer="USA" classification="U"
access="#Roles|Group^MDA-USCG-Msn-District11-ROC">
        <mda:VisitActualArrivalDateTime>
          <nc:DateTime>2025-11-25T00:00:00</nc:DateTime>
        </mda:VisitActualArrivalDateTime>
        <mda:VisitActualDepartureDateTime>
          <mda:DateTime>2025-11-30T00:00:00</mda:DateTime>
        </mda:VisitActualDepartureDateTime>
        <mda:VisitLocationInPort>
          <m:PortName>Port of Portland, Oregon</m:PortName>

<nc:LocationCountryISO3166Alpha2Code>US</nc:LocationCountryISO316
6Alpha2Code>
          <nc:LocationStateName>OR</nc:LocationStateName>
          <nc:LocationCityName>Portland</nc:LocationCityName>
        </mda:VisitLocationInPort>
      </mda:LastPortOfCall>
```



```
      <mda:NextPortOfCallList ownerProducer="USA"
classification="U" access="#Roles|Group^MDA-USCG-Msn-District11-
ROC">
        <mda:NextPortOfCall>
          <mda:VisitExpectedArrivalDateTime>
            <nc:DateTime>2026-01-02T00:00:00</nc:DateTime>
          </mda:VisitExpectedArrivalDateTime>
          <mda:VisitExpectedDepartureDateTime>
            <nc:DateTime>2026-01-07T00:00:00</nc:DateTime>
          </mda:VisitExpectedDepartureDateTime>
          <mda:VisitLocationInPort>
            <m:PortName>Port of Long Beach</m:PortName>

<nc:LocationCountryISO3166Alpha2Code>US</nc:LocationCountryISO316
6Alpha2Code>
            <nc:LocationStateName>CA</nc:LocationStateName>
            <nc:LocationCityName>Long Beach</nc:LocationCityName>
          </mda:VisitLocationInPort>
        </mda:NextPortOfCall>
      </mda:NextPortOfCallList>
      <mda:CDCCargoList ownerProducer="USA" classification="C"
access="#Roles|Group^MDA-USCG-Msn-District11-ROC
Roles|Group^NIMS-FEMA-Msn-RegionIX-IC">
        <mda:CDCCargo>
          <m:CargoDestinationLocation>
            <nc:Address>
              <nc:LocationStateName>CA</nc:LocationStateName>

<nc:LocationCountryISO3166Alpha2Code>US</nc:LocationCountryISO316
6Alpha2Code>
            </nc:Address>
            <m:LocationAugmentation>
              <m:LocationPort>
                <m:PortCodeText>USOAK</m:PortCodeText>
                <m:PortName>Port of Oakland</m:PortName>
              </m:LocationPort>
            </m:LocationAugmentation>
          </m:CargoDestinationLocation>
          <m:CargoHazmatDeclaration>

<m:HazmatDeclarationChemicalCommonName>Pesticide</m:HazmatDeclara
tionChemicalCommonName>
            <m:HazmatDeclarationDescriptionText>Division 2.3
Poisonous Gas</m:HazmatDeclarationDescriptionText>
            <m:HazmatDeclarationMaterialAmountMeasure>
              <nc:MeasureValueText>100</nc:MeasureValueText>
              <nc:MeasureUnitText>Barrel</nc:MeasureUnitText>
            </m:HazmatDeclarationMaterialAmountMeasure>

<m:HazmatDeclarationUNHazmatCode>UN3018</m:HazmatDeclarationUNHaz
matCode>
```

```
          </m:CargoHazmatDeclaration>

<m:CargoPackagedIndicator>true</m:CargoPackagedIndicator>

<m:CargoResidueIndicator>false</m:CargoResidueIndicator>
        </mda:CDCCargo>
      </mda:CDCCargoList>
    </mda:noticeofarrival>
  </gml:featureMember>
</wfs:FeatureCollection>
```


Annex C

Results of TIEs – PEPs and OGC Attribute Store

This annex provides a sample test results from PEPs and the OGC Attribute Store.

--

Tested Component: con terra PEP
Tested Against: OGC IdP? and Attribute Server
Tester Contact:
Date of TIE: 5/18/2015

Request:

```
<?xml version="1.0" encoding="UTF-8"?>
<soap11:Envelope xmlns:soap11="http://schemas.xmlsoap.org/soap/envelope/">
    <soap11:Body>
        <saml2p:AttributeQuery
            ID="_59de63ce-9b85-480e-b0e1-5805b775babd"
            IssueInstant="2015-05-18T14:53:09.398Z" Version="2.0" xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol">
            <saml2:Issuer
                Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity" xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
            <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:SignedInfo>
                    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                    <ds:Reference URI="#_59de63ce-9b85-480e-b0e1-5805b775babd">
                        <ds:Transforms>
                            <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <ds:DigestValue>3qHt8gKeLy/70uPOFq4BYSsEM58=</ds:DigestValue>
                    </ds:Reference>
                </ds:SignedInfo>
                <ds:SignatureValue>....</ds:SignatureValue>
                <ds:KeyInfo>
                    <ds:X509Data>
                        <ds:X509Certificate>....</ds:X509Certificate>
                    </ds:X509Data>
                </ds:KeyInfo>
            </ds:Signature>
            <saml2:Subject xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
                <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">tjacobs</saml2:NameID>
            </saml2:Subject>
        </saml2p:AttributeQuery>
    </soap11:Body>
</soap11:Envelope>
```

Response:

[INSERT]

Tested Component: Secure Dimensions PEP
Tested Against: OGC IdP? and Attribute Server
Tester Contact:
Date of TIE: 5/18/2015
Request:

```
<?xml version="1.0" encoding="UTF-8"?>
<soap-env:Envelope xmlns:soap-env="http://schemas.xmlsoap.org/soap/envelope/">
    <soap-env:Header/>
    <soap-env:Body>
        <samlp:AttributeQuery
            Destination="https://geo4niem.opengeospatial.org:8443/idp/profile/SAML2/SOAP/AttributeQuery"
            ID="_7b2c94e9ceb5fefbd39a932a682e453f6c45384191"
            IssueInstant="2015-05-18T15:15:50Z" Version="2.0"
            xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
            <saml:Issuer>https://ows11.secure-dimensions.com/SP</saml:Issuer>
            <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo>
                    <ds:CanonicalizationMethod
                        Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
    <ds:SignatureMethod
                        Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
  <ds:Reference URI="#_7b2c94e9ceb5fefbd39a932a682e453f6c45384191">
                        <ds:Transforms>
                            <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <ds:DigestValue>gTIcVAbg0o3CDf7ejsrtjeX3JEI=</ds:DigestValue>
                    </ds:Reference>
                </ds:SignedInfo>
                <ds:SignatureValue>....</ds:SignatureValue>
<ds:KeyInfo>
                    <ds:X509Data>
                        <ds:X509Certificate>....</ds:X509Certificate>
                    </ds:X509Data>
                </ds:KeyInfo>
            </ds:Signature>
            <saml:Subject>
                <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">ematthews</saml:NameID>
            </saml:Subject>
        </samlp:AttributeQuery>
    </soap-env:Body>
</soap-env:Envelope>
```

Response:

[INSERT]

Annex D: Revision history

Date	Release	Editor	Primary clauses modified	Description
2013-05-14	03	J Harrison	All	Final project deliverable.
2015-05-26	04	J Harrison	All	Abstract, Introduction, Graphics, and Findings updated based on TB11 test and demo activities
2015-07-17	05	J Harrison	All	Incorporated edits from Testbed 11 Participants and Sponsors
2015-09-19	051	J Harrison	All	Incorporated edits from Testbed 11 Participants and Sponsors
2015-10-12	052	J Harrison	All	Incorporated edits from Testbed 11 Participants and Sponsors
2015-10-21		Carl Reed	Various	Preparation for publication.